SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2016; **9**:4416–4427
Published online 4 October 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1617

RESEARCH ARTICLE

A CRT-based verifiable secret sharing scheme secure against unbounded adversaries

Oğuzhan Ersoy[1,2]*, Thomas Brochmann Pedersen[1], Kamer Kaya[3], Ali Aydın Selçuk[4] and Emin Anarim[2]

[1] TÜBİTAK BİLGEM, Kocaeli, Turkey
[2] Electrical & Electronics Engineering Dept., Boğaziçi University, Istanbul, Turkey
[3] Faculty of Engineering and Natural Sciences, Sabancı University, Istanbul, Turkey
[4] Dept. of Computer Engineering, TOBB University of Economics and Technology, Ankara, Turkey

ABSTRACT

For commitments on secrets, statistical hiding is a must when we are dealing with a long-term secret or when the secret domain is small enough for a brute-force attack by a powerful adversary. Unfortunately, all the Chinese Remainder Theorem-based verifiable secret sharing schemes in the literature are either insecure or suffer from the vulnerability of computationally hiding commitments. To the best of our knowledge, there exist five such studies where two of them were already proven to be insecure. In this work, we first show that two of the remaining schemes are also insecure, that is, the schemes reveal information on the secret even when the adversary is passive. In addition, the remaining one is only secure against a computationally bounded adversary which can be a problem for secret sharing schemes requiring long-term secret obscurity or using small secret domain. We propose a modification for the latter scheme and prove that the modified scheme is a secure verifiable secret sharing scheme against an unbounded adversary. Lastly, as an application, we show how to use the new scheme for joint random secret sharing and analyze the practicality and efficiency of the proposed schemes. Copyright © 2016 John Wiley & Sons, Ltd.

KEYWORDS
verifiable secret sharing; Chinese Remainder Theorem; Asmuth-Bloom; statistically hiding commitments; joint random secret sharing

***Correspondence**
Oğuzhan Ersoy, Electrical & Electronics Engineering Dept., Boğaziçii University, Istanbul, Turkey.
E-mail: oguzhan.ersoy@boun.edu.tr

1. INTRODUCTION

Secret sharing schemes (SSS) play an important role in cryptosystems, especially for safeguarding keys. Many systems are vulnerable to disclose of the single master key by an accident or an attacker. The result of a disclosure would be catastrophic for crucial cases like launching a nuclear missile. Secret sharing precludes a single point of failure by splitting the master secret into several shares. The notion of secret sharing is important in many cryptographic protocols such as multiparty computation, for example, [1–3].

An SSS involves a *dealer* who has a *secret*, a set of *participants* that the secret is shared amongst, and a collection of the authorized subsets of the participants which is called the *access structure*. In threshold cryptography, the access structure is defined by a threshold that is the minimum cardinality of each authorized set.

Shamir[4] and Blakley[5] proposed the first SSSs in 1979. Shamir's SSS is based on Lagrange interpolation, whereas Blakley's scheme is based on hyperplane geometry. There are also Chinese Remainder Theorem (CRT) based SSSs such as Mignotte[6] and Asmuth-Bloom[7].

The dealer in an SSS has a crucial impact on the system; in the malicious case, the dealer may forge the shares of the participants and misdirect them. The need of a trusted dealer raises practical privacy and authenticity concerns for the system. In addition to a malicious dealer, the participants can also cheat during the reconstruction phase. In order to overcome a corrupted dealer and participants, the concept of verifiable secret sharing (VSS) is introduced by Chor *et al.,* based on Shamir's SSS [8]. A VSS scheme enables participants to check the validity of the shares during the distribution and reconstruction phases. Because of its simplicity and provable security, VSS schemes are exploited in several systems like multi-party computation protocols and ad hoc networks[9,10].

1.1. Motivation and our contributions

Although Shamir's SSS has long had verifiable variants[8,11–13], many CRT-based VSS proposals lack proper security. To the best of our knowledge, there are five VSS schemes based on CRT in the literature[14–18]. Kaya and Selçuk already show that[15] and[16] are not robust against a corrupted dealer[14]. In this paper, we first show that even the most recent ones, for example,[17,18] are not secure and robust because the secret is simply revealed to an adversary with $t - 1$ shares. Therefore, the best CRT-based VSS we have is still the one proposed in [14] which is only secure against an adversary with bounded computational power. In particular, a *computationally unbounded* adversary can extract the secret by using the information revealed by the scheme. As it can be seen from the previous works in the literature and attacks on these schemes in this paper, designing CRT-based VSS construction is not a straightforward task.

In this work, we use a *statistically hiding and computationally binding commitment scheme* to have a CRT-based VSS and prove that the proposed scheme is secure for an unbounded adversary which makes it the first fully secure verifiable scheme based on CRT. A statistically hiding commitment is crucial when we are dealing with a long-term secret or when the secret domain is small enough for a brute-force attack by a powerful adversary; for example, such an adversary can find solutions x to the equation $g^x = h$ given the elements g and h of a finite cyclic group G with a sufficiently small order. Considering the recent algorithms for the discrete logarithm problem (DLP), for example,[19], for various fields, revealing g^x for a secret x is not a good idea. Unfortunately, this is the approach followed by the only secure CRT-based VSS [14] from the literature to the best of our knowledge. With statistical hiding, we have the advantage of a committed value remaining hidden forever [20]. As computational bounds increase day by day, it is always important to provide security against unbounded adversaries.

Because a VSS implies robustness against a corrupted dealer, a typical application is joint random secret sharing (JRSS) where playing the role of the dealer, all users jointly generate and share a random secret, for example,[21,22]. A CRT-based JRSS primitive has already been proposed in the literature[14]. We will show that our approach is applicable to JRSS and yields a scheme that is also secure against an unbounded adversary which is not the case for the scheme of[14].

The rest of the paper is organized as follows Section 2 introduces the necessary background on secret sharing, Asmuth-Bloom SSS, and summarizes the related work. The security analysis of the existing CRT-based VSS schemes and their weaknesses are given in Section 3. Sections 4 and 5 explain the proposed CRT-based VSS and JRSS schemes, respectively, in detail. Section 6 concludes the paper.

2. BACKGROUND

An SSS consists of two phases: in the *distribution phase*, the dealer splits the secret into n pieces by using the sharing function and delivers shares to the participants via a secure channel (discrete channel for each participant). In the *reconstruction phase*, a qualified group of participants can reconstruct the secret with the help of the reconstruction function. A *perfect secret sharing scheme* should satisfy the following two conditions:

1. *Correctness*: Any qualified group of participants can reconstruct the secret.
2. *Perfect Privacy*: No unqualified group of participants can obtain any information about the secret.

A (t, n) threshold scheme satisfies that any t shares can recover the secret and less can obtain no information about the secret. Some of the well-known threshold schemes are Shamir's SSS, Blakley's SSS, and Asmuth-Bloom SSS.

We call an SSS *verifiable* if the participants can verify the consistency of their shares. Formally, a VSS scheme has a *verification phase* which can be defined by the following conditions given in [11]:

(1) If the dealer follows the distribution phase, and the dealer and participant i follows the verification protocol, then participant i accepts his share with probability one.

(2) For any two qualified groups of participants G_1 and G_2 such that all shares included are accepted, the following could happen with at most a negligible probability: if s_1 is the recovered secret by G_1 and s_2 by G_2, then $s_1 \neq s_2$.

Adversary model and security: For the security proofs in this paper, we have two types of adversaries:

- A *passive adversary* can access all the information she has, but she does not make them deviate from the protocol. Hence, a passive adversary is *honest but curious*.
- An *active adversary* can access all the information they have and send/broadcast messages on their behalf. Hence, an active adversary is not only curious but also dishonest, that is, she may try to cheat and deviate from the protocol.

We assume that an adversary can corrupt at most $t - 1$ users [23,24]. Because any t users can open the secret, an adversary having t users does not make sense for this scheme. Without loss of generality, we also assume that secure private channels exist between each user pair. The share of each participant is sent via these channels; hence, no one but the participant herself and the dealer knows her share unless she is corrupted. In addition, we assume that a secure and robust broadcast channel exists and when data is broadcast, each user will read the same value. In particular, an active adversary cannot send two different values to two different users in a broadcast message. For the rest of the paper, we will use the notation summarized in Table I.

Chinese Remainder Theorem: Let $m_1, \ldots, m_k$ be pairwise co-primes, and $b_1, \ldots, b_k \in \mathbb{Z}$. The system of equations

$$\begin{aligned} x &\equiv b_1 \bmod m_1 \\ &\vdots \\ x &\equiv b_k \bmod m_k \end{aligned}$$

has a unique solution in $\mathbb{Z}_{M_{(k)}}$ which can be found by the following formula:

$$x = \sum_{i=1}^{k} \alpha_i \cdot \beta_i \cdot b_i \bmod M_{(k)}$$

where $M_{(k)} = \prod_{i=1}^{k} m_i$ and $\alpha_i = \frac{M_{(k)}}{m_i}$, $\beta_i = \left[\frac{m_i}{M_{(k)}}\right]_{m_i}$. Here, $\left[\frac{m_i}{M_G}\right]_{m_i}$ is obtained by first dividing M_G by m_i in $\mathbb{Z}$ and compute the inverse of the result in $\mathbb{Z}_{m_i}$.

2.1. Asmuth-Bloom secret sharing scheme

The Asmuth-Bloom scheme is a CRT-based SSS as shown in Figure 1. Because CRT with t moduli guarantees a unique solution for $y < M_{(t)}$ ($M_{(t)} = \prod_{i=1}^{t} m_i$), the secret

Table I. Notation.

Notation	Explanation
n	The number of users/participants.
t	The threshold, the minimum number of users required to construct the secret.
S	The secret to be shared.
p	A prime specifies the domain of $S \in \mathbb{Z}_p$.
m_i	The prime modulus for user i.
q_i	A safe prime, $2m_i + 1$.
Q	$\prod_{i=1}^{n} q_i$.
$M_{(r)}$	$\prod_{i=1}^{r} m_i$.
$M^{(s)}$	$\prod_{i=1}^{s} m_{n-i+1}$.
y	$d + A \cdot p$, where A is the blinding factor.
y_i	$y \bmod m_i$, the share of user i.
$E(y, r)$	The commitment value of an integer y.
$Range\_Proof(a, R)$	The Boudot's range proof for a being in the range of $(0, R)$.
G	A coalition of users.
M_G	The modulus of coalition G, $\prod_{i \in G} m_i$.
$\lvert G \rvert$	The cardinality of G.
$\mathbb{Z}_a$	The set of all congruence classes modulo a.
$\mathbb{Z}_a^*$	The set of all non-zero congruence classes modulo a.
$[\cdot]_a$	The arithmetic inside is performed in $\mathbb{Z}_a$.

Distribution Phase

To share a secret S, the dealer chooses a set of integers $(p, m_1, m_2, \cdots, m_n)$ (Asmuth-Bloom sequence) such that:

(1) $m_1 < m_2 < \cdots < m_n$ and $S \in \mathbb{Z}_p$.
(2) $gcd(m_i, m_j) = 1$ $(\forall i \neq j)$.
(3) $gcd(p, m_i) = 1$ $(\forall i)$.
(4) $M_{(t)} > p \cdot M^{(t-1)}$.

The dealer chooses an arbitrary A such that $y = S + A \cdot p < M_{(t)}$.
The dealer computes and distributes shares as $y_i = y \bmod m_i \quad (\forall i)$

Reconstruction Phase

A qualified group G can reconstruct S by

$$y = \left[\sum_{P_i \in G} \frac{M_G}{m_i} \cdot \left[\frac{m_i}{M_G}\right]_{m_i} \cdot y_i\right]_{M_G} \quad \text{and } S = y \bmod p$$

Figure 1. Asmuth-Bloom secret sharing scheme.

DOI: 10.1002/sec

S can be extracted by computing first y and then $y \bmod p$. The SSS has the following properties:

Theorem 1 ([7]). *In Asmuth-Bloom SSS, a passive adversary cannot eliminate any candidate from $\mathbb{Z}_p$ for the secret.*

Theorem 2 ([25]). *Asmuth-Bloom SSS is not perfect: the possible secret candidates do not have the same probability for an unqualified group B having less than t shares; every secret candidate will be obtained either $\left\lfloor \frac{M_{(t)}}{pM_B} \right\rfloor$ or $\left\lfloor \frac{M_{(t)}}{pM_B} \right\rfloor + 1$ times when $y \bmod p$ is computed for each possible y candidate.*

Let $\Pr_{(B,S)}(S')$ be the probability of $S' \in \mathbb{Z}_p$ is equal to the shared secret S from an unqualified group B's point of view. For a perfect SSS, $\Pr_{(B,S)}(S') = \Pr_{(B,S)}(S)$ for all possible combinations of S, S', and B. We should point out that, from Theorem 2, the number of appearances of the possible secret values can differ by one and the secret candidates are (negatively or positively) biased to be the secret. Hence, the secret candidates are not be equally likely to be the secret. This can be a problem especially when $\frac{M_{(t)}}{pM_B}$ is small and the bias is large. To alleviate this, Quisquater *et al.,* proposed that $p, m_1, \ldots, m_n$ should be chosen as consecutive primes to make the scheme *asymptotically perfect*[25]. That is, for every B and positive ϵ value, the dealer can choose a prime p such that $\Pr_{(B,S)}(S') - \Pr_{(B,S)}(S) < \epsilon$. For similar reasons, Kaya and Selçuk [26] proposed to change the fourth condition of the *distribution phase* with

$$M_{(t)} > p^2 \cdot M^{(t-1)} \tag{1}$$

In this case, the scheme becomes *statistically secure*, that is, the statistical distance between the distribution $\Pr_{(B,S)}(.)$ and uniform distribution is smaller than a given ϵ with a carefully chosen p.

Theorem 3 ([26]). *The modified Asmuth-Bloom scheme with (1) is a statistically secure secret sharing scheme against a passive adversary.*

Here, we sightly modified the statement of the theorem, but the meaning and the proof are almost the same.

2.2. Related work

The original versions of the Asmuth-Bloom and Mignotte SSSs [6,7] are not verifiable. The first CRT-based VSS scheme has been proposed by Qiong *et al.,* in [15] which uses a similar approach to Pedersen's polynomial-evaluation-based VSS[11]. Later, Iftene proposed the only VSS based on Mignotte's scheme [16] and showed that the security of the scheme is based on the hardness of the DLP.

Kaya and Selçuk[14] proposed another VSS based on the Asmuth-Bloom scheme with robustness analyses of the Quiong *et al.,* and Iftene's schemes[15,16]. They showed that the existing schemes are not robust against a malicious dealer because the dealer can distribute inconsistent shares that lead to different reconstructed secrets for different qualified subsets. To solve this problem, they used a *range proof* to prove that the y value is in the desired (CRT) range. Their scheme assures the validity of the shares not only for malicious participants (reconstruction phase) but also for a malicious dealer (distribution phase).

Recently, two VSS schemes based on Asmuth-Bloom have been proposed [17,18]. In 2014, Harn *et al.,* proposed a very efficient scheme aiming at detecting malicious behavior of the dealer with the assumption that the participants act honestly (which already makes the scheme insecure against an active adversary)[17]. The scheme uses additional verification secrets generated within a given range. Based on these ranges, the participants can have a range guarantee on y. This assures that the dealer cannot distribute inconsistent shares. With the same motivation, Liu *et al.,*[18] proposed a VSS where every participant adds an adjusting value (from a guaranteed range, because the participants are again assumed to be honest) to his share, then all the participants recover an adjusted value for y which is supposed to give no additional information but the range of y.

As mentioned before, VSS schemes which do not employ a CRT-based SSS already exist in the literature. However, CRT-based SSSs such as Asmuth-Bloom are fundamentally different when compared with these SSSs. Hence, designing extensions and other functionalities, such as function sharing, JRSS, and secure multi-party computation, for CRT-based schemes is a challenging task and indeed an interesting problem which recently gained more attention. In fact, as we show in this work, providing the necessary security requirements is hard even for VSS which is arguably a simpler scheme compared with the aforementioned extensions: if one is not careful, she can design an insecure protocol with hidden weaknesses.

2.3. Boudot's range proof

As mentioned in the previous section, a crucial part of the VSS scheme of [14] is the proof that the blinded secret, y, is in the allowed range. Whereas [14] uses the range proof of [27], we use the one presented by Boudot in [28].

Boudot[28] proposed an efficient and non-interactive technique to prove that a committed number lies within an interval. He used the Fujisaki–Okamoto integer commitment scheme[29], where the commitment of an integer y is as follows:

$$D = D(y, r) = g_N^y h_N^r \bmod N,$$

where g_N is an element of high order in $\mathbb{Z}_N^*$, h_N is an element of the group generated by g_N, r is a random integer, and N is an RSA composite whose factorization is unknown. As proved in[28,29], this commitment scheme is statistically hiding and computationally binding assuming that the prime factorization of N is unknown. That is, the committer cannot find another valid proof unless he is computationally unbounded, and the receiver of the commitment cannot distinguish the discrete logarithm, that is, y, from a random value.

The commitment scheme we use, however, is slightly different: let $Q = \prod_{i=1}^{n} q_i$ be a composite number. The commitment to a value, y, is

$$E = E(y, r) = g^y h^r \bmod Q$$

where g is an element in $\mathbb{Z}_Q^*$, and h is an element of the group generated by g. In [28], the author shows how to reduce a range proof for the commitment E to a range proof for the commitment D by a zero-knowledge proof of equality of committed values (see section 3.2 and appendix A of [28]).

3. ANALYSIS OF THE CRT-BASED VERIFIABLE SECRET SHARING SCHEMES

3.1. Kaya and Selçuk's verifiable secret sharing scheme

Instead of Boudot's range proof, Kaya and Selçuk[14] use the range proof technique in[27] as a black box. Their algorithm can be seen in Figure 2.

Their scheme prevents malicious behavior of both dealer and participants in a way that misleading shares can be detected by the participants. Because the commitment is computationally hiding, the secret is leaked to an unbounded adversary. Furthermore, even a computationally bounded adversary can extract the secret from the commitment in the case of small sizes of p.

Lemma 4. *The order of $g \in \mathbb{Z}_Q$ is $M_{(n)}$.*

Proof Sketch. Let $ord(g) = d$ in $\mathbb{Z}_Q$. Because $g^d \equiv 1 \bmod q_i$, then $m_i \mid d$ (for all i's) which concludes to $M_{(n)} \mid d$.

Similarly, because $g^{M_{(n)}} \equiv 1 \bmod q_i$ (for all i's), then $g^{M_{(n)}} \equiv 1 \bmod Q$ by CRT which implies that $d \mid M_{(n)}$. Therefore, $d = M_{(n)}$. □

Lemma 5. *There is exactly one y value satisfying the commitment in mod $M_{(n)}$.*

Proof. Assume that y' and y'' satisfy the commitment such that $E(y') \equiv E(y'') \bmod Q$. By using Lemma 4:

$$\begin{aligned} E(y') \equiv E(y'') \bmod Q &\implies 1 = g^{y'-y''} \bmod Q \\ \implies ord(g) \mid y' - y'' &\implies y' \equiv y'' \bmod M_{(n)} \\ \implies y' = y'' \quad &\text{because} \quad y', y'' \in (0, M_{(t)}) \end{aligned}$$

which implies that only one element satisfies the commitment. □

Distribution Phase

The dealer chooses a set of integers $(p, m_1, m_2, \cdots, m_n)$ such that

- In addition to the modified Asmuth-Bloom requirements in [26], $q_i = 2 \cdot m_i + 1$ is a prime $(\forall i)$.

The dealer chooses an arbitrary A such that $y = S + A \cdot p < M_{(t)}$.
The dealer commits to $E(y) = g^y \bmod QN$ and $Range\_Proof(E(y), M_{(t)})$ where

- $Q = \prod_{i=1}^{n} q_i$ and $g \equiv g_i \bmod q_i$ where $g_i \in \mathbb{Z}_{q_i}^*$ is an element of order m_i.
- $Range\_Proof(E(y), M_{(t)})$ symbolizes the commitments in [27].

The dealer computes shares as $y_i = y \bmod m_i$ and privately distributes $(\forall i)$.
Then, he announces $E(y)$ and $Range\_Proof(E(y), M_{(t)})$.

Verification Phase

All participants check

- the validity of their shares: $g_i^{y_i} \overset{?}{\equiv} E(y) \bmod q_i$,
- the validity of range proof: $Range\_Proof(E(y), M_{(t)})$.

Reconstruction Phase

Let G be a group of participants gathered to reconstruct the secret,
Share of $P_i \in G$ is verified by other participants: $g_i^{y_i} \overset{?}{\equiv} E(y) \bmod q_i$.
After all the shares are verified, G may reconstruct S using CRT.

Figure 2. Kaya and Selçuk's verifiable secret sharing scheme.

DOI: 10.1002/sec

Theorem 6. *Kaya and Selçuk's VSS scheme is insecure against an unbounded passive adversary because the secret value can be found by $\mathcal{O}(p^2)$ exponentiations.*

Proof. From Theorems 1 and 2, it follows that an unqualified group, B, can compute $y \bmod M_B$; thus, there are at most $\frac{M_{(t)}}{M_B}+1$ possible solutions (denoted by PS_B) for group B ($|PS_B| \leq \frac{M_{(t)}}{M_B}+1$). By using Lemma 5, trying all values $y_B \in PS_B$ in the commitment would give the exact one: $E(y) \overset{?}{=} E(y_B) = g^{y_B} \bmod Q$.

For the VSS using the original Asmuth-Bloom sequence, the time complexity of the attack is $\mathcal{O}\left(\frac{M_{(t)}}{M_B}+1\right)$ which is $\mathcal{O}(p)$, whereas for the case of the modified Asmuth-Bloom given in [26], the time complexity will be $\mathcal{O}(p^2)$. □

An attack on this scheme is feasible for small (i.e., 32 bit) secret ranges and insecure against a bounded passive adversary.

3.2. The verifiable secret sharing scheme of Harn *et al.,*

The VSS scheme of Harn *et al.,*[17] aims to provide the range proof of the blinded secret, that is, it just assures that the dealer chooses y between 0 and $M_{(t)}$; all participants are assumed to be honest. The algorithm of Harn et al.,'s VSS can be seen in Figure 3. Detailed explanations can be found in [17].

Lemma 7. *The VSS* [17] *in Figure 3 is not a complete scheme. In the case of $y \geq M_{(t)} - M^{(t-1)}$, it is not possible to choose verification secrets satisfying the conditions in Equation (2).*

Proof. If the dealer chooses A arbitrary as supposed, there is a chance that $y \geq M_{(t)} - M^{(t-1)}$. In that case, there is no space for verification secrets. In other words, $M^{(t-1)} < S_i$ and $M_{(t)} - M^{(t-1)} \leq y$ implies $M_{(t)} < S_i + y$ contradicting with (2). □

A simple correction for the scheme would be to restrict y with $M_{(t)} - M^{(t-1)}$ instead of $M_{(t)}$. However, bounding y between $M^{(t-1)}$ and $M_{(t)} - M^{(t-1)}$ cause an attack in the case of $M_{(t)} \approx p \cdot M^{(t-1)}$. In order to implement an efficient Asmuth-Bloom scheme, the parameters should be chosen such that $M_{(t)}$ is approximately equal to $p \cdot M^{(t-1)}$. In that case, let $B = \{n-r+2, n-r+3, \ldots, n\}$ be an unqualified group of participants such that the group moduli M_B is equal to $M^{(t-1)}$, that is, B knows $y' = y \mod M^{(t-1)}$. Because $M^{(t-1)} < y < M_{(t)} - M^{(t-1)}$, the possible solution set of y is not more than $\{y' + M^{(t-1)}, \ldots, y' + (p-1)M^{(t-1)}\}$ for B. Here, there are at most $p-1$ possible solution for an unqualified group B.

Theorem 8. *Verification secrets leak information about the blinded secret y for a passive adversary.*

Proof. The blinded secret y can be restricted by the following:

- using the first part of the verification:

$$y \in \left(S_{max}^{(1)}, M_{(t)} - S_{max}^{(1)}\right) \qquad (2)$$

Distribution Phase

The dealer chooses a set of integers $(p, m_1, m_2, \cdots, m_n, S)$ in the same way as the original Asmuth-Bloom scheme.

The dealer chooses an arbitrary A such that $y = S + A \cdot p < M_{(t)}$.

The dealer chooses k verification secrets $S_1, \ldots, S_k$ such that

$$M^{(t-1)} < S_i < y \text{ and } S_i + y < M_{(t)}. \qquad (2)$$

The dealer computes shares as $y_{i,0} = y \mod m_i$, $y_{i,j} = S_j \mod m_i$ for $(j = 1, \ldots, k)$ and privately sends $\bigcup_{j=0}^{k}\{y_{i,j}\}$ to user i.

Verification Phase

All participants check the validity of the range of y:

First, they randomly split S_i's into two sets: $S_1^{(1)}, \ldots, S_{k/2}^{(1)}, S_1^{(2)}, \ldots, S_{k/2}^{(2)}$.

1. Then, open the first half of the verification secrets and check that $M^{(t-1)} \overset{?}{<} S_i^{(1)} \overset{?}{<} M_{(t)}$.
2. Divide the rest, into two sets ($S_{i_1}^{(2)}$'s, $S_{i_2}^{(2)}$'s) then calculate and check that $0 \overset{?}{<} y - S_{i_1}^{(2)}$ and $y + S_{i_2}^{(2)} \overset{?}{<} M_{(t)}$.

Reconstruction Phase

The same with the original scheme.

Figure 3. The verifiable secret sharing of Harn *et al.,*

where $S^{(1)}_{max} = \max_{i=1}^{k/2} S^{(1)}_i$.

- using the second part of the verification:

$$\begin{aligned} y &> \max_{i_1,i_2} \left\{K_{i_1}, K_{i_2} - S^{(2)}_{max,i_2}\right\} \\ y &< \min_{i_1,i_2} \left\{K_{i_1} - S^{(2)}_{max,i_1}, K_{i_2}\right\} \end{aligned} \tag{3}$$

where $K_{i_1} = y - S^{(2)}_{i_1}$, $K_{i_2} = y + S^{(2)}_{i_2}$, $S^{(2)}_{max,i_1} = \max_{i_1=1}^{k/4} S^{(2)}_{i_1}$ and $S^{(2)}_{max,i_2} = \max_{i_2=1}^{k/4} S^{(2)}_{i_2}$.

□

If S_is are chosen from a *wide range*, (2) is more useful to eliminate possible solutions, whereas (3) for the *narrow range* case.

In order to determine the range of S_is, the first part of the verification can be used. Because S is randomly divided into $S^{(1)}_i$s and $S^{(2)}_i$s, the distribution of $S^{(1)}_i$s gives some information about the range. In a similar manner, $S^{(2)}_{max,i_1}$ and $S^{(2)}_{max,i_2}$ can be approximated by $S^{(1)}_{max}$ which are required in the second elimination method (3).

3.3. The verifiable secret sharing scheme of Liu *et al.,*

In the scheme of[18], the dealer generates an Asmuth-Bloom sequence and selects the secret $S \in \mathbb{Z}_p$. Then, the dealer chooses an integer, A, in such a way that $y = S+Ap \in (M^{(t-1)} + 2T, M_{(t)} - 2T)$ where $T = \sum_{i=1}^{n} m_i$. The dealer sends share $y_i \equiv y \mod m_i$ to participant i.

In the verification phase, each participant selects an adjusting value, $\lambda_i \in (-(m_i-1), m_i-1)$, and broadcasts the value $M_{(n)}/m_i \cdot \left[m_i/M_{(n)}\right]_{m_i} \cdot y_i + \lambda_i$. Using the CRT formula, the participants can calculate an adjusted value $y^{(adj)}$ of y where:

$$y^{(adj)} = \left[\sum_{i=1}^{n} \frac{M_{(n)}}{m_i} \cdot \left[\frac{m_i}{M_{(n)}}\right]_{m_i} \cdot y_i + \lambda_i\right]_{M_{(n)}}$$

Participants check that $y^{(adj)} \overset{?}{\in} (M^{(t-1)} + T, M_{(t)} - T)$ which implies that $y \in (M^{(t-1)}, M_{(t)})$ and this is enough to say that the dealer cannot distribute inconsistent shares.

Theorem 9. *The VSS proposed by Liu et al.,* [18] *is insecure against a passive adversary.*

Proof. It is assumed that each participant and the dealer act honestly. Note that in the verification phase, every participant will learn $y^{(adj)}$.

An adversarial group B can compute $y' = y \mod M_B$ using their own shares. If $T \ll M_B$ (which in practice is satisfied for all of the unqualified groups with $t-1$ participants) then using y' and $y^{(adj)}$ values, the exact value of y can be easily found, because it is already known that $y^{(adj)} - T < y < y^{(adj)} + T$, and only one value in that interval satisfies the modulo condition y'. □

Note that because m_is are large primes and assumed to be close to each other, $|B| \geq 2$ implies that $T \ll M_B$. In any case, for $B = \{n-1, n\}$, this condition is already satisfied:

$$M_B = m_n \cdot m_{n-1} \gg m_n \cdot n > \sum_{i=1}^{n} m_i = T$$

4. CRT-BASED VERIFIABLE SECRET SHARING SECURE AGAINST AN UNBOUNDED ADVERSARY

As shown before, Kaya and Selçuk's VSS[14] is vulnerable because of the computationally hiding commitment they used. In the proposed scheme, we use Fujisaki–Okamoto commitment $E(y,r) = g^y \cdot h^r \mod Q$ and Boudot's range proof. Using $E(y,r)$ commitment in a VSS is challenging because it is supposed to be seen as a random value for any unauthorized attempt as well as assuring the validity of the commitment for any authorized access. That is why the random value r needs to be collectively constructed by the participants in a way that the participants can then verify their shares by using $E(y,r)$. The proposed VSS scheme is described in Figure 4.

4.1. Analysis of the proposed scheme

Our scheme is based on the following assumptions: the factorization of N is unknown, the DLP in $\mathbb{Z}^*_{q_i}$ is a computationally hard problem, and $\log_{g_i} h_i$ is not known by the dealer nor the participants. A simple way to construct such g_i and h_i's is the following: each participant and the dealer randomly chooses an $a^j \in m_i$ and broadcasts $g_i^{a^j}$ (for $j = 1, \ldots, n+1$), then h_i is computed by the product of all broadcast values for the i^{th} instant, that is, $a_i = \log_{g_i} h_i = \sum_{j=0}^{n+1} a^j \mod m_i$.

There are unique g and h in $\mathbb{Z}_Q$ satisfying $g \equiv g_i \mod m_i$, $h \equiv h_i \mod m_i$ for all i's, and they can be computed by the CRT formula:

$$\begin{aligned} g &= \left[\sum_{i=1}^{n} \frac{Q}{q_i} \cdot \left[\frac{q_i}{Q}\right]_{q_i} \cdot g_i\right]_Q \\ h &= \left[\sum_{i=1}^{n} \frac{Q}{q_i} \cdot \left[\frac{q_i}{Q}\right]_{q_i} \cdot h_i\right]_Q \end{aligned} \tag{4}$$

4.1.1. Correctness.

If the dealer and the participants are honest, then the verification phase passes.

DOI: 10.1002/sec

Distribution Phase

The dealer chooses a set of integers $(p, m_1, m_2, \cdots, m_n)$ such that

- In addition to the modified Asmuth-Bloom requirements in [26], $q_i = 2 \cdot m_i + 1$ is a prime $(\forall i)$.

The dealer chooses an arbitrary A such that $y = S + A \cdot p < M_{(t)}$.
Each participant chooses a random $r_i \in \mathbb{Z}_{m_i}$ and sends it to the Dealer
The dealer commits $E(y, r) = g^y \cdot h^r \bmod Q$ and $Range\_Proof(E(y, r), M_{(t)})$ where

- $r \equiv r_i \bmod m_i$ $(\forall i)$,
- $Q = \prod_{i=1}^{n} q_i$ and $g \equiv g_i \bmod q_i$ where $g_i \in \mathbb{Z}_{q_i}^*$ be an element of order m_i,
- $h \equiv h_i \bmod q_i$ where h_i is an element of the group generated by g_i,
- $Range\_Proof(E(y, r), M_{(t)})$ symbolizes the commitment scheme in [28].

The dealer computes shares as $y_i = y \bmod m_i$ and privately distributes $(\forall i)$.
Then, he announces $E(y, r)$, $Range\_Proof(E(y, r), M_{(t)})$.

Verification Phase

All participants check the validity of the range proof of y,
$Range\_Proof(E(y, r), M_{(t)})$, and the validity of their shares:

$$g_i^{y_i} \cdot h_i^{r_i} \overset{?}{\equiv} E(y, r) \bmod q_i. \tag{5}$$

Reconstruction Phase

Let G be a group of participants gathered to reconstruct the secret,
The share of user $i \in G$ is verified by other participants: $g^{y_i} \cdot h^{r_i} \overset{?}{\equiv} E(y, r) \bmod q_i$.
After all the shares are verified, G may reconstruct S using CRT.

Figure 4. Our proposed verifiable secret sharing scheme.

$$\begin{aligned} E(y, r) \bmod q_i &= g^y \cdot h^r \bmod Q \bmod q_i \\ &= g^y \cdot h^r \bmod q_i \\ &= g_i^y \cdot h_i^r \bmod q_i \\ &= g_i^{y_i} \cdot h_i^{r_i} \bmod q_i. \end{aligned}$$

Lemma 10. *The discrete logarithm of h in base g is co-prime to $M_{(n)}$.*

Proof. Let $a = log_g h$ be the discrete logarithm of h in base g and $log_{g_i} h_i = a_i$, in other words $g_i^{a_i} \equiv h_i \bmod q_i$, for each $i = 1, \ldots, n$. And then, it can be seen that $g^a \equiv h \bmod Q$ where $a \equiv a_i \bmod m_i$ for all i's. Because m_i's are primes and a_i's are not equal to zero, a and $M_{(n)}$ are co-primes. □

Theorem 1 states the security of Asmuth-Bloom secret sharing by showing the existence of a set of elements, $\mathcal{S}_B$, such that no element of $\mathcal{S}_B$ can be ruled out as a possible value of y. In Theorem 3, it is shown that the modified version of Asmuth-Bloom in [26] is a statistical SSS. We now show that the elements of $\mathcal{S}_B$ are also consistent with the additional information obtained by the adversary in the VSS scheme which concludes the following theorem:

Theorem 11. *For an unbounded passive adversary, no possible secret value can be ruled out, and the VSS is a statistical SSS.*

Proof. Let B be an unqualified group of participants $(|B| \le r - 1)$. B knows $\{y_i \equiv y \pmod{m_i} : i \in B\}$, $\{r_i \equiv r \pmod{m_i} : i \in B\}$, and the commitment $c = E(y, r) = g^y h^r \bmod Q$. Let $y' \in [0, M_B]$ be the unique solution to the congruences $y_i \equiv y' \pmod{m_i}$. Because the adversary is unbounded, he can compute the discrete logarithms $\log_g(c) = \log_g(E(y, r)) = \log_g(g^y h^r) = y + ar$ and $\log_g(h) = a$. It follows from (1) that

$$M_{(t)} > p^2 M^{(t-1)} \ge p^2 M_B.$$

Therefore, all elements of the set $\mathcal{S}_B = \{y', y' + M_B, \ldots, y' + p^2 M_B\}$ are possible solutions to the set of congruences $\{y_i \equiv y \pmod{m_i} : i \in B, y \in [0, M_{(t)}]\}$.

Likewise, we define r' as the unique solution in $\mathbb{Z}_{M_B}$ to the set of congruences $\{r_i \equiv r \pmod{m_i} : i \in B\}$, and the set $\mathcal{R}_B = \{r', r' + M_B, \ldots, r' + \frac{M_{(n)} - M_B}{M_B} M_B\}$ of possible solutions to the same set of congruences modulo $M_{(n)}$.

Let $\tilde{y}$ be an arbitrary element of $\mathcal{S}_B$. The solution to the congruence $\log_g(c) \equiv \tilde{y} + a\tilde{r} \pmod{\operatorname{ord}(g)}$, with respect to $\tilde{r}$, is in $\mathcal{R}_B$: $\tilde{r} \equiv a^{-1}(\log_g(c) - \tilde{y}) \equiv a^{-1}((y - \tilde{y}) + ar) \pmod{\operatorname{ord}(g)}$ (where the existence of $a^{-1} \bmod \operatorname{ord}(g)$ follows from Lemmas 4 and 10). Because $y \equiv \tilde{y} \pmod{M_B}$, and $M_B \mid \operatorname{ord}(g)$, $\tilde{r} \equiv r \pmod{M_B}$, so $\tilde{r} \in \mathcal{R}_B$. We conclude that the pair $(\tilde{y}, \tilde{r})$ is consistent with all information available to the adversary, so $\tilde{y}$ cannot be ruled out as a possibility for the true value of y.

Because $(M_B, p) = 1$ the set $\{\tilde{y} \bmod p : \tilde{y} \in \mathcal{S}_B\} = \mathbb{Z}_p$, so no possible secret value, $s \in \mathbb{Z}_p$ can be ruled out. From Theorems 1 and 3, it follows that the VSS is a statistical SSS. □

Consistency of the shares comes with the range proof; by completeness of the range proof, the participants can be sure that every qualified group of participants will acquire the same secret. Participants can check that their shares are actually derived from the blinded secret y by confirming Equation (5).

Theorem 12. *A computationally bounded corrupted dealer cannot distribute inconsistent shares without being detected.*

Proof Sketch. Because the random r is determined by the participants, the dealer cannot give an inconsistent share without knowing a_i which contradicts with our assumption:

$$\begin{aligned} & g^{y_i} \cdot h^{r_i} \equiv g^{y'_i} \cdot h^{r'_i} \bmod q_i \\ \iff\ & g_i^{y_i} \cdot h_i^{r_i} \equiv g_i^{y'_i} \cdot h_i^{r'_i} \bmod q_i \\ \iff\ & y_i + a_i \cdot r_i \equiv y'_i + a_i \cdot r'_i \bmod m_i \\ \iff\ & a_i = (y'_i - y_i) \cdot (r_i - r'_i)^{-1} \bmod m_i \end{aligned}$$

The range proof of y is based on the commitment scheme given by Boudot [28]. For that reason, it is enough to satisfy the requirements of that scheme. Because the proposed VSS scheme uses the bases (g, h) where $g \in \mathbb{Z}_Q^*$ and h is an element of the group generated by g with an unknown order, the range proof commitment is statistically secure in the case that factorization of N is unknown. □

Theorem 13. *A computationally bounded corrupted participant cannot cheat without being detected.*

Proof Sketch. Similar to Theorem 12, participant i cannot cheat unless he knows a_i which contradicts with the assumption:

$$\begin{aligned} & g^{y_i} \cdot h^{r_i} \equiv g^{y'_i} \cdot h^{r'_i} \bmod q_i \\ \iff\ & g_i^{y_i} \cdot h_i^{r_i} \equiv g_i^{y'_i} \cdot h_i^{r'_i} \bmod q_i \\ \iff\ & y_i + a_i \cdot r_i \equiv y'_i + a_i \cdot r'_i \bmod m_i \\ \iff\ & a_i = (y'_i - y_i) \cdot (r_i - r'_i)^{-1} \bmod m_i \end{aligned}$$ □

The efficiency of the proposed VSS scheme is analyzed in Appendix 6.

5. JOINT RANDOM SECRET SHARING

Joint random secret sharing protocols enable a group of users to jointly generate and share a random secret where a dealer is not available. In this work, we are adapting the JRSS scheme given by Kaya and Selçuk [14]. We modify the commitment with respect to our VSS and also use a modified version of the original scheme;

$$M_{(t)} > np^2 M^{(t-1)} \tag{5}$$

$$M = \left\lfloor \frac{M_{(t)}}{n} \right\rfloor \tag{6}$$

where M denotes the domain of y, that is, $y \in \mathbb{Z}_M$. The CRT-based JRSS scheme is given in Figure 5.

5.1. Analysis of the proposed scheme

Theorem 14. *In the modified Asmuth-Bloom scheme with (5) and (6), no possible secret value can be ruled out for an adversary, and the JRSS is a statistical SSS.*

Proof. Let B be the set of $t-1$ users corrupted by the adversary. Let $\mathcal{X}$ be the probability distribution $\Pr(S = \delta)$ over the secret candidates $\delta \in \mathbb{Z}_p$ from the adversary's point of view. The adversary can compute $y' = y \bmod M_B$ and $r' = r \bmod M_B$. Because of (5) and (6), $M/M_B > p^2$. The rest of the proof is similar to that of Theorems 3 and 11. □

5.1.1. Correctness.

Observe that when all users behave honestly, the JRSS scheme works correctly. Let $y = \sum_{i \in \mathcal{B}} y^{(i)}$. It is easy to see that $y < M_{(t)}$, because $y^{(i)} < M$ for all $i \in \mathcal{B}$, where $|\mathcal{B}| \leq n$ and $M = \lfloor M_{(t)}/n \rfloor$. One can see that $y_j = y \bmod m_j$ for all $j \in \mathcal{B}$ by checking

$$\begin{aligned} y \bmod m_j &= \left(\sum_{i \in \mathcal{B}} y^{(i)} \right) \bmod m_j \\ &= \left(\sum_{i \in \mathcal{B}} y_j^{(i)} \right) \bmod m_j \\ &= y_j \bmod m_j = y_j \end{aligned}$$

Hence, each y_i satisfies $y_i = y \bmod m_i$ and $y < M_{(t)}$; y can be constructed with t shares.

For correctness of the verification procedure in (10), one can observe that

$$\begin{aligned} & \left(\prod_{j \in \mathcal{B}} E(y^{(j)}, r^{(j)}) \right) \bmod q_i \\ &= g^{\sum_{j \in \mathcal{B}} y^{(j)}} \cdot h^{\sum_{j \in \mathcal{B}} r^{(j)}} \bmod q_i \\ &= g_i^{\sum_{j \in \mathcal{B}} y^{(j)}} \cdot h_i^{\sum_{j \in \mathcal{B}} r^{(j)}} \bmod q_i \\ &= {g_i}^{y_i} {h_i}^{r_i} \bmod q_i \end{aligned}$$

DOI: 10.1002/sec

Initialization Phase

Each user i chooses random $r_j^{(i)} \in \mathbb{Z}_{m_i}$ for $j = 1, \ldots, n$ and shares $r_j^{(i)}$ with user j.

Each user i calculates his own random as $r^{(i)} \equiv r_i^{(j)} \mod m_j$:

$$r^{(i)} = \left[\sum_{j=1}^{n} \frac{M_{(n)}}{m_j} \cdot \left[\frac{m_j}{M_{(n)}} \right]_{m_j} \cdot r_i^{(j)} \right]_{M_{(n)}} . \tag{9}$$

Distribution Phase

Each user i chooses a secret $S_i \in \mathbb{Z}_p$ and shares it using the VSS scheme as follows:

- He first chooses an arbitrary A_i such that $y^{(i)} = S_i + A_i \cdot p < \lfloor M_{(t)}/n \rfloor = M$
- Then the share for the jth user is computed as $y_j^{(i)} = y^{(i)} \mod m_j$ and privately send to user j
- Then announces $E(y^{(i)}, r^{(i)})$ and $Range\_Proof(E(y^{(i)}, r^{(i)}), M)$.

Verification Phase

Verification of the shares of each user can be done by the same procedure as the VSS

Let $\mathcal{B}$ be the set of users whose shares are verified correctly.

The ith user computes his overall share and r_i as

$$y_i = \left(\sum_{j \in \mathcal{B}} y_i^{(j)} \right) \mod m_i, \quad r_i = \left(\sum_{j \in \mathcal{B}} r_j^{(i)} \right) \mod m_i.$$

Reconstruction Phase

Let G be a group of participants gathered to reconstruct the secret,

Share of $i \in G$ is verified by other participants:

$$g_i^{y_i} \cdot h_i^{r_i} \overset{?}{\equiv} \left(\prod_{j \in \mathcal{B}} E(y^{(j)}, r^{(j)}) \right) \pmod{q_i}. \tag{10}$$

After all the shares are verified, G may reconstruct S using CRT.

Figure 5. The proposed joint random secret sharing scheme.

where $r_i = \left(\sum_{j \in \mathcal{B}} r_j^{(i)} \right) \mod m_i$. Hence, when all users behaves honestly, the proposed JRSS scheme works correctly. The privacy of the secret shared by the JRSS follows from Theorem 14 and the privacy of the modified Asmuth-Bloom scheme.

The consistency and the commitment correctness of the JRSS follows from that of the underlying VSS scheme: if any participant tries to deal inconsistent shares in the sharing phase or tries to provide false shares in the reconstruction phase, this will be detected by the VSS as shown in Theorems 12 and 13. The practicality of the scheme is analyzed in Appendix 6.

6. CONCLUSION

In this work, we pointed out certain security concerns for three VSS schemes based on the CRT in the literature. To the best of our knowledge, there exist five such schemes [14–18] where two of them [15,16] were already proven to be insecure. In this work, we first show that two of the remaining schemes [17,18] are also insecure, and the remaining one [14] is only secure against a computationally bounded adversary. We propose a modification for this scheme and prove that the modified scheme is a secure VSS scheme against an unbounded adversary. Lastly, as an application, we show how to use the new scheme for JRSS.

REFERENCES

1. Ben-Or M, Goldwasser S, Wigderson A. Completeness theorems for non-cryptographic fault-tolerant distributed computation. *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, ACM, New York, NY, USA, 1988; 1–10.
2. Cramer R, Damgård I, Maurer U. General secure multi-party computation from any linear secretsharing scheme. In *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques*, vol. 1807, Preneel B (ed), Proceeding, Lecture Notes in Computer Science. Springer: Bruges, Belgium, 2000; 316–334.

3. Damgård I, Pastro V, Smart N, Zakarias S. Multiparty computation from somewhat homomorphic encryption. In *Advances in Cryptology CRYPTO 2012*, vol. 7417, Safavi-Naini R, Canetti R (eds), Lecture Notes in Computer Science, 2012; 643–662.
4. Shamir A. How to share a secret. *Communications of the ACM* 1979; **22**(11): 612–613.
5. Blakley GR. Safeguarding cryptographic keys. *Proc. of the National Computer Conference,* Arlington 1979; **48**: 313–317.
6. Mignotte M. How to share a secret. *Cryptography*, Springer, 1983; 371–375.
7. Asmuth C, Bloom J. A modular approach to key safeguarding. *IEEE Transactions on Information Theory* 1983; **30**(2): 208–210.
8. Chor B, Goldwasser S, Micali S, Awerbuch B. Verifiable secret sharing and achieving simultaneity in the presence of faults. *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, IEEE, 1985; 383–395.
9. Patra A, Choudhury A, Rangan CP. Efficient asynchronous verifiable secret sharing and multiparty computation. *Journal of Cryptology* 2015; **28** (1): 49–109.
10. Zhenhua C, Shundong L, Qianhong W, Qiong H. A distributed secret share update scheme with public verifiability for ad hoc network. *Security and Communication Networks* 2015; **8**(8): 1485–1493.
11. Pedersen TP. A threshold cryptosystem without a trusted party. *Advances in Cryptology - EUROCRYPT91*, Springer, 1991; 522–526.
12. Feldman P. A practical scheme for non-interactive verifiable secret sharing. *28th Annual Symposium on Foundations of Computer Science, 1987*, IEEE, 1987; 427–438.
13. Liu Y. Linear (k,n) secret sharing scheme with cheating detection. *Security and Communication Networks* 2016; **9**(13): 2115–2121.
14. Kaya K, Selçuk AA. A verifiable secret sharing scheme based on the Chinese Remainder Theorem. In *Progress in Cryptology - INDOCRYPT 2008*, vol. 5365, Chowdhury DR, Rijmen V, Das A (eds), Lecture Notes in Computer Science. Springer: Berlin Heidelberg, 2008; 414–425.
15. Qiong L, Zhifang W, Xiamu N, Shenghe S. A non-interactive modular verifiable secret sharing scheme. *Proceedings. 2005 International Conference on Communications, Circuits and Systems,* IEEE, 2005; **1**: 84–87.
16. Iftene S. Secret sharing schemes with applications in security protocols. *Scientific Annals of Cuza University* 2006; **16**: 63–96.
17. Harn L, Fuyou M, Chang CC. Verifiable secret sharing based on the Chinese Remainder Theorem. *Security and Communication Networks* 2014; **7**(6): 950–957.
18. Liu Y, Harn L, Chang CC. A novel verifiable secret sharing mechanism using theory of numbers and a method for sharing secrets. *International Journal of Communication Systems* 2015; **28**(7): 1282–1292.
19. Joux A. A new index calculus algorithm with complexity L(1=4 + o(1)) in very small characteristic, Cryptology ePrint Archive, Report 2013/095, 2013.
20. Haitner I, Horvitz O, Katz J, Koo CY, Morselli R, Shaltiel R. Advances in Cryptology –EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, 2005; 58–77.
21. Gennaro R, Jarecki S, Krawczyk H, Rabin T. Robust threshold DSS signatures. *Information and Computation* 2001; **164**(1): 54–84.
22. Ingemarsson I, Simmons GJ. A protocol to set up shared secret schemes without the assistance of a mutually trusted party. In *Proc. of EUROCRYPT'91*, vol. 547, LNCS. Springer-Verlag: Brighton, UK, 1990; 266–282.
23. Herzberg A, Jarecki S, Krawczyk H, Yung M. Proactive secret sharing or: How to cope with perpetual leakage. *Advances in CryptologyCRYPT095*, Springer, 1995; 339–352.
24. Darco P, Stinson DR. On unconditionally secure robust distributed key distribution centers. *Advances in CryptologyASIACRYPT 2002*, Springer, 2002; 346–363.
25. Quisquater M, Preneel B, Vandewalle J. On the security of the threshold scheme based on the Chinese Remainder Theorem. *Public Key Cryptography*, Springer, 2002; 199–210.
26. Kaya K, Selçuk AA. Threshold cryptography based on Asmuth-Bloom secret sharing, 2007; 4148–4160.
27. Cao Z, Liu L. Boudots range-bounded commitment scheme revisited. *Information and Communications Security*, Springer, 2007; 230–238.
28. Boudot F. Efficient proofs that a committed number lies in an interval. *Advances in Cryptology - EUROCRYPT 2000*, Springer, 2000; 431–444.
29. Fujisaki E, Okamoto T. Statistical zero knowledge protocols to prove modular polynomial relations. *Advances in Cryptology - CRYPTO'97*, Springer, 1997; 16–30.
30. Hardy GH, Littlewood JE. Some problems of partitio numerorum; iii: on the expression of a number as a sum of primes. *Acta Mathematica* 1923; **44**(1): 1–70.
31. Caldwell CK. An amazing prime heuristic. *Preprint* 2000.

APPENDIX A: PRACTICALITY AND EFFICIENCY OF THE SCHEMES

If both q and $2q+1$ are prime numbers, q is called a Sophie Germain prime. It is believed that the number of Sophie

Table II. Number of Sophie Germain primes less than N[31]. The second column is the actual number of Sophie Germain primes less than N. The third and fourth columns are the integral and ratio approximations on the left and right side of (A.1), respectively.

N	Actual	Integral	Ratio
1 000 000	7746	7811	6917
10 000 000	56 032	56 128	50 822
100 000 000	423 140	423 295	389 107
1 000 000 000	3 308 859	3 307 888	3 074 425
10 000 000 000	26 569 515	26 568 824	24 902 848
100 000 000 000	218 116 524	218 116 102	205 808 662

Germain primes is infinite and because of the conjecture of Hardy and Littlewood[30], for sufficiently large N, the number of Sophie Germain primes less than N is

$$2C\int_2^N \frac{dx}{\log x \log 2x} \approx \frac{2CN}{(\ln N)^2}, \qquad \text{(A.1)}$$

where $C \approx 0.66$ is the twin prime constant. The accuracy of the conjecture and the ratio is in Table II.

For the proposed VSS, a sequence $m_1 < m_2 < \cdots < m_n$ consisting of n Sophie Germain primes is needed. Also, for security issues, this sequence must also satisfy inequality (1). Let us assume that p, the number of secret candidates, is a k-bit prime. From (1), first, each m_i must be at least a $2k$-bit Sophie Germain prime. We know that such primes exist because the number of Sophie Germain primes is infinite. Second, we need to know that we can find a Sophie Germain sequence for every t, n, and k such that the product of the t smallest numbers in the sequence is larger than the product of the $t-1$ largest ones and p^2. Note that the Hardy–Littlewood conjecture says that the density of the Sophie Germain primes less than N is proportional to $1/(\ln N)^2$, where the prime number theorem says that the density of primes less than N is proportional to $1/(\ln N)$. Hence, considering $N \gg \ln N$, finding an Asmuth-Bloom sequence with Sophie Germain primes satisfying (1) should not be much harder than finding such a sequence with ordinary primes.

An analysis of the existence of a desired sequence and the information rate of the proposed schemes can be given as follows: let p be a k-bit prime. Provided that $2^k \gg n$, the number of $2k$-bit Sophie Germain primes is approximately equal to

$$\frac{2C2^{2k+1}}{(\ln 2^{2k+1})^2} - \frac{2C2^{2k}}{(\ln 2^{2k})^2}$$
$$= \frac{C2^{2k+1}}{(\ln 2)^2}\left(\frac{2}{(2k+1)^2} - \frac{1}{(2k)^2}\right)$$

which is much greater than n. Let m_1 be a $2k$-bit Sophie Germain prime and $\ell = \ln m_1$. Let m_i be the $(i-1)$st Sophie Germain prime after m_1. Because of (A.1), we can assume that $m_i \approx m_1 + (i-1)\ell^2$. Note that the ratio m_i/m_j for $i < j$ is bounded previously by $\left(1 + n\ell^2/m_1\right)$. Hence, the inequality

$$m_1 > \frac{p^2 \prod_{i=1}^{t-1} m_{n-i+1}}{\prod_{i=1}^{t-1} m_{i+1}}$$

is satisfied when

$$m_1 > p^2\left(1 + \frac{n\ell^2}{m_1}\right)^{t-1}$$

Because $m_1 \gg n\ell^2$ and $m_1 \gg t$, we can choose $m_1 \approx p^2$, and the information rate of the VSS scheme becomes $|p|/|m_n| \approx |p|/|p^2 + 4n(\ln p)^2| \approx 1/2$. A similar analysis can be carried out for the JRSS scheme as well: Equation (1) is replaced by (5); hence,

$$m_1 > np^2\left(1 + \frac{n\ell^2}{m_1}\right)^{t-1}$$

So the information rate is again

$$\frac{|p|}{|np^2 + 4n(\ln p)^2|} \approx \frac{1}{2}$$

respectively. Although the proposed scheme is not ideal, they are highly practical because the information rate is only 1/2.

DOI: 10.1002/sec