The security of an RSA-based cut-and-choose protocol

THE SECURITY OF AN RSA-BASED CUT-AND-CHOOSE PROTOCOL

THIJS VEUGEN

EIDMA report series
EIDMA-RS.95.01

CIP-DATA KONINKLIJKE BIBLIOTHEEK, DEN HAAG

Veugen, Thijs

The security of an RSA-based cut-and-choose protocol /
Thijs Veugen. - Eindhoven : Euler Institute of Discrete
Mathematics and its Applications, Eindhoven University of
Technology
With ref.
ISBN 90-75332-02-5
NUGI 811/832
Subject headings: cryptography.

The Security of an RSA-based Cut-and-choose Protocol

Thijs Veugen *

December 21, 1995

Abstract

We investigate the security of an RSA-based cut-and-choose protocol (see Figure 1) that is used in untraceable electronic cash systems (e.g. [3, 8, 9, 10]) and credential systems (e.g. [2]). It is a protocol between a user and the signature authorithy. Only the latter is able to compute RSA-signatures. The protocol enables the user to obtain a special RSA-signature that represents money (in case of an electronic cash system) or a credential (in case of a credential mechanism). We describe all possibilities of cheating by a single user that participates in the protocol once, and prove under certain assumptions that there are no other cheating strategies in that case.

Key words RSA, RSA-scheme, RSA-signature, Payment system, Credential mechanism, Cryptographic protocol.

1 Introduction

Several complicated cryptographic protocols use as a building block simple signature protocols in which only one party, called the signature authority, can create signatures and issue them to the other parties, called the individuals. Some of these protocols are based on the cut-and-choose principle to protect the privacy of the user. They are used, for instance, in payment systems (e.g., [3, 8, 9, 10]) and credential systems (e.g., [2]) in which a signature represents money or a credential. In this paper we take as an example the withdrawal protocol of the coin system of [3]. An abstracted version of this protocol is depicted in Figure 1. The abstraction mainly is due to the user's choice of the numbers a_i that actually are the results of complicated computations involving one-way functions. Also the blinding factors are eliminated. In the coin system the signature authority is the bank and the individuals are the users of the payment system. Due to the cut-and-choose principle it is possible for a user to cheat during the protocol without getting caught by

*Group on Information and Communication Theory, Department of Electrical Engineering, Eindhoven University of Technology, PO Box 513, 5600 MB Eindhoven, The Netherlands; email P.J.M.Veugen@ele.tue.nl. The research was done at the Centre for Mathematics and Computer Science, Amsterdam, The Netherlands.

User	Bank
Choose k different numbers $a_i (1 \leq i \leq k)$ that contain ID	
Compute $f_i = F(a_i)(1 \leq i \leq k)$	
Send $f_i (1 \leq i \leq k)$ to the bank	
	Choose randomly set $R \subset \{1, \ldots, k\}$
	Send R to the user
Send $a_i (i \in R)$ to the bank	
	Check "a_i contains user's ID?" $(i \in R)$
	Check $a_i \neq a_j (i, j \in R, i \neq j)$
	Check $f_i = F(a_i)(i \in R)$
	Compute $g \equiv \prod_{i \notin R} f_i \pmod{n}$
	Send g^d to the user

Figure 1: The withdrawal protocol of the coin system in [3].

the bank (with nonnegligeable probability). The security of the system depends on the kind of signatures a cheating user could obtain. This is investigated in this paper.

Consider the following situation: Let n be an RSA-modulus [11], e and d integers such that $e \cdot d \equiv 1 \pmod{\varphi(n)}$ and C a set of numbers coprime with n. The numbers e and n are public. The number d and the factorization of n are only known by the signature authorithy. The elements of C are images of a one-way function F. The sentence "Choose an element a from the domain of F and compute the image $x = F(a)$" is for convenience abbreviated to "Let $x \in C$". Similarly with subsets of C.

We investigate the following problem:

Let $l \geq 1$. Let X_i and Y_i be subsets of C $(i = 1, \ldots, l)$.
Is it feasible to compute, without knowing the factorization of n,
a number z coprime with n such that for each $1 \leq i \leq l$ it is feasible
to compute the e^{th} root of $\prod_{y \in Y_i} y$ from
the e^{th} root of $z \cdot \prod_{x \in X_i} x$ modulo n?

The goal is to characterize, for each $l \geq 1$, the relation between the X_i and Y_i $(1 \leq i \leq l)$, such that it is feasible to compute such a number z. For instance for $l = 1$ the number $z \equiv (\prod_{y \in Y_1} y) \cdot (\prod_{x \in X_1} x)^{-1} \pmod{n}$ can be computed satisfying $(z \cdot \prod_{x \in X_1} x)^d \equiv (\prod_{y \in Y_1} y)^d \pmod{n}$. Hence it is more interesting to look at cases where $l > 1$.

Evertse and van Heyst [5] considered a related problem. They show that computing an RSA-signature of a particular type, from given RSA-signatures of other types, is polynomial time reducible to computing RSA-roots $x^{1/d}$ for random x and some positive integer d. The main reason that these results can not be applied here is that they deal with uniformly chosen numbers and not with numbers manipulatable by the individual. In a follow-up paper [6] they consider a specific interactive protocol and discuss the computability of

some RSA signatures, but the lacking of the cut-and-choose property makes their results unsuitable for our problem.

The second section shows how our main problem relates to cheating strategies. The third section contains the statements of the theorems, followed by their proofs. In the final section some open problems are mentioned.

2 Cheating strategies

In this section it is shown how the results of Section 3 can be applied to the withdrawal protocol of the coin system in [3] (see Figure 1). This is a protocol between a user and the bank based on the RSA-system, where only the bank knows the factorization of the used RSA-modulus n. In this protocol, F is a one-way function, k is an even security parameter and ID is the user's identification number. If one of the verifications performed by the bank fails, the protocol is aborted. In the electronic payment system the number g^d will have a value of, say, one dollar. Each time the user executes the withdrawal protocol with the bank, one dollar is withdrawn from the user's bank account. If the withdrawal protocol is executed correctly, the user obtains a one-dollar-coin (the number g^d). This coin can be used to spend one dollar at a shop. The numbers a_i should contain the identity of the user so if the coin is spent more than once, the identity of the user is revealed with high probability. We call g^d a valid coin if g is the product of $k/2$ images under F which do not need to contain the valid ID. Only valid coins can be spent at a shop. Suppose the user obtains a valid coin of which exactly v $(0 \leq v \leq k/2)$ images contain the correct ID, then the probability that the user can spend this coin at least $t+1$ $(t \geq 0)$ times without getting caught is 2^{-vt} [3]. It is therefore important for the bank to know what kind of valid coins a (cheating) user could obtain from executing the withdrawal protocol.

An honest user chooses k different numbers $a_i (1 \leq i \leq k)$ that contain the user's identification number and computes $f_i = F(a_i) (1 \leq i \leq k)$. Since F is a one-way function it is assumed that $f_i \neq f_j$ for $1 \leq i \neq j \leq k$. A cheating user chooses for at least one f_j $(j \in \{1, \ldots, k\})$ some number $z \in \{1, \ldots, n\}$ instead of $f_j = F(a_j)$ with a_j containing the correct ID. Such a cheating user is caught by the bank if the bank chooses R such that $j \in R$. Since the cardinality of R is equal to $k/2$ in [3], the probability that a cheating user is caught is $\frac{1}{2}$. It is assumed w.l.o.g. that the user forms exactly one f_j $(j \in \{1, \ldots, k\})$ not correctly. To see that nothing is gained by forming two of them, consider user A who cheats by forming f_1 and f_2 incorrectly. Say user A provides the bank with $f_i^a (1 \leq i \leq k)$, where $f_1^a = \mathrm{BAD}_1$, and $f_2^a = \mathrm{BAD}_2$. Now consider a more clever user B who cheats by only forming f_1 incorrectly. User B chooses $f_i^b = f_i^a$, for $3 \leq i \leq k$. User B also chooses f_2^b correctly, and computes $f_1^b \equiv \mathrm{BAD}_1 \cdot \mathrm{BAD}_2 / f_2^b \pmod{n}$. Comparing user A with user B, we see that if both users are not caught, they will obtain exactly the same root. On the other hand, user A is more likely to be caught than user B. However, it is generally true that if only user A is caught (and user B not), then user B does not obtain a valid coin.

We show that the kind of valid coins a cheating user could obtain from executing the withdrawal protocol is determined by the results of Section 3. Suppose, a cheating user participates in the withdrawal protocol and is not caught by the bank. For example,

take $k = 4$, and assume the user chose f_2, f_3, and f_4 correctly, but $f_1 = z$ for some $z \in \{1, \ldots, n\}$. The signature obtained by the user will depend on the bank's choice of R. E.g. if $R = \{2, 3\}$, the user obtains $(z \cdot f_4)^d$. From the received signature the user will try to compute a valid coin. A possible cheating strategy could be: try to compute $(b \cdot f_4)^d$ if the bank choses $R = \{2, 3\}$, $(b \cdot f_3)^d$ if $R = \{2, 4\}$ is chosen, and $(b \cdot f_2)^d$ if the bank's choice is $R = \{3, 4\}$, where b is some incorrectly formed image under F. This is of course a feasible cheating strategy, since the user can choose $z = b$. Another cheating strategy could be: try to compute $(b_1 \cdot b_2)^d$ if $R = \{2, 3\}$ is chosen by the bank, where b_1 and b_2 are incorrectly formed images under F, and not obtain a valid coin if the bank chose either $R = \{2, 4\}$ or $R = \{3, 4\}$. This is also a feasible cheating strategy since the user can choose $z \equiv b_1 \cdot b_2 / f_4 \pmod{n}$. Using the latter strategy, the user obtains a completely false coin with probability $\frac{1}{6}$ but is caught during the withdrawal protocol with probability $\frac{1}{2}$. The formal description of our main problem from the first Section coincides with the problem of deciding which cheating strategies are feasible and which are not. Take for example the above described second cheating strategy. Let $R_1 = \{2, 3\}$, $R_2 = \{2, 4\}$, and $R_3 = \{3, 4\}$ be the possible choices for the bank. Then $X_1 = \{f_4\}$, $X_2 = \{f_3\}$, and $X_3 = \{f_2\}$ correspond with the signatures $(z \cdot \prod_{x \in X_i} x)^d$ the user could obtain. The valid coins the user would like to compute from these are described by $Y_1 = \{b_1, b_2\}$, $Y_2 = \emptyset$, and $Y_3 = \emptyset$ i.e. no valid coins if the bank chooses R_2 or R_3. It would be interesting to know whether, for example, it is feasible for the user to obtain a completely false coin if the bank happens to choose R_1, and simultaneously some valid coin if the bank choses R_2, but no valid coin if R_3 is chosen. From THEOREM 2 of Section 3 it follows that this cheating strategy with $Y_1 = \{b_1, b_2\}$, $Y_2 = \{b_1, f_3\}$ (for example), and $Y_3 = \emptyset$, is infeasible. To see this, first observe that we can assume w.l.o.g. that the sets Y_i are non-empty. Secondly, following the terminology of THEOREM 2, $U = X_1 \cup X_2 = \{f_3, f_4\}$, $I = X_1 \cap X_2 = \emptyset$, and $Y = Y_1 \cap Y_2 = \{b_1\}$. So, according to THEOREM 2, the only feasible choices for Y_1 and Y_2 with this intersection are ($Y_1 = \{f_3, b_1\}$ and $Y_2 = \{f_4, b_1\}$) or ($Y_1 = \{f_4, b_1\}$ and $Y_2 = \{f_3, b_1\}$).

It is also interesting to know whether a user is able to obtain more than one valid coin for some choice R. This possibility is excluded by Lemma 8.

In general, the best feasible cheating strategies for the user are to try to obtain a valid coin with exactly v ($0 \leq v < k/2$) correctly formed numbers. Then the user should choose $k-1$ correctly formed numbers $f_2 \ldots f_k$, $k/2-v$ numbers $b_1 \ldots b_{k/2-v}$ not containing the user's ID, and compute $f_1 \equiv (b_1 \cdot \ldots b_{k/2-v})/(f_2 \cdot \ldots f_{k/2-v}) \pmod{n}$. This strategy succeeds if the bank choses R such that $R \subseteq \{k/2 - v + 1, \ldots, k\}$ which occurs with probability equal to $\frac{(k/2)! \cdot (k/2+v)!}{k! \cdot v!}$. For all these strategies, the user is caught during the protocol with probability $\frac{1}{2}$. Since the probability that a coin with v correctly formed numbers can be spent at least $t+1$ ($t \geq 0$) times without getting caught is equal to 2^{-vt}, the optimal strategy is to try to obtain a completely false coin, since other coins are not likely to be spent more than once.

3 Statements of the theorems

First some notation and terminology is introduced.

n	the RSA-modulus [11]
$\mathbb{Z}_n^*$	the set $\{x \mid 1 \leq x \leq n, \gcd(x,n) = 1\}$
C	a subset of $\mathbb{Z}_n^*$ consisting of the images of a one-way function F
$\varphi(n)$	Euler's Totient function: $\varphi(n) = \lvert\mathbb{Z}_n^*\rvert$
e	a public integer coprime with $\varphi(n)$
d	the multiplicative inverse of e modulo $\varphi(n)$: $e \cdot d \equiv 1 \pmod{\varphi(n)}$
x^d	the e^{th} RSA-root of x modulo n [11]: the unique number y modulo n such that $y^e \equiv x \pmod{n}$.
$\underline{X}$	the product of the elements of the set X modulo n
X^l	the sequence $X_1 X_2 \ldots X_l$
$\mathrm{RC}(X^l, Y^l)$	a predicate that has the value true if and only if it is feasible to compute a number $z \in \mathbb{Z}_n^*$ such that for each $i \in \{1, \ldots, l\}$, it is feasible to compute $(\underline{Y_i})^d$ from $(z \cdot \underline{X_i})^d$ modulo n, without knowing the factorization of n. The predicate is defined for $X_i (1 \leq i \leq l)$, and $Y_i (1 \leq i \leq l)$ subsets of C.
$\cup$	the union of sets
$\cap$	the intersection of sets
$\subseteq$	subset
$\setminus$	setminus
$+$	the union of disjunct sets
$\emptyset$	the empty set
$\div$	the symmetrical difference of sets defined as $A \div B = (A \setminus B) \cup (B \setminus A)$
not subset-related	the sets S_1 to S_k are not subset-related if there are no two sets S_i and S_j $(i, j \in \{1, \ldots, k\}, i \neq j)$ such that $S_i \subseteq S_j$.
$\forall$	for all

In this paper the following three assumptions are made (their interpretation follows below):

1. **Prime assumption:** The integer e is a fixed prime, at least 5.

2. **Rootcomputability assumption:** Let $x, y \in \mathbb{Z}_n^*$. If it is feasible to compute x^d from y^d modulo n, then it is feasible to compute a number $r \in \{0, \ldots, e-1\}$ and a number $s \in \mathbb{Z}_n^*$ such that $x \equiv y^r s^e \pmod{n}$.

3. **Rootinfeasibility assumption:** Let $k \geq 1$ and let x_1 to x_k be k different elements of C. Then it is infeasible to compute numbers $r_1, \ldots, r_k \in \{0, \ldots, e-1\}$ not all zero, and a number $s \in \mathbb{Z}_n^*$ such that $\prod_{i=1,\ldots,k} x_i^{r_i} \equiv s^e \pmod{n}$.

The rootcomputability assumption means that if an RSA-root is computable from another RSA-root, this computation can be done using only multiplications, divisions and exponentiations. It seems natural to analyse RSA-based protocols by considering attacks based only on the multiplicative property of RSA since as yet it is not clear if there is any other structure in the RSA-scheme which could be useful in cheating in the protocol. In any case, as the complexity theoretic problem of reducing everything to the intractability of RSA seems difficult, it makes sense to simplify this problem by making some stronger assumption. The rootinfeasibility assumption means that it is infeasible to compute e^{th} roots on (non-trivial) products of elements of C. The essential restriction on the $r_1, \ldots, r_k$ is that at least one is not zero. Realizing that the numbers in the set C are images of a one-way function makes this assumption reasonable. Note that the rootinfeasibility assumption implies that it is not feasible to find numbers $a_0, \ldots, a_k$ such that $x_0 \equiv x_1 \cdots x_k \pmod{n}$, where $x_i = F(a_i)$ $(0 \leq i \leq k)$. The reason is that otherwise $x_0^{e-1} x_1 \cdots x_k \equiv x_0^e \pmod{n}$. These three assumptions are used throughout the entire paper. The problem that is analysed is:

Let $l \geq 2$. Let $X_i (1 \leq i \leq l)$ be subsets of C that are not subset-related.
Let $Y_i (1 \leq i \leq l)$ be non-empty subsets of C.
Is $\mathrm{RC}(X^l, Y^l)$ true?

The answer to this problem is given by three theorems. Note that only THEOREM 2 is important when applying the results to the withdrawal protocol of the coin system in [3] because the cardinality of R is fixed in this system. There might be other applications where the cardinality of R is not fixed. For these systems and for mathematical completeness we also state THEOREM 1 and THEOREM 3.

From THEOREM 1 it follows that if such a number z is computable, the $Y_i (1 \leq i \leq l)$ are related in only two possible ways. The first possibility is that the $Y_i (1 \leq i \leq l)$ are not subset-related. This is treated in THEOREM 2. The second possibility is that one $Y_j (j \in \{1, \ldots, l\})$ is subset of all the other $Y_i (1 \leq i \leq l, i \neq j)$ and these other $Y_i (1 \leq i \leq l, i \neq j)$ are not subset-related. This second possibility is treated in THEOREM 3 (w.l.o.g. $j = 1$).

THEOREM 1 *Let $l \geq 2$. Let $X_i (1 \leq i \leq l)$ be subsets of C that are not subset-related. Let $Y_i (1 \leq i \leq l)$ be non-empty subsets of C. If $RC(X^l, Y^l)$, then*

1. *the sets Y_1 to Y_l are not subset-related or*
2. *there is a $j \in \{1, \ldots, l\}$ such that the Y_i for $i \neq j$ are not subset-related and $Y_j \subseteq Y_i$ for every i.*

THEOREM 2 *Let $l \geq 2$. Let $X_i (1 \leq i \leq l)$ be subsets of C that are not subset-related. Let $Y_i (1 \leq i \leq l)$ be subsets of C that are not subset-related. Define $U := \bigcup_{i=1,\ldots,l} X_i$, $I := \bigcap_{i=1,\ldots,l} X_i$ and $Y := \bigcap_{i=1,\ldots,l} Y_i$. Then*

$$RC(X^l, Y^l)$$
if and only if
$$\forall_{1 \leq i \leq l} [Y_i = (U \setminus X_i) + Y] \text{ or } \forall_{1 \leq i \leq l} [Y_i = (X_i \setminus I) + Y].$$

From the + operators in Theorem 2 it follows implicitly that if such a number z can be computed, we have $\forall_{1\leq i\leq l}[(U \setminus X_i) \cap Y = \emptyset]$ or $\forall_{1\leq i\leq l}[(X_i \setminus I) \cap Y = \emptyset]$ which are both equivalent to $Y \cap U \subseteq I$.

THEOREM 3 *Let $l \geq 2$. Let $X_i (1 \leq i \leq l)$ be subsets of C that are not subset-related. Let $Y_i (2 \leq i \leq l)$ be subsets of C that are not subset-related. Let Y_1 be a non-empty subset of C such that $Y_1 \subseteq Y_i (1 \leq i \leq l)$. Define $U := \bigcup_{i=2,\ldots,l} X_i$, $I := \bigcap_{i=2,\ldots,l} X_i$ and $Y := \bigcap_{i=2,\ldots,l} Y_i$. Then*

$$RC(X^l, Y^l)$$
if and only if
$$(\forall_{2\leq i\leq l}[Y_i = (U \setminus X_i) + Y] \text{ and } Y = (X_1 \div U) \text{ and } Y_1 = (U \setminus X_1))$$
or
$$(\forall_{2\leq i\leq l}[Y_i = (X_i \setminus I) + Y] \text{ and } Y = (X_1 \div I) \text{ and } Y_1 = (X_1 \setminus I)).$$

Similarly as in Theorem 2, it follows implicitly from the + operators in Theorem 3 that if such a number z can be computed, $Y \cap U \subseteq I$. The extra restriction on the set Y ($Y = (X_1 \div U)$ or $Y = (X_1 \div I)$) reduces this assertion to $U \subseteq X_1 \cup I$ respectively $X_1 \cap U \subseteq I$.

4 Proofs

We need some lemmas to prove the main results. The first lemma, which follows also from results of Evertse and van Heyst [5], shows that coprime exponents in roots can be 'removed'. This result was, among others, also found by Amos Fiat [7].

Lemma 4 *Let $x \in \mathbb{Z}_n^*$ and $a \in \mathbb{Z}_e^*$. Then it is feasible to compute x^d from $(x^a)^d$ modulo n without knowing the factorization of n.*

Proof. Since $\gcd(a, e) = 1$, one can compute (using Euclid's algorithm [4]) $\overline{a} \in \{0, \ldots, e-1\}$ and $\overline{e} \in \{-a, \ldots, 0\}$ such that $a \cdot \overline{a} + e \cdot \overline{e} = 1$. Then $x^d \equiv (x^{a \cdot d})^{\overline{a}} x^{\overline{e}} \pmod{n}$ thus x^d can be computed from $(x^a)^d$ by raising $(x^a)^d$ to the power $\overline{a}$ and multiplying the result with $x^{\overline{e}}$.
(End of Proof)

Lemma 5 shows that sometimes the rootcomputation can be reversed.

Lemma 5 *Let $x \in \mathbb{Z}_n^*$. Let Y be a non-empty subset of C. If it is feasible to compute $(\underline{Y})^d$ from x^d modulo n, then it is feasible to compute x^d from $(\underline{Y})^d$ modulo n.*

Proof. Suppose that it is feasible to compute $(\underline{Y})^d$ from x^d modulo n. According to the rootcomputability assumption $r \in \{0, \ldots, e-1\}$, and $s \in \mathbb{Z}_n^*$ can be computed such that $\underline{Y} \equiv x^r s^e \pmod{n}$. If $r \equiv 0 \pmod{e}$ the e^{th} root of $\underline{Y}$ can be computed, which is in contradiction with the rootinfeasibility assumption. Therefore $\gcd(r, e) = 1$, due to the prime assumption. This means that integers $\overline{r}$ and $\overline{e}$ can be computed such that

$r \cdot \overline{r} + e \cdot \overline{e} = 1$ with the algorithm of Euclid [4]. Thus x^d is computable from $(\underline{Y})^d$, because $x^d \equiv (\underline{Y}^d)^{\overline{r}} x^{\overline{e}} / s^{\overline{r}e} \pmod{n}$.
(End of Proof)

Lemma 6 is a consequence of the root infeasibility assumption. It is an important lemma for the proof of Theorem 7.

Lemma 6 *Let $X_1, X_2, Y_1, Y_2 \subseteq C, a, b \in \mathbb{Z}_e^*$. Suppose that $X_1, X_2 \neq \emptyset, X_1 \cap X_2 = Y_1 \cap Y_2 = \emptyset$. If it is feasible to compute $(\underline{X_1} \cdot \underline{X_2}^{-1} \cdot \underline{Y_1}^a \cdot \underline{Y_2}^b)^d$ modulo n, then $\{X_1, X_2\} = \{Y_1, Y_2\}$.*

Proof. Suppose it is feasible to compute an integer $s \in \mathbb{Z}_n^*$ such that $\underline{X_1} \cdot \underline{X_2}^{-1} \cdot \underline{Y_1}^a \cdot \underline{Y_2}^b \equiv s^e \pmod{n}$. Due to the rootinfeasibility assumption the left side of this equation must somehow reduce to a trivial product. Therefore from $X_1 \cap X_2 = \emptyset$ can be concluded that $(X_1 \cup X_2) \subseteq (Y_1 \cup Y_2)$. E.g. suppose that there is an $x \in X_1$ such that $x \notin Y_1 \cup Y_2$, then $\underline{X_1} \cdot \underline{X_2}^{-1} \cdot \underline{Y_1}^a \cdot \underline{Y_2}^b$ can be written as $x \cdot \prod_{y \in X_1 \cup X_2 \cup Y_1 \cup Y_2, y \neq x} y^{r_y}$ for some numbers r_y which contradicts the rootinfeasibility-assumption. Similarly from $Y_1 \cap Y_2 = \emptyset$, and $a, b \in \mathbb{Z}_e^*$ can be concluded that $(Y_1 \cup Y_2) \subseteq (X_1 \cup X_2)$. If $Y_1 \cap X_1 \neq \emptyset$ and $Y_1 \cap X_2 \neq \emptyset$ one obtains, using again the rootinfeasibility assumption, $a + 1 \equiv a - 1 \equiv 0 \pmod{e}$ so $2 \equiv 0 \pmod{e}$ which is a contradiction. For reasons of symmetry ($Y_1 \subseteq X_2$ or $Y_1 \subseteq X_1$) and ($Y_2 \subseteq X_2$ or $Y_2 \subseteq X_1$). Thus $\{X_1, X_2\} = \{Y_1, Y_2\}$ since X_1 and X_2 are not empty.
(End of Proof)

The case $l = 2$ is solved in the following theorem.

Theorem 7 *Let X_1 and X_2 be subsets of C that are not subset-related. Let Y_1 and Y_2 be non-empty subsets of C. Then RC(X^2, Y^2) if and only if $\{Y_1, Y_2\} = \{X_1 \div X_2, X_1 \setminus X_2\}$ or $\{Y_1, Y_2\} = \{X_1 \div X_2, X_2 \setminus X_1\}$ or $\{Y_1 \setminus Y_2, Y_2 \setminus Y_1\} = \{X_1 \setminus X_2, X_2 \setminus X_1\}$.*

Proof. Define $\alpha_1 := X_1 \setminus X_2, \alpha_2 := X_2 \setminus X_1, \beta_1 := Y_1 \setminus Y_2, \beta_2 := Y_2 \setminus Y_1$ and $Y := Y_1 \cap Y_2$. First the "only if" part is proved. Suppose RC(X^2, Y^2) holds. According to the definition of RC, Lemma 5, and the rootcomputability assumption, numbers $z \in \mathbb{Z}_n^*$, $r_1, r_2 \in \{0, \ldots, e-1\}$, and $s_1, s_2 \in \mathbb{Z}_n^*$ are computed such that $z \cdot \underline{X_1} \equiv \underline{Y_1}^{r_1} \cdot s_1^e \pmod{n}$, and $z \cdot \underline{X_2} \equiv \underline{Y_2}^{r_2} \cdot s_2^e \pmod{n}$. From these two equalities the number $s \equiv s_1 \setminus s_2 \pmod{n}$ can be computed that satisfies $s^e \equiv \underline{X_1} \cdot \underline{X_2}^{-1} \cdot \underline{Y_1}^{-r_1} \cdot \underline{Y_2}^{r_2} \equiv \underline{\alpha_1} \cdot \underline{\alpha_2}^{-1} \cdot \underline{\beta_1}^{-r_1} \cdot \underline{\beta_2}^{r_2} \cdot \underline{Y}^{r_2 - r_1} \pmod{n}$. If $r_1 = 0$ the relation $z \cdot \underline{X_1} \equiv s_1^e \pmod{n}$ holds. This contradicts the rootinfeasibility assumption because RC(X^2, Y^2) implied that $(\underline{Y_1})^d$ can be computed from $(z \cdot \underline{X_1})^d$. The conclusion is that $r_1 \in \mathbb{Z}_e^*$, and for reasons of symmetry $r_2 \in \mathbb{Z}_e^*$. Two cases are considered:

1. If $r_1 = r_2$ the relation $s^e \equiv \underline{\alpha_1} \cdot \underline{\alpha_2}^{-1} \cdot \underline{\beta_1}^{-r_1} \cdot \underline{\beta_2}^{r_2}$ holds so $\{\alpha_1, \alpha_2\} = \{\beta_1, \beta_2\}$ by Lemma 6.

2. If $r_1 \neq r_2$ the numbers $r_2 - r_1$ and e are coprime. Applying the rootinfeasibility assumption provides $Y \subseteq \alpha_1 \cup \alpha_2$ and ($r_1 - r_2 \equiv \pm 1 \pmod{e}$ or $Y = \emptyset$). Similarly it follows that ($r_2 \equiv \pm 1 \pmod{e}$ or $\beta_2 = \emptyset$) and ($r_1 \equiv \pm 1 \pmod{e}$ or $\beta_1 = \emptyset$). If

β_1, β_2 and Y are not empty one obtains $r_1 \equiv \pm 1 \pmod{e}$, $r_2 \equiv \pm 1 \pmod{e}$ and $r_1 - r_2 \equiv \pm 1 \pmod{e}$ which contradicts the prime assumption ($e > 3$). So three cases can be considered:

- If $\beta_1 = \emptyset$ the relation $s^e \equiv \underline{\alpha_1} \cdot \underline{\alpha_2}^{-1} \cdot \underline{\beta_2}^{r_2} \cdot \underline{Y}^{r_2 - r_1} \pmod{n}$ holds so $\{\alpha_1, \alpha_2\} = \{\beta_2, Y\}$ by Lemma 6. Therefore $Y_2 = \beta_2 + Y = \alpha_1 + \alpha_2 = X_1 \div X_2$ and $Y_1 = Y \in \{\alpha_1, \alpha_2\}$.
- If $\beta_2 = \emptyset$ the set Y_1 is equal to $X_1 \div X_2$ and $Y_2 \in \{\alpha_1, \alpha_2\}$ for reasons of symmetry.
- If $Y = \emptyset$ the relation $s^e \equiv \underline{\alpha_1} \cdot \underline{\alpha_2}^{-1} \cdot \underline{\beta_1}^{-r_1} \cdot \underline{\beta_2}^{r_2} \pmod{n}$ holds thus $\{\alpha_1, \alpha_2\} = \{\beta_1, \beta_2\}$ according to Lemma 6.

Now the "if" part is proved.

- If $(Y_1, Y_2) = (X_1 \setminus X_2, X_1 \div X_2)$ or $(Y_1, Y_2) = (X_1 \div X_2, X_2 \setminus X_1)$ or $(Y_1 \setminus Y_2, Y_2 \setminus Y_1) = (X_1 \setminus X_2, X_2 \setminus X_1)$ one can compute numbers $a, b \in \{1, \ldots, e-1\}$ such that $\underline{X_1} \cdot \underline{Y_2}^b \equiv \underline{X_2} \cdot \underline{Y_1}^a \pmod{n}$, namely $(a, b) = (2, 1)$, $(1, 2)$ and $(1, 1)$ respectively. In these cases $z \equiv \underline{X_1}^{-1} \cdot \underline{Y_1}^a \pmod{n}$ is computed that satisfies $z \cdot \underline{X_1} \equiv \underline{Y_1}^a \pmod{n}$ and $z \cdot \underline{X_2} \equiv \underline{Y_2}^b \pmod{n}$. Therefore $\mathrm{RC}(X^2, Y^2)$ by Lemma 4.
- If $(Y_1, Y_2) = (X_2 \setminus X_1, X_1 \div X_2)$ or $(Y_1, Y_2) = (X_1 \div X_2, X_1 \setminus X_2)$ or $(Y_1 \setminus Y_2, Y_2 \setminus Y_1) = (X_2 \setminus X_1, X_1 \setminus X_2)$ one can compute numbers $a, b \in \{1, \ldots, e-1\}$ such that $\underline{X_1} \cdot \underline{Y_1}^a \equiv \underline{X_2} \cdot \underline{Y_2}^b \pmod{n}$, namely $(a, b) = (2, 1)$, $(1, 2)$ and $(1, 1)$ respectively. In these cases $z \equiv \underline{X_1}^{-1} \cdot \underline{Y_1}^{-a} \pmod{n}$ is computed that satisfies $z \cdot \underline{X_1} \equiv \underline{Y_1}^{-a} \pmod{n}$ and $z \cdot \underline{X_2} \equiv \underline{Y_2}^{-b} \pmod{n}$. Therefore $\mathrm{RC}(X^2, Y^2)$ by Lemma 4 and the fact that it is easy to compute the multiplicative inverse modulo n.

(End of Proof)

A counterexample of Theorem 7 for $e = 3$ is $X_1 = \{x_1, x_3\}$, $X_2 = \{x_2\}$, $Y_1 = \{x_1, x_2\}$, $Y_2 = \{x_2, x_3\}$ and $z \equiv x_2/x_3 \pmod{n}$. A consequence of Theorem 7 is that in the general case ($l \geq 2$) the Y_i must be all different. Before Theorem 7 is generalized to $l \geq 2$, we show that a user is not able to obtain more than one valid coin with one execution of the withdrawal protocol.

Lemma 8 *Let X be a non-empty subset of C. Let $z \in \mathbb{Z}_n^*$. Let Y_1 and Y_2 be non-empty subsets of C. If it is feasible to compute $(\underline{Y_1})^d$ and $(\underline{Y_2})^d$ from $(z \cdot \underline{X})^d$ modulo n, then $Y_1 = Y_2$.*

Proof. From Lemma 5 follows that $(z \cdot \underline{X})^d$ can be computed from $(\underline{Y_1})^d$ and from $(\underline{Y_2})^d$ modulo n. From the rootcomputability-assumption follows then that it is feasible to compute r_1 and r_2, $0 < r_1, r_2 < e$, and $s_1, s_2 \in \mathbb{Z}_n^*$ such that $z\underline{X} \equiv (\underline{Y_1})^{r_1} s_1^e \pmod{n}$ and $z\underline{X} \equiv (\underline{Y_2})^{r_2} s_2^e \pmod{n}$. Note that when $r_1 = 0$ the number $(\underline{X})^d$ could be computed which contradicts the rootinfeasibility-assumption. We obtain that $(\underline{Y_1})^{r_1} (\underline{Y_2})^{-r_2} \equiv (s_2/s_1)^e$

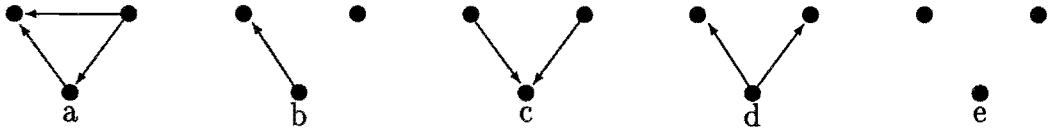

Figure 2: The five possible graphs up to isomorphism for three different sets.

(mod n). From the rootinfeasibility-assumption can be concluded that $r_1 = r_2$ and $Y_1 = Y_2$.
(End of Proof)

Next three lemmas are presented to extend Theorem 7 to the case $l = 3$. These three lemmas describe the (im)possible subset-relations for the $Y_i (1 \leq i \leq 3)$. In Figure 2 are all possible subset-relations for three different sets up to isomorphism. In this figure an arrow means "is subset of".

The following lemma shows that graph (a) of Figure 2 can never occur as subset-relation graph of Y_1, Y_2 and Y_3.

Lemma 9 *Let $X_i (1 \leq i \leq 3)$ be subsets of C that are not subset-related. Let $Y_i (1 \leq i \leq 3)$ be non-empty subsets of C. If $RC(X^3, Y^3)$, it is impossible that $Y_1 \subseteq Y_2 \subseteq Y_3$.*

Proof. Suppose that $Y_1 \subseteq Y_2 \subseteq Y_3$ and $\mathrm{RC}(X^3, Y^3)$. From Theorem 7 it follows that $Y_2 = X_1 \div X_2$, $Y_1 \in \{X_1 \setminus X_2, X_2 \setminus X_1\}$, $Y_3 = X_2 \div X_3$ and $Y_2 \in \{X_2 \setminus X_3, X_3 \setminus X_2\}$. From $Y_2 \in \{X_2 \setminus X_3, X_3 \setminus X_2\}$ and $Y_2 = X_1 \div X_2$, it is concluded that $X_1 \setminus X_2 = \emptyset$ or $X_2 \setminus X_1 = \emptyset$, which contradicts the fact that X_1 and X_2 are not subset-related.
(End of Proof)

The following lemma shows that graph (b) of Figure 2 can never occur as subset-relation graph of Y_1, Y_2 and Y_3.

Lemma 10 *Let $X_i (1 \leq i \leq 3)$ be subsets of C that are not subset-related. Let $Y_i (1 \leq i \leq 3)$ be non-empty subsets of C. If $RC(X^3, Y^3)$, it is impossible that simultaneously $Y_1 \subseteq Y_2$, $Y_1 \not\subseteq Y_3$, $Y_3 \not\subseteq Y_1$, $Y_2 \not\subseteq Y_3$ and $Y_3 \not\subseteq Y_2$.*

Proof. Suppose that $Y_1 \subseteq Y_2$, $Y_1 \not\subseteq Y_3$, $Y_3 \not\subseteq Y_1$, $Y_2 \not\subseteq Y_3$, $Y_3 \not\subseteq Y_2$, and $\mathrm{RC}(X^3, Y^3)$. From Theorem 7 it follows that $Y_2 = X_1 \div X_2$, $Y_1 \in \{X_1 \setminus X_2, X_2 \setminus X_1\}$, $\{Y_1 \setminus Y_3, Y_3 \setminus Y_1\} = \{X_1 \setminus X_3, X_3 \setminus X_1\}$ and $\{Y_2 \setminus Y_3, Y_3 \setminus Y_2\} = \{X_2 \setminus X_3, X_3 \setminus X_2\}$.

1. If $Y_1 = X_1 \setminus X_2$ and $Y_2 \setminus Y_3 = X_2 \setminus X_3$ the set $Y_1 \cap (Y_2 \setminus Y_3)$ is empty. Therefore $X_1 \setminus X_3 = Y_1 \setminus Y_3 = \emptyset$ since $Y_1 \subseteq Y_2$, which contradicts the fact that X_1 and X_3 are not subset-related.

2. If $Y_1 = X_1 \setminus X_2$ and $Y_2 \setminus Y_3 = X_3 \setminus X_2$ the equality $X_2 \setminus (X_1 \cup X_3) = (X_1 \div X_2) \cap (X_2 \setminus X_3) = Y_2 \cap (Y_3 \setminus Y_2) = \emptyset$ holds and $(X_1 \cap X_2) \setminus X_3 = (X_1 \setminus X_3) \cap (X_2 \setminus X_3) = (Y_1 \setminus Y_3) \cap (Y_3 \setminus Y_2) = \emptyset$. So $X_2 \setminus X_3 = \emptyset$, which contradicts the fact that X_2 and X_3 are not subset-related.

3. If $Y_1 = X_2 \setminus X_1$ and $Y_2 \setminus Y_3 = X_2 \setminus X_3$ the equality $(X_1 \cap X_3) \setminus X_2 = (X_1 \div X_2) \cap (X_3 \setminus X_2) = Y_2 \cap (Y_3 \setminus Y_2) = \emptyset$ holds and $X_3 \setminus (X_1 \cup X_2) = (X_3 \setminus X_1) \cap (X_3 \setminus X_2) = (Y_1 \setminus Y_3) \cap (Y_3 \setminus Y_2) = \emptyset$. So $X_3 \setminus X_2 = \emptyset$ which contradicts the fact that X_2 and X_3 are not subset-related.

4. If $Y_1 = X_2 \setminus X_1$ and $Y_2 \setminus Y_3 = X_3 \setminus X_2$ the set $Y_1 \cap (Y_2 \setminus Y_3)$ is empty. Therefore $X_3 \setminus X_1 = Y_1 \setminus Y_3 = \emptyset$ since $Y_1 \subseteq Y_2$, which contradicts the fact that X_1 and X_3 are not subset-related.

(End of Proof)

The following lemma shows that graph (c) of Figure 2 can never occur as subset-relation graph of Y_1, Y_2 and Y_3.

Lemma 11 *Let $X_i (1 \leq i \leq 3)$ be subsets of C that are not subset-related. Let $Y_i (1 \leq i \leq 3)$ be non-empty subsets of C. If $RC(X^3, Y^3)$, it is impossible that simultaneously $Y_2 \subseteq Y_1$, $Y_3 \subseteq Y_1$, $Y_2 \not\subseteq Y_3$, and $Y_3 \not\subseteq Y_2$.*

Proof. Suppose that $Y_2 \subseteq Y_1$, $Y_3 \subseteq Y_1$, $Y_2 \not\subseteq Y_3$, $Y_3 \not\subseteq Y_2$, and $\mathrm{RC}(X^3, Y^3)$. From Theorem 7 it follows that $Y_1 = X_1 \div X_2$, $Y_2 \in \{X_1 \setminus X_2, X_2 \setminus X_1\}$, $Y_1 = X_1 \div X_3$, $Y_3 \in \{X_1 \setminus X_3, X_3 \setminus X_1\}$ and $\{Y_2 \setminus Y_3, Y_3 \setminus Y_2\} = \{X_2 \setminus X_3, X_3 \setminus X_2\}$. So $X_1 \setminus X_2 = X_1 \setminus X_3$ and $X_2 \setminus X_1 = X_3 \setminus X_1$ since $X_1 \div X_2 = X_1 \div X_3$.

1. If $Y_2 = X_1 \setminus X_2$ the set Y_3 is equal to $X_3 \setminus X_1$ so $\{X_1 \setminus X_2, X_3 \setminus X_1\} = \{Y_2, Y_3\} = \{Y_2 \setminus Y_3, Y_3 \setminus Y_2\} = \{X_2 \setminus X_3, X_3 \setminus X_2\}$. Therefore $Y_2 = \emptyset$ or $Y_3 = \emptyset$ because $(X_2 \setminus X_3) \cap (X_1 \setminus X_2) = (X_2 \setminus X_3) \cap (X_3 \setminus X_1) = \emptyset$. Contradiction.

2. If $Y_2 = X_2 \setminus X_1$ the set Y_3 is equal to $X_1 \setminus X_3$ so $\{X_2 \setminus X_1, X_1 \setminus X_3\} = \{Y_2, Y_3\} = \{Y_2 \setminus Y_3, Y_3 \setminus Y_2\} = \{X_2 \setminus X_3, X_3 \setminus X_2\}$. Therefore $Y_2 = \emptyset$ or $Y_3 = \emptyset$ because $(X_3 \setminus X_2) \cap (X_2 \setminus X_1) = (X_3 \setminus X_2) \cap (X_1 \setminus X_3) = \emptyset$. Contradiction.

(End of Proof)

We first prove Theorem 1 using the last three lemmas, and then Theorems 2 and 3.

Proof of THEOREM 1. The proof goes by induction on l. For $l = 2$ the statement is trivial. Suppose the statement holds for certain $l \geq 2$. It is proved that the statement holds for $l + 1$ by considering two cases:

1. If the sets Y_1 to Y_l are not subset-related three subcases are considered.

   - If $Y_{l+1} \subseteq Y_1$ the set Y_{l+1} is a subset of Y_i for each $i \in \{1, \ldots, l\}$ otherwise graph (a) or (b) of Figure 2 will occur as subgraph in the subset-relation-graph of $Y_i, 1 \leq i \leq l + 1$.
   - If $Y_{l+1} \supseteq Y_1$, graph (a), (b) or (c) of Figure 2 will occur as subgraph in the subset-relation-graph of $Y_i, 1 \leq i \leq l + 1$. Contradiction.

- If Y_{l+1} and Y_1 are not subset-related, Y_1 to Y_{l+1} are not subset-related otherwise graph (b) of Figure 2 will occur as subgraph in the subset-relation-graph of $Y_i, 1 \leq i \leq l+1$.

2. If the sets Y_2 to Y_l are not subset-related and Y_1 is contained in each of them (w.l.o.g. $j = 1$), three subcases are considered.

   - If $Y_{l+1} \subseteq Y_1$ graph (a) of Figure 2 will occur as subgraph in the subset-relation-graph of $Y_i, 1 \leq i \leq l+1$. Contradiction.
   - If $Y_{l+1} \supseteq Y_1$ the sets Y_2 to Y_{l+1} are not subset-related otherwise graph (a) of Figure 2 will occur as subgraph in the subset-relation-graph of $Y_i, 1 \leq i \leq l+1$.
   - If Y_{l+1} and Y_1 are not subset-related graph (b) or (c) of Figure 2 will occur as subgraph in the subset-relation-graph of $Y_i, 1 \leq i \leq l+1$. Contradiction.

So the statement holds for $l+1$.
(End of Proof)

Proof of THEOREM 2. First the "only if" part is proved. From Theorem 7 it follows that $\forall_{1\leq i,j\leq l}[\{Y_i \setminus Y_j, Y_j \setminus Y_i\} = \{X_i \setminus X_j, X_j \setminus X_i\}]$. Let $i \in \{1,\ldots,l\}$. Suppose there are j_1 and j_2 such that j_1, j_2 and i are distinct, $Y_i \setminus Y_{j_1} = X_i \setminus X_{j_1}$ and $Y_i \setminus Y_{j_2} = X_{j_2} \setminus X_i$ then $X_i \setminus (X_{j_1} \cup X_{j_2}) = (X_i \setminus X_{j_1}) \cap (X_i \setminus X_{j_2}) = (Y_i \setminus Y_{j_1}) \cap (Y_{j_2} \setminus Y_i) = \emptyset$. Two cases are considered:

- If $Y_{j_1} \setminus Y_{j_2} = X_{j_1} \setminus X_{j_2}$ the equality $(X_{j_1} \cap X_i) \setminus X_{j_2} = (X_{j_1} \setminus X_{j_2}) \cap (X_i \setminus X_{j_2}) = (Y_{j_1} \setminus Y_{j_2}) \cap (Y_{j_2} \setminus Y_i) = \emptyset$ holds. So $X_i \subseteq X_{j_2}$ because $X_i \subseteq X_{j_1} \cup X_{j_2}$ and $X_{j_1} \cap X_i \subseteq X_{j_2}$, which contradicts the fact that X_i and X_{j_2} are not subset-related.

- If $Y_{j_1} \setminus Y_{j_2} = X_{j_2} \setminus X_{j_1}$ the equality $(X_{j_2} \cap X_i) \setminus X_{j_1} = (X_{j_2} \setminus X_{j_1}) \cap (X_i \setminus X_{j_1}) = (Y_{j_1} \setminus Y_{j_2}) \cap (Y_{j_2} \setminus Y_i) = \emptyset$ holds. So $X_i \subseteq X_{j_1}$ because $X_i \subseteq X_{j_1} \cup X_{j_2}$ and $X_{j_2} \cap X_i \subseteq X_{j_1}$, which contradicts the fact that X_i and X_{j_1} are not subset-related.

So $\forall_{1\leq j\leq l}[Y_i \setminus Y_j = X_i \setminus X_j]$ or $\forall_{1\leq j\leq l}[Y_i \setminus Y_j = X_j \setminus X_i]$. This holds for each $i \in \{1,\ldots,l\}$ so $\forall_{1\leq i,j\leq l}[Y_i \setminus Y_j = X_i \setminus X_j]$ or $\forall_{1\leq i,j\leq l}[Y_i \setminus Y_j = X_j \setminus X_i]$. These two cases are considered:

- $\forall_{1\leq i,j\leq l}[Y_i \setminus Y_j = X_j \setminus X_i]$
  Choose an arbitrary i from $\{1,\ldots,l\}$. From $\forall_{1\leq j\leq l}[(X_j \setminus X_i) \subseteq Y_i]$ it follows that $U \setminus X_i = \bigcup_{j=1,\ldots,l}(X_j \setminus X_i) \subseteq Y_i$. Define Z_i such that $Y_i = (U \setminus X_i) + Z_i$. Since $Z_i \cap (X_i \setminus X_j) \subseteq Y_i \cap (Y_j \setminus Y_i) = \emptyset$ for every $j \in \{1,\ldots,l\}$ one obtains $Z_i \cap (X_i \setminus I) = Z_i \cap \bigcup_{j=1,\ldots,l}(X_i \setminus X_j) = \emptyset$. Also $Z_i \cap (U \setminus X_i) = \emptyset$ by definition of Z_i, so $Z_i \cap (U \setminus I) = \emptyset$. Let $j \in \{1,\ldots,l\}$. From $Z_i \subseteq Y_i \subseteq (Y_i \setminus Y_j) \cup Y_j = (X_j \setminus X_i) \cup (U \setminus X_j) \cup Z_j \subseteq (U \setminus I) \cup Z_j$ and $Z_i \cap (U \setminus I) = \emptyset$ it follows that $Z_i \subseteq Z_j$. This holds for every i and j so all Z_i are the same.
  Let $i \in \{1,\ldots,l\}$. Because $Z_i \cap (U \setminus I) = \emptyset$ one derives $Z_i = Z_i + \bigcap_{j=1,\ldots,l}(U \setminus X_j) = \bigcap_{j=1,\ldots,l}((U \setminus X_j) + Z_i) = \bigcap_{j=1,\ldots,l} Y_j = Y$.

- $\forall_{1\le i,j\le l}[Y_i \setminus Y_j = X_i \setminus X_j]$
  Choose an arbitrary i from $\{1,\ldots,l\}$. From $\forall_{1\le j\le l}[(X_i \setminus X_j) \subseteq Y_i]$ it follows that $X_i \setminus I = \bigcup_{j=1,\ldots,l}(X_i \setminus X_j) \subseteq Y_i$. Define Z_i such that $Y_i = (X_i \setminus I) + Z_i$. Since $Z_i \cap (X_j \setminus X_i) \subseteq Y_i \cap (Y_j \setminus Y_i) = \emptyset$ for every $j \in \{1,\ldots,l\}$ one obtains $Z_i \cap (U \setminus X_i) = Z_i \cap \bigcup_{j=1,\ldots,l}(X_j \setminus X_i) = \emptyset$. Also $Z_i \cap (X_i \setminus I) = \emptyset$ by definition of Z_i, so $Z_i \cap (U \setminus I) = \emptyset$. Let $j \in \{1,\ldots,l\}$. From $Z_i \subseteq Y_i \subseteq (Y_i \setminus Y_j) \cup Y_j = (X_i \setminus X_j) \cup (X_j \setminus I) \cup Z_j \subseteq (U \setminus I) \cup Z_j$ and $Z_i \cap (U \setminus I) = \emptyset$ it follows that $Z_i \subseteq Z_j$. This holds for every i and j so all Z_i are the same.
  Let $i \in \{1,\ldots,l\}$. Because $Z_i \cap (U \setminus I) = \emptyset$ one derives $Z_i = Z_i + \bigcap_{j=1,\ldots,l}(X_j \setminus I) = \bigcap_{j=1,\ldots,l}((X_j \setminus I) + Z_i) = \bigcap_{j=1,\ldots,l} Y_j = Y$.

Now the "if" part is proved by considering the two cases:

- If $\forall_{1\le i\le l}[Y_i = (U \setminus X_i) + Y]$ the number $z \equiv (\underline{U} \cdot \underline{Y})^{-1} \pmod{n}$ is computed. This choice for z realizes $\mathrm{RC}(X^l, Y^l)$ because $z \cdot \underline{X_i} \equiv \underline{Y_i}^{-1} \pmod{n}$ for each $1 \le i \le l$.
- If $\forall_{1\le i\le l}[Y_i = (X_i \setminus I) + Y]$ the number $z \equiv \underline{I}^{-1} \cdot \underline{Y} \pmod{n}$ is computed. This choice for z realizes $\mathrm{RC}(X^l, Y^l)$ because $z \cdot \underline{X_i} \equiv \underline{Y_i} \pmod{n}$ for each $1 \le i \le l$.

(End of Proof)

Proof of THEOREM 3. First the "only if" is proved. From Theorem 7 it follows that $Y_1 \in \{X_1 \setminus X_i, X_i \setminus X_1\}$ and $Y_i = X_1 \div X_i$ for $2 \le i \le l$. Considering the sets Y_2 to Y_l induces two possibilities according to Theorem 2:

- If $\forall_{2\le i\le l}[Y_i = (U \setminus X_i) + Y]$ the set $(U \setminus X_i) + Y$ is equal to $X_1 \div X_i$ so $(X_i \setminus X_1) \subseteq Y$ for $2 \le i \le l$ thus $(U \setminus X_1) \subseteq Y$. Two cases are considered:
  1. If $Y_1 = (X_2 \setminus X_1)$ the set Y_1 is equal to $(X_i \setminus X_1)$ for $2 \le i \le l$ so $Y = Y_i \setminus (U \setminus X_i) = (X_1 \div X_i) \setminus (U \setminus X_i) = (X_1 \setminus U) + (X_i \setminus X_1) = X_1 \div U$.
  2. If $Y_1 = (X_1 \setminus X_2)$ the set Y_1 is equal to $(X_1 \setminus X_i)$ for $2 \le i \le l$ so $U = (U \setminus X_1) + (X_1 \cap U) \subseteq Y \cup I$. Therefore $U \subseteq I$ since $(U \setminus I) \cap Y = \emptyset$. Due to the definitions of U and I this is only possible if $l = 2$ so $Y = Y_2 = X_1 \div I$ and $Y_1 = (X_1 \setminus I)$.
- If $\forall_{2\le i\le l}[Y_i = (X_i \setminus I) + Y]$ the set $(X_i \setminus I) + Y$ is equal to $X_1 \div X_i$ so $(X_i \setminus I) \subseteq (X_i \setminus X_1)$ for $2 \le i \le l$ thus $(U \setminus I) \subseteq (U \setminus X_1)$. Two cases are considered:
  1. If $Y_1 = (X_1 \setminus X_2)$ the set Y_1 is equal to $(X_1 \setminus X_i)$ for $2 \le i \le l$ so $Y = Y_i \setminus (X_i \setminus I) = (X_1 \div X_i) \setminus (X_i \setminus I) = (X_1 \setminus X_i) + (I \setminus X_1) = X_1 \div I$.
  2. If $Y_1 = (X_2 \setminus X_1)$ the set Y_1 is equal to $(X_i \setminus X_1)$ for $2 \le i \le l$ so $(U \setminus I) \subseteq (U \setminus X_1) = (I \setminus X_1)$. Therefore $U \subseteq I$ so $l = 2$ and $Y = Y_2 = X_1 \div U$ and $Y_1 = (U \setminus X_1)$.

Now the "if" part is proved by considering the two possibilities.

- If $(\forall_{2\leq i\leq l}[Y_i = (U \setminus X_i) + Y]$ and $Y = (X_1 \div U)$ and $Y_1 = (U \setminus X_1))$, the number $z \equiv (\underline{U} \cdot \underline{Y})^{-1} \pmod{n}$ is computed. This choice for z realizes $\mathrm{RC}(X^l, Y^l)$ because $z \cdot \underline{X_i} \equiv \underline{Y_i}^{-1} \pmod{n}$ for $2 \leq i \leq l$, and $z \cdot \underline{X_1} \equiv \underline{Y_1}^{-2} \pmod{n}$ (Lemma 4).
- If $(\forall_{2\leq i\leq l}[Y_i = (X_i \setminus I) + Y]$ and $Y = (X_1 \div I)$ and $Y_1 = (X_1 \setminus I))$, the number $z \equiv \underline{I}^{-1} \cdot \underline{Y} \pmod{n}$ is computed. This choice for z realizes $\mathrm{RC}(X^l, Y^l)$ because $z \cdot \underline{X_i} \equiv \underline{Y_i} \pmod{n}$ for $2 \leq i \leq l$, and $z \cdot \underline{X_1} \equiv \underline{Y_1}^2 \pmod{n}$ (Lemma 4).

(End of Proof)

5 Open problems and discussion

We investigated the case of a single user participating in the withdrawal protocol once. At least two other attacks are possible. The first one is a single user executing the withdrawal protocol several times and thereafter trying to combine the received signatures to obtain one or more valid coins. The second possible attack is several colluding users executing the withdrawal protocol attempting to combine their signatures. Formally these two attacks can be described as follows: Let m be the number of colluding users. Let $l \geq 1$. Let X_{ij} $(i = 1, \ldots, m, j = 1, \ldots, l)$ and $Y_j (j = 1, \ldots, l)$ be subsets of C. Is it feasible to compute, without knowing the factorization of n, numbers $z_i (1 \leq i \leq m)$ coprime with n such that for each $1 \leq j \leq l$ it is feasible to compute $(\underline{Y_j})^d$ from the numbers $(z_i \cdot \underline{X_{ij}})^d (1 \leq i \leq m)$ modulo n?

It would also be interesting to know whether the rootcomputability assumption can be weakened so that the three main theorems still hold. At best one would only need the assumption that RSA is secure.

Note that we do not claim that the considered withdrawal protocol is the most efficient protocol for issuing blinded RSA signatures. In fact, a more efficient protocol exists [1] that is provably equally secure as the Schnorr scheme [12]. From a mathematical point of view, our results remain interesting and could also be useful in other areas due to the abstraction from the actual protocol.

Acknowledgement I would like to thank Gilles Brassard, David Chaum, Matthijs Coster, Jan-Hendrik Evertse, Eugène van Heyst and Henk van Tilborg for their useful comments and discussions.

References

[1] Brands, S.A., Restrictive blinding of secret-key certificates, CWI, Report CS-R9509.

[2] Chaum, D. and J.H. Evertse, A secure and privacy-protecting protocol for transmitting personal information between organizations, Proc. of Crypto '86, pp. 118-167.

[3] Chaum, D., A. Fiat and M. Naor, Untraceable electronic cash, Proc. of Crypto '88, pp. 319-327.

[4] Euclid, The elements, Vol. 7, Proposition 2, 300 B.C. (The thirteen books of Euclid's Elements, Vol. 2, T.L. Heath, Dover Publications Inc., New York, 1956, pp. 298-300.)

[5] Evertse, J.H. and E. van Heyst, Which new RSA-signatures can be computed from certain given RSA-signatures?, Journal of Cryptology, Vol. 5, No. 1, 1992, pp. 41-52.

[6] Evertse, J.H. and E. van Heyst, Which new RSA signatures can be computed from RSA signatures, obtained in a specific interactive protocol?, Proc. of Eurocrypt '92, pp. 378-389.

[7] Fiat, A., Batch RSA, Advances in Cryptology-CRYPTO'89, Springer-Verlag, pp. 175-185.

[8] Hayes, B., Anonymous one-time signatures and flexible untraceable electronic cash, Proc. of Auscrypt '90, pp. 294-305.

[9] Okamoto, T. and K. Ohta, Disposable zero-knowledge authentications and their applications to untraceable electronic cash, Proc. of Crypto '89, pp.481-496.

[10] Okamoto, T. and K. Ohta, Universal electronic cash, Proc. of Crypto '91, pp. 324-337.

[11] Rivest, R.L., A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Comm. ACM, Vol. 21, Feb. 1978, pp. 120-126.

[12] Schnorr, C., Efficient signature generation by smart cards, Journal of Cryptology, Vol. 4, No. 3, 1991, pp. 161-174.