Lattice-Based Threshold-Changeability for Standard CRT Secret-Sharing Schemes

Ron Steinfeld, Josef Pieprzyk, Huaxiong Wang
Centre for Advanced Computing – Algorithms and Cryptography
Dept. of Computing, Macquarie University, Australia
{rons, josef, hwang}@ics.mq.edu.au

Abstract

We consider the problem of increasing the threshold parameter of a secret-sharing scheme after the setup (share distribution) phase, without further communication between the dealer and the shareholders. Previous solutions to this problem require one to start off with a non-standard scheme designed specifically for this purpose, or to have secure channels between shareholders. In contrast, we show how to increase the threshold parameter of the *standard* CRT secret-sharing scheme without secure channels between the shareholders. Our method can thus be applied to existing CRT schemes even if they were set up without consideration to future threshold increases.

Our method is a positive cryptographic application for lattice reduction algorithms, and we also use techniques from lattice theory (geometry of numbers) to prove statements about the correctness and information-theoretic security of our constructions.

Keywords: Secret-Sharing, Changeable Threshold, Lattice Reduction, Geometry of Numbers

1 Introduction

Background. A (t, n)-threshold secret-sharing scheme is a fundamental cryptographic primitive, which allows a *dealer* owning a secret to distribute this secret among a group of n *shareholders* in such a way that any t shareholders can reconstruct the secret, but no subset of less than t shareholders can gain information on the secret. Two classical constructions for (t, n) secret-sharing schemes are the integer-based Chinese Remainder Theorem (CRT) scheme [18, 1] and the Shamir polynomial-based scheme [21].

A common application for (t, n) secret-sharing schemes is for achieving *robustness* of distributed security systems. A distributed system is called robust if system security is maintained even against an attacker who manages to break into/eavesdrop up to a certain number of components of the distributed system. For example, access control to a system can be enforced using a secret shared among n system servers using a (t, n)-threshold secret-sharing scheme, while maintaining security if less than t servers are compromised. In such applications, the threshold parameter t must be determined by a security policy, based on an assessment which is a compromise between the value of the protected system and attacker resources and capabilities on the one hand (which require as high a threshold as possible) and user convenience and cost on the other hand (which require as low a threshold as possible). In many settings, the system value and attacker capabilities are likely to change over time, thus requiring the security policy and hence threshold parameter t to *vary over time.* In particular, an increase in system value or attacker capabilities after the initial setup with a relatively low threshold parameter t, will require an increase in the threshold parameter to a higher value $t' > t$. The longer the lifetime of the system, the more likely that such a change will be needed.

Note that we assume that shareholders will cooperate honestly in making the transition to the larger threshold $t' > t$. Indeed, the attacker in our setting is assumed to be an *outsider*.

Previous Solutions. A trivial solution to the problem of increasing the threshold parameter of a (t, n)-threshold secret-sharing scheme to $t' > t$ is for the shareholders to discard their old shares and for the dealer to distribute new shares of a (t', n) secret-sharing scheme to all shareholders. However, this solution is not very attractive, since it requires the dealer to be involved after the setup stage and moreover requires a secure channel between the dealer and each shareholder. Such channels may not exist or may be difficult to establish after the initial setup stage. A much better solution would allow the threshold to be changed at any time without any communication between the dealer and shareholders after the setup stage. Such 'dealer-free' solutions to the threshold increase problem have been proposed in the literature (see related work below), but they all suffer from other disadvantages: either secure channels between the shareholders are required, or they require one to start off with a non-standard (t, n)-threshold scheme designed specifically for threshold changeability.

Our Contributions. In this paper, we present a new method for increasing the threshold of the *standard* CRT (t, n)-threshold secret-sharing scheme[18, 1]. In contrast to previous solutions, our method does not require communication between the dealer and shareholders after the initial setup stage nor between shareholders, and can be applied to existing CRT schemes even if they were set up without consideration to future threshold increase. The basic idea of our method is the following: to increase the threshold from t to $t' > t$, the shareholders add an appropriate amount of random noise to their shares (or delete a certain fraction of the bits of their share) to compute *subshares* which contain *partial* information about (e.g. half the bits of) the original shares. Since the subshares contain only partial information about the original shares, a set of t subshares is no longer sufficient to reconstruct the secret uniquely, but if one observes a sufficiently larger number $t' > t$ of subshares then one can expect the secret to be uniquely determined by these t' subshares (e.g. if the subshares contain only half the information in the original shares then one can expect that $t' = 2t$ subshares will uniquely determine the secret). By replacing the share *combiner* algorithm of the original (t, n)-threshold secret-sharing with an appropriate 'error-correction' algorithm which can uniquely recover the secret from any t' subshares, we obtain the desired threshold increase from t to t', leaving the secret unchanged, and without any secure channels.

Our efficient 'error-correction' combiner algorithm for the CRT secret-sharing scheme is constructed using lattice basis reduction techniques. Thus, our method is a new positive cryptographic application for lattice reduction algorithms. Furthermore, we also use techniques from lattice theory (geometry of numbers) to prove concrete statements about the correctness and security of our construction. Although our threshold-increase method does not yield a perfect (t', n) secret-sharing scheme, we prove useful results about the information-theoretic security of our method. Roughly speaking, we prove that for any desired $\epsilon > 0$, our method can be used to change the threshold to $t' > t$ (meaning that any t' subshares can be used to recover the secret) such that any $t_s < t' - (t'/t)$ observed subshares leak to the attacker at most a fraction ϵ of the entropy of the secret, where ϵ can be made as small as we wish by an appropriate choice of security parameter.

Related Work. Several approaches to changing the parameters of a threshold scheme in the absence of the dealer have been proposed in the literature. The technique of *secret redistribution*[6, 16] involves communication among the shareholders to 'redistribute' the secret using the new threshold parameter. Although this technique can be applied to standard secret-sharing schemes, its disadvantage is the need for secure channels for communication between shareholders. Methods for changing threshold which do not require secure channels have been studied in [4, 14, 15, 13], but they all require the initial secret-sharing scheme to be a non-standard one, specially designed for threshold increase (as a simple example of such a non-standard scheme, the dealer could provide each shareholder with two shares of the secret: one share for a (t, n) scheme and one share for a (t', n) scheme).

Our scheme uses a lattice-based 'error-correction' algorithm which is a slight variant of an algorithm for 'Noisy Chinese Remaindering in the Lee Norm' due to Shparlinski and Steinfeld [22]. The authors of [22] left it as an open problem to find a cryptographic application of their algorithm. Our work shows one such application. We remark also that although the *correctness* proof of our scheme is based on the work of [22], our *security* proof is new and the lattice-based techniques used may be of independent interest. Indeed, our results provide a (probabilistic) lower bound on the number of solutions to the noisy Chinese remaindering problem when the solution is not unique, whereas [22] only analyze the case when the solution is unique (up to an interval).

Strong provable statements on the security of the *standard* CRT secret-sharing scheme have been recently obtained by Quisquater et al [19], improving on previous results by Goldreich et al [8]. Our proven security result for the changeable-threshold variant of the standard CRT scheme uses entirely different techniques. Although our security result for the changeable-threshold CRT scheme is not as strong as those obtained in [19] for the standard CRT scheme, we believe it is still sufficient for many applications.

We would like to remark on the relation between our threshold increase method and the method for making secret-sharing schemes robust against cheating shareholders using error-correction [17]. In both methods, the share combiner (for a scheme with threshold t) receives $t' > t$ 'noisy' shares and applies an error-correction algorithm to overcome the noise and recover the secret. However, the type of noise which needs to be corrected (and hence also the decoding algorithm) is inherently different in the two cases. In the cheater robustness case, the noise vector (whose ith entry is the additive error in the ith share) is bounded in the *Hamming* norm: if the number of cheating shareholders is at most k then we know that up to k of the t' shares will be *arbitrarily corrupted* while the remaining shares will be correct. In our threshold increase case, the noise vector is bounded in the *Lee* norm: we have that *all* t' shares are corrupted but only by a *small* (in absolute value) additive noise. Note that a Hamming-bounded noise is not suitable for our threshold-increase method: we require that all shares be corrupted in an identical manner, to ensure that *any* subset of t shareholders cannot obtain information on the secret, and *any* subset of $t' > t$ shareholders can recover the secret. On the other hand, our Lee-bounded noise error-correction method cannot handle the Hamming-bounded noise where some shares are arbitrarily corrupted.

Chinese Remainder codes are well known in communication applications as error-correction codes [7]. As mentioned above, our share combiner algorithm (and the related algorithm of [22]) can be viewed as an error-correction algorithm for a Chinese Remainder code variant, correcting noise bounded in the Lee norm. However, we are not aware of communication applications for this type of error-correction. In such applications the Hamming-bounded noise seems more relevant. Appropriate Hamming-bounded noise error-correction algorithms for Chinese Remainder Codes are discussed in [8, 5].

Finally, we remark that in a companion paper [23], we show that lattice-based methods can also be used to change the threshold of the standard Shamir[21] polynomial-based secret-sharing scheme. The general ideas and results obtained for the Shamir scheme are analogous to those obtained here for the CRT scheme, although they differ in the details of the lattices involved.

Organization of This Paper. Section 2 presents definitions and known results on lattices, and a number-theoretic lemma that we use. In Section 3, we provide definitions of changeable-threshold secret-sharing schemes and their correctness/security notions. In Section 4 we present the original CRT (t, n)-threshold secret sharing scheme, and our threshold-changing algorithms to increase the threshold to $t' > t$. We then provide concrete proofs of the correctness and security properties of our scheme. To improve the readability of the paper, proofs of some lemmas have been omitted from the main text and included in the Appendix.

2 Preliminaries

2.1 Notation

Lee Norm $\| \cdot \|_{L,\mathbf{p}}$. For a prime p and an integer z we denote *Lee norm of z modulo p* as $\|z\|_{L,p} = \min_{k \in \mathbb{Z}} |z - kp|$. More generally, given a vector of n primes $\mathbf{p} = (p_1, \dots, p_n)$, we denote the *Lee norm of z modulo* $\mathbf{p}$ by $\|z\|_{L,\mathbf{p}} = \max_{1 \le i \le n} \|z\|_{L,p_i}$.

Infinity Norm $\| \cdot \|_\infty$. For a vector $\mathbf{z} = (z_1, \dots, z_n) \in \mathbb{Q}^n$, we denote the infinity norm of $\mathbf{z}$ by $\|\mathbf{z}\|_\infty = \max_{1 \le i \le n} |z_i|$.

Sets. For a set S, we denote by $\#S$ the size of S. For any set S and integer n, we denote by S^n the set of all n-tuples of elements from S and by $D(S^n)$ the set of all n-tuples of *distinct* elements from S. For integer n, we denote by $[n]$ the set $\{1, 2, \dots, n\}$.

2.2 Lattices

Here we collect several known results that we use about lattices, which can be found in [10, 11, 9]. Let $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ be a set of n linearly independent vectors in $\mathbb{R}^n$. The set

$$\mathcal{L} = \{\mathbf{z} \colon \mathbf{z} = c_1 \mathbf{b}_1 + \ldots + c_n \mathbf{b}_n,\ c_1, \dots, c_n \in \mathbb{Z}\}$$

is called an *n-dimensional (full-rank) lattice* with *basis* $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$. Given a basis $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n) \in \mathbb{R}^n$ for a lattice $\mathcal{L}$, we define the associated *basis matrix* $M_{\mathcal{L},\mathbf{B}}$ to be the (full-rank) $n \times n$ matrix whose ith row is the ith basis vector $\mathbf{b}_i$ for $i = 1, \dots, n$. The quantity $|\det(M_{\mathcal{L},\mathbf{B}})|$ is called the *determinant* of the lattice $\mathcal{L}$ and is denoted by $\det(\mathcal{L})$. Although a given lattice $\mathcal{L}$ has an infinite number of bases $\mathbf{B}$, the lattice determinant $\det(\mathcal{L})$ is independent of the choice of $\mathbf{B}$ (i.e. the absolute value of the determinant of any basis matrix of $\mathcal{L}$ is equal to $\det(\mathcal{L})$).

Given a lattice $\mathcal{L}$, the problem of finding a shortest vector in a lattice which is known as the *shortest vector problem*, or SVP. An algorithm is called a *SVP approximation algorithm with $\| \cdot \|_\infty$-approximation factor γ_{SVP}* if it is guaranteed to find a lattice vector such that $\|\mathbf{v}\|_\infty \le \gamma_{SVP} \min_{\mathbf{v} \in \mathcal{L}} \|\mathbf{v}\|_\infty$. The celebrated *LLL algorithm* of Lenstra, Lenstra and Lovász [12] is a polynomial time SVP approximation algorithm with $\| \cdot \|_\infty$-approximation factor $\gamma_{LLL} = n^{1/2} 2^{n/2}$.

In this paper we actually need to solve a variation of SVP called the *closest vector problem* (CVP): given a basis of a lattice $\mathcal{L}$ in $\mathbb{R}^n$ and a "target" vector $\mathbf{t} \in \mathbb{R}^n$, find a lattice vector $\mathbf{v}$ such that $\|\mathbf{v} - \mathbf{t}\|_\infty$ is minimized. An algorithm is called a *CVP approximation algorithm with $\| \cdot \|_\infty$-approximation factor γ_{CVP}* if it is guaranteed to find a lattice vector such that $\|\mathbf{v} - \mathbf{t}\|_\infty \le \gamma_{CVP} \min_{\mathbf{v} \in \mathcal{L}} \|\mathbf{v} - \mathbf{t}\|$. Babai[2] has shown how to convert the LLL algorithm into a polynomial time CVP approximation algorithm with $\| \cdot \|_\infty$-approximation factor $\gamma_{Bab} = n^{1/2} 2^{n/2}$. This algorithm suffices for our application.

We need the following definition of *successive Minkowski minima* of a lattice.

Definition 2.1 (Minkowski Minima). *Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$. For $i = 1, \dots, n$, the ith succesive Minkowski minimum of $\mathcal{L}$, denoted $\lambda_i(\mathcal{L})$, is the smallest real number such that there exists a set $\{\mathbf{b}_1, \dots, \mathbf{b}_i\}$ of i linearly-independent vectors in $\mathcal{L}$ with $\|\mathbf{b}_j\|_\infty \le \lambda_i(\mathcal{L})$ for all $j = 1, \dots, i$.*

Note that $\lambda_1(\mathcal{L})$ is just the shortest infinity-norm over all non-zero vectors in $\mathcal{L}$.

A classical result is Minkowski's "first theorem" in the geometry of numbers.

Theorem 2.1 (Minkowski's First Theorem). *Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$ and let $\lambda_1(\mathcal{L})$ denote the first Minkowski minimum of $\mathcal{L}$ (see Def. 2.1). Then $\lambda_1(\mathcal{L}) \le \det(\mathcal{L})^{\frac{1}{n}}$.*

The following is a generalization of Minkowski's "first theorem", which is due to Blichfeldt and van der Corput(see [10]). The original theorem is general and lower bounds the number of lattice points in any origin-symmetric convex set. However, for our purposes the following special case is sufficient.

Theorem 2.2 (Blichfeldt-Corput). *Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$ and let K denote the origin-centered box $\{\mathbf{v} \in \mathbb{R}^n : \|\mathbf{v}\|_\infty < H\}$ of volume $Vol(K) = (2H)^n$. Then the number of points of the lattice $\mathcal{L}$ contained in the box K is at least $2 \cdot Int\left(\frac{Vol(K)}{2^n \det(\mathcal{L})}\right) + 1$, where for any $z \in \mathbb{R}$, $Int(z)$ denotes the largest integer which is strictly less than z.*

We will also use the following version of Minkowski's "second theorem" in the geometry of numbers [10]. Similarly to above, it is in fact also a special case of the original theorem.

Theorem 2.3 (Minkowski's Second Theorem). *Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$ and let $\lambda_1(\mathcal{L}),\ldots,\lambda_n(\mathcal{L})$ denote the n Minkowski minima of $\mathcal{L}$ (see Definition 2.1). Then $\lambda_1(\mathcal{L}) \cdots \lambda_n(\mathcal{L}) \leq 2^n \det(\mathcal{L})$.*

2.3 A Number-Theoretic Lemma

The following is a fundamental lemma that we use, interestingly, for *both* the correctness and security proofs of our CRT construction. The lemma gives an upper bound on the probability that, for n randomly chosen primes $(p_1, \ldots, p_n)$, there will exist a "small" non-trivial integer z ($0 < z < \widehat{A}$) such that the integer $B \cdot z$ has "small" residues modulo all the primes $p_1, \ldots, p_n$ ($\|B \cdot z\|_{L,p_i} < H$ for all $i = 1, \ldots, n$), where $B \geq H$ is a fixed integer. This lemma is a slight variant of a similar result due to Shparlinski and Steinfeld [22].

Lemma 2.1. *Let $\mathcal{P}_\ell$ denote a set of primes all exceeding 2^ℓ. Fix integers $\widehat{A}$, $\widehat{H} \in \mathbb{Z}_{\widehat{A}}$ and $\widehat{B} \geq \widehat{H}$. Let $\mathcal{E}_{\ell,n}(\widehat{A}, \widehat{H}, \widehat{B}) \subseteq \mathcal{P}_\ell^n$ denote the set of n-component prime vectors $\mathbf{p} = (p_1, \ldots, p_n)$ such that there exists $z \in \mathbb{Z}_{\widehat{A}} \backslash \{0\}$ with $\|\widehat{B} \cdot z\|_{L,\mathbf{p}} < \widehat{H}$. The size of the set $\mathcal{E}_{\ell,n}(\widehat{A}, \widehat{H}, \widehat{B})$ is upper bounded as follows:*

$$\#\mathcal{E}_{\ell,n}(\widehat{A}, \widehat{H}, \widehat{B}) \leq \widehat{A}\left(\frac{2\widehat{H}\log(\widehat{B}\widehat{A} + \widehat{H})}{\ell}\right)^n.$$

Proof. Suppose that $\mathbf{p} = (p_1, \ldots, p_n) \in \mathcal{P}_\ell^n$ is such that there exists $z \in \mathbb{Z}$ such that

$$0 < z < \widehat{A} \qquad \text{and} \qquad \|\widehat{B} \cdot z\|_{L,\mathbf{p}} < \widehat{H}. \tag{1}$$

Then, for each $i \in \{1, \ldots, n\}$, there exists $\delta_i \in \mathbb{Z}$ such $|\delta_i| < \widehat{H}$ and p_i divides $\widehat{B} \cdot z + \delta_i$. It follows that $p_i \in S_z$ for all $i \in \{1,...,n\}$, where S_z is the set of prime divisors in $\mathcal{P}_\ell$ of all integers in the interval $I(z, \widehat{H}) = [\widehat{B} \cdot z - (\widehat{H} - 1), \widehat{B} \cdot z + (\widehat{H} - 1)]$. Observe that $I(z, \widehat{H})$ contains less than $2\widehat{H}$ integers, all upper bounded by $\widehat{B} \cdot \widehat{A} + \widehat{H}$, and we also know that $0 \notin I(z, \widehat{H})$ because $\widehat{B} \geq \widehat{H}$. Hence, using the fact that all primes in $\mathcal{P}_\ell$ exceed 2^ℓ, we find that each integer in $I(z, H)$ is divisible by at most $\ell^{-1}\log(\widehat{B} \cdot \widehat{A} + \widehat{H})$ primes from $\mathcal{P}_\ell$, and we have $\#S_z < 2\widehat{H}\ell^{-1}\log(\widehat{B} \cdot \widehat{A} + \widehat{H})$.

So for each possible choice of $z \in \mathbb{Z}_{\widehat{A}} \backslash \{0\}$, there are less than $(2\widehat{H}\ell^{-1}\log(\widehat{B} \cdot \widehat{A} + \widehat{H}))^n$ "bad" choices for $\mathbf{p} = (p_1, \ldots, p_n) \in \mathcal{P}_\ell^n$ such that (1) is satisfied. Since there are less than $\widehat{A}$ possible values for z, we get the desired bound on the number $\#\mathcal{E}_{\ell,n}(\widehat{A}, \widehat{H}, \widehat{B})$ of "bad" vectors $\mathbf{p}$. □

3 Definition of Changeable-Threshold Secret-Sharing Schemes

We will use the following definition of a threshold secret-sharing scheme, which is a slight modification of the definition in [19].

Definition 3.1 (Threshold Scheme). *A (t, n)-threshold secret-sharing scheme* $\mathsf{TSS} = (\mathsf{GC}, \mathsf{D}, \mathsf{C})$ *consists of three (possibly probabilistic) efficient algorithms:*

1 GC *(Public Parameter Generation): Takes as input a security parameter $k \in \mathcal{N}$ and returns a string $x \in \mathcal{X}$ of public parameters.*

2 D *(Dealer Setup): Takes as input a security/public parameter pair (k, x) and a secret s from the secret space $\mathcal{S}(k, x) \subseteq \{0, 1\}^k$ and returns a list of n shares $\mathbf{s} = (s_1, \ldots, s_n)$, where s_i is in the ith share space $\mathcal{S}_i(k, x)$ for $i = 1, \ldots, n$. We denote by*

$$\mathsf{D}_{k,x}(.,.) : \mathcal{S}(k, x) \times \mathcal{R}(k, x) \to \mathcal{S}_1(k, x) \times \cdots \times \mathcal{S}_n(k, x)$$

the mapping induced by algorithm D *(here $\mathcal{R}(k, x)$ denotes the space of random inputs to the probabilistic algorithm* D*).*

3 C *(Share Combiner): Takes as input a security/public parameter pair (k, x) and any subset $\mathbf{s}_I = (s_i : i \in I)$ of t out of the n shares, and returns a recovered secret $s \in \mathcal{S}(k, x)$. (here I denotes a subset of $[n]$ of size $\#I = t$).*

The correctness, communication efficiency, and security properties of a (t, n)-threshold secret-sharing scheme can be quantified by the following definitions, which are modifications of those in [19].

Definition 3.2 (Correctness, Efficiency, Security). *A (t, n) threshold secret-sharing scheme* $\mathsf{TSS} = (\mathsf{GC}, \mathsf{D}, \mathsf{C})$ *is said to be:*

1 δ_c-correct*: If the secret recovery failure probability p_f is at most δ_c, where*

$$p_f \overset{\text{def}}{=} \Pr_{x=\mathsf{GC}(k)\in\mathcal{X}}[\mathsf{C}_{k,x}(\mathbf{s}_I) \neq s \text{ for some } (s, r) \in \mathcal{S}(k, x) \times \mathcal{R}(k, x) \text{ and } I \subseteq [n] : \mathbf{s} = \mathsf{D}_{k,x}(s, r)],$$

and we define $\mathbf{s}_I \overset{\text{def}}{=} \{s_i : i \in I\}$ for each share vector $\mathbf{s} = (s_1, \ldots, s_n)$ and subset $I \subseteq [n]$.

We say that TSS *is asymptotically correct if, for any $\epsilon > 0$, there exists $k_0 \in \mathcal{N}$ such that* TSS *is ϵ-correct for all $k > k_0$.*

2 δ_e-efficient*: If the (maximal) ratio of share length to secret length is at most δ_e, that is*

$$\frac{\log(\#\mathcal{S}_i(k, x))}{\log(\#\mathcal{S}(k, x))} \leq \delta_e,$$

for all $i = 1, \ldots, n$.

3 $(t_s, \delta_s, \epsilon_s)$-secure *with respect to the secret probability distribution $P_{k,x}$ on $\mathcal{S}(k, x)$: If, with probability at least $1 - \delta_s$ over the choice of public parameters $x = \mathsf{GC}(k)$, the worst-case secret entropy loss for any t_s observed shares is at most ϵ_s, that is*

$$|L_{k,x}(\mathbf{s}_I)| \overset{\text{def}}{=} |H(s \in \mathcal{S}(k, x)) - H(s \in \mathcal{S}(k, x)|\mathbf{s}_I)| < \epsilon_s,$$

for all $\mathbf{s} \in \mathcal{S}_1(k, x) \times \cdots \times \mathcal{S}_n(k, x)$ and $I \subseteq [n]$ with $\#I \leq t_s$. We say that TSS *is asymptotically t_s-secure with respect to $P_{k,x}$ if, for any $\epsilon > 0$ and $\epsilon' > 0$ there exists $k_0 \in \mathcal{N}$ such that* TSS *is $(t_s, \epsilon', \epsilon \cdot k)$-secure with respect to $P_{k,x}$ for all $k > k_0$.*

The following definition of the *Threshold Changeability* without dealer assistance for a secret sharing scheme is a modification of the definition in [15].

Definition 3.3 (Threshold-Changeability). *A (t, n)-threshold secret-sharing scheme* $\mathsf{TSS} = (\mathsf{GC}, \mathsf{D}, \mathsf{C})$ *is called* threshold-changeable *to t' with δ_c-correctness, δ_e-efficiency and $(t_s, \delta_s, \epsilon_s)$-security with respect to secret distribution $P_{x,k}$, if there exist n efficient sub-share generation algorithms $\mathsf{H}_i : \mathcal{S}_i(k, x) \to \mathcal{T}_i(k, x)$ for $i = 1, \ldots, n$, and an efficient sub-share combination algorithm C' such that the modified (t', n)-threshold scheme* $\mathsf{TSS}' = (\mathsf{GC}, \mathsf{D}', \mathsf{C}')$*, with modified shares*

$$\mathsf{D}'_{k,x}(s, x) \overset{\text{def}}{=} (\mathsf{H}_1(s_1), \ldots, \mathsf{H}_n(s_n)) \in \mathcal{T}_1(k, x) \times \cdots \mathcal{T}_n(k, x), \;\; \textit{with } (s_1, \ldots, s_n) = \mathsf{D}_{k,x}(s, x),$$

is δ_c-correct, δ_e-efficient and $(t_s, \delta_s, \epsilon_s)$-secure with respect to $P_{k,x}$. TSS *is called* asymptotically threshold-changeable to (t_s, t') with respect to $P_{k,x}$ *if there exist algorithms $\mathsf{H}_i : \mathcal{S}_i(k, x) \to \mathcal{T}_i(k, x)$ $(i = 1, \ldots, n)$ and C' such that the (t', n)-threshold scheme TSS' defined above is asymptotically correct and asymptotically t_s-secure with respect to $P_{k,x}$.*

Remark on δ_c-correctness of a (t, n) scheme. The δ_c-correctness requirement, although probabilistic, is quite strong since it is only probabilistic in the choice of public parameter x: With at least $1 - \delta_c$ probability, the algorithm GC will output a 'good' scheme parameter x for which the scheme reconstruction works *perfectly*, i.e. for such x the secret is *guaranteed* to always be recovered by the combiner from *any* t shares.

Remarks on $(t_s, \epsilon_s, \delta_s)$-security. The $(t_s, \epsilon_s, \delta_s)$ requirement guarantees that with at least $1 - \delta_s$ probability, GC will output a 'good' scheme parameter x for which *any* t_s observed shares $\mathbf{s}_I$ leak at most $L_{k,x}(\mathbf{s}_I) < \epsilon_s$ bits of entropy of the secret s. Note that: (1) As for correctness above, in our scheme we can efficiently verify that an x is good, so ϵ_s need not be negligible, (2) The requirement that $L_{k,x}(\mathbf{s}_I) < \delta_s$ *for all* $\mathbf{s}_I$, is a worst-case requirement and hence much stronger than simply requiring that the *average value* of $L_{k,x}(\mathbf{s}_I)$ is less than δ_s , and (3) Assuming the entropy of the secret space is at least k bits, the asymptotic t_s-security requirement says that the *fraction* ϵ_s/k of the secret entropy lost can be made as small as we wish with a suitably large security parameter k.

4 Threshold-Changeability for Integer-CRT Secret-Sharing

4.1 The Standard Integer-CRT Scheme

The standard Integer-CRT (t, n)-threshold secret sharing scheme is defined as follows.

(t, n)-Threshold Secret Sharing Scheme $\mathsf{CRTTSS} = (\mathsf{GC}, \mathsf{D}, \mathsf{C})$

1 $\mathsf{GC}(k)$ (Public Parameter Generation): Pick a (not necessarily random) prime p_0 from the interval $[2^{k-1}, 2^k]$. Generate n distinct random primes $\mathbf{p} = (p_1, \ldots, p_n) \in D(\mathcal{P}_k^n)$, where $\mathcal{P}_k$ denotes the set of primes in the interval $[2^k, 2^{k+1}]$ (note that $p_i > p_0$ for all $i \in [n]$). The public parameter string is $x = (p_0, \mathbf{p})$. The secret space is $\mathcal{S}(k, x) = \mathbb{Z}_{p_0}$. The share spaces are $\mathcal{S}_i(k, x) = \mathbb{Z}_{p_i}$ for $i = 1, \ldots, n$. The dealer randomness space is $\mathcal{R}(k, x) = \mathbb{Z}_{P_{t-1}}$, where P_{t-1} is the product of the $t - 1$ *smallest* primes among $(p_1, \ldots, p_n)$.

2 $\mathsf{D}_{k,x}(s, r)$ (Dealer Setup): To share secret $s \in \mathbb{Z}_{p_0}$, choose a uniformly random $r \in \mathbb{Z}_{P_{t-1}}$ and compute the integer $a = s + r \cdot p_0$. The ith share is $s_i = a \bmod p_i$ for $i = 1, \ldots, n$.

3 $\mathsf{C}_{k,x}(\mathbf{s}_I)$ (Share Combiner): To combine shares $\mathbf{s}_I = (s_i : i \in I)$ for some $I \subseteq [n]$ with $\#I = t$, compute by Chinese Remaindering the unique $b \in \mathbb{Z}_{\prod_{i \in I} p_i}$ such that $b \equiv s_i \pmod{p_i}$ for all $i \in I$. The recovered secret is $s = b \bmod p_0$.

4.2 Threshold-Changing Algorithms

Our threshold-changing subshare generation and combination algorithms to change the (t, n)-threshold scheme $\mathsf{CRTTSS} = (\mathsf{GC}, \mathsf{D}, \mathsf{C})$ into a (t', n)-threshold scheme $\mathsf{CRTTSS}' = (\mathsf{GC}, \mathsf{D}', \mathsf{C}')$ are defined as follows. Note that the subshare combiner algorithm uses an efficient CVP approximation algorithm $\mathsf{A_{CVP}}$ with $\| \cdot \|_\infty$-approximation factor γ_{CVP}. We define $\Gamma_{CVP} = \log(\lceil \gamma_{CVP} + 1 \rceil)$ (if we use the Babai poly-time CVP algorithm, we have $\Gamma_{CVP} \leq 1 + 0.5(t' + 1 + \log(t' + 1))$).

Changing Threshold to $t' > t$

1. $\mathsf{H}_i(s_i)$ (ith Subshare Generation): To transform share $s_i \in \mathbb{Z}_p$ of original (t, n)-threshold scheme into subshare $t_i \in \mathbb{Z}_p$ of desired (t', n)-threshold scheme ($t' > t$) the ith shareholder does the following (for all $i = 1, \ldots, n$):
   (a) Determine noise bound H which guarantees δ_c-correctness:
      i. Set $H = \max(\lfloor 2^{\alpha \cdot k - 1} \rfloor, 1)$ with
      ii. $\alpha = 1 - \frac{1+\delta_F}{(t'/t)} > 0$ (noise bitlength fraction) and
      iii. $\delta_F = \left(\frac{t'/t}{k}\right) \left(\log(\delta_c^{-1/t'} n(kt + \Gamma_{CVP})) + 2\Gamma_{CVP} + 5\right)$.
   (b) Compute $\mathsf{H}_i(s_i) = t_i = B \cdot s_i + r_i \bmod p_i \in \mathbb{Z}_{p_i}$ for a uniformly random integer r_i with $|r_i| < H$, where $B = 2^{\Gamma_{CVP}} H \in \mathbb{Z}$.

2 $\mathsf{C}'_{k,x}(\mathbf{t}_I)$: To combine subshares $\mathbf{t}_I = (t_i : i \in I)$ for some $I = \{i[1], \ldots, i[t']\} \subseteq [n]$ with $\#I = t'$, do the following:
   (a) Build the following $(t' + 1) \times (t' + 1)$ matrix $M_{\mathcal{L}_{CRT}(\mathbf{p}_I, B, H, A)}$, whose rows form a basis for a full-rank lattice $\mathcal{L}_{CRT}(\mathbf{p}_I, B, H, A)$ in $\mathbb{Q}^{t'+1}$:

$$M_{\mathcal{L}_{CRT}(\mathbf{p}_I, B, H, A)} = \begin{pmatrix} p_{i[1]} & 0 & \ldots & 0 & 0 \\ 0 & p_{i[2]} & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & p_{i[t']} & 0 \\ B & B & \ldots & B & H/A \end{pmatrix}. \qquad (2)$$

   Here $H = \max(\lfloor 2^{\alpha \cdot k - 1} \rfloor, 1)$, $\alpha = 1 - \frac{1+\delta_F}{(t'/t)}$, $\delta_F = \left(\frac{t'/t}{k}\right) \left(\log(\delta_c^{-1/t'} n(kt + \Gamma_{CVP})) + 2\Gamma_{CVP} + 5\right)$, $B = 2^{\Gamma_{CVP}} H$, and $A = p_0 P_{t-1}$, where P_{t-1} is the product of the $t - 1$ *smallest* primes among $(p_1, \ldots, p_n)$.
   (b) Define $\overline{\mathbf{t}} = (t_{i[1]}, \ldots, t_{i[t']}, 0) \in \mathbb{Z}^{t'+1}$.
   (c) Run the CVP approximation algorithm $\mathsf{A_{CVP}}$ on the lattice $\mathcal{L}_{CRT}(\mathbf{p}_I, B, H, A)$ given by $M_{\mathcal{L}_{CRT}(\mathbf{p}_I, B, H, A)}$ and the target vector $\overline{\mathbf{t}}$. Denote by $\overline{\mathbf{c}} = (c_1, \ldots, c_{t'}, c_{t'+1}) \in \mathbb{Q}^{t'+1}$ the output vector returned by the algorithm, which approximates the closest vector to $\overline{\mathbf{t}}$ in the lattice $\mathcal{L}_{CRT}(\mathbf{p}_I, B, H, A)$.
   (d) Compute $\widehat{a} = (A/H) \cdot c_{t'+1} \in \mathbb{Z}$. The recovered secret is $\widehat{s} = \widehat{a} \bmod p_0$.

Remark 1. The reason for multiplying the shares s_i by the integer $B \geq (\gamma_{CVP} + 1)H$ before adding the noise, is that otherwise, the secret may not be uniquely recoverable from the noisy subshares.

Remark 2. It is not difficult to see that our method of adding a 'small' random noise integer r_i with $|r_i| < H$ to the share multiple Ba modulo each prime p_i, is essentially equivalent (in the sense of information on the secret) to passing the residues $Ba \bmod p_i$ through a deterministic function which chops off the $\log(2H) \approx \alpha \cdot k$ least-significant bits of the k-bit residues $Ba \bmod p_i$, and this also yields shorter subshares than in our method above, yielding $(1-\alpha)$-efficiency, instead of 1-efficiency as above. However, since reducing the length of the original shares is not our main goal, we have chosen to present our scheme as above since it simplifies the analysis of our scheme, and also allows for more fine control over the 'noise' bound.

4.3 Correctness

The following is a concrete statement of correctness for our scheme. It shows that the choice of the parameter δ_F in our scheme suffices to achieve δ_c-correctness for all sufficiently large security parameters k.

Theorem 4.1 (Correctness). *The scheme* CRTTSS' *(with parameter choice $\delta_c = k^{-t'}$) is asymptotically correct. Concretely, the (t', n) scheme* CRTTSS' *is δ_c-correct as long as the security parameter k satisfies the inequality*

$$k \geq \left(\frac{t'/t}{t'/t - 1}\right)\left(\log(\delta_c^{-1/t'} n(kt + \Gamma_{CVP})) + 2\Gamma_{CVP} + 6\right).$$

Proof. Let $x = (p_0, \mathbf{p})$ be a vector of primes which determines an instance of CRTTSS. For a subset $I = \{i[1], \ldots, i[t']\} \subseteq [n]$ of size $\#I = t'$, we say that $\mathbf{p}$ is *bad with respect to I* if there exists a secret $s \in \mathcal{S}_{k,x} = \mathbb{Z}_{p_0}$ and randomness $r \in Z_{P_{t-1}}$ and $\mathbf{r} \overset{\text{def}}{=} (r_{i[1]}, \ldots, r_{i[t']}) \in (-H, H)^{t'}$ for $\mathsf{D}'_{k,x}$ such that $\mathsf{C}'_{k,x}$ fails to recover the secret s from the given subshare vector $\mathbf{t}_I = \mathsf{D}'_{k,x}(s, (r, \mathbf{r})) = (B \cdot a + r_{i[1]} \bmod p_{i[1]}, \ldots, B \cdot a + r_{i[t']} \bmod p_{i[t']})$, where $a = s + r \cdot p_0 \in \mathbb{Z}_A$, $A = p_0 P_{t-1}$ and P_{t-1} is the product of the $t-1$ smallest primes in $\mathbf{p}$. We say that $\mathbf{p}$ is *bad* if there exists $I \subseteq [n]$ of size $\#I = t'$ such that $\mathbf{p}$ is bad with respect to I.

Observe that the failure probability p_f in the correctness Definition 3.2 is exactly the probability that a prime vector $\mathbf{p} = (p_1, \ldots, p_n)$ chosen uniformly at random from the set $D(\mathcal{P}_k^n)$ is bad. We now deduce an upper bound on the fraction δ of bad vectors in $D(\mathcal{P}_k^n)$ as a function of the scheme parameters. Suppose that $\mathbf{p}$ is bad with respect to some $I \in [n]$ with $\#I = t'$. This means that there exist $a \in \mathbb{Z}_A$ and $\mathbf{r} = (r_{i[1]}, \ldots, r_{i[t']}) \in (-H, H)^{t'}$ such that C' returns the wrong secret $\widehat{s} = \widehat{a} \bmod p_0 \neq a \bmod p_0 \overset{\text{def}}{=} s$ on input

$$\mathbf{t}_I = (t_1, \ldots, t_{t'}) = (B \cdot a + r_{i[1]} - k_1 p_{i[1]}, \ldots, B \cdot a + r_{i[t']} - k_{t'} p_{i[t']}), \tag{3}$$

for some vector $\mathbf{k} = (k_1, \ldots, k_{t'}) \in \mathbb{Z}^{t'}$. But this means that

$$\widehat{a} = (A/H)c_{t'+1} \not\equiv (A/H)a \pmod{p_0}, \tag{4}$$

where

$$\mathbf{c} = (c_1, \ldots, c_{t'+1}) = (B \cdot \widehat{a} - \widehat{k}_{i[1]} p_{i[1]}, \ldots, B \cdot \widehat{a} - \widehat{k}_{i[t']} p_{i[t']}, \frac{\widehat{a}}{A} H) \tag{5}$$

is the vector returned by $\mathsf{A_{CVP}}$ on input the lattice $\mathcal{L}_{CRT}(\mathbf{p}_I, B, H, A)$ with target vector $\overline{\mathbf{t}}_I = (t_1, \ldots, t_{t'}, 0)$, and

$$\mathbf{a_k} = (a_1, \ldots, a_{t'+1}) \overset{\text{def}}{=} (B \cdot a - k_1 p_{i[1]}, \ldots, B \cdot a - k_{t'} p_{i[t']}, \frac{a}{A} H),$$

is the lattice vector in $\mathcal{L}_{CRT}$ corresponding to $a = s + r \cdot p_0$, which satisfies

$$\|\mathbf{a_k} - \overline{\mathbf{t}}_I\|_\infty = \|(r_{i[1]}, \ldots, r_{i[t']}, \frac{a}{A} H)\|_\infty < H, \tag{6}$$

using $a < A$ and $|r_{i[j]}| < H$ for all $j = 1, \ldots, t'$. Since $\mathsf{A}_{\mathsf{CVP}}$ is a CVP approximation algorithm with $\|.\|_\infty$-approximation factor γ_{CVP}, the lattice vector $\mathbf{c}$ which it returns satisfies

$$\|\mathbf{c} - \overline{\mathbf{t}}_I\|_\infty < \gamma_{CVP} \cdot H. \tag{7}$$

Applying the triangle inequality, it follows from (6) and (7) that the lattice vector $\boldsymbol{z} = \boldsymbol{c} - \mathbf{a_k} = (z_1, \ldots, z_{t'+1})$ is 'short', namely $\|\boldsymbol{z}\|_\infty < (\gamma_{CVP} + 1)H$, but is non-zero, namely $z_{t'+1} \neq 0$ (using (4)). We conclude that if $\mathbf{p}$ is bad with respect to I then there exists an integer $z \stackrel{\text{def}}{=} |\frac{A}{H} z_{t'+1}|$ which satisfies both

$$0 < |z| < (\gamma_{CVP} + 1)A \leq 2^{\Gamma_{CVP} + (k+1)\cdot t} \stackrel{\text{def}}{=} \widehat{A}$$

and

$$\|B \cdot z\|_{L, \mathbf{p}_I} < 2^{\Gamma_{CVP}} H \stackrel{\text{def}}{=} \widehat{H},$$

where $\mathbf{p}_I \stackrel{\text{def}}{=} (p_{i[1]}, \ldots, p_{i[t']})$ and $B = 2^{\Gamma_{CVP}} H = \widehat{H}$.

It now follows from Lemma 2.1 that there is a fraction of at most $\#\mathcal{E}_{k,t'}(\widehat{A}, \widehat{H}, B)/\#D(\mathcal{P}_k^{t'}) \leq \widehat{A}(2\widehat{H}\log(B\widehat{A} + \widehat{H})k^{-1})^{t'}/\#D(\mathcal{P}_k^{t'})$ choices for $\mathbf{p}_I \in \mathcal{P}_k^{t'}$ such that $\mathbf{p}$ is bad with respect to I. Since there are $\binom{n}{t'}$ possible choices for I, we have that the fraction δ of bad vectors in $D(\mathcal{P}_k^n)$ is upper bounded as

$$\delta \leq \frac{\binom{n}{t'}\widehat{A}\left(2\widehat{H}\log(B\widehat{A} + \widehat{H})k^{-1}\right)^{t'}}{\#D(\mathcal{P}_k^{t'})}. \tag{8}$$

It is known[20] that the number of primes $\#\mathcal{P}_k$ in the interval $[2^k, 2^{k+1}]$ is lower bounded as

$$\#\mathcal{P}_k \geq 2^{k-1}/k \text{ for all } k \geq 5. \tag{9}$$

Also, we have

$$\frac{\#\mathcal{P}_k^{t'}}{\#D(\mathcal{P}_k^{t'})} = \left(\frac{\#\mathcal{P}_k}{\#\mathcal{P}_k}\right) \cdot \left(\frac{\#\mathcal{P}_k}{\#\mathcal{P}_k - 1}\right) \cdots \left(\frac{\#\mathcal{P}_k}{\#\mathcal{P}_k - (t'-1)}\right) \leq 2^{t'}, \tag{10}$$

as long as the condition $\#\mathcal{P}_k - (t'-1) \geq \#\mathcal{P}_k/2$ holds, which using (9) is implied by the condition

$$k - \log k \geq \log t' + 2. \tag{11}$$

Plugging (9) and (10) in (8) we find, assuming (11), the following sufficient condition for having $\delta \leq \delta_c$ (i.e. δ_c-correctness):

$$\frac{2^{t'}\binom{n}{t'}\widehat{A}(2\widehat{H}\log(\widehat{B}\widehat{A} + \widehat{H})k^{-1}]^{t'}}{(2^{k-1}k^{-1})^{t'}} \leq \delta_c. \tag{12}$$

Now, using $\widehat{B}\widehat{A} + \widehat{H} = (\widehat{A} + 1)\widehat{H} \leq 2\widehat{A}\widehat{H}$ (since $\widehat{A} \geq 1$) and assuming the condition

$$2^{\alpha \cdot k - 1} \geq 1, \tag{13}$$

so that $H = 2^{\alpha \cdot k - 1}$, the condition (12) becomes $2^{2t' + t + (t'+1)\Gamma_{CVP}}\binom{n}{t'}((t + \alpha)k + 2\Gamma_{CVP} + t)^{t'} \leq 2^{((1-\alpha)t' - t)\cdot k}\delta_c$. Using $\alpha < 1$, $\frac{1}{t'}\log(\binom{n}{t'}\delta_c^{-1}) \leq \log(\delta_c^{-1}n)$, $(2t' + t + (t'+1)\Gamma_{CVP})/t' \leq 2\Gamma_{CVP} + 3$ (since $t/t' \leq 1$ and $t' \geq 1$), and $\log((t+1)(k+1) + 2\Gamma_{CVP}) \leq \log(4kt + 2\Gamma_{CVP}) \leq 2 + \log(kt + \Gamma_{CVP})$ (using $t \geq 1$ and $k \geq 1$), we finally get the following sufficient condition for δ_c-correctness (assuming $k \geq 5$, (11) and (13)):

$$\delta_F \geq \left(\frac{t'/t}{k}\right)\left(\log(\delta_c^{-1/t'} n(kt + \Gamma_{CVP})) + 2\Gamma_{CVP} + 5\right). \tag{14}$$

The condition (14) is satisfied by the scheme parameter choice $\delta_F = (\frac{t'/t}{k})(\log(\delta_c^{-1/t'} n(kt + \Gamma_{CVP})) +$

$2\Gamma_{CVP}+5)$. Substituting this value of δ_F in (13) (recalling that $\alpha = 1 - \frac{1+\delta_F}{t'/t}$), we see that (13) is equivalent to the claimed inequality

$$k \geq \left(\frac{t'/t}{t'/t-1}\right)\left(\log(\delta_c^{-1/t'} n(kt + \Gamma_{CVP})) + 2\Gamma_{CVP} + 6\right). \tag{15}$$

Finally we observe, using $t'/t > 1$ that (15) implies that $k - \log k \geq \log n + (\frac{t'/t}{t'/t-1})(\log(\delta_c^{-1/t'} t) + 6) \geq \log t' + 2$ so that $k \geq 5$ and (11) are both implied by (15). Finally, to establish the claimed asymptotic correctness, we observe that with $\delta_c = k^{-t'} = o(1)$, the right-hand side of (15) is $O(\log k)$ so, since $\log k = o(k)$, (15) is satisfied for all sufficiently large k. This completes the proof. □

4.4 Security

The concrete security of our scheme is given by the following result. It shows that, for fixed (t', n), and with $\delta_c = \delta_s = k^{-t'} = o(1)$, our (t', n) scheme leaks at most fraction $o(1)$ of the entropy of the secret as long as less than $t' - t'/t$ subshares are observed by the attacker. For example if we increase the threshold from t to $t' = 2t$, then we have almost perfect security as long as $t_s < t' - t'/t = t' - 2$ shares are observed by the attacker (we can of course choose a slightly larger $t' \approx 2t + 2$ if we want to guarantee security against attackers observing up to $2t$ shares, but then to guarantee reconstruction we would need $2t + 2$ subshares to be combined).

We remark that the limitation $t_s \leq t' - t'/t$ for security is inherent to our approach of adding noise to the subshares and not to our CRT-based implementation. This is because, as noted in Section 4, our approach of increasing the threshold from t to $t' = R' \cdot t$ by adding about $(1 - 1/R')k$ bits of noise to shares is essentially equivalent to reducing the length of shares by a factor R'. Thus each subshare can provide at most k/R' bits of information on the secret and since t' subshares contain all the information on the secret, it follows that perfect security cannot be achieved when $t_s > t' - R'$ subshares are observed.

We also remark that although we state in Theorem 4.2 a lower bound on the conditional *Shannon* entropy of the secret $H(s \in \mathcal{S}(k,x)|\boldsymbol{s}_I)$ for any observed share value $\boldsymbol{s}_I$, our proof shows the stronger result that the stated bound is also a lower bound on the conditional *min-entropy* $H_\infty(s \in \mathcal{S}(k,x)|\boldsymbol{s}_I) = \log(1/\max_{s\in\mathcal{S}(k,x)} P_{k,x}(s|\boldsymbol{s}_I))$ (where $P_{k,x}(s|\boldsymbol{s}_I)$ denotes the conditional probability distribution of s given $\boldsymbol{s}_I$), and hence also a lower bound on the conditional *Rényi* entropy of s given $\boldsymbol{s}_I$. This means we can apply the privacy amplification results of [3] to derive a secret s' (by hashing s with a public randomly chosen function from a universal hash family) such that a provably negligible absolute amount of entropy of s' is leaked by the observed shares $\boldsymbol{s}_I$.

Note that for improved readability of the proof of Theorem 4.2, the proofs of some lemmas have been placed in the Appendix.

Theorem 4.2 (Security). *The scheme* CRTTSS′ *(with $\delta_c = k^{-t'}$) is asymptotically $Int(t' - t'/t)$-secure with respect to the uniform secret distribution $s \in \mathbb{Z}_{p_0}$. Concretely, scheme* CRTTSS′ *is $(t_s, \delta_s, \epsilon_s)$-secure, with:*

$$t_s = \frac{t' - t'/t}{1 + \delta_F} = \frac{t' - t'/t}{1 + \left(\frac{t'/t}{k}\right)\theta},$$

$$\delta_s = \delta_c,\ \epsilon_s = \max((\beta + 4)(t_s + 1), t + 1),$$

assuming that the security parameter k satisfies the inequality

$$k \geq \max\left(\frac{t'/t}{t'/t-1}\left(\theta + \beta(t_s + 1) + t + 1\right), (\beta + 3)(t_s + 1)^2 + 1\right). \tag{16}$$

Here

$$\theta = \log(\delta_c^{-1/t'} n(kt + \Gamma_{CVP})) + 2\Gamma_{CVP} + 5$$

and

$$\beta = \frac{\log(2\delta_c^{-1}\binom{n}{t_s})}{t_s + 1} + \log(4kt + \Gamma_{CVP} + 1) + 5.$$

Proof. Let $x = (p_0, \mathbf{p})$ denote the scheme public parameters, where $\mathbf{p} = (p_1, \dots, p_n)$. Fix $I = \{i[1], \dots, i[t_s]\} \subseteq [n]$ with $\#I = t_s$, and let $\mathbf{s}_I = (s_{i[1]}, \dots, s_{i[t_s]}) \in \mathbb{Z}_{p_{i[1]}} \times \cdots \mathbb{Z}_{p_{i[t_s]}}$ be an observed subshare vector. The subshares are given by:

$$s_{i[j]} = B \cdot a + r_{i[j]} \bmod p_{i[j]} \text{ for } j = 1, \dots, t_s,$$

where $a = s + r \cdot p_0$ is uniformly distributed on $\mathbb{Z}_A$.

It follows from the above that the conditional probability $P_{k,x}(s|\mathbf{s}_I)$ of the secret taking the value $s \in \mathbb{Z}_{p_0}$ given the observed sub-share vector $\mathbf{s}_I$ is given by:

$$P_{k,x}(s|\mathbf{s}_I) = \frac{\#\{(a, \mathbf{r}_I) \in \mathbb{Z}_A \times (-H, H)^{t_s} : B \cdot a + r_{i[j]} \equiv s_{i[j]} \pmod{p_{i[j]}} \forall j \in [t_s] \text{ and } a \equiv s \pmod{p_0}\}}{\#\{(a, \mathbf{r}_I) \in \mathbb{Z}_A \times (-H, H)^{t_s} : B \cdot a + r_{i[j]} \equiv s_{i[j]} \pmod{p_{i[j]}} \forall j \in [t_s]\}}.$$

Using the fact that for each $a \in \mathbb{Z}_A$ there is at most one $\mathbf{r}_I \in (-H, H)^{t_s}$ such that $B \cdot a + r_{i[j]} \equiv s_{i[j]}$ (mod $p_{i[j]}$) for all $j \in [t_s]$, the above simplifies to:

$$P_{k,x}(s|\mathbf{s}_I) = \frac{\#S_{s,p_0}(\mathbf{p}_I, A, B, H)}{\#S_{0,1}(\mathbf{p}_I, A, B, H)}, \tag{17}$$

where for integers $(\widehat{s}, \widehat{p}_0)$ we define the set $S_{\widehat{s},\widehat{p}_0}$ by

$$S_{\widehat{s},\widehat{p}_0}(\mathbf{p}_I, A, B, H, \mathbf{s}_I) \stackrel{\text{def}}{=} \{a \in \mathbb{Z}_A : \|B \cdot a - s_{i[j]}\|_{L,p_{i[j]}} < H \forall j \in [t_s] \text{ and } a \equiv \widehat{s} \pmod{\widehat{p}_0}\}.$$

We will derive a probabilistic lower bound on $\#S_{0,1}$ and upper bound on $\#S_{s,p_0}$ which both hold for all except a fraction $\delta_I \leq \delta_s/\binom{n}{t_s}$ of 'bad' choices for $\boldsymbol{p}_I \in D((\mathcal{P}_k)^{t_s})$ assuming k satisfies the inequality (16) (with t_s and δ_s defined in the theorem statement). We then apply these bounds to (17) to get a bound $P_{k,x}(s|\boldsymbol{s}_I) \leq 2^{\epsilon_s}/p_0$ for all s (with ϵ_s defined in the theorem statement) so that for fixed I, entropy loss is bounded as $L_{k,x}(\boldsymbol{s}_I) \leq \epsilon_s$, except for fraction δ_I of $\boldsymbol{p}_I \in D((\mathcal{P}_k)^{t_s})$. It then follows that $L_{k,x}(\boldsymbol{s}_I) \leq \epsilon_s$ for *all* $I \subseteq [n]$ with $\#I = t_s$ except for a fraction $\delta \leq \binom{n}{t_s}\delta_I \leq \delta_s$ of $\boldsymbol{p} \in D((\mathcal{P}_k)^n)$ assuming that k satisfies (16), which proves the theorem.

Reduction to Lattice Point Counting. It remains to derive lower and upper bounds on the size of the set $S_{\widehat{s},\widehat{p}_0}$. The following lemma reduces this problem to finding lower and upper bounds on the number of points $\#V_{\widehat{s},\widehat{p}_0}$ of a certain lattice in a certain box.

Lemma 4.1. *Let A, B, H be positive integers, $\mathbf{p}_I = (p_{i[1]}, \dots, p_{i[t_s]})$ a vector of primes greater or equal to $2H$, $\mathbf{s}_I = (s_{i[1]}, \dots, s_{i[t_s]}) \in \mathbb{Z}^{t_s}$, $\widehat{p}_0 \in \mathbb{Z}$ a positive divisor of A, and $\widehat{s} \in \mathbb{Z}_{\widehat{p}_0}$. Let $\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0)$ denote the full-rank lattice in $\mathbb{Q}^{t_s+1}$ with basis consisting of the rows of the matrix*

$$M_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0) \stackrel{\text{def}}{=} \begin{pmatrix} p_{i[1]} & 0 & \dots & 0 & 0 \\ 0 & p_{i[2]} & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & p_{i[t_s]} & 0 \\ B \cdot \widehat{p}_0 & B \cdot \widehat{p}_0 & \dots & B \cdot \widehat{p}_0 & \frac{2H}{A/\widehat{p}_0} \end{pmatrix},$$

and define the vector

$$\widehat{\mathbf{s}}_I \overset{\text{def}}{=} \left(s_{i[1]} - B \cdot \widehat{s}, \ldots, s_{i[t_s]} - B \cdot \widehat{s}, H \cdot \frac{A/\widehat{p}_0 - 1}{A/\widehat{p}_0} \right) \in \mathbb{Q}^{t_s+1}.$$

Then the sizes of the following two sets are equal:

$$S_{\widehat{s},\widehat{p}_0}(\mathbf{p}_I, A, B, H, \mathbf{s}_I) \overset{\text{def}}{=} \{a \in \mathbb{Z}_A : \|B \cdot a - s_{i[j]}\|_{L,p_{i[j]}} < H \forall j \in [t_s] \text{ and } a \equiv \widehat{s} \pmod{\widehat{p}_0}\},$$

and

$$V_{\widehat{s},\widehat{p}_0}(\mathbf{p}_I, A, B, H, \widehat{\mathbf{s}}_I) \overset{\text{def}}{=} \{\mathbf{v} \in \mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0) : \|\mathbf{v} - \widehat{\mathbf{s}}_I\|_\infty < H\}.$$

Finding a Lower Bound on $\#V_{0,1}$. We reduce the "non-homogenous" problem of lower bounding the number $\#V_{\widehat{s},\widehat{p}_0}(\mathbf{p}_I, A, B, H, \widehat{\mathbf{s}}_I)$ of points of the lattice $\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0)$ in the box $T_{\mathbf{s}_I}(H) \overset{\text{def}}{=} \{\mathbf{v} \in \mathbb{Q}^{t_s+1} : \|\mathbf{v} - \widehat{\mathbf{s}}_I\|_\infty < H\}$ centered on $\widehat{\mathbf{s}}_I$ (which is in general not a lattice vector), to

1 The "homogenous" problem of lower bounding the number of points of the lattice $\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0))$ in an origin-centered box of the form $T_{\mathbf{0}}(H') \overset{\text{def}}{=} \{\mathbf{v} \in \mathbb{Q}^{t_s+1} : \|\mathbf{v}\|_\infty < H'\}$, and

2 Finding an upper bound on the (t_s+1)th Minkowski minimum $\lambda_{t_s+1}(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0))$ of the latticeWe will see that this upper bound holds for at least a fraction $1 - \epsilon_\beta$ of $\mathbf{p}_I \in \mathcal{P}_\ell^{t_s}$ whenever a certain explicit condition holds.

This reduction can be precisely stated as follows.

Lemma 4.2. *With the notation of Lemma 4.1,*

$$\#V_{\widehat{s},\widehat{p}_0}(\mathbf{p}_I, A, B, H, \widehat{\mathbf{s}}_I) \geq \#\{\mathbf{v} \in \mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0)) : \|\mathbf{v}\|_\infty < H - \epsilon\},$$

where

$$\epsilon \leq \left(\frac{t_s+1}{2}\right) \lambda_{t_s+1}(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0)).$$

To solve the "homogenous" problem (1) above we apply the Blichfeldt-Corput generalization of Minkowski's "first theorem" in the geometry of numbers (Theorem 2.2 in Sec. 2). Noting that $\det(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0)) = P_I \cdot \frac{2H}{A/\widehat{p}_0}$, where $P_I = \prod_{j \in [t_s]} p_{i[j]}$, and the volume of the box $\{\mathbf{v} \in \mathbb{R}^{t_s+1} : \|\mathbf{v}\|_\infty < H - \epsilon\}$ is $[2(H-\epsilon)]^{t_s+1}$, we find, using the fact that $Int(z) \geq z - 1$ for all $z \in \mathbb{R}$ that,

$$\#\{\mathbf{v} \in \mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0) : \|\mathbf{v}\| < H - \epsilon\} \geq \frac{(A/\widehat{p}_0)(H-\epsilon)^{t_s+1}/H}{P_I} - 1. \tag{18}$$

To solve the second problem (2) above of upper bounding the (t_s+1)th Minkowski minimum $\lambda_{t_s+1}(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0))$, we apply Minkowski's "second theorem" in the geometry of numbers (Theorem 2.3 in Sec. 2) to reduce this problem to the problem of *lower bounding* the first Minkowski minimum $\lambda_1(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0))$. Namely, since $\lambda_i(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0)) \geq \lambda_1(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0))$ for all $i \in [t_s]$, then Minkowski's theorem gives

$$\lambda_{t_s+1}(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0)) \leq \frac{2^{t_s+1} \det(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0))}{\lambda_1(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0))^{t_s}}. \tag{19}$$

Lower Bounding the first Minkowski Minimum. By applying the number-theoretic Lemma 2.1(Sec. 2), we obtain the following (probabilistic) lower bound on $\lambda_1(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0))$.

Lemma 4.3. *Fix positive integers $(k, A, B, H, \widehat{p}_0, t_s)$, and real $\beta > 0$ such that $k \geq 5$, $k - \log k \geq \log t_s + 2$, $\widehat{p}_0$ is a divisor of A, and $A/\widehat{p}_0 \geq 2^k \geq 2H$. If the condition*

$$1 \leq 2^{-\beta} \left(\frac{2^{k \cdot t_s} 2H}{A/\widehat{p}_0} \right)^{\frac{1}{t_s+1}} \leq \frac{1}{4} \min(B, 2^k) \tag{20}$$

holds, then for at least a fraction $1 - 2^{-[\beta - (\log\log(2^{k+2}\frac{B}{H}A)+5)](t_s+1)}$ of $\mathbf{p}_I \in D(\mathcal{P}_k^{t_s})$, we have

$$\lambda_1 \left(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0) \right) \geq 2^{-\beta} \cdot \det(\mathcal{L}_{CRT}\left(\mathbf{p}_I, A, B, H, \widehat{p}_0\right))^{\frac{1}{t_s+1}}.$$

Note that $A = p_0 P_{t-1}$ depends on $\mathbf{p}_I$ whereas our Lemma 4.3 assumes that A is a fixed integer. However, it is easy to see that if $A_L = p_0 2^{(t-1)k}$ denotes a fixed lower bound on A then $\# S_{s,p_0}(\mathbf{p}_I, A, B, H, \mathbf{s}_I) \leq S_{s,p_0}(\mathbf{p}_I, A_H, B, H, \mathbf{s}_I)$. So, fixing $\beta > 0$ (to be determined later) and applying Lemma 4.3 with $A = A_L$ and $(\widehat{s}, \widehat{p}_0) = (0, 1)$, we have, except for a fraction of at most

$$\delta_I(1) \leq 2^{-[\beta - (\log\log(2^{k+2}\frac{B}{H}A_L)+5)](t_s+1)} \tag{21}$$

of $\mathbf{p}_I \in D(\mathcal{P}_k^{t_s})$ and assuming conditions

$$1 \leq 2^{-\beta} \left(\frac{2^{kt_s} 2H}{A_L} \right)^{\frac{1}{t_s+1}} \leq \frac{1}{4} \min(B, 2^k) \tag{22}$$

and

$$k \geq 5 \text{ and } k - \log k \geq \log t_s + 2 \tag{23}$$

and

$$A \geq 2^k \geq 2H, \tag{24}$$

that $\lambda_1 \left(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, 1) \right) \geq 2^{-\beta} \cdot \det(\mathcal{L}_{CRT}\left(\mathbf{p}_I, A, B, H, 1\right))^{\frac{1}{t_s+1}}$. The latter bound and Minkowski's second theorem give $\lambda_{t_s+1} \left(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, 1) \right) \leq 2^{(\beta+1)t_s+1} \cdot \det(\mathcal{L}_{CRT}\left(\mathbf{p}_I, A, B, H, 1\right))^{\frac{1}{t_s+1}}$, and so using Lemma 4.2 we have $\# \mathbf{v}_{0,1}(\mathbf{p}_I) \geq \# \{ \mathbf{v} \in \mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, 1) : \|\mathbf{v}\|_\infty < H/2 \}$ as long as

$$\frac{t_s+1}{2} 2^{(\beta+1)t_s+1} \cdot \det(\mathcal{L}_{CRT}\left(\mathbf{p}_I, A, B, H, 1\right))^{\frac{1}{t_s+1}} \leq \frac{H}{2}. \tag{25}$$

Applying the Blichfeldt-Corput theorem to the box $\{ \mathbf{v} \in \mathbb{Q}^{t_s+1} : \|\mathbf{v}\|_\infty < H/2 \}$, we get $\# \mathbf{v}_{0,1}(\mathbf{p}_I) \geq 2Int \left(\frac{(H/2)^{t_s+1}}{2^{t_s+1} \det(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, 1))} \right) + 1$ and using $2Int(z) + 1 \geq 2z - 1 \geq z$ for all $z \geq 2$, we conclude that

$$\# \mathbf{v}_{0,1}(\mathbf{p}_I) \geq \frac{H^{t_s+1}}{2^{2(t_s+1)} \det(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, 1))}, \tag{26}$$

except for a fraction $\delta_I(1)$ of $\mathbf{p}_I \in D(\mathcal{P}_k^{t_s})$ bounded in (21), and assuming that conditions (22), (23), (24) and (25) hold. Note that condition (24) is satisfied because $A = p_0 P_{t-1} \geq P_{t-1} \geq 2^k$ assuming $t \geq 2$ (we may assume this because for $t = 1$, $t_s = 0$ so the theorem is trivially true), and $2H < 2^{\alpha k} \leq 2^k$ since $\alpha \leq 1$. Also note that using $\beta > 0$ and assuming $t_s \geq t$ (as we will explain below, our our analysis need only apply for $t \geq t_s$), we see that the right-hand inequality in (22) is implied by (25).

Finding an Upper Bound on $\# V_{s,p_0}(\mathbf{p}_I)$. We reduce the problem of upper bounding $\# V_{s,p_0}(\mathbf{p}_I, A, B, H, \widehat{\mathbf{s}}_I)$ to the problem of lower bounding the first Minkowski minimum $\lambda_1(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, p_0))$, and then apply Lemma 4.3. The reduction can be stated as follows.

Lemma 4.4. *For any lattice $\mathcal{L}$ in $\mathbb{R}^n$, vector $\mathbf{s} \in \mathbb{R}^n$, and $H > 0$, we have*

$$\#\{\mathbf{v} \in \mathcal{L} : \|\mathbf{v} - \mathbf{s}\|_\infty < H\} \leq \left[\frac{2H}{\lambda_1(\mathcal{L})} + 1\right]^n.$$

Applying Lemma 4.4, we get $\#V_{\widehat{s},\widehat{p_0}}(\mathbf{p}_I, A, B, H, \widehat{\mathbf{s}}_I) \leq \left[\frac{4H}{\lambda_1((\mathcal{L}_{CRT}(\mathbf{p}_I, B\cdot\widehat{p_0}, 2H, \frac{A}{\widehat{p_0}})))}\right]^{t_s+1}$ as long as the condition

$$\lambda_1(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, p_0)) \leq 2H \tag{27}$$

holds. To apply the lower bound of Lemma 4.3, we let $A_H = p_0 2^{(t-1)(k+1)}$ be a fixed upper bound on A. Then applying the lemma with $A = A_H$ and $(uhs, \widehat{p_0}) = (s, p_0)$ we have, except for at most a fraction

$$\delta_I(p_0) \leq 2^{-[\beta - (\log\log(2^{k+2}\frac{B}{H}A_H)+5)](t_s+1)} \tag{28}$$

of $\mathbf{p}_I \in D(\mathcal{P}_k^{t_s})$, assuming conditions (23) and (24) and

$$1 \leq 2^{-\beta}\left(\frac{2^{kt_s}2H}{A_H/p_0}\right)^{\frac{1}{t_s+1}} \leq \frac{1}{4}\min(B, 2^k) \tag{29}$$

that $\lambda_1\left(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, p_0)\right) \geq 2^{-\beta} \cdot \det(\mathcal{L}_{CRT}\left(\mathbf{p}_I, A, B, H, p_0)\right)^{\frac{1}{t_s+1}}$. Plugging this into the above upper bound on $\#V_{\widehat{s},\widehat{p_0}}$, we obtain

$$\#V_{\widehat{s},\widehat{p_0}}(\mathbf{p}_I, A, B, H, \widehat{\mathbf{s}}_I) \leq 2^{(\beta-2)(t_s+1)}\frac{H^{t_s+1}}{\det(\mathcal{L}_{CRT}\left(\mathbf{p}_I, A, B, H, p_0)\right)} \tag{30}$$

except for at most a fraction $\delta_I(p_0)$ of $\mathbf{p}_I \in D(\mathcal{P}_k^{t_s})$ bounded in (28) and assuming conditions (27) and (29). Notice that the left-hand inequality of (29) and (27) are both implied by the condition

$$2^{2-\beta}\det(\mathcal{L}_{CRT}\left(\mathbf{p}_I, A, B, H, p_0)\right)^{\frac{1}{t_s+1}} \leq H. \tag{31}$$

Putting it Together. Plugging our bounds on $\#V_{0,1} = \#S_{0,1}$ and $\#V_{s,p_0} = \#S_{s,p_0}$ from (26) and (30) into (17) we obtain

$$P_{k,x}(s|\mathbf{s}_I) \leq 2^{\epsilon_s}/p_0 \text{ with } \epsilon_s = \max((\beta+4)(t_s+1), t+1), \tag{32}$$

as claimed (with β to be determined), for all except at most a fraction δ_I of $\mathbf{p}_I \in D(\mathcal{P}_k^{t_s})$, where, using (21) and (28),

$$\delta_I \leq \delta_I(1) + \delta_I(p_0) \leq 2^{1-[\beta-(\log\log(2^{k+2}\frac{B}{H}A_H)+5)](t_s+1)}, \tag{33}$$

and assuming the conditions (23), (25), the left-hand inequality in (22), the left-hand inequality in (29) and (31). Now recall that to achieve the claimed $\delta_s \leq \delta_c$ we need to show that $\delta_I \leq \delta_c\binom{n}{t_s}^{-1}$. Using the upper bound (33), and recalling that $B/H = 2^{\Gamma_{CVP}}$ and $A_H = p_0 2^{(t-1)(k+1)} \leq 2^{t(k+1)}$ so $\log(2^{k+2}\frac{B}{H}A_H) \leq 4kt + \Gamma_{CVP} + 1$, we see that the desired bound $\delta_I \leq \delta_c\binom{n}{t_s}^{-1}$ is satisfied by choosing

$$\beta = \frac{\log(2\delta_c^{-1}\binom{n}{t_s})}{t_s+1} + \log(4kt + \Gamma_{CVP} + 1) + 5, \tag{34}$$

as in the theorem statement.

We now show that the inequality (16) satisfied by k implies the assumed conditions (23), the left-hand inequality in (22), and the left-hand inequality in (29). To see this, note that both the left-hand inequality in (22), and the left-hand inequality in (29) are satisfied if

$$1 \le 2^{-\beta}\left(\frac{2^{kt_s}2H}{p_0 2^{(t-1)(k+1)}}\right). \tag{35}$$

But assuming

$$2^{\alpha\cdot k-1} \ge 2 \tag{36}$$

we have $2H \ge 2^{\alpha k-1}$ and using $\alpha = 1 - \frac{1+\delta_F}{t'/t}$, $t_s \ge t$, and the definition of $\delta_F = \left(\frac{t'/t}{k}\right)\theta(k)$ with $\theta(k) = \left(\log(\delta_c^{-1/t'} n(kt+\Gamma_{CVP})) + 2\Gamma_{CVP} + 5\right)$ we see after straightforward algebraic manipulation that (35) and also (36) and (23) are all satisfied as long as k satisfies the inequality

$$k \ge \frac{t'/t}{t'/t-1}(\theta(k)+t+1+\beta(t_s+1)), \tag{37}$$

which is implied by (16).

Now we show that the choice of $t_s = \frac{t'-t'/t}{1+\delta_F}$ implies that conditions (25) and (31) are satisfied. First, using that $\det(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, 1)) = p_0^{-1}\det(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, p_0))$, we see that (31) implies (25) as long as

$$2^{-[(\beta+1)t_s+\log(t_s+1)+1](t_s+1)} p_0 \ge 2^{(\beta-2)(t_s+1)}. \tag{38}$$

Using $p_0 \ge 2^{k-1}$, $\log(t_s+1) \le t_s+1$ (since $t_s \ge 1$), we find that (38) is implied by $k \ge (\beta+3)(t_s+1)^2+1$, which is in turn implied by (16). Now, (31) is implied by the condition $\frac{P_{I,max}2H}{A_L/p_0} \le 2^{(\beta-2)(t_s+1)}H^{t_s+1}$, where $P_{I,max} = 2^{(k+1)t_s}$ is an upper bound on P_I and $A_L = p_0 2^{(t-1)k}$ is a lower bound on A. Using (36), we have $H \ge 2^{\alpha k-2}$ and so (31) is satisfied as long as $2^{(k+1)t_s-(t-1)k+1} \le 2^{(\beta-2)(t_s+1)+(\alpha k-2)t_s}$. Rearranging the last inequality gives the sufficient condition $(1-\alpha-\frac{\beta-5}{k})t_s \le t-1+\frac{\beta-1}{k}$, and using $1-\alpha = \frac{1+\delta_F}{t'/t}$ and $0 < \frac{\beta-5}{k} \le \frac{1+\delta_F}{t'/t}$ (where the last inequality follows from the choice of β and k satisfying (34) and (37)), we conclude that both (25) and (31) are satisfied as long as

$$t_s \le \frac{t'-t'/t}{1+\delta_F}, \tag{39}$$

which is satisfied by the theorem hypothesis $t_s = \frac{t'-t'/t}{1+\delta_F}$.

This completes the proof of the claimed values for $(t_s, \delta_s, \epsilon_s)$ and the inequality for k. However, note that our arguments above also assumed that $t_s = \frac{t'-t'/t}{1+\delta_F} \ge t$. For the case $t_s < t$, we can apply the security bound in [19] for the standard CRT secret-sharing scheme. This bound gives $\epsilon_s \le \log(2p_0/C(I))$ for any $I \subseteq [n]$ with $\#I = t_s < t$, where $C(I) = \lfloor\frac{P_{t-1}}{\prod_{\nu\in I}p_\nu}\rfloor$. Using $P_{t-1} \ge 2^{(t-1)k}$ and $\prod_{\nu\in I}p_\nu \le 2^{(t-1)(k+1)}$, we get $C(I) \ge \lfloor p_0/2^{t-1}\rfloor \ge p_0/2^t$ assuming $k \ge t+1$ (which is implied by (16)). So for $t_s < t$, we have $\epsilon_s \le \log(2p_0/(p_0/2^t)) \le t+1$, so our claimed bound $\epsilon_s = \max((\beta+4)(t_s+1), t+1)$ holds also for $t_s < t$ (for all public parameters).

Finally, to establish the asymptotic security claim, note that when $\delta_c = k^{-c}$ for some constant $c > 0$, we get $\beta = O(\log k)$ and $\theta = O(\log k)$, so (16) is satisfied for sufficiently large k and $\epsilon_s = O(\log k)$ so the fraction of lost entropy $\epsilon_s/k = o(1)$. This completes the proof of the theorem. □

An immediate consequence of the above results is the following.

Corollary 4.1. *The standard (t,n) CRT threshold secret-sharing scheme* CRTTSS *is asymptotically threshold-changeable to $(Int(t'-t'/t), t')$ for any $t' > t$, where $Int(z)$ denotes the largest integer strictly less than z.*

5 Conclusion

We have shown an application of lattice theory to enable threshold-changeability of CRT secret-sharing schemes. Our results are analogous to those obtained by lattice methods for the polynomial-based Shamir secret-sharing scheme [23], despite the differences in the details of the lattices involved.

There are several open problems related to our scheme. The first is to improve our security bounds. Another problem is to extend the application of our 'noisy' Chinese remaindering decoding algorithm. One possible extension is to the method to detecting/identifying cheating shareholders who provide incorrect shares to the share combiner algorithm. A known approach [17] to cheater detection involves using extra 'redundant' shares: the combiner for a (t, n) scheme asks for $t' > t$ shares. For the CRT secret sharing scheme, the problem of detecting/correcting up to k incorrect shares is equivalent to error detection/correction for a Chinese Remainder code, where the share error vector has *Hamming* weight at most k. The cheating *detection* problem for $k \leq t' - t$ cheaters can be efficiently solved for both the original CRT scheme as well as our threshold-changeable version of it: the combiner applies the (t, n) reconstruction algorithm to any subset of t shares out of the t' received shares to recover the integer a and then checks that all t' received shares are consistent (for our changeable threshold scheme this means checking that $\|t_i - B \cdot a\|_{L,p_i} < H$ for all the received subshares t_i). For the cheater *identification* problem, one could use the Hamming norm error correction algorithms of [8, 5] for the original CRT scheme. However, identifying cheaters efficiently in our changeable threshold scheme requires an error correction algorithm for the CRT code with up to k incorrect shares, and where *all* the correct CRT shares are corrupted by small additive noise (after multiplication by a known constant). An interesting problem could be to construct such an efficient error correction algorithm (better than trying to combine every subset of t shares and checking for consistency of at least $t' - k$ shares), perhaps by combining in some way our Lee norm error correction method with the Hamming norm error correction methods of [8, 5].

Acknowledgements. The authors would like to thank Scott Contini and Igor Shparlinski for helpful discussions. This work was supported by ARC grants DP0451484 and DP0345366.

References

[1] C. Asmuth and J. Bloom. A Modular Approach to Key Safeguarding. *IEEE Trans. on Information Theory*, 29:208–210, 1983.

[2] L. Babai. On Lovasz' Lattice Reduction and the Nearest Lattice Point Problem. *Combinatorica*, 6:1–13, 1986.

[3] C.H. Bennett, G. Brassard, C. Crépau, and U.M. Maurer. Generalized Privacy Amplification. *IEEE Trans. on Information Theory*, 41:1915–1923, 1995.

[4] C. Blundo, A. Cresti, A. De Santis, and U. Vaccaro. Fully Dynamic Secret Sharing Schemes. In *CRYPTO '93*, volume 773 of *LNCS*, pages 110–125, Berlin, 1993. Springer-Verlag.

[5] D. Boneh. Finding Smooth Integers in Short Intervals using CRT Decoding. In *Proc. 32-nd ACM Symp. on Theory of Comput.*, pages 265–272, New York, 2000. ACM Press.

[6] Y. Desmedt and S. Jajodia. Redistributing Secret Shares to New Access Structures and Its Application. Technical Report ISSE TR-97-01, George Mason University, 1997.

[7] C. Ding, D. Pei, and A. Salomaa. *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography.* World Scientific, Singapore, 1996.

[8] O. Goldreich, D. Ron, and M. Sudan. Chinese Remaindering with Errors. *IEEE Transactions on Information Theory*, 46:1330–1338, 2000.

[9] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization.* Springer-Verlag, 1993.

[10] P. Gruber and C. Lekkerkerker. *Geometry of Numbers.* Elsevier Science Publishers, 1987.

[11] E. Hlawka, J. Schoißengeier, and R. Taschner. *Geometric and Analytic Number Theory.* Springer-Verlag, 1991.

[12] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[13] A. Maeda, A. Miyaji, and M. Tada. Efficient and Unconditionally Secure Verifiable Threshold Changeable Scheme. In *ACISP 2001*, volume 2119 of *LNCS*, pages 402–416, Berlin, 2001. Springer-Verlag.

[14] K. Martin. Untrustworthy Participants in Secret Sharing Schemes. In *Cryptography and Coding III*, pages 255–264. Oxford University Press, 1993.

[15] K. Martin, J. Pieprzyk, R. Safavi-Naini, and H. Wang. Changing Thresholds in the Absence of Secure Channels. *Australian Computer Journal*, 31:34–43, 1999.

[16] K. Martin, R. Safavi-Naini, and H. Wang. Bounds and Techniques for Efficient Redistribution of Secret Shares to New Access Structures. *The Computer Journal*, 42:638–649, 1999.

[17] R.J. McEliece and D.V. Sarwate. On Sharing Secrets and Reed-Solomon Codes. *Comm. of the ACM*, 24:583–584, 1981.

[18] M. Mignotte. How To Share a Secret. In *Eurocrypt '82*, volume 149 of *LNCS*, pages 371–375, Berlin, 1983. Springer-Verlag.

[19] M. Quisquater, B. Preneel, and J. Vandewalle. On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem. In *PKC 2002*, volume 2274 of *LNCS*, pages 199–210, Berlin, 2002. Springer-Verlag.

[20] J.B. Rosser and L. Schoenfeld. Approximate Formulas for Some Functions of Prime Numbers. *Illinois. J. Math.*, 6:64–94, 1962.

[21] A. Shamir. How To Share a Secret. *Comm. of the ACM*, 22:612–613, 1979.

[22] I.E. Shparlinski and R. Steinfeld. Noisy Chinese Remaindering in the Lee Norm. *Journal of Complexity*, 20:423–437, 2004.

[23] R. Steinfeld, H. Wang, and J. Pieprzyk. Lattice-Based Threshold Changeability for Standard Shamir Secret-Sharing Schemes. In *Asiacrypt 2004*, volume 3329 of *LNCS*, pages 170–186. Springer-Verlag, 2004.

A Proof of Lemma 4.1

We define a mapping $f : S_{\widehat{s},\widehat{p}_0} \to V_{\widehat{s},\widehat{p}_0}$ and show that f is 1-1 and onto.

The mapping f is defined as follows. To each integer $a = k_a \cdot \widehat{p}_0 + \widehat{s} \in S_{\widehat{s},\widehat{p}_0}$ (note that $k_a \in \mathbb{Z}_{A/\widehat{p}_0}$ for all such a), we associate the lattice vector $f(a) = \mathbf{v}_{k_a,\mathbf{k}_a}$, where

$$\mathbf{v}_{k_a,\mathbf{k}_a} \overset{\text{def}}{=} (B\widehat{p}_0 k_a + k_{a,1}p_{i[1]}, \ldots, B\widehat{p}_0 k_a + k_{a,t_s}p_{i[t_s]}, \frac{k_a}{A/\widehat{p}_0}2H) \in \mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0), \tag{40}$$

and $\mathbf{k}_a = (k_{a,1}, \ldots, k_{a,t_s})$ is the unique vector in $\mathbb{Z}^{t_s}$ such that

$$\|\mathbf{v}_{k_a,\mathbf{k}_a} - \widehat{\mathbf{s}}_I\|_\infty < H. \tag{41}$$

To show that f is a well-defined mapping from $S_{\widehat{s},\widehat{p}_0}$ to $V_{\widehat{s},\widehat{p}_0}$, we need to show that for each $a = k_a \cdot \widehat{p}_0 + \widehat{s} \in S_{\widehat{s},\widehat{p}_0}$ there exists a unique $\mathbf{k}_a \in \mathbb{Z}^{t_s}$ satisfying (41). Indeed, $a = k_a\widehat{p}_0 + \widehat{s} \in S_{\widehat{s},\widehat{p}_0}$ implies by definition that $\|B(k_a\widehat{p}_0 + \widehat{s}) - s_{i[j]}\|_{L,p_{i[j]}} < H$ and hence that there exists $k_{a,j} \in \mathbb{Z}$ such that $|B(k_a\widehat{p}_0 + \widehat{s}) - s_{i[j]} + k_{a,j}p_{i[j]}| = |Bk_a\widehat{p}_0 + k_{a,j}p_{i[j]} - \widehat{\mathbf{s}}_I[j]| < H$ for all $j \in [t_s]$, and since $k_a \in \mathbb{Z}_{A/\widehat{p}_0}$ we also have $|\mathbf{v}_{k_a,\mathbf{k}_a}[t_s+1] - \widehat{\mathbf{s}}_I[t_s+1]| = |(\frac{k_a}{A/\widehat{p}_0})2H - (\frac{A/\widehat{p}_0 - 1}{A/\widehat{p}_0})| < H$, so there exists $\mathbf{k}_a \in \mathbb{Z}^{t_s}$ satisfying (41). To show that $\mathbf{k}_a$ satisfying (41) is unique, note that for any $\mathbf{k} = (k_1, \ldots, k_{t_s}) \in \mathbb{Z}^{t_s}$ which is not equal to $\mathbf{k}_a$, there exists a coordinate $j \in [t_s]$ for which $k_j = k_{a,j} + u$ for some non-zero integer u, and this implies that $|\mathbf{v}_{k_a,\mathbf{k}}[j] - \widehat{\mathbf{s}}_I[j]| = |Ba + (k_{a,j} + u)p_{i[j]} - s_{i[j]}| \geq |u|p_{i[j]} - H \geq p_{i[j]} - H \geq H$ (using $|Ba + k_{a,j}p_{i[j]} - s_{i[j]}| < H$, $|u| \geq 1$ and $p_{i[j]} \geq 2H$), so that (41) is not satisfied by $\mathbf{k}$, and $\mathbf{k}_a$ is unique as claimed.

To show that f is 1-1, we simply observe that for any distinct pair $a^{(1)} = k_a^{(1)}\widehat{p}_0 + \widehat{s}$ and $a^{(2)} = k_a^{(2)}\widehat{p}_0 + \widehat{s}$ in $S_{\widehat{s},\widehat{p}_0}$ we have $k_a^{(1)} \neq k_a^{(2)}$ so the lattice vectors $f(a^{(1)})$ and $f(a^{(2)})$ differ in the (t_s+1)th coordinate. Hence f is 1-1.

To show that f is onto, observe that any vector $\mathbf{v}$ in $V_{s,p}$ has the form $\mathbf{v} = \mathbf{v}_{k_a,\mathbf{k}_a}$ defined in (40) for some $k_a \in \mathbb{Z}$ and $\mathbf{k}_a = (k_{a,1}, \ldots, k_{a,t_s}) \in \mathbb{Z}^{t_s}$, and satisfies (41). Let $a = k_a\widehat{p}_0 + \widehat{s}$. Then by construction we know that $f(a) = \mathbf{v}_{k_a,\mathbf{k}_a}$, and it remains to show that $a \in S_{\widehat{s},\widehat{p}_0}$. Indeed, (41) implies that $|B\widehat{p}_0k_a + k_{a,j}p_{i[j]} - (s_{i[j]} - B\widehat{s})| = |B(\widehat{p}_0k_a + \widehat{s}) - s_{i[j]}| < H$ so $\|Ba - s_{i[j]}\|_{L,p_{i[j]}} < H$ for all $j \in [t_s]$. Also, $|(\frac{k_a}{A/\widehat{p}_0})2H - (\frac{A/\widehat{p}_0 - 1}{A/\widehat{p}_0})H| < H$ so $|2k_a - (A/\widehat{p}_0 - 1)| < A/\widehat{p}_0$ which implies that $k_a \in \mathbb{Z}_{A/\widehat{p}_0}$. Thus $a = \widehat{p}_0k_a + \widehat{s} \in \mathbb{Z}_A$ (using $\widehat{s} \in \mathbb{Z}_{\widehat{p}_0}$) and hence $a \in S_{\widehat{s},\widehat{p}_0}$, as required, and f is onto. This completes the proof. □

B Proof of Lemma 4.2

We lower bound the number of lattice points in the box $K_1 = \{\mathbf{v} \in \mathbb{R}^{t_s+1} : \|\mathbf{v} - \mathbf{s}_I\|_\infty < H\}$ of side length $2H$ which is centered on the non-lattice vector $\mathbf{s}_I$, by the number of lattice points in the box $K_2 = \{\mathbf{v} \in \mathbb{R}^{t_s+1} : \|\mathbf{v} - \mathbf{s}'_I\|_\infty < H - \epsilon\}$ of side length $2(H - \epsilon)$, which is centered on a lattice vector $\mathbf{s}'_I$. We obtain the lattice vector $\mathbf{s}'_I$ by 'rounding' the non-lattice vector $\mathbf{s}_I$ to a 'nearby' lattice vector. Suppose that the 'rounding error' $\|\mathbf{s}_I - \mathbf{s}'_I\|_\infty = \epsilon$. Then it is easy to see by the triangle inequality that the box K_2 defined above is fully contained within the box K_1, and thus the number of lattice points inside K_2 is indeed a lower bound on the number of lattice points in K_1. In turn, since any lattice is invariant under additions of any lattice vector, it follows that the number of lattice points in the box K_2 is equal to the number of points in the origin-centered box $\{\mathbf{v} \in \mathbb{R}^{t_s+1} : \|\mathbf{v}\|_\infty < H - \epsilon\}$, which is the desired result.

It remains to prove the claimed bound on the rounding error $\epsilon = \|\mathbf{s}_I - \mathbf{s}'_I\|_\infty$. By definition of the (t_s+1)th Minkowski minimum λ_{t_s+1} of the lattice, we know that there exists a set $(\mathbf{b}_1, \ldots, \mathbf{b}_{t_s+1})$ of t_s+1 linearly-independent lattice vectors such that $\|\mathbf{b}_j\|_\infty < \lambda_{t_s+1}$ for all $j = 1, \ldots, t_s+1$. Note that although the vectors $(\mathbf{b}_1, \ldots, \mathbf{b}_{t_s+1})$ do not necessarily form a basis for the lattice, they do necessarily form a basis for the vector space $\mathbb{R}^{t_s+1}$ over $\mathbb{R}$. Hence any vector $\mathbf{s}_I \in \mathbb{R}^{t_s+1}$ can be expanded as $\mathbf{s}_I = c_1\mathbf{b}_1 + \cdots + c_{t_s+1}\mathbf{b}_{t_s+1}$ for some real coefficients $c_1, \ldots, c_{t_s+1}$. Now let $\mathbf{s}'_I$ denote the lattice vector which is obtained by rounding the coefficients $c_1, \ldots, c_{t_s+1}$ to the nearest integers, i.e. we let

$$\mathbf{s}'_I = \widehat{c}_1\mathbf{b}_1 + \cdots + \widehat{c}_{t_s+1}\mathbf{b}_{t_s+1},$$

where for $i = 1, \dots, t_s + 1$, $\widehat{c}_i$ denotes integer closest to c_i. Then the rounding error is

$$\epsilon = \|\mathbf{s}_I - \mathbf{s}'_I\|_\infty = \| \sum_j (c_j - \widehat{c}_j)\mathbf{b}_j\|_\infty \le \frac{1}{2}\sum_j \|\mathbf{b}_j\|_\infty \le \left(\frac{t_s+1}{2}\right)\lambda_{t_s+1},$$

as claimed. This completes the proof. □

C Proof of Lemma 4.3

Let Δ denote a positive real number (to be chosen later) which satisfies $\Delta_{min} \le \Delta \le \Delta_{max}$ for some fixed positive integers (to be chosen later) $\Delta_{min} \ge 1$ and $\Delta_{max} \le \min(B\widehat{p}_0, 2^k)$. Note that Δ may depend on the choice of $\mathbf{p}_I$ but we assume the fixed bounds Δ_{min} and Δ_{max} do not depend on $\mathbf{p}_I$.

Now, observe that any $\mathbf{v} \in \mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0)$ is of the form

$$\mathbf{v}_{b,\mathbf{k}} \overset{\text{def}}{=} (B\widehat{p}_0 b + k_1 p_{i[1]}, \dots, B\widehat{p}_0 b + k_{t_s} p_{i[t_s]}, \frac{b}{A/\widehat{p}_0} 2H) \in \mathbb{Q}^{t_s+1},$$

for some $b \in \mathbb{Z}$ and $\mathbf{k} = (k_1, \dots, k_{t_s}) \in \mathbb{Z}^{t_s}$.

We now upper bound the fraction δ of $\mathbf{p}_I \in D(\mathcal{P}_k^{t_s})$ such that $\lambda_1(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0)) < \Delta$, i.e. such that there exists a non-zero vector $\mathbf{v}_{b,\mathbf{k}} \in \mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0)$ with $\|\mathbf{v}_{b,\mathbf{k}}\|_\infty < \Delta$.

For the case $b = 0$, we have, assuming $\mathbf{v}_{0,\mathbf{k}} \ne \mathbf{0}$ that $\mathbf{k} \ne \mathbf{0}$ and hence $\|\mathbf{v}_{0,\mathbf{k}}\|_\infty \ge \min_{j \in [t_s]} p_{i[j]} \ge 2^k \ge \Delta_{max} \ge \Delta$.

For the case $b \ne 0$, suppose that $\|\mathbf{v}_{b,\mathbf{k}}\|_\infty < \Delta$ for some $\mathbf{k} \in \mathbb{Z}^{t_s}$. Then, considering the last coordinate of $\mathbf{v}_{b,\mathbf{k}}$, we know that the integer $|b|$ satisfies

$$0 < |b| < \frac{A/\widehat{p}_0}{2H}\Delta \le \left\lceil \frac{A/\widehat{p}_0}{2H}\Delta_{max} \right\rceil.$$

Also, considering the first t_s coordinates of $\mathbf{v}_{b,\mathbf{k}}$, the integer $|b|$ also satisfies

$$\|(B\widehat{p}_0)|b|\|_{L,\mathbf{p}_I} < \Delta \le \Delta_{max}.$$

So, applying Lemma 2.1 (with parameters $\ell = k$, $n = t_s$, $\widehat{A} = \left\lceil \frac{A/\widehat{p}_0}{2H}\Delta_{max} \right\rceil$, $\widehat{H} = \Delta_{max}$ and $\widehat{B} = B\widehat{p}_0 \ge \Delta_{max}$) we conclude that $\lambda_1(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0)) \ge \Delta$ for all except at most a fraction δ of $\mathbf{p}_I \in D(\mathcal{P}_k^{t_s})$, where

$$\delta \le \frac{\widehat{A}\left(2\widehat{H}\log(\widehat{B}\widehat{A} + \widehat{H})k^{-1}\right)^{t_s}}{\#D(\mathcal{P}_k^{t_s})}.$$

Now, using $\widehat{B} \ge \widehat{H}$ and $\widehat{B} \ge 1$ we have $\widehat{B}\widehat{A} + \widehat{H} \le 2\widehat{B}\widehat{A}$. Also we know[20] that $\#\mathcal{P}_k \ge 2^{k-1}k^{-1}$ for all $k \ge 5$ and hence $\#\mathcal{P}_k^{t_s}/\#D(\mathcal{P}_k^{t_s}) \le 2^{t_s}$ using $\#\mathcal{P}_k - (t_s - 1) \ge \#\mathcal{P}_k/2$ which is implied by the hypothesis $k - \log k \ge \log t_s + 2$ (these inequalities are obtained as in the proof of Theorem 4.1). Plugging these bounds in the above inequality for δ we get

$$\delta \le \frac{2^{t_s}\widehat{A}\left(2\widehat{H}\log(2\widehat{A}\widehat{B})\right)^{t_s}}{2^{(k-1)t_s}}.$$

Using $\widehat{A} = \left\lceil \frac{A/\widehat{p}_0}{2H}\Delta_{max} \right\rceil \le \frac{A/\widehat{p}_0}{H}\Delta_{max}$ (since $A/\widehat{p}_0 \ge 2H$ and $\Delta_{max} \ge \Delta_{min} \ge 1$), and recalling that

$\widehat{H} = \Delta_{max}$, $\widehat{B} = B\widehat{p}_0$, we obtain

$$\delta \leq 2^{(4+\log\log(2\frac{B}{H}A\Delta_{max}))t_s+1} \frac{\Delta_{max}^{t_s+1}}{\left(\frac{P_{I,max}2H}{A/\widehat{p}_0}\right)}, \tag{42}$$

where $P_{I,max} = 2^{(k+1)t_s}$ is an upper bound on P_I. Now, observing that $\det(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0)) = \left(\frac{P_I 2H}{A/\widehat{p}_0}\right)$, let us choose

$$\Delta = 2^{-\beta} \det(\mathcal{L}_{CRT}(\mathbf{p}_I, A, B, H, \widehat{p}_0))^{\frac{1}{t_s+1}},$$

which is lower bounded for all $\mathbf{p}_I \in \mathcal{P}_k^{t_s}$ by the fixed integer

$$\Delta_{min} = \left\lfloor 2^{-\beta} \left(\frac{P_{I,min}2H}{A/\widehat{p}_0}\right)^{\frac{1}{t_s+1}} \right\rfloor,$$

(where $P_{I,min} = 2^{k \cdot t_s}$ is a lower bound on P_I), and upper bounded for all $\mathbf{p}_I \in \mathcal{P}_k^{t_s}$ by the fixed integer

$$\Delta_{max} = \left\lceil 2^{-\beta} \left(\frac{P_{I,max}2H}{A/\widehat{p}_0}\right)^{\frac{1}{t_s+1}} \right\rceil.$$

With the above choices, the assumed conditions $\Delta_{min} \geq 1$ and $\Delta_{max} \leq \min(B, 2^k)$ can be readily seen to be implied by the lemma hypothesis

$$1 \leq 2^{-\beta} \left(\frac{2^{k \cdot t_s}2H}{A/\widehat{p}_0}\right)^{\frac{1}{t_s+1}} \leq \frac{1}{4}\min(B, 2^k),$$

and plugging the values of Δ_{min} and Δ_{max} in (42) gives us the claimed bound

$$\delta \leq 2^{-[\beta-(\log\log(2^{k+2}\frac{B}{H}A)+5)](t_s+1)}$$

for the 'bad' fraction of $\mathbf{p}_I \in D(\mathcal{P}_k^{t_s})$. This completes the proof. □

D Proof of Lemma 4.4

Let N denote the number of points of the lattice $\mathcal{L}$ in the box $K_1 = \{\mathbf{v} \in \mathbb{R}^n : \|\mathbf{v} - \mathbf{s}\|_\infty < H\}$. Suppose that on each lattice point $\mathbf{v}$ in the box , we center an open box $S_\mathbf{v} = \{\mathbf{z} \in \mathbb{R}^n : \|\mathbf{z} - \mathbf{v}\|_\infty < \lambda_1(\mathcal{L})/2\}$ of side length $\lambda_1(\mathcal{L})/2$. Note that as $\mathbf{v}$ runs through all lattice vectors in the box K_1, the boxes $S_\mathbf{v}$ are disjoint (because by the triangle inequality, the existence of a vector $\mathbf{z}$ in two of the boxes $S_{\mathbf{v_1}}$ and $S_{\mathbf{v_2}}$ implies that $\|\mathbf{v}_1 - \mathbf{v}_2\|_\infty < \lambda_1(\mathcal{L})$, which is a contradiction since $\mathbf{v}_1 - \mathbf{v}_2$ is itself a lattice vector), and occupy a total volume $N \cdot \lambda_1(\mathcal{L})^n$.

On the other hand, applying the triangle inequality again, we have that all the above N disjoint boxes $S_\mathbf{v}$ are contained within the box $K_2 = \{\mathbf{z} \in \mathbb{R}^n : \|\mathbf{v} - \mathbf{s}\|_\infty < H + \lambda_1(\mathcal{L})/2\}$, which has volume $Vol(K_2) = (2H + \lambda_1(\mathcal{L}))^n$.

It follows that

$$Vol(K_2) = (2H + \lambda_1(\mathcal{L}))^n \geq N \cdot \lambda_1(\mathcal{L})^n,$$

and therefore,

$$N \leq \left(\frac{2H}{\lambda_1(\mathcal{L})} + 1\right)^n,$$

as required. This completes the proof. □