The ISC Int'l Journal of Information Security

January 2016, Volume 8, Number 1 (pp. 25–38)

http://www.isecure-journal.org

On the Design and Security of a Lattice-Based Threshold Secret Sharing Scheme☆

Hamidreza Amini Khorasgani [1], Saba Asaad [1], Hossein Pilaram [1], Taraneh Eghlidos [2,*], and Mohammad Reza Aref [1]

[1] *Information Systems and Security Lab (ISSL), Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran*

[2] *Electronics Research Institute, Sharif University of Technology, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: 28 July 2015
Revised: 3 November 2015
Accepted: 9 December 2015
Published Online: 15 December 2015

Keywords:
Threshold Secret Sharing Scheme, Closest Vector Problem, Lattice-based Cryptography.

ABSTRACT

In this paper, we introduce a method of threshold secret sharing scheme (TSSS) in which secret reconstruction is based on Babai's nearest plane algorithm. In order to supply secure public channels for transmitting shares to parties, we need to ensure that there is no quantum threats to these channels. A solution to this problem can be the utilization of lattice-based cryptosystems for these channels, which requires designing lattice-based TSSSs. We investigate the effect of lattice dimension on the security and correctness of the proposed scheme. Moreover, we prove that for a fixed lattice dimension the proposed scheme is asymptotically correct. We also give a quantitative proof of security from the information theoretic viewpoint.

1 Introduction

Lattice-based cryptography is one of the most popular areas in mathematical cryptography nowadays. It has received considerable attention in order to build secure cryptographic primitives such as signature schemes, hash functions and public key cryptosystems. Moreover, its rapid development is due in part to security against quantum-computer based attacks as well as efficiency and simplicity of basic operations.

A secret sharing scheme is a method of sharing a secret data by distributing some values, called shares, among a number of parties, called participants. In such a scheme, a dealer is an authority who undertakes the task of computing each share and sending it to the corresponding participant through a secure channel which can be modelled by a public key cryptosystem. Moreover, sharing the secret is performed in such a way that only the authorized subsets of participants are able to recover the secret.

The potential resistance of lattice-based cryptography against quantum algorithms provides an appropriate platform for designing new public key cryptosystems for secure transmission of data [1–3]. This fact motivates to design a new secret sharing scheme which is compatible with lattice nature of the underlying cryptosystem.

The notion of secret sharing was introduced by Shamir [4] and Blakely [5] in 1979, independently. While the Shamir's TSSS is based on polynomial interpolation over finite fields [4], Blakely's scheme is based on hyperplane geometry [5]. However, in 1983 another TSSS was introduced by Asmuth and

☆ This article is an extended version of an ISCISC'2014.

* Corresponding author.

Email addresses: hraminikh@alum.sharif.edu (H. Amini Khorasgani), saba_asaad@alum.sharif.edu (S. Asaad), h_pilaram@ee.sharif.edu (H. Pilaram), teghlidos@sharif.edu (T. Eghlidos), aref@sharif.edu (M.R. Aref)

ISSN: 2008-2045

Bloom [6] which was different fundamentally from both previous schemes. Their scheme is based on Chinese Remainder Theorem [6]. All aforementioned schemes, are of a particular type of secret sharing scheme, called TSSS. In a (t, n) TSSS, shares are distributed among n participants, in such a way that any coalition of size t or more of them are able to recover the secret but smaller group cannot obtain any information about the secret and reconstruct it. Later, several other schemes have been introduced and different features were added to those schemes [7–9].

Secret sharing has a lot of practical applications in cryptography, among them are secure multiparty computations [10], secure online auctions [11], electronic voting systems [12] and information hiding [13].

In this paper, which is an extension of [14], a novel (t, n) TSSS, $t \leq n$, is introduced using a lattice construction. To the best of our knowledge, the only lattice-based TSSSs are those of Bansarkhani *et al.* [15] and Georgescu [16], both of which are (n, n) TSSS, which requires all participants pooling their shares to recover the secret, while in the proposed scheme any set of qualified participants are able to recover the secret. Asaad *et al.* [17] proposed a variant of (t, n) TSSS based on lattice. In [17], each share is an element of $\mathbb{Z}_p$ computed by adding a random noise to a random multiple of the secret chosen from $\mathbb{Z}_p$.

In the proposed scheme, each share, given to each participant, is computed by adding a random noise to the inner product of two random vectors, where one of the vectors is fixed such that its first component is the secret and the second vector is associated with the corresponding participant. The advantages of the proposed scheme over that of Asaad *et al.* are twofold. First, we discuss, in Section 5.3, using inner product of the two vectors instead of two random field elements to produce the shares providing a tradeoff between correctness and security of our scheme with respect to the choice of the length of those random vectors. Second, we analyse the security and correctness of the proposed scheme precisely by specifying the level of security and correctness achieved with regard to different parameters. Moreover, we study the effect of different parameters on the correctness and security of the proposed scheme using MATLAB. However, the authors of [17] have shown that the secret entropy loss converges to zero when p goes to infinity, but they have not discussed about the level of security and correctness of their proposed scheme.

Here, we apply a similar mathematical approach used by Steinfeld *et al.* [18], to design a new variant of lattice-based (t, n) TSSS, different from Shamir's. Steinfeld *et al.* [18] have designed a new method for increasing the threshold in the standard Shamir secret sharing scheme after distributing shares among participants without communication between them. They have used lattice reduction algorithms to increase the threshold.

The proposed TSSS is composed of three phases: public parameters generation, share distribution and secret reconstruction. In the first phase, the dealer chooses n distinct m-dimensional vectors $\boldsymbol{l}^{(i)}$ uniformly at random and an m-dimensional vector $\boldsymbol{a}$ whose first component is assigned to the secret while the remaining $m - 1$ components are random values. In the second phase, the dealer computes the shares by adding some noise e_i to the inner product of $\boldsymbol{l}^{(i)}$ and $\boldsymbol{a}$, for each i. In the last phase, a combiner (server), generates a $(t + m)$-dimensional lattice basis, exploiting t out of n vectors $\boldsymbol{l}^{(i)}$ and a $(t + m)$-dimensional vector $\boldsymbol{t}'$ using t out of n shares which is close to the certain lattice point, whose $(t + 1)^{th}$ component is a known fraction of the secret. Running an approximation algorithm, namely Babai's nearest plane algorithm [19], to find the closest vector of the lattice, generated by the aforementioned basis, to the vector $\boldsymbol{t}'$, the secret is to be recovered.

Moreover, we improve the lower bound for the security parameter k stated in [14] and show that for a certain security level we need less computations than that mentioned in [14]. Also, we investigate the effect of the parameter m on the security and correctness of the scheme, when m varies in the interval $[2,\ t - 1]$.

The rest of this paper is organized as follows. Section 2 provides necessary concepts and notations used in the rest of the paper. The formal definition of secret sharing scheme is described in Section 3. Section 4 is dedicated to the proposed lattice-based TSSS.The correctness and security of this scheme are discussed in Section 5 and the proofs of the theorems are given in this section. Furthermore, we examine the effects of some parameters on the correctness and security of the proposed scheme. Finally, we give a summery and then conclude the paper.

2 Preliminaries

2.1 Notations

In this paper, we denote matrices with upper-case bold letters while row vectors are denoted by lowercase bold letters.The inner product of two row vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ is denoted by $< \boldsymbol{a}, \boldsymbol{b} >$, in short as $\boldsymbol{a}\boldsymbol{b}^T$, the i^{th} element of an n-dimensional vector $\boldsymbol{v}$ is denoted by $\boldsymbol{v}_i$ and we write $\boldsymbol{v} = (\ \boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$. In addition, if $\boldsymbol{M}$ is a matrix then its entry located in the i^{th} row and j^{th} column is denoted by $\boldsymbol{M}_{ij}$. We denote the i^{th} row and the j^{th} column of $\boldsymbol{M}$ by $\boldsymbol{M}_{i*}$ and $\boldsymbol{M}_{*j}$, respectively. For a finite set A, $|A|$ denotes the number of elements in A. For integers m and n, $A^{m\times n}$ denotes the set of all matrices with m rows and n columns, whose entries are chosen from A. We use $D(A^{m\times n})$ to denote the subset of $A^{m\times n}$ that contains all matrices from $A^{m\times n}$ with distinct nonzero rows.

We use different norms in this paper, defined as follows. For an integer a and a prime p, we denote the Lee norm of a modulo p, defined as $\min_{t\in\mathbb{Z}}|a-tp|$, by $\|a\|_{L,p}$. Using this definition, the Lee norm of a vector $\boldsymbol{a}$ modulo p which is defined as $\max_{1\le i\le n}\|a_i\|_{L,p}$ is shown as $\|\boldsymbol{a}\|_{L,p}$. The infinity norm of a vector $\boldsymbol{a}$ in $\mathbb{R}^n$ is defined as $\|\boldsymbol{a}\|_\infty=\max_{1\le i\le n}|a_i|$.

For a real number a, $Int(a)$ shows the largest integer number, strictly less than a, and for any probability distribution D by $x\leftarrow D$ we mean that x is chosen from the probability distribution D. In addition, for any set A, we use U_A to denote the uniform distribution over the set A. In this paper, whenever we use $\log(\cdot)$, we mean the logarithmic function with base 2.

Moreover, for a discrete random variable X which takes values in an alphabet $\mathcal{X}$ with probability distribution $P_X(\cdot)$, the support of X, denoted by $SUPP_X$, is defined as the set of all those values in $\mathcal{X}$ for which the value of P_X is nonzero. Considering this definition, the Shannon entropy of the random variable X with probability distribution $P_X(\cdot)$, is defined as follows:

$$H(X)=\sum_{a\in SUPP_X}-P_X(a)\log(P_X(a))$$

Furthermore, if $P_X(\cdot|e)$ denotes the conditional probability distribution of the random variable X given the event e such that $\Pr(e)>0$, then the conditional entropy of X given the event e is defined as follows:

$$H(X|e)=\sum_{a\in SUPP_{X|e}}-P_X(a|e)\log(P_X(a|e))$$

where $SUPP_{X|e}$ denotes the set of all $a\in\mathcal{X}$ such that $P_X(a|e)>0$.

2.2 Lattices

Let $B=\{\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n\}$ be a set of n linearly independent vectors in $\mathbb{R}^m$. The lattice generated by B is defined by $\mathcal{L}(B)=\{\sum_{i=1}^n c_i\cdot\boldsymbol{b}_i : c_i\in\mathbb{Z}\}$ as the set of all integer linear combinations of the vectors $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n$. The integers m and n are known as the dimension and rank of this lattice, respectively. The set B is called a basis for the lattice $\mathcal{L}(B)$. Note that a lattice may have more than one basis. Moreover, It is an obvious requirement that $m\ge n$. If $m=n$, the lattice is called full rank.

So far, no efficient algorithms are known for many lattice problems unless one considers approximation solutions for them. The shortest vector problem (SVP), is the most basic ones. In the approximation version of this problem, that is γ-approximate SVP, assuming that a lattice basis B is given, the goal is to find a nonzero lattice vector, whose norm is not greater than $\gamma_{svp}\min_{\boldsymbol{a}\in\mathcal{L}(B)\setminus\{\boldsymbol{0}\}}\|\boldsymbol{a}\|_\infty$. The basis reduction algorithm of Lenstra, Lenstra, Lovasz, for short LLL algorithm [20], is the basic algorithm in the lattice context. This algorithm runs in polynomial time and is used in the approximation versions of SVP and Closest Vector Problem (CVP) with an approximation factor of $n^{1/2}2^{n/2}$ with regard to infinity norm. In this paper, we use an approximation version of CVP to find a vector $\boldsymbol{a}$ in a lattice, defined by a given basis B, within distance $\gamma_{cvp}\min_{\boldsymbol{b}\in\mathcal{L}(\mathrm{B})}\|\boldsymbol{b}-\boldsymbol{t}\|_\infty$ of the given target vector $\boldsymbol{t}$ in $\mathbb{R}^n$. According to Babai [19], we can use the so-called nearest plane algorithm to solve the approximation version of CVP with an approximation factor of $n^{1/2}2^{n/2}$ regarding infinity norm.

In the following, we quote the necessary definitions and theorems from [18] and [21] used in the rest of this paper:

Definition 1 (Minkowski's successive minima): Let $\Lambda\subset\mathrm{R}^{\mathrm{n}}$ be a full rank lattice. For any integer $k\le n$, $\lambda_k(\Lambda)$, called the k^{th} successive minimum of lattice Λ, is defined as the smallest $r>0$ such that there exist at least k linearly independent lattice vectors $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_k$, whose infinity norms are bounded by r.

Theorem 1 (Minkowski's First Theorem): Let $\Lambda\subset\mathbb{R}^n$ be a full rank lattice and $\lambda_1(\Lambda)$, denoting the first Minkowski minimum of the lattice Λ. Then $\lambda_1(\Lambda)\le\det(\Lambda)^{\frac{1}{n}}$.

Theorem 2 (Minkowski's Second Theorem): Let $\Lambda\subset\mathbb{R}^n$ be a full rank lattice. If $\lambda_1(\Lambda),\ldots,\lambda_n(\Lambda)$ denote the first n Minkowski minima of the lattice Λ defined with respect to infinity norm (see *Definition 1*), then $\prod_{i=1}^n\lambda_i(\Lambda)\le\det(\Lambda)$.

Theorem 3 (Blichfeldt-Corput): Let $\Lambda\subset\mathbb{R}^n$ be a full rank lattice and $B=\{\boldsymbol{v}\in\mathbb{R}^n : \|\boldsymbol{v}\|_\infty<N,\ \forall N\in\mathbb{R}^+\}$, then there exist at least $2Int\left(\frac{(2N)^n}{2^n\det(\Lambda)}\right)+1$ lattice points in B.

In the following we give a generalization of the algebraic counting Lemma (Lemma 1 in [18]) introduced first by Steinfeldt, Pieprzyk and Wang (SPW) [18].

2.3 A Generalization of SPW Algebraic Counting Lemma

Steinfeld *et al.* [18] introduced an algebraic counting Lemma to prove the correctness and security of a lattice-based threshold changeable secret sharing scheme. In the following, we state a generalization of SPW Counting Lemma and prove it in an almost similar manner. We use this lemma to prove the security and correctness of the proposed scheme.

Lemma 1: suppose that m, t, E are positive integers and p is a prime. Moreover, assume that $A \subseteq \mathbb{Z}_p^{1\times m}$ is a non-empty set and $h_{m,t,E,p} \subseteq \mathbb{Z}_p^{t\times m}$ denotes the set of matrices $\boldsymbol{M} \in \mathbb{Z}_p^{t\times m}$ for which there exists at least a nonzero vector $\boldsymbol{v} \in A$ such that $\left\|\boldsymbol{v}\boldsymbol{M}^{\boldsymbol{T}}\right\|_{L,p} < E$. Then,$|h_{m,t,E,p}|$, the number of elements in the set $h_{m,t,E,p}$, is at most equal to the value $|A|\,(2E)^t p^{(m-1)t}$.

Proof. Assume that $\boldsymbol{M} \in h_{m,t,E,p}$. Then, according to the definition of $h_{m,t,E,p}$ there exists a nonzero vector $\boldsymbol{v} \in A$ such that for any integer $i \leq t$, $\|<\boldsymbol{M}_{i*}, \boldsymbol{v}>\|_{L,p} < E$. Thus, based on the definition of Lee norm module p, for each $i \leq t$, $\min_{t\in\mathbb{Z}} |<\boldsymbol{M}_{i*}, \boldsymbol{v}> -tp| < E$. Hence, for each $i \leq t$ there exists an integer number r_i such that $|<\boldsymbol{M}_{i*}, \boldsymbol{v}> -r_i p| < E$. Defining $e_i \triangleq <\boldsymbol{M}_{i*}, \boldsymbol{v}> -r_i p$, we can say that there exist t integers $e_1, \ldots, e_t$ in $\mathbb{Z}_p$ such that for any integer $i \leq t$:

$$|e_i| < E \tag{1}$$

$$<\boldsymbol{M}_{i*}, \boldsymbol{v}> \equiv e_i \ mod(p) \tag{2}$$

Since $\boldsymbol{v}$ is a nonzero vector, there exists at least an integer value j, $1 \leq j \leq m$, such that $v_j \neq 0$. Now, we can rewrite the equation (2) as $v_j\boldsymbol{M}_{i,j} + \sum_{t=1,t\neq j}^{m} v_t\boldsymbol{M}_{i,t} \equiv e_i \ mod(p)$. Thus, the value $\boldsymbol{M}_{i,j}$ is specified uniquely as the value $v_j^{-1}\left(e_i - \sum_{t=1,t\neq j}^{m} v_t\boldsymbol{M}_{i,t}\right) \ mod(p)$.

Consequently, for each e_i in $\mathbb{Z}_p$ and nonzero vector $\boldsymbol{v}\in A$ there are at most p^{m-1} vectors $\boldsymbol{M}_{i*}$ such that $<\boldsymbol{M}_{i*}, \boldsymbol{v}> \equiv e_i \ mod(p)$, so for each vector $\boldsymbol{e} = (e_1, \ldots, e_t) \in \mathbb{Z}_p^{1\times t}$ and nonzero vector $\boldsymbol{v}\in A$ there are at most $p^{(m-1)t}$ matrices $\boldsymbol{M}$ such that for any integer $i \leq t$, (1) and (2) hold. Finally, based on the fact that the number of possible values for the vectors $\boldsymbol{e}$ and $\boldsymbol{v}$ are fewer than $(2E)^t$ and $|A|$, respectively, the assertion hold. ∎

3 Secret Sharing Scheme

In this section, we give the definition of a TSSS that we use in this paper. This definition is given in [18].

Definition 2 (Threshold Scheme): A (t, n) $TSSS = (PPG, DS, SC)$ consists of three efficient algorithms which are defined as follows:

1) *PPG (Public Parameter Generation):* This is an efficient algorithm which takes as input a security parameter $k \in \mathcal{K}$ while returning as output a string of public parameters $x \in \mathcal{X}$.

2) *DS (Dealer Setup):* This is a probabilistic algorithm which takes as input $(1^k, x)$ as a pair of security/ public parameter and also s as a secret that comes from the secret space $\mathcal{S}\left(1^k, x\right) \subseteq \{0,1\}^{k+1}$ while returning as output a vector of shares $\boldsymbol{s} = (\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n)$, whose i^{th} component is in the i^{th} share space $\mathcal{S}_i(1^k, x)$ for any integer $i \leq n$. We use $\mathcal{R}(1^k, x)$ to denote the space of random inputs and denote the mapping corresponding to the algorithm DS by:

$$DS_{(1^k,x)}(\cdot,\cdot) : \mathcal{S}\left(1^k, x\right) \times \mathcal{R}\left(1^k, x\right) \rightarrow \prod_{i=1}^{n} \mathcal{S}_i(1^k, x)$$

3) *SC (Share Combiner):* The input to this algorithm is a pair of security/ public parameter $(1^k, x)$ and a subset $\{\boldsymbol{s}_{i_1}, \cdots, \boldsymbol{s}_{i_t}\}$ of t out of the n shares and its output is the recovered secret $s \in \mathcal{S}\left(1^k, x\right)$.

In the following, the correctness and security of the above-defined (t, n) TSSS are given [18].

Definition 3 (Correctness, Security): A (t, n) threshold secret sharing scheme $TSSS = (PPG, DS, SC)$ is called as:

1) δ_c-correct, when the probability of failure in secret recovery, denoted by p_{fail}, taken over public parameters $x = PPG\,(k) \in \mathcal{X}$, is at most δ_c. For a given pair $(1^k, x)$ the failure of secret recovery means that there exist at least a pair (s, r) in $\mathcal{S}\left(1^k, x\right) \times \mathcal{R}\left(1^k, x\right)$ and t indices $i_1, \ldots, i_t$ in the set $\{1, \ldots, n\}$ such that $SC_{(1^k,x)}\left(s_{i_1}, \ldots, s_{i_t}\right) \neq s$, where $(s_1, \ldots, s_n) = DS_{(1^k,x)}\left(s, r\right)$. Precisely, p_{fail} is defined as follows:

$$\begin{aligned} p_{fail} \triangleq pr\{&x = PPG(k) \in \mathcal{X} : \exists\ (s, r) \in \mathcal{S}(1^k, x) \times \mathcal{R}(1^k, x) \\ &\text{such that}(s_1, \ldots, s_n) = DS_{(1^k,x)}(s, r), \\ &\exists\ i_1, \ldots, i_t\ ,\ SC_{(1^k,x)}(s_{i_1}, \ldots, s_{i_t}) \neq s\} \end{aligned}$$

Moreover, the $TSSS$ is asymptotically correct if for any $\delta > 0$, there exists $k_0 \in \mathcal{K}$ such that if $k > k_0$ then $TSSS$ is δ-correct.

2) $(t_s, \delta_s, \epsilon_s, s \leftarrow P_{\mathcal{S}(1^k,x)})$-secure, when the probability of the secret entropy loss does not exceed the given value ϵ_s, is at least $1 - \delta_s$. Here, the secret s is sampled from $\mathcal{S}\left(1^k, x\right)$ w.r.t. the probability distribution $P_{\mathcal{S}(1^k,x)}$ and the probability is computed over public parameters $x = PPG\,(k) \in \mathcal{X}$ for any arbitrary t_s observed shares. Precisely, the following probability

$$\begin{aligned} p_s \triangleq pr\{&x = PPG(k) :\ leak_{(1^k,x)}(\boldsymbol{\mu}_{i_1}, \ldots, \boldsymbol{\mu}_{i_{t_s}})\ \leq \epsilon_s, \\ &\forall\ (\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_n) \in \prod_{i=1}^{n} \mathcal{S}_i(1^k, x)\ \forall i_1, \ldots, i_{t_s}, \\ &s \leftarrow P_{\mathcal{S}(1^k,x)}, (s_1, \ldots, s_n) = D_{(1^k,x)}(s, r) \&\ r \leftarrow U_{\mathcal{R}(1^k,x)}\} \end{aligned}$$

is at least $1 - \delta_s$ where the secret entropy loss corresponding to the observed shares $\boldsymbol{\mu}_{i_1}, \ldots, \boldsymbol{\mu}_{i_{t_s}}$, denoted by $leak_{(1^k,x)}\left(\boldsymbol{\mu}_{i_1}, \ldots, \boldsymbol{\mu}_{i_{t_s}}\right)$, is defined as follows:

$$leak_{(1^k,x)}\left(\boldsymbol{\mu}_{i_1}, \ldots, \boldsymbol{\mu}_{i_{t_s}}\right) \triangleq$$
$$\left| H\left(s\right) - H\left(s \,\middle|\, \boldsymbol{s}_{i_j} = \boldsymbol{\mu}_{i_j},\ j = 1, \ldots, t_s\right) \right|$$

Furthermore, the $TSSS$ is said to be asymptotically t_s-secure with respect to $P_{\mathcal{S}(1^k,x)}$ when for sufficiently large chosen security parameter k, there is a high probability that the maximum ratio of secret entropy loss to the security parameter, as the approximate number of bits required to represent the secret, will be arbitrarily small; to be more exact, the following condition should be satisfied:

$\forall\, \delta > 0,\ \forall \epsilon > 0\, \exists k_0 :\ \forall\, k > k_0\, TSSS\, is\ (t_s, \delta, \epsilon \cdot k)$-secure

4 Lattice-based Threshold Secret Sharing Scheme

In this section, we propose a new lattice-based TSSS, inspired by the approach of [18]. In the proposed scheme, the secret is reconstructed using Babai's nearest plane algorithm for solving the closest vector problem with approximation factor γ_{cvp}. In the following, Γ_{cvp} denotes the value $\log(\lceil \gamma_{cvp} + 1 \rceil)$ and we note that $\Gamma_{\text{cvp}} \leq 1 + 0.5(t+m+\log(t+m)\ )$ if the Babai's nearest plane algorithm is used.

4.1 The proposed (t, n) TSSS algorithm:

(1) $PPG(k)$:

a) Select prime p such that $p > n$ and $2^k \leq p \leq 2^{k+1}$.

b) Choose n distinct random vectors $\boldsymbol{l}^{(i)} = \left(\boldsymbol{l}_1^{(i)}, \ldots, \boldsymbol{l}_m^{(i)}\right) \in \mathbb{Z}_p^m$, $i = 1, \ldots, n$, where $2 \leq m \leq t-1$ is an arbitrary integer.

c) Choose the value of noise bound N as follows to ensure that the proposed scheme is δ_c-correct: $N \triangleq \left\lfloor \frac{p^\eta}{2} \right\rfloor$, $\eta \triangleq 1 - \frac{m}{t} - \zeta, \zeta \triangleq \frac{1}{k}(log\left(\delta_c^{-\frac{1}{t}}.n\right) + \Gamma_{cvp} + 1)$.

(2) DS (Dealer Setup): To share secret $s \in \mathbb{Z}_p$, choose $m-1$ random integers $a_1, \ldots, a_{m-1}$ in $\mathbb{Z}_p$. Considering $\boldsymbol{a} = (s, a_1, \ldots, a_{m-1}) \in \mathbb{Z}_p^{1\times m}$, we set the i^{th} share to be $s_i = \left(< \boldsymbol{l}^{(i)}, \boldsymbol{a} > + e_i\right)\ mod(p)$ in which the integer e_i is chosen uniformly at random in the interval $(-N, N)$.

(3) $SC(s_{i_1}, \ldots, s_{i_t})$ (Share Combiner): Let $\boldsymbol{M}_{n\times m}$ denote the matrix whose i^{th} row is the vector $\boldsymbol{l}^{(i)}$ for $i \in \{1, \ldots, n\}$. To recover the secret using subshares $\{s_{i_1}, \ldots, s_{i_t}\}$ such that δ_c-correctness is guaranteed, do the following steps:

a) Corresponding to the set $I = \{i_1, \cdots, i_t\}$, define the matrix $(\boldsymbol{M}_I)_{t\times m}$ satisfying $(\boldsymbol{M}_I)_{r\times s} = \boldsymbol{l}_s^{(i_r)}$ for $r \in \{1, \ldots, t\}$ and $s \in \{1, \ldots, m\}$.

$$\boldsymbol{M}_I = \begin{bmatrix} l_1^{i_1} & l_2^{i_1} & \cdots & l_m^{i_1} \\ \vdots & \vdots & \ddots & \vdots \\ l_1^{i_t} & l_2^{i_t} & \cdots & l_m^{i_t} \end{bmatrix}$$

b) Build the following full rank square matrix $\boldsymbol{M}_{\boldsymbol{M}_I,N,p}$, whose columns form a basis for a full rank lattice $\mathcal{L}_{\boldsymbol{M}_I,N,p}$:

$$\boldsymbol{M}_{\boldsymbol{M}_I,N,\text{p}} = \begin{bmatrix} p\mathbf{I}_t & \boldsymbol{M}_{\text{I}} \\ \mathbf{0}_{t+m} & N/p\mathbf{I}_m \end{bmatrix}$$

where $\boldsymbol{I}_t$ and $\boldsymbol{I}_m$ denote identity matrices of size t and m, respectively and $\mathbf{0}_{t+m}$ is a zero matrix of size $t+m$.

c) Define the target vector

$$\boldsymbol{t}' = (s_{i_1}, \ldots, s_{i_t}, 0, \ldots, 0)_{1\times(t+m)}$$

d) Run CVP approximation algorithm $A_{\boldsymbol{CVP}}$ on the lattice $\mathcal{L}_{\boldsymbol{M}_I,N,p}$ and the target vector $\boldsymbol{t}'$. Let us denote the output of this algorithm by $\boldsymbol{c} = (c_1, \ldots, c_t, c_{t+1}, \ldots, c_{t+m})$, then the secret is recovered by computing $s^* = \frac{p}{N}\boldsymbol{c}_{t+1} mod(p)$.

5 Analysis of Correctness and Security

5.1 Correctness

Theorem 4 (Correctness): The proposed TSSS is asymptotically correct choosing $\delta_c = O(1/poly(k))$. In fact for any $0 < \delta_c < 1$ the (t, n)-TSSS is δ_c-correct for all $k \geq k_0'$, where$k_0' \triangleq \frac{1}{1-\frac{m}{t}}(\log\left(\delta_c^{-\frac{1}{t}}.n\right) + \Gamma_{\text{cvp}} + 2)$.

Proof. First of all, let $I = \{i_1, \cdots, i_t\} \subseteq \{1, \cdots, n\}$ be a subset of indices, related to those participants trying to reconstruct the secret. In order to calculate $s_{i_j} = \left(\boldsymbol{l}^{(i_j)}\boldsymbol{a}^T + e_{i_j}\right) mod\,(p)\,, j = 1, \cdots, t$, one should deduct the integer $k_j p$ from $< \boldsymbol{l}^{(i_j)}, \boldsymbol{a} > + e_{i_j}$, where

$$k_j = \left\lfloor (\boldsymbol{l}^{(i_j)}\boldsymbol{a}^T + e_{i_j})/p \right\rfloor \in \mathbb{Z}\ .$$

Then, define $\beta_j \triangleq \boldsymbol{l}^{(i_j)}\boldsymbol{a}^T - k_j p$ for $j = 1,\cdots,t$. Now, consider the following lattice vector:

$$\boldsymbol{w} = -\sum_{i=1}^{t} k_i (\boldsymbol{M}_{\boldsymbol{M}_I,N,p})_{*i} + s(\boldsymbol{M}_{\boldsymbol{M}_I,N,p})_{*t+1} + \sum_{i=1}^{m-1} a_i (\boldsymbol{M}_{\boldsymbol{M}_I,N,p})_{*t+1+i}$$

which can be represented as the following vector:

$$\boldsymbol{w} = (\beta_1, \ldots, \beta_t, sN/p,\ \ a_1 N/p, \ldots,\ a_{m-1}N/p)$$

Now, note that for $j = 1, \ldots, t$ we have:

$$\begin{aligned} s_{i_j} &= \left(\boldsymbol{l}^{(i_j)}\boldsymbol{a}^T + e_{i_j}\right) mod\,(p) \\ &= \boldsymbol{l}^{(i_j)}\boldsymbol{a}^T + e_{i_j} - k_j p \\ &= \beta_j + e_{i_j} \end{aligned}$$

Therefore, the target vector can be written as follows:

$$\boldsymbol{t}' = (\beta_1 + e_{i_1}, \ldots, \beta_t + e_{i_t}, 0, \ldots, 0)_{1\times(t+m)}$$

Now, considering $\left|e_{i_j}\right| < N$ for $j = 1, \ldots, t$, the lattice vector $\boldsymbol{w}$

is roughly close, with regard to infinity norm, to the target vector $\boldsymbol{t}'$. In fact, since $\boldsymbol{w} - \boldsymbol{t}' = (e_{i_1}, \ldots, e_{i_t}, \frac{a_1 N}{p}, \ldots, \frac{a_{m-1}N}{p})$ and for each i, $|a_i| < p$ we have:

$$\left\|\boldsymbol{w} - \boldsymbol{t}'\right\|_\infty < N \tag{3}$$

Therefore, running CVP-approximation algorithm A_{CVP}, with approximation factor γ_{cvp}, on inputs $\boldsymbol{t}'$ and the lattice $\mathcal{L}_{\mathrm{M_I,N,p}}$, we can get as output the lattice vector $\boldsymbol{c}$ satisfying the following inequality:

$$\left\|\boldsymbol{c} - \boldsymbol{t}'\right\|_\infty < \gamma_{cvp}\left\|\boldsymbol{w} - \boldsymbol{t}'\right\|_\infty < \gamma_{cvp} N \tag{4}$$

Now, define $\boldsymbol{z} \triangleq \boldsymbol{c} - \boldsymbol{w}$, and use triangle inequality to conclude from (4) that:

$$\|\boldsymbol{z}\|_\infty = \|\boldsymbol{c} - \boldsymbol{w}\|_\infty \leq (\gamma_{cvp} + 1)N \tag{5}$$

In case $\frac{p}{N}\boldsymbol{c}_{t+1} \equiv \frac{p}{N}\boldsymbol{w}_{t+1} \equiv s\ mod(p)$, the secret can be reconstructed correctly by the combiner. In other case, there exists a lattice vector $\boldsymbol{z} = \boldsymbol{c} - \boldsymbol{w}$ such that the following inappropriate case occurs:

$$\frac{p}{N}\boldsymbol{z}_{t+1} = \frac{p}{N}\boldsymbol{c}_{t+1} - \frac{p}{N}\boldsymbol{w}_{t+1} \not\equiv 0 mod(p) \tag{6}$$

Now, if the matrix $\boldsymbol{M}_I$, for a fixed I, is such that the aforementioned inappropriate case happens, then we call it a bad matrix. Let us denote the fraction of bad matrices for a fixed I by δ_I. In fact, δ_I is the fraction of all matrices $\boldsymbol{M}_I \in D(\mathbb{Z}_p^{t\times m})$ for which $\mathcal{L}_{\boldsymbol{M}_I,N,p}$ contains at least a short and inappropriate vector $\boldsymbol{z}$ which satisfies the relations (5) and (6). Now, we try to find an upper bound on δ_I. To achieve this aim, we define the following function from $\mathbb{Z}_p^m$ to $\mathbb{Z}_p$, with regard to $\boldsymbol{z} = (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_{t+m}) \in \mathcal{L}_{\boldsymbol{M}_I,N,p}$, in the following way:

$$F_{\boldsymbol{z}}(\boldsymbol{l}_{1\times m}) \triangleq < (p\boldsymbol{z}_{t+1}/N, \ldots, p\boldsymbol{z}_{t+m}/N), \boldsymbol{l} > mod(p)$$

First, we show that $F_{\boldsymbol{z}}$ for each $\boldsymbol{z} \in \mathcal{L}_{\boldsymbol{M}_I,N,p}$ is well defined. To do this, We note that according to the definition of a lattice, the columns of the matrix $\boldsymbol{M}_{\boldsymbol{M}_I,N,p}$ form a basis for the lattice $\mathcal{L}_{\boldsymbol{M}_I,N,p}$. Now, Let us denote the i^{th} coordinate of the vector $\boldsymbol{z} \in \mathcal{L}_{\boldsymbol{M}_I,N,p}$ with respect to this basis by $\pi_i(\boldsymbol{z}) \in \mathbb{Z}$ and hence we can write

$$\boldsymbol{z} = \sum_{i=1}^{t+m} \pi_i(\boldsymbol{z})(\boldsymbol{M}_{\boldsymbol{M}_I,N,p})_{*i}$$

Now, according to the structure of the matrix $\boldsymbol{M}_{\boldsymbol{M}_I,N,p}$, we have:

$$\boldsymbol{z}_j = \pi_j(\boldsymbol{z})\,p + \sum_{k=1}^{m} \pi_{t+k}(\boldsymbol{z})\boldsymbol{l}_k^{(i_j)}, \quad j = 1, \ldots, t$$

and,

$$\boldsymbol{z}_j = \frac{\pi_j(\boldsymbol{z})\,N}{p}, \quad j = t+1, \ldots, t+m.$$

Thus, $\frac{p}{N}\boldsymbol{z}_{t+i} \in \mathbb{Z}$ for $i = 1, \ldots, m$ and since it is not difficult to see that $F_{\boldsymbol{z}}$ is a function, we conclude that $F_{\boldsymbol{z}}$ is well defined. Moreover, for$j = 1, \ldots, t$ we can write

$$F_{\boldsymbol{z}}\left(\boldsymbol{l}^{(i_j)}\right) = \sum_{k=1}^{m} \frac{p}{N}\boldsymbol{z}_{t+k}\boldsymbol{l}_k^{(i_j)}\ mod(p)$$

$$= \sum_{k=1}^{m} \pi_{t+k}(\boldsymbol{z})\boldsymbol{l}_k^{(i_j)}\ mod(p)$$

Hence, we have $\boldsymbol{z}_j = F_{\boldsymbol{z}}\left(\boldsymbol{l}^{(i_j)}\right) + \pi_j(\boldsymbol{z})\,p$ and consequently $F_{\boldsymbol{z}}\left(\boldsymbol{l}^{(i_j)}\right) \equiv \boldsymbol{z}_j\ mod\,(p)$ for $j = 1, \ldots, t$. Moreover, we can write:

$$\min_{k\in\mathbb{Z}}\left|F_{\boldsymbol{z}}\left(\boldsymbol{l}^{(i_j)}\right) - kp\right| = |\boldsymbol{z}_j - \pi_j(\boldsymbol{z})\,p - kp| < |\boldsymbol{z}_j|$$

and therefore (5) implies that $\left\|F_{\boldsymbol{z}}\left(\boldsymbol{l}^{(i_j)}\right)\right\|_{L,p} < (\gamma_{cvp} + 1)\,N \leq 2^{\Gamma_{\mathrm{cvp}}}N$. Now, we use Lemma 1 with $E = 2^{\Gamma_{\mathrm{cvp}}}N$ and $|A| \leq \mathrm{p^m}$ to find an upper bound for δ_I, for each fixed I, as follows:

$$\delta_I \leq p^m(2E)^t p^{(m-1)t} / \left|D(\mathbb{Z}_p^{t\times m})\right|$$

where $D(\mathbb{Z}_p^{t\times m})$ denotes the number of matrices in the set $\mathbb{Z}_p^{t\times m}$ with distinct non-zero rows which is equal to $(p^m-1)(p^m-2)\cdots(p^m-t)$. Hence, the probability δ of a uniformly chosen matrix $\boldsymbol{M} \in D(\mathbb{Z}_p^{n\times m})$ for which there exists at least a subset of indices $I = \{i_1, \cdots, i_t\} \subseteq \{1, \cdots, n\}$ such that $\boldsymbol{M}_I$ is bad, is at most:

$$\delta \leq \frac{\binom{n}{t} p^m (2E)^t p^{(m-1)t}}{(p^m-1)(p^m-2)\cdots(p^m-t)} \tag{7}$$

Note that in obtaining (7) we have used the union bound and the fact that the number of subsets of the set $\{1, \cdots, n\}$ with t elements is equal to $\binom{n}{t}$.

In the following discussion, we prove that if $k \geq k_0'$, then the right-hand side of the inequality (7) is less than δ_c. First, note that the condition $k.\eta \geq 1$ is implied by $k \geq k_0'$ because $k_0' \triangleq \frac{1}{1-\frac{m}{t}}(\log\left(\delta_c^{-\frac{1}{t}}.n\right) + \Gamma_{\mathrm{cvp}} + 2)$ and according to the definition of η, $k.\eta$ is equal to $k\left(1 - \frac{m}{t}\right) - \log\left(\delta_c^{-\frac{1}{t}}.n\right) - \Gamma_{\mathrm{cvp}} - 1$. Since

$2^k \leq p$, the condition $k.\eta \geq 1$ implies that $p^\eta \geq 2$. Let R denote the value $\frac{p^{mt}}{(p^m-1)(p^m-2)\cdots(p^m-t)}$. From (7) we conclude that the sufficient condition for $\delta \leq \delta_c$ is

$$N \leq \frac{1}{2^{\Gamma_{\mathrm{cvp}}+1}} \left(\delta_c p^{t-m}/R \, \binom{n}{t}\right)^{\frac{1}{t}} \tag{8}$$

Since $k'_0 \geq log(2t)$, it follows that $p^m - i \geq p^m - t \geq \frac{p^m}{2}$ for $i = 1,\ldots,t$, therefore $(p^m-1)(p^m-2)\cdots(p^m-t) \geq \frac{p^{mt}}{2^t}$,and so $R^{\frac{1}{t}} \leq 2$. Moreover, we observe that $\binom{n}{t}^{\frac{1}{t}} \leq (n^t)^{\frac{1}{t}} = n$, and since $N \triangleq \left\lfloor \frac{p^\eta}{2} \right\rfloor$ we have $N \leq \frac{p^\eta}{2}$. Therefore, according to the definition of η, (8) is implied by satisfying the following condition:

$$\zeta \geq \left[\Gamma_{cvp} + log\left(\delta_c^{-\frac{1}{t}} n\right) + 1\right] / logp \tag{9}$$

However, (9) is fulfilled by the choice of parameter ζ used in the proposed scheme.

Finally, we need to show that the proposed scheme is asymptotically correct. To this aim, $\delta_c = O(1/poly(k))$ results in $\delta_c^{-1/t} = O(poly(k))$. Therefore, for any $\delta > 0$, δ-correctness is achieved whenever k is chosen sufficiently large such that $\delta > \delta_c$ and $k \geq O(\log(nkt) + \Gamma_{\mathrm{cvp}} + 2)$. Note that $\frac{\log k}{k} = o(1)$, therefore k can be chosen sufficiently large in order to satisfy the mentioned conditions. ∎

5.2 Security

In this section, we prove that our proposed TSSS scheme is secure according to Definition 3.

Theorem 5 (Security): The proposed TSSS is asymptotically $Int(t - \frac{t}{m})$-secure when $s \leftarrow U_{\mathbb{Z}_p}$ and $\delta_c = O(1/poly(k))$. More precisely, for any $0 < \delta_c < 1$ the proposed TSSS is $(t_s, \delta_s, \epsilon_s, s \leftarrow U_{\mathbb{Z}_p})$-secure, choosing the parameters as follows:

$$t_s \leq \left\lfloor (t - t/m)/(1 + \frac{t/m}{k}\left(log\left(\delta_c^{-\frac{1}{t}} n\right) + \Gamma_{cvp} + 1\right)) \right\rfloor$$

$$\delta_s = \delta_c, \quad \epsilon_s = (\sigma+7)(t_s+m) + 1 , \quad \sigma = \frac{\log(2\delta_c^{-1}\binom{n}{t_s})}{t_s + m - 1}$$

$$k \geq k_0 = max(k'_0 + \frac{(\sigma+3)(\mathrm{t/m} + 1)}{1 - m/t}, \ Z),$$

where k'_0 is defined as in Theorem 4 and

$$Z = \begin{cases} \frac{A+B+C+\frac{m}{t_s}}{D}, & t_s < m \\ \frac{A+B+C+1}{D}, & t_s \geq m \end{cases}$$

where

$$A = \log\left(2\delta_c^{-1}\binom{n}{t_s}\right) + \Gamma_{cvp} + 3$$
$$B = \left(1 + \frac{m}{t_s}\right)\log(t_s + m)$$
$$C = \left(1 + \frac{m}{t_s}\right)(\sigma+3)(t_s+m-1)$$
$$D = m(\frac{1}{t_s} - \frac{1}{t})$$

Proof. Suppose that $I = \{i_1, \cdots, i_{t_s}\} \subseteq \{1, \cdots, n\}$ is a subset of indices and $\boldsymbol{\mu} \in \mathbb{Z}_p^{1\times n}$ is a fixed vector of n shares. Moreover, the vector $\boldsymbol{a} \in \mathbb{Z}_p^{1\times m}$ and the noise vector $(\boldsymbol{e}_{i_1}, \ldots, \boldsymbol{e}_{i_{t_s}}) \in (-N, N)^{1\times t_s}$ are chosen uniformly at random. Let $P_{k,x}(s \mid \boldsymbol{s}_I = \boldsymbol{\mu}_I)$ denote the conditional probability that the secret takes the value s given that the random share vector $\boldsymbol{s}_I = (\boldsymbol{s}_{i_1}, \ldots, \boldsymbol{s}_{i_{t_s}})$ takes the value $\boldsymbol{\mu}_I = (\boldsymbol{\mu}_{i_1}, \ldots, \boldsymbol{\mu}_{i_{t_s}})$. In view of the fact that $p > 2N$, for each $\boldsymbol{a} \in \mathbb{Z}_p^{1\times m}$, there exists at most a noise vector $(\boldsymbol{e}_{i_1}, \ldots, \boldsymbol{e}_{i_{t_s}}) \in (-N, N)^{1\times t_s}$ such that $\boldsymbol{l}^{(i_j)}\boldsymbol{a}^T + \boldsymbol{e}_{i_j} \equiv \boldsymbol{\mu}_{i_j} mod(p)$ for $j = 1, \ldots, t_s$. Hence, we have:

$$P_{k,x}(s \mid \boldsymbol{s}_I = \boldsymbol{\mu}_I) = \frac{\left|\left\{\boldsymbol{a} \in \mathbb{Z}_p^{1\times m} : \left\|\boldsymbol{l}^{(i_j)}\boldsymbol{a}^T - \boldsymbol{\mu}_{i_j}\right\|_{L,p} < N, \ \forall j \in I, \ \boldsymbol{a}_1 \equiv s \ mod(p)\right\}\right|}{\left|\left\{\boldsymbol{a} \in \mathbb{Z}_p^{1\times m} : \left\|\boldsymbol{l}^{(i_j)}\boldsymbol{a}^T - \boldsymbol{\mu}_{i_j}\right\|_{L,p} < N , \ \forall j \in I\right\}\right|}$$

Now, for some integers $s' \geq 0$, $q \geq 1$, define the following set:

$$S_{s',q} \triangleq \left\{\boldsymbol{a} \in \mathbb{Z}_p^{1\times m} : \left\|\boldsymbol{l}^{(i_j)}\boldsymbol{a}^T - \boldsymbol{\mu}_{i_j}\right\|_{L,p} < N \quad \forall j \in I , \ \boldsymbol{a}_1 \equiv s' \ mod(q)\right\}$$

Consequently, we have:

$$P_{k,x}(s \mid \boldsymbol{s}_I = \boldsymbol{\mu}_I) = |S_{s,p}|/|S_{0,1}| \tag{10}$$

In the following, we try to find a lower bound on the value $|S_{0,1}|$ and an upper bound on the value $|S_{s,p}|$ for all but a fraction δ_I of inappropriate choices of $\boldsymbol{M}_I \in D(\mathbb{Z}_p^{t\times m})$. Moreover, according to (10) we can find an upper bound on the probability $P_{k,x}(s \mid \boldsymbol{s}_I = \boldsymbol{\mu}_I)$ for the fraction $1 - \delta_I$ of appropriate choices of $\boldsymbol{M}_I \in D(\mathbb{Z}_p^{t_s\times m})$. First of all, we use the following lemma which indicates that $|S_{s',q}|$ is equal to the number of points in the intersection of a particular lattice and a hypercube of side length $2N$.

Lemma 2: Let us fix integers m, t_s, p, N and q such that $p \geq 2N$ and p is divisible by q. Moreover, let $s' \in \mathbb{Z}_q$, $\boldsymbol{l}^{(\mathrm{i})} = \left(\boldsymbol{l}_1^{(\mathrm{i})}, \ldots, \boldsymbol{l}_m^{(\mathrm{i})}\right) \in \mathbb{Z}_p^{1\times m}$ for $i = 1, \ldots, n$, and $\boldsymbol{\mu}_I = \left(\boldsymbol{\mu}_{i_1}, \ldots, \boldsymbol{\mu}_{i_{t_s}}\right) \in \mathbb{Z}_p^{1\times t_s}$. Now, consider matrices $\boldsymbol{M}_{n\times m}$ and $(\boldsymbol{M}_I)_{t_s\times m}$ such that $\boldsymbol{M}_{ij} = \boldsymbol{l}_j^{(i)}$ for $i = 1, \ldots, n$, $j = 1, \ldots, m$ and $(\boldsymbol{M}_I)_{rs} = \boldsymbol{l}_s^{(i_r)}$ for $r = 1, \ldots, t_s$, $s = 1, \ldots, m$. Define the lattice $\mathcal{L}_{\boldsymbol{M}_I,q}$ generated by the columns of the following matrix $\boldsymbol{M}'_{\boldsymbol{M}_I,q}$:

$$\begin{bmatrix} p & 0 & \cdots & 0 & ql_1^{(i_1)} & l_2^{(i_1)} & \cdots & l_m^{(i_1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p & ql_1^{(i_{t_s})} & l_2^{(i_{t_s})} & \cdots & l_m^{(i_{t_s})} \\ 0 & 0 & \cdots & 0 & 2Nq/p & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 2N/p & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 2N/p \end{bmatrix}$$

and the following vector

$$\boldsymbol{\mu}_I' = (\theta_1, \ldots, \theta_{t_s}, N\left(1 - \frac{1+2s'}{p}\right), N\left(1-\frac{1}{p}\right), \ldots, N\left(1-\frac{1}{p}\right)),$$

where $\theta_j \triangleq \boldsymbol{\mu}_{i_j} - s'\boldsymbol{l}_1^{(i_j)}$ $j = 1, \ldots, t_s$. Then, the number of elements in the two following sets

$$S_{s',q} \triangleq$$

$$\left\{\boldsymbol{b} \in \mathbb{Z}_p^{1\times m} : \left\|\boldsymbol{l}^{(i_j)}\boldsymbol{b}^T - \boldsymbol{\mu}_{i_j}\right\|_{L,p} < N \quad \forall\ j\ ,\ \boldsymbol{b}_1 \equiv s'\ mod(q)\right\},$$

$$V_{s',q} \triangleq \left\{\boldsymbol{v}\in\mathcal{L}_{\boldsymbol{M}_I,q}: \left\|\boldsymbol{v}-\boldsymbol{\mu}_I'\right\|_\infty < N\right\}$$

are equal.

For the proof of Lemma 2 we refer to Appendix.

Regarding Lemma 2, we are going to find a lower bound on the number of points in the intersection of the lattice $\mathcal{L}_{\boldsymbol{M}_I,q}$ and the set $\mathcal{B}\left(\boldsymbol{\mu}_I', N\right) \triangleq \left\{\boldsymbol{v} \in Q^{t_s+m} : \left\|\boldsymbol{v} - \boldsymbol{\mu}_I'\right\|_\infty < N\right\}$.

Lemma 3 [18]: Suppose that Λ is a full rank lattice in $\mathbb{R}^n$, and $\boldsymbol{\mu} \in \mathbb{R}^n$ is an arbitrary vector and $N > 0$. Then, we have

$$\left|\{\boldsymbol{v} \in \Lambda : \|\boldsymbol{v} - \boldsymbol{\mu}\|_\infty < N\}\right| \geq \left|\{\boldsymbol{v} \in \Lambda : \|\boldsymbol{v}\|_\infty < N - \varepsilon\}\right|$$

where $\varepsilon = \frac{n}{2}\lambda_n(\mathcal{L})$.

Based on Theorem 2 for any lattice Λ we have:

$$\lambda_{t_s+m}(\Lambda).\lambda_1(\Lambda)^{t_s+m-1} \leq \det(\Lambda) \tag{11}$$

Lemma 4: Let m, t_s, p, N, q be positive integers, σ be a positive real number and p is a prime such that $p \geq \max\{2N, 2t_s\}$ and $q \in \{1, p\}$. For each $\boldsymbol{M}_I \in D(\mathbb{Z}_p^{t_s\times m})$ let $\boldsymbol{M}'_{\boldsymbol{M}_I,q}$ be the matrix defined in Lemma 2. Define $\mathcal{L}_{\boldsymbol{M}_I}^{(1)}$ the lattice generated by the columns of the matrix obtained by eliminating the $(t_s+1)^{th}$ row and column of $\boldsymbol{M}'_{\boldsymbol{M}_I,q}$. In the case that $q = 1$, if

$$1 \leq 2^{-(\sigma+3)}\det\left(\mathcal{L}_{\boldsymbol{M}_I,1}\right)^{\frac{1}{t_s+m}} \leq N, \tag{12}$$

then for at least a fraction $1 - 2^{-\sigma(t_s+m)}$ of the matrices $M_I \in D(\mathbb{Z}_p^{t_s\times m})$ we have

$$\lambda_1(\mathcal{L}_{\boldsymbol{M}_I,1}) \geq 2^{-(\sigma+3)}\det\left(\mathcal{L}_{\boldsymbol{M}_I,1}\right)^{\frac{1}{t_s+m}} \tag{13}$$

in the case that $q = p$, if

$$1 \leq 2^{-(\sigma+3)}\det\left(\mathcal{L}_{\boldsymbol{M}_I}^{(1)}\right)^{\frac{1}{t_s+m-1}} \leq N, \tag{14}$$

then for at least a fraction $1 - 2^{-\sigma(t_s+m-1)}$ of the matrices $\boldsymbol{M}_I \in D(\mathbb{Z}_p^{t_s\times m})$ we have

$$\lambda_1(\mathcal{L}_{\boldsymbol{M}_I}^{(1)}) \geq \lambda_1(\mathcal{L}_{\boldsymbol{M}_I,p}) \geq 2^{-(\sigma+3)}\det\left(\mathcal{L}_{\boldsymbol{M}_I}^{(1)}\right)^{\frac{1}{t_s+m-1}} \tag{15}$$

For the proof of Lemma 4 we refer to Appendix.

Now, we turn back to the rest of proof of Theorem 5. For a fixed $\sigma>0$, we say that $\boldsymbol{M}_I \in D(\mathbb{Z}_p^{t_s\times m})$ is bad if at least one of the bounds (13) or (15) does not hold. We denote the fraction of matrices $\boldsymbol{M}_I$ (for $I = \{i_1, \cdots, i_{t_s}\}$) for which $\lambda_1\left(\mathcal{L}_{\boldsymbol{M}_I,q}\right) < \Delta$ by $\delta_I(q)$ where $\mathcal{L}_{\boldsymbol{M}_I,q}$ was defined in Lemma 2. If the conditions given in Lemma 4 hold, then the fraction δ_I of bad matrices $\boldsymbol{M}_I \in D(\mathbb{Z}_p^{t_s\times m})$ is upper bounded as follows:

$$\delta_I \leq \delta_I(1) + \delta_I(p) \leq 2^{-\sigma(t_s+m)}(1+2^\sigma) \tag{16}$$

Suppose that $\boldsymbol{M}_I \in D(\mathbb{Z}_p^{t_s\times m})$ is not bad and the inequality (13) is true, then combine inequality (11) for $\Lambda = \mathcal{L}_{\boldsymbol{M}_I,1}$ with inequality (13) to obtain the inequality $\lambda_{t_s+m}\left(\mathcal{L}_{\boldsymbol{M}_I,1}\right) \leq \det\left(\mathcal{L}_{\boldsymbol{M}_I,1}\right)^{\frac{1}{t_s+m}} 2^{(\sigma+3)(t_s+m-1)}$ which follows that for $\varepsilon = \frac{(t_s+m)}{2}\lambda_{t_s+m}\left(\mathcal{L}_{\boldsymbol{M}_I,1}\right)$ we have $\varepsilon \leq \frac{(t_s+m)}{2}\det\left(\mathcal{L}_{\boldsymbol{M}_I,1}\right)^{\frac{1}{t_s+m}} 2^{(\sigma+3)(t_s+m-1)}$, and as a result if we use Lemma 3 for $\Lambda = \mathcal{L}_{\boldsymbol{M}_I,1}$ and $\varepsilon = \frac{(t_s+m)}{2}\lambda_{t_s+m}\left(\mathcal{L}_{\boldsymbol{M}_I,1}\right)$ we conclude that $|V_{0,1}| \geq |\{\boldsymbol{v} \in \mathcal{L}_{\boldsymbol{M}_I,1} : \|\boldsymbol{v}\|_\infty < N - \varepsilon\}|$. Therefore, if

$$\mathrm{X} \triangleq \frac{(t_s+m)}{2}\det\left(\mathcal{L}_{\boldsymbol{M}_I,1}\right)^{\frac{1}{t_s+m}} 2^{(\sigma+3)(t_s+m-1)} \leq \frac{N}{2}$$

by using the Blichfeldt-Corpot theorem (Theorem 3) we find out that $|V_{0,1}| \geq 2Int(\mathrm{Y}) + 1$ where $\mathrm{Y} \triangleq \frac{(N/2)^{t_s+m}}{2^{t_s+m}\det\left(\mathcal{L}_{\boldsymbol{M}_I,1}\right)}$. Moreover, if $\mathrm{X} \leq \frac{N}{2}$ then $\mathrm{Y} \geq 1$, and so $2Int(\mathrm{Y}) + 1 \geq \mathrm{Y}$ and therefore, $|V_{0,1}| \geq \mathrm{Y}$. Furthermore, the inequality $\mathrm{X} \leq \frac{N}{2}$ results in the right hand side of (12).

To summarize the discussion above, we proved that:

$$|V_{0,1}| \geq \frac{(N/2)^{t_s+m}}{2^{t_s+m}\det\left(\mathcal{L}_{\boldsymbol{M}_I,1}\right)} \tag{17}$$

provided that $\boldsymbol{M}_I$ is not bad; $p \geq \max\{2N, 2t_s\}$; the left hand side of (12) and the inequality $(t_s+m)\, 2^{(\sigma+3)(t_s+m-1)}\det\left(\mathcal{L}_{\boldsymbol{M}_I,1}\right)^{\frac{1}{t_s+m}} \leq N$ hold.

Lemma 5: Suppose that $\mathcal{L}_{\boldsymbol{M}_I,p}$ and $\mathcal{L}_{\boldsymbol{M}_I}^{(1)}$ are the lattices defined in Lemma 4, $\boldsymbol{\mu}_I'$ is the vector defined in lemma 2 and $\boldsymbol{\mu}_I''$ is the vector obtained from

$\boldsymbol{\mu}_I^{'}$ by eliminating its $(t_s+1)^{th}$ coordinate. Then $\left|V_{s',p}\right| \leq \left|V_{s',p}^{(1)}\right|$ where

$$V_{s',p} \triangleq \left\{\boldsymbol{w} \in \mathcal{L}_{\boldsymbol{M}_I,p}: \left\|\boldsymbol{w}-\boldsymbol{\mu}_I^{'}\right\|_\infty < N\right\}$$

$$V_{s',p}^{(1)} \triangleq \left\{\boldsymbol{w} \in \mathcal{L}_{\boldsymbol{M}_I}^{(1)}: \left\|\boldsymbol{w}-\boldsymbol{\mu}_I^{''}\right\|_\infty < N\right\}.$$

For the proof of Lemma 5 we refer to the Appendix.

Lemma 6 [18]*:* For any full rank lattice Λ in $\mathbb{R}^n$, vector $\boldsymbol{\mu} \in \mathbb{R}^n$, and $N > 0$, we have

$$|\{\boldsymbol{v} \in \Lambda : \|\boldsymbol{v}-\boldsymbol{\mu}\|_\infty < N\}| \leq \left(\frac{2N}{\lambda_1(\Lambda)}+1\right)^n.$$

Now, we return to the rest of the proof of Theorem 5. Suppose that $\boldsymbol{M}_I \in D(\mathbb{Z}_p^{t_s\times m})$ is not bad, then by Lemma 5 and 6 we conclude that

$$|V_{s,p}| \leq \left|V_{s,p}^{(1)}\right| \leq \left(\frac{2N}{\lambda_1\left(\mathcal{L}_{\boldsymbol{M}_I}^{(1)}\right)}+1\right)^{t_s+m-1}$$

Moreover, according to lemma 4, if $p \geq \max\{2N, 2t_s\}$ and $1 \leq 2^{-(\sigma+3)}\det(\mathcal{L}_{\boldsymbol{M}_I}^{(1)})^{\frac{1}{t_s+m-1}} \leq N$, then $\lambda_1(\mathcal{L}_{\boldsymbol{M}_I}^{(1)}) \geq 2^{-(\sigma+3)}\det\left(\mathcal{L}_{\boldsymbol{M}_I}^{(1)}\right)^{\frac{1}{t_s+m-1}}$, which results in the inequality $|V_{s,p}| \leq \left(\frac{2N}{2^{-(\sigma+3)}\det\left(\mathcal{L}_{\boldsymbol{M}_I}^{(1)}\right)^{\frac{1}{t_s+m-1}}}+1\right)^{t_s+m-1}$.

Since we supposed that $2^{-(\sigma+3)}\det\left(\mathcal{L}_{\boldsymbol{M}_I}^{(1)}\right)^{\frac{1}{t_s+m-1}} \leq N$, we have $\frac{2N}{2^{-(\sigma+3)}\det\left(\mathcal{L}_{\boldsymbol{M}_I}^{(1)}\right)^{\frac{1}{t_s+m-1}}} \geq 1$ and hence

$$\frac{2N}{2^{-(\sigma+3)}\det(\mathcal{L}_{\boldsymbol{M}_I}^{(1)})^{\frac{1}{t_s+m-1}}}+1 \leq 2\times\frac{2N}{2^{-(\sigma+3)}\det(\mathcal{L}_{\boldsymbol{M}_I}^{(1)})^{\frac{1}{t_s+m-1}}}$$

As a result, we have the following inequality

$$|V_{s,p}| \leq \left(2\times\frac{2N}{2^{-(\sigma+3)}\det\left(\mathcal{L}_{\boldsymbol{M}_I}^{(1)}\right)^{\frac{1}{t_s+m-1}}}\right)^{t_s+m-1}$$

$$\leq 2^{(\sigma+5)(t_s+m-1)}N^{t_s+m-1}/\det\left(\mathcal{L}_{\boldsymbol{M}_I}^{(1)}\right).$$

To summarize the discussion above, we proved that:

$$|V_{s,p}| \leq 2^{(\sigma+5)(t_s+m-1)}N^{t_s+m-1}/\det\left(\mathcal{L}_{\boldsymbol{M}_I}^{(1)}\right) \quad (18)$$

provided that $\boldsymbol{M}_I \in D(\mathbb{Z}_p^{t_s\times m})$ is not bad, and the inequalities $p \geq \max\{2N, 2t_s\}$ and $1 \leq 2^{-(\sigma+3)}\det(\mathcal{L}_{\boldsymbol{M}_I}^{(1)})^{\frac{1}{t_s+m-1}} \leq N$ hold.

Suppose that the above sufficient conditions for holding the inequalities (17) and (18) are satisfied. Then, at least with probability $1-\delta_I$, the following inequality holds:

$$p_{(1^k,x)}(s \mid \boldsymbol{s}_I = \boldsymbol{\mu}_I) = |V_{s,p}|/|V_{0,1}| < 2^{(\sigma+7)(t_s+m)+1}/p$$

As a result, the secret entropy loss is upper bounded as follows:

$$leak_{(1^k,x)}\left(\boldsymbol{\mu}_{i_1},\ldots,\boldsymbol{\mu}_{i_{t_s}}\right) \leq (\sigma+7)(t_s+m)+1 = \epsilon_s,$$

with probability at least $1-\delta_I$, for a fixed subset of indices$I = \{i_1,\cdots,i_{t_s}\} \subseteq \{1,\cdots,n\}$, a fixed vector $\boldsymbol{\mu}_I = (\boldsymbol{\mu}_{i_1},\ldots,\boldsymbol{\mu}_{i_{t_s}}) \in \mathbb{Z}_p^{1\times t_s}$ and a uniformly distributed $M_I \in D(\mathbb{Z}_p^{t_s\times m})$. Finally, using union bound probability, we conclude that $leak_{(1^k,x)}\left(\boldsymbol{\mu}_{j_1},\ldots,\boldsymbol{\mu}_{j_{t_s}}\right) \leq \epsilon_s$ does not hold for at least some subset of indices $J = \{j_1,\cdots,j_{t_s}\} \subseteq \{1,\cdots,n\}$ with probability at most $\delta = \binom{n}{t_s}2^{1-\sigma(t_s+m-1)}$. Note that we have $\delta \leq \delta_c$ if we choose $\sigma = \frac{\log(2\delta_c^{-1}\binom{n}{t_s})}{t_s+m-1}$.

Now, we prove that by choosing t_s and k_0 as mentioned in Theorem 5, the sufficient conditions for holding the inequalities (16) and (17) are satisfied. First, note that the left inequality of (12) implies the left inequality of (14). Moreover, assume that $2^{(\sigma+3)(\frac{t}{m}+1)} \leq 2N$, then the left inequality of (12) holds. Therefore, Since $2N > p^\eta - 2$ and $p \geq 2^k$, it follows that the sufficient condition for realizing the left inequality of (12) is $2^{(\sigma+3)(\frac{t}{m}+1)+1} \leq 2^{k\eta}$ which is satisfied by the condition,

$$k \geq k_0^{'} + \frac{1}{1-\frac{m}{t}}(\sigma+3)(\frac{t}{m}+1).$$

Moreover, owing to the fact that $2^k \leq p$ and $\frac{p^\eta}{4} \leq N = \left\lfloor\frac{p^\eta}{2}\right\rfloor$, the sufficient condition for $(t_s+m)\,2^{(\sigma+3)(t_s+m-1)}\det(\mathcal{L}_{\boldsymbol{M}_I,1})^{\frac{1}{t_s+m}} \leq N$ when $t_s \leq m$ is:

$$k > \frac{A+B+C+\frac{m}{t_s}}{D},$$

and since $p \leq 2^{k+1}$ and $\frac{p^\eta}{4} \leq N$, the sufficient condition for $(t_s+m)\,2^{(\sigma+3)(t_s+m-1)}\det(\mathcal{L}_{\boldsymbol{M}_I,1})^{\frac{1}{t_s+m}} \leq N$ when $t_S \geq m$ is:

$$k > \frac{A+B+C+1}{D},$$

where A, B, C and D are defined as in Theorem 5. Finally, we observe that the right inequality of (14) is obtained by the condition

$$p^{\frac{t_s-m+1}{t_s+m+1}} \leq 2^{(\sigma+3)} - \frac{m-1}{t_s+m-1}N^{\frac{t_s}{t_s+m-1}}$$

which is satisfied by the condition

$$t_s \leq \frac{(t-\frac{t}{m})}{1+\frac{\frac{t}{m}}{k}\left(log\left(\delta_c^{-\frac{1}{t}}n\right)+\Gamma_{cvp}+1\right)}$$

mentioned in Theorem 5.

Since $\delta_c = O(1/poly(k))$, we have $\delta_s = \delta_c = o(1)$. Since $\binom{n}{t_c} < n^{t_s}$, it follows that $t_s = \left\lfloor\frac{t-\frac{t}{m}}{1+o(1)}\right\rfloor$, and thus $t_s = Int(t-t/m)$ when k is sufficiently large.

Therefore, $\sigma = O(\log(k)\ )$ and $\epsilon_s = o(k)$. This completes the proof of security of the proposed scheme. ■

5.3 Parameter Analysis

In this section, we discuss the effects of the parameters m and t_s on the correctness and security parameters, as follows.

According to Theorem 4, if it is necessary for the (t, n)-TSSS to be δ_c-correct for some fixed n, t, δ_c and Γ_{cvp},while $2 \le m \le t-1$, then choosing a greater value for m implies choosing a larger value for k which in turn implies the larger p. It means that more computations are required. Therefore, it seems that choosing a smaller value for m is more appropriate.

Now, we are interested in studying the effect of the parameter m on the security of our scheme that is discussed in Theorem 5. With this aim in view, let us fix some value for $\delta_c = \delta_s$ in the interval $(0, 1)$. Moreover, we suppose that our scheme is $(t_s,\ \delta_s,\ \epsilon_s,\ s \leftarrow U_{\mathbb{Z}_p})$-secure requiring that all conditions stated in Theorem 5 are satisfied.

Let $Q = \log\left(\delta_c^{-\frac{1}{t}}.n\right)\ + \Gamma_{\text{cvp}} + 1$, then

$$t_s \le \left\lfloor \frac{t - \frac{t}{m}}{1 + \frac{t}{mk}Q} \right\rfloor \qquad (19)$$

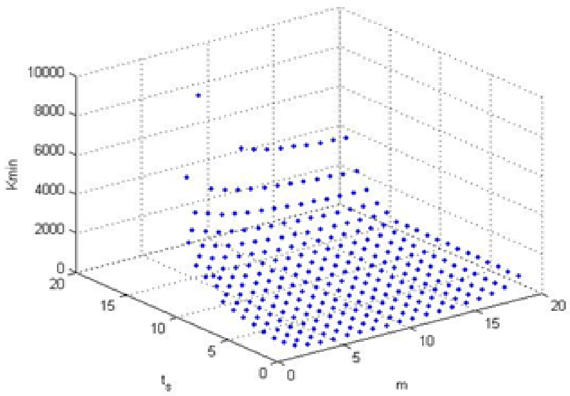

Figure 1. k_{min} as a function of m and t_s for parameters $n = 50$, $t = 20$ and $\delta_c = 2^{-30}$.

Since $\frac{t}{mk}Q > 0$, we have $t_s \le \lfloor t - \ \frac{t}{m} \rfloor$. Moreover, we conclude from (19) that:

$$\frac{t}{mk}Q \le \frac{t - \frac{t}{m}}{t_s} - 1,$$

and since $t_s \le t - \ \frac{t}{m}$ we have:

$$k \ge \frac{tQt_s}{m\,(t - t_s) - t}$$

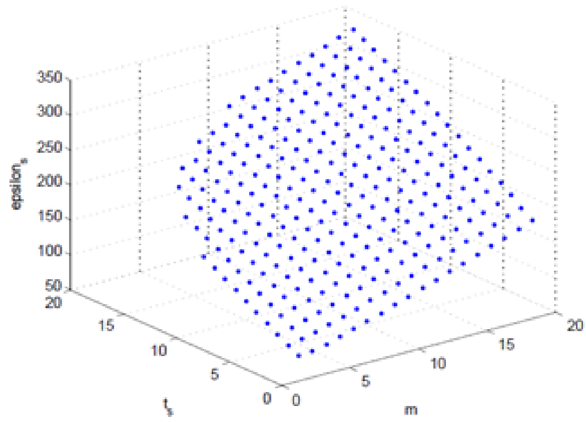

Figure 2. ϵ_s *as a function of* m *and* t_s *for parameters* $n = 50$, $t = 20$ *and* $\delta_c = 2^{-30}$.

Let $B = \frac{tQt_s}{m(t-t_s)-t}$. So, the following lower bound for the security parameter k is obtained:

$$k \ge \max\left(k_0,\ B\right) \triangleq k_{min}$$

Figure 1 shows the effects of m and t_s on k_{min} for $n = 50$, $t = 20$, and $\delta_c = 2^{-30}$. Furthermore, the effects of m and t_s on

$$\epsilon_s = \left(\frac{\log\left(2\delta_c^{-1}\binom{n}{t_s}\right)}{t_s + m - 1} + 7 \right)(t_s + m) +\ 1;$$

$$2 \le m \le t - 1,\ 1 \le t_s \le \left\lfloor t - \ \frac{t}{m} \right\rfloor$$

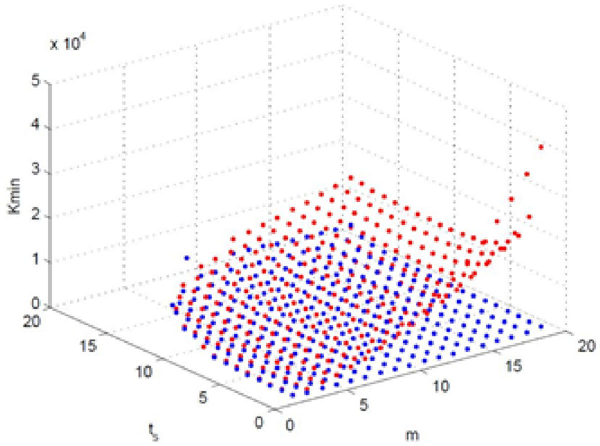

Figure 3. Comparison between k_{min} of the TSSS scheme proposed in [14] *(red points)* and k_{min} of the TSSS scheme proposed in this paper *(blue points)* for parameters $n = 50$, $t = 20$ and $\delta_c = 2^{-30}$.

is shown in Figure 2, where the same values are chosen for the parameters n, t, and δ_c. In this way, we suppose that the parameters m and t_s are chosen prior to the choice of the parameters k and ϵ_s such that the proposed scheme is $(t_s,\ \delta_s,\ \epsilon_s,\ s \leftarrow U_{\mathbb{Z}_p})$-secure.

Figure 1 and Figure 2 show that for a fixed m, any increase in the parameter t_s implies that k_{min} and ϵ_s being increased, as expected from Definition 4 (security). In fact, from Definition 4 we conclude that in a (t, n) TSSS with the fixed parameter m, the entropy loss is an increasing function of the number of observed shares t_s.

Moreover, Figure 1 shows that for a fixed t_s the amount of k_{min} is a decreasing function of the lattice dimension m. This fact represents a tradeoff between correctness and security of the scheme with respect to the choice of m.

In this paper we improved the amount of parameter Z, defined in Theorem 5 and used for choosing the security parameter k. The smaller value of Z results in the smaller security parameter k. Figure 3 compares the effects of m and t_s on k_{min} for the proposed TSSS and [14], where $n = 50$, $t = 20$ and $\delta_c = 2^{-30}$. Figure 3 shows that less computations are required for a certain amount of security in the proposed TSSS in comparison with [14].

6 Conclusion

In this paper, we have introduced a (t, n) TSSS based on lattice construction. Such a scheme is useful for distributing the share values securely using a lattice-based public key primitive. By this motivation, a new TSSS which is consistent with lattice nature of the underlying primitive, is designed. We have analyzed the proposed scheme by proving its asymptotic correctness, due to the probabilistic construction of the share values. Moreover, we have given a quantitative proof of its asymptotic security from the information theoretic viewpoint. Finally, we have studied the effect of the parameters on the security and correctness of our scheme.

References

[1] O. Goldreich, S. Goldwasser, and S. Halevi. “Public-key cryptosystems from lattice reduction problems.” Advances in Cryptology CRYPTO’97, pp. 112-131, Springer Berlin Heidelberg, 1997.

[2] J. Hoffstein, J. Pipher, and J.H. Silverman. “NTRU: A ring-based public key cryptosystem.” In International Algorithmic Number Theory Symposium, pp. 267-288. Springer Berlin Heidelberg, 1998.

[3] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography.” Journal of the ACM (JACM) vol. 56, no. 6, p. 34, 2009.

[4] A. Shamir, “How to share a secret.” Communications of the ACM 22, no. 11, pp.612-613, 1979.

[5] G.R. Blakeley, “Safeguarding cryptographic keys.” Proc. of the National Computer Conference, vol. 48, pp. 313-317, 1979.

[6] C. Asmuth, and J. Bloom. “A modular approach to key safeguarding.” IEEE transactions on information theory, vol.30, no. 2, pp. 208-210, 1988.

[7] L. J. Pang, and Y.M. Wang. “A new multi-secret sharing scheme based on Shamir’s secret sharing.” Applied Mathematics and Computation, vol. 167, no. 2, pp. 840-848, 2005.

[8] K. M Martin, J. Pieprzyk, R. Safavi-Naini, and H. Wang, “Changing thresholds in the absence of secure channels.” In Australasian Conference on Information Security and Privacy, pp. 177-191, Springer Berlin Heidelberg, 1999.

[9] T. P. Pedersen, “Non-interactive and information-theoretic secure verifiable secret sharing.” In Annual International Cryptology Conference, pp. 129-140. Springer Berlin Heidelberg, 1991.

[10] D. Chaum, C. Crépeau, and I. Damgard. “Multiparty unconditionally secure protocols.” In Proceedings of the twentieth annual ACM symposium on Theory of computing, pp. 11-19. ACM, 1988.

[11] K. Q. Nguyen and J. Traoré. “An online public auction protocol protecting bidder privacy.” In Australasian Conference on Information Security and Privacy, pp. 427-442, Springer Berlin Heidelberg, 2000.

[12] B. Schoenmakers, “A simple publicly verifiable secret sharing scheme and its application to electronic voting.” In Annual International Cryptology Conference, pp. 148-164. Springer Berlin Heidelberg, 1999.

[13] Thien, Chih-Ching, and Ja-Chen Lin. “Secret image sharing.” Computers & Graphics, vol. 26, no. 5, pp. 765-770, 2002.

[14] H. A. Khorasgani, S. Asaad, T. Eghlidos, & M. R. Aref. “A lattice-based threshold secret sharing scheme”. In 11^{th} International ISC Conference on. Information Security and Cryptology (ISCISC), pp. 173-179, 2014.

[15] R. El Bansarkhani, and M. Meziani. “An efficient lattice-based secret sharing construction.” In IFIP International Workshop on Information Security Theory and Practice, pp. 160-168. Springer Berlin Heidelberg, 2012.

[16] A. Georgescu, “A LWE-based secret sharing scheme.” IJCA Special Issue on Network Security and Cryptography, NSC, no. 3, pp. 27-29, 2011.

[17] S. Asaad, H.A. Khorasgani, T. Eghlidos and M. R. Aref, “Sharing secret using lattice construction”, In Telecommunications (IST), 7^{th} International Symposium on, pp. 901-906, 2014.

[18] R. Steinfeld, J. Pieprzyk, and H. Wang. “Lattice-based threshold changeability for standard Shamir secret-sharing schemes.” Information Theory, IEEE Transactions on, vol. 53, no. 7, pp.

2542-2559, 2007.

[19] L. Babai, “On Lovász lattice reduction and the nearest lattice point problem.” Combinatorica, vol. 6, no. 1, pp. 1-13, 1986.

[20] A. K. Lenstra, H. W. Lenstra, and L. Lovász. “Factoring polynomials with rational coefficients.” Mathematische Annalen, vol. 261, no. 4, pp. 515-534, 1982.

[21] D. Micciancio, S. Goldwasser. “Complexity of Lattice Problems, A Cryptographic Perspective.” 1^{st} Ed., Springer, 2002.

Hamidreza Amini Khorasgani received two B.S. degrees in electrical engineering (communications) and pure mathematics from Isfahan University of Technology, Isfahan, Iran and the M.S. degree in electrical engineering (communication cryptology) from Sharif University of Technology, Tehran, Iran in 2012 and 2014, respectively. His research interests include information theory, coding theory, and cryptography with an emphasis on lattices and secure computations.

Saba Asaad received her B.S. degree in electrical engineering and the M.S. degree in communication systems from the Sharif University of Technology, Tehran, Iran, in 2012 and 2014, respectively. She is currently working on her Ph.D. dissertation in the school of electrical and computer engineering of University of Tehran. Her research interests are information theory, wireless system and cryptography.

Hossein Pilaram received his B.S. degree in Electrical Engineering and the M.S. degree in Communication Systems from the Sharif University of Technology, Tehran, Iran, in 2010 and 2012, respectively. He is currently working on his Ph.D. dissertation at the department of electrical engineering of Sharif University of Technology. His research interests are cryptography, coding theory, and mobile networks.

Taraneh Eghlidos received her B.S. degree in Mathematics in 1986, from the University of Shahid Beheshti, Tehran, Iran, and the M.S. degree in industrial mathematics in 1991 from the University of Kaiserslautern, Germany. She received her Ph.D. degree in Mathematics in 2000, from the University of Giessen, Germany. She joined the Sharif University of Technology in 2002 and she is currently an associate professor in the Electronics Research Institute of SUT. Her research interests include interdisciplinary research areas such as symmetric and asymmetric cryptography, application of coding theory in cryptography, and mathematical modeling for representing and solving real world problems. Her current research interests include lattice based cryptography and code based cryptography.

Mohammad Reza Aref received the B.S. degree in 1975 from the University of Tehran, Iran, and the M.S. and Ph.D. degrees in 1976 and 1980, respectively, from Stanford University, Stanford, CA, USA, all in electrical engineering. He returned to Iran in 1980 and was actively engaged in academic affairs. He was a Faculty member of Isfahan University of Technology from 1982 to 1995. He has been a professor of electrical engineering at Sharif University of Technology, Tehran, since 1995, and has published more than 290 technical papers in communication and information theory and cryptography in international journals and conferences proceedings. His current research interests include areas of communication theory, information theory, and cryptography.

Appendix

Proof of Lemma 2:

Proof. Define the function $f\colon S_{s',q} \longrightarrow V_{s',q}$ which maps an arbitrary vector $\boldsymbol{b}^* = (kq+s', b_2^*, \ldots, b_m^*)$ in $S_{s',q}$ to the vector

$$f(\boldsymbol{b}^*) \triangleq \sum_{i=1}^{t_s} k_i (\boldsymbol{M}'_{M_{I,q}})_{*i} + k(\boldsymbol{M}'_{M_{I,q}})_{*t_s+1} + \sum_{i=2}^{m} b_i^* (\boldsymbol{M}'_{M_{I,q}})_{*t_s+i}$$

where the coefficients $k_1, \ldots, k_{t_s}$ are chosen such that $\left\| f(\boldsymbol{b}) - \boldsymbol{\mu}'_I \right\|_\infty < N$. In the following, we prove that this function is well defined, i.e. there exist unique coefficients $k_1, \ldots, k_{t_s}$ such that $\left\| f(\boldsymbol{b}) - \boldsymbol{\mu}'_I \right\|_\infty < N$.

Moreover, we show that f is one to one and onto. Fix $\boldsymbol{b}=\left(kq+s^{'},b_2^*,\ldots,b_m^*\right)\in S_{s^{'},q}$. Since $0\le kq+s^{'}\le p-1$, and $0\le b_i^*\le p-1$, it follows that for $i=2,\ldots,m$, $\left|k\frac{2Nq}{p}-N(1-\frac{1+2s^{'}}{p})\right|<N$ and $\left|b_i^*\frac{2N}{p}-N(1-\frac{1}{p})\right|<N$. Moreover, due to the fact that for each j we have $\left\|\boldsymbol{l}^{(i_j)}\boldsymbol{b}^T-\boldsymbol{\mu}_{i_j}\right\|_{L,p}<N$, there exists $\tilde{k}_j$ for $j=1,\ldots,t_s$ such that $\left|<\boldsymbol{b},\boldsymbol{l}^{(i_j)}>-\boldsymbol{\mu}_{i_j}+\tilde{k}_jp\right|<N$. Therefore, for $j=1,\ldots,t_s$ the following inequality holds:

$$\left|kq\boldsymbol{l}_1^{(i_j)}+b_2^*\boldsymbol{l}_2^{(i_j)}+\cdots+b_{m-1}^*\boldsymbol{l}_m^{(i_j)}+\tilde{k}_jp-\theta_j\right|<N.$$

Thus, we define $k_j\triangleq\tilde{k}_j$ and we conclude that $\left\|f(\boldsymbol{b})-\boldsymbol{\mu}_I^{'}\right\|_\infty<N$. Now, to prove the uniqueness of k_j's we suppose that there is at least one $1\le j\le t_s$ for which there exists $k_j^{(1)}\ne\tilde{k}_j$ such that

$$\left|kq\boldsymbol{l}_1^{(i_j)}+b_2^*\boldsymbol{l}_2^{(i_j)}+\cdots+b_m^*\boldsymbol{l}_m^{(i_j)}+k_j^{(1)}p-\theta_j\right|<N.$$

The last two inequalities result in $p<\left|\tilde{k}_jp-k_j^{(1)}p\right|<2N$ which contradicts with the assumption and this proves the uniqueness of k_j's. Now, suppose that $\boldsymbol{v}=\sum_{i=1}^{t_s+m}v_i(\boldsymbol{M}^{'}_{\boldsymbol{M}_I,q})_{*i}\in V_{S^{'},q}$, so $\|\boldsymbol{v}-\boldsymbol{\mu}_I^{'}\|_\infty<N$ which results in $0\le v_{t_s+1}q+s^{'}\le p-1$ and $0\le v_{t_s+i}\le p-1$, for $i=2,\ldots,m$. By defining $\boldsymbol{w}\triangleq(v_{t_s+1}q+s^{'},v_{t_s+2},\ldots,v_{t_s+m})\in S_{s^{'},q}$ we have $f(\boldsymbol{w})=\boldsymbol{v}$. Therefore, the function f is onto. It is straightforward to show that f is injective by the definition. ■

Proof of Lemma 4:

Proof. Fix positive integers $\Delta\le 2\mathrm{N}$ and $q\in\{1,p\}$. We denote the fraction of matrices $\boldsymbol{M}_I$ (for $I=\{i_1,\cdots,i_{t_s}\}$) for which $\lambda_1(\mathcal{L}_{\boldsymbol{M}_I,q})<\Delta$ by $\delta_I(q)$. Based on the definition of $\boldsymbol{M}^{'}_{\boldsymbol{M}_I,q}$, any vector $\boldsymbol{v}\in\mathcal{L}_{\boldsymbol{M}_I,q}$ is of the form:

$$\boldsymbol{v}=(\boldsymbol{M}_{\boldsymbol{I}*1}\boldsymbol{a}^{'T}+k_1p,\ldots,\ \boldsymbol{M}_{\boldsymbol{I}*t_s}\boldsymbol{a}^{'T}+k_{t_s}p,\ 2N\boldsymbol{a}_1^{'}/p,\ldots,\ 2N\boldsymbol{a}_m^{'}/p)$$

for some integers $k_1,\cdots,k_{t_s}$ and vector $\boldsymbol{a}^{'}=(\boldsymbol{a}_1^{'},\ldots,\boldsymbol{a}_m^{'})$ in $\mathbb{Z}^m$ such that $\boldsymbol{a}_1^{'}\equiv 0\ mod(q)$. Now, suppose that $\lambda_1(\mathcal{L}_{\boldsymbol{M}_I,q})<\Delta$, so there exists at least a nonzero vector $\boldsymbol{v}=(\boldsymbol{M}_{\boldsymbol{I}*1}\boldsymbol{a}^{'T}+k_1p,\ldots,\ \boldsymbol{M}_{\boldsymbol{I}*t_s}\boldsymbol{a}^{'T}+k_{t_s}p,2N\boldsymbol{a}_1^{'}/p,\ldots,2N\boldsymbol{a}_m^{'}/p)\in\mathcal{L}_{\boldsymbol{M}_I,q}$ such that $\|\boldsymbol{v}\|_\infty<\Delta$, and therefore for each $i=1,\ldots,m$, $\left|2N\boldsymbol{a}_i^{'}/p\right|<\Delta$. But we know that $\Delta\le 2N$, so we conclude that $\left|\boldsymbol{a}_i^{'}\right|<p$ for each $i=1,\ldots,m$. Moreover, owing to the fact that $\boldsymbol{v}$ is a nonzero vector, if for each i, $\boldsymbol{a}_i^{'}=0$ then $\boldsymbol{v}=(k_1p,\ldots,k_{t_s}p,0,\ldots,0)$. So there exists at least one j in $\{1,\ldots,t_s\}$ such that $k_j\ne 0$, therefore $\|\boldsymbol{v}\|_\infty\ge|k_jp|\ge p\ge 2N\ge\Delta$. Thus, the fraction $\delta_I(q)$ is at most equal to the fraction of matrices $\boldsymbol{M}_I\in D(\mathbb{Z}_p^{t_s\times m})$ for which there exists a vector $\boldsymbol{v}\in\mathcal{L}_{\boldsymbol{M}_I,q}$, with $\|\boldsymbol{v}\|_\infty<\Delta$, such that the relations $\boldsymbol{a}^{'}\ne\boldsymbol{0}\ mod\,(p)$ and $\boldsymbol{a}_1^{'}=0\ mod\,(q)$ hold. We denote $\boldsymbol{a}^{'}\ mod\,(p)\ne\boldsymbol{0}$ by $\boldsymbol{a}^{''}$. In case $q=1$, we conclude from $\|\boldsymbol{v}\|_\infty<\Delta$ that $\left\|<\boldsymbol{a}^{''},\ \boldsymbol{M}_{I*j}>\right\|_{L,p}<\Delta$, for $j=1,\ldots,t_s$ and $\left\|\boldsymbol{a}_i^{''}\right\|_{L,p}<\frac{\Delta}{2N}p$ for $i=1,\ldots,m$. Therefore, by Lemma 1 we have:

$$\delta_I(1)\le\frac{\left(\frac{2\Delta}{2N}p+1\right)^m(2\Delta)^{t_s}p^{(m-1)t_s}}{\left(\left|D\left(\mathbb{Z}_p^{t_s\times m}\right)\right|\right)}$$

$$\le\frac{\left(\frac{2\Delta}{N}p\right)^m(2\Delta)^{t_s}p^{(m-1)t_s}}{(p^m-1)(p^m-2)\cdots(p^m-t_s)}$$

and since $p^m-j\ge\frac{p^m}{2}$, for $j=1,\ldots,t_s$, we have $(p^m-1)(p^m-2)\cdots(p^m-t_s)\ge\left(\frac{p^m}{2}\right)^{t_s}$ resulting in $\delta_I(1)\le\frac{\left(\frac{2\Delta}{N}p\right)^m(2\Delta)^{t_s}p^{(m-1)t_s}}{\left(\frac{p^m}{2}\right)^{t_s}}$. Since $\det(\mathcal{L}_{\boldsymbol{M}_I,1})=p^{t_s-m}(2N)^m$, we conclude that $\delta_I(1)\le\frac{2^{2(t_s+m)}\Delta^{t_s+m}}{\det(\mathcal{L}_{\boldsymbol{M}_I,1})}$. It is easy to see that by the choice of $\Delta=\left\lfloor 2^{-(\sigma+2)}\det(\mathcal{L}_{\boldsymbol{M}_I,1})^{\frac{1}{t_s+m}}\right\rfloor$, we have $\delta_I(1)\le 2^{-\sigma(t_s+m)}$ (note that since $1\le 2^{-(\sigma+3)}\det(\mathcal{L}_{\boldsymbol{M}_I,1})^{\frac{1}{t_s+m}}\le N$, by this choice we have $\Delta\le 2\mathrm{N}$). Hence, for at least a fraction $1-2^{-\sigma(t_s+m)}$ of the matrices $\boldsymbol{M}_I$ we have $\lambda_1(\mathcal{L}_{\boldsymbol{M}_I,1})\ge 2^{-(\sigma+3)}\det(\mathcal{L}_{\boldsymbol{M}_I,1})^{\frac{1}{t_s+m}}$.

In case $q=p$, we conclude from $\|\boldsymbol{v}\|_\infty<\Delta$ that $\left\|<\boldsymbol{a}^{''},\ \boldsymbol{M}_{I*j}>\right\|_{L,p}<\Delta$, for $j=1,\ldots,t_s$ and $\left\|\boldsymbol{a}_i^{''}\right\|_{L,p}<\frac{\Delta}{2N}p$, for $i=2,\ldots,m$. Therefore, by Lemma 1 we have:

$$\delta_I(p)\le\frac{\left(\frac{2\Delta}{2N}p+1\right)^{m-1}(2\Delta)^{t_s}p^{(m-1)t_s}}{\left(\left|D\left(\mathbb{Z}_p^{t_s\times m}\right)\right|\right)}$$

with the same approach for $q=1$, we can prove that $\delta_I(p)\le\frac{2^{2(t_s+m-1)}\Delta^{t_s+m-1}}{\det\left(\mathcal{L}^{(1)}_{\boldsymbol{M}_I}\right)}$ which results in $\delta_I(p)\le 2^{-\sigma(t_s+m-1)}$, by the choice of $\Delta=\left\lfloor 2^{-(\sigma+2)}\det\left(\mathcal{L}^{(1)}_{\boldsymbol{M}_I}\right)^{\frac{1}{t_s+m-1}}\right\rfloor$, Therefore, for at least a fraction $1-2^{-\sigma(t_s+m-1)}$ of the matrices $\boldsymbol{M}_I\in D(\mathbb{Z}_p^{t_s\times m})$ we have $\lambda_1(\mathcal{L}_{\boldsymbol{M}_I,p})\ge 2^{-(\sigma+3)}\det\left(\mathcal{L}^{(1)}_{\boldsymbol{M}_I}\right)^{\frac{1}{t_s+m-1}}$. From the definitions of $\mathcal{L}^{(1)}_{\boldsymbol{M}_I}$ and $\mathcal{L}_{\boldsymbol{M}_I,p}$ and similar justification given in the proof of Lemma 4 of [18], we have $\lambda_1(\mathcal{L}^{(1)}_{\boldsymbol{M}_I})\ge\lambda_1(\mathcal{L}_{\boldsymbol{M}_I,p})$. This completes the proof. ■

Proof of Lemma 5:

Proof. We prove this lemma following a similar approach given in the proof of Lemma 5 in [18]. First, we note that if $\boldsymbol{w} \in V_{s',p}$ then there exists some integer k such that $\boldsymbol{w}_{t_s+1} = 2Nk$. Since $\left\|\boldsymbol{w} - \boldsymbol{\mu}_I^{'}\right\|_\infty < N$, it follows that $\left|\boldsymbol{w}_{t_s+1} - N(\frac{1+2s'}{p})\right| < N$, so we have $k = 0$ which results in $\boldsymbol{w}_{t_s+1} = 0$.

Define $f: V_{s',p} \to V_{s',p}^{(1)}$ as a relation between $V_{s',p}$ and $V_{s',p}^{(1)}$ which maps each vector $\boldsymbol{w} \in V_{s',p}$ to vector $\boldsymbol{w}^{(1)} = f(\boldsymbol{w})$, obtained from $\boldsymbol{w}$ by eliminating its $(t_s+1)^{th}$ coordinate. Now, according to the definition of lattices $\mathcal{L}_{\boldsymbol{M}_I,p}$ and $\mathcal{L}_{\boldsymbol{M}_I}^{(1)}$ and the structure of the matrix $\boldsymbol{M}^{'}_{\boldsymbol{M}_I,q}$, it is observed that when $\boldsymbol{w} \in V_{s',p}$ we have $f(\boldsymbol{w}) \in \mathcal{L}_{\boldsymbol{M}_I}^{(1)}$. Moreover, we see that if $\left\|\boldsymbol{w} - \boldsymbol{\mu}_I^{'}\right\|_\infty < N$ then $\left\|f(\boldsymbol{w}) - \boldsymbol{\mu}_I^{''}\right\|_\infty < N$. Therefore, the relation f is a well defined function from $V_{s',p}$ to $V_{s',p}^{(1)}$. Finally, suppose that $f(\boldsymbol{u}) = f(\boldsymbol{w})$ for some $\boldsymbol{u}, \boldsymbol{w} \in V_{s',p}$. Since $\boldsymbol{u}, \boldsymbol{w} \in V_{s',p}$, it follows that $\boldsymbol{u}_{t_s+1} = \boldsymbol{w}_{t_s+1}$ and from $f(\boldsymbol{u}) = f(\boldsymbol{w})$ we conclude that other coordinates of $\boldsymbol{u}$ and $\boldsymbol{w}$ are equal. Hence, f is a one to one function which results in $\left|V_{s',p}\right| \leq \left|V_{s',p}^{(1)}\right|$. ■