A Probability Inequality with Application to Lattice Theory

Tian Kun

Abstract Here we mainly provide a probability inequality about GGH public-key encryption scheme. Given a constant σ, we first choose a lattice vector $v \in \mathbb{Z}^n$, and a small error vector e is generated satisfying $|e| \leqslant \sigma$. The ciphertext result c could be computed by the function $f_{B,\sigma}(v, e) = Bv + e$ with a public basis B. To extract the message v, the function $f^{-1}_{B,\sigma}(c) = B^{-1}[c]_R$ will be used based on the private basis R. In this work we produce a bound for the error probability of $v \neq B^{-1}[c]_R$. We also illustrate the way choosing σ such that the error probability is arbitrarily small.

Keywords Probability inequality · Encryption scheme · Lattice

1 Introduction

Given a full-rank lattice $L \subset \mathbb{Z}^n$, we denote the public basis of L by B and private basis of L by R. Both B and R are $n \times n$ invertible matrices. In the GGH public-key encryption scheme, for a plaintext vector $v \in \mathbb{Z}^n$, the random error vector e is chosen by setting the absolute value of each entry no more than a constant σ, where σ is a positive real number. The ciphertext c is computed by $c = f_{B,\sigma}(v, e) = Bv + e \in \mathbb{R}^n$. Using the results of BaBai and some other ones (Ajtai, 1996; Ajtai & Dwork, 1997; Babai, 1986; Coppersmith & Shamir, 1997; Goldreich et al., 1997; Micciancio, 2001; Hoffstein et al., 2017, 1998), we can decipher the plaintext $v = B^{-1}[c]_R$ given B, R and ciphertext c. Here the lattice point $[c]_R$ is obtained by representing c as a linear combination on the columns of R and rounding the coefficients in this linear combination to the nearest integers. The problem is that how σ should be chosen so that we can get a right plaintext v or guarantee a low error probability. We show three theorems to solve this problem. A probability inequality is given to estimate the bound of inversion error probability.

T. Kun (✉)
School of Mathematics, Renmin University of China, Beijing 100872, China
e-mail: tkun19891208@ruc.edu.cn

Z. Zheng (ed.), *Proceedings of the Second International Forum on Financial Mathematics and Financial Technology*, Financial Mathematics and Fintech,
https://doi.org/10.1007/978-981-99-2366-3_2

2 Main Results

Theorem 1 *B is the public basis and R is the private basis of lattice L. $v \in \mathbb{Z}^n$, e is the random error vector, $|e|_\infty \leqslant \sigma$, $c = f_{B,\sigma}(v, e) = Bv + e$. Then $B^{-1}[c]_R = v$ if and only if $[R^{-1}e] = 0$, here $[R^{-1}e]$ denotes the vector in $\mathbb{Z}^n$ which is obtained by rounding each entry in $R^{-1}e$ to the nearest integer.*

Proof Let $T = B^{-1}R$, then

$$B^{-1}[c]_R = B^{-1}[Bv + e]_R = B^{-1}R[R^{-1}(Bv + e)] = T[T^{-1}v + R^{-1}e]$$

since $T = B^{-1}R$ is a unimodular matrix, T^{-1} is also a unimodular matrix. $v \in \mathbb{Z}^n$, so $T^{-1}v \in \mathbb{Z}^n$.

$$B^{-1}[c]_R = T[T^{-1}v + R^{-1}e] = v + T[R^{-1}e]$$

Thus $B^{-1}[c]_R = v$ is equivalent to $T[R^{-1}e] = 0$, and this equality holds if and only if $[R^{-1}e] = 0$.

Remark 1 This theorem gives an equivalent condition to check whether the decryption result is accurate.

Theorem 2 *Let R be the private basis of lattice L. e is the random error vector such that $|e|_\infty \leqslant \sigma$. Suppose the maximum L_1 norm of the rows in R^{-1} is ρ. Then if $\sigma < \frac{1}{2\rho}$, $[R^{-1}e] = 0$ holds.*

Proof Let $R^{-1} = (c_{ij})_{n\times n}$, $R^{-1}e = (a_1, a_2, ..., a_n)^T$, i.e., $a_i = \sum_{j=1}^{n} c_{ij}e_j$, $1 \leqslant i \leqslant n$.

$$|a_i| = |\sum_{j=1}^{n} c_{ij}e_j| \leqslant |e_j||\sum_{j=1}^{n} c_{ij}| \leqslant \sigma\rho < \frac{1}{2}$$

This means that $[R^{-1}e] = 0$.

Remark 2 Theorem 2 shows how σ can be chosen so that no inversion error occurs.

Theorem 3 *Let an $n \times n$ matrix R be the private basis used in the inversion of $f_{B,\sigma}$, and denote the maximum L_∞ norm of the rows in R^{-1} by $\frac{r}{\sqrt{n}}$. Then the probability of inversion errors is bounded by*

$$P\{[R^{-1}e] \neq 0\} \leqslant 2n \cdot exp\left(-\frac{1}{8\sigma^2 r^2}\right),$$

here $e = (e_1, e_2, ..., e_n)^T$ and $e_1, e_2, ..., e_n$ are n independent random variables such that $|e_i| \leqslant \sigma$ and $E(e_i) = 0$ for $1 \leqslant i \leqslant n$.

Lemma 1 *For any non-negative random variable X with finite expectation $E(X)$ and any positive real number μ, we have*

$$P\{X \geqslant \mu\} \leqslant \frac{E(X)}{\mu}.$$

Proof Here we treat X as a random variable of continuous type. For the other situations, the proof is similar. Let $f(x)$ be the probability density function of X. Since $E(X) = \int_0^{+\infty} xf(x)\mathrm{d}x \geqslant \int_\mu^{+\infty} xf(x)\mathrm{d}x \geqslant \int_\mu^{+\infty} \mu f(x)\mathrm{d}x = \mu P\{X \geqslant \mu\}$, then we have $P\{X \geqslant \mu\} \leqslant \frac{E(X)}{\mu}$.

Lemma 2 *Given random variable X satisfying $-a \leqslant X \leqslant a$ with $E(X) = 0$, here $a > 0$. For any real number λ, we have*

$$E(e^{\lambda X}) \leqslant exp\left(\frac{\lambda^2 a^2}{2}\right).$$

Proof For any real number λ, $f(x) = e^{\lambda x}$ is a convex function. Notice that

$$x = \frac{x+a}{2a} \cdot a + \frac{a-x}{2a} \cdot (-a), \quad -a \leqslant x \leqslant a$$

then

$$f(x) \leqslant \frac{x+a}{2a} f(a) + \frac{a-x}{2a} f(-a)$$

$$e^{\lambda x} \leqslant \frac{x+a}{2a} e^{\lambda a} + \frac{a-x}{2a} e^{-\lambda a}$$

$$E(e^{\lambda X}) \leqslant E(\frac{X+a}{2a} e^{\lambda a} + \frac{a-X}{2a} e^{-\lambda a}) = \frac{1}{2}(e^{\lambda a} + e^{-\lambda a})$$

Let $t = \lambda a$, next we prove that $\frac{1}{2}(e^t + e^{-t}) \leqslant \exp(\frac{t^2}{2})$. This inequality is equivalent to

$$\ln \frac{e^t + e^{-t}}{2} \leqslant \frac{t^2}{2}$$

Let $g(t) = \frac{t^2}{2} - \ln \frac{e^t+e^{-t}}{2}$, then $g'(t) = t - \frac{e^t-e^{-t}}{e^t+e^{-t}}$ and $g'(0) = 0$. Since $g''(t) \geqslant 0$, we get $g'(t) \leqslant 0$ if $t \leqslant 0$ and $g'(t) \geqslant 0$ if $t \geqslant 0$. Then $g(t) \geqslant g(0) = 0$ and we complete the proof.

Lemma 3 *Suppose $X_1, X_2, ..., X_n$ are n independent random variables. For $1 \leqslant i \leqslant n$, we have $-a \leqslant X_i \leqslant a$ and $E(X_i) = 0$, here $a > 0$. Let $S_n = \sum_{i=1}^n X_i$, $\varepsilon > 0$, then*

$$P\{|S_n| \geqslant \varepsilon\} \leqslant 2exp(-\frac{\varepsilon^2}{2na^2}).$$

Proof For any $\lambda > 0$, based on Lemma 1, we can get

$$P\{S_n \geqslant \varepsilon\} = P\{e^{\lambda S_n} \geqslant e^{\lambda\varepsilon}\} \leqslant \frac{E(e^{\lambda S_n})}{e^{\lambda\varepsilon}}$$

Since $X_1, X_2, ..., X_n$ are independent random variables, combine with Lemma 2,

$$E(e^{\lambda S_n}) = \prod_{i=1}^{n} E(e^{\lambda X_i}) \leqslant \prod_{i=1}^{n} e^{\frac{\lambda^2 a^2}{2}} = e^{\frac{n\lambda^2 a^2}{2}}$$

$$P\{S_n \geqslant \varepsilon\} \leqslant \frac{E(e^{\lambda S_n})}{e^{\lambda\varepsilon}} \leqslant e^{-\lambda\varepsilon + \frac{n\lambda^2 a^2}{2}}$$

Let $\lambda = \frac{\varepsilon}{na^2}$, therefore, the above inequality becomes to

$$P\{S_n \geqslant \varepsilon\} \leqslant \exp\left(-\frac{\varepsilon^2}{2na^2}\right)$$

In the same way, we can prove that

$$P\{S_n \leqslant -\varepsilon\} \leqslant \exp\left(-\frac{\varepsilon^2}{2na^2}\right)$$

Thus

$$P\{|S_n| \geqslant \varepsilon\} \leqslant 2\exp\left(-\frac{\varepsilon^2}{2na^2}\right)$$

Proof of Theorem 3. Now we can prove Theorem 3 given at first according to Lemma 3.
Let $R^{-1} = (c_{ij})_{n\times n}$, $e = (e_1, e_2, ..., e_n)^T$, here $e_1, e_2, ..., e_n$ are n independent random variables such that $|e_i| \leqslant \sigma$ and $E(e_i) = 0$ for $1 \leqslant i \leqslant n$.
We denote $R^{-1}e = (a_1, a_2, ..., a_n)^T$, i.e., $a_i = \sum_{j=1}^{n} c_{ij}e_j$, $1 \leqslant i \leqslant n$.
Since $|c_{ij}| \leqslant \frac{r}{\sqrt{n}}$ and $|e_j| \leqslant \sigma$, then the random variable $c_{ij}e_j$ is limited to the interval $[-\frac{r\sigma}{\sqrt{n}}, \frac{r\sigma}{\sqrt{n}}]$. Based on Lemma 3,

$$P\{|a_i| \geqslant \frac{1}{2}\} = P\{|\sum_{j=1}^{n} c_{ij}e_j| \geqslant \frac{1}{2}\} \leqslant 2\exp(-\frac{(\frac{1}{2})^2}{2n(\frac{r\sigma}{\sqrt{n}})^2}) = 2\exp(-\frac{1}{8\sigma^2 r^2})$$

$$P\{[R^{-1}e] \neq 0\} \leqslant \sum_{i=1}^{n} P\{|a_i| > \frac{1}{2}\} \leqslant \sum_{i=1}^{n} P\{|a_i| \geqslant \frac{1}{2}\} \leqslant 2n \cdot \exp(-\frac{1}{8\sigma^2 r^2})$$

Thus the inequality in Theorem 3 holds.

Corollary 1 $P\{[R^{-1}e] \neq 0\} < \varepsilon$ *if* $\sigma < \left(2r\sqrt{2\ln\frac{2n}{\varepsilon}}\right)^{-1}$.

Proof $\sigma < \left(2r\sqrt{2\ln\frac{2n}{\varepsilon}}\right)^{-1} \Leftrightarrow 2n \cdot \exp\left(-\frac{1}{8\sigma^2 r^2}\right) < \varepsilon$, from Theorem 3,

$$P\{[R^{-1}e] \neq 0\} \leqslant 2n \cdot \exp\left(-\frac{1}{8\sigma^2 r^2}\right) < \varepsilon$$

Remark 3 Theorem 3 provides a way to estimate the bound of inversion error probability, and Corollary 1 gives a detailed bound for σ based on Theorem 3 to get the error probability no more than a constant ε.

3 Conclusions

In this work we mainly present a probability inequality about GGH public-key encryption scheme. In this scheme, we first take a lattice vector $v \in \mathbb{Z}^n$ and generate a small error vector e such that $|e| \leqslant \sigma$. Given a public basis B, the function $f_{B,\sigma}(v, e) = Bv + e$ computes the ciphertext result c. To decrypt, the private basis R and the function $f_{B,\sigma}^{-1}(c) = B^{-1}[c]_R$ will be used to extract the message v. We give a bound for the error probability of $v \neq B^{-1}[c]_R$ and explain how to choose σ in order to obtain the error probability no more than a given constant ε.

References

Ajtai, M. (1996). Generating hard instances of lattice problems. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (pp. 99–108).

Ajtai, M., Dwork, C. (1997). A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the 29th Annual ACM Symposium on Theory of Computing* (pp. 284–293).

Babai, L. (1986). On Lovasz lattice reduction and the nearest lattice point problem. *Combinatorica, 6,* 1–13.

Coppersmith, D., & Shamir, A. (1997). Lattice attacks on NTRU. *Advances in Cryptology, 1233,* 52–61.

Goldreich, O., Goldwasser, S., & Halevi, S. (1997). Public-key cryptosystems from lattice reduction problems. *Annual International Cryptology Conference, 1294,* 112–131.

Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: a ring based public key cryptosystem. *Algorithmic Number Theory, 1423,* 267–288.

Hoffstein, J., Pipher, J., Schanck, J. M., et al. (2017). Choosing parameters for NTRUEncrypt. *Topics in Cryptology, 10159,* 3–18.

Micciancio, D. (2001). Improving lattice based cryptosystems using the hermite normal form. *International Cryptography and Lattices Conference, 2146,* 126–145.