Algebraic Tori in Cryptography

by

Nicholas Charles Alexander

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 2005

Author's declaration for electronic submission of a thesis

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Communicating bits over a network is expensive. Therefore, cryptosystems that transmit as little data as possible are valuable. This thesis studies several cryptosystems that require significantly less bandwidth than conventional analogues. The systems we study, called torus-based cryptosystems, were analyzed by Karl Rubin and Alice Silverberg in 2003 [RS03]. They interpreted the XTR [LV00] and LUC [SL93] cryptosystems in terms of quotients of algebraic tori and birational parameterizations, and they also presented CEILIDH, a new torus-based cryptosystem. This thesis introduces the geometry of algebraic tori, uses it to explain the XTR, LUC, and CEILIDH cryptosystems, and presents torus-based extensions of van Dijk, Woodruff, et al. [vDW04, vDGP^{+}05] that require even less bandwidth. In addition, a new algorithm of Granger and Vercauteren [GV05] that attacks the security of torus-based cryptosystems is presented. Finally, we list some open research problems.

Acknowledgments

I wish to thank my supervisors, Edlyn Teske and Alfred Menezes, for their time and efforts on my behalf. I could not have asked for better supervision. In addition, I thank Rob Granger and Isabelle Dechene for their feedback.

Dedication

To my parents, Ros and Gordon, for all that they have done for me.

Nomenclature

$\mathbb{A}^1$	Affine space: $\mathbb{A}^1(k) \cong k$	10
$\mathbb{G}_m$	The general multiplicative group: $\mathbb{G}_m(k) \cong k^\times$	10
$\mathbb{N}_H$	Norm maps defined in terms of Galois groups $H \subset G$.	18
$\mathbb{S}_{i,F}$	The i-th symmetric map $\mathbb{S}_{i,F} : \operatorname{Res}_{L/F} \mathbb{A}^1 \xrightarrow{\sim} \mathbb{A}^{\mathrm{Gal}(L/F)} \longrightarrow \mathbb{A}^1$.	23
$\mathbb{T}_G$	The norm-1 torus viewed in terms of the Galois group G.	20
$\mathcal{A}_L$	The Weil restriction of affine space: $\mathcal{A}_L := \operatorname{Res}_{L/k} \mathbb{A}^1$.	23
$\mathcal{G}_L$	The Weil restriction of the multiplicative group: $\mathcal{G}_L := \operatorname{Res}_{L/k} \mathbb{G}_m$.	23
$\mathcal{N}_{L/F}$	Norm maps defined for Weil restrictions of varieties.	25
$\mathcal{S}_{\text{traces}}$	The set of XTR traces viewed as a variety.	35
$\mathcal{S}_{i,F}$	The i-th symmetric map $\mathcal{S}_{i,F} : \mathcal{A}_L \xrightarrow{\sim} \mathcal{A}_F$.	24
$\mathcal{T}_L$	The norm-1 torus viewed as a variety.	25
$\mathcal{T}r_{L/F}$	Trace maps defined for Weil restrictions of varieties.	25
$\mathcal{X}_F$	The image of $\mathcal{T}_L$ in $\mathcal{G}_L/\Sigma_H$	43
μ	The Möbius function.	72
$\Phi_n(x)$	The n-th cyclotomic polynomial.	2

Σ_S The group of permutations rearranging the set S. 41

$\mathrm{Gal}(L/k)$ The Galois group of L over k. 11

$\mathrm{Res}_{L/k}$ The restriction of scalars from L to k. 11

$\varphi(n)$ The Euler totient function. 2

$A(X)$ The coordinate ring of the affine variety X. 45

C_N The cyclic group of order N. 20

$G_{q,n}$ The primitive subgroup of order $\Phi_n(q)$ of $\mathbb{F}_{q^n}^\times$. 8

$k(X)$ The function field of the variety X. 46

$L_n(\alpha, c)$ $L_n(\alpha, c) = \exp\left((c + o(1))(\ln n)^\alpha (\ln\ln n)^{1-\alpha}\right)$. 98

$N_{L/F}$ The field norm map $N_{L/F}(x) = \prod_{\sigma \in \mathrm{Gal}(L/F)} \sigma(x)$. 4

s_i The i-th symmetric polynomial. 23

S_{traces} The set of XTR traces viewed as a subset of $\mathbb{F}_{q^6}^\times$. 35

$T_n(\mathbb{F}_q)$ The norm-1 torus viewed as a subgroup of $\mathbb{F}_{q^n}^\times$. 8

V^G The G-conjugates of the variety V. 10

W_d The repeated divisor preventing $T_m(\mathbb{F}_{q^d}) \cong \prod_{e|d} T_{me}(\mathbb{F}_q)$. 79

${\Sigma_H}'$ The permutations that preserve the norm-1 torus $\mathbb{T}_G$. 42

rational A variety V is rational if $V \cong \mathbb{A}^d$ for some integer d. 55

stably rational A variety V is stably rational if $V \times \mathbb{A}^D \cong \mathbb{A}^E$ for integers D, E. 72

t The "trace map" of XTR, $t : (\mathbb{A}^{\mathrm{Gal}(L/F)})^3 \longrightarrow \mathbb{A}^{\mathrm{Gal}(L/F)}$. 37

torus An algebraic group V is an algebraic torus if $V \cong \mathbb{G}_m^d$ for some integer d. 26

Contents

List of Figures

Chapter 1

Introduction

Communicating bits over a network is expensive. Therefore, cryptosystems that transmit as little data as possible are valuable. However, there is a trade-off: the smaller the amount of information communicated, the easier it is for an attacker to compromise system security. This thesis presents a series of cryptosystems that achieve security levels comparable to "conventional" cryptosystems, while requiring significantly less bandwidth — they transmit only about 1/3 the bits of traditional analogues[1].

A common "conventional" cryptosystem is the textbook Diffie-Hellman protocol for key exchange [DH76, MvOV96]. The Diffie-Hellman protocol operates in a subgroup of the multiplicative group of a finite field $\mathbb{F}_{q^n}^\times$, and as such transmits elements of $\mathbb{F}_{q^n}^\times$. These elements can be represented as polynomials in $\mathbb{F}_q[x]$ of degree less than n, and these polynomials can be represented as list of coefficients in $\mathbb{F}_q$. These coefficients are in turn represented as an integer between 0 and $q-1$. It follows that each finite field element transmitted by the textbook Diffie-Hellman protocol requires

$$n \log q$$

bits to communicate.

The security of the textbook Diffie-Hellman protocol relies on the presumed intractability of the following computational problem[2]:

[1] The cryptosystems presented have low bandwidth requirements, but are all inefficient relative to the information-theoretic bound.

[2] More precisely, the textbook Diffie-Hellman protocol relies on the Diffie-Hellman problem, but for

Discrete Logarithm Problem (DLP) in a finite field. Let $g \in \mathbb{F}_{q^n}^{\times}$ and $h \in \langle g \rangle$ be given. The problem is to find an integer x such that $h = g^x$.

Clearly, the discrete logarithm problem (DLP) is computationally feasible in finite fields of small size, so in order for the textbook Diffie-Hellman protocol to be secure, the bit-size of the field,

$$n \log q$$

must be large. Since the textbook Diffie-Hellman protocol transmits finite fields elements, field sizes large enough to ensure cryptographic security also increase the cost of bandwidth significantly.

Torus-based cryptosystems improve on conventional cryptosystems by representing some elements of large finite fields compactly, and therefore they transmit fewer bits. A working definition of the elements that are compactly represented is:

Working definition of the norm-1 torus. The norm-1 torus $T_n(\mathbb{F}_q)$ is the subgroup of $\mathbb{F}_{q^n}^{\times}$ of order $\Phi_n(q)$, where $\Phi_n(x)$ denotes the n-th cyclotomic polynomial[3].

Since

$$\deg \Phi_n(x) = \varphi(n),$$

where $\varphi(n)$ denotes the Euler totient function, the norm-1 torus $T_n(\mathbb{F}_q)$ has order roughly $q^{\varphi(n)}$. Therefore, any representation requires at least

$$\varphi(n) \log q$$

bits to represent all $T_n(\mathbb{F}_q)$.

The XTR cryptosystem [LV00] is an example of a cryptosystem that compactly represents the elements of the norm-1 torus $T_6(\mathbb{F}_q) \subset \mathbb{F}_{q^6}^{\times}$. Elements of $\mathbb{F}_{q^6}^{\times}$ usually require

$$6 \log q$$

bits to represent, but XTR achieves a representation requiring only

$$2 \log q$$

simplicity we will assume the Diffie-Hellman problem and the discrete logarithm problem are equivalent. See [MvOV96] for a complete discussion.

[3] More precisely, $T_n(\mathbb{F}_q)$ is the $\mathbb{F}_q$-rational points of the norm-1 torus; see Chapter 2.

bits. (Note that $\varphi(6) = 2$.) Using this compact representation, the XTR analogue of textbook Diffie-Hellman transmits only

$$1/3$$

the number of bits that the conventional key agreement scheme transmits. Moreover, the security of XTR depends on the same DLP in $\mathbb{F}_{q^n}^\times$ that textbook Diffie-Hellman depends on. In general, all the torus-based cryptosystems give a compact representation of the norm-1 torus

$$T_n(\mathbb{F}_q) \subset \mathbb{F}_{q^n}^\times$$

using only

$$\varphi(n) \log q$$

bits, while achieving comparable security to the surrounding finite field multiplicative group $\mathbb{F}_{q^n}^\times$. This reduction in bandwidth costs makes torus-based cryptosystems attractive in bandwidth constrained environments. (In fact, the results of Granger and Vercauteren, considered in Chapter 6, show that the systems are closely linked.)

1.1 Perspective of this thesis

We emphasize the geometry of algebraic tori throughout, and, to avoid lengthy exposition, it is assumed that the reader has some knowledge of algebraic geometry. Specifically, we assume the reader is familiar with affine varieties, morphisms of varieties, rational maps, and birational equivalence, and suggest [Ful69, Har95] for reference. The motivation for this perspective comes from the major conjecture in the study of algebraic tori in cryptography. Voskresenskii's Conjecture (Conjecture 4.2) is a geometric question, and we feel it is most likely that it will be answered with the tools of algebraic geometry. Therefore, we use the language and elementary techniques of the field without reservation. At the same time, we have tried to present the ideas simply, which has entailed the loss of some mathematical rigor.

1.2 Structure of this thesis

Much of this thesis is devoted to understanding the XTR cryptosystem. The LUC [SL93] and XTR [LV00] cryptosystems were introduced, in 1993 and 2000 respectively, entirely in terms of the order $\Phi_n(q)$ subgroup of a finite field $\mathbb{F}_{q^n}^\times$. The interpretation of LUC and XTR in terms of algebraic tori was given much later, in 2003, by Karl Rubin and Alice Silverberg [RS03, RS04a]. They recognized that the order $\Phi_n(q)$ subgroup of $\mathbb{F}_{q^n}^\times$ corresponds to the $\mathbb{F}_q$-rational points of a certain geometric object, called a norm-1 torus. Therefore, the first thing this thesis does is develop the geometry of norm-1 tori. Chapter 2 shows that the order $\Phi_n(q)$ subgroup of $\mathbb{F}_{q^n}^\times$ contains the elements of $\mathbb{F}_{q^n}^\times$ that have norm[4] unity down to every proper subfield of $\mathbb{F}_{q^n}$, and then uses the theory of Weil restriction of scalars to lift the finite field norm maps that define $T_n(\mathbb{F}_q)$ to maps that define an algebraic variety. Finally, the connection between the order $\Phi_n(q)$ subgroup of $\mathbb{F}_{q^n}^\times$ and the literature surrounding algebraic tori is established.

Using their geometric perspective, Rubin and Silverberg interpreted the LUC and XTR cryptosystems in terms of maps giving explicit rational parameterizations of special quotients of norm-1 tori. Chapter 3 uses the geometry of norm-1 tori presented in Chapter 2 to understand this interpretation of XTR[5]. It exploits the lifted norm maps and the geometric definition of the order $\Phi_6(q)$ subgroup of $\mathbb{F}_{q^6}^\times$ to define a group action of S_3 on the norm-1 torus $T_6(\mathbb{F}_q)$ that correspond to the trace map used by XTR, and then explains the role of the trace map in XTR as a birational parameterization of a quotient of the norm-1 torus.

Rubin and Silverberg also introduced a new cryptosystem, called CEILIDH, based entirely on birational parameterizations of algebraic tori. Like XTR, CEILIDH represents elements of $T_6(\mathbb{F}_q) \subset \mathbb{F}_{q^6}^\times$ using only $2\log q$ bits. Unlike XTR, however, CEILIDH is not easily understood in terms of finite field arithmetic; a purely geometric development is most natural. Chapter 4 gives such a presentation of CEILIDH, and shows that rational norm-1 tori yield compact representations suitable for cryptographic application.

Together, Chapters 3 and 4 explain Figures 1.1 and 1.2, graphically depicting the XTR and CEILIDH cryptosystems.

The reduction in bandwidth, by a factor of 3, that XTR achieved in 2000, and that

[4] By norm, we mean the field norm map $N_{L/F}(x) = \prod_{\sigma \in \mathrm{Gal}(L/F)} \sigma(x)$.

[5] LUC can be seen as a simplified XTR, so we only present the XTR cryptosystem.

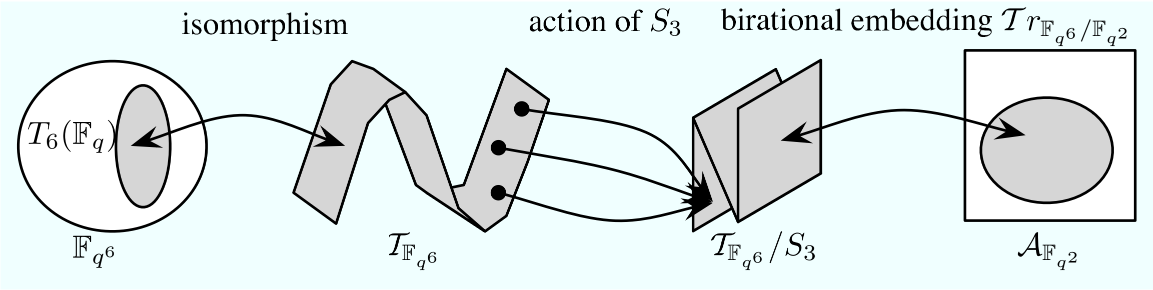

isomorphism
action of S_3
birational embedding $\mathcal{T}r_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}$
$T_6(\mathbb{F}_q)$
$\mathbb{F}_{q^6}$
$\mathcal{T}_{\mathbb{F}_{q^6}}$
$\mathcal{T}_{\mathbb{F}_{q^6}}/S_3$
$\mathcal{A}_{\mathbb{F}_{q^2}}$

Figure 1.1: The geometry of the XTR cryptosystem is explained in Chapter 3.

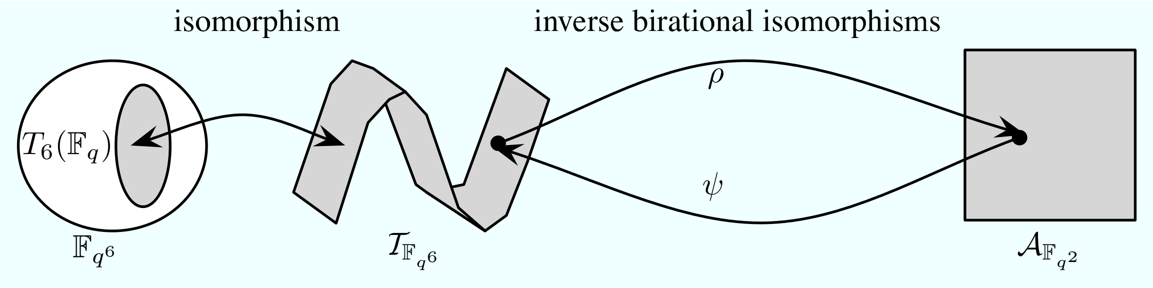

isomorphism
inverse birational isomorphisms
ρ
ψ
$T_6(\mathbb{F}_q)$
$\mathbb{F}_{q^6}$
$\mathcal{T}_{\mathbb{F}_{q^6}}$
$\mathcal{A}_{\mathbb{F}_{q^2}}$

Figure 1.2: The geometry of the CEILIDH cryptosystem is explained in Chapter 4.

CEILIDH matched in 2003, was the best compression ratio known until 2004, when van Dijk and Woodruff [vDW04] generalized the ideas of CEILIDH. They introduced new torus-based cryptosystems with protocols that represent elements of $\mathbb{F}_{q^{30}}^{\times}$ using only

$$\varphi(30)\log q = 8\log q$$

bits[6]. It follows that these cryptosystems achieve the superior compression ratio

$$30/\varphi(30) = 30/8 = 3.75.$$

Chapter 5 develops the theory of stably rational tori, a class larger than the class of rational tori exploited by CEILIDH. We show how these stably rational tori are exploited in the improved T_{30} cryptosystem of van Dijk, Woodruff, et al [vDGP$^+$05] to achieve compression better than both XTR and CEILIDH.

[6] The new cryptosystems achieve superior compression ratios as the number of torus elements transmitted tends to infinity; see Chapter 5 for a thorough discussion.

Chapter 6 embeds the geometry of tori into the world of cryptography, showing how to use the results of the preceding chapters. Practical issues, such as protocols, parameter selection, and reductionist security arguments, are considered. Finally, Chapter 6 counters the constructive uses of tori presented in Chapters 3 through 5 by presenting some of the first destructive uses of algebraic tori in cryptography. Specifically, the algorithms of Granger and Vercauteren [GV05] exploiting the rational geometry of norm-1 tori to attack the DLP in algebraic tori are presented.

We conclude with some open questions and directions for future research in Chapter 7.

1.3 Contributions of this thesis

This thesis synthesizes a large body of published research into a consistent framework, emphasizing the role of the geometry of tori in cryptography. It does not contain new results.

It does contain several original examples that help to make the constructions presented concrete. Many of these examples clarify the bewildering array of notation introduced in the original research publications, and this exposition will save the reader the effort of decryption. In addition, Example 4.8 is an original construction of independent value.

The exposition of Chapter 5 sets down most of the proofs omitted in van Dijk et al [vDGP$^+$05], and provides independent verification of those results.

This thesis also contains many figures graphically detailing the constructed maps, which help the reader understand the cryptosystems considered. The figures above, which contrast the XTR and CEILIDH cryptosystems, are representative examples, because they clearly show the key geometric difference between XTR and CEILIDH. We believe these figures will be of considerable benefit to readers first approaching this material.

Chapter 2

Algebraic tori

In this chapter, we introduce algebraic tori, the mathematical objects that Rubin and Silverberg use to study the XTR cryptosystem and to construct the CEILIDH cryptosystem [RS03, RS04a]. We first present three equivalent characterizations of certain algebraic groups called norm-1 tori, and use these characterizations to better understand norm-1 tori. Then we prove that the groups we call "norm-1 tori" are in fact algebraic tori, a well-studied class of geometric objects. This gives the geometric insight into norm-1 tori that Rubin and Silverberg exploit.

This chapter presents much of the material found in [RS03] and [RS04a], but our presentation differs significantly. Several examples support the material, and overall our presentation is much less dense.

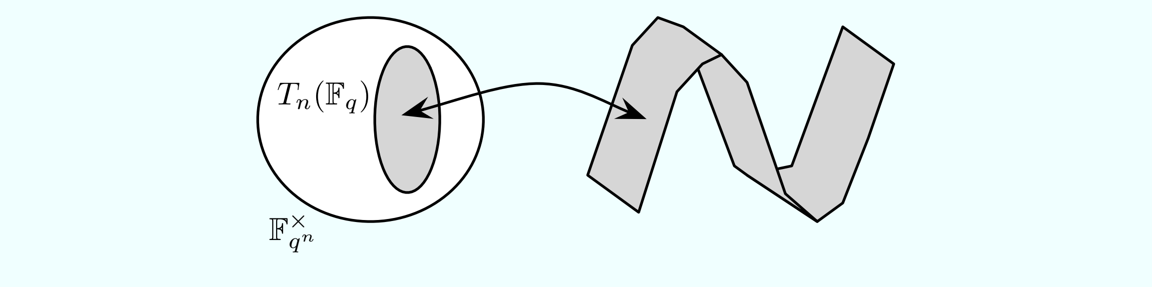


Figure 2.1: We present a geometric interpretation of $T_n(\mathbb{F}_q)$, the order $\Phi_n(q)$ subgroup of $\mathbb{F}_{q^n}^\times$.

2.1 An algebraic representation of norm-1 tori

Let q be a prime power, and let n be a positive integer. Since the n-th cyclotomic polynomial $\Phi_n(q)$ divides $|\mathbb{F}_{q^n}^\times| = q^n - 1$, there always exists a subgroup of $\mathbb{F}_{q^n}^\times$ of order $\Phi_n(q)$.

Definition 2.1. *Let $G_{q,n}$ be the order $\Phi_n(q)$ subgroup of $\mathbb{F}_{q^n}^\times$.*

We call $G_{q,n}$ the primitive subgroup of $\mathbb{F}_{q^n}$, since we later show that $G_{q,n}$ does not embed into any proper subfield of $\mathbb{F}_{q^n}^\times$ (Theorem 6.2).

Observe that the subgroup used in the XTR cryptosystem is the special case $G_{q,6}$ with $n = 6$ [LV00]; henceforth, we will consider the general case with n not necessarily 6.

The following theorem describes the norm-1 torus algebraically, equating it with the primitive subgroup $G_{q,n}$.

Theorem 2.2. *[RS03, Lemma 7] (Algebraic characterization of the norm-1 torus.) Define the set of elements of norm 1 down to every proper subfield to be*

$$T_n(\mathbb{F}_q) = \{x \in \mathbb{F}_{q^n}^\times : N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(x) = 1 \, \text{for each} \, d|n, d < n\}.$$

Then $T_n(\mathbb{F}_q) = G_{q,n}$.

Proof. For each $d|n$, the subfield norm map is a multiplicative homomorphism, from which it follows that $T_n(\mathbb{F}_q)$ is a subgroup of $\mathbb{F}_{q^n}^\times$. Since $\mathbb{F}_{q^n}^\times$ is a cyclic group, the theorem will follow if we show $T_n(\mathbb{F}_q)$ has group order $\Phi_n(q)$. Let c denote $|T_n(\mathbb{F}_q)|$. For a subfield $\mathbb{F}_{q^d}$, the Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^d})$ is generated by the d-th power Frobenius map $x \mapsto x^{q^d}$, and thus for $x \in T_n(\mathbb{F}_q)$, we have that

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(x) = x^{q^d} \cdot x^{q^{2d}} \cdots x^{q^n} = x^{(q^n-1)/(q^d-1)} = 1.$$

Hence $c|(q^n - 1)/(q^d - 1)$ for each $d|n$, and we have

$$c| \gcd \left\{ \frac{q^n - 1}{q^d - 1} : d|n \, \text{and} \, d < n \right\}.$$

Recalling the decomposition $x^m - 1 = \prod_{e|m} \Phi_e(x)$ [LN94, Theorem 2.45], we see that $c|\Phi_n(q)$.

There exist polynomials $f_d(t) \in \mathbb{Z}[t]$ such that

$$\sum_{d|n, d<n} f_d(t) \frac{t^n - 1}{t^d - 1} = \Phi_n(t);$$

for a proof, consult [dB53, Theorem 1], or [Sch64, Theorem 2]. It follows that $\Phi_n(q) | \gcd\{(q^n - 1)/(q^d - 1) : d|n \text{ and } d < n\}$. But this means $\Phi_n(q)|c$, and thus $c = \Phi_n(q)$. It follows that $T_n(\mathbb{F}_q) = G_{q,n}$. □

We have shown that the subgroup $G_{q,n}$ of order $\Phi_n(q)$ is the collection of finite field elements that satisfy the strong algebraic "norm-1" property. We call $T_n(\mathbb{F}_q)$ the norm-1 torus partly because all its elements have norm unity down to each subfield, but we must wait until Section 2.4 to understand why we call $T_n(\mathbb{F}_q)$ a "torus". However, we have provided our first representation of norm-1 tori.

2.2 Weil restriction of scalars

Now that we have demonstrated an algebraic characterization of the primitive subgroup of $\mathbb{F}_{q^n}^\times$, we turn to providing a geometric characterization. First, we study the process of "restriction of scalars", and then we introduce geometric norm and trace maps that allow Rubin and Silverberg to identify the norm-1 torus $T_n(\mathbb{F}_q)$ with an algebraic variety.

In this section, let L be a finite separable extension of k. Consider an algebraic variety V defined over L. To what extent does the large field L determine the variety V? Is there a variety defined over the small field k that is, in some sense, equivalent to V? André Weil asked if there is a variety W defined over k such that V is birational to W, and he answered his question affirmatively in [Wei58]. Figure 2.2 depicts the situation.

We denote the restricted variety W by $\operatorname{Res}_{L/k} V$, and we say that $\operatorname{Res}_{L/k} V$ is the "Weil restriction of scalars of V from L down to k", or, if there is no ambiguity, just the "Weil restriction of V". (For an exposition in the language of schemes, see [Vos98, Section 3.12].)

2.2.1 Definitions

First, the following varieties are fundamental.

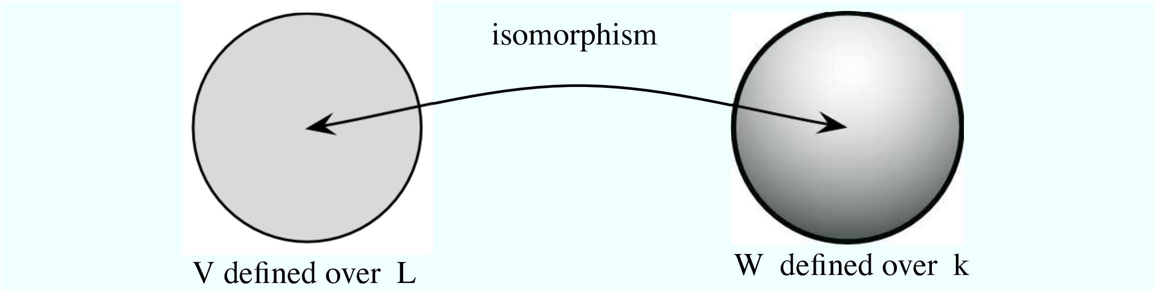


Figure 2.2: W is the "restriction of scalars from L to k" of V.

Definition 2.3. *Denote affine space by $\mathbb{A}^1$, and denote the general multiplicative group by $\mathbb{G}_m$. We have*

$$\mathbb{A}^1(k) \cong k$$

and

$$\mathbb{G}_m(k) \cong k^\times.$$

To consider the properties of the Weil restriction variety $\operatorname{Res}_{L/k} V$, we need some notation.

Definition 2.4. *Let V be a variety and G a finite set. Write*

$$V^G := \bigoplus_{\sigma \in G} V,$$

where $\oplus$ denotes direct sum: $A \oplus B = \{(a, b) : a \in A, b \in B\}$.

Remark 2.5. We notate an element $x \in V^G$ as

$$x = (\ldots, x_\sigma, x_\tau, \ldots) = (x_e, \sigma(x_\sigma), \tau(x_\tau), \ldots) = (x_\sigma)_{\sigma \in G},$$

where each element x_σ is a distinct point in the variety V (and thus may have multiple components itself). To be clear, x_σ is not necessarily equal to x_τ.

We understand σ and τ to range over G in the first and second notations.

Finally, observe that V^G is itself a variety.

This notation makes it easy to discuss Galois actions, because there is natural group action defined on V^G that can be interpreted as a Galois action.

Definition 2.6. *If G is a group, G acts on V^G by permuting indices.*

For example, if $G = \{e, g, g^2\}$ is the cyclic group of order three and V is a variety, then

$$g(x_e, x_g, x_{g^2}) = (x_{eg}, x_{gg}, x_{gg^2}) = (x_g, x_{g^2}, x_e) \in V^G.$$

Definition 2.7. *Let L extend the field k. Denote the Galois group of L over k by*

$$\mathrm{Gal}(L/k).$$

The following theorem, a modification of a theorem stated by Rubin and Silverberg, provides the technical tools we need.

Theorem 2.8. *[RS04a, Proposition 2.2] Let L/k be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/k)$. Let V be an affine variety defined over L. Then there exists an affine variety $\mathrm{Res}_{L/k} V$ defined over the base field k such that*

i. *there is a bijection between the sets of points*

$$(\mathrm{Res}_{L/k} V)(k) \xrightarrow{\sim} V(L);$$

ii. *there are projections*

$$\pi_\sigma : \mathrm{Res}_{L/k} V \longrightarrow V,$$

for each $\sigma \in G$, with each π_σ a morphism defined over L, such that the direct sum

$$\oplus\pi_\sigma : \mathrm{Res}_{L/k} V \xrightarrow{\sim} V^G$$

is an isomorphism defined over L;

iii. *there is a group action of G on $\mathrm{Res}_{L/k} V$ that is compatible with the isomorphism above, ie there is a commutative diagram*

$$\begin{tikzcd}
\mathrm{Res}_{L/k} V \arrow[r, "\sim"] \arrow[d, "G"'] & V^G \arrow[d, "G"] \\
\mathrm{Res}_{L/k} V \arrow[r, "\sim"] & V^G
\end{tikzcd}$$

with the left vertical map the natural action of G point-wise on $\mathrm{Res}_{L/k} V$, and the right vertical map the action of G on V^G described in Definition 2.4.

2.2.2 The realification of the complex numbers

Let us consider some of the details of Theorem 2.8. We motivate the first part of the theorem by considering the "realification" of the complex numbers, which we consider as the affine variety $\mathbb{A}^1(\mathbb{C})$. We seek a variety $W = \operatorname{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{A}^1$ such that the $\mathbb{C}$-rational points $\mathbb{A}^1(\mathbb{C})$ are isomorphic to the $\mathbb{R}$-rational points $W(\mathbb{R})$. This perspective is natural: we normally express a complex number z in terms of the basis $\{1, i\}$, so that $z = a + bi$, with both components a and b real numbers and i a square root of -1. Therefore, we normally identify the complex numbers with two copies of the real numbers. Hence, $\mathbb{A}^1(\mathbb{C}) = \mathbb{A}^2(\mathbb{R})$, and it is clear that $\mathbb{A}^1$ over $\mathbb{C}$ is isomorphic to $W = \mathbb{A}^2$ over $\mathbb{R}$ (the isomorphism being defined over $\mathbb{C}$).

The fundamental step in the identification above is fixing a basis for $\mathbb{C}$ as an extension of $\mathbb{R}$, and this identification generalizes to finite extensions of a base field. (We do not consider extensions that are not finitely generated.) Let us push further. Consider an affine variety V presented as the zero locus of a set (finite, by the Hilbert Basis Theorem [J99, Theorem 6.3.5]) of polynomial equations. Suppose that V is defined over L, a finite extension of k, and that $\{\alpha_1, \ldots, \alpha_j\}$ is a basis for L over k. Then for each point

$$(x_1, \ldots, x_r) \in V$$

in the variety V, there is a unique decomposition

$$(c_{11}\alpha_1 + c_{12}\alpha_2 + \cdots + c_{1j}\alpha_j, \ldots, c_{r1}\alpha_1 + c_{r2}\alpha_2 + \cdots + c_{rj}\alpha_j) \in V$$

inherited from the underlying field. We use this decomposition to construct a variety W with the desired properties by considering the polynomial equations defining V as equations relating the basis elements α_i. The following example clarifies.

Example 2.9. Consider the variety $V = V(z^2 + 1)$, and let $L = \mathbb{C}$ and $k = \mathbb{R}$. In this case, we have $V(\mathbb{C}) = \{i, -i\}$. We seek a variety W such that $V(\mathbb{C}) \cong W(\mathbb{R})$. Fixing the standard basis $\{1, i\}$ of $\mathbb{C}$ over $\mathbb{R}$, we write an element of V as $z = a + bi$, with both a and b real. The equation $z^2 + 1 = 0$ can be written as $(a + bi)(a + bi) + 1 = 0$, which expands to the simultaneous equations

$$\begin{aligned} a^2 - b^2 + 1 &= 0 \\ 2ab &= 0. \end{aligned}$$

Denote by W the zero locus of these equations. Since $2ab = 0$, one of a and b is 0. If $b = 0$, there are no real solutions to $a^2 + 1 = 0$; if $a = 0$, there are two solutions, $b = 1$ and $b = -1$. Thus $W(\mathbb{R}) = \{(0,1), (0,-1)\}$, and we can identify $(0,1) \longleftrightarrow i$ and $(0,-1) \longleftrightarrow -i$, as expected.

The bijections between $V(\mathbb{C})$ and $W(\mathbb{R})$ are:

$$\begin{array}{ccc} V(\mathbb{C}) & \longrightarrow & W(\mathbb{R}) \\ a + bi & \longmapsto & (a,b) \end{array}$$

$$\begin{array}{ccc} W(\mathbb{R}) & \longrightarrow & V(\mathbb{C}) \\ (a,b) & \longmapsto & a + bi. \end{array}$$

Remark 2.10. We make the following observations. First, the bijections are defined over the complex numbers; second, the maps depend on the choice of basis for L over k; and third, the maps between $V(\mathbb{C})$ and $W(\mathbb{R})$ are the restriction of the maps between $\mathbb{A}^1(\mathbb{C})$ and $\mathbb{A}^2(\mathbb{R})$ discussed earlier.

Example 2.11. Consider the restriction of scalars, from $\mathbb{F}_{2^3}$ down to $\mathbb{F}_2$, of the variety $\mathbb{G}_m$. For concreteness, let w be a solution to $t^3 + t + 1 = 0$ over $\mathbb{F}_2$, so that $\{1, \omega, \omega^2\}$ is a basis for $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$.

The variety $\mathbb{G}_m$ can be represented as the zero locus $V(xy = 1)$. With this description, it is easy to see that

$$\mathbb{G}_m(\mathbb{F}_{2^3}) = \left\{ \begin{array}{l} (1,1), \\ (\omega, \omega^2 + 1), (\omega + 1, \omega^2 + \omega), (\omega^2 + \omega + 1, \omega^2), \\ (\omega^2 + 1, \omega), (\omega^2 + \omega, \omega + 1), (\omega^2, \omega^2 + \omega + 1) \end{array} \right\}.$$

Expressing $x = x_0 + \omega x_1 + \omega^2 x_2$ and $y = y_0 + \omega y_1 + \omega^2 y_2$, the equation $xy = 1$ is equivalent to $(x_0 + \omega x_1 + \omega^2 x_2)(y_0 + \omega y_1 + \omega^2 y_2) = 1$. (Each coefficient x_i, y_i is in $\mathbb{F}_2$.) This system is equivalent to the following system of equations that compares powers of ω:

$$\begin{array}{rcl} x_0y_0 + x_2y_1 + x_1y_2 & = & 1 \\ x_1y_0 + x_0y_1 + x_2y_1 + x_1y_2 + x_2y_2 & = & 0 \\ x_2y_0 + x_1y_1 + x_0y_2 + x_2y_2 & = & 0. \end{array}$$

The solution set, over $\mathbb{F}_2$, is:

$$(\operatorname{Res}_{\mathbb{F}_{2^3}/\mathbb{F}_2} \mathbb{G}_m)(\mathbb{F}_2) = \left\{ \begin{array}{l} ((1,0,0),(1,0,0)), \\ ((0,1,0),(1,0,1)),((1,1,0),(0,1,1)),((1,1,1),(0,0,1)), \\ ((1,0,1),(0,1,0)),((0,1,1),(1,1,0)),((0,0,1),(1,1,1)) \end{array} \right\},$$

where we notate a solution $((x_0,x_1,x_2),(y_0,y_1,y_2))$. Observe that there is a bijection of sets

$$\mathbb{G}_m(\mathbb{F}_{2^3}) \xrightarrow{\sim} (\operatorname{Res}_{\mathbb{F}_{2^3}/\mathbb{F}_2} \mathbb{G}_m)(\mathbb{F}_2).$$

2.2.3 Weil restriction and Galois actions

The second and third parts of Theorem 2.8 describe an isomorphism between the Weil restriction of V and several copies of V [Wei58]. We now consider this perspective.

Let $G = \operatorname{Gal}(L/k)$. We will show that the set V^G has a natural interpretation as the variety V and its Galois conjugates. For an element σ of G, we will sometimes write the Galois conjugates, under the action of σ, of the points of the variety V as

$$V^\sigma = \{\sigma(x) : x \in V\}.$$

With this notation, we can express the complete set of Galois conjugates of points on the variety V as

$$V^G = \bigoplus_{\sigma\in G} V \cong \bigoplus_{\sigma\in G} V^\sigma.$$

Thus Theorem 2.8 is telling us that the Weil restriction of scalars $\operatorname{Res}_{L/k} V$ is managing the Galois conjugates of V. Since the Galois conjugates of V are determined by the extension L over k, $\operatorname{Res}_{L/k} V$ is encoding the structure of the underlying fields of definition, as well as the interplay between them and the variety V.

To demonstrate this “structure encoding”, let us continue the “realification” of the complex numbers that we began in Section 2.2.2. (For an exposition in the language of schemes, see [Vos98, p. 40].)

Example 2.12. Let $L = \mathbb{C}$ and $k = \mathbb{R}$, and consider the variety $V = \mathbb{A}^1$. Theorem 2.8 tells us that

$$\operatorname{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{A}^1 \cong \mathbb{A}^G,$$

with $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Since $G = \{e, \sigma\}$, with σ the automorphism of $\mathbb{C}$ fixing $\mathbb{R}$ and mapping i to $-i$, we can view $\mathrm{Res}_{\mathbb{C}/\mathbb{R}} V$ as $V \oplus V^\sigma$. Recall that the $\mathbb{R}$-rational points of $\mathrm{Res}_{\mathbb{C}/\mathbb{R}} V$ are precisely those fixed by the Galois action of G. Since the natural action of G on V^G is equivalent to the action of G on V as a variety, we can describe the set of fixed points explicitly. A point $(u, \sigma(v)) \in V \oplus V^\sigma$ corresponds to a point in $(\mathrm{Res}_{\mathbb{C}/\mathbb{R}} V)(\mathbb{R})$ exactly when $\sigma(u, \sigma(v)) = (u, \sigma(v))$. The action of σ on V^G permutes the factors, so

$$\sigma(u, \sigma(v)) = (\sigma(v), u) = (\sigma(v), \sigma(\sigma(u))),$$

where the action of σ is applied twice to u in the second equality to express $(\sigma(v), \sigma(\sigma(u)))$ as an element of $V \oplus V^\sigma$. Thus, an element $(u, \sigma(v))$ is fixed by σ if and only if $u = \sigma(v)$, and there are natural bijections of sets

$$(\mathrm{Res}_{\mathbb{C}/\mathbb{R}} V)(\mathbb{R}) \xrightarrow{\sim} \{(u, \sigma(u)) : u \in V(\mathbb{C})\} \xrightarrow{\sim} \{(u, u) : u \in V(\mathbb{C})\} \xrightarrow{\sim} V(\mathbb{C}).$$

We see that the $\mathbb{R}$-rational points of $\mathrm{Res}_{\mathbb{C}/\mathbb{R}} V$ correspond exactly to the pairs consisting of a $\mathbb{C}$-rational point of V and its Galois conjugate.

Example 2.12 shows that the representation of a variety via the Weil restriction of scalars provides a natural notation for reasoning about Galois actions on varieties. Let us consider another case to gain familiarity. This time, we consider the natural Galois action on the Weil restriction constructed in Example 2.11.

Example 2.13. Let G denote $\mathrm{Gal}(\mathbb{F}_{2^3}/\mathbb{F}_2)$, and denote the 2-Frobenius σ. Recall that the points of $\mathbb{G}_m^G$ are the triples

$$\left\{(x_e, \sigma(x_\sigma), \sigma^2(x_{\sigma^2})) : x_{\mathrm{e}}, x_\sigma, x_{\sigma^2} \in \mathbb{G}_m\right\}.$$

Observe that, since x_e is not necessarily equal to x_σ, we have

$$|\mathbb{G}_m^G(\mathbb{F}_{2^3})| = |\mathbb{G}_m(\mathbb{F}_{2^3})|^3 = 7^3.$$

A point x in $\mathbb{G}_m^G$ is $\mathbb{F}_2$-rational exactly when it is fixed by G, which means that

$$x = \sigma(x) = \sigma^2(x),$$

or, when expressed as permuted tuples in $\mathbb{G}_m^G$,

$$(x_e, \sigma(x_\sigma), \sigma^2(x_{\sigma^2})) = (\sigma^2(x_{\sigma^2}), x_e, \sigma(x_\sigma)) = (\sigma(x_\sigma), \sigma^2(x_{\sigma^2}), x_e),$$

which is expressed in $\mathbb{G}_m \oplus \mathbb{G}_m^\sigma \oplus \mathbb{G}_m^{\sigma^2}$ as

$$(x_e, \sigma(x_\sigma), \sigma^2(x_{\sigma^2})) = (\sigma^2(x_{\sigma^2}), \sigma(\sigma^2(x_e)), \sigma^2(\sigma^2(x_\sigma))) = (\sigma(x_\sigma), \sigma(\sigma(x_{\sigma^2})), \sigma^2(\sigma(x_e))).$$

Equating components, we see that

$$x_e = \sigma^2(x_{\sigma^2}) = \sigma(x_\sigma),$$

and thus the point $x \in \mathbb{G}_m^G$ is $\mathbb{F}_2$-rational if it is of the form

$$x = (x_e, x_e, x_e),$$

with $x_e \in \mathbb{G}_m(\mathbb{F}_{2^3})$. Thus the bijection of sets follows:

$$\mathbb{G}_m^G(\mathbb{F}_2) \xrightarrow{\sim} \mathbb{G}_m(\mathbb{F}_{2^3}).$$

So far, we have considered the bijection between $(\operatorname{Res}_{L/k} V)(k)$ and $V(L)$, and certain aspects of the isomorphism between $\operatorname{Res}_{L/k} V$ and V^G. Unfortunately, the isomorphism of Theorem 2.8 (ii) depends on the set of distinct embeddings of L into the algebraic closure $\bar{k}$ of k [Wei58], and a complete exposition would lead us far afield. However, we can still use Theorem 2.8, and we do so to lift the norm maps that define the norm-1 torus $T_n(\mathbb{F}_q)$ over a finite field to maps that act on a general variety.

2.3 Norm maps and a geometric representation of norm-1 tori

In this section, we present the norm and trace maps of Rubin and Silverberg that lift $N_{L/F}$ and $\operatorname{Tr}_{L/F}$ to algebraic varieties. First, for each subfield $k \subseteq F \subseteq L$, we seek maps $\mathbb{N}_{L/F}$ and $\mathbb{T}r_{L/F}$ that make the following diagrams commute:

$$\begin{tikzcd} L \arrow[r, "\sim"] \arrow[d, "N_{L/F}"'] & \mathbb{A}^{\mathrm{Gal}(L/k)}(k) \arrow[d, "\mathbb{N}_{L/F}"] \\ F \arrow[r, "\sim"] & \mathbb{A}^{\mathrm{Gal}(F/k)}(k) \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} L \arrow[r, "\sim"] \arrow[d, "\mathrm{Tr}_{L/F}"'] & \mathbb{A}^{\mathrm{Gal}(L/k)}(k) \arrow[d, "\mathbb{T}r_{L/F}"] \\ F \arrow[r, "\sim"] & \mathbb{A}^{\mathrm{Gal}(F/k)}(k) \end{tikzcd} .$$

(We use the notation $\mathbb{N}_{L/F}$ and $\mathbb{T}r_{L/F}$ to remind the reader that these maps are defined over $\mathbb{A}^G$ for suitable groups G.)

Remark 2.14. Our larger goal is to present a variety $\mathcal{T}_{\mathbb{F}_{q^n}}$ that is a geometric equivalent of $T_n(\mathbb{F}_q)$. This variety has points defined over the algebraic closure $\bar{\mathbb{F}}_q$, whereas we have defined $T_n(\mathbb{F}_q)$ to be a subset of $\mathbb{F}_{q^n}^\times$. Some of our results yield full isomorphisms over $\bar{\mathbb{F}}_q$: for example,

$$\mathcal{T}_{\mathbb{F}_{q^n}} \cong \mathbb{T}_{\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)}.$$

However, in some cases we present only a bijection

$$T_n(\mathbb{F}_q) \xrightarrow{\sim} \mathcal{T}_{\mathbb{F}_{q^n}}(\mathbb{F}_q),$$

because we can reason more simply about an explicit map. These maps are the content of Theorem 2.8. For more, see Remarks 2.18 and 2.21.

2.3.1 Group theoretic norm maps

We develop geometric norm maps with the aid of norm maps given in terms of Galois groups. Recall that in Section 2.2, we showed that $\mathbb{A}^1(L)$ can be interpreted as the k-rational points of the Weil restriction $\operatorname{Res}_{L/k}\mathbb{A}^1$. The same holds for an arbitrary subfield $k \subseteq F \subseteq L$: $\mathbb{A}^1(L)$ can be interpreted as the F-rational points of the Weil restriction $\operatorname{Res}_{L/F}\mathbb{A}^1$. Thus we can consider any subfield $k \subseteq F \subseteq L$ without loss of generality. For each subfield $k \subseteq F \subseteq L$, we fix an explicit map between the F-rational points $(\operatorname{Res}_{L/F}\mathbb{A}^1)(F)$ and a subset of the tuples in $\mathbb{A}^{\mathrm{Gal}(L/F)}$, as per Example 2.12, and use this identification to build norm maps.

Definition 2.15. *Define injections by*

$$\begin{gathered}\iota_{L/F} : \mathbb{A}^1 \longrightarrow \mathbb{A}^{\mathrm{Gal}(L/F)}\\ \iota_{L/F}(x) \longrightarrow (x, \sigma(x), \ldots) = (x_e, x_\sigma, \ldots) = (\sigma(x))_{\sigma \in \mathrm{Gal}(L/F)}\end{gathered}$$

and

$$\begin{gathered}\iota_{F/k} : \mathbb{A}^1 \longrightarrow \mathbb{A}^{\mathrm{Gal}(F/k)}\\ \iota_{F/k}(x) \longrightarrow (x, \sigma(x), \ldots) = (x_e, x_\sigma, \ldots) = (\sigma(x))_{\sigma \in \mathrm{Gal}(F/k)}\end{gathered}$$

The injections $\iota_{L/F}$ and $\iota_{F/k}$ are trivial, but we emphasize that they are defined over the algebraic closure $\bar{k}$ of k.

Suppose x is an element of L, which we view as $\mathbb{A}^1(L)$. Then it is easy to see that the finite field norm map

$$N_{L/F}(x) = \prod_{\sigma \in \mathrm{Gal}(L/F)} \sigma(x)$$

can be expressed equivalently as

$$n_{L/F}((x_e, x_\sigma, \ldots) = \prod_{\sigma \in \mathrm{Gal}(L/F)} x_\sigma.$$

In other words,

$$N_{L/F}(x) = n_{L/F}(\iota_{L/F}(x)).$$

The map $n_{L/F}$ mixes representations, mapping tuples of Galois conjugates to finite field elements, and we address this in the following manner. The representation $\mathbb{A}^G$ is really encoding information about the group G; let us maintain consistency and define our norm maps in terms of subgroups H of G (for appropriate Galois groups G). Observe that this is reasonable for field norm maps, because $\mathrm{Gal}(L/F)$ is a subgroup of $\mathrm{Gal}(L/k)$. Rubin and Silverberg make the following definition.

Definition 2.16. *[RS04a, Section 2] Let H be a subgroup of an abelian group G. Define a norm map $\mathbb{N}_H$ by*

$$\mathbb{N}_H : \mathbb{A}^G \longrightarrow \mathbb{A}^{G/H}$$
$$\mathbb{N}_H((x_\sigma)_{\sigma \in G}) = \left(\prod\nolimits_{\sigma \in gH} x_\sigma\right)_{gH \in G/H}.$$

To gain familiarity with Definition 2.16, we consider a concrete example.

Example 2.17. Let $L = \mathbb{F}_{q^6}$, let $F = \mathbb{F}_{q^2}$, and let $k = \mathbb{F}_q$. Denote by σ the q-Frobenius, so that

$$G = \mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_q) = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$$

and

$$H = \mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2}) = \{e, \sigma^2, \sigma^4\}.$$

Let x be an element of L. Then

$$N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(x) = x\sigma^2(x)\sigma^4(x) \in \mathbb{F}_{q^2},$$

and, using our injection $\iota_{L/F}$,

$$\begin{aligned}\mathbb{N}_H((x,\sigma(x),\ldots,\sigma^5(x))) &= \left(\prod_{\gamma\in gH}\gamma(x)\right)_{gH\in G/H}\\ &= \left(\prod_{\gamma\in\{g,g\sigma^2,g\sigma^4\}}\gamma(x)\right)_{gH\in\{\{e,\sigma^2,\sigma^4\},\{\sigma,\sigma^3,\sigma^5\}\}}\\ &= \left(x\sigma^2(x)\sigma^4(x),\sigma(x)\sigma^3(x)\sigma^5(x)\right)\in\mathbb{A}^{\mathrm{Gal}(F/k)}.\end{aligned}$$

The resulting element of $\mathbb{A}^{\mathrm{Gal}(F/k)}$ corresponds, by the map $\iota_{F/k}$, to the finite field element $x\sigma^2(x)\sigma^4(x) \in F$, which is precisely $N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(x)$. Thus, the group theoretic norm map corresponds to the finite field norm map for elements in the field L.

Remark 2.18. It is important to note that the group theoretic norm maps $\mathbb{N}_G$ are defined for points in extension fields of L. Even though we rarely consider this explicitly, our argument that T_n is an algebraic torus (Theorem 2.36) does use this fact. (For more, see Remarks 2.14 and 2.21.)

In general, the equivalence of $\mathbb{N}_{\mathrm{Gal}(L/F)}$ and $N_{L/F}$ follows from the Fundamental Correspondence of Galois Theory [J99, Theorem 9.6.6]. The following theorem summarizes.

Theorem 2.19. *[RS04a, Section 2] Let $k \subseteq F \subseteq L$ be Galois extensions of fields. We have the following commutative diagram:*

$$\begin{tikzcd} L \arrow[r, hook] \arrow[d, "N_{L/F}"'] & \mathbb{A}^{\mathrm{Gal}(L/k)} \arrow[d, "\mathbb{N}_{\mathrm{Gal}(L/F)}"] \\ F \arrow[r, hook] & \mathbb{A}^{\mathrm{Gal}(F/k)} \end{tikzcd}.$$

We have invested this effort in equivalent group theoretic norm maps because they permit a second characterization of the norm-1 torus $T_n(\mathbb{F}_q)$: in particular, we achieve a characterization that captures the role of the Galois group of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

Definition 2.20. *[RS04a, Section 2] (Group-theoretic definition of the norm-1 torus.) Let $k \subseteq F \subseteq L$ be Galois extensions of fields, and denote* $\mathrm{Gal}(L/k)$ *by G. Then the norm-1 torus is*

$$\mathbb{T}_G := \mathrm{Ker}\left[\mathbb{G}_m^G \xrightarrow{\oplus \mathbb{N}_H} \bigoplus_{1 \neq H \subseteq G} \mathbb{G}_m^{G/H}\right],$$

where

$$\oplus_{\mathbb{N}_H}(x) = (\mathbb{N}_H(x))_{1 \neq H \subseteq G} = (\ldots, \mathbb{N}_H(x), \mathbb{N}_J(x), \ldots).$$

Two equivalent definitions are

$$\mathbb{T}_G := \bigcap_{1 \neq H \subseteq G} \mathrm{Ker}\, \mathbb{N}_H,$$

and

$$\mathbb{T}_G := \left\{x \in \mathbb{G}_m^G : \mathbb{N}_H(x) = (1)_{\sigma \in H} \,\text{for every nontrivial subgroup}\, H \,\text{of}\, G\right\}.$$

Remark 2.21. With reference to Remarks 2.14 and 2.18, we note that $\mathbb{T}_G \subset \mathbb{A}^G$ is a variety with points over the algebraic closure $\bar{k}$.

Observe that the equivalence of norm maps shown by Theorem 2.19 also demonstrates that there is a natural identification

$$\mathbb{T}_{\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)}(\mathbb{F}_q) \xrightarrow{\sim} T_n(\mathbb{F}_q).$$

To complete this section on group-theoretic norm maps, we will use them to present a simpler characterization of $\mathbb{T}_G$ (and hence of T_n). The intuition is that the norm maps $\mathbb{N}_H$ are determined by the primes dividing $|H|$, and that the power of each prime dividing $|H|$ is irrelevant. In other words, the norm of an element in $\mathbb{A}^G$ is determined completely by its norm relative to each prime order subgroup H of G.

Definition 2.22. *Denote by C_N the cyclic group of order N.*

Lemma 2.23. *[RS04a, Proposition 2.6] Let p^a be the largest power of p that divides $|G|$. Let β be an element of $\mathbb{A}^G$. Then $\mathbb{N}_{C_p}(\beta) = 1$ implies that $\mathbb{N}_{C_{p^k}}(\beta) = 1$ for every $1 \leqslant k \leqslant a$.*

Proof. Let g generate C_{p^a}, so that $g^{p^{a-k}}$ generates C_{p^k} for each $1 \leqslant k \leqslant a$. By assumption, $\mathbb{N}_{C_p}(\beta) = 1$ means that

$$\begin{aligned}
\mathbb{N}_{C_p}((\beta_\gamma)_{\gamma \in C_{p^a}}) &= \left(\prod_{x\gamma \in xC_p} \beta_{x\gamma} \right)_{xC_p \in C_{p^a}/C_p} \\
&= \left(\prod_{\ell=0}^{p-1} \beta_{xg^{\ell p^{a-1}}} \right)_{x=g^0,\ldots,g^{p^{a-1}-1}} \\
&= (1)_{x=g^0,\ldots,g^{p^{a-1}-1}}.
\end{aligned}$$

Let the induction hypothesis be that the lemma is true for all powers j less than some k; then we have

$$\begin{aligned}
\mathbb{N}_{C_{p^{k+1}}}((\beta_\gamma)_{\gamma \in C_{p^a}}) &= \left(\prod_{x\gamma \in xC_{p^{k+1}}} \beta_{x\gamma} \right)_{xC_{p^{k+1}} \in C_{p^a}/C_{p^{k+1}}} \\
&= \left(\prod_{\ell=0}^{p^{k+1}-1} \beta_{xg^{\ell p^{a-(k+1)}}} \right)_{x=g^0,\ldots,g^{p^{a-(k+1)}-1}} \\
&= \left(\prod_{\ell=0}^{p^{k+1}-1} \beta_{xg^{(qp^k+r)p^{a-k-1}}} \right)_{x=g^0,\ldots,g^{p^{a-k-1}-1}} \\
&= \left(\prod_{\ell=0}^{p^{k+1}-1} \beta_{xg^{rp^{a-k-1}}g^{qp^{a-1}}} \right)_{x=g^0,\ldots,g^{p^{a-k-1}-1}} \\
&= (1)_{x=g^0,\ldots,g^{p^{a-k-1}-1}},
\end{aligned}$$

where we have used the induction hypothesis (applied to the coset representative $xg^{rp^{a-k-1}}$) to establish the final equality. The claim follows. □

Remark 2.24. The reader may have observed that Lemma 2.23 is merely an encoding of the following observation for finite fields. For simplicity, let us work a concrete example. Consider $\mathbb{F}_{q^8}$, and let $\mathrm{Gal}(\mathbb{F}_{q^8}/\mathbb{F}_q) = \langle \sigma \rangle$. Then

$$N_{\mathbb{F}_{q^8}/\mathbb{F}_{q^2}}(x) = x\sigma^2(x)\sigma^4(x)\sigma^6(x) = (x\sigma^4(x))\sigma^2(x\sigma^4(x)).$$

It follows that if $N_{\mathbb{F}_{q^8}/\mathbb{F}_{q^4}}(x) = x\sigma^4(x) = 1$, then $\mathbb{N}_{\mathbb{F}_{q^8}/\mathbb{F}_{q^2}}(x) = 1$. In terms of Galois groups, the norm relative to the subgroup of order 2, $\mathrm{Gal}(\mathbb{F}_{q^8}/\mathbb{F}_{q^4})$, determined the norm relative to the subgroup of order 2^2, $\mathrm{Gal}(\mathbb{F}_{q^8}/\mathbb{F}_{q^2})$. Thus, this example connects the equivalent formulation of Lemma 2.23 with the algebraic properties of the finite field $\mathbb{F}_{q^n}$.

Lemma 2.23 establishes the following elegant characterization of $\mathbb{T}_G$.

Definition 2.25. *[RS04a, Proposition 2.6] Write $G = C_{p_1^{k_1}} \times \cdots \times C_{p_t^{k_t}}$, with each factor group $C_{p_i^{k_i}}$ cyclic, and having prime power order. Then two equivalent characterizations of the norm-1 torus $\mathbb{T}_G$ are*

$$\mathbb{T}_G = \{\beta \in \mathbb{G}_m^G : \mathbb{N}_{C_{p_i}}(\beta) = (1)_{\sigma\in G/C_{p_i}} \,\text{for every index}\, 1 \leqslant i \leqslant t\}$$

and

$$\mathbb{T}_G = \{\beta = (\beta_\sigma)_{\sigma\in G} : \prod_{\tau\in C_{p_i}} \beta_{\sigma\tau} = 1 \,\text{for every element}\, \sigma \in G \,\text{and index}\, 1 \leqslant i \leqslant t\}.$$

These equivalent formulations reward our search for alternative definitions of the torus.

Definition 2.25 is a fundamental piece of Rubin and Silverberg's proof that T_n is an algebraic torus (Theorem 2.36), but first we will show how they used this perspective to develop geometric norm maps.

2.3.2 Geometric norm maps

This section parallels the previous section, but has loftier goals. Not only do we seek geometric norm maps, we seek an entire family of geometric symmetric maps, of which the norm and the trace are the extreme members. (The name "symmetric map" is chosen because the maps are invariant under permutations of their arguments, like the symmetric polynomials.) The additional symmetric maps we present will feature prominently in Chapter 3.

We adopt a notational convention: varieties written in calligraphic typeface are Weil restrictions of the corresponding variety. (Scalars are always restricted to k, the base field.)

Definition 2.26. *Denote the Weil restriction of affine space by*

$$\mathcal{A}_F := \mathrm{Res}_{F/k}\,\mathbb{A}^1$$

and the Weil restriction of the multiplicative subgroup by

$$\mathcal{G}_F := \operatorname{Res}_{F/k} \mathbb{G}_m.$$

With this notation, we seek maps that make the following diagrams commute:

$$\begin{tikzcd} L \arrow[r, "\sim"] \arrow[d, "N_{L/F}"'] & \mathcal{A}_L(k) \arrow[d, "\mathcal{N}_{L/F}"] \\ F \arrow[r, "\sim"] & \mathcal{A}_F(k) \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} L \arrow[r, "\sim"] \arrow[d, "\operatorname{Tr}_{L/F}"'] & \mathcal{A}_L(k) \arrow[d, "\mathcal{T}r_{L/F}"] \\ F \arrow[r, "\sim"] & \mathcal{A}_F(k) \end{tikzcd}.$$

(Again, we use the notation $\mathcal{N}_{L/F}$ and $\mathcal{T}r_{L/F}$ to remind the reader that these maps are defined relative to $\mathcal{A}_L$ and $\mathcal{A}_F$.)

Let $k \subseteq F \subseteq L$ be finite Galois extensions, and let $G = \operatorname{Gal}(L/k)$. Let $H = \operatorname{Gal}(L/F)$, and note that H is a subgroup of G; denote the index of H in G by $\ell = [G : H]$.

We need some notation.

Definition 2.27. *Let s_i denote the i-th symmetric polynomial, where the number of indeterminates is implicit.*

Now we can define the symmetric maps.

Definition 2.28. *[RS04a, Equation (2.1)] For each index $1 \leqslant i \leqslant \ell$, define symmetric maps $\mathbb{S}_{i,F}$ by the composition*

$$\mathbb{S}_{i,F} : \operatorname{Res}_{L/F} \mathbb{A}^1 \xrightarrow{\sim} \mathbb{A}^{\operatorname{Gal}(L/F)} \longrightarrow \mathbb{A}^1,$$

where the isomorphism on the left is provided by Theorem 2.8 (ii), and the map on the right is the i-th symmetric polynomial s_i of the ℓ projection maps

$$\pi_\sigma : \mathbb{A}^{\operatorname{Gal}(L/F)} \longrightarrow \mathbb{A}^1$$

for each $\sigma \in G$, also provided by Theorem 2.8 (ii).

In other words, the map $\mathbb{S}_{i,F}$ is

$$\mathbb{S}_{i,F}(x) = s_i(\ldots, \pi_\sigma(x), \ldots) = s_i(\ldots, \sigma(x), \ldots) = s_i\left((\sigma(x))_{\sigma \in \operatorname{Gal}(L/F)}\right). \tag{2.1}$$

The following theorem shows that the maps $\mathbb{S}_{i,F}$ lift the finite field norm maps.

Theorem 2.29. *[RS04a, Proposition 2.3] Let $k \subseteq F \subseteq L$ be a finite Galois extension of fields, and let $\mathbb{S}_{i,F}$ be as in Definition 2.28. Then*

i. the maps $\mathbb{S}_{i,F}$ are defined over F, and

ii. for each $1 \leqslant i \leqslant \ell$, there is a commutative diagram

$$\begin{tikzcd}
(\operatorname{Res}_{L/F} \mathbb{A}^1)(F) \arrow[r, "\sim"] \arrow[d, "\mathbb{S}_{i,F}"'] & L \arrow[d, "s_{i,F}"] \\
\mathbb{A}^1(F) \arrow[r, "\sim"] & F
\end{tikzcd},$$

where $s_{i,F}(x)$ is the i-th symmetric polynomial evaluated on the set of Galois conjugates of x over the subfield F:

$$s_{i,F}(x) = s_i\big((\tau(x))_{\tau \in \operatorname{Gal}(L/F)}\big) .$$

Proof. The maps $\mathbb{S}_{i,F}$ are clearly invariant under the action of $\operatorname{Gal}(L/F)$, which means they are defined over F. Recall that we have the bijection of Theorem 2.8 (i),

$$(\operatorname{Res}_{L/F} \mathbb{A}^1)(F) \xrightarrow{\sim} \left\{(\sigma(x))_{\sigma \in \operatorname{Gal}(L/F)} : x \in \mathbb{A}^1(L)\right\},$$

and the injection $\iota_{L/F} : (\operatorname{Res}_{L/F} \mathbb{A}^1)(F) \xrightarrow{\sim} L$ of Definition 2.15 takes $x \longmapsto (\sigma(x))_{\sigma \in \operatorname{Gal}(L/F)}$. Evaluating the top and bottom maps shows that the diagram commutes. □

Observe that $\operatorname{Res}_{F/k} \operatorname{Res}_{L/F} \mathbb{A}^1 \cong \operatorname{Res}_{L/k} \mathbb{A}^1$, so for each subfield $F \subseteq L$, we can compose the symmetric maps $\mathbb{S}_{i,F}$ and Weil restriction to obtain maps

$$\mathcal{S}_{i,F} : \mathcal{A}_L \longrightarrow \mathcal{A}_F.$$

The preceding theorem explains why we call $\mathcal{S}_{\ell,F}$ the norm from L down to F, and $\mathcal{S}_{1,F}$ the trace of L over F. The following definition uses most of the interpretations at our disposal.

Definition 2.30. *[RS04a, Section 2] Define*

$$\begin{array}{c} \mathcal{N}_{L/F} : \mathcal{A}_L \longrightarrow \mathcal{A}_F \\ \mathcal{N}_{L/F}(x) = \mathbb{S}_{\ell,F}((x_\sigma)_{\sigma \in \operatorname{Gal}(L/F)}) = s_\ell(\ldots, \sigma(x), \ldots) = \prod_{\sigma \in \operatorname{Gal}(L/F)} \sigma(x) \end{array},$$

and

$$\begin{array}{c} \mathcal{T}r_{L/F} : \mathcal{A}_L \longrightarrow \mathcal{A}_F \\ \mathcal{T}r_{L/F}(x) = \mathbb{S}_{1,F}((x_\sigma)_{\sigma\in \mathrm{Gal}(L/F)}) = s_1(\ldots,\sigma(x),\ldots) = \sum_{\sigma\in\mathrm{Gal}(L/F)} \sigma(x) \end{array} .$$

Now that we have presented the lifted norm maps of Rubin and Silverberg, a geometric description of the torus is immediate.

Definition 2.31. *[RS04a, Definition 2.4] Let $\mathcal{T}_L$ be the intersection of the kernels of the lifted norm maps restricted to $\mathcal{G}_L$:*

$$\mathcal{T}_L := \mathrm{Ker}\left[\mathcal{G}_L \overset{\oplus\mathcal{N}_{L/F}}{\longrightarrow} \bigoplus_{k\subseteq F\subsetneq L} \mathcal{G}_F\right].$$

Two equivalent definitions are

$$\mathcal{T}_L := \bigcap_{k\subseteq F\subsetneq L} \mathrm{Ker}\,\mathcal{N}_{L/F}$$

and

$$\mathcal{T}_L := \left\{x\in\mathcal{G}_L : \mathcal{N}_{L/F}(x) = 1\in\mathcal{A}_F \,\text{for every subfield}\, k\subseteq F\subsetneq L\right\}.$$

Theorem 2.29 shows that the $\mathbb{F}_q$-rational points of $\mathcal{T}_{\mathbb{F}_{q^n}}$ are precisely

$$\mathcal{T}_{\mathbb{F}_{q^n}}(\mathbb{F}_q) = \left\{x\in\mathcal{G}_{\mathbb{F}_{q^n}}(\mathbb{F}_q) : \mathcal{N}_{\mathbb{F}_{q^n}/F}(x) = 1\,\text{for each}\,\mathbb{F}_q\subseteq F\subsetneq\mathbb{F}_{q^n}\right\}.$$

Now, recall the algebraic characterization of the norm-1 torus given by Theorem 2.2:

$$T_n(\mathbb{F}_q) = \{x\in\mathbb{F}_{q^n} : N_{\mathbb{F}_{q^n}/F}(x) = 1\,\text{for each}\,\mathbb{F}_q\subseteq F\subsetneq\mathbb{F}_{q^n}\}.$$

Clearly, we have a bijection

$$\mathcal{T}_{\mathbb{F}_{q^n}}(\mathbb{F}_q) \xrightarrow{\sim} T_n(\mathbb{F}_q).$$

Rubin and Silverberg extend this bijection to an isomorphism, which follows from our discussion.

Theorem 2.32. *[RS04a, Section 2] There exists an isomorphism of algebraic groups*

$$\mathcal{T}_{\mathbb{F}_{q^n}} \cong \mathbb{T}_{\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)}.$$

Finally, we have achieved a geometric definition of the norm-1 torus!

2.4 Algebraic tori

In this section, we explain why we call $T_n(\mathbb{F}_q)$ a torus. Before doing this, however, we remark upon the cryptographic consequences of the previous sections.

Remark 2.33. At this point, it is important to note that our geometric definition of $T_n(\mathbb{F}_q)$ could be exploited to achieve compression in cryptographic protocols. If there is an effectively computable birational embedding

$$\rho : \mathcal{T}_{\mathbb{F}_{q^n}} \hookrightarrow \mathbb{A}^d$$

for some integer d strictly less than n, we have achieved a compact representation of $T_n(\mathbb{F}_q)$, because we usually are only able to embed $\mathcal{T}_{\mathbb{F}_{q^n}}$ in $\mathbb{A}^n$. That is, $x \in \mathcal{T}_{\mathbb{F}_{q^n}}(\mathbb{F}_q) \subset \mathbb{A}^n(\mathbb{F}_q)$ requires

$$n \log q$$

bits to represent, but $\rho(x) \in \rho(\mathcal{T}_{\mathbb{F}_{q^n}}(\mathbb{F}_q)) \subset \mathbb{A}^d(\mathbb{F}_q)$ requires only

$$d \log q$$

bits to represent.

However, even our geometric definition of $\mathcal{T}_{\mathbb{F}_{q^n}}$ does not make it clear that such an embedding of $\mathcal{T}_{\mathbb{F}_{q^n}}$ exists, much less lead us to find such an embedding explicitly! To explain why we expect $\mathcal{T}_{\mathbb{F}_{q^n}}$ to be embeddable in an affine space of dimension $d < n$, we interpret $\mathcal{T}_{\mathbb{F}_{q^n}}$ as an algebraic torus and call upon the extensive literature studying these objects.

We begin by defining, in some generality, algebraic tori.

Definition 2.34. *Let k be a field, and let k_s be a fixed separable closure of k. Let V be a commutative algebraic group defined over k, so that V is an algebraic variety equipped with two morphisms $\oplus : V \times V \to V$ and $\ominus : V \to V$ which make V a group.*

We call an algebraic group V an algebraic torus if there exists a morphism of varieties $V \to \mathbb{G}_m^d$, defined over the closure k_s, for some positive integer d, that is also an isomorphism of groups.

If $k \subseteq L \subseteq k_s$ and V is isomorphic to $\mathbb{G}_m^d$ over L, we say that L splits the torus V.

Remark 2.35. Isomorphisms of algebraic groups are not the same as isomorphisms of groups, because in the former the maps must be morphisms of varieties.

It is immediate that $\mathbb{G}_m^d$ is an algebraic torus for each positive integer d, but we are also in a position to give non-trivial examples of algebraic tori. Consider the variety $\mathcal{G}_L = \operatorname{Res}_{L/k} \mathbb{G}_m$; the isomorphism of Theorem 2.8 (ii) gives that $\mathcal{G}_L \cong \mathbb{G}_m^{\operatorname{Gal}(L/k)}$, and it is clear that this means $\mathcal{G}_L \cong \mathbb{G}_m^{|\operatorname{Gal}(L/k)|}$. Thus $\mathcal{G}_L$ is an algebraic torus split by L; the dimension of $\mathcal{G}_L$ as a variety is trivially $|\operatorname{Gal}(L/k)|$.

Rubin and Silverberg show that in certain cases, the variety $\mathcal{T}_L$ is an algebraic torus. In particular, the variety $\mathcal{T}_{\mathbb{F}_{q^n}}$ over a finite field $\mathbb{F}_q$ is an algebraic torus for all integers n. This is the result that enables our entire study of tori in cryptography.

In fact, this result actually shows more than just the finite field case $\mathcal{T}_{\mathbb{F}_{q^n}}$. The result is that if $\operatorname{Gal}(L/k)$ is cyclic, then $\mathcal{T}_L$ is an algebraic torus of dimension $\varphi(n)$ split by L. Of course, since we are primarily interested in finite fields, we are not limited by restricting to field extensions with cyclic Galois groups.

Rubin and Silverberg state that the isomorphism identifying $\mathcal{A}_L$ and $\mathbb{A}^{\operatorname{Gal}(L/k)}$ is the only isomorphism, in the sense of Figure 2.3.

$$\begin{tikzcd}
\mathcal{A}_L \arrow[r, "\sim"] \arrow[d, dash] & \mathbb{A}^{\operatorname{Gal}(L/k)} \arrow[d, dash] \\
\mathcal{G}_L \arrow[r, "\sim"] \arrow[d, dash] & \mathbb{G}_m^{\operatorname{Gal}(L/k)} \arrow[d, dash] \\
\mathcal{T}_L \arrow[r, "\sim"] & \mathbb{T}_{\operatorname{Gal}(L/k)}
\end{tikzcd}$$

Figure 2.3: The horizontal maps are restrictions of the one isomorphism of Theorem 2.8 (ii).

We exploit this equivalence in the proof of the following theorem.

Theorem 2.36. *[RS04a, Proposition 2.6] Suppose G is cyclic. Write $G = \prod_{i=1}^t G_i$ with each subgroup G_i cyclic of prime-power order $p_i^{a_i}$, and each $p_i \neq p_j$ when $i \neq j$. For each index i, let H_i denote the cyclic subgroup of G_i or order p_i, and fix a set C_i of coset representatives of the quotient G_i/H_i. Let $\Gamma_i = G_i - C_i$ and define $\Gamma = \prod_{i=1}^t \Gamma_i$. Then* *there is a composition*

$$\mathbb{T}_G \hookrightarrow \mathbb{G}_m^G \twoheadrightarrow \mathbb{G}_m^\Gamma$$

that is an isomorphism.

Proof. We construct a map $\psi : \mathbb{G}_m^\Gamma \to \mathbb{T}_G$ as follows. Consider an element $\alpha \in \mathbb{G}_m^\Gamma$, and write

$$\alpha = (\alpha_g)_{g \in G}.$$

For each element $g \in G$, express g as a direct product $g = \gamma_1 \cdots \gamma_t$, with each γ_i in the prime-power cyclic subgroup G_i. We show that we can "avoid" a single element in each subgroup G_i, namely the distinguished coset representative. Let $I_g = \{i : \gamma_i \in C_i\}$ be the set of indices of factors γ_i that have been distinguished as coset representatives, and let $D_g = \prod_{i \in C_g} (H_i - \{1\})$ be the direct product of the non-trivial elements of the prime cyclic subgroups H_i. The intuition is that I_g is the set of indices of the elements g that are not in Γ, and D_g is the corresponding set of Galois conjugates.

Define an element $\beta = (\beta_g)_{g \in G}$ in $\mathbb{G}_m^G$ with components

$$\beta_g = (\prod_{\tau \in D_g} \alpha_{g\tau})^{(-1)^{|I_g|}}.$$

We have $g\tau \in \Gamma$ for every $\tau \in D_g$, for suppose $j \in I_g$ corresponds to a factor γ_j that is not a coset representative: then τ has a factor from $H_j - \{1\}$ and the product $g\tau$ has no factor in C_j. Also, for each $g \in \Gamma$, we have every factor $\gamma_i \in \Gamma_i$, so that the index set I_g is empty, the conjugate set D_g is the single element set $\{1\}$, and the product β_g is just α_g.

We claim that the constructed element β is in the torus $\mathbb{T}_G$. Fix a g in G and write g as a direct product $g = \gamma_1 \cdots \gamma_t$, and fix an index j with $1 \leqslant j \leqslant t$. By the definition of C_j, there is a unique coset representative $c_j \in C_j$ such that $c_j \in H_j\gamma_j$. Let $\eta_j = c_j\gamma_j^{-1} \in H_j$. Now consider an element $\delta \in H_j - \{\eta_j\}$; from the factor decomposition of $g\delta$, we see that $I_{g\eta_j} = I_{g\delta} \cup \{j\}$, and that $D_{g\eta_j} = D_{g\delta} \times (H_j - \{1\})$. Observe that $D_{g\delta}$ is independent of the choice of $\delta \in H_j - \{\eta_j\}$, and use this fact to write

$$\begin{aligned}
\beta_{g\eta_j} &= (\prod_{\tau \in D_{g\eta_j}} \alpha_{g\eta_j\tau})^{(-1)^{|I_{g\eta_j}|}} \\
&= (\prod_{\theta \in H_j - \{1\}} \prod_{\tau \in D_{g\delta}} \alpha_{g\eta_j\theta\tau})^{(-1)^{|I_{g\eta_j}|}} \\
&= (\prod_{\theta \in H_j - \{1\}} \prod_{\tau \in D_{g\delta}} \alpha_{g\eta_j\theta\tau})^{(-1)^{|I_{g\delta}|+1}} \\
&= (\prod_{\theta\eta_j \in H_j - \{\eta_j\}} \prod_{\tau \in D_{g\delta}} \alpha_{g(\theta\eta_j)\tau})^{(-1)^{|I_{g\delta}|+1}} \\
&= \prod_{\theta\eta_j \in H_j - \{\eta_j\}} \beta^{-1}_{g(\theta\eta_j)}.
\end{aligned}$$

Thus we have $\prod_{\theta \in H_j} \beta_{g\theta} = 1$ for each element $g \in G$ and each $1 \leqslant j \leqslant t$, so by our simplifying Lemma 2.23, $\beta = (\beta_g)_{g \in G} \in \mathbb{T}_G$, as claimed.

The map $\psi : \mathbb{G}_m^\Gamma \longrightarrow \mathbb{T}_G$ is injective, for suppose two distinct elements of $\mathbb{G}_m^\Gamma$, say $x = (x_\gamma)_{\gamma \in \Gamma}$ and $y = (y_\gamma)_{\gamma \in \Gamma}$, map to the same element:

$$\psi(x) = \psi(y) = b = (b_g)_{g \in G}.$$

Consider the element $z = (x_\gamma^{-1} y_\gamma)_{\gamma \in \Gamma}$; by assumption, there is a $\gamma \in \Gamma$ with $x_\gamma^{-1} y_\gamma \neq 1$. Now, writing $\psi(\cdot) = (\psi(\cdot)_g)_{g \in G}$,

$$\psi(z)_g = (\prod_{\tau \in D_g} x_{g\tau}^{-1} y_{g\tau})^{(-1)^{|I_g|}} = \psi(x)_g^{-1} \psi(y)_g = b_g^{-1} b_g = 1.$$

But, using the observation made above, for $\gamma \in \Gamma$ we have $\psi(x)_\gamma = x_\gamma$, and thus $\psi(z)_\gamma = 1$ for every $\gamma \in \Gamma$. This contradicts $x_\gamma^{-1} y_\gamma \neq 1$, and $x \neq y$; it follows that ψ is injective.

Now we show that $\psi : \mathbb{G}_m^\Gamma \longrightarrow \mathbb{T}_G$ is surjective. Suppose $x = (x_g)_{g \in G}$ is an element of $\mathbb{T}_G$. Without loss of generality, we can assume that $x_\gamma = 1$ for every $\gamma \in \Gamma$. We will show that $x_g = 1$ for every $g \in G$. Then, since ψ preserves the indices γ, meaning

$$\psi((x_\gamma)_{\gamma \in \Gamma})_\gamma = x_\gamma,$$

and since $\psi((x_\gamma)_{\gamma \in \Gamma}) \in \mathbb{T}_G$, it will follow that ψ is surjective.

We prove $x_g = 1$ for every $g \in G$ by induction on $|I_g|$. Again, write each element $g \in G$ as a direct product $g = \gamma_1 \cdots \gamma_t$, with each γ_i in the prime-power cyclic subgroup G_i. If $|I_g| = 0$, then $\gamma_i \in \Gamma_i$ for every index i, so $g \in \Gamma$ and $\beta_g = 1$ by assumption. If $|I_\gamma| = r \geqslant 1$, then some $\gamma_j \notin \Gamma_j$ for some index j. Observe that

$$1 = \prod_{\tau \in H_j} \beta_{g\tau} = \beta_g \prod_{\tau \in H_j - \{1\}} \beta_{g\tau}.$$

If $\tau \in H_j - \{1\}$, then we have $\gamma_j \tau \in \Gamma_j$ and thus $|I_{g\tau}| \leqslant r - 1$. Therefore, by induction, we have $\beta_{g\tau} = 1$ for every $\tau \in H_j - \{1\}$. It follows that $\beta_g = 1$ for every $g \in G$.

We conclude that the map $\psi : \mathbb{G}_m^\Gamma \xrightarrow{\sim} \mathbb{T}_G$ is a bijection. Since the group operation on $\mathbb{G}_m^\Gamma$ is component-wise multiplication, it is straightforward to verify that ψ preserves the group structure of $\mathbb{T}_G$.

Finally, the map $\psi^{-1} : \mathbb{T}_G \xrightarrow{\sim} \mathbb{G}_m^\Gamma$ is an isomorphism. □

Remark 2.37. After Remark 2.33, the reader might assume that Theorem 2.36 provides an embedding

$$\mathcal{T}_{\mathbb{F}_{q^n}} \hookrightarrow \mathbb{G}_m^{\varphi(n)} \subset \mathbb{A}^{\varphi(n)},$$

and thus an inclusion

$$T_n(\mathbb{F}_q) \subset \mathbb{F}_q^{\varphi(n)}.$$

However, this is not correct. Theorem 2.36 is a statement about the group structure of the norm-1 torus, while Remark 2.33 is a statement about the geometric structure of the norm-1 torus. While Theorem 2.36 does strongly suggest that such an embedding exists, it does not provide one. (One possible problem is that it is not immediate that the maps suggested by the proof are well-defined rational functions.)

However, for some tori T_n the embedding suggested by Theorem 2.36 exists; we will present some explicit examples in Chapter 4.

2.5 Summary of results

We summarize the major results of this chapter for easy reference.

We presented three representations of the norm-1 torus:

- We gave an algebraic representation, $T_n(\mathbb{F}_q) \subset \mathbb{F}_{q^n}$ with norm $N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}$ (Theorem 2.2);
- We gave a group theoretic representation, $\mathbb{T}_{\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)} \subset \mathbb{A}^{\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)}$ with norm $\mathbb{N}_{\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^d})}$ (Definition 2.20);
- And we gave a geometric interpretation, $\mathcal{T}_{\mathbb{F}_{q^n}} \subset \mathcal{A}_{\mathbb{F}_{q^n}}$ with norm $\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}$ (Definition 2.31).

Finally, we used these representations to prove that T_n is an algebraic torus (Theorem 2.36).

Our task now is to apply these results to the XTR cryptosystem.

Chapter 3

Quotients of algebraic tori and XTR

In this chapter, we show how Rubin and Silverberg use the results of Chapter 2 to understand the XTR cryptosystem of Lenstra and Verheul [LV00]. Rubin and Silverberg's goal was to extend the XTR cryptosystem to the next largest cryptographically interesting field extension [RS03, RS04a], but before we can explain the desired extension, we need to introduce the XTR cryptosystem.

3.1 The algebra of XTR

Let $L = \mathbb{F}_{q^6}$ extend $k = \mathbb{F}_q$, and let $F = \mathbb{F}_{q^2}$ be the quadratic subfield of L. Let $H = \mathrm{Gal}(L/F)$, and denote the q-Frobenius map by σ, so that we have

$$H = \mathrm{Gal}(L/F) = \{e, \sigma^2, \sigma^4\}.$$

The XTR cryptosystem exploits the following fact.

Theorem 3.1. *[LV00, Lemma 2.2.1] Let g be an element of the torus $T_6(\bar{\mathbb{F}}_q)$. Then $\mathrm{Tr}_{L/F}(g)$ determines the characteristic polynomial of g over F.*

Proof. The characteristic polynomial $\chi(t)$ of g over F is

$$\begin{aligned}\chi(t) &= (t-g)(t-\sigma^2(g))(t-\sigma^4(g)) \\ &= t^3 - t^2(g+\sigma^2(g)+\sigma^4(g)) + t(g\sigma^2(g)+\sigma^2(g)\sigma^4(g)+g\sigma^4(g)) - g\sigma^2(g)\sigma^4(g)).\end{aligned}$$

Now, $g \in T_6(\bar{\mathbb{F}}_q)$ means that $N_{L/F} = g\sigma^2(g)\sigma^4(g) = 1$ and $N_{L/\mathbb{F}_{q^3}}(g) = g\sigma^3(g) = 1$, and

$$g\sigma^2(g) + \sigma^2(g)\sigma^4(g) + g\sigma^4(g) = \frac{1}{\sigma^4(g)} + \frac{1}{g} + \frac{1}{\sigma^2(g)} = \sigma(g) + \sigma^5(g) + \sigma^3(g) = \sigma(\mathrm{Tr}_{L/F}(g)),$$

so

$$\chi(t) = t^3 - \mathrm{Tr}_{L/F}(g)t^2 + \sigma(\mathrm{Tr}_{L/F}(g))t - 1.$$

Thus, all the coefficients of the characteristic polynomial $\chi(t)$ of g are determined by the trace $\mathrm{Tr}_{L/F}(g)$. □

Theorem 3.1 allows the XTR cryptosystem to represent elements x of $T_6(\mathbb{F}_q)$ by their characteristic polynomials; these polynomials are then represented by the single coefficient $\mathrm{Tr}_{L/F}(x) \in F$. Therefore, an element $x \in T_6(\mathbb{F}_q)$, which usually requires

$$6 \log q$$

bits to represent, requires only

$$2 \log q$$

bits to represent. More precisely, 3 elements $\{g, \sigma^2(g), \sigma^4(g)\}$ of $T_6(\mathbb{F}_q)$ are represented by $\mathrm{Tr}_{L/F}(g)$.

To be cryptographically useful, it must be possible to compute with trace representations. To this end, [LV00, Section 2] gives optimized algorithms to compute

$$\mathrm{Tr}_{L/F}(g^{ab})$$

from the representation $\mathrm{Tr}_{L/F}(g^a)$ and the exponent b. This allows an XTR analogue to the Diffie-Hellman key agreement scheme [LV00, Section 4], which requires only 1/3 the bandwidth of the conventional Diffie-Hellman key agreement scheme in $\mathbb{F}_{q^6}^\times$.

Remark 3.2. Much work has been published improving the efficiency of the XTR computations [SL02, SL01] and related torus-based cryptosystems [GPS04].

Now that we have seen how the XTR cryptosystem compresses elements of $T_6(\mathbb{F}_q) \subset \mathbb{F}_{q^6}^\times$, we can explain the extension desired by Rubin and Silverberg. They wanted to construct a variant of XTR that compresses elements of the degree 30 extension $\mathbb{F}_{q^{30}}$ over $\mathbb{F}_q$. Elements of $\mathbb{F}_{q^{30}}^\times$ usually require

$$30 \log q$$

bits of storage, but they hoped to achieve a representation of elements of $T_{30}(\mathbb{F}_q) \subset \mathbb{F}_{q^{30}}^\times$ requiring only

$$\varphi(30) \log q = 8 \log q$$

bits of storage. Unfortunately, the most natural extensions of XTR do not achieve this goal. To explain why these extensions fail to yield the desired compression, we present Rubin and Silverberg's geometric interpretation of the XTR cryptosystem, and show how they use algebro-geometric tools to disprove the most natural conjectures.

First, we consider the XTR case.

3.2 The geometry of XTR

Rubin and Silverberg's strategy is to interpret the trace map used by XTR as a birational isomorphism between a special quotient variety and the affine plane.

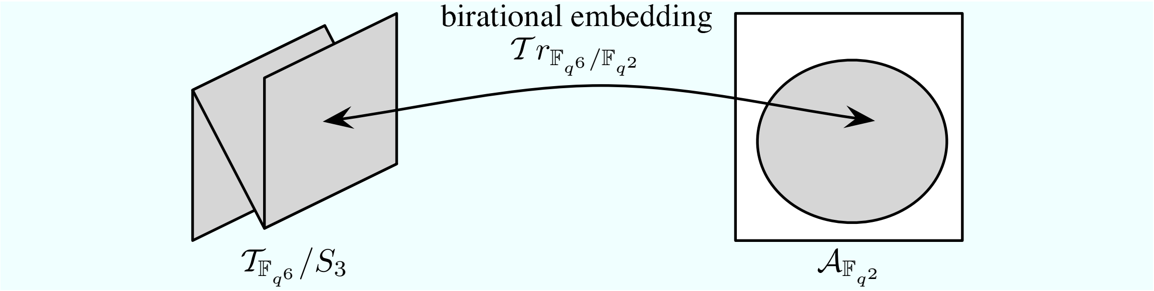

birational embedding
$\mathcal{T}r_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}$
$\mathcal{T}_{\mathbb{F}_{q^6}}/S_3$
$\mathcal{A}_{\mathbb{F}_{q^2}}$

Figure 3.1: A geometric interpretation of the trace map, as a birational isomorphism.

In Chapter 2, we showed how Rubin and Silverberg connected $T_6(\mathbb{F}_q) \subset \mathbb{F}_{q^6}^\times$, the subgroup used in the XTR cryptosystem, with the algebraic torus $\mathcal{T}_{\mathbb{F}_{q^6}}$. We now show how they connect the set of XTR traces with an algebraic variety.

3.2.1 The set of XTR traces

Again, let $L = \mathbb{F}_{q^6}$ extend $k = \mathbb{F}_q$, and let $F = \mathbb{F}_{q^2}$ be the quadratic subfield of L. Let $G = \mathrm{Gal}(L/k) = \{e, \sigma, \ldots, \sigma^5\}$, let $H = \mathrm{Gal}(L/F) = \{e, \sigma^2, \sigma^4\}$, and let $\mathrm{Gal}(F/k) = \{e, \sigma^3\}$.

Remark 3.3. The unusual notation for $\mathrm{Gal}(F/k)$, $\{e, \sigma^3\}$ instead of $\{e, \sigma\}$, was chosen because we need to work with the pairs $(e, \sigma^3), (\sigma, \sigma^4), (\sigma^2, \sigma^5)$. The connection between these pairs and $\mathrm{Gal}(F/k)$ is most obvious with σ^3 instead of σ.

Denote by S_{traces} the set of XTR traces, so

$$S_{\text{traces}} := \{\mathrm{Tr}_{L/F}(x) : x \in T_6(\mathbb{F}_q) \subset L\} \subset F.$$

Rubin and Silverberg prove that for a suitable action of the symmetric group S_3 on three symbols, there is a variety $\mathcal{S}_{\text{traces}}$ and an embedding

$$\mathcal{T}_L/S_3 \hookrightarrow \mathcal{A}_F$$

such that $\mathcal{S}_{\text{traces}}(k)$ is the image of the composition

$$\mathcal{T}_L(k) \longrightarrow (\mathcal{T}_L/S_3)(k) \hookrightarrow \mathcal{A}_F(k),$$

and the set of XTR traces S_{traces} is the image of $\mathcal{S}_{\text{traces}}(k)$ under a bijection $\mathcal{A}_F(k) \xrightarrow{\sim} F$. This is Theorem 3.7, but there is some work to be done before we can prove this result.

Theorem 3.1, exploited by XTR to represent elements of $T_6(\mathbb{F}_q)$ by traces, suggests that the equivalence of Galois conjugates under the trace map is important. In the interpretation of Rubin and Silverberg, this equivalence is expressed by an action of S_3 on the norm-1 torus $\mathcal{T}_L$.

3.2.2 Equating Galois equivalence and a group action

The crucial results of this section are explicit bijections that allow us to construct a group action that expresses the equivalence of Galois conjugates under the trace map $\mathrm{Tr}_{L/F}$. These bijections expand the presentation of [RS03, Section 7].

Let $\{x, \sigma^3(x)\}$ be a normal basis of F over k, and let $\{y, \sigma^2(y), \sigma^4(y)\}$ be a normal basis of $\mathbb{F}_{q^3}$ over k, so that $\{\alpha, \sigma(\alpha), \ldots, \sigma^5(\alpha)\}$, with $\alpha = xy$, is a normal basis of L over k. (Such bases exist for all finite fields, by the Normal Basis Theorem [LN94, Theorem 2.35].)

Observe that, in this basis, the trace map over F of an element

$$a = \alpha a_0 + \sigma(\alpha)a_1 + \cdots + \sigma^5(\alpha)a_5$$

is

$$\begin{aligned}
\mathrm{Tr}_{L/F}(a) &= a + \sigma^2(a) + \sigma^4(a) \\
&= (a_0 + a_2 + a_4)(\alpha + \sigma^2(\alpha) + \sigma^4(\alpha)) + \\
&\quad (a_1 + a_3 + a_5)\sigma(\alpha + \sigma^2(\alpha) + \sigma^4(\alpha)) \\
&= (a_0 + a_2 + a_4)x(y + \sigma(y) + \sigma^2(y)) + \\
&\quad (a_1 + a_3 + a_5)\sigma^3(x)(y + \sigma(y) + \sigma^2(y)) \\
&= \big(y + \sigma(y) + \sigma^2(y)\big)\left((a_0 + a_2 + a_4)x + (a_1 + a_3 + a_5)\sigma^3(x)\right).
\end{aligned}$$

To simplify matters, we want to remove the factor $y + \sigma^2(y) + \sigma^4(y)$, which we denote by λ. Since $\sigma^4(y) = \sigma(y)$, we have that $\sigma(\lambda) = \lambda$, and thus $\lambda \in k$. Also, λ is invertible, since $y, \sigma^2(y), \sigma^4(y)$ are linearly independent.

If we now normalize our bases by λ^{-1}, so that our basis for F over k is $\{\lambda^{-1}x, \lambda^{-1}\sigma^3(x)\}$ and our basis for L over k is $\{\lambda^{-1}\alpha, \lambda^{-1}\sigma(\alpha), \ldots, \lambda^{-1}\sigma^5(\alpha)\}$, then

$$\begin{aligned}
&\mathrm{Tr}_{L/F}(\lambda^{-1}\alpha a_0 + \lambda^{-1}\sigma(\alpha)a_1 + \cdots + \lambda^{-1}\sigma^5(\alpha)a_5) = \\
&\quad (a_0 + a_2 + a_4)x + (a_1 + a_3 + a_5)\sigma^3(x),
\end{aligned} \tag{3.1}$$

which has a particularly simple form. We can now define bijections that capture this simplicity.

Definition 3.4. *Define bijections*

$$\begin{gathered}
\tau : L \xrightarrow{\sim} \left((\mathbb{A}^{\mathrm{Gal}(L/F)})^3\right)(k) \\
\tau(\lambda^{-1}\alpha a_0 + \lambda^{-1}\sigma(\alpha)a_1 + \cdots + \lambda^{-1}\sigma^5(\alpha)a_5) = ((a_0, a_3), (a_2, a_5), (a_4, a_1))
\end{gathered}$$

and

$$\begin{gathered}
\phi : F \xrightarrow{\sim} \left(\mathbb{A}^{\mathrm{Gal}(F/k)}\right)(k) \\
\phi(\lambda^{-1}\alpha a_0, \lambda^{-1}\sigma^3(\alpha)a_3) = (a_0, a_3)
\end{gathered}\ .$$

The key point is that τ and ϕ give a non-standard representation of L as $\left((\mathbb{A}^{\mathrm{Gal}(L/F)})^3\right)(k)$, which suggests a group action on the factors. Rubin and Silverberg define a "trace map" t with simple form, where we have chosen the non-standard notation t to emphasize the fact that the domain and range of t do not follow the conventions of Chapter 2.

Definition 3.5. *[RS03, Theorem 13] Define the "trace map"*

$$t : (\mathbb{A}^{\mathrm{Gal}(L/F)})^3 \longrightarrow \mathbb{A}^{\mathrm{Gal}(L/F)}$$

by

$$t((a_0, a_3), (a_2, a_5), (a_4, a_1)) = (a_0 + a_2 + a_4, a_1 + a_3 + a_5).$$

Examining (3.1), we have the following theorem.

Theorem 3.6. *[RS03, Theorem 13] The "trace map" t makes the following diagram commute:*

$$\begin{tikzcd} L \arrow[r, "\tau"] \arrow[d, "\mathrm{Tr}_{L/F}"'] & \left(\left(\mathbb{A}^{\mathrm{Gal}(L/F)}\right)^3\right)(k) \arrow[d, "t"] \\ F \arrow[r, "\phi"] & \left(\mathbb{A}^{\mathrm{Gal}(L/F)}\right)(k) \end{tikzcd},$$

where the maps τ and ϕ are those of Definition 3.4.

Theorem 3.6 makes one of the symmetric maps of Theorem 2.29 explicit, and yields a natural action of the symmetric group S_3 on the product $(\mathbb{A}^{\mathrm{Gal}(L/F)})^3$ and the restriction $(\mathbb{G}_m^{\mathrm{Gal}(F/k)})^3$. Specifically, a permutation in S_3 acts on $(\mathbb{A}^{\mathrm{Gal}(L/F)})^3$ by permuting the factors $\mathbb{A}^{\mathrm{Gal}(L/F)}$. The pull-back of this action defines an action of S_3 on $\mathcal{A}_L = \mathrm{Res}_{L/k}\,\mathbb{A}^1$ and $\mathcal{G}_L = \mathrm{Res}_{L/k}\,\mathbb{G}_m$, and it is clear that the "trace" t and the trace $\mathrm{Tr}_{L/F}$ are invariant under the action and the pull-back, respectively. Thus, the equivalence of Galois conjugates under the trace map is identified with the defined action of S_3 on $\mathcal{A}_L$.

3.2.3 The action of the symmetric group S_3 on the torus T_6

Now that we have an action of S_3 on $\mathcal{A}_L$, we must understand what this action on the norm-1 torus $T_6(\mathbb{F}_q)$ means in the cryptosystem XTR. To aid understanding, Figure 3.2 depicts the trace map as a birational parameterization.

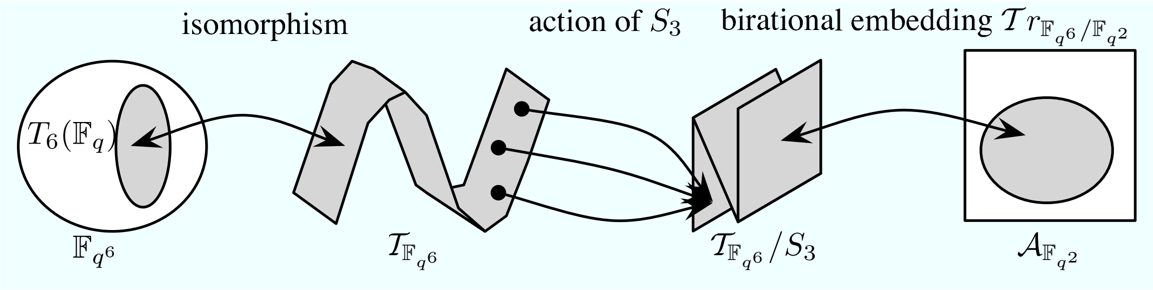

isomorphism
action of S_3
birational embedding $\mathcal{T}r_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}$
$T_6(\mathbb{F}_q)$
$\mathbb{F}_{q^6}$
$\mathcal{T}_{\mathbb{F}_{q^6}}$
$\mathcal{T}_{\mathbb{F}_{q^6}}/S_3$
$\mathcal{A}_{\mathbb{F}_{q^2}}$

Figure 3.2: The trace map parameterizes a quotient variety.

Observe that Figure 3.2 claims that the image of $\mathcal{T}_{\mathbb{F}_{q^6}}$ in $\mathcal{A}_{\mathbb{F}_{q^6}}/S_3$ is a subset of $\mathcal{T}_{\mathbb{F}_{q^6}}$, or in other words that the action of S_3 stabilizes the norm-1 torus. We will show this explicitly, since this case is instructive when we later consider more general actions that stabilize tori.

Using the isomorphism $\mathcal{T}_L \cong \mathbb{T}_G$, consider a point $x = (x_0, \ldots, x_5)$ in the torus $\mathbb{T}_G$, and recall that the components of x satisfy the relations $x_0x_3 = x_1x_4 = x_2x_5 = 1$ and $x_0x_2x_4 = x_1x_3x_5 = 1$. Every permutation in S_3 is a product of transpositions, so without loss of generality we consider only transpositions. The map τ acts as

$$x \longmapsto ((x_0, x_3), (x_2, x_5), (x_4, x_1)),$$

and it is clear that a transposition maintains the relations of x. For example, the action of $(12) \in S_3$ is

$$(12)\tau(x) = ((x_2, x_5), (x_0, x_3), (x_4, x_1)),$$

and the inverse map is

$$\tau^{-1}((12)\tau(x)) = (x_2, x_1, x_0, x_5, x_4, x_3).$$

By inspection each permutation preserves the multiplicative relations, and hence the torus $\mathbb{T}_G$.

Since the torus is stabilized under the action of S_3, the image of $\mathcal{T}_L$ in the quotient $\mathcal{G}_L/S_3$ is a well-defined variety.

However, the most significant part of Figure 3.2 is the rightmost birational embedding. What this embedding says is that the natural trace map establishes a one-to-one correspondence between the sets of Galois conjugates of elements of the norm-1 torus and their traces over the quadratic subfield $\mathbb{F}_{q^2}$. Of course, this merely translates the discussion of Section 3.1, but our geometric interpretation will show its power later. Theorem 3.7 supports Figure 3.2.

Theorem 3.7. *[RS03, Theorem 13] There is a birational embedding*

$$\mathcal{T}_L/S_3 \hookrightarrow \mathcal{A}_F$$

such that $\mathcal{S}_{\text{traces}}(k)$ is the image of $\mathcal{T}_L(k)$ in the composition

$$\mathcal{T}_L(k) \longrightarrow (\mathcal{T}_L/S_3)(k) \hookrightarrow \mathcal{A}_F(k).$$

Proof. Following the proof given by Rubin and Silverberg, we have

$$\begin{tikzcd}
\mathcal{T}_L \arrow[r, hook] & \mathcal{G}_L \arrow[r, hook] & \mathcal{A}_L \arrow[r, "\sim"] \arrow[d, "\mathcal{T}r_{L/F}"'] & \left(\mathbb{A}^{\mathrm{Gal}(F/k)}\right)^3 \arrow[d, "t"] \\
 & & \mathcal{A}_F \arrow[r, "\sim"] & \mathbb{A}^{\mathrm{Gal}(F/k)}
\end{tikzcd} ,$$

with the top and bottom isomorphisms provided by Theorem 2.8, the left vertical map the constructed trace provided by Theorem 2.29, and the right vertical map the "trace" t of Definition 3.5.

The preceding discussion and the explicit construction of the top and bottom isomorphisms show that the morphism $\mathcal{T}r_{L/F} : \mathcal{A}_L \longrightarrow \mathcal{A}_F$ factors through the quotient $\mathcal{A}_L/S_3$, and thus restricts to a morphism

$$\mathrm{Tr} : \mathcal{T}_L/S_3 \longrightarrow \mathcal{A}_F.$$

Since Theorem 2.36 shows that

$$\mathcal{T}_L \cong \mathbb{T}_{\mathrm{Gal}(L/k)} \cong \mathbb{G}_m^2 \cong \mathcal{G}_F,$$

we see that $\mathcal{T}_L$ is a variety of dimension 2. Since $\mathcal{A}_F$ is also a variety of dimension 2, to prove that there is an embedding $\mathcal{T}_L/S_3 \hookrightarrow \mathcal{A}_F$ we need only show that the restricted trace morphism Tr is injective.

Consider an element $a \in \mathcal{T}_L(k)$. Using the isomorphism τ of Definition 3.4, we may view $a = (a_0, a_1, a_2)$ with each $a_i \in \mathbb{A}^{\mathrm{Gal}(F/k)}(k)$. Suppose $b \in \mathcal{T}_L$ has $\mathrm{Tr}(b) = \mathrm{Tr}(a)$, with Tr the restriction of $\mathcal{T}r$ defined above. By Theorem 3.1 and the appropriate lifting isomorphisms, Tr determines all the symmetric functions of b_0, b_1, b_2, from which follows the set equality $\{a_0, a_1, a_2\} = \{b_0, b_1, b_2\}$. But this is precisely the statement that a is conjugate to b by an element of S_3, and that $a = b$ in the quotient $\mathcal{T}_L/S_3(\mathrm{k})$.

Finally, the set $\mathcal{S}_{\text{traces}}(k)$ is the image of the composition

$$\mathcal{T}_L(k) \longrightarrow (\mathcal{T}_L/S_3)(k) \hookrightarrow \mathcal{A}_F(k)$$

by definition. □

Translating between the many representations of the norm-1 torus, this says that the natural trace map $\mathrm{Tr}_{L/F} : \mathbb{F}_{q^6} \longrightarrow \mathbb{F}_{q^2}$ is an explicit isomorphism identifying the norm-1 torus $T_6(\mathbb{F}_q)$ modulo Galois equivalence with the set of XTR traces S_{traces}. This is illustrated in Figure 3.3.

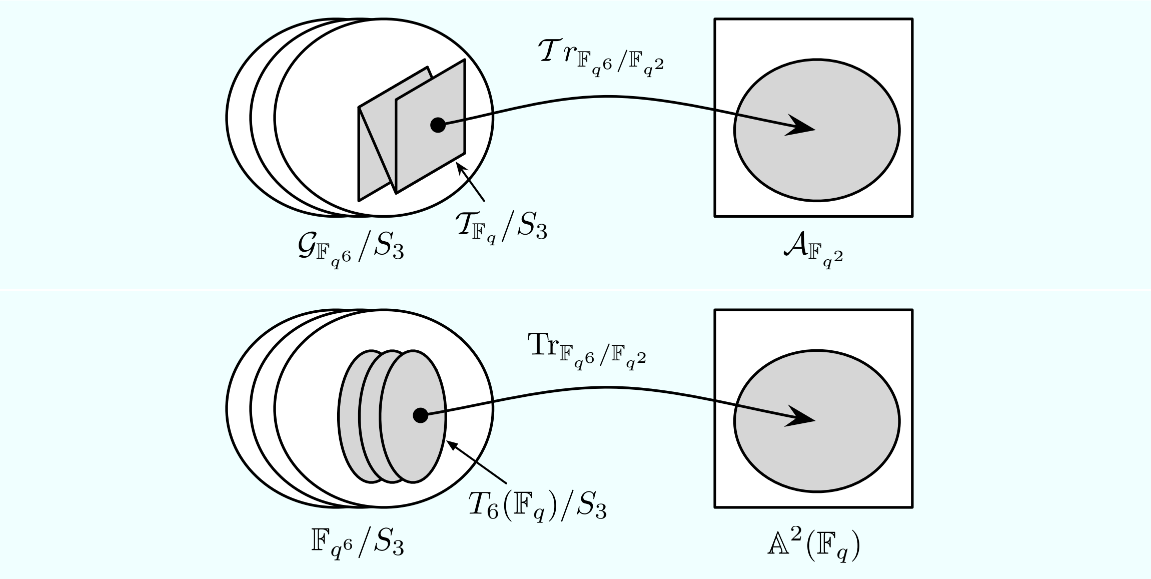

$\mathcal{T}r_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}$
$\mathcal{T}_{\mathbb{F}_q}/S_3$
$\mathcal{G}_{\mathbb{F}_{q^6}}/S_3$
$\mathcal{A}_{\mathbb{F}_{q^2}}$
$\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}$
$T_6(\mathbb{F}_q)/S_3$
$\mathbb{F}_{q^6}/S_3$
$\mathbb{A}^2(\mathbb{F}_q)$

Figure 3.3: The trace map compresses the norm-1 torus modulo Galois equivalence.

The preceding results establish Figures 3.1, 3.2, and 3.3, which graphically depict the geometry of the XTR cryptosystem.

3.3 Group actions on tori

Theorem 3.7 is a special case of a more general theorem that explains certain group actions on tori. The purpose of this section is to explain the general case, and detail how XTR fits into this larger framework.

Rubin and Silverberg define general actions on tori with the aid of some notation. As usual, let L be a Galois extension of k with cyclic Galois group $G = \mathrm{Gal}(L/k)$, and let $F \subset L$ be a subfield. Denote by H the Galois group $\mathrm{Gal}(L/F)$. Unlike other sections, we assume that

$$n = [L : k] = |G|$$

is square-free. In the most cryptographically interesting cases, n is the product of the first few primes, so our assumption is not cryptographically limiting.

Definition 3.8. *[RS04a, Definition 3.1] Let Σ_S denote the group of permutations rearranging the set S.*

Write $G = \prod_{i=1}^{t} G_i$, with the G_i cyclic groups of distinct prime order. Since n is square-free, there is a natural inclusion of Σ_H into Σ_G. The permutation group Σ_G acts naturally on $\mathbb{A}^G$, and the inclusion $\Sigma_H \subset \Sigma_G$ gives an action of Σ_H on $\mathbb{A}^G$ which lifts to an action on $\mathcal{A}_L$ via Theorem 2.8. Since the action of Σ_H merely shuffles components, Σ_H preserves $\mathbb{G}_m^G$ (equivalently, $\mathcal{G}_L$), but the action of Σ_H does not necessarily preserve the torus $\mathbb{T}_G$ (equivalently, $\mathcal{T}_L$). Specifically, we will see that if $|H|$ is divisible by two distinct primes, Σ_H does not preserve $\mathcal{T}_L$.

Remark 3.9. In the XTR case, $|\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})| = 3$ is divisible by only one prime, and the norm-1 torus $\mathcal{T}_{\mathbb{F}_{q^6}}$ is preserved by $\Sigma_{\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})}$, which we identified with S_3.

Observe that the permutation groups Σ_{G_i} correspond to the field extensions $F \subset L$ of prime degree, ie extensions with $[L : F]$ prime. The following result shows that the groups corresponding to these extensions preserve $\mathcal{T}_L$.

Theorem 3.10. *[RS04a, Lemma 3.5] The action of Σ_{G_i} preserves $\mathcal{T}_L$.*

Proof. Rubin and Silverberg use the isomorphisms of Theorem 2.8 (ii) to prove that every $\tau \in \Sigma_{G_i}$ preserves $\mathbb{T}_G$. We need to show that for every element $x = (x_\sigma)_{\sigma \in G} \in \mathbb{T}_G$, we have

$\tau(x) = (x_{\tau\sigma})_{\sigma \in G} \in \mathbb{T}_G$. By Lemma 2.23 simplifying the definition of $\mathbb{T}_G$, it suffices to show that $\Pi_{\sigma \in G_j} x_{\tau(\gamma\sigma)} = 1$ for every $\gamma \in G$.

Write $\gamma = \gamma_1 \cdots \gamma_t$ with each $\gamma_j \in G_j$. Since $\tau \in \Sigma_{G_i}$, τ fixes all the γ_j save γ_i and $\tau(\gamma) = \tau(\gamma\gamma_i^{-1}\gamma_i) = \gamma\gamma_i^{-1}\tau(\gamma_i)$; thus $\prod_{\sigma \in G_i} x_{\tau(\gamma\sigma)} = \prod_{\sigma \in G_i} x_{\gamma\gamma_i^{-1}\tau(\gamma_i\sigma)}$, and γ_i permutes G_i to yield

$$\prod_{\sigma \in G_i} x_{\tau(\gamma\sigma)} = \prod_{\sigma \in G_i} x_{\gamma\gamma_i^{-1}\sigma} = 1.$$

Finally, for each product over $\sigma \in G_j$ with $j \neq i$, we have $\tau(\gamma\sigma) = \tau(\gamma)\sigma$ and

$$\prod_{\sigma \in G_j} x_{\tau(\gamma\sigma)} = \prod_{\sigma \in G_j} x_{\tau(\gamma)\sigma} = 1.$$

Thus, the torus is preserved under the action of Σ_{G_i}. □

Now that we know certain actions that preserve $\mathcal{T}_L$, we would like a converse theorem that tells us exactly which actions preserve the torus. Theorem 3.12 provides this converse.

Write $H = \prod H_i$, with the set of factors $\{H_i\}$ a subset of the set of factors $\{G_i\}$ of G. Following Rubin and Silverberg, we make the following definition.

Definition 3.11. *Let*

$$\Sigma'_H := \prod \Sigma_{H_i} \subseteq \Sigma_H.$$

The intuition is that the group Σ'_H acts on $\mathbb{T}_G$ by permuting components within the individual multiplicative relations that define $\mathbb{T}_G$, but does not permute the components between relations.

Theorem 3.12. *[RS04a, Proposition 3.6] Let $\sigma \in \Sigma_H$. If $\sigma(\mathbb{T}_G) \subseteq \mathbb{T}_G$, then $\sigma \in \Sigma'_H$.*

Proof. The proof of this proposition is a constructive induction that we omit to save space. □

Theorem 3.12 tells us that some permutations $\pi \in \Sigma_H$ are “bad”, in the sense that they do not preserve the norm-1 torus. The following notation makes it easier to discuss the effects of Σ_H on the norm-1 torus.

Definition 3.13. *Let $\mathcal{X}_F$ denote the image of $\mathcal{T}_L$ in $\mathcal{G}_L/\Sigma_H$.*

Remark 3.14. It would be convenient to speak of the quotient $\mathcal{T}_L/\Sigma_H$, but the action of a permutation $\pi \in \Sigma_H$ can map an element $x \in \mathcal{T}_L$ to an element $\pi(x) \notin \mathcal{T}_L$. Figure 3.4 illustrates this occurrence.

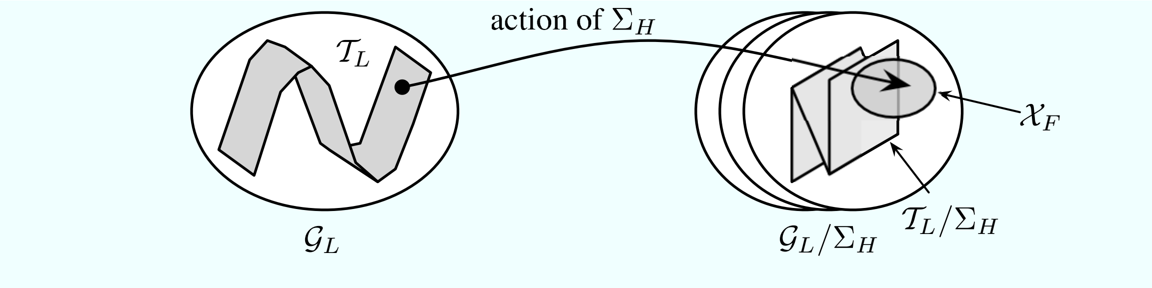


Figure 3.4: Some group actions do not preserve the norm-1 torus.

Remark 3.15. When Σ_H does preserve the torus $\mathcal{T}_L$, the variety $\mathcal{X}_F$ is the analogue of the set $\mathcal{S}_{\text{traces}}$ of XTR traces.

According to Rubin and Silverberg, the final theorem describing group actions in the XTR cryptosystem follows from Theorem 3.12.

Theorem 3.16. *[RS04a, Proposition 3.7] The induced map*

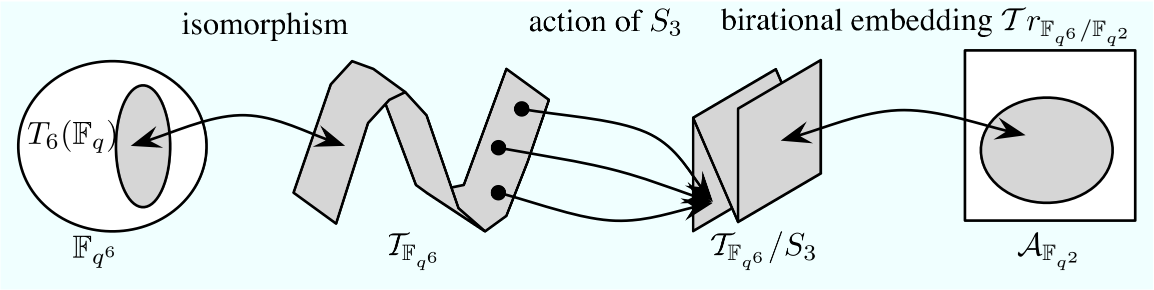
$$\mathcal{T}_L/\Sigma'_H \longrightarrow \mathcal{X}_F$$

is a birational isomorphism.

This theorem explains the role of the action of S_3 on the torus $\mathcal{T}_{\mathbb{F}_{q^6}}$, and of the parameterization of $\mathcal{X}_{\mathbb{F}_{q^2}}$ of Theorem 3.7 given by the trace map over $\mathbb{F}_{q^2}$. In the XTR case, $\Sigma_H = \Sigma'_H = S_3$, and we have the sequence of maps

$$\mathcal{T}_{\mathbb{F}_{q^6}} \longrightarrow \mathcal{T}_{\mathbb{F}_{q^6}}/\Sigma'_H \longrightarrow \mathcal{X}_{\mathbb{F}_{q^2}} \longrightarrow \mathcal{A}_{\mathbb{F}_{q^2}}.$$

Referring to Figure 3.2, duplicated below, Theorem 3.16 establishes the middle arrows, labeled “action of S_3”.


isomorphism
action of S_3
birational embedding $\mathcal{T}r_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}$
$T_6(\mathbb{F}_q)$
$\mathbb{F}_{q^6}$
$\mathcal{T}_{\mathbb{F}_{q^6}}$
$\mathcal{T}_{\mathbb{F}_{q^6}}/S_3$
$\mathcal{A}_{\mathbb{F}_{q^2}}$

However, the most important part of Theorem 3.7 is not the birational isomorphism

$$\mathcal{T}_{\mathbb{F}_{q^6}}/\Sigma'_H \longrightarrow \mathcal{X}_{\mathbb{F}_{q^2}};$$

the most important part is that the trace map parameterizes the variety $\mathcal{X}_{\mathbb{F}_{q^2}}$:

$$\mathcal{T}r_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} : \mathcal{X}_{\mathbb{F}_{q^2}} \xrightarrow{\sim} \mathcal{A}_{\mathbb{F}_{q^2}}.$$

We examine this more carefully in the next section.

3.4 Parameterizing quotient varieties

Rubin and Silverberg use algebraic geometry to explain why the trace map parameterizes $\mathcal{X}_{\mathbb{F}_{q^2}}$. Again, let L be a Galois extension of k with cyclic Galois group $G = \mathrm{Gal}(L/k)$, and suppose $n = [L : k] = |G|$ is square-free. Let $F \subset L$ be a subfield, let $H = \mathrm{Gal}(L/F)$, and write $n = de$ with $[F : k] = d$.

Theorem 3.17. *[RS04a, Proposition 3.2] For each index $1 \leqslant i \leqslant e$, the symmetric map $\mathcal{S}_{i,F}$ of Section 2.3.2 factors through $\mathcal{G}_L/\Sigma_H$. Together, the symmetric maps make the following diagram commute, where the vertical map f is an isomorphism:*

$$\begin{tikzcd}
\mathcal{G}_L \arrow[r, two heads] \arrow[drr, "\oplus_{i=1}^{e}\mathcal{S}_{i,F}"'] & \mathcal{G}_L/\Sigma_H \arrow[r, hook] & \mathcal{A}_L/\Sigma_H \arrow[d, "f = \oplus_{i=1}^{e}\mathcal{S}_{i,F}"] \\
 & & (\mathcal{A}_F)^e
\end{tikzcd}$$

Proof. We elaborate on the proof of Rubin and Silverberg. Theorem 2.29 and the definition of $\mathcal{S}_{i,F}$ yield that $\mathcal{S}_{i,F}$ is Σ_H invariant, and hence factors through $\mathcal{A}_L/\Sigma_H$. We must prove that the right hand map f is an isomorphism. The form of the isomorphism $\operatorname{Res}_{L/F} \mathbb{A}^1 \longrightarrow \mathbb{A}^H$ and the definition of $\mathcal{S}_{i,F}$ as the Weil restriction of $\mathbb{S}_{i,F}$, yield that it suffices to prove the theorem in the case $F = k$, so $e = n$. We appeal to a standard result of algebraic geometry [Ful69, Chapter 2, Proposition 1]:

Proposition 3.18. *Let $A(X)$ denote the coordinate ring of the affine variety X. For affine varieties X and Y, let $\psi : X \longrightarrow Y$ be a polynomial map, and define the pull-back*

$$f^* : A(Y) \longrightarrow A(X)$$

to be

$$f^*(g) = g \circ f.$$

Then the map f is an isomorphism $X \cong Y$ if and only the map f^* is an isomorphism $A(X) \cong A(Y)$.

In our case, $A(\mathcal{A}_L) = k[\ldots, x_\sigma, \ldots]$, with the x_σ indexed by the elements of $\operatorname{Gal}(L/k)$, and thus $A(\mathcal{A}_L/\Sigma_G) = k[\ldots, x_\sigma, \ldots]^{\Sigma_G}$, the ring of Σ_G-invariant polynomials. Also, $A((A_k)^n) \cong k[\ldots, x_\sigma, \ldots]$. Denote the symmetric polynomials of the x_σ by $s_1, \ldots, s_n$. The definition of f means $f(\ldots, x_\sigma, \ldots) = (s_1, \ldots, s_n)$, and thus for a map $g \in (\mathcal{A}_k)^n$, the pull-back satisfies $f^*(g) = g(s_1, \ldots, s_n)$, and by abuse of notation, $f^*(A((\mathcal{A}_k)^n)) \cong k[s_1, \ldots, s_n]$. Thus, f is an isomorphism if

$$k[s_1, \ldots, s_n] \cong k[\ldots, x_\sigma, \ldots]^{\Sigma_G}.$$

The symmetric polynomials are Σ_G-invariant by definition, and it follows from the Fundamental Theorem of Symmetric Polynomials [LN94, p. 29] that every polynomial in $k[x_1, \ldots, x_n]^{\Sigma_G}$ is a polynomial combination of the s_i. Thus the right hand map f is an isomorphism. □

Theorem 3.17 allows us to connect the symmetric functions $\mathcal{S}_{i,F}$ (of which the trace map is $\mathcal{S}_{1,F}$) with the field of rational functions $\mathcal{X}_F \longrightarrow k$.

Theorem 3.19. *[RS04a, Corollary 3.4] Let $\phi = (\phi_1, \ldots, \phi_d) : \mathcal{A}_F \longrightarrow \mathbb{A}^d$ be an isomorphism, where d is the extension degree of F over k.*

Then the function field of $\mathcal{X}_F$, denoted $k(\mathcal{X}_F)$, is generated by the following symmetric functions:

$$k(\mathcal{X}_F) = k(\phi_j \circ \mathcal{S}_{i,F} : 1 \leqslant j \leqslant d, 1 \leqslant i \leqslant e = n/d).$$

Proof. Since $\mathcal{A}_L$ is an affine variety, the function field $k(\mathcal{A}_L)$ is identified with the quotient field of $A(\mathcal{A}_L)$. From the calculation of the coordinate ring $A(\mathcal{A}_L)$ of Theorem 3.17, the identification

$$k(\mathcal{A}_L) = k(\phi_1 \circ \mathcal{S}_{1,F}, \ldots, \phi_d \circ \mathcal{S}_{e,F})$$

follows. Finally, $\mathcal{X}_F$ is a subvariety of $\mathcal{A}_L$, so the restriction of the maps $\phi_j \circ \mathcal{S}_{i,F}$ to $\mathcal{X}_F$ generate $k(\mathcal{X}_F)$. □

In the case of XTR, we have $d = 2$, and Theorem 3.1 shows that $\mathcal{S}_{1,\mathbb{F}_{q^2}}$ determines $\mathcal{S}_{2,\mathbb{F}_{q^2}}$ (restricted to $\mathcal{X}_{\mathbb{F}_{q^2}}$), so the map

$$f = \oplus_{i=1}^{3} \mathcal{S}_{i,\mathbb{F}_{q^2}}$$

on $\mathcal{X}_{\mathbb{F}_{q^2}}$ can be expressed as

$$(\mathcal{T}r_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}, p(\mathcal{T}r_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}), 1) \in k(\mathcal{X}_{\mathbb{F}_{q^2}})^3,$$

with p a suitable polynomial, by abuse of notation. If we project only the first coordinate, we have the result of XTR: a birational embedding

$$\mathcal{T}r_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} = \mathcal{S}_{1,\mathbb{F}_{q^2}} : \mathcal{X}_{\mathbb{F}_{q^2}} \hookrightarrow \mathcal{A}_{\mathbb{F}_{q^2}}.$$

3.5 The LUC case

In the LUC [SL93, SS95] cryptosystem, we have $k = \mathbb{F}_q$, $F = \mathbb{F}_q$, and $L = \mathbb{F}_{q^2}$. Observe that for $x \in T_2(\mathbb{F}_q) \subset \mathbb{F}_{q^2}$, the minimal polynomial of x is

$$\chi(t) = (t - x)(t - x^q) = t^2 - (x + x^q)t + x^{q+1} = t^2 - \mathrm{Tr}_{L/F}(x)t + 1.$$

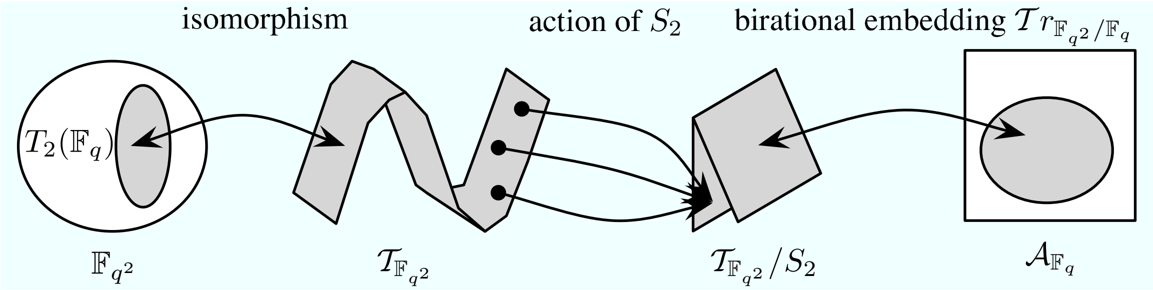

isomorphism
action of S_2
birational embedding $\mathcal{T}r_{\mathbb{F}_{q^2}/\mathbb{F}_q}$
$T_2(\mathbb{F}_q)$
$\mathbb{F}_{q^2}$
$\mathcal{T}_{\mathbb{F}_{q^2}}$
$\mathcal{T}_{\mathbb{F}_{q^2}}/S_2$
$\mathcal{A}_{\mathbb{F}_q}$

Figure 3.5: The geometry of the LUC cryptosystem.

Therefore LUC can represent $T_2(\mathbb{F}_q)$ by minimal polynomials in exactly the same way XTR represented $T_6(\mathbb{F}_q)$ by minimal polynomials. Figure 3.5 depicts this graphically.

Summarizing several sections, we studied group actions on tori and explained how Rubin and Silverberg interpret the LUC and XTR cryptosystems as group actions on tori and fortuitous birational parameterizations. After considering the structure of $\mathcal{X}_F$, we will show how Rubin and Silverberg use this theory to analyze proposed extensions to the XTR cryptosystem.

3.6 Some quotient varieties are not groups

Cryptosystems usually work in groups, such as $T_n(\mathbb{F}_q) \subset \mathbb{F}_{q^n}^\times$, but there is no reason to believe $\mathcal{X}_{\mathbb{F}_{q^d}}$ will be a group, since Section 3.4 does not consider the structure of the quotient variety $\mathcal{X}_F$. In the case of the XTR cryptosystem, $\mathcal{X}_{\mathbb{F}_{q^2}}$ is not a group, and this explains why XTR does not have a natural multiplication algorithm [LV00]. Let us explore why this is so.

The key point is that multiplication in the norm-1 torus $T_6(\mathbb{F}_q)$ does not preserve S_3 orbits. This means that multiplying two elements in the quotient variety $\mathcal{T}_{\mathbb{F}_{q^6}}/S_3$ is not well-defined. Let $x \in T_6(\mathbb{F}_q)$ correspond to the three conjugates $x, \sigma^2(x), \sigma^4(x)$ in $\mathcal{X}_{\mathbb{F}_{q^2}}$, and let $y \in T_6(\mathbb{F}_q)$ correspond to the three conjugates $y, \sigma^2(y), \sigma^4(y)$. For multiplication to be well defined in $\mathcal{X}_{\mathbb{F}_{q^2}}$, all the possible products

$$xy, \sigma^2(x)y, \sigma^4(x)y, x\sigma^2(y), \ldots, \sigma^4(x)\sigma^4(y)$$

must be in the same S_3 orbit. However, this is generally not the case; for example, it is not always true that the set

$$\{xy, \sigma^2(xy), \sigma^4(xy)\}$$

is the same as the set

$$\{x\sigma^2(y), \sigma^2(x\sigma^2(y)), \sigma^4(x\sigma^2(y))\}.$$

This means that $\mathcal{X}_{\mathbb{F}_{q^2}}$ is not a group, which explains the non-standard "multiplication" algorithm of the XTR cryptosystem.

However, exponentiation in the norm-1 torus $T_6(\mathbb{F}_q)$ does preserve S_3 orbits. Letting x correspond to the conjugates $x, \sigma^2(x), \sigma^4(x)$, it does not matter which representative we choose to exponentiate. In other words,

$$\{x^j, \sigma^2(x^j), \sigma^4(x^j)\} = \{\sigma^2(x)^j, \sigma^2(\sigma^2(x)^j), \sigma^4(\sigma^2(x)^j)\} = \{\sigma^4(x)^j, \sigma^2(\sigma^4(x)^j), \sigma^2(\sigma^4(x)^j)\}.$$

This fact enables the XTR cryptosystem to compute something meaningful in the quotient $\mathcal{X}_{\mathbb{F}_{q^2}}$.

More generally, Rubin and Silverberg show many fields $k \subset F \subset L$ such that $\mathcal{X}_F$ is not a group [RS03, Section 7].

3.7 Beyond XTR

It is natural to exploit the function field perspective of Theorems 3.17 and 3.19 to analyze proposed extensions to XTR. Rubin and Silverberg's strategy is to show that higher dimensional analogues of XTR require parameterizing higher dimensional varieties $\mathcal{X}$. Natural extensions of XTR would parameterize $\mathcal{X}$ by the family of symmetric maps $\mathcal{S}_{i,F}$ developed in Section 2.3.2, which are the general analogue to the trace map. However, Rubin and Silverberg show that the natural symmetric functions do not generate the function fields $k(\mathcal{X})$, and so cannot parameterize these varieties $\mathcal{X}$. Therefore, the symmetric maps do not yield an analogue to Figure 3.1, and do not compress elements of $\mathbb{F}_{q^{30}}$.

We concentrate on the refuted conjecture of Bosma, Hutton, and Verheul, that would have extended XTR.

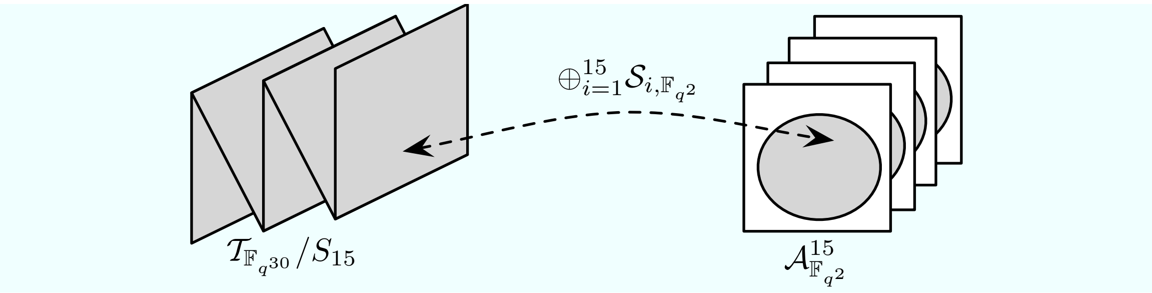

$\oplus_{i=1}^{15}\mathcal{S}_{i,\mathbb{F}_{q^2}}$
$\mathcal{T}_{\mathbb{F}_{q^{30}}}/S_{15}$
$\mathcal{A}^{15}_{\mathbb{F}_{q^2}}$

Figure 3.6: The symmetric maps are not a birational isomorphism.

Conjecture 3.20. *[BHV02, Conjecture 1 (d, e)-**BPV**] Let $n = de$, with $e > 1$, and let q be a prime-power.*

For an element $h \in T_n(\mathbb{F}_q) \subset \mathbb{F}_{q^n}$, let $P_h^{(d)}$ denote the characteristic polynomial of h over the subfield $\mathbb{F}_{q^d}$, and write

$$P_h^{(d)} = X^e + a_{e-1}X^{e-1} + \cdots + a_1X + a_0$$

Let u_d be the least value of u for which $Q_j \in \mathbb{Z}[X_1^{(0)}, \ldots, X_1^{(d-1)}, X_2^{(0)}, \ldots, X_2^{(d-1)}, \ldots, X_u^{(0)}, \ldots, X_u^{(d-1)}]$ exist, for $1 \leqslant j \leqslant e-u-1$, such that for every prime p and every element $h \in T_n(\mathbb{F}_q)$ that is not contained in a proper subfield of $\mathbb{F}_{p^n}$, the coefficient a_j of $P_h^{(d)}$ is given by

$$a_j = \bar{Q}_j(a_{e-1}, a_{e-1}^p, \ldots, a_{e-1}^{p^{d-1}}, a_{e-2}, a_{e-2}^p, \ldots, a_{e-2}^{p^{d-1}}, \ldots, a_{e-u}, a_{e-u}^p, \ldots, a_{e-1}^{p^{d-1}}),$$

for $1 \leqslant j \leqslant e-u-1$, where $\bar{Q}_j$ denotes Q_j with coefficients reduced modulo p.

Then $u_d = \lceil \varphi(n)/d \rceil$.

In the most cryptographically interesting case, when $n = 30$, the conjecture suggests that the norm-1 torus $T_{30}(\mathbb{F}_q)$ has the special property that all fifteen symmetric functions over $\mathbb{F}_{q^2}$ are determined by the first four symmetric functions (alternatively, that all thirty symmetric functions over $\mathbb{F}_q$ are determined by the first eight). This is a natural extension of the XTR situation, where all three symmetric functions over $\mathbb{F}_{q^2}$ are determined by the first.

For some choices of a field $\mathbb{F}_{q^n}$ and a subfield $\mathbb{F}_{q^d}$, it is not difficult to fix a representation of $\mathbb{F}_{q^n}$ and enumerate points in $T_n(\mathbb{F}_q)$ that explicitly demonstrate that Conjecture

(d, e)-**BPV** is false. Rubin and Silverberg do this in the cases

$$(q, n, d) \in \{(7, 30, 1), (7, 30, 2), (11, 30, 1), (11, 30, 2)\}.$$

More interesting is their algebro-geometric result.

Theorem 3.21. *[RS04a, Theorem 5.3] There is a finite set P of prime numbers such that if $\mathrm{char}(k) \notin P$, L/k is cyclic of degree 30, $k \subset F \subset L$ with $d := [F : k] = 1\,\mathrm{or}\,2$, and $\phi = (\phi_1, \ldots, \phi_d) : \mathcal{A}_F \longrightarrow \mathbb{A}^d$ is an isomorphism, then the function field $k(\mathcal{X}_F)$ is not generated by*

$$\{\phi_j \circ \mathcal{S}_{i,F} : 1 \leqslant i \leqslant \lceil 8/d \rceil, 1 \leqslant j \leqslant 8\}.$$

Proof. Rubin and Silverberg use algebraic geometry this is beyond the scope of this presentation, but we will sketch the ideas of their proof. Let us consider only the case $n = 30$, $d = 1$, so that $L = \mathbb{F}_{q^{30}}$ and $F = \mathbb{F}_q$, and $G = H = \mathrm{Gal}(L/k)$.

The proof is by contradiction in a special case, followed by a geometric lifting argument. We first consider the contradiction.

Theorem 3.19 demonstrates that the components of all thirty maps

$$\{\phi_j \circ \mathcal{S}_{i,F} : 1 \leqslant i \leqslant 30, 1 \leqslant j \leqslant 8\}$$

generate the function field $k(\mathcal{X}_F)$. Now, recall that Theorem 3.17 asserts that there is an isomorphism

$$f : \mathcal{A}_L/\Sigma_H \xrightarrow{\sim} (\mathcal{A}_k)^{30}$$

given by

$$f : \oplus_{i=1}^{30} \mathcal{S}_{i,F} : \mathcal{A}^L/\Sigma_H \longrightarrow (\mathcal{A}_k)^{30}.$$

The fundamental observation is that if we assume that the first eight symmetric functions $\mathcal{S}_{1,F}, \ldots, \mathcal{S}_{8,F}$ determine the remaining symmetric functions $\mathcal{S}_{9,F}, \ldots, \mathcal{S}_{30,F}$, we need only consider the "partial" map of the first eight components

$$s : \oplus_{i=1}^{8} \mathcal{S}_{i,F} : \mathcal{A}^L/\Sigma_H \longrightarrow (\mathcal{A}_k)^{8}$$

instead of the complete map of thirty components. Now, since f is an isomorphism, and we have assumed that the first eight symmetric functions determine the remaining twenty-two, it must be that s is an isomorphism.

However, if s is not an isomorphism, then we may conclude that the first eight symmetric functions do not determine the remaining twenty-two. In this case, the first eight symmetric functions do not generate $k(\mathcal{X}_F)$.

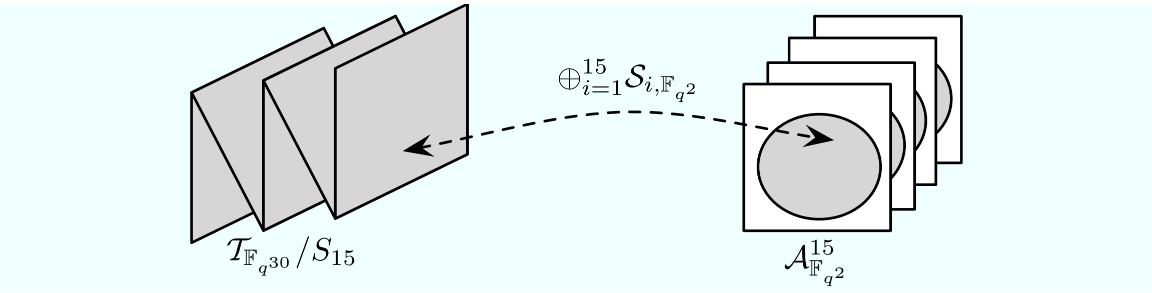
To achieve a contradiction, Rubin and Silverberg proved that s is not an isomorphism over $\mathbb{F}_{11^{30}}$. They did this by finding points $x, y \in \mathbb{T}_G(\mathbb{F}_{11^{30}})$ such that x and y were distinct modulo the action of Σ_H, but had the property that $s(x) = s(y)$. At this point, they were able to conclude that the symmetric functions $\mathcal{S}_{1,F}, \ldots, \mathcal{S}_{8,F}$ did not determine the remaining functions $\mathcal{S}_{9,F}, \ldots, \mathcal{S}_{30,F}$ over the field $\mathbb{F}_{11}$, refuting one instance of Conjecture 3.20.

It is important to note that these computational results could have been discovered without reference to any geometric interpretation. We could then say that some instances of Conjecture 3.20 are false. However, the computational result can be extended significantly with the help of some algebraic geometry.

The points x and y, and the function s, can be lifted to a field extension of $\mathbb{Q}_{11}$ of characteristic 0, yielding a neighbourhood, in the 11-adic topology, where s is not a bijection. It follows that s is not a birational isomorphism $\mathcal{X}_F \longrightarrow \mathbb{A}^8$ over all fields of characteristic 0.

Rubin and Silverberg then prove that outside a finite set of primes P, the function s reduced modulo a prime p is not a birational isomorphism over all fields of characteristic p. This lifting and reducing process relies on two deep results, Hensel's Lemma and Nakayama's Lemma; see [RS04a] for the complete proof. □

Theorem 3.21 establishes Figure 3.6, repeated below: the symmetric maps do not yield a birational parameterization of $\mathcal{T}_{\mathbb{F}_{q^{30}}}$.


$\oplus_{i=1}^{15} \mathcal{S}_{i,\mathbb{F}_{q^2}}$
$\mathcal{T}_{\mathbb{F}_{q^{30}}}/S_{15}$
$\mathcal{A}^{15}_{\mathbb{F}_{q^2}}$

Remark 3.22. Rubin and Silverberg also claim that no eight symmetric maps determine all of the others [RS03, Remark 5], and suggest that the symmetric maps cannot be manipulated in some fashion to parameterize the quotient varieties consider in Theorem 3.21.

By interpreting computational results in their elegant geometric framework, Rubin and Silverberg refute the conjectures most likely to extend the XTR scheme. Their result is a fitting end to the many pages of equivalent characterizations we have detailed in the previous two chapters.

But, where else do we look for extensions?

Chapter 4

Rational tori and CEILIDH

The purpose of this chapter is to present the CEILIDH cryptosystem [RS03], which extends the XTR cryptosystem. To understand the new cryptosystem, we use insight into the birational geometry of algebraic tori developed in Chapter 3. Unfortunately, CEILIDH does not provide a bandwidth savings greater than the $\varphi(6)/6 = 1/3$ of XTR. In addition, even though the new cryptosystem does not best the XTR cryptosystem compression ratio, it allows us to present new conjectures that, if established, will improve compression.

This chapter is organized in the following manner. First, we outline CEILIDH and explain the birational geometry underpinning the system. Then we introduce the new conjectures, and show how they would extend the system. Motivated by these conjectures and known partial results, we present the birational parameterizations that Rubin and Silverberg constructed.

For this chapter, fix a finite field $\mathbb{F}_q$ with $q > 3$ odd, and as always let σ denote the q-Frobenius endomorphism. We choose $q > 3$ odd only to ensure that certain simple field representations are possible.

4.1 Rational tori in cryptography

Figure 4.1 depicts the geometric perspective of XTR presented in Chapter 3. The key features of this interpretation are the birational maps between the geometric objects. Juxtaposed beneath Figure 4.1, Figure 4.2 depicts the geometry of CEILIDH. The key feature is the rightmost birational isomorphism.

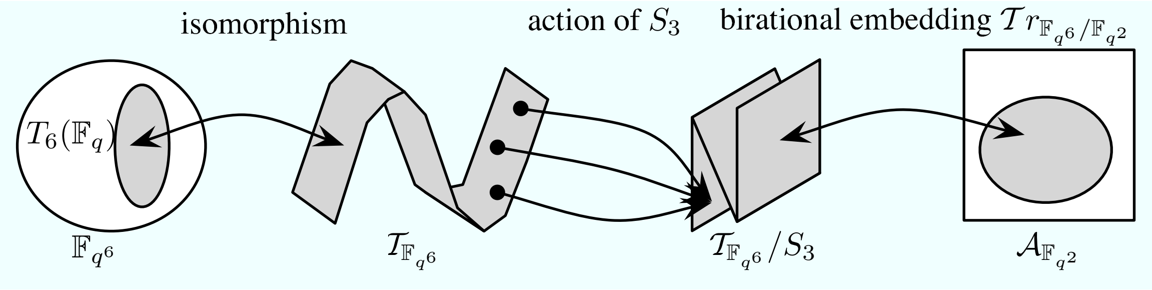

isomorphism
action of S_3
birational embedding $\mathcal{T}r_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}$
$T_6(\mathbb{F}_q)$
$\mathbb{F}_{q^6}$
$\mathcal{T}_{\mathbb{F}_{q^6}}$
$\mathcal{T}_{\mathbb{F}_{q^6}}/S_3$
$\mathcal{A}_{\mathbb{F}_{q^2}}$

Figure 4.1: The geometry of the XTR cryptosystem.

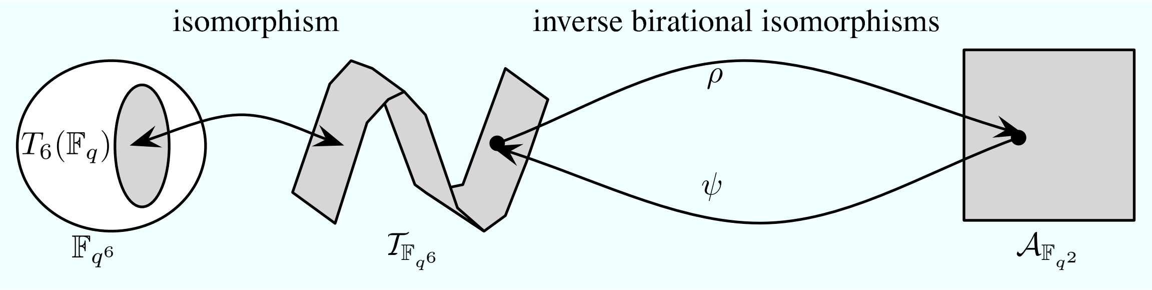

isomorphism
inverse birational isomorphisms
ρ
ψ
$T_6(\mathbb{F}_q)$
$\mathbb{F}_{q^6}$
$\mathcal{T}_{\mathbb{F}_{q^6}}$
$\mathcal{A}_{\mathbb{F}_{q^2}}$

Figure 4.2: The geometry of the CEILIDH cryptosystem.

In the XTR cryptosystem, the trace map embeds

$$(\mathcal{T}_{\mathbb{F}_{q^6}}/S_3)(\mathbb{F}_q) \hookrightarrow \mathcal{A}_{\mathbb{F}_{q^2}}(\mathbb{F}_q),$$

and the challenge was to understand the quotient variety $\mathcal{T}_{\mathbb{F}_{q^6}}/S_3$. The CEILIDH cryptosystem avoids forming a quotient variety, which simplifies the system significantly. It exploits "custom-built" inverse parameterizations

$$\rho : \mathcal{T}_{\mathbb{F}_{q^6}}(\mathbb{F}_q) \xrightarrow{\sim} \mathbb{A}^2(\mathbb{F}_q)$$

and

$$\psi : \mathbb{A}^2(\mathbb{F}_q) \xrightarrow{\sim} \mathcal{T}_{\mathbb{F}_{q^6}}(\mathbb{F}_q).$$

At this point we can appeal to the canon of algebraic geometry, because the existence of a birational isomorphism between the norm-1 torus $\mathcal{T}_{\mathbb{F}_{q^6}}$ and two dimensional affine space $\mathbb{A}^2$ means that the norm-1 torus is rational.

Definition 4.1. *Let V be an affine variety. If there exists a birational isomorphism between V and $\mathbb{A}^d$ for some positive integer d, we say that the variety V is rational.*

It follows from Theorem 2.36 that if the norm-1 torus $\mathcal{T}_{\mathbb{F}_{q^n}}$ is rational, it must be birationally isomorphic to $\mathbb{A}^{\varphi(n)}$. This is because $\mathcal{T}_{\mathbb{F}_{q^n}}$ is isomorphic as a group to $\mathbb{G}_m^{\varphi(n)}$, which is birationally isomorphic to $\mathbb{A}^{\varphi(n)}$. Thus, if the norm-1 torus is rational, we have an identification

$$\mathcal{T}_{\mathbb{F}_{q^n}} \xrightarrow{\sim} \mathbb{A}^{\varphi(n)}.$$

Since this identification is a birational parameterization, it may be undefined on varieties of strictly smaller dimension than $\mathcal{T}_{\mathbb{F}_{q^n}}$; therefore some torus elements may not by compactly represented. For cryptographically interesting tori and field sizes q, the number of such elements is $O(1/q)$, and therefore negligible. In fact, the constructions we present are undefined only at a small constant number of torus elements, and we therefore do not even consider undefined points in the protocols presented later.

At this point, it should be clear that the rationality of the torus $\mathcal{T}_{\mathbb{F}_{q^n}}$ is closely connected to the existence of cryptosystems providing large compression ratios. Luckily, we can connect the question of the rationality of the norm-1 torus to existing work.

Conjecture 4.2. *(Voskresenskii, [Vos98]) If L is a cyclic extension of a field k, then the norm-1 torus $\mathcal{T}_L$ is rational.*

As stated, Conjecture 4.2 is more general than we need. Because $\mathbb{F}_{q^n}$ is always a cyclic extension of $\mathbb{F}_q$, the conjecture states that $\mathcal{T}_{\mathbb{F}_{q^n}}$ is rational for every n. If we believe the conjecture, we should be able to achieve a cryptosystem with compression ratio $n/\varphi(n)$ for every integer n — which is remarkable, because $n/\varphi(n)$ can be made arbitrarily large. However,

$$n/\varphi(n) < \ln \ln n$$

for all $n > 6$, so the degree of the field extension quickly becomes too large for practical use. Additionally, in practice protocols operate in a subgroup of the torus T_n, and in this subgroup, classical attacks will be hopelessly impractical, allowing a much smaller torus to be used. It follows that arbitrarily efficient cryptographic protocols could be realized — if the rational isomorphisms of Definition 4.1 were made explicit and implemented efficiently, but there is not always practical value in doing so.

Unfortunately, Voskresenskii's Conjecture appears unassailable. However, it certainly is a natural conjecture that, if established, promises to significantly improve the XTR cryptosystem. In this sense, Conjecture 4.2 replaces Conjecture 3.20.

Let $n = |\operatorname{Gal}(L/k)|$ be the degree of the extension field. Two results suggest that it is possible to construct explicit birational isomorphisms between $\mathcal{T}_{\mathbb{F}_{q^n}}$ and $\mathbb{A}^{\varphi(n)}$ for certain integers n. Voskresenskii [Vos98, Chapter 2] shows that $\mathcal{T}_L$ is rational when n is a prime power. More important to us, Klyachko [Kly88] shows $\mathcal{T}_L$ is rational when n is a product of two prime powers. Voskresenskii [Vos99] claimed to have a proof for general n in the case where k is of characteristic zero, but according to Rubin and Silverberg [RS03, Section 4], there is a flaw in his argument.

4.2 The construction of CEILIDH

Motivated by Klyachko's result that $\mathcal{T}_{\mathbb{F}_{q^6}}$ is rational, this section presents the explicit parameterization of $T_6(\mathbb{F}_q)$ given by Rubin and Silverberg [RS03, Section 5]. Recall that

$$T_6(\mathbb{F}_q) = \left\{ x \in \mathbb{F}_{q^6}^\times : N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(x) = 1 \,\text{and}\, N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}(x) = 1 \right\}.$$

We will find explicit maps ρ and ψ such that

$$\rho : T_6(\mathbb{F}_q) \xrightarrow{\sim} \mathbb{A}^2(\mathbb{F}_q)$$

and

$$\psi : \mathbb{A}^2(\mathbb{F}_q) \longrightarrow T_6(\mathbb{F}_q)$$

are inverse birational isomorphisms when lifted to T_6 and $\mathbb{A}^2$. Our presentation follows Rubin and Silverberg's original presentation, adding small details and diagrams where helpful.

4.2.1 Norm-1 elements

Since $\mathbb{F}_{q^6}$ is a quadratic extension of $\mathbb{F}_{q^3}$, it is easy to represent the elements with norm 1. Let $\mathbb{F}_{q^6} = \mathbb{F}_{q^3}(x)$ for a suitable element x, and suppose the non-trivial element of

$\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^3})$ is σ^3. It is clear that for every $\beta \in \mathbb{F}_{q^3}$, the element $(\beta + x)/(\beta + \sigma^3(x))$ has norm

$$N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}\left(\frac{\beta + x}{\beta + \sigma^3(x)}\right) = \left(\frac{\beta + x}{\beta + \sigma^3(x)}\right)\sigma^3\left(\frac{\beta + x}{\beta + \sigma^3(x)}\right) = \left(\frac{\beta + x}{\beta + \sigma^3(x)}\right)\left(\frac{\beta + \sigma^3(x)}{\beta + x}\right) = 1.$$

In fact, almost all elements with norm 1 are of this form.

Theorem 4.3. *(Hilbert's Theorem 90) Let L be a finite Galois extension of k, and let $G = \mathrm{Gal}(L/k)$ by cyclic with generator σ. Then an element $\beta \in L$ has norm 1 if and only if $\beta = \gamma/\sigma(\gamma)$ for some element $\gamma \in L$.*

It follows from Theorem 4.3 that only the identity element 1 is not of the special form $(\beta + x)/(\beta + \sigma^3(x))$.

Let $\{\alpha_1, \alpha_2, \alpha_3\}$ be a basis for $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$; recalling that $\mathbb{F}_{q^6} = \mathbb{F}_{q^3}(x)$, we have that $\{\alpha_1, \alpha_2, \alpha_3, x\alpha_1, x\alpha_2, x\alpha_3\}$ is a basis for $\mathbb{F}_{q^6}$ over $\mathbb{F}_q$. Define an injective map

$$\xi : \mathbb{A}^3(\mathbb{F}_q) \hookrightarrow \mathbb{F}_{q^6}^\times$$

by

$$\xi(u_1, u_2, u_3) = \frac{\gamma + x}{\gamma + \sigma^3(x)},$$

with

$$\gamma = \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3.$$

We saw that $N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}(\xi(u_1, u_2, u_3)) = 1$ for each triple (u_1, u_2, u_3).

If we define

$$U = \left\{(u_1, u_2, u_3) : N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\xi(u_1, u_2, u_3)) = 1\right\},$$

then by Theorem 4.3, the restriction of ξ to U gives a bijection

$$\xi : U \xrightarrow{\sim} T_6(\mathbb{F}_q) - \{1\}.$$

Moreover, since σ is a polynomial function, ξ is a morphism.

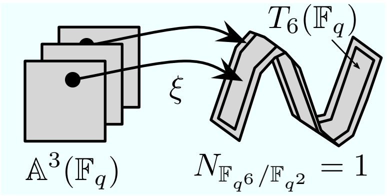

$T_6(\mathbb{F}_q)$
ξ
$\mathbb{A}^3(\mathbb{F}_q)$
$N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} = 1$

Figure 4.3: The map ξ on all $\mathbb{A}^3(\mathbb{F}_q)$.

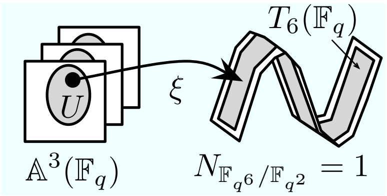

$T_6(\mathbb{F}_q)$
ξ
U
$\mathbb{A}^3(\mathbb{F}_q)$
$N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} = 1$

Figure 4.4: The map ξ restricted to U.

4.2.2 The variety U

Rubin and Silverberg claim that U is a hypersurface in $\mathbb{A}^3(\mathbb{F}_q)$ defined by a single quadratic equation in u_1, u_2, u_3, and we will demonstrate this. It suffices to establish the claim for a single basis of $\mathbb{F}_{q^6}$ over $\mathbb{F}_q$, so let $\{\alpha, \sigma^2(\alpha), \sigma^4(\alpha)\}$ be a normal basis of $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$, and let $\mathbb{F}_{q^2} = \mathbb{F}_q(x)$ with $x^2 = R$ and R a non-square in $\mathbb{F}_q$. (Note that a non-square R always exists, since q is odd.) The pairwise products $\{\alpha, \sigma^2(\alpha), \sigma^4(\alpha), x\alpha, x\sigma^2(\alpha), x\sigma^4(\alpha)\}$ form a basis of $\mathbb{F}_{q^6}$ over $\mathbb{F}_q$.

An element $u = (u_1, u_2, u_3)$ of U satisfies $N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\xi(u)) = 1$, so that denoting

$$\gamma = \alpha u_1 + \sigma^2(\alpha)u_2 + \sigma^4(\alpha)u_3$$

we have

$$1 = \xi(u)\sigma^2(\xi(u))\sigma^4(\xi(u)) = \left(\frac{\gamma + x}{\gamma - x}\right)\sigma^2\left(\frac{\gamma + x}{\gamma - x}\right)\sigma^4\left(\frac{\gamma + x}{\gamma - x}\right).$$

Thus

$$(\gamma + x)\sigma^2(\gamma + x)\sigma^4(\gamma + x) = (\gamma - x)\sigma^2(\gamma - x)\sigma^4(\gamma - x),$$

and since σ^2 fixes x, this expression simplifies to

$$2x\left(\sigma(\gamma)\sigma^2(\gamma) + \sigma(\gamma)\sigma^4(\gamma) + \sigma^2(\gamma)\sigma^4(\gamma) - R\right) = 0.$$

Since σ also fixes u_1, u_2, u_3, we see that each term $\sigma(\gamma), \sigma^2(\gamma), \sigma^4(\gamma)$ is linear in the variables u_1, u_2, u_3. It follows that U is the zero locus of a quadratic in u_1, u_2, u_3, as claimed.

4.2.3 Parameterizing U

Rubin and Silverberg parameterize the quadratic surface $U \subset \mathbb{A}^3(\mathbb{F}_q)$ by a map with domain $\mathbb{A}^2(\mathbb{F}_q)$.

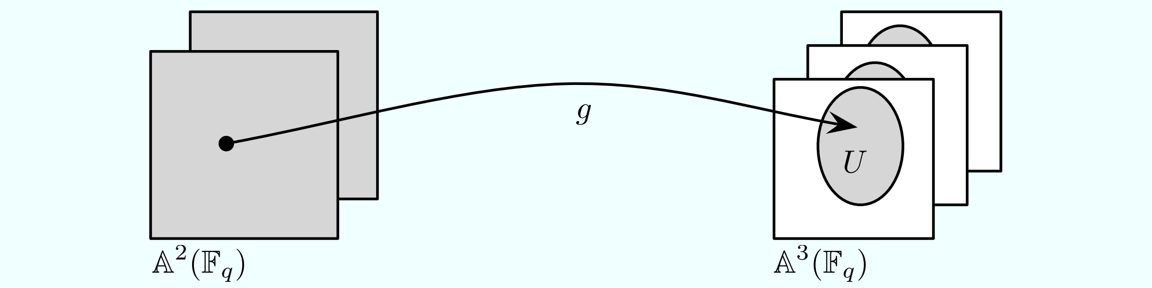


Figure 4.5: Parameterizing U.

We use the construction called "stereographic projection from a point". As an example of projection from a point, Figure 4.6 illustrates the familiar identification of the sphere with the plane. (Note that the north pole itself is not identified with a point of the plane.)

Distinguish a point $a = (a_1, a_2, a_3)$ on the surface U. We are going to identify the surface U with the plane by projecting from the point a, which is the equivalent of the north pole in Figure 4.6.

We can assume that the plane tangent to U at the point a is given by the single equation $u_1 = \alpha_1$, since we are free to modify our basis $\{\alpha_1, \alpha_2, \alpha_3\}$.

For each pair of parameters $(v_1, v_2) \in \mathbb{A}^2(\mathbb{F}_q)$, consider the line

$$L : a + t(1, v_1, v_2).$$

We appeal to Bezout's Theorem [Har95, Theorem 18.3] to show that L intersects U at precisely two points. (The line L can be seen in Figure 4.8.)

Remark 4.4. Bezout's Theorem applies only to projective varieties, but it is possible to define projective varieties $\mathcal{L}$ and $\mathcal{U}$ corresponding to L and U, verify that these projective

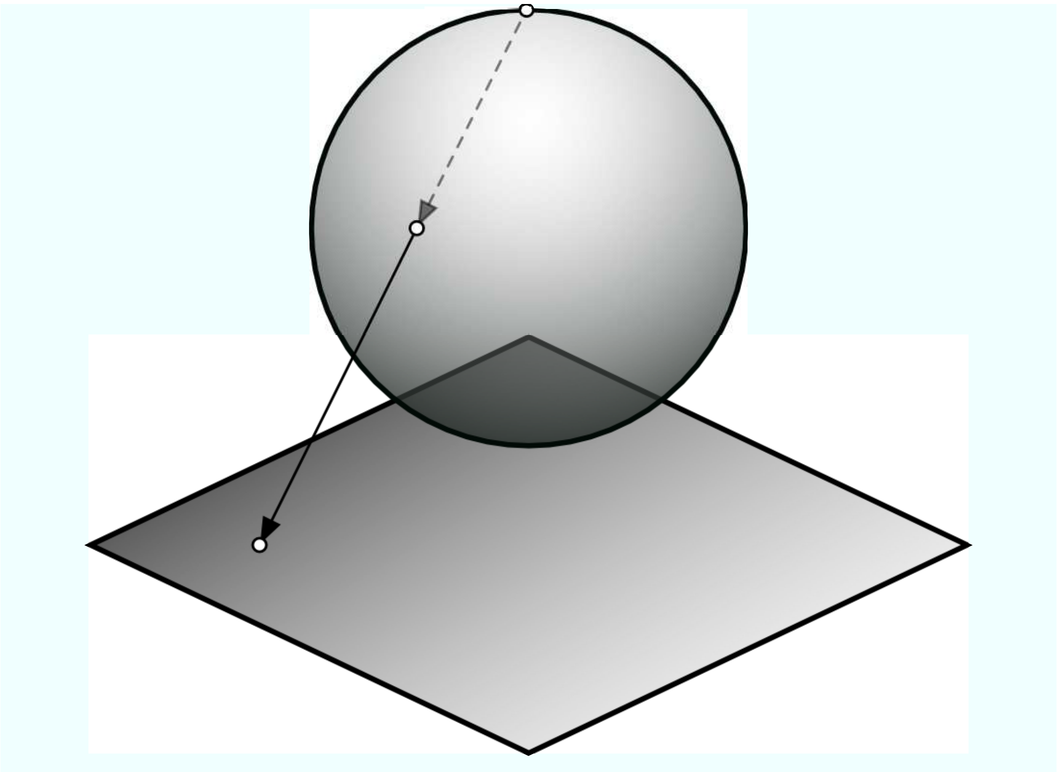


Figure 4.6: Stereographic projection from the north pole identifies the sphere and the plane.

varieties satisfy the conditions of Bezout's Theorem, consider intersections "at infinity", and conclude that L intersects U at two points. We appeal to the reader's understanding of algebraic geometry at this point, because a complete demonstration would take us far afield.

One of the points of intersection is the trivial intersection $t = 0$ at the point a; the second intersection is at a point

$$a + \frac{1}{f(v_1, v_2)}(1, v_1, v_2),$$

where $f(v_1, v_2) \in \mathbb{F}_q[v_1, v_2]$ is an explicit polynomial that can be easily computed. (The polynomial f depends on the point a and the choice of basis for $\mathbb{F}_{q^6}$ over $\mathbb{F}_q$. We detail the calculation of f, for some finite fields of special form, in Examples 4.7 and 4.8.)

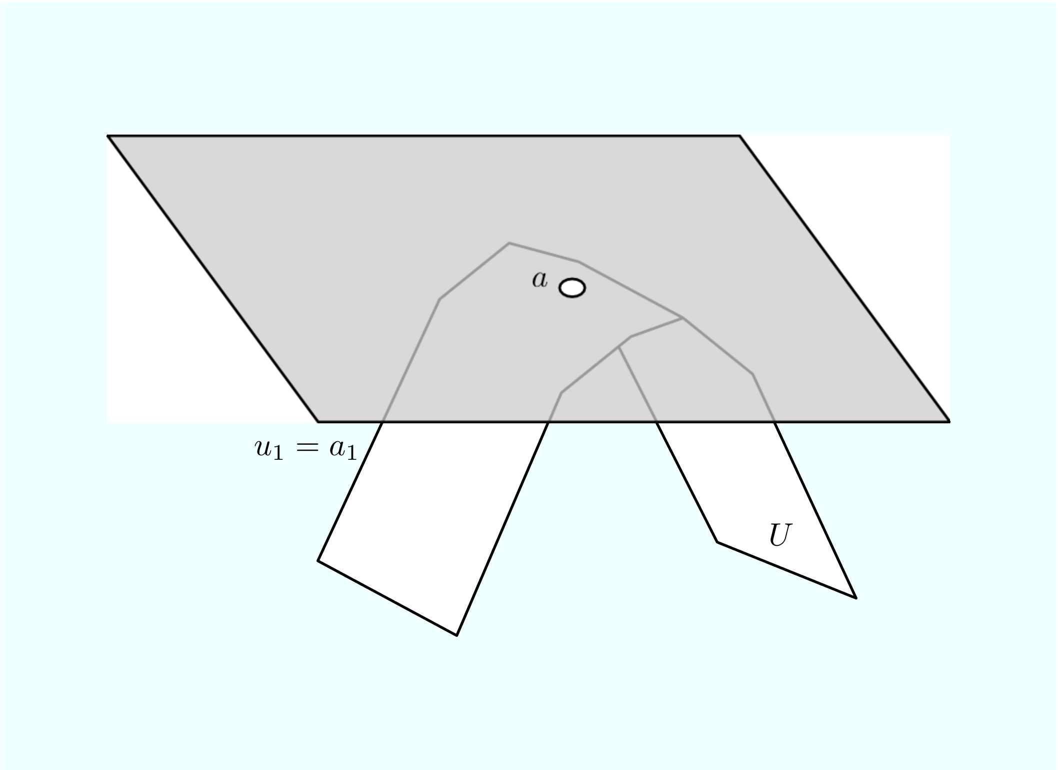


Figure 4.7: The plane tangent to U at a.

Remark 4.5. The set $V(f)$ of points (v_1, v_2) where $f(v_1, v_2) = 0$ corresponds to the "intersections at infinity" in Bezout's Theorem.

Define a bijection

$$g : \mathbb{A}^2(\mathbb{F}_q) - V(f) \xrightarrow{\sim} U - \{a\},$$

where g maps a pair (v_1, v_2) to the non-trivial point of intersection defined above:

$$g(v_1, v_2) = a + \frac{1}{f(v_1, v_2)}(1, v_1, v_2).$$

Figure 4.8 shows the map g.

The map g is clearly an injection, since no two distinct lines intersect at more than one point. It follows that the composition $\xi \circ g$ defines a bijection

$$\psi : \mathbb{A}^2(\mathbb{F}_q) - V(f) \xrightarrow{\sim} T_6(\mathbb{F}_q) - \{1, \xi(a)\}.$$

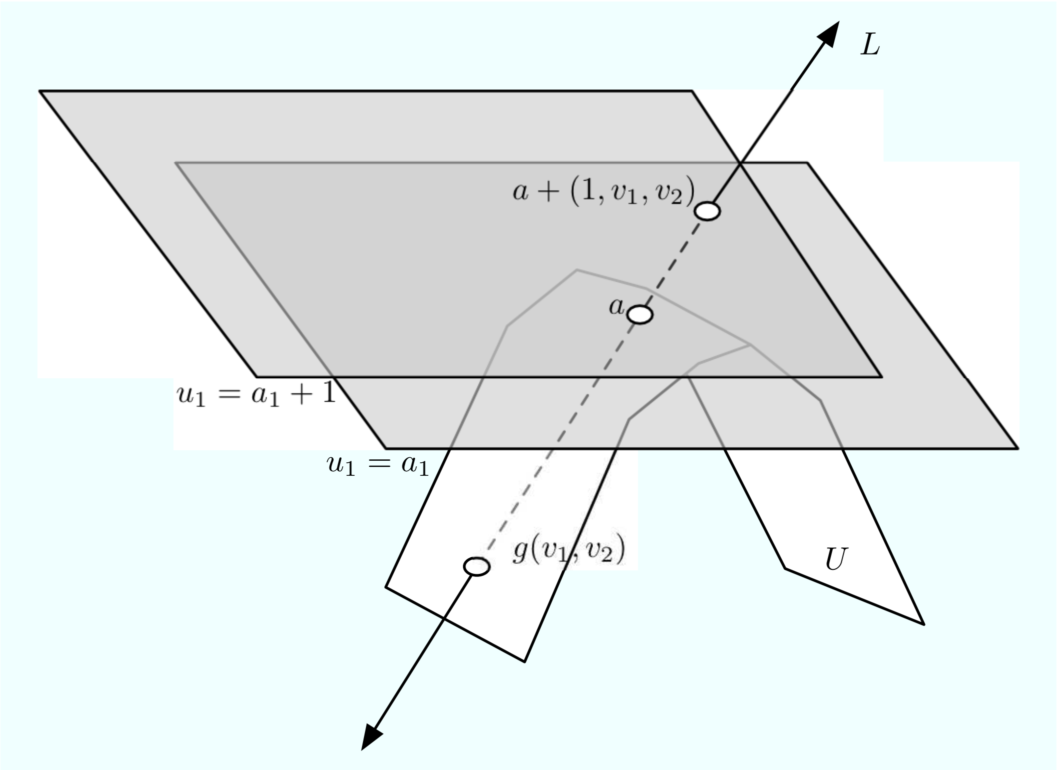


Figure 4.8: The map g is the projection, from the point a, of (v_1, v_2) onto the surface U.

Rubin and Silverberg also compute the inverse of ψ. Given an element $\beta \in T_6(\mathbb{F}_q) - \{1, \xi(a)\}$, express β as

$$\beta = \beta_1 + \beta_2 x,$$

with β_1 and β_2 in $\mathbb{F}_{q^3}$. Observe that $\beta_2 \neq 0$, since if $\beta_2 = 0$ we would have

$$N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}(\beta) = N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}(\beta_1) = \beta_1^{q^3+1} = \beta_1^2 = 1,$$

so $\beta_1 = \pm 1$. However,

$$N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(-1) = (-1)^{q^4+q^2+1} = (-1)(-1)(-1) = -1 \neq 1,$$

so we must have $\beta_1 = 1$. However, we assumed $\beta \neq 1$, so we may conclude that $\beta_2 \neq 0$.

Write

$$(1 + \beta_1)/\beta_2 = u_1\alpha_1 + u_2\alpha_2 + u_3\alpha_3,$$

with each u_i in $\mathbb{F}_q$. Then it is straightforward to verify that

$$\rho : T_6(\mathbb{F}_q) - \{1, \xi(a)\} \xrightarrow{\sim} \mathbb{A}^2(\mathbb{F}_q) - V(f)$$
$$\rho(\beta) = \left(\tfrac{u_2 - a_2}{u_1 - a_1}, \tfrac{u_3 - a_3}{u_1 - a_1}\right)$$

is an inverse to ψ.

4.2.4 The complete parameterization

Observe that in the preceding discussion, at no time did we actually that an input x was an element of $\mathbb{F}_{q^6}^\times$. It follows that our bijections ρ and ψ are really more than bijections; they are defined over $\bar{\mathbb{F}}_q$.

Theorem 4.6. *[RS03, Theorem 10] The maps ρ and ψ lift to inverse birational isomorphisms between the norm-1 torus $\mathcal{T}_{\mathbb{F}_{q^6}}$ and the affine plane $\mathbb{A}^2$.*

We have a birational parameterization of the norm-1 torus T_6!

4.3 Explicit rational maps

To gain familiarity with the choices involved in Rubin and Silverberg's construction, let us work some examples. The first was given by Rubin and Silverberg.

Example 4.7. [RS03, Example 11] Fix a prime power $q \equiv 2 (\operatorname{mod} 9)$, and observe that a primitive ninth root of unity ζ_9 exists in $\mathbb{F}_{q^6}$. Thus a primitive third root of unity $\zeta_3 = \zeta_9^3$ exists in $\mathbb{F}_q$; let

$$x = \zeta_3$$

and let

$$y = \zeta_9 + \zeta_9^{-1}.$$

We have that $\mathbb{F}_{q^2} = \mathbb{F}_q(x)$, since $x^2 + x + 1 = 0$, and that $\mathbb{F}_{q^3} = \mathbb{F}_q(y)$, since $y^3 - 3y + 1 = 0$ and y satisfies no non-zero polynomial of degree less than 3. Choosing the basis $\{1, y, y^2 - 2\}$

for $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$, and computing the Galois conjugates for these basis elements in terms of y, we find the following relations:

$$\begin{aligned} y^{q^4} &= y^2 - 2 \\ (y^2-2)^{q^4} &= -(y^2-2) - y \\ y^{q^2} &= -(y^2-2) - y \\ (y^2-2)^{q^2} &= y. \end{aligned}$$

For all triples (u_1, u_2, u_3), the image $\xi(u_1, u_2, u_3)$ satisfies the norm condition over the cubic subfield $\mathbb{F}_{q^3}$, so we need only find the quadratic equation that defines

$$U = \{(u_1, u_2, u_3) \in \mathbb{A}^3(\mathbb{F}_q) : N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\xi(u_1, u_2, u_3)) = 1\}.$$

Recall that $\xi(u_1, u_2, u_3) = \frac{\gamma + x}{\gamma + \sigma^3(x)}$ with $\gamma = u_1 + yu_2 + (y^2-2)u_3$. Since $N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\beta) = \beta\sigma^2(\beta)\sigma^4(\beta) = \beta^{q^4+q^2+1}$, we have

$$U = \left\{ (u_1, u_2, u_3) \in \mathbb{A}^3(\mathbb{F}_q) : \left(\frac{\gamma + x}{\gamma + \sigma^3(x)} \right)^{q^4+q^2+1} = 1 \right\}.$$

Since $q \equiv 2 (\operatorname{mod} 3)$, we find $\sigma^3(x) \equiv x^{q^3} \equiv x^q \equiv x^2 (\operatorname{mod} q)$, so that U is the zero locus (in the variables u_1, u_2, u_3) of

$$(\gamma^{q^4} + x)(\gamma^{q^2} + x)(\gamma + x) = (\gamma^{q^4} + x^2)(\gamma^{q^2} + x^2)(\gamma + x^2).$$

Subtracting the right side from the left, we get

$$(x - x^2)\left[(\gamma\gamma^{q^2} + \gamma^{q^2}\gamma^{q^4} + \gamma\gamma^{q^4}) - (\gamma + \gamma^{q^2} + \gamma^{q^4}) \right] = 0. \qquad (4.1)$$

The following relations hold for the Galois conjugates of γ:

$$\begin{aligned} \gamma^{q^4} &= u_1^{q^4} + y^{q^4} u_2^{q^4} + (y^2-2)^{q^4} u_3^{q^4} \\ &= u_1 + (y^2-2)u_2 - ((y^2-2) + y)u_3 \\ \gamma^{q^2} &= u_1^{q^2} + y^{q^2} u_2^{q^2} + (y^2-2)^{q^2} u_3^{q^2} \\ &= u_1 - ((y^2-2) + y)u_2 + yu_3. \end{aligned}$$

These relations allow us to simplify (4.1) above to

$$3(x - x^2)(u_1^2 - u_2^2 - u_3^2 - u_1 + u_2 u_3) = 0,$$

and since $3 \neq 0$, by our assumption on q, and $x - x^2 \neq 0$, we have

$$U = V(u_1^2 - u_2^2 - u_3^2 - u_1 + u_2 u_3),$$

the zero locus of the quadratic $u(u_1, u_2, u_3) = u_1^2 - u_2^2 - u_3^2 - u_1 + u_2 u_3$ in the three variables u_1, u_2, u_3.

Distinguish the point

$$a = (0, 0, 0).$$

The Jacobian matrix of U evaluated at the point a is

$$\mathrm{Jac}(U)(a) = \begin{pmatrix} \frac{\partial u}{\partial u_1} & \frac{\partial u}{\partial u_2} & \frac{\partial u}{\partial u_3} \end{pmatrix} = \begin{pmatrix} 2u_1 - 1 & -2u_2 + u_3 & -2u_3 + u_2 \end{pmatrix}(a) = \begin{pmatrix} -1 & 0 & 0 \end{pmatrix},$$

and we have that the tangent plane to U at the point a is $u_1 = a_1 = 0$, as desired.

For each point (v_1, v_2) of $\mathbb{A}^2(\mathbb{F}_q)$ we need to compute the intersection of U and the line $a + t(1, v_1, v_2)$. Since $a = (0, 0, 0)$, we make the substitutions

$$\begin{aligned} u_1 &= t \\ u_2 &= tv_1 \\ u_3 &= tv_2. \end{aligned}$$

We have

$$u(t, tv_1, tv_2) = t^2 - (tv_1)^2 - (tv_2)^2 - t + (tv_1)(tv_2) = 0.$$

Ignoring the trivial solution, $t = 0$, that corresponds to the intersection at the point a, we compute that

$$t = 1/(1 - v_1^2 - v_2^2 - v_1 v_2),$$

and that the polynomial $f(v_1, v_2)$ is

$$f(v_1, v_2) = 1 - v_1^2 - v_2^2 - v_1 v_2.$$

Thus, the map g is given by

$$g(v_1, v_2) = (1, v_1, v_2)/(1 - v_1^2 - v_2^2 - v_1 v_2)$$

and therefore we have the bijection

$$\begin{array}{rcl} \multicolumn{3}{c}{\psi : \mathbb{A}^2(\mathbb{F}_q) - V(f) \xrightarrow{\sim} T_6(\mathbb{F}_q) - \{1, \xi(a)\}} \\ \psi(v_1, v_2) & = & \xi(\frac{1}{f(v_1,v_2)}, \frac{v_1}{f(v_1,v_2)}, \frac{v_2}{f(v_1,v_2)}) \\ & = & \frac{1+yv_1+(y^2-2)v_2+f(v_1,v_2)x}{1+yv_1+(y^2-2)v_2+f(v_1,v_2)x^2}. \end{array}$$

Finally, note that $\xi(a) = \zeta_3/\zeta_3^2 = \zeta_3^2$. For an element $\beta = \beta_1 + \beta_2 x$ of $T_6(\mathbb{F}_q) - \{1, \zeta_3^2\}$, write

$$(1 + \beta_1)/\beta_2 = u_1 + yu_2 + (y^2 - 2)u_3.$$

Then the inverse map ρ is

$$\rho(\beta) = (u_2/u_1, u_3/u_1).$$

Figure 4.9 diagrams the complete example.

Summarizing the example, we chose a basis of $\mathbb{F}_{q^6}$ over $\mathbb{F}_q$ and a point a such that the tangent plane to the variety U at a had special form. We then used the geometric technique of stereographic projection to associate each point of a plane with a distinct point of the variety U. Finally, we identified the variety U and the norm-1 torus $T_6(\mathbb{F}_q)$, resulting in inverse birational isomorphisms between T_6 and $\mathbb{A}^2$.

We have successfully presented a rational parameterization of the torus $T_6(\mathbb{F}_q)$ over a large family of fields $\mathbb{F}_q$. (In fact, this example applies also to prime powers $q \equiv 5(\operatorname{mod} 9)$ with minor transpositions throughout.)

The following example is original.

Example 4.8. Let q be a prime power such that $q \equiv 1(\operatorname{mod} 3)$, so that there exists a non-cube R modulo q, and such that $q \equiv 3(\operatorname{mod} 4)$, so that -1 is not a square modulo q. (Recall that R is a non-cube exactly when $R^{(q-1)/3} \not\equiv 1(\operatorname{mod} q)$, so it is easy to recognize a suitable R.) Let $y^3 = R$; then $\mathbb{F}_{q^3} = \mathbb{F}_q(y)$, and $\{R, y + y^2, y^2 - y\}$ is a basis of $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$. Also, we have that $R^{(q-1)/3}$ is a primitive cube root of unity; write $q = 3k + 1$ and let

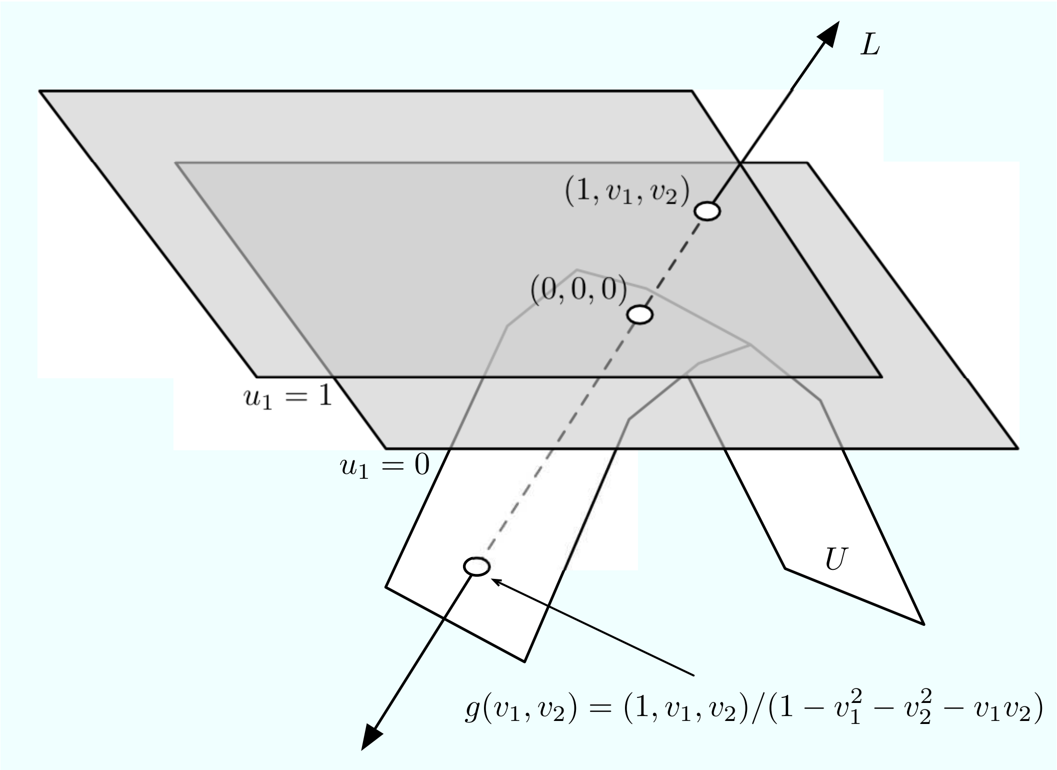


Figure 4.9: The geometry of Example 4.7.

$\omega = R^k$, so that $\omega^2 + \omega + 1 = 0$. Finally, let $x^2 = S$, with S a non-square; then we have that $\mathbb{F}_{q^2} = \mathbb{F}_q(x + 1)$. The following relations hold among the Galois conjugates of y:

$$\begin{aligned} y^{q^2} &= \omega^2 y \\ y^{q^4} &= \omega y \\ y^{2q^2} &= \omega y^2 \\ y^{2q^4} &= (\omega y^2)^{q^2} = \omega^2 y^2. \end{aligned}$$

If we let $\gamma = Ru_1 + (y + y^2)u_2 + (y^2 - y)u_3$, then U is defined by the locus of

$$(\gamma + x)(\gamma^{q^2} + x)(\gamma^{q^4} + x) \quad = \quad (\gamma - x)(\gamma^{q^2} - x)(\gamma^{q^4} - x).$$

This locus is the zero set of a quadratic u, with

$$u(u_1, u_2, u_3) = S + 3R(Ru_1^2 - u_2^2 + u_3^2) = 0.$$

The Jacobian matrix of U is

$$\mathrm{Jac}(U) = \left(\begin{array}{ccc} \frac{\partial u}{\partial u_1} & \frac{\partial u}{\partial u_2} & \frac{\partial u}{\partial u_3} \end{array} \right) = \left(\begin{array}{ccc} 6R^2u_1 & -6Ru_2 & 6Ru_3 \end{array} \right).$$

In the previous example, we considered the case when the tangent plane to U at a point a was expressed as the plane $u_1 = a_1$; now we vary from this template slightly. Instead of the plane $u_1 = a_1$, we distinguish a point a such that the tangent plane to U at a is $u_3 = a_3$. (Alternatively, we could reorder our basis elements.) For a point $a = (a_1, a_2, a_3)$ on the surface U, to be determined shortly, we consider two cases.

First, if $a_1 = a_2 = 0$, then the remaining coordinate a_3 must be a solution to the equation $S + 3Ru_3^2 = 0$.

Second, if $a_1 = a_3 = 0$, then the remaining coordinate a_2 must be a solution to the equation $S - 3Ru_2^2 = 0$.

Since -1 is not a square modulo q, one of the preceding equations has a solution; without loss of generality, suppose $a_1 = a_2 = 0$ and select an arbitrary root

$$a_3 = \sqrt{-S/(3R)}.$$

Then the tangent plane to U at the point

$$a = (0, 0, \sqrt{-S/(3R)})$$

satisfies $u_3 = a_3$.

For each pair $(v_1, v_2) \in \mathbb{F}_q \times \mathbb{F}_q$, we consider the intersections of U and the line $a + t(v_1, v_2, 1)$. Substituting, we have

$$\begin{array}{rcl} S + 3R(R(tv_1)^2 - (tv_2)^2 + (a_3+t)^2) & = & 0 \\ Rt^2v_1^2 - t^2v_2^2 + a_3^2 + 2a_3t + t^2 & = & -S/(3R) \\ Rt^2v_1^2 - t^2v_2^2 + 2a_3t + t^2 & = & 0, \end{array}$$

so that the non-trivial intersection has parameter

$$t = -2a_3/(Rv_1^2 - v_2^2 + 1) = -\left(2\sqrt{-S/(3R)}\right)/(Rv_1^2 - v_2^2 + 1),$$

which results in the polynomial

$$f(v_1, v_2) = -(1/(2a_3))(Rv_1^2 - v_2^2 + 1) = -\left(1/(2\sqrt{-S/(3R)})\right)(Rv_1^2 - v_2^2 + 1).$$

Finally, we can write down equations defining the maps ψ and ρ.

$$\begin{array}{c} \psi : \mathbb{A}^2(\mathbb{F}_q) - V(f) \xrightarrow{\sim} T_6(\mathbb{F}_q) - \{1, \xi(a)\} \\ \psi(v_1, v_2) = \frac{Rv_1+(y+y^2)v_2+(y^2-y)+f(v_1,v_2)x}{Rv_1+(y+y^2)v_2+(y^2-y)-f(v_1,v_2)x} \end{array} .$$

Figure 4.10 diagrams the parts of the preceding construction.

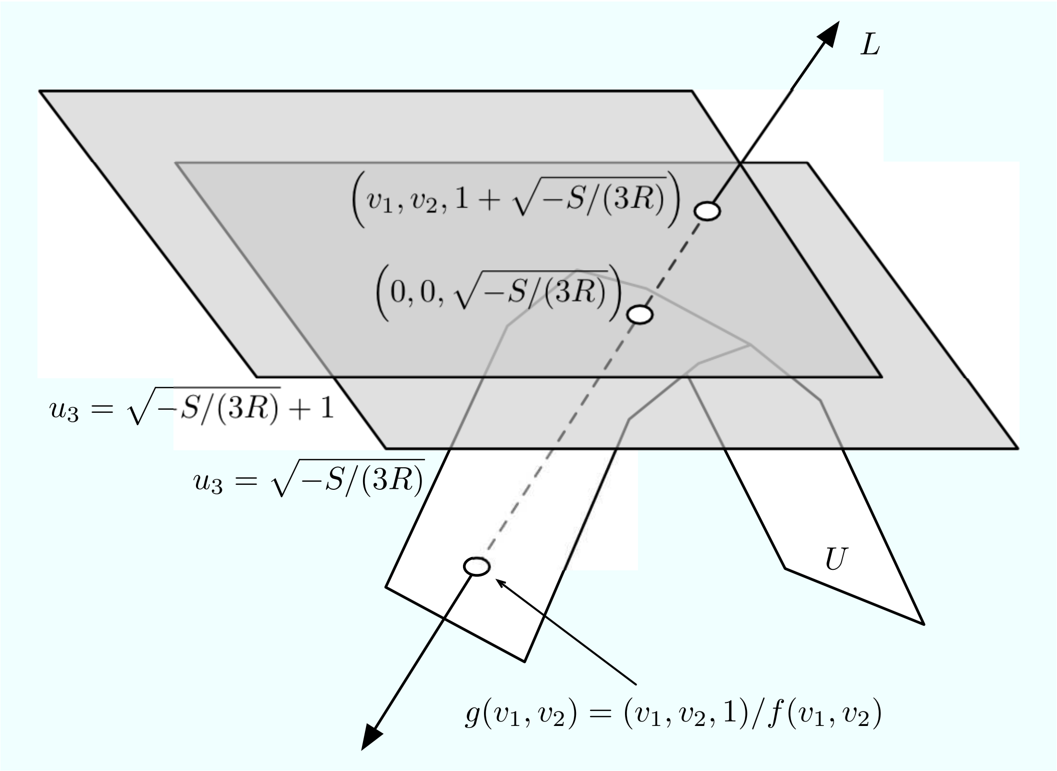

L
$\left(v_1, v_2, 1 + \sqrt{-S/(3R)}\right)$
$\left(0, 0, \sqrt{-S/(3R)}\right)$
$u_3 = \sqrt{-S/(3R)} + 1$
$u_3 = \sqrt{-S/(3R)}$
U
$g(v_1, v_2) = (v_1, v_2, 1)/f(v_1, v_2)$

Figure 4.10: The geometry of Example 4.8.

For the inverse map, express an element of $T_6(\mathbb{F}_q) - \{1, \xi(a)\}$ in the form $\beta = \beta_1 + \beta_2 x$ and write $(1 + \beta_1)/\beta_2 = Ru_1 + (y + y^2)u_2 + (y^2 - y)u_3$. Then

$$\begin{array}{c} \rho : T_6(\mathbb{F}_q) - \{1, \xi(a_3)\} \xrightarrow{\sim} \mathbb{A}^2(\mathbb{F}_q) - V(f) \\ \rho(\beta) = (\frac{u_1}{u_3 - \sqrt{-S/(3R)}}, \frac{u_2}{u_3 - \sqrt{-S/(3R)}}), \end{array}$$

and we have another effectively computable rational parameterization of the torus T_6, albeit over a significantly smaller family of fields $\mathbb{F}_q$.

4.4 Summary

In this chapter, we connected compact representations of norm-1 tori to an existing conjecture from the literature of algebraic geometry. We explored some of the ramifications of Conjecture 4.2 on the existence of rational norm-1 tori, and considered the state of knowledge surrounding it. Informed by the result that the torus T_6 is rational, we presented Rubin and Silverberg's general procedure for constructing birational isomorphisms

$$T_6(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^2,$$

and gave details of the procedure in two cases.

Moreover, we explained that the cryptosystem CEILIDH does not achieve a better compression ratio than the XTR cryptosystem achieves, and that the rationality of the variety $\mathcal{T}_{\mathbb{F}_{q^{30}}}$ is the problem preventing the CEILIDH system from improving. In the next chapter, we present a generalized notion of rational varieties and explain how this generalization can be used to implement a cryptosystem that does improve upon the XTR compression ratio.

Chapter 5

Stably rational tori

In this chapter, we present a generalization of the notion of rational variety, and show that this generalization can be used to achieve compression ratios better than the 1/3 achieved by the XTR and CEILIDH cryptosystems. We present work published in two research papers. The first paper, due to van Dijk and Woodruff, suggested generalizing rationality to stable rationality, and presented an inefficient scheme that exploited that generalization [vDW04]. The second paper, due to seven authors including van Dijk and Woodruff, extended the previous scheme and streamlined the implementation, making it computationally feasible [vDGP$^+$05]. Indeed, they implemented the scheme and showed that it performed similarly to existing schemes. Unfortunately, neither scheme achieves a savings when compressing a single torus element; they only achieve a savings when multiple torus elements are compressed. We will explain why this is the case in Section 5.1, before we consider the details of the construction.

First, let us outline the strategy of the schemes. To achieve an asymptotically higher compression ratio, van Dijk and Woodruff extend the rational maps technique of Rubin and Silverberg to higher dimensional tori, including the next largest cryptographically interesting tori T_{30} and T_{210}. Since it is not known if the torus T_{30} is rational, an explicit parameterization is not their goal; instead, van Dijk and Woodruff generalize the notion of rational variety, and show that their generalization yields a decomposition of tori that parameterizes $T_{30}(\mathbb{F}_q)$ as a factor of a larger product. They then show that such a decomposition yields a high compression ratio when many torus elements are compressed.

The precise property van Dijk and Woodruff use is stable rationality.

Definition 5.1. *Let V be an affine variety. If there exist non-negative integers D and E such there is a birational isomorphism between $V \times \mathbb{A}^D$ and $\mathbb{A}^E$, we say that the variety V is stably rational.*

Observe that a rational variety is trivially stably rational, with $D = 0$ and E the dimension of V.

The crucial point is that the norm-1 torus $\mathcal{T}_{\mathbb{F}_{q^n}}$ may be stably rational even though we do not know that it is rational. This means that it may be possible to find explicit birational maps

$$T_n(\mathbb{F}_q) \times \mathbb{F}_q^f \xrightarrow{\sim} \mathbb{F}_q^g, \tag{5.1}$$

for appropriate integers f and g, even when n is not the product of two prime powers. It is this stably rational property that van Dijk and Woodruff exploit to achieve compressed representations of $T_{30}(\mathbb{F}_q)$ and $T_{210}(\mathbb{F}_q)$.

Remark 5.2. In fact, an identity of the form (5.1) always exists: Voskresenskii [Vos98, Section 5.1] has shown that for every field L with cyclic Galois group, the norm-1 torus $\mathcal{T}_L$ is stably rational.

This chapter develops the chronologically later results of van Dijk et al. [vDGP$^+$05], but follows the presentation and proofs of the earlier exposition of van Dijk and Woodruff [vDW04].

The original result of van Dijk and Woodruff is an efficiently computable bijection

$$\theta_1 : T_n(\mathbb{F}_q) \times \prod_{d|n,\mu(\frac{n}{d})=-1} \mathbb{F}_{q^d}^\times \xrightarrow{\sim} \prod_{d|n,\mu(\frac{n}{d})=1} \mathbb{F}_{q^d}^\times, \tag{5.2}$$

where μ denotes the Möbius inversion function [LN94, Definition 3.22].

However, this decomposition is not an isomorphism of mathematical structures; instead, it is only a computable bijection between simple structures. In fact, the results of van Dijk and Woodruff follow from group order considerations alone. In contrast to the CEILIDH parameterizations, which were entirely geometric, there is no strong geometric intuition underlying the construction.

Before we construct the bijection θ_1, let us show that such a map is valuable to cryptographers.

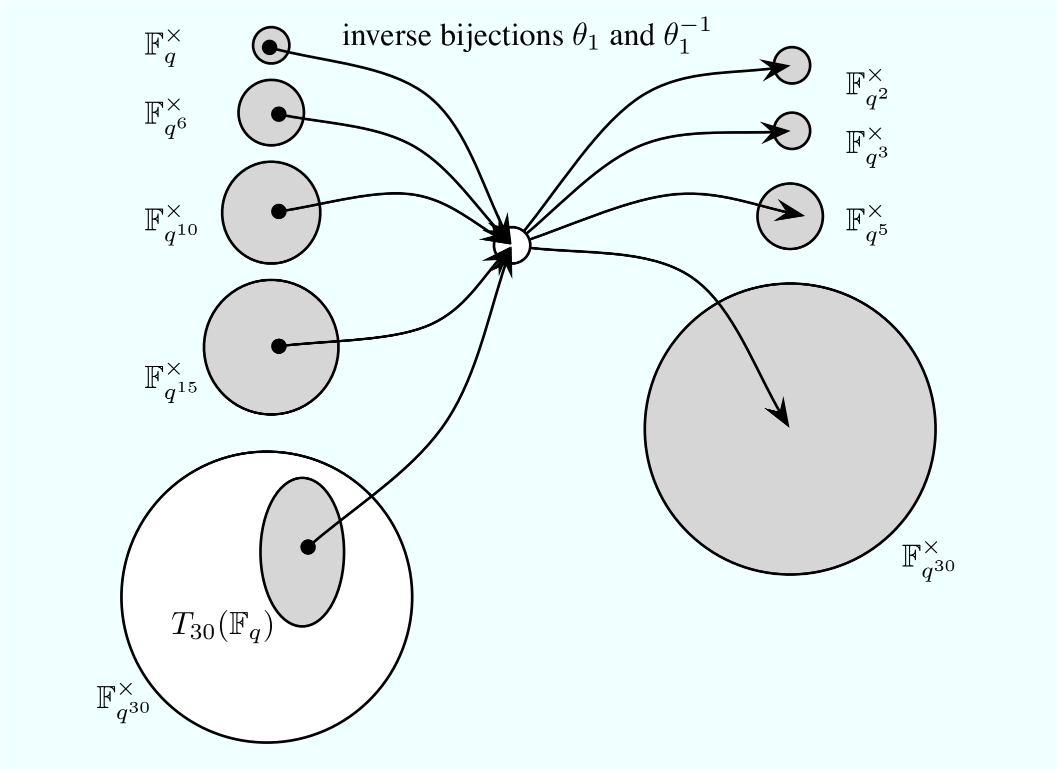

$\mathbb{F}_q^\times$
inverse bijections θ_1 and θ_1^{-1}
$\mathbb{F}_{q^6}^\times$
$\mathbb{F}_{q^{10}}^\times$
$\mathbb{F}_{q^{15}}^\times$
$T_{30}(\mathbb{F}_q)$
$\mathbb{F}_{q^{30}}^\times$
$\mathbb{F}_{q^2}^\times$
$\mathbb{F}_{q^3}^\times$
$\mathbb{F}_{q^5}^\times$
$\mathbb{F}_{q^{30}}^\times$

Figure 5.1: The case $n = 30$ of the bijection θ_1 of van Dijk and Woodruff.

5.1 Asymptotically optimal compression

In this section, suppose that we have a bijection of the form (5.2), so

$$\theta_1 : T_n(\mathbb{F}_q) \times \prod_{d|n,\mu(\frac{n}{d})=-1} \mathbb{F}_{q^d}^\times \xrightarrow{\sim} \prod_{d|n,\mu(\frac{n}{d})=1} \mathbb{F}_{q^d}^\times,$$

and its inverse

$$\theta_1^{-1} : \prod_{d|n,\mu(\frac{n}{d})=1} \mathbb{F}_{q^d}^\times \xrightarrow{\sim} T_n(\mathbb{F}_q) \times \prod_{d|n,\mu(\frac{n}{d})=-1} \mathbb{F}_{q^d}^\times,$$

can be efficiently computed.

Our goal is to compress a sequence of M torus elements

$$\{a_i\}_{i=1}^M \subset T_n(\mathbb{F}_q)^*.$$

Let

$$\mathbb{F}_q^{\sigma^-(n)} = \prod_{d|n, \mu(\frac{n}{d})=-1} \mathbb{F}_{q^d}^\times,$$

and let

$$\mathbb{F}_q^{\sigma^+(n)} = \prod_{d|n, \mu(\frac{n}{d})=1} \mathbb{F}_{q^d}^\times.$$

The crucial observation is that the order of $\mathbb{F}_q^{\sigma^+(n)}$ is greater than the order of $\mathbb{F}_q^{\sigma^-(n)}$. One way to see this is to observe that

$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(\frac{n}{d})},$$

and then consider the polynomial degrees on each side. Then we see that [LN94, Theorem 3.23]

$$\varphi(n) = \sum_{d|n} \mu(\frac{n}{d})d.$$

Thus, we have a bijection

$$\mathbb{F}_q^{\sigma^+(n)} \cong \mathbb{F}_q^{\sigma^-(n)} \times \mathbb{F}_q^{\varphi(n)},$$

and therefore we may consider the equivalent map

$$\theta_1 : T_n(\mathbb{F}_q) \times \mathbb{F}_q^{\sigma^-(n)} \xrightarrow{\sim} \mathbb{F}_q^{\varphi(n)} \times \mathbb{F}_q^{\sigma^-(n)}.$$

Using this map θ_1, we can compress the sequence of torus elements $\{a_i\}_{i=1}^M$ with the following procedure.

First, compute

$$(c_1, z_1) = \theta_1(a_1, z_0) \in \mathbb{F}_q^{\varphi(n)} \times \mathbb{F}_q^{\sigma^-(n)},$$

where $z_0 = (1, 1, \dots, 1) \in \mathbb{F}_q^{\sigma^-(n)}$. Now, compute

$$(c_2, z_2) = \theta_1(a_2, z_1),$$

and in general

$$(c_{i+1}, z_{i+1}) = \theta_1(a_{i+1}, z_i).$$

In this way, the sequence $\{a_i\}_{i=1}^M$ is mapped to the pair

$$\left(\{c_i\}_{i=1}^M, z_M\right).$$

Of course, given the pair $\left(\{c_i\}_{i=1}^M, z_M\right)$, we must be able to recover the sequence $\{a_i\}_{i=1}^M$. This is done by computing

$$\theta_1^{-1}(c_M, z_M) = (a_M, z_{M-1}),$$

followed by

$$\theta_1^{-1}(c_{M-1}, z_{M-1}) = (a_{M-1}, z_{M-2}),$$

and in general

$$\theta_1^{-1}(c_{i-1}, z_{i-1}) = (a_{i-1}, z_{i-2}).$$

Thus the encoding $\{a_i\}_{i=1}^M \longrightarrow \left(\{c_i\}_{i=1}^M, z_M\right)$ is invertible.

Now, we need to establish the claim that the sequence $\{c_i\}_{i=1}^M$ in fact requires fewer bits than the sequence $\{a_i\}_{i=1}^M$. By assumption, each element $a_i \in \mathbb{F}_{q^n}^\times$ requires $n \log q$ bits of storage, and each element $c_i \in \mathbb{F}_q^{\varphi(n)}$ requires $\varphi(n) \log q$ bits of storage. It follows that the sequence $\{a_i\}_{i=1}^M$ requires

$$Mn \log q$$

bits of storage, and also that the pair $\left(\{c_i\}_{i=1}^M, z_M\right)$ requires

$$M\varphi(n) \log q + |\mathbb{F}_q^{\sigma^-(n)}| \log q$$

bits of storage. Thus, as the number M of torus elements compressed tends to infinity, the compression ratio approaches

$$\frac{\varphi(n)}{n}.$$

This is asymptotically optimal compression, since the norm-1 torus T_n is of dimension $\varphi(n)$, and hence $T_n(\mathbb{F}_q)$ requires at least $\varphi(n) \log q$ bits to represent.

We now turn to realizing efficiently computable maps θ_1.

5.2 Preliminaries

In fact, [vDW04] generalizes the effectively computable bijection θ_1 somewhat. Recall that we defined

$$T_n(\mathbb{F}_q) = \left\{ x \in \mathbb{F}_{q^n}^\times : N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(x) = 1 \, \text{for each subfield} \, \mathbb{F}_{q^d} \subsetneq \mathbb{F}_{q^n} \right\},$$

and that these points are precisely the $\mathbb{F}_q$-rational points of $\mathcal{T}_{\mathbb{F}_{q^n}}$ (see Section 2.3.2). In this section, we will need to work with the $\mathbb{F}_{q^d}$-rational points of $\mathcal{T}_{\mathbb{F}_{q^n}}$, so we recall that for $\mathbb{F}_q \subseteq \mathbb{F}_{q^\ell} \subseteq \bar{\mathbb{F}}_q$, we defined

$$T_n(\mathbb{F}_{q^\ell}) = \left\{ x \in \mathbb{F}_{q^{\ell n}} : N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(x) = 1 \, \text{for each subfield} \, \mathbb{F}_{q^d} \subsetneq \mathbb{F}_{q^n} \right\}.$$

This captures the dependence of what we call the norm-1 torus on the field of definition.

Fix a divisor m of n. Our goal is to present efficiently computable bijections θ_m and θ_m^{-1}, where

$$\theta_m \quad : \quad T_n(\mathbb{F}_q) \times \prod_{d | \frac{n}{m}, \mu(\frac{n}{md}) = -1} T_m(\mathbb{F}_{q^d}) \xrightarrow{\sim} \prod_{d | \frac{n}{m}, \mu(\frac{n}{md}) = 1} T_m(\mathbb{F}_{q^d}). \tag{5.3}$$

Observe that the original result (5.2) of van Dijk and Woodruff is the case of (5.3) with $m = 1$, since $T_1(\mathbb{F}_{q^d}) = \mathbb{F}_{q^d}^\times$.

We stress that the maps θ_m are bijections only. They are not group isomorphisms that preserve multiplicative structure, and they are not geometric isomorphisms defined for all points over the algebraic closure of our base field. In fact, in this chapter we are only interested in computational results, so we restrict ourselves to a finite field $\mathbb{F}_q$ throughout. In addition, the symbol '$\cong$' is to be read as "group isomorphism" for the remainder of this chapter (before, we used '$\cong$' to denote an isomorphism of varieties). Finally, recall that we denote the cyclic group of order N by C_N.

We need an effective version of the Fundamental Theorem of Abelian Groups [J99, Theorem 2.4.12].

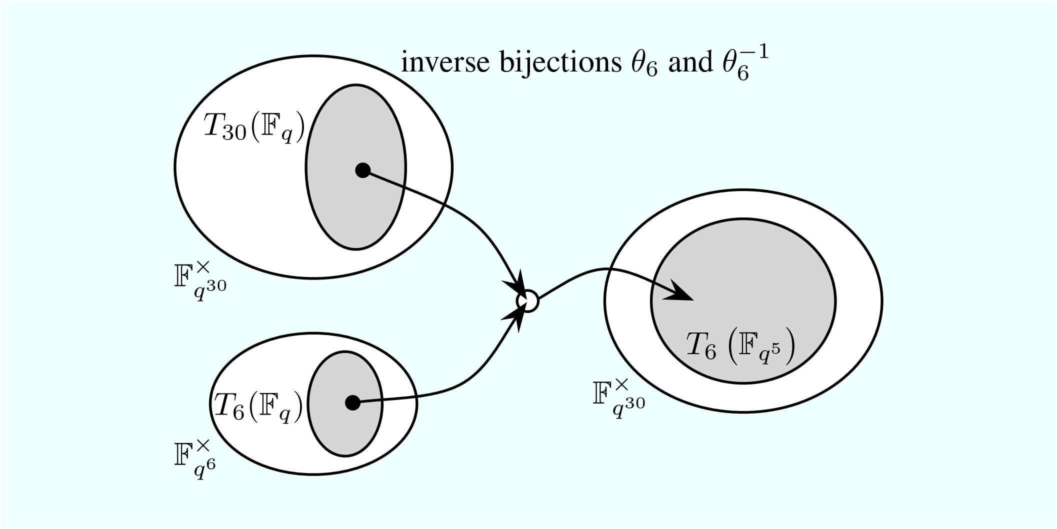

inverse bijections θ_6 and θ_6^{-1}
$T_{30}(\mathbb{F}_q)$
$\mathbb{F}_{q^{30}}^\times$
$T_6(\mathbb{F}_q)$
$\mathbb{F}_{q^6}^\times$
$T_6(\mathbb{F}_{q^5})$
$\mathbb{F}_{q^{30}}^\times$

Figure 5.2: The case $n = 30$, $m = 6$ of the bijection (5.3), $\theta_6 : T_{30}(\mathbb{F}_q) \times T_6(\mathbb{F}_q) \xrightarrow{\sim} T_6(\mathbb{F}_{q^5})$.

Proposition 5.3. *Suppose $n = r_1 r_2 \cdots r_k$, with the r_i pairwise relatively prime positive integers. Then there exist efficiently computable isomorphisms*

$$C_n \xrightarrow{\sim} \prod_i C_{r_i}$$

$$\prod_i C_{r_i} \xrightarrow{\sim} C_n.$$

Proof. For a proof emphasizing the computational complexity of the bijections, see [vDW04, Lemma 1]. □

5.3 Motivating identities

In this section, we concentrate on one factor $T_m(\mathbb{F}_{q^d})$ in the domain of θ_m. Following van Dijk and Woodruff, we will demonstrate a bijection between the factor $T_m(\mathbb{F}_{q^d})$ and a product of tori.

Let us consider some suggestive isomorphisms. We need the following standard result on cyclotomic polynomials [LN94, Theorem 2.45].

Proposition 5.4. *If p is a prime, and a is a positive integer not divisible by p, then*

$$\Phi_{ap}(x)\Phi_a(x) = \Phi_a(x^p).$$

This identity suggests the following result.

Theorem 5.5. *[vDGP+05, Theorem 2] If p is a prime, q is a prime power, a is a positive integer, a is not divisible by p, and* $\gcd(\Phi_{ap}(q), \Phi_a(q)) = 1$, *then*

$$T_{ap}(\mathbb{F}_q) \times T_a(\mathbb{F}_q) \cong T_a(\mathbb{F}_{q^p}).$$

(Recall that '$\cong$' denotes "group isomorphism".)

Proof. Recall that $T_n(\mathbb{F}_q)$ is isomorphic to a subgroup of $\mathbb{F}_{q^n}^*$ of order $\Phi_n(q)$. Since $\mathbb{F}_{q^n}^*$ is cyclic for every n, each of the factors on the left is cyclic. Since the factors on the left have relatively prime orders, the left hand side is isomorphic to a cyclic group of order $\Phi_{ap}(q) \cdot \Phi_a(q)$, by Proposition 5.3. The right hand side is isomorphic to a subgroup of $\mathbb{F}_{q^{ap}}^*$, and hence is cyclic of order $\Phi_a(x^p)$. By Proposition 5.4, the left factors and the right side have the same order, and thus Proposition 5.3 yields an isomorphism. □

Proposition 5.4 extends naturally.

Theorem 5.6. *If m and d are integers with* $\gcd(m, d) = 1$, *then*

$$\Phi_m(x^d) = \prod_{e|d} \Phi_{me}(x).$$

Proof. We prove the result by induction on the number of prime divisors of d. If $d = p$ is itself prime, then the result is just Proposition 5.4. Now suppose the result is true for any m, and for all d with at most r prime divisors. Consider a prime p that does not divide m. Then

$$\begin{aligned}
\Phi_m(x^{dp}) &= \Phi_m(x^d)\Phi_{mp}(x^d) \\
&= \prod_{e|d} \Phi_{me}(x) \cdot \prod_{e|d} \Phi_{mpe}(x) \\
&= \prod_{e|dp} \Phi_{me}(x).
\end{aligned}$$

□

We would like to extend Theorem 5.5 to prove $T_m(\mathbb{F}_{q^d}) \cong \prod_{e|d} T_{me}(\mathbb{F}_q)$, but we can not do so: in general these objects are not isomorphic. The immediate obstacle is that we cannot guarantee $\gcd(\Phi_{me}(q), \Phi_{mf}(q)) = 1$ for each pair of divisors $e|d, f|d$, with $e \neq f$. The presence of repeated divisors in the orders of the groups $T_{me}(\mathbb{F}_q)$ prevents the natural isomorphism. Therefore, our first task is to explain how to isolate the repeated divisors.

5.4 Isolating the repeated divisors

The technical tools to handle the repeated divisors in the product $\prod_{e|d} \Phi_{me}(x)$ are provided by van Dijk and Woodruff [vDW04, Section 3].

First, let us clarify the meaning of repeated divisors.

Definition 5.7. *For each $d|\frac{n}{m}$, let W_d be the smallest positive integer such that*

$$\gcd(\Phi_{me}(q), \Phi_{mf}(q), \Phi_m(q^d)/W_d) = 1$$

for every pair of divisors $e|d, f|d$, with $d \neq e$.

W_d is the repeated divisor preventing natural isomorphisms. Therefore, the offending subsets of $T_{me}(\mathbb{F}_q)$ must be isolated and handled separately.

Lemma 5.8. *Let $d|\frac{n}{m}$, and let W_d be defined as above. Then*

$$\gcd(W_d, \Phi_m(q^d)/W_d) = 1.$$

Proof. We follow the proof of [vDW04, Lemma 2]. Suppose a prime p divides W_d. By the definition of W_d, there must be $e|d, f|d$, with $e \neq f$, such that $p|\gcd(\Phi_{me}(q), \Phi_{mf}(q))$. Now, if $p|\Phi_m(q^d)/W_d$ we would have $p|\gcd(\Phi_{me}(q), \Phi_{mf}(q), \Phi_m(q^d)/W_d) = 1$, a contradiction. Therefore $\gcd(W_d, \Phi_m(q^d)/W_d) = 1$. $\square$

This result allows van Dijk and Woodruff to split each torus $T_m(\mathbb{F}_{q^d})$ into two pieces, one of size $\Phi_m(q^d)/W_d$, and the other of size W_d. The first piece can be handled with the help of Theorem 5.3. We hope that W_d, the size of the piece that cannot be easily handled, is "small" for each d, so that the forthcoming Lemma 5.10 result takes care of most of $T_m(\mathbb{F}_{q^d})$.

First, some notation.

Definition 5.9. *Fix an integer $d|\frac{n}{m}$, and let W_d be defined as above. For each divisor $e|d$, let*

$$y_e = \gcd(\Phi_{me}(q), \Phi_m(q^d)/W_d).$$

The values y_e are the sizes of the groups in the domain of θ_m after we have removed the repeated divisors.

Lemma 5.10. *For $d|\frac{n}{m}$, let W_d be defined as above, and for $e|d$, let y_e be defined as above. Then*

$$T_m(\mathbb{F}_{q^d}) \cong C_{W_d} \times (\prod_{e|d} C_{y_e}).$$

Proof. We follow the proof of [vDW04, Lemma 2]. We must show three things: first, that the group orders on the left and on the right are the same; second, that $\gcd(W_d, y_e) = 1$ for each $e|d$, and third, that $\gcd(y_e, y_f) = 1$ for each $e|d, f|d$, with $e \neq f$.

First, we have that $\prod_{e|d} y_e = \prod_{e|d} \gcd(\Phi_{me}(q), \Phi_m(q^d)/W_d)$. Now, suppose a prime $p|\gcd(\Phi_{me}(q), \Phi_m(q^d)/W_d)$ for some $e|d$. Then p does not divide $\Phi_{mf}(q)$ for $f|d$ with $e \neq f$, since otherwise we would have $p|\gcd(\Phi_{me}(q), \Phi_{mf}(q), \Phi_m(q^d)/W_d) = 1$, a contradiction. This means that we can pull out divisors in the product to write

$$\begin{aligned}
\prod_{e|d} y_e &= \prod_{e|d} \gcd(\Phi_{me}(q), \Phi_m(q^d)/W_d) \\
&= \gcd(\prod_{e|d} \Phi_{me}(q), \Phi_m(q^d)/W_d) \\
&= \gcd(\Phi_m(q^d), \Phi_m(q^d)/W_d) \\
&= \Phi_m(q^d)/W_d.
\end{aligned}$$

Second, we have that

$$\gcd(W_d, y_e) = \gcd(W_d, \gcd(\Phi_{me}(q), \Phi_m(q^d)/W_d)) = \gcd(W_d, \Phi_{me}(q), \Phi_m(q^d)/W_d),$$

and the final term certainly divides $\gcd(W_d, \Phi_m(q^d)/W_d) = 1$, so $\gcd(W_d, y_e) = 1$.

Finally, for $e \neq f$,

$$\begin{aligned}
\gcd(y_e, y_f) &= \gcd(\gcd(\Phi_{me}(q), \Phi_m(q^d)/W_d), \gcd(\Phi_{mf}(q), \Phi_m(q^d)/W_d)) \\
&= \gcd(\Phi_{me}(q), \Phi_{mf}(q), \Phi_m(q^d)/W_d),
\end{aligned}$$

which is 1 by the definition of W_d. Thus, Proposition 5.3 applies and

$$T_m(\mathbb{F}_{q^d}) \cong C_{W_d} \times (\prod_{e|d} C_{y_e}).$$

□

5.5 Bijections for the repeated factors

We would like to decompose the factor C_{W_d} further. Unfortunately, we do not have an interpretation of C_{W_d} in terms of algebraic tori, or even an interpretation as a product of cyclic groups: C_{W_d} may not be isomorphic to a conceptually simple structure. The best we can do is present an effectively computable bijection between sets of equal sizes. The following bijection of van Dijk and Woodruff does this by providing a table lookup, that is efficient provided W_d is small.

Definition 5.11. *Fix a divisor $d|\frac{n}{m}$, and let W_d be defined as above. For each divisor $e|d$, let*

$$z_e = \gcd(\Phi_{me}(q), W_d).$$

The values z_e are the sizes of the repeated divisors in the orders of the groups in the domain of θ_m.

Lemma 5.12. *[vDW04, Lemma 3] There exist bijections between C_{W_d} and $\prod_{e|d} C_{z_e}$, requiring $O(\log W_d + \log n + \log\log q)$ time to evaluate, and $O(W_d n^{1+\varepsilon} \log q)$ storage, for any constant $\varepsilon > 0$.*

Proof. Observe that if a prime p divides $\gcd(\Phi_{me}(q), \Phi_{mf}(q))$, then $p \nmid \Phi_m(q^d)/W_d$: if $p|\Phi_m(q^d)/W_d$, then $p|\gcd(\Phi_{me}(q), \Phi_{mf}(q), \Phi_m(q^d)/W_d) = 1$, which is a contradiction. This means that if $p^k \| \Phi_m(q^d)$, then $p^k \| W_d$, and thus we can write

$$\prod_{e|d} \gcd(\Phi_{me}(q), W_d) = \gcd(\prod_{e|d} \Phi_{me}(q), W_d).$$

Hence

$$\prod_{e|d} |C_{z_e}| = \prod_{e|d} \gcd(\Phi_{me}(q), W_d) = \gcd(\prod_{e|d} \Phi_{me}(q), W_d) = \gcd(\Phi_m(q^d), W_d) = W_d.$$

This means there exists a bijection between the two groups, viewed as sets (recall that we do not preserve group structure).

Now choose a generator g of C_{W_d}, and generators C_e of C_{z_e}. Make a table that maps g^i to a unique tuple $(C_e^{i_e})_{e|d}$ for each index $0 \leqslant i \leqslant W_d$. If we implement the table so that lookups are efficient in both directions, then we can evaluate either bijection using standard algorithms in time $O(\log W_d + \log n + \log\log q)$ (for example, as an indexed hash table). Additionally, since the sum of divisors of n is bounded by $O(n^{1+\varepsilon})$ for any constant $\varepsilon > 0$, the table requires space bounded by $O(W_d n^{1+\varepsilon} \log q)$. □

In practice we can choose W_d to be insignificant in comparison to the other parameters of the cryptographic scheme, so that the computation and storage required to evaluate the bijection above is not a performance bottleneck. However, the best proved result is due to van Dijk and Woodruff: they show that for certain fields, W_d grows sub-linearly with the degree n of the torus T_n [vDW04, Section 4.3].

Remark 5.13. In the following theorems, we assume that W_d is "small" for each $d|\frac{n}{m}$, so that the maps of Lemma 5.12 are efficiently computable.

Corollary 5.14. *Fix a divisor $d|\frac{n}{m}$. Assuming that the table-based maps of Lemma 5.12 are efficiently computable, Lemma 5.10 and Lemma 5.12 show that we have efficiently computable bijections*

$$T_m(\mathbb{F}_{q^d}) \xrightarrow{\sim} (\prod_{e|d} C_{y_e}) \times (\prod_{e|d} C_{z_e}).$$

Now that we have shown how van Dijk and Woodruff decompose the torus $T_m(\mathbb{F}_{q^d})$ into a product of cyclic groups, we need to show how to glue those groups back together into a product of tori.

Lemma 5.15. *[vDW04, Lemma 4] Fix a divisor $d|\frac{n}{m}$, and let y_e and z_e be as defined above. Then, assuming that the maps of Lemma 5.12 are efficiently computable, there are efficiently computable bijections*

$$(\prod_{e|d} C_{y_e}) \times (\prod_{e|d} C_{z_e}) \xrightarrow{\sim} \prod_{e|d} T_{me}(\mathbb{F}_q).$$

Proof. It suffices to show that for each $e|d$, we have $C_{y_e} \times C_{z_e} \cong T_{me}(\mathbb{F}_q)$. First, the group orders match:

$$y_e z_e = \gcd(\Phi_{me}(q), \Phi_m(q^d)/W_d) \cdot \gcd(\Phi_{me}(q), W_d) = \Phi_{me}(q),$$

since $\gcd(\Phi_m(q^d)/W_d, W_d) = 1$, by Proposition 5.8. Second, we have

$$\begin{aligned} \gcd(y_e, z_e) &= \gcd(\gcd(\Phi_{me}(q), \Phi_m(q^d)/W_d), \gcd(\Phi_{me}(q), W_d)) \\ &= \gcd(\Phi_{me}(q), \Phi_m(q^d)/W_d, \Phi_{me}(q), W_d), \end{aligned}$$

which certainly divides $\gcd(\Phi_m(q^d)/W_d, W_d) = 1$. Now, since the left product $C_{y_e} \times C_{z_e}$ and the right torus $T_{me}(\mathbb{F}_q)$ are isomorphic to cyclic groups of the same order, Proposition 5.3 gives an efficient isomorphism between them. □

The following bijection, implicit in the statement of [vDGP$^+$05, Theorem 4], completes our presentation of van Dijk and Woodruff's treatment of the extra factors in the bijections θ_m.

Corollary 5.16. *Assuming the table-based maps of Lemma 5.12 are efficient, there exist efficiently computable bijections*

$$T_m(\mathbb{F}_{q^d}) \xrightarrow{\sim} \prod_{e|d} T_{me}(\mathbb{F}_q)$$

and

$$\prod_{e|d} T_{me}(\mathbb{F}_q) \xrightarrow{\sim} T_m(\mathbb{F}_{q^d}).$$

5.6 Bijections for high dimensional tori

Finally, we are ready to show how van Dijk and Woodruff exploit the preceding lemmas to demonstrate the complete bijection θ_m. First, we prove the result relating group orders.

Theorem 5.17. *[vDGP$^+$05, Theorem 3] If n is square-free and m is a divisor of n, then*

$$\Phi_n(x) \prod_{d|\frac{n}{m},\ \mu(\frac{n}{md})=-1} \Phi_m(x^d) = \prod_{d|\frac{n}{m},\ \mu(\frac{n}{md})=1} \Phi_m(x^d).$$

Proof. For each square free integer n, we prove the equivalent statement

$$\Phi_n(x) = \prod_{d|\frac{n}{m}} \Phi_m(x^d)^{\mu(\frac{n}{md})},$$

by induction on the number of prime divisors of m.

First, suppose that $n = p_1 \cdots p_r$ has r prime divisors with each p_i distinct. If $m = n$, then $\prod_{d|\frac{n}{m}} \Phi_m(x^d)^{\mu(\frac{n}{md})} = \Phi_m(x)^{\mu(\frac{n}{m})} = \Phi_n(x)$ as desired.

Let the induction hypothesis be that the statement is true for m dividing n with m having at least $2 \leq k \leq r$ prime divisors and consider, for an appropriate prime p dividing m, the statement for $\frac{m}{p}$, which has strictly fewer prime divisors than m. Then

$$\begin{aligned}
\prod_{d \ \mid \ n/\frac{m}{p}} \Phi_{\frac{m}{p}}(x^d)^{\mu(\frac{n/\frac{m}{p}}{d})} &= \prod_{d|\frac{n}{m}} \Phi_{\frac{m}{p}}(x^d)^{\mu(\frac{np}{md})} \cdot \prod_{d|\frac{n}{m}} \Phi_{\frac{m}{p}}(x^{dp})^{\mu(\frac{np}{m(dp)})} \\
&= \prod_{d|\frac{n}{m}} \Phi_{\frac{m}{p}}(x^d)^{\mu(\frac{np}{md})} \cdot \prod_{d|\frac{n}{m}} \Phi_{\frac{m}{p}}(x^d)^{\mu(\frac{np}{m(dp)})} \Phi_m(x^d)^{\mu(\frac{np}{m(dp)})} \\
&= \prod_{d|\frac{n}{m}} \Phi_{\frac{m}{p}}(x^d)^{-\mu(\frac{n}{md})} \cdot \prod_{d|\frac{n}{m}} \Phi_{\frac{m}{p}}(x^d)^{\mu(\frac{n}{md})} \cdot \prod_{d|\frac{n}{m}} \Phi_m(x^d)^{\mu(\frac{n}{md})} \\
&= \Phi_n(x),
\end{aligned}$$

by an application of Proposition 5.4 (which applies, since $m|n$ is square-free) and the induction hypothesis. □

Theorem 5.18. *[vDGP$^+$05, Theorem 4] Let m be a divisor of n. Assuming the table-based maps of Lemma 5.12 are efficient, there exist efficiently computable bijections θ_m and θ_m^{-1}, where*

$$\theta_m \quad : \quad T_n(\mathbb{F}_q) \times \prod_{d|\frac{n}{m}, \mu(\frac{n}{md})=-1} T_m(\mathbb{F}_{q^d}) \xrightarrow{\sim} \prod_{d|\frac{n}{m}, \mu(\frac{n}{md})=1} T_m(\mathbb{F}_{q^d}).$$

Proof. We follow the proof of [vDW04, Theorem 3]. By Corollary 5.16, we have

$$T_m(\mathbb{F}_{q^d}) \xrightarrow{\sim} \prod_{e|d} T_{me}(\mathbb{F}_q),$$

so we can view the bijection as a map between products of tori. The theorem will follow if we show that the tori on the left are the same as the tori on the right, and this is equivalent to showing that the following multiset equality holds:

$$\{n\} \cup \bigcup_{d|\frac{n}{m}, \mu(\frac{n}{md})=-1} \{me : e|d\} = \bigcup_{d|\frac{n}{m}, \mu(\frac{n}{md})=1} \{me : e|d\}.$$

Now by Theorem 5.17, $\Phi_n(x) \prod_{d|\frac{n}{m}, \mu(\frac{n}{md})=-1} \Phi_m(x^d) = \prod_{d|\frac{n}{m}, \mu(\frac{n}{md})=1} \Phi_m(x^d)$. Applying Theorem 5.6 to factor each side into irreducible polynomials, we see

$$\Phi_n(x) \prod_{d|\frac{n}{m}, \mu(\frac{n}{md})=-1} \prod_{e|d} \Phi_{me}(x) = \prod_{d|\frac{n}{m}, \mu(\frac{n}{md})=1} \prod_{e|d} \Phi_{me}(x).$$

This identity holds in the polynomial ring $\mathbb{Q}[x]$, which is a unique factorization domain; thus, the polynomials on the left must be the same as the polynomials on the right. Since the cyclotomic polynomials are irreducible over $\mathbb{Q}$ [LN94, Theorem 2.45], this factorization establishes the desired multiset equality, and the theorem follows. □

5.7 Bounding the repeated divisors

In the preceding sections, we showed how van Dijk and Woodruff isolate and handle the repeated divisors preventing natural isomorphisms between $T_m(\mathbb{F}_{q^d})$ and $\prod_{e|d} T_{me}(\mathbb{F}_{q^d})$, but we have not yet considered the computational impact of these divisors. The definition of W_d shows that we need not consider each divisor $d|\frac{n}{m}$ separately: it suffices to analyze only n, since $W_d | W_{\frac{n}{m}} | W_n$. Therefore, it suffices to consider only $m = 1$, or the original bijection (5.2) of van Dijk and Woodruff.

However, there is another issue: in the bijection θ_1, we need table storage for every divisor d of n. Since $d(n)$, the number of divisors of n, satisfies

$$d(n) > 2^{(1-\varepsilon)\frac{\log n}{\log \log n}}$$

infinitely often for every $\varepsilon > 0$ [HW79, Theorem 317], the number of tables could be more computationally significant than an upper bound for W_d. In practice, however, n is fixed (and, in fact, has few divisors), so the storage required to implement the bijection θ_1 is not significant.

The asymptotic growth of W_n has been analyzed by van Dijk and Woodruff [vDW04, Section 4.3], and they show that, under some conditions,

$$W_n = O\left(n^{0.75}\right).$$

Their analysis is restricted to fields $\mathbb{F}_q$ with field order q satisfying rather onerous congruence conditions, and is somewhat artificial because they consider W_n as a function of n, and bound W_n as n tends to infinity. This conflicts with common practice, which fixes n and lets the field order $\mathbb{F}_q$ tend to infinity. These limitations of the analysis are not an issue in practice, because we can efficiently choose parameters so that any repeated factors are negligible. In summary, van Dijk and Woodruff's sub-linear bound on the repeated factors W_n is a theoretical result supporting the validity of the method, but it does not address the instances used in practice.

Let us outline van Dijk and Woodruff's result. To make their strong statement about the growth of W_n, the authors need to make strong assumptions about the field order q, which plays a prominent role in Definition 5.7 specifying W_n. To make these assumptions, they give a probabilistic Las Vegas algorithm, algorithm PSA [vDW04, Section 4.3], that, if it terminates, finds a field $\mathbb{F}_q$ with field order q satisfying the congruences needed for the analysis. They then analyze algorithm PSA and show that, when the algorithm terminates,

$$W_n = O\left(n^{0.75}\right).$$

Finally, van Dijk and Woodruff show that algorithm PSA terminates with high probability. The analysis depends heavily on the asymptotic density of primes p such that $p - 1$ is square-free, which is far from our field.

Unfortunately, van Dijk and Woodruff state that the algorithm does not find the cryptographically best parameters for the $n = 30$ case until the field order q is of approximately 500 bits, and therefore the analysis is irrelevant in practice, since it is not applicable to fields of cryptographic size (which have $30q \approx 1024$ or $q \approx 35$). However, the theoretical result is important because it suggests that the technique is practicable in some cases.

5.8 Exploiting the bijections of CEILIDH

The original bijection θ_1 of van Dijk and Woodruff [vDW04] is as in Theorem 5.18 with divisor $m = 1$. However, observe that $T_1(\mathbb{F}_{q^d}) = \mathbb{F}_{q^d}^\times$ is rational; this motivates the following recursive procedure. If m is chosen so that T_m is rational, then each extra factor $T_m(\mathbb{F}_{q^d})$ in the range of θ_m can itself be compactly represented, yielding even greater savings. In practice, choosing m the product of two distinct primes is best, because these are tori T_m we know to be rational. We will only consider the case $m = 6$, for which we have the CEILIDH maps of Chapter 4.

When $m = 6$ and $n = 30$, van Dijk et al. point out that the situation is even more fortuitous. They show that $\gcd(\Phi_{30}(q), \Phi_5(q)) = 1$, independent of q (this follows from [vDW04, Lemma 6]). Thus Theorem 5.5 establishes the isomorphism

$$T_{30}(\mathbb{F}_q) \times T_6(\mathbb{F}_q) \cong T_6(\mathbb{F}_{q^5}),$$

and the maps of CEILIDH yield a birational parameterization

$$T_{30}(\mathbb{F}_q) \times \mathbb{A}^2(\mathbb{F}_q) \xrightarrow{\sim} \mathbb{A}^2(\mathbb{F}_{q^5}) \xrightarrow{\sim} \mathbb{A}^{10}(\mathbb{F}_q). \tag{5.4}$$

For $n = 210$, we have the slightly weaker effectively computable bijections

$$T_{210}(\mathbb{F}_q) \times T_6(\mathbb{F}_{q^5}) \times T_6(\mathbb{F}_{q^7}) \xrightarrow{\sim} T_6(\mathbb{F}_{q^{35}}),$$

yielding a birational parameterization

$$T_{210}(\mathbb{F}_q) \times \mathbb{A}^{24}(\mathbb{F}_q) \xrightarrow{\sim} \mathbb{A}^{72}(\mathbb{F}_q).$$

In general, if T_m is rational, let

$$D(m,n) = \varphi(m) \sum_{d \mid \frac{n}{m}, \mu(\frac{n}{md}) = -1} d;$$

then we have a parameterization

$$T_n \times \mathbb{A}^{D(m,n)} \xrightarrow{\sim} \mathbb{A}^{\varphi(n)+D(m,n)}.$$

In fact, van Dijk et al. even improve this result. First, we relate the group orders:

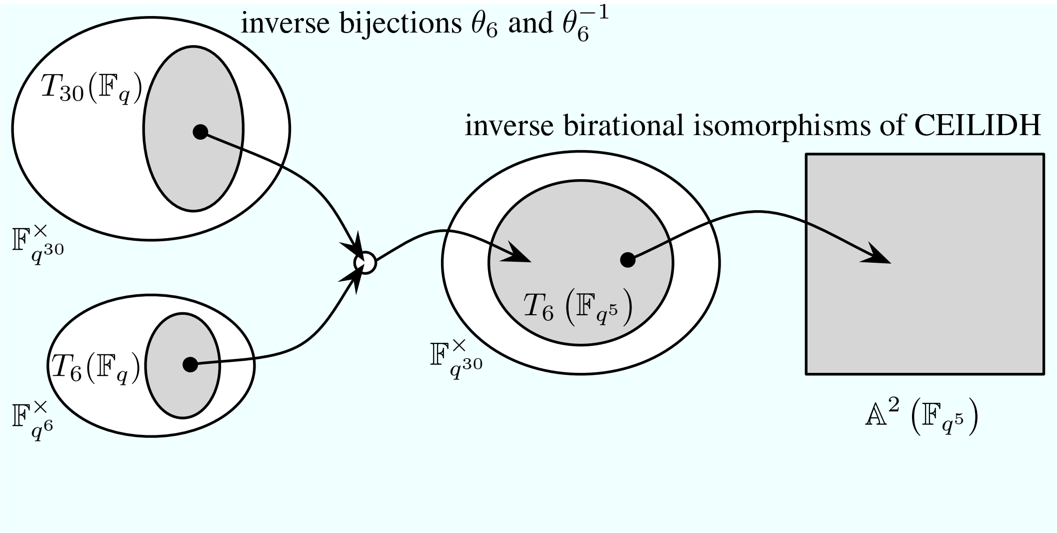

inverse bijections θ_6 and θ_6^{-1}
$T_{30}(\mathbb{F}_q)$
$\mathbb{F}_{q^{30}}^\times$
$T_6(\mathbb{F}_q)$
$\mathbb{F}_{q^6}^\times$
inverse birational isomorphisms of CEILIDH
$T_6\left(\mathbb{F}_{q^5}\right)$
$\mathbb{F}_{q^{30}}^\times$
$\mathbb{A}^2\left(\mathbb{F}_{q^5}\right)$

Figure 5.3: Exploiting the CEILIDH parameterizations for even greater compression.

Theorem 5.19. *[vDGP+05, Theorem 5] Let $n = p_1p_2\cdots p_k$ be the product of $k \geqslant 2$ distinct primes. Then*

$$\Phi_n(x)\prod_{i=2}^{k-1}\Phi_{p_1\cdots p_i}(x^{p_{i+2}\cdots p_k}) = \Phi_{p_1p_2}(x^{p_3\cdots p_k}),$$

where for index $i = k-1$ the empty product $x^{p_{k+1}\cdots p_k}$ is interpreted as x.

Proof. The proof is by induction on the number of prime divisors of n. The statement is vacuously true for $k = 2$. Suppose the statement is true for all n with at most $k \geqslant 2$ divisors $p_1, \ldots, p_k$, and consider a prime p_{k+1} distinct from each p_i. By Theorem 5.4, $\Phi_{np_{k+1}}(x)\Phi_n(x) = \Phi_n(x^{p_{k+1}})$, and multiplying each side of the identity by the product $\prod_{i=2}^{k-1}\Phi_{p_1\cdots p_i}((x^{p_{k+1}})^{p_{i+2}\cdots p_k})$, we have

$$\begin{aligned}\Phi_{np_{k+1}}(x)\Phi_n(x)\prod_{i=2}^{k-1}\Phi_{p_1\cdots p_i}((x^{p_{k+1}})^{p_{i+2}\cdots p_k}) &= \Phi_n(x^{p_{k+1}})\prod_{i=2}^{k-1}\Phi_{p_1\cdots p_i}((x^{p_{k+1}})^{p_{i+2}\cdots p_k})\\ \Phi_{np_{k+1}}(x)\prod_{i=2}^{k}\Phi_{p_1\cdots p_i}(x^{p_{i+2}\cdots p_kp_{k+1}}) &= \Phi_{p_1p_2}(x^{p_3\cdots p_kp_{k+1}}),\end{aligned}$$

which establishes the identity. □

The techniques detailed in the preceding sections extend to give bijections

$$T_n(\mathbb{F}_q) \times \prod_{i=2}^{k} T_{p_1 \cdots p_i}(\mathbb{F}_{q^{p_{i+2} \cdots p_k p_{k+1}}}) \xrightarrow{\sim} T_{p_1 p_2}(\mathbb{F}_{q^{p_3 \cdots p_k p_{k+1}}}).$$

In the case $n = 210$, we obtain

$$T_{210}(\mathbb{F}_q) \times T_{30}(\mathbb{F}_q) \times T_6(\mathbb{F}_{q^7}) \xrightarrow{\sim} T_6(\mathbb{F}_{q^{35}}).$$

However, using identity (5.4), we have

$$T_{30}(\mathbb{F}_q) \times \mathbb{A}^2(\mathbb{F}_q) \xrightarrow{\sim} \mathbb{A}^{10}(\mathbb{F}_q),$$

and so, since

$$T_6(\mathbb{F}_{q^7}) \xrightarrow{\sim} \mathbb{A}^{14}(\mathbb{F}_q) \cong \mathbb{A}^2(\mathbb{F}_q) \times \mathbb{A}^{12}(\mathbb{F}_q),$$

we obtain

$$T_{210}(\mathbb{F}_q) \times \mathbb{A}^{22}(\mathbb{F}_q) \xrightarrow{\sim} \mathbb{A}^{70}(\mathbb{F}_q).$$

Although the computation required can be significant [vDGP$^+$05, Section 6], the asymptotic compression obtained by this recursive chaining is attractive for applications with high bandwidth requirements.

For example, van Dijk et al. adapt an electronic voting scheme of Kiayias and Yung [KY02] to use an optimized parameterization of $T_{30}(\mathbb{F}_q)$. Compared to a voting scheme due to Damgärd and Jurik [DJ03], their torus based modification reduces the bandwidth required by a factor of roughly 6.5 [vDGP$^+$05, Appendix A]. This type of application, where many torus elements will be transmitted, is ideally suited to the compression maps given above.

5.9 Summary

We have done three things in this chapter. First, we presented a generalization of the notion of rational parameterization, and explained how this generalization is used to construct cryptosystems with compression better than the XTR and CEILIDH cryptosystems. Second, we presented some parameterizations of stably rational tori. Finally, we cited a theoretical result that suggests that the technique described can be practicable in more situations than the optimized implementation presented in [vDGP$^+$05]. This completes our coverage of extensions to the XTR and CEILIDH cryptosystems.

Chapter 6

Cryptography

In this chapter, we discuss the security of torus-based cryptosystems over finite fields. We present torus-based analogues of standard cryptographic protocols, due to Rubin and Silverberg [RS03], that motivate our security analysis. We consider the norm-1 torus $T_n(\mathbb{F}_q)$ as a subgroup of the multiplicative group $\mathbb{F}_{q^n}^\times$, and argue that torus-based cryptosystems are as secure as traditional cryptosystems based on discrete logarithms in $\mathbb{F}_{q^n}^\times$, for similar parameter choices. We present the two attacks currently believed to be most applicable to torus-based cryptosystems, before presenting an efficient probabilistic algorithm that selects finite fields such that the tori $T_6(\mathbb{F}_q)$ and $T_{30}(\mathbb{F}_q)$ are secure against these attacks. Finally, we present recent results of Granger and Vercauteren [GV05] on the security of discrete logarithms in algebraic tori, and show that these results impact the security of existing cryptosystems.

6.1 Torus-based cryptosystems

This section shows how Rubin and Silverberg [RS03, Section 6] use the maps developed in Chapter 4 to realize public-key cryptosystems that require less communication than traditional analogues.

6.1.1 The CEILIDH protocols

For concreteness, we will only consider cryptosystems based on the two dimensional torus T_6, but the ideas presented extend naturally to any torus that has been explicitly birationally parameterized.

There are several parts to a torus-based cryptosystem. First, system-wide parameters must be established; these include the choice of a torus T, of a base field k, and of birational isomorphisms between the torus and affine space. Second, each user must generate a public/private key pair, and publish the public information. Finally, the users of the system must standardize protocols and implementation details. Since the choices of finite fields and birational isomorphisms can be quite involved, we will abstract away some of these details to simplify the presentation of the communication protocols.

We always choose k to be a finite field of prime order q, and we always let T be T_6. Let ℓ be a prime divisor of $\Phi_6(q)$; we work in the subgroup of $T_6(\mathbb{F}_q) \subset \mathbb{F}_{q^6}^\times$ of order ℓ. Distinguish a generator α of this order ℓ subgroup to be the base element of the cryptosystem. Finally, fix a birational parameterization

$$\rho : T_6(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^2$$

and its inverse

$$\psi : \mathbb{F}_q^2 \longrightarrow T_6(\mathbb{F}_q).$$

(The maps ρ and ψ of Example 4.7 are suitable birational parameterizations.)

The system-wide parameters, made public to all users of the cryptosystem, are the torus $T_6(\mathbb{F}_q)$, the field $\mathbb{F}_q$, the generator α and its order ℓ, and the maps ρ and ψ. The compressed representation $\rho(\alpha)$ could be distributed instead of the generator α.

It is necessary to represent messages as elements of the torus T, and Rubin and Silverberg show how to do this [RS04b, Section 3.7]. First, represent the message in $\mathbb{F}_q^2$ as two integers x, y between 0 and $q - 1$. If α is chosen such that the order ℓ of α satisfies

$$\Phi_6(q) = s \cdot \ell$$

with s a small integer, then we expect that the output $\psi(x, y)$ can be forced to be in the subgroup generated by α by inserting some redundant bits into x and y and repeating trials.

With a message encoding and parameters decided, there are natural analogues to most common cryptosystems.

6.1.2 Torus-based key agreement

This key agreement scheme is an analogue of the Diffie-Hellman key agreement [DH76]. Two users, Alice and Bob, use this protocol to share a secret between themselves, while communicating only over an insecure channel.

1. Alice chooses a random integer exponent a in the range $1 \leqslant a \leqslant \ell - 1$, and uses it to compute the random power $\alpha^a \in T_6(\mathbb{F}_q)$. She sends Bob the compressed representation
$$P_A := \rho(\alpha^a) \in \mathbb{F}_q^2.$$
At the same time as Alice is choosing her exponent a, Bob chooses a random integer exponent b in the range $1 \leqslant b \leqslant \ell - 1$. He simultaneously uses it to send Alice the compressed representation
$$P_B := \rho(\alpha^b) \in \mathbb{F}_{q^2}.$$
2. Alice decompresses P_B and exponentiates by a to compute
$$\psi(P_B)^a = \alpha^{ab} \in T_6(\mathbb{F}_q).$$
Simultaneously, Bob decompresses P_A and exponentiates by b to compute
$$\psi(P_A)^b = \alpha^{ab} \in T_6(\mathbb{F}_q).$$
3. Alice and Bob share $\alpha^{ab} \in T_6(\mathbb{F}_q)$, or if they prefer, the compressed representation $\rho(\alpha^{ab}) \in \mathbb{F}_q^2$.

6.1.3 Torus-based encryption

This encryption scheme is an analogue of ElGamal encryption; see, for example, [ElG85] or [MvOV96, Chapter 8]. In this scenario, Bob wishes to send Alice a message over an insecure channel, with the condition that only Alice can read the message.

1. Alice must first generate a public/private key pair. She chooses a random integer exponent a in the range $1 \leqslant a \leqslant \ell - 1$, keeps a as her private key, and publishes her public key
$$\mathrm{Pub}_A = \rho(\alpha^a) \in \mathbb{F}_q^2.$$

2. To encrypt his message, Bob first represents the message as an element M of the group generated by α. He then chooses a random blinding exponent k in the range $1 \leqslant k \leqslant \ell - 1$, and computes the blind
$$\gamma = \rho(\alpha^k) \in \mathbb{F}_q^2$$
and the blinded message
$$\delta = \rho(M\psi(\mathrm{Pub}_A)^k) \in \mathbb{F}_q^2.$$
Bob sends Alice the pair (γ, δ).

3. To decrypt Bob's cipher-text pair (γ, δ), Alice decompresses both and computes
$$\psi(\delta)\psi(\gamma)^{-a} = M(\alpha^a)^k(\alpha^k)^{-a} = M \in T_6(\mathbb{F}_q).$$

6.1.4 Torus-based digital signatures

This digital signature scheme is an analogue of ElGamal signatures; see, for example, [ElG85] or [MvOV96, Chapter 11]. Alice wants to digitally sign a message to be sent to Bob, where the message is represented as an element M in the group generated by α. To do this, she needs a cryptographic hash function
$$H : \{0,1\}^\star \longrightarrow \mathbb{Z}/\ell\mathbb{Z};$$
for more information on cryptographic hash functions, see [MvOV96, Chapter 9].

1. First, Alice needs to generate a public/private key pair, which she does exactly the same way she does for the torus-based encryption scheme. She chooses a random integer exponent a in the range $1 \leqslant a \leqslant \ell - 1$, and keeps a as her private key while distributing her public key
$$\mathrm{Pub}_A := \rho(\alpha^a) \in \mathbb{F}_q^2.$$

2. To sign the message represented by M, Alice chooses a random integer k in the range $1 \leqslant k \leqslant \ell - 1$ and computes the blind

   $$\gamma = \rho(\alpha^k) \in \mathbb{F}_q^2.$$

   She then computes the blinded value

   $$\delta = k^{-1}(H(M) - aH(\gamma)) \pmod{\ell}.$$

   She sends Bob her signature on the message M, the pair (γ, δ).

3. To verify Alice's signature pair (γ, δ) on the message represented by M, Bob computes

   $$\mathrm{Sig} := \psi(\mathrm{Pub}_A)^{H(\gamma)}\psi(\gamma)^{\delta} \in T_6(\mathbb{F}_q)$$

   and compares Sig with $\alpha^{H(M)} \in T_6(\mathbb{F}_q)$. If Alice's signature is well formed, then

   $$\mathrm{Sig} = \psi(\mathrm{Pub}_A)^{H(\gamma)}\psi(\gamma)^{\delta} = (\alpha^a)^{H(\gamma)}(\alpha^k)^{k^{-1}(H(M)-aH(\gamma))} = \alpha^{H(M)} \in T_6(\mathbb{F}_q).$$

   Bob accepts Alice's signature if and only if Sig and $\alpha^{H(M)}$ are equal in the torus $T_6(\mathbb{F}_q)$.

All the protocols presented depend on the DLP in the group $T_6(\mathbb{F}_q)$. (Technically, the analogues of Diffie-Hellman key agreement and ElGamal encryption depend on the Diffie-Hellman problem, but for simplicity we will consider only the discrete logarithm problem.)

Definition 6.1. *Let G be a finite group written multiplicatively. Given two elements, g and h in G, with $h \in \langle g \rangle$, the discrete logarithm problem is to compute an integer x such that*

$$h = g^x.$$

We call the triple (G, g, h) an instance of the discrete logarithm problem.

A complete review of the DLP from a cryptographic perspective is far beyond the scope of this work, so we will be satisfied to say that the DLP in the multiplicative group of finite fields is believed to be intractable for sufficiently large field sizes, and underlies many cryptosystems used by industry. Comprehensive coverage can be found in [MvOV96, Chapter 3].

6.2 Discrete logarithms in $\mathbb{F}_{q^n}^\times$

Let n be a fixed positive integer and let $\mathbb{F}_q$ be a finite field. Rubin and Silverberg claim that their torus-based cryptosystems are essentially as secure as existing cryptosystems based on the discrete logarithm problem [RS03, Section 6] [RS04b, Section 3.11] [GV05].

An instance of the DLP in $\mathbb{F}_{q^n}^\times$ can be reduced as follows. Suppose $h \in \mathbb{F}_{q^n}^\times$ is given, and that g generates $\mathbb{F}_{q^n}^\times$. We wish to compute x such that

$$h = g^x,$$

ie the triple $(\mathbb{F}_{q^n}, g, h)$ is an instance of the discrete logarithm problem.

Applying the norm maps $N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}$ to g and h, for subfields $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$, yields a collection of discrete logarithm problems

$$\left\{ \left(\mathbb{F}_{q^d}^\times, N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(g), N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(h) \right) \right\}_{d|n}.$$

It follows that if these problems in the smaller fields $\mathbb{F}_{q^d}$ can be solved, then the solutions can be combined to solve the original problem modulo

$$\operatorname{lcm}\left(\{\Phi_d(q)\}_{d|n} \right).$$

Since all the problems with $d < n$ are in strictly smaller subfields, it is not unreasonable to expect these problems to be computable.

The remaining modular information is determined by a DLP in the torus $T_n(\mathbb{F}_q)$, and, as observed by Rubin and Silverberg, we expect this problem to be the most difficult.

If we consider only the order of the multiplicative group of the extension field $\mathbb{F}_{q^n}$, we have that

$$|\mathbb{F}_{q^n}^\times| = q^n - 1.$$

Recalling the relation

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

and the fact that, by Theorem 2.2, the order of the norm-1 torus $T_d(\mathbb{F}_q)$ is $\Phi_d(q)$, we see that we are very near to a group isomorphism

$$\mathbb{F}_{q^n}^\times \cong \prod_{d|n} T_d(\mathbb{F}_q).$$

Unfortunately, the norm-1 torus orders $\Phi_d(q)$ may share repeated divisors, so we cannot appeal to the Fundamental Theorem of Abelian Groups (Theorem 5.3) to establish an isomorphism.

Throughout this chapter, we will be dogged by the fact that $\mathbb{F}_{q^n}^\times$ is not isomorphic to the product of norm-1 tori $\prod_{d|n} T_d(\mathbb{F}_q)$, but we will simplify matters by assuming that the product of the repeated divisors is negligible when compared to the complete discrete logarithm computation, which is a reasonable assumption in cryptographic applications. The following result supports our assumption: Voskresenskii [Vos98, pp. 60-61] shows that there is a birational isomorphism of algebraic groups

$$\mathbb{F}_{q^n}^\times \longrightarrow \prod_{d|n} T_d(\mathbb{F}_q),$$

and Rubin and Silverberg [RS04b, Section 3.11] claim that the prime divisors of the orders of the kernel and co-kernel of this homomorphism all divide n. This decomposition allows us to conclude that the DLP in $\mathbb{F}_{q^n}^\times$ is at most as difficult as the discrete logarithm problems in the collection of norm-1 tori $\{T_d(\mathbb{F}_q)\}_{d|n}$.

Of course, if the DLP can be efficiently solved in $\mathbb{F}_{q^n}^\times$, then the DLP in the torus $T_n(\mathbb{F}_q)$ can be efficiently solved as well, since $T_n(\mathbb{F}_q)$ is a subgroup of $\mathbb{F}_{q^n}^\times$.

Summarizing, we conclude that solving the DLP in the multiplicative group

$$\mathbb{F}_{q^n}^\times$$

is equivalent to solving discrete logarithm problems in all the norm-1 tori

$$\{T_d(\mathbb{F}_q)\}_{d|n},$$

and that the most difficult of these problems is in the norm-1 torus

$$T_n(\mathbb{F}_q).$$

6.3 Attacks on tori inherited from finite fields

Since $T_n(\mathbb{F}_q)$ is a subgroup of $\mathbb{F}_{q^n}^\times$, any algorithm for computing discrete logarithms in (subgroups of) $\mathbb{F}_{q^n}^\times$ is applicable. Randomized attacks that solve the DLP in $\mathbb{F}_{q^n}^\times$ come in two flavours. The first flavour attacks the entire multiplicative group $\mathbb{F}_{q^n}^\times$. The second flavour attacks only a subgroup of $T_n(\mathbb{F}_q)$.

6.3.1 Attacks on the entire multiplicative group

The best attack known that works on the entire multiplicative group of a finite field is the Number Field Sieve [Gor93]. To express the running time of the Number Field Sieve, it is necessary to embed the subgroup $T_n(\mathbb{F}_q)$ into the smallest possible finite field, say

$$T_n(\mathbb{F}_q) \subset \mathbb{F}_{q^s}.$$

Then the heuristic asymptotic running time of the Number Field Sieve is bounded by

$$L_{q^s}(1/3, 1.923),$$

where $L_n(\alpha, c)$ is the asymptotic function

$$L_n(\alpha, c) = \exp\left((c + o(1))(\ln n)^\alpha (\ln \ln n)^{1-\alpha}\right),$$

which expresses how close a function is to polynomial in $\ln n$. When $\alpha = 0$, L_n is polynomial:

$$L_n(0, c) = \exp\left((c + o\left(1\right)) \ln \ln n\right) = (\ln n)^{c+o(1)} = O\left((\ln n)^{c+1}\right);$$

on the other hand, when $\alpha = 1$, L_n is fully exponential:

$$L_n(1, c) = \exp\left((c + o(1)) \ln n\right) = n^{c+o(1)} = O\left(n^{c+1}\right).$$

Thus, since $T_n(\mathbb{F}_q) \subset \mathbb{F}_{q^n}^\times$, the Number Field Sieve solves instances of the DLP in subexponential (but super-polynomial) time. In fact, the smallest field $\mathbb{F}_{q^s}$ that $T_n(\mathbb{F}_q)$ embeds into is $\mathbb{F}_{q^n}$, by the following theorem.

Theorem 6.2. *[BHV02, Lemma 1 correcting [Len97, Lemma 2.4]] The smallest field that $T_n(\mathbb{F}_q)$ embeds into is $\mathbb{F}_{q^n}$, ie*

$$T_n(\mathbb{F}_q) \not\subset \mathbb{F}_{q^m}$$

for all $m|n$ with $m < n$.

Proof. Let ℓ be a prime dividing $|T_n(\mathbb{F}_q)| = \Phi_n(q)$ but not dividing n. (For large q, such an ℓ exists with high probability, and the proof can be modified in the exceptional cases.) Since ℓ does not divide n, over the polynomial ring $\mathbb{F}_\ell[X]$, we have

$$\gcd(X^n - 1, nX^{n-1}) = 1,$$

and it follows that $X^n - 1$ has no repeated roots in the algebraic closure $\bar{\mathbb{F}}_\ell$. Since

$$X^n - 1 = \prod_{d|n} \Phi_d(X),$$

and since q is a root of $\Phi_n(X)$ in $\mathbb{F}_\ell$, we see that no other factor $\Phi_d(X)$ can have q as a root in $\mathbb{F}_\ell$. Therefore,

$$\Phi_d(q) \not\equiv 0 (\operatorname{mod} \ell),$$

for all $d|n$ with $d < n$, from which it follows that, for $m|n$ with $m < n$,

$$q^m - 1 = \prod_{e|m} \Phi_e(q) | \prod_{d|n, d<n} \Phi_d(q) \not\equiv 0 (\operatorname{mod} \ell).$$

Since there is a subgroup of order ℓ in $T_n(\mathbb{F}_q)$, and this subgroup does not embed into any subfield $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$, we conclude that the smallest field $T_n(\mathbb{F}_q)$ embeds into is $\mathbb{F}_{q^n}$. □

Thus, in our analysis, $\mathbb{F}_{q^s} = \mathbb{F}_{q^n}$, and the Number Field Sieve requires running time bounded by

$$L_{q^n}(1/3, 1.923).$$

Therefore, to ensure that DLP instances are computationally infeasible, the field order

$$q^n - 1$$

must be very large. Since our torus-based cryptosystems need the torus T_n to be rational, and the only torus for which we have constructed a birational parameterization is T_6, n is a fixed small integer in our analysis. Therefore, the difficulty of computing discrete logarithms is directly proportional to the field size q.

6.3.2 Attacks on a subgroup

The best attack known that works a the subgroup of $T_n(\mathbb{F}_q)$ is Pollard's Rho Method [Pol78, Tes98]. The running time of Pollard's Rho Method is fully exponential in the size of the target subgroup, but by using the Pohlig-Hellman reduction [PH78] to subgroups of prime order, we can compute discrete logarithms in a subgroup of $T_n(\mathbb{F}_q)$ in time bounded by

$$O\left(\sqrt{\ell}\right),$$

where ℓ is the largest prime divisor of $|T_n(\mathbb{F}_q)| = \Phi_n(q)$. Therefore, to ensure that DLP instances are computationally infeasible, the largest prime

$$\ell | \Phi_n(q)$$

must be very large. Ideally, a subgroup of $T_n(\mathbb{F}_q)$ of order ℓ close to $\Phi_n(q)$ is used, with ℓ just large enough to prevent Pollard's Rho Method, and $|\mathbb{F}_{q^n}|$ just large enough to prevent the Number Field Sieve.

6.4 Selecting parameters to avoid attacks

Motivated by the two requirements of Section 6.3 that are needed to ensure the discrete logarithm problem is computationally infeasible, we make the following definitions.

Definition 6.3. *Let*

$$\ell_{\text{bits}}$$

be a positive integer such that the Pollard Rho algorithm is computationally infeasible in a group of prime order ℓ, with

$$\ell \approx 2^{\ell_{\text{bits}}}.$$

Definition 6.4. *Let*

$$N_{\text{bits}}$$

be a positive integer such that the Number Field Sieve is computationally infeasible in finite field multiplicative groups $F^\times$ of order N, with

$$N \approx 2^{N_{\text{bits}}}.$$

For input security parameters ℓ_{bits} and N_{bits}, the following algorithms generate parameters for torus-based cryptosystems, such as CEILIDH and the system based on $T_{30}(\mathbb{F}_q)$ [vDW04]. (For the details of choosing parameters for the XTR cryptosystem, see [LV00].)

The first algorithm is a specialization of the method of Rubin and Silverberg [RS03, Section 6].

1. For concreteness, suppose that
$$N_{\text{bits}} = 1024$$
and
$$\ell_{\text{bits}} = 160.$$
These choices provide heuristic security comparable to the RSA cryptosystem with 1024 bit modulus [LV00, Section 3].

2. Fix the torus degree $n = 6$, and let the maps parameterizing $T_6(\mathbb{F}_q)$ be those of Example 4.7. To render the Number Field Sieve computationally infeasible, we need $|\mathbb{F}_{q^6}^\times|$ large. Thus, we must find a prime q with
$$q^6 \approx 2^{N_{\text{bits}}} \approx 2^{1024},$$
which means that q is approximately 170 bits. By the Prime Number Theorem [HW79, Theorem 6], there are approximately
$$\frac{2^{170}}{\ln 2^{170}} - \frac{2^{169}}{\ln 2^{169}} \approx 6.3 \times 10^{48} \approx 2^{162}$$
primes of 170 bits, which means that it is feasible to generate primes of the desired size by selecting random 170 bit integers and testing for primality.

3. To use the maps of Example 4.7, we need $q \equiv 2 \pmod 9$. By the Chebotarev Density Theorem [SJ96], the proportion of primes congruent to 2 modulo 9 is
$$\frac{1}{\varphi(9)} = \frac{1}{6}.$$
Thus choosing random primes until we find one congruent to 2 modulo 9 is feasible.

4. To render Pollard's Rho method computationally infeasible, we also need that $\Phi_6(q)$ is divisible by a large prime ℓ of about 160 bits. Although there is no theoretical guarantee, we expect about
$$2^{162}(\ln 161 - \ln 160) \approx 3.6 \times 10^{46} \approx 2^{154}$$
primes q such that $\Phi_6(q)$ has a large prime divisor of about 160 bits, and in practice $\Phi_6(q)$ can be partially factored and tested for primality efficiently.

The preceding algorithm produces primes q, suitable for use with the torus $T_6(\mathbb{F}_q)$, in negligible time. Note that we do not fix the prime ℓ and generate a suitable q; this would require finding a q such that ℓ is a root of $\Phi_6(x)$ modulo q.

In the case of the stably rational torus system of van Dijk and Woodruff (Chapter 5), which is based on the torus $T_{30}(\mathbb{F}_q)$, the relative sparseness of suitable primes requires a slightly more complicated scheme. We therefore present the following modification, also due to Rubin and Silverberg [RS04b, Section 3.10].

1. Again, for concreteness, suppose that
$$N_{\text{bits}} = 1024$$
and
$$\ell_{\text{bits}} = 160.$$

2. Since the torus degree is $n = 30$, we need to find a prime q such that
$$q^{30} \approx 2^{1024},$$
or
$$q \approx 2^{35}.$$
Generating such primes randomly is easy, but the probability that a large prime ℓ divides $\Phi_{30}(q)$ is prohibitively small.

3. To increase the chances of finding a large prime ℓ dividing $\Phi_{30}(q)$, choose a random prime
$$p \equiv 1 (\operatorname{mod} 30)$$
with
$$p \approx 2^{30}.$$
There are $\varphi(30) = 8$ elements $1 \leqslant x \leqslant p-1$ that have multiplicative order exactly 30 modulo p. (If g generates $\mathbb{F}_p$, then $g^{\frac{p-1}{30}}$ generates a cyclic subgroup of order 30, which has 8 generators.) Denote the eight primitive thirtieth roots of unity
$$x_1, \ldots, x_8.$$

4. Choose random primes $q \approx 2^{35}$ such that

   $$q \equiv x_i (\operatorname{mod} p), \quad \text{for some } 1 \leqslant i \leqslant 8.$$

   (Again, the Chebotarev Density Theorem tells us this is feasible.)

   Since each x_i is a primitive thirtieth root of unity modulo p, it follows that

   $$\Phi_{30}(q) \equiv \Phi_{30}(x_i) \equiv 0 (\operatorname{mod} p).$$

   We hope to find q such that $\Phi_{30}(q)/p$ is divisible by a large prime factor ℓ.

5. Because

   $$\Phi_{30}(q)/p \approx q^8/p \approx 2^{280}/2^{30} \approx 2^{250},$$

   and we want to find a prime $\ell \approx 2^{160}$ dividing $\Phi_{30}(q)/p$, we expect to need to remove factors between about 2^{90} and 2^{100} from $\Phi_{30}(q)/p$. Rubin and Silverberg suggest that the Elliptic Curve Method [HL87], optimized for factors in this range, can be used to remove factors from $\Phi_{30}(q)/p$. Finally, we test to see if what remains after the factoring has been done is a prime ℓ of size approximately 2^{160}.

Rubin and Silverberg [vDW04, Section 5.5] claim that it is possible to generate primes $q \approx 2^{32}$ with the desired properties at the rate of one every several minutes, and also that primes $q \approx 2^{64}$ can be generated at the rate of one every several few hours. Since system-wide parameters rarely need to be changed, these results demonstrate that these cryptosystems can be instantiated with parameter choices believed to be secure.

Now that we have considered the best attacks known based on the interpretation of the torus $T_n(\mathbb{F}_q)$ as a subgroup of $\mathbb{F}_{q^n}^\times$, and shown how to select parameters such that these attacks are believed to be computationally infeasible, we turn to a radical new attack based on the representation of norm-1 tori.

6.5 Relation calculus for algebraic tori

In the previous sections, we chose prime fields $\mathbb{F}_q$ and argued that the norm-1 torus $T_n(\mathbb{F}_q)$ over $\mathbb{F}_q$ was secure with respect to the best attacks known. In this section, we present new research of Granger and Vercauteren [GV05] that, in certain cases, shows that norm-1 tori over extension fields $\mathbb{F}_{p^m}$ are "not secure". By "not secure", we mean that the DLP can be solved in time significantly less than the time required by Pollard's Rho algorithm, but not necessarily that real world parameter choices are weak. We emphasize that the new results of Granger and Vercauteren do not cryptographically weaken the security of norm-1 tori over prime fields; they only weaken tori over certain extension fields. The attack does target tori over prime fields, by embedding them into lower dimensional rational tori over extensions fields, but the attack runs in the same time as Pollard's Rho Method in the full torus. In practice, when a smaller subgroup of $T_n(\mathbb{F}_q)$ is used, Pollard's Rho Method is superior. Since XTR and CEILIDH are usually instantiated over prime fields, these systems are not compromised. However, these results are significant because they demonstrate that the structure of norm-1 tori, used to construct cryptosystems, can also be exploited to destructive cryptographic advantage by a cryptanalyst.

The work of Granger and Vercauteren is an application of an idea of Gaudry [Gau]. Gaudry's idea was to abstract the approaches of index calculus algorithms, attacking the DLP in multiplicative groups of finite fields [Adl79] and the Jacobians of hyperelliptic curves [ADH94, Gau00, The03], to a purely algebraic attack against arbitrary algebraic groups, and in particular elliptic curve cryptosystems. We will give a brief sketch of Gaudry's relation calculus before describing specializations to norm-1 tori.

Suppose that $G = (\mathcal{P}, \otimes)$ is a group, written multiplicatively. If we distinguish two elements $P \in \mathcal{P}$ and $Q \in \mathcal{P}$, with $Q \in \langle P \rangle$, then the DLP (G, P, Q) is well defined, ie we must find x such that

$$Q = P^x.$$

Our strategy is to distinguish a decomposition base

$$\mathcal{B} = \{P_1, \dots, P_M\} \subset \mathcal{P},$$

and hope to find relations of the form

$$Q^{\alpha_i} P^{\beta_i} = \bigotimes_{j=1}^{|\mathcal{B}|=M} P_j^{e_{ij}}. \tag{6.1}$$

Such relations involve only P, Q, and the decomposition base elements P_i.

If we find enough relations of the form (6.1), then the system

$$\begin{pmatrix} \alpha_1 & \beta_1 & e_{1P_1} & e_{1P_2} & \cdots & e_{1P_M} \\ \alpha_2 & \beta_2 & e_{2P_1} & e_{2P_2} & \cdots & e_{2P_M} \\ \vdots & & & & & \vdots \end{pmatrix}$$

will be over-determined, and with high probability a linear identity

$$Q^\alpha P^\beta = 1$$

can be computed. From this linear identity, the value of x can be computed, solving the DLP.

Of course, this high level overview completely glosses over the technical details crucial to all index calculus algorithms. In order to flesh out the skeleton, we must demonstrate how several things are done. We must:

i. Explain how to choose a decomposition base $\mathcal{B}$.

ii. Explain how to find relations of the form (6.1).

iii. Argue that finding "enough" relations is computationally feasible.

iv. Argue that solving the resulting linear system is computationally feasible.

Let us do these things for the torus $T_2(\mathbb{F}_q)$.

6.6 Relation calculus for the torus $T_2(\mathbb{F}_{p^m})$

In this section, we describe an algorithm for solving discrete logarithms in the torus $T_2(\mathbb{F}_{p^m})$.

6.6.1 Algorithm description

Torus representation. By Hilbert's Theorem 90 (Theorem 4.3), every element of $T_2(\mathbb{F}_{p^m})$ can be represented as

$$\frac{z}{\sigma(z)},$$

with $z \in \mathbb{F}_{p^{2m}}$. We can make this representation explicit by fixing a basis for $\mathbb{F}_{p^{2m}}$ over $\mathbb{F}_{p^m}$. Let $\delta \in \mathbb{F}_{p^m} \backslash \mathbb{F}_p$ be a non-square, and represent $\mathbb{F}_{p^{2m}}$ as

$$\mathbb{F}_{p^m}[\gamma]/(\gamma^2 - \delta),$$

with polynomial basis $\{1, \gamma\}$. With this representation, every element in $T_2(\mathbb{F}_{p^m})$ save 1 can be written as $\frac{x-\gamma}{x+\gamma}$, with $x \in \mathbb{F}_{p^m}$, so that

$$T_2(\mathbb{F}_{p^m}) = \left\{ \frac{x-\gamma}{x+\gamma} : x \in \mathbb{F}_{p^m} \right\} \cup \{1\}.$$

Observe that this representation makes clear that there are

$$p^m + 1 = \Phi_2(p^m)$$

elements in $T_2(\mathbb{F}_{p^m})$.

Decomposition base. With this description of the torus $T_2(\mathbb{F}_{p^m})$ in mind, we define our decomposition base to be

$$\mathcal{B} = \left\{ \frac{a-\gamma}{a+\gamma} : a \in \mathbb{F}_p \right\}.$$

Observe that this representation makes clear that

$$|\mathcal{B}| = p,$$

and thus our linear system will have $p + 2$ unknowns, which means that we require about $p + 3$ relations.

Remark 6.5. As observed by Granger and Vercauteren [GV05, Section 4.2], if $\delta \in \mathbb{F}_p$, then for any element $a \in \mathbb{F}_p$,

$$\frac{a-\gamma}{a+\gamma} = \left(\frac{a-\gamma}{a+\gamma}\right)\left(\frac{a-\gamma}{a-\gamma}\right) = \frac{a^2 - 2a\gamma + \gamma^2}{a^2 - \gamma^2} = \frac{a^2 + \delta - 2a\gamma}{a^2 - \delta} \in \mathbb{F}_{p^2},$$

which means that this choice of δ makes the factor base a subset of a subvariety of $T_2(\mathbb{F}_{p^m})$:

$$\mathcal{B} \subset T_2(\mathbb{F}_p).$$

It follows that the only torus elements we could decompose over this $\mathcal{B}$ are elements in $T_2(\mathbb{F}_p)$, so that we would not be able to solve most discrete logarithm problems in $T_2(\mathbb{F}_{p^m})$.

Relation finding. We hope to find relations of the form

$$P^j Q^k = P_1 \otimes P_2 \otimes \cdots \otimes P_m,$$

with each P_i in the factor base $\mathcal{B}$. (Remark 6.6 explains why we seek relations incorporating exactly m elements.)

Since the operation $\otimes$ in the group $T_2(\mathbb{F}_{p^m})$ is just multiplication in the finite field, we hope to solve

$$P^j Q^k = P_1 P_2 \cdots P_m.$$

Representing $P^j Q^k$ by

$$R = P^j Q^k = \frac{r - \gamma}{r + \gamma},$$

with $r \in \mathbb{F}_{p^m}$, we are hoping to find elements $P_i = \frac{a_i - \gamma}{a_i + \gamma}$ such that

$$\prod_{i=1}^{m} \left(\frac{a_i - \gamma}{a_i + \gamma} \right) = \frac{r - \gamma}{r + \gamma}. \tag{6.2}$$

Since we want the P_i to be in the decomposition base $\mathcal{B}$, the a_i are unknowns in $\mathbb{F}_p$. Granger and Vercauteren [GV05, Section 4.3] show how to solve for the a_i. Their method exploits the symmetry of the set $\{a_1, \ldots, a_m\}$ to obtain a system M of m linear equations over $\mathbb{F}_p$. When a solution to the system M exists, it may correspond to a decomposition of R of the form (6.2). The potential decomposition is then checked to see if a relation has been found.

Remark 6.6. The reason we seek relations incorporating exactly m elements of the factor base is because elements of $\mathbb{F}_{p^m}$ are represented as polynomials of degree less than m: the system M consists of m equations relating the roots $a_1, \ldots, a_m$ to each other, with respect to a polynomial basis $\{1, t, \ldots, t^{m-1}\}$ of $\mathbb{F}_{p^m}$. Since there are m basis elements $\{1, t, \ldots, t^{m-1}\}$, the linear system yields relations when there are m unknowns $a_1, \ldots, a_m$, or equivalently m elements $P_1, \ldots, P_m$.

Analysis. Checking to see if a relation decomposes over the decomposition base $\mathcal{B}$, and computing the coefficients a_i in (6.2) can be done relatively easily. The crucial question is, "How long does it take to find enough relations?" (Recall that "enough relations" is $O(p)$ relations.)

Granger and Vercauteren [GV05, Section 4.4] provide the following estimate. They show that the number of elements of $T_2(\mathbb{F}_{p^m})$ generated by m elements of the decomposition base $\mathcal{B}$ is roughly

$$\frac{|\mathcal{B}|^m}{m!} \approx \frac{p^m}{m!}.$$

Since

$$|T_2(\mathbb{F}_{p^m})| \approx p^m,$$

under reasonable assumptions we expect one in every $m!$ relations we try to decompose over the factor base. The theorem that accounts for the computation required by the "relation decomposition stage" follows.

Theorem 6.7. *[GV05, Theorem 1] The expected running time of the T_2 algorithm to compute discrete logarithms in $T_2(\mathbb{F}_{p^m})$ is*

$$O\left(m!p(m^3 + m^2 \log p) + m^3p^2\right)$$

operations in $\mathbb{F}_p$.

Theorem 6.7 shows that the T_2 algorithm performs best when

$$m! = p,$$

which is equivalent to

$$m \log m \approx p.$$

In this case, Granger and Vercauteren show that the T_2 algorithm runs in expected time

$$L_{p^m}\left(1/2, c\right),$$

for some positive constant c. Cryptographically meaningful comparison with the expected running time of the Number Field Sieve, is not possible at this time, because the constant c is not well understood, and no comparable reference implementations exist. Moreover, for some parameters, the Number Field Sieve runs in time $L_{p^{2m}}\left(1/2, c'\right)$. Therefore our assumption that the number field sieve runs in time $L_{p^{2m}}(1/3, 1.923)$, which is the most conservative security assumption, may incorrectly indicate that the Number Field Sieve is superior to the attack of Granger and Vercauteren.

6.6.2 Cryptographic significance

To demonstrate the feasibility of their algorithm, Granger and Vercauteren include computational data [GV05, Section 4.4]. Using an unoptimized Magma [BCP97] implementation, they assessed the practicality of their algorithm in cases where it is likely to be feasible.

Since we require $O(p)$ relations, we must be able to find a kernel vector in a system of dimension $O(p)$; with this requirement in mind, the authors assumed that the linear algebra is computationally feasible only when $p \leqslant 2^{23}$.

Table 6.1 summarizes some of Granger and Vercauteren's feasibility results [GV05, Table 1]. In the table, the size of the torus is constant across each row, and • marks the combinations of p and m that can be attacked with the Magma implementation.

											m					
$\lvert\mathbb{F}_{p^{2m}}\rvert$	$\lvert T_2(\mathbb{F}_{p^m})\rvert$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2^{200}	2^{100}					•	•	•	•	•	•	•	•	•	•	•
2^{300}	2^{150}							•	•	•	•	•	•	•	•	•
2^{400}	2^{200}									•	•	•	•	•	•	•
2^{500}	2^{250}											•	•	•	•	
2^{600}	2^{300}															
2^{700}	2^{350}															

Table 6.1: The Magma T_2 implementation is feasible for some values of p and m.

In addition, the authors show that if the values of p and m chosen are even feasible with their Magma implementation, the T_2 algorithm in the whole torus $T_2(\mathbb{F}_{p^m})$ outperforms Pollard's Rho method in a subgroup of $\mathbb{F}_{p^{2m}}$ of order 2^{160}. Thus their algorithm is cryptographically significant, in the sense that any improvement on Pollard's Rho method is a potential weakness.

The existence of an algorithm superior to Pollard's Rho in even a single instance shows that the structure of norm-1 tori can also be used by a potential cryptanalyst, and that some care must be exercised when designing cryptosystems. As an example, note that in the XTR and CEILIDH cryptosystems,

$$T_6(\mathbb{F}_q) \subset T_2(\mathbb{F}_{q^3}),$$

so that the T_2 attack applies with $m = 3$; however, as shown in Table 6.1, there are no field sizes such that the T_2 attack is both practical and superior to Pollard's Rho method. However, in the system based on $T_{30}(\mathbb{F}_q)$ of Chapter 5, we have

$$T_{30}(\mathbb{F}_q) \subset T_2(\mathbb{F}_{q^{15}}),$$

and the field sizes that can be handled by the Magma implementation are approaching those used in cryptographic applications. Ultimately, however, the LUC [SL93], XTR [LV00], and CEILIDH [RS03] cryptosystems over a prime field are not compromised by the T_2 attack of Granger and Vercauteren.

We conclude that the T_2 attack is interesting in theory, but does not directly damage the torus-based cryptosystems we have studied.

6.7 Relation calculus for the torus $T_6(\mathbb{F}_{p^m})$

We also sketch Granger and Vercauteren's attack on the the torus $T_6(\mathbb{F}_{p^m})$ [GV05, Section 5].

6.7.1 Algorithm description

For concreteness, fix a finite field $\mathbb{F}_p$ with $p \equiv 2 (\operatorname{mod} 9)$, and let

$$\mathbb{F}_{p^m} = \mathbb{F}_p[t]/(f(t))$$

be represented by the polynomial basis

$$\{1, t, \ldots, t^{m-1}\}.$$

We use the rational maps developed in Example 4.7 to parameterize the torus $T_6(\mathbb{F}_{p^m})$. Recall that these maps exploit the field representations $\mathbb{F}_{p^{2m}} = \mathbb{F}_{p^m}(x)$ with $x^2 + x + 1 = 0$, and $\mathbb{F}_{p^{3m}} = \mathbb{F}_{p^m}(y)$ with $y^3 - 3y + 1 = 0$.

The elements of $T_6(\mathbb{F}_{p^m})$ are represented via the map

$$\begin{gathered}\psi : \mathbb{A}^2(\mathbb{F}_{p^m}) \longrightarrow T_6(\mathbb{F}_{p^m}) \\ \psi(v_1, v_2) = \tfrac{1+v_1y+v_2(y^2-2)+(1-v_1^2-v_2^2+v_1v_2)x}{1+v_1y+v_2(y^2-2)+(1-v_1^2-v_2^2+v_1v_2)x^2}.\end{gathered}$$

Choose the decomposition base

$$\mathcal{B} = \{\psi(at, 0) : a \in \mathbb{F}_p\} = \left\{ \frac{1 + (at)y + (1 - (at)^2)x}{1 + (at)y + (1 - (at)^2)x^2} \right\}.$$

Observe that the more natural choice $\{\psi(a, 0) : a \in \mathbb{F}_p\}$ is a subset of the subvariety $T_6(\mathbb{F}_p) \subset T_6(\mathbb{F}_{p^m})$; the $\mathcal{B}$ defined above generates "enough" of $T_6(\mathbb{F}_{p^m})$ for the relation calculus to be successful.

We seek relations of the form

$$P^j Q^k = P_1 \otimes P_2 \otimes \cdots \otimes P_{2m},$$

with each P_i in the factor base $\mathcal{B}$. We search for relations incorporating exactly $2m$ elements because $T_6(\mathbb{F}_{p^m})$ is $2m$ dimensional over the ground field $\mathbb{F}_p$; another way to say the same thing is that each element P_i represents a single degree of freedom in the $2m$-dimensional torus $\operatorname{Res}_{\mathbb{F}_{p^m}/\mathbb{F}_p} T_6$.

Representing

$$P^j Q^k = \psi(r_1, r_2) = \frac{1 + r_1 y + r_2(y^2 - 2) + (1 - r_1^2 - r_2^2 + r_1 r_2)x}{1 + r_1 y + r_2(y^2 - 2) + (1 - r_1^2 - r_2^2 + r_1 r_2)x^2} \in T_6(\mathbb{F}_{p^m}),$$

we seek to decompose

$$\prod_{i=1}^{2m} \left(\frac{1 + (a_i t)y + (1 - (a_i t)^2)x}{1 + (a_i t)y + (1 - (a_i t)^2)x^2} \right) = \frac{1 + r_1 y + r_2(y^2 - 2) + (1 - r_1^2 - r_2^2 + r_1 r_2)x}{1 + r_1 y + r_2(y^2 - 2) + (1 - r_1^2 - r_2^2 + r_1 r_2)x^2}. \quad (6.3)$$

Upon expansion and symmetrization, (6.3) yields a system of 3 non-linear equations over $\mathbb{F}_{p^m}$, or $3m$ non-linear equations over $\mathbb{F}_p$ (in $2m$ unknowns) [GV05, Section 5.3]. Granger and Vercauteren solve this non-linear system with standard Gröbner basis techniques [Fau99, Fau02], and use these solutions to find relations between P and Q.

6.7.2 Cryptographic significance

Rather than detail the entire T_6 algorithm, we will be satisfied to consider its cryptographic significance. Unfortunately, the Gröbner basis computations needed are sensitive to slight changes to the input, making their running time difficult to estimate. In response, Granger and Vercauteren estimate the running time of their algorithm using several pessimistic heuristics concerning the efficiency of the Gröbner basis computations. They also tested a prototype implementation in Magma. They conclude that their algorithm is theoretically superior to Pollard's Rho method when

$$m = 5,$$

even though it is only computationally feasible when

$$|\mathbb{F}_{p^m}| \leqslant 2^{600}.$$

They also claim an improvement in running time (measured in seconds) by a factor of more than 2^{20} over Pollard's Rho Method in a subgroup of order 2^{160} in several cases [GV05, Table 2].

Granger and Vercauteren show that their T_6 algorithm does not impact the security of the XTR and the CEILIDH cryptosystems over prime fields. However, the attack does apply to cryptosystems constructed using the torus $T_{30}(\mathbb{F}_q)$, because

$$T_{30}(\mathbb{F}_p) \subset T_6(\mathbb{F}_{p^5}).$$

In addition, it applies to a proposed extension of XTR to fields of the form $\mathbb{F}_{p^{6\ell}}$ [LKY$^+$01]. These results have challenged the security of discrete logarithm cryptosystems in extension fields of degree thirty, although, at this time, the algorithm is not feasible in fields of cryptographic size. Even so, Granger and Vercauteren have shown the discrete logarithm problem in $T_{30}(\mathbb{F}_{p^m})$ to be less difficult than previously believed.

6.8 Summary

In this section, we presented the protocols of Rubin and Silverberg for torus-based cryptography. Motivated by these protocols, we discussed the two attacks inherited from finite fields most likely to attack torus-based cryptosystems, and showed how to choose parameters that are believed to make these attacks infeasible. In addition, we discussed new algorithms specific to algebraic tori and showed that they are cryptographically relevant. Based on the results of Granger and Vercauteren, we believe that:

- Cryptosystems based on the torus $T_6(\mathbb{F}_p)$ over a prime field of order p, such as the XTR and CEILIDH cryptosystems, are secure when instantiated with correctly chosen parameters.

- Cryptosystems based on the torus $T_{30}(\mathbb{F}_q)$, such as those due to van Dijk, Woodruff, et al. presented in Chapter 5, may be insecure, and further work must be done to assess the practicality of the T_6 algorithm in $T_6(\mathbb{F}_{p^5})$ for cryptographic field sizes.

Chapter 7

Conclusion

This thesis presented algebraic tori and their applications to cryptography. We gave an elementary presentation of norm-1 tori, and used this understanding to interrogate the pioneering work of Rubin and Silverberg interpreting the LUC and XTR cryptosystems geometrically. In addition, we showed that insight into the rational geometry of norm-1 tori leads to the simplified CEILIDH cryptosystem, and explained that the improved stably rational cryptosystems of van Dijk, Woodruff, and co-authors, generalize the rational property exploited by CEILIDH. Finally, we showed that the new attacks of Granger and Vercauteren exploiting the rational geometry of norm-1 tori must be considered when designing cryptosystems that work in small degree extension fields.

While the constructive and destructive uses of algebraic tori in cryptography presented in this thesis are significant, there remain many open questions in the field. Some possibilities for future work include:

Establishing Voskresenskii's Conjecture. If Voskresenskii's Conjecture on the rationality of norm-1 tori (Conjecture 4.2) is true, then in theory any compression ratio can be attained, because for any positive constant C there exists n such that

$$n/\varphi(n) > C.$$

Of course, for each rational torus, explicit birational maps parameterizing it would be needed, and constructing such maps might not be easy. However, it is possible that the proof of the conjecture suggests how to construct the requisite parameterizations. Therefore, the “grand prize”of torus-based cryptography must be Voskresenskii’s Conjecture. Unfortunately, the theory of norm-1 tori is deep, and there is no reason to believe the conjecture will be settled in the foreseeable future.

Parameterizing the torus quotient $T_{210}/(S_2 \times S_3 \times S_5 \times S_7)$. Rubin and Silverberg proved (Theorem 3.21) that the symmetric maps, which are the natural extension of the XTR trace map, do not parameterize the quotient $T_{30}/\left(S_2 \times S_3 \times S_5\right)$. Their proof relied on a computation specific to the torus T_{30}. Although Theorem 3.21 suggests otherwise, it is possible that the symmetric maps parameterize the quotient $T_{210}/\left(S_2 \times S_3 \times S_5 \times S_7\right)$. Further investigation into this case, and perhaps proof that the quotient variety $\mathcal{X}_{\mathbb{F}_{q^d}}$ is not rational for various fields $\mathbb{F}_{q^n}$ and subfields $\mathbb{F}_{q^d}$, would further our understanding of the LUC and XTR cryptosystems.

Investigating lossy compression. Rubin and Silverberg [RS04b, Section 6.7] claim to have constructed $s:1$ rational maps

$$T_{30}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^8,$$

with s a small integer.

Such maps could be used to implement a lossy compression scheme representing elements of $T_{30}(\mathbb{F}_q)$ by elements in $\mathbb{F}_q^8 \times \{1, 2, \ldots, s\}$, and might be more efficient than the stably rational cryptosystems of Chapter 5. Optimization of such maps, and a better understanding of the cryptographic repercussions of this compact representation, would be a valuable contribution to the field of torus-based cryptography. For example, the “relation calculus” of Gaudry, used by Granger and Vercauteren, does not rely on a concept of unique factorization. Can this calculus be used with $s:1$ rational parameterizations of algebraic tori?

Improving the attacks of Granger and Vercauteren. The bottle-neck in the T_6 algorithm of Granger and Vercauteren is the Gröbner basis computation necessary for testing if a relation is found. They analyzed [GV05, Section 5.3] the bases computed, and empirically determined that the bases had special form. Specializing their algorithm to exploit the form of the equations solved in the relation finding step might strengthen the already promising results presented.

Using norm-1 tori over binary fields. Although this thesis considers only constructions over fields of odd order, the theory of norm-1 tori presented is unchanged over fields of characteristic 2. Is it possible that torus-based cryptography can be made more efficient over binary fields? How do the attacks of Granger and Vercauteren compare to optimized discrete logarithm computations in binary fields?

Using norm-1 tori in other settings. The concept of norm is ubiquitous in mathematics; for instance, number fields and ideal class groups have well-defined norm maps. Therefore, we suggest a speculative research programme exploring cryptographic applications of (analogues of) norm-1 tori over different structures. Such an alternative structure could be a field, but could be also be a more general object, such as a ring.

Bibliography

[ADH94] L. M. Adleman, J. DeMarrais, and M.-D. A. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields. In *ANTS-I: Proceedings of the First International Symposium on Algorithmic Number Theory*, pages 28–40. Springer-Verlag, 1994.

[Adl79] L. M. Adleman. A subexponential algorithm for the discrete logarithm problem with applications. In *Proc. of the 20th Annual IEEE Symposium on Foundations of Computer Science*, pages 55–60, 1979.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The magma algebra system i: The user language. *J. Symbolic Comp.*, 24:235–265, 1997.

[BHV02] W. Bosma, J. Hutton, and E. R. Verheul. Looking beyond XTR. In *ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 46–63. Springer-Verlag, 2002.

[dB53] N. G. de Bruijn. On the factorization of cyclic groups. *Indagationes Mathematicae*, 15:370–377, 1953.

[DH76] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22:644–654, 1976.

[DJ03] I. Damgard and M. Jurik. A length-flexible threshold cryptosystem with applications. In *Australasian Conference on Information Security and Privacy*

(ACISP), volume 2727 of *Lecture Notes in Computer Science*, pages 350–364. Springer, 2003.

[ElG85] T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.

[Fau99] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1-3):61–88, June 1999.

[Fau02] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *International Symposium on Symbolic and Algebrai Computation Symposium - ISSAC 2002, Villeneuve d'Ascq, France*, July 2002.

[Ful69] W. Fulton. *Algebraic Curves: an Introduction to Algebraic Geometry.* W. A. Benjamin, New York, 1969.

[Gau] P. Gaudry. Index calculus for abelian varieties and the elliptic curve discrete logarithm problem. Preprint available at http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/.

[Gau00] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 19–34. Springer, 2000.

[Gor93] D. M. Gordon. Discrete logarithms in GF(p) using the number field sieve. *SIAM J. Discrete Math.*, 6(1):124–138, 1993.

[GPS04] R. Granger, D. Page, and M. Stam. A comparison of CEILIDH and XTR. In *Algorithmic Number Theory, 6th International Symposium, ANTS-VI*, pages 235–249. Springer, June 2004.

[GV05] R. Granger and F. Vercauteren. On the discrete logarithm problem in algebraic tori. In *Advances in Cryptology (CRYPTO 2005)*, volume 3621 of *Lecture Notes in Computer Science*, pages 66–85. Springer, 2005.

[Har95] J. Harris. *Algebraic Geometry: a First Course.* Springer, 1995.

[HL87] Jr. H.W. Lenstra. Factoring integers with elliptic curves. *Annals of Mathematics*, 126:649–673, 1987.

[HW79] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, 1979.

[J99] B. Fraleigh J. *A First Course in Abstract Algebra.* Addison-Wesley, 6 edition, 1999.

[Kly88] A. A. Klyachko. On the rationality of tori with a cyclic splitting field. In *Arithmetic and geometry of varieties (Russian)*, pages 73–78. Kuybyshev University Press, Kuybyshev, 1988.

[KY02] A. Kiayias and M. Yung. Self-tallying elections and perfect ballot secrecy. In *Public Key Cryptography - 5th International Workshop on Practice and Theory in Public Key Cryptosystems*, volume 2274 of *Lecture Notes in Computer Science*, pages 141–158. Springer, 2002.

[Len97] A. K. Lenstra. Using cyclotomic polynomials to construct efficient discrete logarithm cryptosystems over finite fields. In *ACISP 1997: Proceedings of the Second Australasian Conference on Information Security and Privacy*, pages 127–138, London, UK, 1997. Springer-Verlag.

[LKY$^+$01] S. Lim, S. Kim, I. Yie, J. Kim, and H. Lee. XTR extended to GF(p^{6m}). In *SAC 2001: Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, pages 301–312. Springer-Verlag, 2001.

[LN94] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and Their Applications.* Cambridge University Press, 1994.

[LV00] A. K. Lenstra and E. R. Verheul. The XTR public key system. In *CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Sciences*, pages 1–19. Springer-Verlag, 2000.

[MvOV96] A. Menezes, P. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996.

[PH78] S. C. Pohlig and M. E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE-Transactions on Information Theory*, 24:106–110, 1978.

[Pol78] J. M. Pollard. Monte Carlo methods for index computation (mod p). *Mathematics of Computation*, 32(143):918–924, 1978.

[RS03] K. Rubin and A. Silverberg. Torus-based cryptography. In *CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Sciences*, pages 349–365. Springer, 2003.

[RS04a] K. Rubin and A. Silverberg. Algebraic tori in cryptography. In *High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, number 41 in Fields Institute Communications Series, pages 317–326. American Mathematical Society, Providence, RI, 2004.

[RS04b] K. Rubin and A. Silverberg. Using primitive subgroups to do more with fewer bits. In *Algorithmic Number Theory (ANTS VI)*, volume 3076 of *Lecture Notes in Computer Science*, pages 18–41. Springer, 2004.

[Sch64] I. J. Schoenberg. A note on the cyclotomic polynomial. *Mathematika*, 11:131–136, 1964.

[SJ96] P. Stevenhagen and H. W. Lenstra Jr. Chebotarev and his density theorem. *The Mathematical Intelligencer*, 18(2):26–37, 1996.

[SL93] P. J. Smith and M. J. J. Lennon. LUC: A new public key system. In *IFIP/Sec '93: Proceedings of the IFIP TC11, Ninth International Conference on Information Security*, pages 103–117. North-Holland, 1993.

[SL01] M. Stam and A. K. Lenstra. Speeding up xtr. In *ASIACRYPT 2001: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security*, pages 125–143. Springer, 2001.

[SL02] M. Stam and A. K. Lenstra. Efficient subgroup exponentiation in quadratic and sixth degree extensions. In *CHES*, pages 318–332, 2002.

[SS95] P. Smith and C. Skinner. A public-key cryptosystem and a digital signature based on the lucas function analogue to discrete logarithms. In J. Pieprzyk, editor, *Advances in Cryptology – ASIACRYPT 94*, volume 917 of *Lectures Notes in Computer Science*, pages 357–364. Springer-Verlag, 1995.

[Tes98] E. Teske. Speeding up Pollard's rho method for computing discrete logarithms. In *Algorithmic Number Theory Symposium ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, pages 541–554. Springer-Verlag, 1998.

[The03] N. Theriault. Index calculus attack for hyperelliptic curves of small genus. In *Advances in Cryptology – ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Computer Science*, pages 75–92. Springer, 2003.

[vDGP+05] M. van Dijk, R. Granger, D. Page, K. Rubin, A. Silverberg, M. Stam, and D. Woodruff. Practical cryptography in high dimensional tori. In *EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*. Springer, 2005.

[vDW04] M. van Dijk and D. Woodruff. Asymptotically optimal communication for torus-based cryptography. In *CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 157–178. Springer, 2004.

[Vos98] V. E. Voskresenskii. *Algebraic Groups and Their Birational Invariants*. Number 179 in Translations of Mathematical Monographs. American Mathematical Society, Providence, RI, 1998.

[Vos99] V. E. Voskresenskii. Stably rational algebraic tori. *Les XXèmes Journées Arithmétiques (Limoges, 1997), Journal de Théorie des Nombres de Bordeaux*, 11:263–268, 1999.

[Wei58] A. Weil. The field of definition of a variety. *American Journal of Mathematics*, 78:509–524, 1958.