On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem

Michaël Quisquater*, Bart Preneel, and Joos Vandewalle

Katholieke Universiteit Leuven,
Department Electrical Engineering-ESAT, COSIC,
Kasteelpark Arenberg 10, B–3001 Heverlee, Belgium
michael.quisquater@esat.kuleuven.ac.be

Abstract. Threshold schemes enable a group of users to share a secret by providing each user with a share. The scheme has a threshold $t+1$ if any subset with cardinality $t+1$ of the shares enables the secret to be recovered.
In 1983, C. Asmuth and J. Bloom proposed such a scheme based on the Chinese remainder theorem. They derived a complex relation between the parameters of the scheme in order to satisfy some notion of security. However, at that time, the concept of security in cryptography had not yet been formalized.
In this paper, we revisit the security of this threshold scheme in the modern context of security. In particular, we prove that the scheme is asymptotically optimal both from an information theoretic and complexity theoretic viewpoint when the parameters satisfy a simplified relationship. We mainly present three theorems, the two first theorems strengthen the result of Asmuth and Bloom and place it in a precise context, while the latest theorem is an improvement of a result obtained by Goldreich *et al.*

1 Introduction

A threshold scheme enables a secret to be shared among a group of l members providing each member with a share. The scheme has a threshold $t+1$ if any subset with cardinality $t+1$ out of the l shares enables the secret to be recovered. We will use the notation $(t+1, l)$ to refer to such a scheme.

Ideally, in a $(t+1)$ threshold scheme, t shares should not give any information on the secret. We will discuss later how to express this information. In the $80ies$, several algebraic constructions of $(t+1, l)$ threshold schemes were proposed.

Shamir used the Lagrange polynomial interpolation. In the Shamir scheme [S79], the secret space is usually a field[1] and the secret consist of the constant term of a polynomial $p(x)$ of degree at most t if the threshold is $t+1$. The shares are $p(x_i)$, where the x_i's are public and belong to the secret space. Blakley

* F.W.O.-research fellow, sponsored by the Fund for Scientific Research – Flanders (Belgium).

[1] Note that this condition might be relaxed, see e.g [DF94].

D. Naccache and P. Paillier (Eds.): PKC 2002, LNCS 2274, pp. 199–210, 2002.

used projective spaces to construct such schemes [B79]. Karnin *et al.* consider variations on the previous schemes using coding theory [KGH83].

Mignotte [M82] and Asmuth and Bloom [AB83] used congruence classes and the Chinese remainder theorem to define $(t+1, l)$ threshold schemes. The public parameters are the co-prime and increasing numbers p_i's, $i = 0, \ldots, l$. First the secret $r_0 \stackrel{\triangle}{=} s$ is chosen from the secret space $\mathbb{Z}_{p_0}$. Then the values r_i's are randomly chosen in $\mathbb{Z}_{p_i}$ for $i = 1, \cdots, t$ if the threshold is $t+1$. Using the Chinese remainder theorem, $Y \in \mathbb{Z}_{\prod_{i=0}^{t} p_i}$ is computed such that $Y \equiv r_i \bmod p_i$ for $i = 0, \ldots, t$. The shares are $s_i = Y \bmod p_i$ for $i = 1, \ldots, l$. Note that Mignotte [M82] defined the secret as Y and dropped the space depending on p_0. The main advantage of the schemes [M82] and [AB83] over [S79] (and [B79]) is that the computational complexity of the reconstruction of the secret from $t+1$ shares behaves as $\mathcal{O}(t+1)$ while it behaves as $\mathcal{O}((t+1) \cdot log^2(t+1))$ for the Shamir scheme.

It is known that any set of t shares of a $(t+1, l)$ Shamir scheme gives no information from an information theoretic and complexity theoretic viewpoint. The argument can be found in [S79], even if the concepts used are not the same. Also, the sizes of the share spaces and the secret space are equal. Therefore, the Shamir scheme is called ideal and perfect zero-knowledge (see the definitions 5 and 7 in section 2).

However, in the $(t+1, l)$ threshold scheme based on the Chinese remainder theorem, the sizes of the share spaces and the secret space are not equal. In addition, few results are known about the information on the secret given by any set of t shares. In the scheme of Mignotte [M82], any share substantially decreases the entropy of the secret. Asmuth and Bloom [AB83] showed that the entropy of the secret decreases "not too much" when t shares are known provided that the parameters of the scheme satisfy a complex condition. The problem with this approach is that the notion of security is unclear, moreover the way one has to choose the parameters might led to schemes far from ideal schemes. Goldreich *et al.* [GRS00] show that any set of $t-1$ shares gives no information on the secret using the zero-knowledge theory provided that the parameters on the system satisfy a natural condition (the primes p_i's have to be consecutive).

In this paper, we revisit the security of the threshold scheme based on the Chinese remainder theorem when the parameters are consecutive primes using modern concepts of security in cryptography [GB01]. We introduce the concept of an asymptotically perfect and an asymptotically ideal schemes which are natural relaxations of perfect and ideal schemes. We prove that the $(t+1, l)$ threshold scheme based on the Chinese remainder theorem with consecutive primes is asymptotically ideal (and therefore asymptotically perfect) and perfect zero-knowledge. This means, in both cases, that t shares give no information on the secret. The two first theorems strengthen the result of Asmuth and Bloom [AB83], while the latest is an improvement of a result in [GRS00].

This paper is organized as follows. In section 2, we discuss basic definitions of threshold schemes, including the definition of an asymptotically perfect and

an asymptotically ideal scheme. In section 3, we detail the threshold scheme to be studied. Section 4 describes the previous work on the security of Chinese remainder theorem based threshold schemes. In section 5, we find an upper bound on the loss of entropy of the secret generated by shares when the secret is uniformly selected. Using these result, we prove that the scheme is asymptotically perfect and asymptotically ideal when the secret is uniformly chosen and the parameters of the system satisfy a natural condition (the primes p_i's are consecutive). Finally, we prove that the scheme with consecutive primes is perfect zero-knowledge.

2 Theoretical Notions about Threshold Schemes

In this section, we present different definitions related to threshold schemes. Definitions $1, 3, 5, 7$ are slight modifications of those presented in [DF94]. Definitions $2, 4, 6$ are introduced in the current paper.

Let us first define a threshold scheme.

Definition 1. *Let $\mathcal{X}$ be a set of pairs of public and security parameters. A $(t+1, l)$ threshold scheme is a collection of pairs of algorithms $(Share_{(x,1^k)}$, $Combine_{(x,1^k)})$, where $(x, 1^k) \in \mathcal{X}$, such that:*

1. *$Share_{(x,1^k)}$ is a probabilistic polynomial time algorithm taking as input a secret s coming from the secret space $\mathcal{S}(x, 1^k) \subseteq \{0,1\}^k$ and producing as output a set of l shares s_i coming each from the share space $\mathcal{S}_i(x, 1^k)$, $i = 1, \ldots, l$.*
2. *$Combine_{(x,1^k)}$ is a polynomial time algorithm taking as input any set of $t+1$ shares out of the l and producing as output the unique secret s.*

Note that in this definition, no probability is associated to the secret space $\mathcal{S}(x, 1^k)$.

Next, we define the loss of entropy of the secret generated by the knowledge of a set shares. So far as the authors know this definition is new in the context of the threshold scheme. Note that this quantity is related to the average mutual information (see [G68]). The concept of loss of entropy of the secret will be used in the definition of perfect and asymptotically perfect schemes.

Definition 2. *Let $(Share_{(x,1^k)}, Combine_{(x,1^k)})$ be a $(t+1, l)$ threshold scheme. Let $P(x, 1^k)$ be the probability distribution on $\mathcal{S}(x, 1^k)$. Then, we define the loss of entropy of the secret generated by the knowledge of $\{s_i : i \in I\}$ by the values:*

$$\Delta_{(x,1^k)}(s_i : i \in I) = H(s \in \mathcal{S}(x, 1^k)) - H(s \in \mathcal{S}(x, 1^k) | s_i : i \in I)$$

where $H(\cdot)$ [2] is the entropy function.

[2] The entropy of S selected from the alphabet $\mathcal{S}$ is defined as

$$H(S) = \sum_{s \in \mathcal{S}} P(S = s) \log(1/P(S = s)).$$

Remark 1. Note that while the average mutual information is always positive, the loss of entropy $\Delta(y) = H(S) - H(S|Y = y)$ may be negative. Consider the random variable $S \in \{-1, 0, 1\}$ such that $P(S = -1) = 7/8$, $P(S = 0) = 1/16$ and $P(S = 1) = 1/16$. Consider the random variable Y taking the value 1 if $S \geq 0$ and 0 otherwise, we have $P(S = -1|Y = 1) = 0$, $P(S = 0|Y = 1) = 1/2$ and $P(S = 1|Y = 1) = 1/2$. Therefore, $\Delta(1) = H(S) - H(S|Y = 1) = (7/8 \log(8/7) + 1/16 \log(16) + 1/16 \log(16)) - (1/2 \log(1/2) + 1/2 \log(1/2)) = 0.668 - 1 \approx -0.33$.

Let us introduce now a probability distribution $P(x, 1^k)$ on the secret space $\mathcal{S}(x, 1^k)$.

The following definition enables us to define the security of a threshold scheme from an information theoretic viewpoint. This definition depends on the set of probability distributions $P(x, 1^k)$.

Definition 3. *A threshold scheme $(t + 1, l)$ is called perfect with respect to the set of probability distributions $P(x, 1^k)$ on $\mathcal{S}(x, 1^k)$ if for all $(x, 1^k) \in \mathcal{X}$, it holds that:*

- $H(s \in \mathcal{S}(x, 1^k)) \neq 0$ *and,*
- *for all $I \subset \{1 \dots l\}$ with $|I| \leq t$, we have*

$$\Delta_{(x,1^k)}(s_i : i \in I) = 0.$$

Let us introduce the asymptotic version of the previous definition. This relaxation will enable us to prove that the threshold scheme based on the Chinese remainder theorem is asymptotically perfect while it is not perfect in the strict sense.

Definition 4. *A threshold scheme $(t+1, l)$ is asymptotically perfect with respect to the set of probabilities $P(x, 1^k)$, if for all $\epsilon > 0$, there exists $k_0 \geq 0$ such that for all $(x, 1^k) \in \mathcal{X}$ with $k \geq k_0$, we have for all $I \subset \{1, \dots, l\}$ with $|I| \leq t$,*

$$|\Delta_{(x,1^k)}(s_i : i \in I)| \leq \epsilon.$$

and $H(s \in \mathcal{S}(x, 1^k)) \neq 0$.

Remark 2. $|I|$ denotes the cardinality of the set I.

Remark 3. Note that it is essential to take the absolute value here, as Δ may be negative. However, if the distribution of the secret is uniform, one has $\Delta \geq 0$.

While security is an important factor, efficiency in terms of memory usage is also of great interest. This efficiency is measured by comparing the size of the share spaces to the size of the secret space. Indeed, the length of the elements depend on the size of these spaces if an optimal representation is used. The definition of an ideal scheme includes the property of security and efficiency.

Definition 5. *A threshold scheme $(t+1, l)$ is ideal with respect to the set of probabilities $P(x, 1^k)$ if:*

- *it is perfect with respect to this set of probabilities and,*
- *if for all $(x, 1^k) \in \mathcal{X}$, we have*

$$|\mathcal{S}_i(x, 1^k)| = |\mathcal{S}(x, 1^k)| \quad \forall i = 1, \ldots, l.$$

Let us introduce the asymptotic version of the previous definition. This relaxation will enable us to prove that the threshold scheme based on the Chinese remainder theorem is asymptotically ideal even though it is not strictly ideal.

Definition 6. *A threshold scheme $(t+1, l)$ is asymptotically ideal with respect to the set of probabilities $P(x, 1^k)$ if:*

- *it is asymptotically perfect with respect to this set of probabilities and,*
- *for all $\epsilon > 0$, there exists some $k_0 \geq 0$ such that for all $(x, 1^k) \in \mathcal{X}$ with $k \geq k_0$, we have for all $i \in \{1, \ldots, l\}$,*

$$|\mathcal{S}_i(x, 1^k)| / |\mathcal{S}(x, 1^k)| \leq 1 + \epsilon$$

When the shared key is associated to a public key, the entropy of the secret is zero. Therefore, we can not use the concept of perfect scheme to study the security of the schemes used in conjunction with public key cryptosystems. In order to solve this problem, Desmedt and Frankel [DF94] proposed to use the zero-knowledge theory. Working this way, it is possible to study the security of a threshold scheme even if the shared key is related to a public key.

Definition 7. *A threshold scheme $(t+1, l)$ is perfect zero-knowledge if there exists a set of probabilistic polynomial time algorithms $Simul(x, 1^k)$ such that for all polynomial $poly(\cdot)$, there exists some $k_0 \geq 0$ such that for all $(x, 1^k) \in \mathcal{X}$ with $k \geq k_0$, we have for all $s \in \mathcal{S}(x, 1^k)$ and for all $I \subset \{1, \ldots, l\}$ with $|I| \leq t$,*

$$\sum_{s_I \in \mathcal{S}_I(x, 1^k)} |P(I_{|Share_{(x,1^k)}(s)} = s_I) - P(Simul(x, 1^k) = s_I)| \leq 1/poly(k),$$

where s_I, $\mathcal{S}_I(x, 1^k)$, and $I_{|(s_1, \ldots, s_l)}$ and represent respectively $(s_{i_1}, \ldots, s_{i_j})$, $\mathcal{S}_{i_1}(x, 1^k) \times \ldots \times \mathcal{S}_{i_j}(x, 1^k)$ and $(s_{i_1}, \ldots, s_{i_j})$ for $I = \{i_1, \ldots, i_j\}$.

Note that this definition is independent of the probability distribution $P(x, 1^k)$ on $\mathcal{S}(x, 1^k)$.

In the next section, we present the threshold scheme whose security we study in the following sections.

3 Threshold Scheme Based on the CRT

Below, we describe two algorithms, corresponding to the sharing and reconstruction phases, of the threshold scheme based on the Chinese remainder theorem. We adopted the version present in [GRS00]. In the remainder of the text, $x \in_R S$ means that x is selected from S with an uniform probability.

Initialisation:
Let $t+1 \leq l$ and consider the primes $p_0 < p_1 < p_2 < ... < p_l$.

Sharing:
To share a secret $r_0 \stackrel{\triangle}{=} s \in \mathbb{Z}_{p_0}$, the dealer:

1. chooses $r_1 \in_R \mathbb{Z}_{p_1}$,..., $r_t \in_R \mathbb{Z}_{p_t}$;
2. determines $Y \in \mathbb{Z}_P$ where $P \stackrel{\triangle}{=} \prod_{i=0}^{t} p_i$ such that $Y \equiv r_i \bmod p_i$ for $i = 0, 1, ..., t$;
3. computes the shares $s_i = Y \bmod p_i$ for $i = 1, ..., l$.

This algorithm is denoted by $Share_{(t+1,p_0,...,p_l,1^{|p_0|})}(s) = (s_1, \ldots, s_l)$.

Reconstruction:
Given a set of $t+1$ shares $\{s_i : i \in I\}$, the secret s is recovered as follow:

1. compute $X \in \mathbb{Z}_{\prod_{i \in I} p_i}$ such that $X \equiv s_i \bmod p_i$ for $i \in I$, using the Chinese remainder theorem;
2. compute $s = X \bmod p_0$.

This algorithm is denoted by $Comb_{(t+1,p_0,...,p_l,1^{|p_0|})}(s_i : i \in I) = s$.

Remark 4. $|p_i|$ denotes the number of bits of p_i.

Remark 5. There are many different versions of the threshold scheme based on the Chinese remainder in the literature. Mignotte [M82] and Asmuth and Bloom [AB83] used coprime numbers p_i's while Goldreich *et al.* [GRS00] focused only on prime numbers. Also, Mignotte [M82] defined the secret as Y in the sharing algorithm and dropped the space depending on p_0. This last version lead to a very insecure scheme.

4 Previous Work about the Security of the Threshold Scheme Based on the CRT

In [M82], they compute the equivalent of the loss on entropy of the secret generated by the knowlegde on shares (see definition 2 in section 2). Note that the security of this scheme is quite weak.

The scheme [AB83] is a modification of the scheme [M82] by considering the secret $Y \bmod p_0$ instead of Y itself. In addition, they [AB83] request that the parameters of the system (the co-prime numbers p_i's) are increasing numbers and that

$$\prod_{i=1}^{t+1} p_i > p_0 \prod_{i=1}^{t} p_{l-i+1} \tag{1}$$

for a $(t+1, l)$ threshold scheme such that the entropy of the secret decreases "not too much" when t shares are known. First, notice that the notion of security

used is quite unclear. Note that at this time, modern security concepts were not yet build and therefore the notion of security of a threshold scheme did not make use of them. Also, this condition (1) might lead to schemes where the size of the shares are much more bigger that the size of the secret (if we choose p_0 very small) which we try to avoid. Finally, in practice, we have to generate co-prime numbers (usually primes numbers) and check whether the condition (1) is satisfied which is not very handy.

In [GRS00], Goldreich *et al.* advice to choose the primes (co-prime numbers are likely valid as well) as close as possible and prove that $t-1$ shares (or less) give no information on the secret in the sens of the zero-knowledge theory for a $(t+1, l)$ threshold scheme.

5 Security of a Threshold Scheme Based on the CRT

In the following Lemma, we compute an upper bound on the loss of entropy of the secret generated by the knowledge of shares when the secret is uniformly selected from the secret space. Recall that $x \in_R S$ means that x is selected from S with an uniform probability.

Lemma 1. *Let the secret $s \in_R \mathbb{Z}_{p_0}$, the shares s_i $(i = 1, ..., l)$ be generated by the algorithm $Share_{(t+1,p_0,...,p_l,1^{|p_0|})}(s)$, and $I \subseteq \{1, ..., l\}$.*
The loss of entropy of the secret $s \in_R \mathbb{Z}_{p_0}$ generated by the knowledge of the shares $\{s_i \in \mathbb{Z}_{p_i} : i \in I\}$ satisfies the following relations:

$$\begin{array}{ll} \Delta_{(t,p_0,...,p_l)}(s_i : I) \leq \log\left((p_0(\lfloor (C(I)+1)/p_0 \rfloor + 1)/C(I)\right) & if\ C(I) \neq 0, \\ = \log p_0 & otherwise, \end{array}$$

where $C(I) = \lfloor \prod_{i=0}^{t} p_i / \prod_{v \in I} p_v \rfloor$.

Proof. Define $C^*(I) \stackrel{\triangle}{=} \prod_{i=0}^{t} p_i / \prod_{v \in I} p_v$, $C(I) \stackrel{\triangle}{=} \lfloor C^*(I) \rfloor$ and $P \stackrel{\triangle}{=} \prod_{i=0}^{t} p_i$.

Consider the case $C(I) \neq 0$.

Let's prove that for all $s \in \mathbb{Z}_{p_0}$, $P(S = s | s_i : i \in I) \leq (\lfloor (C(I)+1)/p_0 \rfloor + 1)/C(I)$.

Let $s \in \mathbb{Z}_{p_0}$. Denote with V, the set of possible values for $X \in \mathbb{Z}_P$ given the set $\{s_i : i \in I\}$.

In order to determine a lower bound B on the cardinality of V, we study the number of solutions $X \in \mathbb{Z}_P$ of the linear system $X \equiv s_i \bmod p_i$ for all $i \in I$. From the Chinese remainder theorem, it follows that the solutions of this system are $X_0 + r \cdot \prod_{i \in I} p_i$, where X_0 is the unique solution of the system in $\mathbb{Z}_{\prod_{i \in I} p_i}$ and $r \in [0, \ldots, C(I) - 1]$ or $[0, \ldots, C(I)]$ depending on the value of X_0. Therefore, $B = C(I)$.

Similarly, in order to determine an upper bound A on the number of elements $X \in V$ such that $X \bmod p_0$, we study the number of solutions $r \in [0, \ldots, C(I)]$ of the system $s \equiv X_0 + r \cdot \prod_{i \in I} p_i \bmod p_0$, or equivalently $r \equiv (s - X_0) \cdot (\prod_{i \in I} p_i)^{-1} \bmod p_0$. It follows that $A = \lfloor (C(I)+1)/p_0 \rfloor + 1$.

Eventually, we have $P(S = s|s_i : i \in I) \leq A/B = (\lfloor (C(I)+1)/p_0 \rfloor + 1)/C(I)$. By definition

$$H(S|s_i : i \in I) \geq \log(C(I)/(\lfloor (C(I)+1)/p_0 \rfloor + 1)).$$

Moreover, s is uniformly chosen in $\mathbb{Z}_{p_0}$, therefore $H(S) = \log(p_0)$. We find

$$\Delta_{(t,p_0,\ldots,p_l)}(s_i : I) \leq \log\left(p_0 \cdot (\lfloor (C(I)+1)/p_0 \rfloor + 1)/C(I)\right).$$

The case $C(I) = 0$ is trivial since the set of shares $\{s_i : i \in I\}$ enables us to recover the secret exactly using the Chinese remainder theorem. Hence, it follows that $H(S|s_i : i \in I) = 0$.

□

In the remainder of the text, we only consider threshold schemes with consecutive primes. We will refer to such threshold shemes using the notation $(Share_{(t+1,l,p_0,1^{|p_0|})}, Comb_{(t+1,l,p_0,1^{|p_0|})})$.

Using the previous Lemma, we can prove the asymptotical perfection of the scheme when the secret is uniformly chosen and the primes p_i's are consecutive. Remind that $|p_i|$ denotes the number of bits of p_i.

Theorem 1. *The $(t+1, l)$ threshold scheme based on the Chinese remainder theorem with consecutive primes p_i's is asymptotically perfect with respect to the uniform probability on $\mathbb{Z}_{p_0}$.*

More formally, for all $\epsilon > 0$, there exists some $k_0 \geq 0$ such that for all threshold schemes $(Share_{(t+1,l,p_0,1^{|p_0|})}, Comb_{(t+1,l,p_0,1^{|p_0|})})$ with $|p_0| \geq k_0$ we have for all $I \subset \{1, \ldots, l\}$ with $|I| \leq t$,

$$|\Delta_{(t+1,l,p_0,1^{|p_0|})}(s_i : i \in I)| \leq \epsilon.$$

Proof. First, we have that $\Delta_{(t,p_0,\ldots,p_l)}(s_i : i \in I) \geq 0$ by the remark on the definition (2).

Define $C^*(I) \stackrel{\triangle}{=} \prod_{i=0}^{t} p_i / \prod_{v \in I} p_v$ and $C(I) \stackrel{\triangle}{=} \lfloor C^*(I) \rfloor$.

By hypothesis, the primes p_i's $(0 \leq i \leq l)$ are consecutive. It follows that $p_{i+1} < p_i + p_i^{1/2+1/21}$ for p_i sufficiently large (see [R88], p. 193).

Consider the case $|I| = t$.

If $I = \{1, \ldots, t\}$, it follows from the Chinese remainder theorem that $\Delta_{(t,p_0,\ldots,p_l)}(s_i : i \in I) = 0$.

Assume $I \neq \{1, \ldots, t\}$. Because the primes p_i's are consecutive, it holds that $C(I) > 0$, for all sufficiently large prime p_0. Also, $C(I) = \lfloor p_0 \cdot \prod_{i=1}^{t} p_i / \prod_{i \in I} p_i \rfloor \leq \lfloor p_0 \cdot p_t/(p_t+2) \rfloor$. Note that $\lfloor p_0 \cdot p_t/(p_t+2) \rfloor < p_0 - 1$ if and only if $p_t/(p_t+2) < (p_0-1)/p_0$. This last inequality is equivalent to $p_t < 2p_0 - 2$, which holds for p_0 sufficiently large because the primes p_i's are consecutive. Therefore $C(I) < p_0 - 1$, for all prime p_0 sufficiently large and for all $I \neq \{1, \ldots, t\}$ such that $|I| = t$.

We deduce that $p_0 \cdot (\lfloor (C(I)+1)/p_0 \rfloor + 1)/C(I) = p_0/C(I)$, for all sufficiently large prime p_0. Using Lemma 1, we have

$$\Delta_{(t,p_0,\ldots,p_l)}(s_i : I) \leq \log(p_0/C(I)). \tag{2}$$

Because the primes p_i's are consecutive, it holds that, for all sufficiently large p_0

$$p_0^{t+1}/(p_0^t + \sum_i a_i p_0^{b_i}) \leq C^*(I)$$

where $a_i \in \mathbb{R}^+$ and $0 < b_i < t$, for all i.

For all sufficiently large primes p_0 and for all $I \neq \{1, \ldots, t\}$ with $|I| = t$, it holds

$$p_0/C(I) \leq p_0/(C^*(I) - 1) \leq p_0(p_0^t + \sum_i a_i p_0^{b_i})/(p_0^{t+1} - (p_0^t + \sum_i a_i p_0^{b_i})).$$

Applying the logarithm operator and using (2), we get

$$\Delta_{(p_0,\ldots,p_l)}(s_i : i \in I) \leq \log(p_0(p_0^t + \sum_i a_i p_0^{b_i})/(p_0^{t+1} - (p_0^t + \sum_i a_i p_0^{b_i}))).$$

The upper bound converges to 0 when p_0 converges to infinity.

Consider the case $|I| < t$. It holds that $\Delta_{(p_0,\ldots,p_l)}(s_i : i \in I) \leq \log((C^*(I) + 2 + 2p_0)/(C^*(I) - 1))$. Note that $2 + 2p_0$ and -1 are negligible in front of $C^*(I)$. Therefore this upper bound converges to 0 when the prime p_0 converges to infinity. The result follows. □

The next theorem tells us that the threshold scheme is moreover asymptotically ideal.

Theorem 2. *The $(t + 1, l)$ threshold scheme based on the Chinese remainder theorem with consecutive primes p_i's is asymptotically ideal with respect to the uniform probability on $\mathbb{Z}_{p_0}$.*

More formally,

- *$(Share_{(t+1,l,p_0,1^{|p_0|})}, Comb_{(t+1,l,p_0,1^{|p_0|})})$ is asymptotically perfect with respect to this probability distribution and,*
- *for all $\epsilon > 0$, there exists some $k_0 \geq 0$ such that for all p_0 with $|p_0| \geq k_0$ the consecutive primes p_i's satisfy $p_i/p_0 \leq 1 + \epsilon$ for $i = 0, \ldots, l$.*

Proof. The first part comes from the previous theorem.

Let us prove the second part. The primes p_i's $(0 \leq i \leq l)$ are consecutive, it follows that $p_{i+1} < p_i + p_i^{1/2+1/21}$ for p_i's sufficiently large (see [R88], p. 193). This means that for all $j \geq 0$, $p_j < p_0 + f(p_0)$ where $f(p_0)/p_0 \geq 0$ converges to 0 if p_0 converges to infinity. The result follows. □

Eventually, we prove that this scheme is perfect zero-knowledge when the secret is uniformly selected and the primes p_i's are consecutive. Goldreich *et al.* [GRS00] proved that for the $(t + 1, l)$ threshold scheme with consecutive primes p_i's, $t - 1$ shares give no information on the secret from a complexity theoretic viewpoint. By improving the last part of their proof, we are able to prove that in fact t shares give no information on the secret.

Theorem 3. *The threshold scheme $(t+1, l)$ based on the Chinese remainder theorem with consecutive primes p_i's is perfect zero-knowledge.*

More formally, there exists a set of polynomial algorithms, denoted by $Sim_{(t+1,l,p_0,1^{|p_0|})}$, such that for all polynomials $p(\cdot)$, there exists some $k_0 \geq 0$ such that for all threshold schemes $(Share_{(t+1,l,p_0,1^{|p_0|})}, Comb_{(t+1,l,p_0,1^{|p_0|})})$ and $|p_0| \geq k_0$, we have

for all $s \in \mathbb{Z}_{p_0}$ and for all $I \subset \{1, \ldots, l\}$ such that $|I| \leq t$,

$$\frac{1}{2} \sum_{s_I \in \mathbb{Z}_{p_I}} |P(I_{|Share_{(t+1,l,p_0,1^{|p_0|})}(s)} = s_I) - P(Sim_{(t+1,l,p_0,1^{|p_0|})} = s_I)| \leq \frac{1}{p(|p_0|)},$$

where $I_{|(s_1,\ldots,s_l)}$, $\mathbb{Z}_{p_I}$ and s_I represent respectively $(s_{i_1}, \ldots, s_{i_j})$, $\mathbb{Z}_{p_{i_1}} \times \cdots \times \mathbb{Z}_{p_{i_j}}$ and $(s_{i_1}, \ldots, s_{i_j})$ for $I = \{i_1, \ldots, i_j\}$.

Proof. Define $K \stackrel{\triangle}{=} \prod_{i=1}^{t} p_i$, $M(I) \stackrel{\triangle}{=} \prod_{i \in I} p_i$. The notation $[x]_y$ indicates the minimum positive representant of x mod y.

First, note that $I_{|Share_{(t+1,l,p_0,1^{|p_0|})}(s)} = ([Y(s)]_{p_i} : i \in I)$, where $Y(s) \in \mathbb{Z}_{p_0 \cdot K}$ is the random variable computed according to the sharing phase on the secret $s \in \mathbb{Z}_{p_0}$.

We claim that $Sim_{(t+1,l,p_0,1^{|p_0|})} = ([Y(s')]_{p_i} : i \in I)$, where $Y(s') \in \mathbb{Z}_{p_0 \cdot K}$ is the random variable computed according to the sharing phase on the value $s' \in \mathbb{Z}_{p_0}$ chosen at random.

Therefore, we have to prove that for all polynomial $p(\cdot)$, there exists a $k_0 \geq 0$ such that for all p_0 with $|p_0| \geq k_0$, we have,

for all $s \in \mathbb{Z}_{p_0}$ and for all $I \subset \{1, \ldots, l\}$ with $|I| \leq t$,

$$\frac{1}{2} \sum_{s_I \in \mathbb{Z}_{p_I}} |P([Y(s)]_{p_i} = s_i : i \in I) - P([Y(s')]_{p_i} = s_i : i \in I)| \leq \frac{1}{p(|p_0|)}.$$

Let $I \subset \{1, ..., l\}$ such that $|I| \leq t$.

By the Chinese remainder theorem, there is a bijection between $\mathbb{Z}_{M(I)}$ and $\prod_{i \in I} \mathbb{Z}_{p_i}$.

Therefore, the left hand side of the previous inequality is equivalent to:

$$\frac{1}{2} \sum_{z=0}^{M(I)-1} |P([Y(s)]_{M(I)} = z) - P([Y(s')]_{M(I)} = z)|. \tag{3}$$

Note that

$$|P([Y(s)]_{M(I)} = z) - P([Y(s')]_{M(I)} = z)| \leq$$
$$|P([Y(s)]_{M(I)} = z) - P(U_{M(I)} = z)| + |P([Y(s')]_{M(I)} = z) - P(U_{M(I)} = z)|,$$

where $U_{M(I)}$ is a uniform random variable on $\mathbb{Z}_{M(I)}$.

Let us find an upper bound on the first term of the right hand side of the inequality.

Because of the bijection between $\prod_{i=0}^{t} \mathbb{Z}_{p_i}$ and $\mathbb{Z}_{p_0 K}$, $Y(s) = s + r \cdot p_0$ with $r \in_R \mathbb{Z}_K$. Note that r is the only random element in this expression. The addition

of s and the multiplication by p_0 together induce a permutation of the elements of $\mathbb{Z}_{M(I)}$. Therefore,

$$\sum_{z=0}^{M(I)-1} |P([Y(s)]_{M(I)} = z) - P(U_{M(I)} = z)| =$$

$$\sum_{z=0}^{M(I)-1} |P([r]_{M(I)} = z) - P(U_{M(I)} = z)| \tag{4}$$

Splitting the sum into two parts, we get

$$\begin{aligned}(4) = &\textstyle\sum_{z=0}^{[K]_{M(I)}-1} |P([r]_{M(I)} = z) - P(U_{M(I)} = z)| \\ &+ \textstyle\sum_{z=[K]_{M(I)}}^{M(I)-1} |P([r]_{M(I)} = z) - P(U_{M(I)} = z)|\end{aligned}$$

Note that if $0 \le z \le [K]_{M(I)} - 1$,

$$P([r]_{M(I)} = z) = (((K - [K]_{M(I)})/M(I)) + 1)/K,$$

and if $[K]_{M(I)} \le z \le M(I) - 1$,

$$P([r]_{M(I)} = z) = (K - [K]_{M(I)})/M(I)K.$$

Also,

$$P(U_{M(I)} = z) = 1/M(I).$$

Therefore,

$$(4) = 2\left([K]_{M(I)}/K - [K]^2_{M(I)}/M(I)K\right). \tag{5}$$

Because, the primes are consecutives, $p_{i+1} < p_i + p_i^{1/2+1/21}$. It follows that $M(I) < p_0^{|I|} + \sum_i a_i p_0^{b_i}$, where $a_i \in \mathbb{R}_0^+$ and $b_i < |I|$, for all i.

If $|I| < t$, for all p_0 large enough, we have

$$M(I) < p_0^{|I|} + \sum_i a_i p_0^{b_i} < p_0^t < K.$$

Therefore,

$$(3) \le 2M(I)/K \le 2(p_0^{|I|} + \sum_i a_i p_0^{b_i})/p_0^t. \tag{6}$$

If $|I| = t$, $M(I) > K$ because the primes increase.

Therefore,

$$(3) \le 2(M(I) - K)/K \le 2(p_0^t + \sum_i a_i p_0^{b_i} - p_0^t)/p_0^t. \tag{7}$$

In both cases, the upper bound behaves as the inverse of an exponential in $|p_0|$, where $|p_0|$ denotes the number of bits of p_0. Also, both bounds depend neither on s nor on I. Therefore, (3) is bounded by the maximum of the bounds (6) and (7) over all $I \subset \{1, \ldots, l\}$ with $|I| \le t$. The result follows. □

6 Conclusions

In this paper, we analyzed the security of a threshold scheme based on the Chinese remainder theorem in the context of theoretical cryptography. We have introduced the definition of an asymptotically perfect and asymptotically ideal schemes that are natural relaxations of perfect and ideal schemes. We have proved that the scheme based on the CRT is asymptotically ideal and perfect zero-knowledge if the parameters of the system satisfy a natural condition. Those properties imply that any set of t shares of a $(t+1, l)$ threshold scheme based on the Chinese remainder theorem gives no information on the secret.

Acknowledgements

The authors would like to thank Philippe Delsarte and Jacques Stern for their interest in this work and for their valuable suggestions. Also, they would like to thank Madhu Sudan for answering some questions. We are also grateful to the anonymous referees for their valuable remarks. Michael Quisquater is a F.W.O.-research fellow, sponsored by the Fund for Scientific Research – Flanders (Belgium).

References

AB83. Asmuth, C., Bloom, J.: A modular approach to key safeguarding. *IEEE Trans. inform. Theory*, 1983, **IT-29**, pp. 208–210.

B79. Blakley, G.R.: Safeguarding cryptographic keys. *AFIPS Conf. Proc.*, 1979, **48**, pp. 313–317.

DF94. Desmedt, Y., Frankel, Y.: Homomorphic zero-knowledge threshold schemes over any finite abelian group. *SIAM J. discr. math.*, 1994, **7**, pp. 667–679.

G68. Gallager, R.G.: Information Theory and Reliable Communication. Willey, 1968.

GB01. Goldwasser S., Bellare M.: Lectures Notes on Cryptography. 1996–2001. http://www-cse.ucsd.edu/users/mihir/papers/gb.html.

GRS00. Goldreich, O., Ron, D., Sudan, M.: Chinese remainder with errors. *IEEE Trans. Inform. Theory*, 2000, **IT-46**, pp. 1330–1338.

KGH83. Karnin, E.D., Greene, J.W., Hellman, M.E.: On secret sharing systems. *IEEE Trans. Inform. Theory*, 1983, **IT-29**, pp. 35–41.

M82. Mignotte, M.: How to share a secret. Advances in Cryptology – Eurocrypt'82, LNCS, 1983, **149**, Springer-Verlag, pp. 371–375.

R88. Ribenboim, P.: The Book of Prime Number Records. Springer-Verlag, 1988.

S79. Shamir, A.: How to share a secret. *Commun. ACM* 1979, **22**, pp. 612–613.

SV88. Stinson, D.R., Vanstone S.A. *SIAM J. discr. math.*, 1988, **1**, pp. 230–236.