IN SEARCH OF MATHEMATICAL PRIMITIVES FOR DERIVING UNIVERSAL PROJECTIVE HASH FAMILIES

MARÍA ISABEL GONZÁLEZ VASCO AND JORGE L. VILLAR

Abstract. We provide some guidelines for deriving new projective hash families of cryptographic interest. Our main building blocks are so called *group action systems*; we explore what properties of this mathematical primitives may lead to the construction of cryptographically useful projective hash families. We point out different directions towards new constructions, deviating from known proposals arising from Cramer and Shoup's seminal work.

1. Introduction and Outline

In [3], Cramer and Shoup presented a practical encryption scheme that could be proven IND-CCA secure in the standard model. Later, in [4, 5] the authors generalized that construction introducing a celebrated methodology for deriving IND-CCA schemes based on a new mathematical tool for cryptography: universal projective hash families. We start this contribution by recalling the basic notions and results related to this cryptographic primitive of increasing relevance (see Section 2). Also in [4, 5], so called *group systems* were introduced by Cramer and Shoup as atomic building blocks for projective hash families. Moreover, choosing the underlying group system wisely, one could actually prove the derived projective hash family to be cryptographically useful in a very strict sense.

We introduce a generalization of Cramer and Shoup´s group systems, called *group action systems* and prove that, similarly, simple properties of this building blocks guarantee the desired cryptographic robustness of the derived projective hash families. Section 3 is devoted to the introduction of this new primitive, as well as to pointing out which properties of the underlying group action systems are suited for cryptographic applications.

In search for specific constructions, in Section 4 we focus on a special type of group action systems, so called *automorphism group systems*, which

Date: July 12, 2005.

Key words and phrases. Projective Hash Families and Provable Security and Public Key Encryption.

are derived from the action of a certain subgroup of automorphisms on a given base group (these were recently defined in [14]). Section 5 roughly sketches some other types of action group systems of (potential) cryptographic relevance. Also, we note there that our work can actually be seen as a generalization of Cramer and Shoup´s original construction, for their celebrated abelian setting also yields concrete instances in our framework.

2. Some Preliminaries

2.1. **Cryptographically Useful Hash Families.** Families of hash functions have been widely used as essential building blocks of various cryptographic primitives. General hash functions are simply defined as mappings transforming n-bit strings into m-bit strings, which exist independently of any intractability assumption (See 3.5.1. of [7]). Together with one way permutations, general hash functions allow for the construction of pseudo-random generators. So called universal hash families were first defined in [6], as a tool for designing an algorithm for key storage and retrieval. The main feature of such families is, roughly speaking, a somehow strong collision resistance property. Later on, in 1989 [12], Naor and Yung introduced so called universal one way hash functions, which fulfill a kind of relaxed collision resistance property, which is referred to as *hardness to form designated collisions* or *target collision resistance* (see [8]). The existence of provable secure signature schemes can be derived from the existence of universal one way hash functions. Again, for a detailed discussion on the different definitions and application of these "classical" hash families, we refer the interested reader to [7, 8].

Whilst the above mentioned families are efficiently computable and essentially play the role of protecting the integrity of certain values, we will focus on a more recent type of hash families, which in addition have a special behaviour w.r.t. a certain subset of their domain. So called *universal projective hash families* were introduced by Cramer and Shoup [4, 5] as a valuable cryptographic primitive for deriving provable secure encryption schemes. We recall (informally) the basic definitions given in [5]:

Let X, Π be finite non-empty sets, and K some finite index set. Consider a family $H = \{H_k : X \longrightarrow \Pi\}_{k\in K}$ of mappings from X into Π, and let $\alpha : K \longrightarrow S$ be a map from K into some finite non-empty set S (which may be seen as a projection).

Definition 1. *Let H, K, X, Π, S, and α be as above. Then, for a given subset $L \subset X$, we refer to the tuple $\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$, as* projective hash family *(PHF) for (X, L) if for all $k \in K$ the restriction of H_k to*

L is determined by $\alpha(k)$, i. e., for all $x \in L$ and $k_1, k_2 \in K$ the equality $\alpha(k_1) = \alpha(k_2)$ implies $H_{k_1}(x) = H_{k_2}(x)$. Moreover, we say that $\mathbf{H}$ *is*

- ε-universal *if for any $x \in X \setminus L$ and for $k \in K$ (chosen uniformly at random), the probability of correctly guessing $H_k(x)$ from x and $\alpha(k)$ is at most ε.*
- ε-*universal*$_2$ *if for any $x, x^* \in X \setminus L$, $x \neq x^*$, for $k \in K$ chosen uniformly at random, the probability of correctly guessing $H_k(x)$ from $\alpha(k)$ and $H_k(x^*)$ is at most ε.*
- ε-smooth *if the probability distributions of $(x, s, H_k(x))$ and (x, s, π), where k, x and π are chosen uniformly at random in K, $X \setminus L$ and Π, respectively, and $s = \alpha(k)$, are ε-close.*[1]
- strongly universal$_2$ *if for $k \in K$ chosen uniformly at random, for any $x, x^* \in X \setminus L$, $x \neq x^*$ the random variables*
  : - *$\xi_k := H_k(x)$, conditioned to $\alpha(k)$*
  : - *η_k, the variable ξ_k conditioned to both $\alpha(k)$ and $H_k(x^*)$.*
  are statistically close to the uniform distribution over Π.[2]

Note that the concepts above limit the amount of information about the behaviour of a map H_k on $X \setminus L$, given by $\alpha(k)$. Clearly, for each case $\alpha(k)$ determines $H_k \mid_L$ completely. However, $\alpha(k)$ hardly gives any information about $H_k \mid_{X \setminus L}$ if the family is universal. If $\mathbf{H}$ is universal$_2$, not even knowing, besides the projection given by α, some information about the behaviour of H on a fixed (arbitrary) point of $X \setminus L$ will help on guessing its action on a new point $x \in X \setminus L$. Smoothness is achieved if, on average (taken over $k \in K$, $x \in X \setminus L$), guessing $H_k(x)$ given α is no better than a random guess. Strongly universal$_2$ is roughly speaking worst-case smoothness, i.e., fixing any $x \in X \setminus L$, $H_k(x)$ is (close to) a uniform random variable on Π, whose distribution is induced by choosing k uniformly at random. Moreover, this still holds if the behaviour of H on a given point of $X \setminus (L \cup \{x\})$ is known.

2.2. **Relations among Different Types of PHFs.** Clearly, Definition 1 results on a kind of hierarchy, as it is easy to see that strongly universal$_2$ PHSs are smooth, and similarly universal$_2$ PHFs are also universal. That is, roughly speaking, strongly universal$_2$ PHFs are the ones in which the projection gives less information about how $\{H_k\}_{k \in K}$ acts on $X \setminus L$, whereas given a PHF that can only be proven universal it may be the case that α leaks relevant information of what goes on outside L. However, there are

[1] A stronger notion of smoothness (which we will refer to as *worst case smoothness*) may be defined by imposing that, for any $x \in X \setminus L$ the distribution of $H_k(x)$ conditioned to s is ε-close to the uniform distribution over Π. This is actually achieved in most cases.

[2] This definition first appeared in [11].

efficient generic methods of 'upgrading' the weaker types of PHFs to achieve more robust constructions. More precisely:

- Cramer and Shoup gave a construction for turning any ε-universal PHF into ε-universal$_2$ (see Lemma 2 of [4]);
- applying the Leftover Hash Lemma [9], Cramer and Shoup also give a way to construct a smooth[3] PHF from a given ε-universal PHF, (Lemma 4 of [4]);
- given a concrete universal PHF, it is often possible to find a more efficient dedicated upgrading method than the ones mentioned above (see, for instance Section 7.3 of [4]);
- analogously as in Lemma 4 [4], ε-universal$_2$ PHFs can be transformed into strongly universal$_2$ PHFs, by a similar application of the Leftover Hash Lemma, since given $x, x^* \in X \setminus L, x \neq x^*$, $\alpha(k)$ and $H_k(x^*)$, the min-entropy of $H_k(x)$ is at least $\log_2 \frac{1}{\varepsilon}$.

2.3. **Cryptographic Applications of PHFs.** Projective hash families are essential building blocks in some recent proposals of encryption schemes that can be proven IND-CCA secure in the standard model. Not only Cramer and Shoup's generic design for such schemes has lead to the construction of practical instantiations [3, 4, 5], also recently Kurosawa and Desmedt [11] have proposed an efficient IND-CCA hybrid encryption scheme based on strongly universal$_2$ PHFs (see also [15]).

Also, a theoretical construction using non abelian groups as a base and inspired by that of Cramer and Shoup, has been presented in [14].

Roughly speaking, in the encryption scheme proposed by Cramer and Shoup [4, 5] a message $m \in \Pi$ is encrypted by using $H_k(x)$ as a one time pad; while the value of k is kept secret, x and $\alpha(k)$ are made public. Those holding k have access to a *private evaluation algorithm* allowing them to evaluate H_k on any $x \in X$, whereas those holding only the public key can only access a *public evaluation algorithm* that computes $H_k(x)$ only for $x \in L$. IND-CCA security is achieved by appending to the ciphertext a 'proof of integrity' obtained from a universal$_2$ HPS.

In [11], Kurosawa and Desmedt design a hybrid encryption scheme where the image $H_k(x)$ of a point $x \in L$ is used as input of a *key derivation function* supplying keys for both a symmetric encryption scheme and a *message authentication code*. Further applications of PHFs will surely appear in different areas of cryptography and some are actually already arising; for instance, recently Gennaro and Lindell [16] have proposed a general framework for password-based authenticated key exchange which makes use of

[3]Actually *worst case smoothness* is achieved.

smooth projective hash functions. Also, using smooth projective hash families with some additional properties Kalai designed a 2-out-of-1 *oblivious transfer* protocol that has been presented at Eurocrypt 2005 [10].

3. Group-Action Based PHF

In search of suitable projective hash families that could be used for their above mentioned scheme, Cramer and Shoup designed a construction method that took as a starting point certain atomic abelian group theoretic tools, defined as *group systems* [4, 5]. We now generalize their definition in order to capture cases in which no underlying group structure on X is assumed.

3.1. **Group Action Systems.** Let X be a finite set and consider a finite (not necessarily abelian) group H left-acting on X. Thus, each element $\phi \in H$ can be seen as an element of the symmetric group on X, and for all $\phi_1, \phi_2 \in H$ and $x \in X$, $(\phi_1\phi_2)x = \phi_1(\phi_2 x)$.

Take also S some finite group and $\chi : H \longrightarrow S$ a group homomorphism. Note that for any $\phi \in H$, $\chi(\phi)$ gives some (limited) information about ϕ, and thus χ provides partial information about the action of H on X. This partial information will eventually play the role of the information given by α in the PHFs we will be constructing.

Definition 2. *Let X, H, S and χ be defined as above. Then the tuple (X, H, χ, S) is called a* group action system.

Let us consider the action of $\ker\chi$ in X, defined by the action of H. For any $x \in X$, let us denote by $[x]$ the $(\ker\chi)$-orbit of x, i.e.,

$$[x] := \{\phi x \mid \phi \in \ker\chi\}.$$

Note that the action of H on the set of points that remain fixed by $\ker\chi$ is completely determined by χ. Let us thus define

$$L := \{x \in X \mid |[x]| = 1\},$$

that is $L := \{x \in X \mid [x] = \{x\}\}$.

Observe that $\ker\chi \subseteq \mathrm{Stab}(L)$ although they are not necessarily equal. Also, H leaves L invariant, as for any $\phi \in H$ and $x \in L$, ϕx is fixed by all $\psi \in \ker\chi$, as there exists $\rho \in \ker\chi$ s.t. $\psi\phi = \phi\rho$ and thus $\psi\phi x = \phi\rho x = \phi x$.

As our aim is to construct cryptographically useful PHFs, the systems above will be useful for us if χ gives little information about the action of H on $X \setminus L$; thus, we will be particularly interested in those systems for which the $(\ker\chi)$-orbits of elements in $X \setminus L$ are large.

Definition 3. *Let $p > 1$ be a positive integer. The group action system (X, H, χ, S) is* p-diverse *if $|[x]| \geq p$ for all $x \in X \setminus L$.*

Lemma 1. *Let (X, H, χ, S) be a group action system, and let p be the smallest prime dividing $|\ker \chi|$. Then (X, H, χ, S) is p-diverse.*

Proof. Note that $\ker \chi$ acts on X, and thus $|[x]|$ divides $|\ker \chi|$, so if $x \in X \backslash L$ (i.e., if $|[x]| \neq 1$) then $|[x]|$ is at least p. □

3.2. **Group Action PHFs.** As in [4, 5, 14], we outline the construction of a projective hash family from a group action system plus some additional elements:

Let us consider a group action system (X, H, χ, S), and denote by $\hbar : K \to H$ a bijection from a suitable index set K (which will later serve as the private key space). Noting that $\chi(\hbar(k))$ determines the action of $\hbar(k)$ on L completely, it is easy to see that the tuple $(H, K, X, L, X, S, \chi \circ \hbar)$ is a projective hash family.

Definition 4. *Any PHF constructed from a group action system as described above is called* group action projective hash family *(AcPHF). Such a projective hash family is made explicit by the tuple $(X, H, K, S, \chi, \hbar)$.*

It is our aim to prove that, if the group action projective hash family has certain nice properties, the resulting AcPHF will be ε-universal for some $\varepsilon > 0$. We start by demonstrating that for any $x \in X$, choosing $k \in K$ uniformly at random (that is, choosing uniformly at random a group element in H), given $\chi(\hbar(k))$, there are exactly $|[x]|$ equally probable candidates for $\hbar(k)x$.

Lemma 2. *Let (X, H, χ, S) be a group action system and let $x \in X$. If $\phi \in H$ is chosen uniformly at random, once $s = \chi(\phi)$ is given then ϕ is uniformly distributed on the coset $\chi^{-1}(s)$ and ϕx is uniformly distributed on the set $\{\psi x \,|\, \psi \in \chi^{-1}(s)\}$, that is, on a set of cardinality equal to $|[x]|$.*

Proof. Clearly, as ϕ is chosen uniformly at random, once we fix $s = \chi(\phi)$, the resulting distribution is uniform on $\chi^{-1}(s)$. Moreover, for any $x \in X$, ϕx is uniformly distributed on

$$\{\psi x \,|\, \psi \in \chi^{-1}(s)\}$$

provided that the sets

$$S_y = \{\psi \in \chi^{-1}(s) \mid \psi x = y\}$$

are of the same size for all $y \in \{\psi x, \psi \in \chi^{-1}(s)\}$. But this is straightforward to see, as all S_y are left cosets modulo $\ker \chi \cap \mathrm{Stab}(\{x\})$. □

Proposition 1. *Let $\mathbf{H} = (X, H, K, S, \chi, \hbar)$ be a group action projective hash family. If the underlying group action system (X, H, χ, S) is p-diverse then $\mathbf{H}$ is $1/p$-universal.*

Proof. From Lemma 2, for any $x \in X \setminus L$, the probability of guessing the right value of $\hbar(k)x$ for a random choice of $k \in K$ given $\chi(\hbar(k))$ is $1/|[x]|$, that is at most $1/p$. □

Once a universal projective hash family is constructed choosing the right elements according to the results above, the generic method of [5] may be used in order to transform it into a smooth projective hash family. Moreover, this transformation is sometimes superfluous: in some special cases, smoothness can even be guaranteed directly.

Proposition 2. *Let* $\mathbf{H} = (X, H, K, S, \chi, \hbar)$ *be a group action projective hash family. If the whole set* $X \setminus L$ *is a single orbit under the action of* $\ker \chi$ *then* $\mathbf{H}$ *is* $|L|/|X|$*-smooth.*

Proof. Let $x \in X \setminus L$. From Lemma 2, $\hbar(k)x$ is uniformly distributed on a set of size $|[x]| = |X \setminus L|$. Then, the statistical distance between $\hbar(k)x$ and the uniform distribution on X is

$$\frac{1}{2} \sum_{x \in X \setminus L} \left| \frac{1}{|X| - |L|} - \frac{1}{|X|} \right| + \frac{1}{2} \sum_{x \in L} \frac{1}{|X|} = \frac{|L|}{|X|},$$

thus the probability distribution of $\hbar(k)x$ is $|L|/|X|$-close to the uniform distribution on X □

Thus, from a universal PHF one can derive a smooth PHF. Similarly, a simple extension of a universal PHF leads to the construction of a universal$_2$ PHF.

3.3. **Universal$_2$ Extended AcPHFs.** In [5], the authors outline a generic transformation from any ε-universal projective hash family to an ε-universal$_2$ extended projective hash family. As done in [4, 5, 14] we give a more efficient extension for the case of AcPHFs.

Let $\mathbf{H} = (X, H, K, S, \chi, \hbar)$ be a group action projective hash family such that the underlying group action system (X, H, χ, S) is p-diverse. Let q be the smallest prime factor of $|H|$. Further on, denote by n a positive integer and by E a finite set. Let us define a new extended projective hash family $\hat{\mathbf{H}}$ by means of $n+1$ independent copies of $\mathbf{H}$ and a "gluing" function $g_\gamma^H : H^{n+1} \to H$ defined by:

$$g_\gamma^H(\phi_0, \ldots, \phi_n) := \phi_0 \phi_1^{\gamma_1} \cdots \phi_n^{\gamma_n}$$

where $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}^n$.

Similarly, we define $g_\gamma^S : S^{n+1} \to S$ by

$$g_\gamma^S(s_0, \ldots, s_n) := \chi(g_\gamma^H(\phi_0, \ldots, \phi_n)) = s_0 s_1^{\gamma_1} \cdots s_n^{\gamma_n},$$

where $\phi_j \in \chi^{-1}(s_j)$ for all $j = 0, \ldots, n$.

At this point, $\hat{K} = K^{n+1}$, $\hat{S} = S^{n+1}$ and the natural extensions $\hat{\chi}$ of χ and $\hat{\hbar}$ of $\hbar$ are considered. The set X is extended to $\hat{X} = X \times E$. Further on, given $\hat{k}$, we define $\Phi_{\hat{k}} : X \times E \longrightarrow X$ by

$$\Phi_{\hat{k}}(x, e) := g^H_{\Gamma(x,e)}(\hat{\hbar}(\hat{k}))x,$$

where $\Gamma : (x, e) \mapsto (\Gamma_1(x, e), \ldots, \Gamma_n(x, e))$ is an injective map from $X \times E$ into $\{0, \ldots, q-1\}^n$. Let us denote by $\hat{H}$ the set $\{\Phi_{\hat{k}} \,|\, \hat{k} \in \hat{K}\}$.

The soundness of our construction will rely on the commutativity of the following diagram:

$$\begin{array}{ccc} H^{n+1} & \xrightarrow{g^H_\gamma} & H \\ \downarrow{\scriptstyle \hat{\chi}} & & \downarrow{\scriptstyle \chi} \\ \hat{S} & \xrightarrow[g^S_\gamma]{} & S \end{array}$$

We will now proof that

$$\hat{\mathbf{H}} = (\hat{H}, \hat{K}, X \times E, L \times E, X, \hat{S}, \hat{\chi} \circ \hat{\hbar})$$

is a $1/p$-universal$_2$ projective hash family. Recall that this actually means that for any $x \in X \setminus L$ and $e \in E$ if $\hat{k} \in \hat{K}$ is chosen uniformly at random and $\hat{\chi}(\hat{\hbar}(\hat{k}))$, $\Phi_{\hat{k}}(x^*, e^*)$ are known (for some $x^* \in X \setminus (L \cup \{x\})$ and $e^* \in E$), the probability of guessing $\Phi_{\hat{k}}(x, e)$ correctly is at most $1/p$. Let us start by obtaining an analogue of Lemma 2.

Lemma 3. *Let $\hat{\mathbf{H}}$ be as above, $x \in X$ and $e \in E$. Then, if $\hat{\phi} \in H^{n+1}$ is chosen uniformly at random, once $\hat{s} = \hat{\chi}(\hat{\phi})$ is fixed, then $\phi = g^H_{\Gamma(x,e)}(\hat{\phi})$ is uniformly distributed on the coset $\chi^{-1}(s)$, where $s = g^S_{\Gamma(x,e)}(\hat{s})$. Moreover, ϕx is uniformly distributed on the set $\{\psi x \,|\, \psi \in \chi^{-1}(s)\}$, that is, on a set of cardinality equal to $|[x]|$.*

Proof. It is clear that in the conditional probability space, ϕ is uniformly distributed on the set $g^H_{\Gamma(x,e)}(\hat{\chi}^{-1}(\hat{s}))$. Let us show that this set is just the coset $\chi^{-1}(s)$. Clearly, $g^H_{\Gamma(x,e)}(\hat{\chi}^{-1}(\hat{s})) \subseteq \chi^{-1}(s)$ since

$$\chi(g^H_{\Gamma(x,e)}(\hat{\chi}^{-1}(\hat{s}))) = g^S_{\Gamma(x,e)}(\hat{\chi}^{-1}(\hat{\chi}(\hat{s}))) = s.$$

Conversely, $g^H_{\Gamma(x,e)}(\hat{\chi}^{-1}(\hat{s}))$ contains a whole coset modulo $\ker \chi$. To see this, pick an element $\psi \in g^H_{\Gamma(x,e)}(\hat{\chi}^{-1}(\hat{s}))$.

Then, there exists $\hat{\psi} = (\psi_0, \psi_1, \ldots, \psi_n) \in \hat{\chi}^{-1}(\hat{s})$ such that $\psi = g^H_{\Gamma(x,e)}(\hat{\psi})$. For each $\eta \in \ker \chi$, $\eta\psi = g^H_{\Gamma(x,e)}(\eta\psi_0, \psi_1, \ldots, \psi_n)$ is also in $\hat{\chi}^{-1}(\hat{s})$. From this point, the proof proceeds exactly as in Lemma 2. □

Proposition 3. *If (X, H, χ, S) is p-diverse then $\hat{\mathbf{H}}$ is a $1/p$-universal projective hash family.*

Proof. From Lemma 3, for any $x \in X \setminus L$ and $e \in E$, the probability of guessing the right value of $\Phi_{\hat{k}}(x, e) = g^H_{\Gamma(x,e)}(\hat{h}(\hat{k}))x$ for a random choice of $\hat{k} \in \hat{K}$ given $\hat{\chi}(\hat{h}(\hat{k}))$ is $1/|[x]|$, that is at most $1/p$. □

Next, we show that $\hat{\mathbf{H}}$ is also universal$_2$.

Lemma 4. *Let (X, H, χ, S) be a p-diverse AcPHF. For any $e, e^* \in E$, $x \in X \setminus L$ and $x^* \in X \setminus \{x\}$, if $\hat{\phi} \in H^{n+1}$ is chosen uniformly at random, once $\hat{s} = \hat{\chi}(\hat{\phi})$ is fixed, then the random variables $\phi = g^H_{\Gamma(x,e)}(\hat{\phi})$ and $\phi^* = g^H_{\Gamma(x^*,e^*)}(\hat{\phi})$ are independent.*

Proof. From Lemma 3, ϕ and ϕ^* are uniformly distributed on $\chi^{-1}(s)$ and $\chi^{-1}(s^*)$, respectively, where $s := g^S_{\Gamma(x,e)}(\hat{s})$ and $s^* := g^S_{\Gamma(x^*,e^*)}(\hat{s})$. Now let i be the smallest integer such that $\Gamma_i(x, e) \neq \Gamma_i(x^*, e^*)$, that surely exists since Γ is injective. Now, for any fixed values $\phi_j \in \chi^{-1}(s_j)$ for $j = 1, \ldots, i-1, i+1, \ldots, n$ let us consider the map

$$\begin{array}{rccc} \triangle_i : & \chi^{-1}(s_0) \times \chi^{-1}(s_i) & \longrightarrow & \chi^{-1}(s) \times \chi^{-1}(s^*) \\ & (\phi_0, \phi_i) & \longrightarrow & (\phi, \phi^*), \end{array}$$

where, as above, $\phi = g^H_{\Gamma(x,e)}(\hat{\phi})$ and $\phi^* = g^H_{\Gamma(x^*,e^*)}(\hat{\phi})$. By defining

$$\begin{array}{l} \psi_L = \phi_1^{\Gamma_1(x,e)} \cdots \phi_{i-1}^{\Gamma_{i-1}(x,e)} = \phi_1^{\Gamma_1(x^*,e^*)} \cdots \phi_{i-1}^{\Gamma_{i-1}(x^*,e^*)}, \\ \psi_R = \phi_{i+1}^{\Gamma_{i+1}(x,e)} \cdots \phi_n^{\Gamma_n(x,e)} \quad \text{and} \\ \psi_R^* = \phi_{i+1}^{\Gamma_{i+1}(x^*,e^*)} \cdots \phi_n^{\Gamma_n(x^*,e^*)} \end{array}$$

we can write

$$\triangle_i(\phi_0, \phi_i) = (\phi_0 \psi_L \phi_i^{\Gamma_i(x,e)} \psi_R, \phi_0 \psi_L \phi_i^{\Gamma_i(x^*,e^*)} \psi_R^*).$$

The map $\triangle_i$ is injective. Indeed, consider two pairs (ϕ_0, ϕ_i) and $(\bar{\phi}_0, \bar{\phi}_i)$ in $\chi^{-1}(s_0) \times \chi^{-1}(s_i)$ such that $\triangle_i(\phi_0, \phi_i) = \triangle_i(\bar{\phi}_0, \bar{\phi}_i)$. Then, $\phi_0 \psi_L \phi_i^{\Gamma_i(x,e)} = \bar{\phi}_0 \psi_L \bar{\phi}_i^{\Gamma_i(x,e)}$ and $\phi_0 \psi_L \phi_i^{\Gamma_i(x^*,e^*)} = \bar{\phi}_0 \psi_L \bar{\phi}_i^{\Gamma_i(x^*,e^*)}$. Combining these two equalities, we obtain

$$\phi_i^{\Gamma_i(x^*,e^*) - \Gamma_i(x,e)} = \bar{\phi}_i^{\Gamma_i(x^*,e^*) - \Gamma_i(x,e)},$$

that leads to $\phi_i = \bar{\phi}_i$ and then to $\phi_0 = \bar{\phi}_0$.[4] Thus, $\triangle_i$ is injective.

Then, as $\chi^{-1}(s_0) \times \chi^{-1}(s_i)$ and $\chi^{-1}(s) \times \chi^{-1}(s^*)$ have the same (finite) cardinality, $\triangle_i$ is a bijection. So, if (ϕ_0, ϕ_i) is chosen uniformly at random in

[4]Note that, as $|\Gamma_i(x^*, e^*) - \Gamma_i(x, e)| < q$, we have $\gcd(\Gamma_i(x^*, e^*) - \Gamma_i(x, e), |H|) = 1$. So there are $a, b \in \{0, \ldots, |H| - 1\}$ such that $a(\Gamma_i(x^*, e^*) - \Gamma_i(x, e)) = 1 + b|H|$, and, consequently, $\phi_i^{a(\Gamma_i(x^*,e^*) - \Gamma_i(x,e))} = \phi_i^{1+b|H|} = \phi_i$.

$\chi^{-1}(s_0) \times \chi^{-1}(s_i)$ then (ϕ, ϕ^*) is uniformly distributed on $\chi^{-1}(s) \times \chi^{-1}(s^*)$, for any choice of ϕ_j, $j = 1, \ldots, i-1, i+1, \ldots, n$. Then, the same occurs when the whole tuple $\hat{\phi}$ is chosen uniformly at random in $\hat{\chi}^{-1}(\hat{s})$. Consequently, ϕ and ϕ^* are independent uniformly distributed random variables. □

Proposition 4. *If (X, H, χ, S) is p-diverse then $\hat{\mathbf{H}}$ is a $1/p$-universal$_2$ projective hash family.*

Proof. The independence from Lemma 4 in particular implies that knowledge of $\Phi_{\hat{k}}(x^*, e^*) = \phi^* x^*$ does not affect the probability distribution of $\Phi_{\hat{k}}(x, e) = \phi x$. Thus, by Lemma 3, $\Phi_{\hat{k}}(x, e)$ is uniformly distributed on a set of size $|[x]|$. Then, $\hat{\mathbf{H}}$ is $1/p$-universal$_2$. □

Proposition 5. *If (X, H, χ, S) is p-diverse and then $\mathbf{H}$ is ε-smooth (worst-case), then, $\hat{\mathbf{H}}$ is strongly ε-universal$_2$ projective hash family.*

Proof. Clearly, by lemmas 3 and 4, $\Phi_{\hat{k}}(x, e)$ is uniformly distributed on a set of size $|[x]|$, independently of the value of $\Phi_{\hat{k}}(x^*, e^*)$. As $\mathbf{H}$ is ε-smooth then $\Phi_{\hat{k}}(x, e) = \phi x$ is ε-close the uniform distribution in X, for any choice of $x \in X \setminus L$ and $e \in E$. □

Recall that Cramer and Shoup's construction for an IND-CCA encryption scheme required a hard subset membership problem $\mathcal{M}$ and two suitable HPSs. From the above results it follows that these may be derived from suitable group action systems. Similarly, diverse group action systems provide strongly universal$_2$ projective hash families for the Kurosawa-Desmedt encryption scheme.

4. A Special Case: Automorphism Group PHFs

Let us suppose we consider a group action system consisting of a group X and a suitable subgroup $H \leq \mathrm{Aut}(X)$, together with a homomorphism $\chi : H \longmapsto S$, for a suitable group S. Note that, in this case, the set L defined in Section 3.1 is actually a group. Such group action systems are exactly the so called *automorphism group systems* defined in [14]. According to the corresponding terminology of [14], we will refer to the PHFs constructed from this special type of group action system as *automorphism projective hash families* (APHF). Even though it may seem plausible to look for p-diverse automorphism group systems leading to PHFs suitable for cryptographic applications, no concrete examples are, to the best of our knowledge, at hand. We will try to make a step further in this direction along this section.

Clearly, the natural starting point is a group X together with a special subgroup L which fulfills some special properties[5]. For the moment, let us keep in mind we aim at constructing a family of hash functions which will be easy to evaluate in L, provided some extra information (given by χ) that should however not help outside L. Thus, we may consider a projection χ so that L is stabilized by all elements of $\ker\chi$. Moreover, for achieving p-diversity we should aim at examples in which actually L is maximal with respect to this condition, that is, for any $K \subseteq X$, if $\ker\chi \subseteq \mathrm{Stab}_H(K)$, then $K \subseteq L$. It is easy to see that with these conditions, L must exactly be the subgroup defined as in 3.1, i.e. L is exactly the set of points with singleton $(\ker\chi)$-orbits.

Also, we would like that non-singleton $(\ker\chi)$-orbits are as large as possible. A naive way to do so is selecting a group X s.t. $|\operatorname{Aut}(X)|$ has only large prime divisors. Actually, many known results relating $|X|$ and $|\operatorname{Aut}(X)|$ could be used for that purpose, for instance:

- if a group X is complete[6], then $\operatorname{Aut}(X) \cong X$. Examples of complete groups are S_n $(n \neq 2, 6)$, automorphism groups of nonabelian simple groups, etc. (see, for instance, Chapter 7 of [13]).
- if S is a simple group with trivial outer automorphisms group, and π is the set of prime divisors of $|S|$ then $X = S \times \Pi_{p\in\pi} C_p$ satisfies $|\operatorname{Aut}(X)| = \phi(|X|)$, where ϕ is the Euler totient function ($\phi(n) = |\mathbb{Z}/n\mathbb{Z}^\times|$), see [2].

However, once the group X (and thus its order) is fixed, there are plenty of other factors influencing the soundness of this construction. Much research should be devoted in order to be able to provide concrete examples in this setting.

5. Examples

As we have already argued, it seems indeed hard to achieve new concrete constructions of PHFs making use of so called automorphism group systems. In the hope that the notion of *action group systems* introduced in this contribution may yield new ideas, we sketch some possible lines of future research. However, let us first see that at least our setting does not yield an empty theory, namely, that the known (abelian) constructions also fit our framework.

Known Constructions. Cramer and Shoup presented in [4] group theoretic constructions of universal projective hash families based on abelian groups. Their main building blocks are so called *group systems*;

[5]Recall, again the notion of *hard subset membership problem.*

[6]Centerless, and such that $\operatorname{Aut}(X) = \operatorname{Inn}(X)$.

Definition 5. *Let X, L and Π be finite abelian groups, where L is a proper subgroup of X and consider $\mathcal{H}$ a suitable subgroup of the homomorphism group between X and Π. Then the tuple $(\mathcal{H}, X, L, \Pi)$ is called a* group system.

Abelian group systems also yield natural examples of automorphism group projective hash families as defined in Section 4. Let us consider an abelian group system (H, X, L, Π).

Note that for any $h \in \mathrm{Hom}(X, \Pi)$ the mapping $\phi(x, \pi) := (x, h(x)\pi)$ is actually an element of $\mathrm{Aut}(X \times \Pi)$. Denote by Ψ the group monomorphism defined by:

$$\begin{array}{rccc} \Psi: & \mathrm{Hom}(X,\Pi) & \longrightarrow & \mathrm{Aut}(X\times\Pi) \\ & h & \longrightarrow & \phi \end{array}.$$

Now clearly, $(X \times \Pi, \Psi(H), \chi \circ \Psi^{-1}, S)$ is an automorphism group system from which a projective hash family can be derived as described in [14] (see also Section 4). Thus, all concrete constructions from [4, 5] yield examples in our new setting.

An Example Using Linear Groups. Let us consider the vector space $X = \mathbb{F}_q^n$, with q prime, and $\{\alpha_1, \ldots, \alpha_n\}$ a $\mathbb{F}_q$-basis of X. Consider H a subgroup of $GL(n, q)$, leaving a d-dimensional subspace L invariant. For a given $M \in GL(n, q)$, denote by M_d the matrix representing the linear transformation induced by M on L. Clearly,

$$\begin{array}{rccc} \chi: & H & \longrightarrow & GL(d,q) \\ & M & \longrightarrow & M_d, \end{array}$$

is a group homomorphism.

Now, diversity of the corresponding group action system$(X,H,\chi,GL(d,q))$ can be proven if H is chosen with care (ideally, $|H|$ should only have large prime divisors).

A Geometric Example. Let π be a finite projective plane over a prime finite field $\mathbb{F}_q$. Automorphisms of π are usually called *collineations*, it is easy to see that the action of a collineation is faithful both on the point-set and on the line-set of π. An *elation* is a collineation fixing both each point of a fixed line l (called the *axis*) and each line through a point C in l (C is usually referred to as the *center*). Recall that the fixed points of a non-identical elation are exactly the points on the axis, while the only fixed lines are those incident in the center. Let X be the point-set of π, L a fixed line in π and C a fixed point on L. Take H as the group consisting of all elations with center C. Notice that every elation in H induces a permutation of the points of L, since the center C is contained in L. For basic notions on collineation groups of finite planes, see [1].

Let us define χ as the group homomorphism translating each elation in H into the corresponding permutation of L.

$$\begin{array}{rccc} \chi: & H & \longrightarrow & S_L \\ & \zeta & \longrightarrow & \zeta_{|L}, \end{array}$$

Clearly, $\ker\chi$ is exactly the subgroup of all elations in H with axis L. Note that, moreover, the points in L are exactly the points of X stabilized by $\ker\chi$. On the other hand, if A is an arbitrary point outside L, each elation in $\ker\chi$ is uniquely determined by the image of A, that can be any point in the line defined by C and A, except for C (as an elation is completely determined giving its center, axis and the image of a point outside the axis). Hence, $|\ker\chi| = q$ and therefore q-diversity is guaranteed in this construction.

6. Concluding Remarks

We presented a general method for deriving cryptographically useful universal projective hash families based on group actions. Group action systems, our main building blocks, are inspired and also generalize so-called group systems introduced by Cramer-Shoup. We point out how simple properties of the underlying group action system translate into security qualities of the derived cryptographic construction. In addition, our arguments allow for the use of nonabelian groups and may shed some light into the design of group-based cryptographic tools with sound security guarantees.

Acknowledgements. The authors are indebted to Rainer Steinwandt for many interesting discussions, careful proof reading of an earlier version of this paper and several comments improving Section 5. Part of this research was done while the authors visited the *Centre de Recerca Matemàtica* on the occasion of the Research Program on Contemporary Cryptology (Spring 2005).

References

[1] Bonisoli, J.: On collineation groups of finite planes. Lecture notes from the course *Finite Geometries and Their Applications* Available at `http://www.maths.qmul.ac.uk/~pjc/design/notes.html` 1–27, (1999).

[2] Bray, J., Wilson, R. A.: On the orders of automorphism groups of finite groups. Bull. London Math. Soc., to appear.

[3] Cramer, R., Shoup, V.: A practical public key cryptosystem secure against adaptive chosen ciphertext attacks. Advances in Cryptology — CRYPTO'98 , **Vol. 1462** of *Lecture Notes in Computer Science*, 424–441. Springer, (1998).

[4] Cramer, R., Shoup, V.: Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. Cryptology ePrint Archive: Report 2001/085, (2001). Electronically available at `http://eprint.iacr.org/2001/085/`.

[5] Cramer, R., Shoup, V.: Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. Advances in Cryptology — EUROCRYPT 2002, **Vol. 2332** of *Lecture Notes in Computer Science*, 45–64. Springer, (2002).
[6] Carter, J., Wegman, W.:Universal Classes of Hash Functions. *Journal of Computer and System Sciences*, **Vol 18** 143–154, (1979).
[7] Goldreich, O.:Foundations of Cryptography, Vol. 1. Cambridge University Press, (2001).
[8] Goldreich, O.: Foundations of Cryptography, Vol. 2. *Cambridge University Press*,(2004).
[9] Impagliazo, R., Levin, L.A., Luby, A. Pseudorandom Generators from any One-Way Function. In *21st STOC, Proceedings*, 12–24. Springer, (1989).
[10] Kalai, Y.I.: Smooth Projective Hashing and Two-Message Oblivious Transfer. In *Advances in Cryptology. Proceedings of EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 78–95. Springer, (2005).
[11] Kurosawa, K., Desmedt, Y.: A New Paradim of Hybrid Encryption Scheme. *Advances in Cryptology. Proceedings of CRYPTO 2004*, **Vol. 3152** of *Lecture Notes in Computer Science*, 426–442. Springer, (2004).
[12] Naor, M., Yung, M.: Public-key Cryptosystems Provably Secure against Chosen Ciphertext Attacks. *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, 427–437. ACM Press, (1990).
[13] Rotman, J.J.: An Introduction to the Theory of Groups, 4rd Ed.. *Springer*, (1999).
[14] González Vasco, M.I., Martínez, C., Steinwandt, R., Villar, J.L.: A new Cramer-Shoup like methodology for group based provable secure encryption schemes. In *Proceedings of the Second Theory of Cryptography Conference TCC 2005*, **Vol. 3378** of *Lecture Notes in Computer Science*, 495–509. Springer, (2005).
[15] Gennaro, R., Lindell, Y.: A Framewok for Passord-Based Authenticated Key Exchange. Cryptology ePrint Archive: Report 2003/032, 2003. Electronically available at `http://eprint.iacr.org/2003/032/`.
[16] Gennaro, R., Shoup, V.: A Note on an Encryption Scheme of Kurosawa and Desmedt. Cryptology ePrint Archive: Report 2004/194, 2004. Electronically available at `http://eprint.iacr.org/2004/194/`.

María Isabel González Vasco, Área de Matemática Aplicada, Universidad Rey Juan Carlos, C/ Tulipán s/n. 28933, Móstoles, Madrid, Spain
E-mail address: `mariaisabel.vasco@urjc.es`

Jorge L. Villar, Departamento de Matemática Aplicada IV, Univ. Politécnica de Catalunya, Campus Nord, c/Jordi Girona, 1–3, 08034 Barcelona, Spain
E-mail address: `jvillar@ma4.upc.edu`