# Amostragem Gaussiana aplicada à Criptografia Baseada em Reticulados

**Jheyne N. Ortiz**[1], **Ricardo Dahab**[1], **Diego F. Aranha**[1]

[1]Instituto de Computação – Universidade Estadual de Campinas (UNICAMP)
Campinas – SP – Brasil

{jheyne.ortiz,rdahab,dfaranha}@ic.unicamp.br

***Abstract.*** *In Lattice-Based Cryptography, cryptosystems usually require sampling lattice points and integers following a Gaussian distribution. Sampling lattice points can also be used to solve variants of the SVP (Shortest Vector Problem) and CVP (Closest Vector Problem). This work presents constant-time implementations of the Knuth-Yao and discrete Ziggurat methods for Gaussian sampling over integers. The Knuth-Yao implementation was applied to sampling over lattices and to the Ring-LWE-based (Learning with Errors over Rings) encryption scheme. Our experiments targeted an Intel Ivy Bridge processor and all implementations are in C++ supported by Victor Shoup's NTL library.*

***Resumo.*** *Na Criptografia Baseada em Reticulados, vários esquemas requerem a amostragem de vetores de um reticulado e de inteiros seguindo uma distribuição que, convencionalmente, é Gaussiana. A amostragem de vetores de um reticulado pode também ser usada para resolver variantes dos problemas SVP (vetor mais curto) e CVP (vetor mais próximo). Este trabalho apresenta implementações com tempo de execução constante para os métodos Knuth-Yao e Ziggurat Discreto, apropriados à amostragem Gaussiana sobre os inteiros. Uma implementação para o método Knuth-Yao é aplicada à amostragem sobre reticulados e ao esquema de encriptação baseado no problema LWE (Learning with Errors) sobre anéis. Os experimentos foram feitos em processador Intel Ivy Bridge, usando C++ com suporte da biblioteca NTL de Victor Shoup.*

## 1. Introdução

A Criptografia Baseada em Reticulados é um conjunto de primitivas criptográficas calcado em problemas difíceis em reticulados, capazes de prover encriptação [Lyubashevsky et al. 2010, Stehlé and Steinfeld 2011], assinatura digital [Ducas et al. 2013, Hoffstein et al. 2014], acordo de chaves [Bos et al. 2015, Alkim et al. 2015] e esquemas funcionais [O'Neill 2010, Boneh et al. 2011]. Até o presente, tais primitivas se mostraram resistentes a ataques clássicos e quânticos. Além de resistentes a ataques quânticos, esquemas como o de encriptação baseado no problema Ring-LWE [Lyubashevsky et al. 2012] (*Learning with Errors over Rings*) e o NTRU [Hoffstein et al. 2010] são simples e eficientes, sendo candidatos à substituição de criptossistemas em uso atualmente, ameaçados pelos algoritmos de Peter Shor.

Esquemas sobre reticulados, como a Encriptação Baseada em Identidades [Agrawal et al. 2010], as funções de resumo seguidas de assinatura [Gentry et al. 2008] e Baseada em Atributos [Boneh et al. 2014], requerem a

amostragem de vetores estatisticamente próximos de um reticulado. Além disso, a amostragem sobre os inteiros é um passo nos métodos de amostragem em reticulados [Gentry et al. 2008, Peikert 2010], além de necessária em esquemas de encriptação [Lyubashevsky et al. 2012] e no esquema de assinatura [Ducas et al. 2013] baseados no problema Ring-LWE [Regev 2005]. Usualmente, ambos os tipos de amostragens seguem uma distribuição Gaussiana.

No esquema de encriptação baseado no problema Ring-LWE, a amostragem de ruídos ocorre na fase de encriptação, que comumente é implementada em um dispositivo vulnerável a ataques por canais laterais. Similarmente, como demonstrado por Bruinderink et al., o esquema de assinatura BLISS é suscetível a ataques por canais laterais, bem como o amostrador utilizado na fase de assinatura [Bruinderink et al. 2016]. Assim, a fim de evitar ataques por canais laterais de tempo, uma medida preventiva é a implementação com tempo de execução constante, que descorrelaciona a latência do algoritmo da informação que está sendo processada.

**Objetivos.** Em concordância com os fatores motivadores acima expostos, nosso objetivo aqui é o estudo e a implementação segura de métodos para amostragem Gaussiana de vetores de reticulados e de inteiros. Em particular, a implementação de algoritmos específicos para o esquema de encriptação baseado no Ring-LWE, para um esquema HIBE (*Hierarchical Identity-Based Encryption*) [Mochetti and Dahab 2014] e para reticulados NTRU [Hoffstein et al. 2010, Lyubashevsky and Prest 2015, Ducas and Prest 2015].

**Contribuições.** Neste trabalho, implementações com tempo constante dos algoritmos Knuth-Yao [Knuth and Yao 1976] e Ziggurat discreto [Buchmann et al. 2014] são propostas para a tarefa de amostragem de inteiros conforme uma distribuição Gaussiana. Por ser um método mais eficiente e mais propício a implementações resistentes a ataques por canais de tempo, uma implementação do método Knuth-Yao de propósito geral é aplicada ao contexto de amostragem Gaussiana de pontos de um reticulado. Ainda, este trabalho apresenta uma implementação para o Knuth-Yao específica para o esquema de encriptação baseado no problema Ring-LWE [Lyubashevsky et al. 2012], cuja distribuição de erros tem parâmetros fixos. Como resultado desta dissertação, resultados preliminares foram publicados no XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais [Ortiz et al. 2015a], e agraciado com o prêmio de terceiro melhor artigo, e no X Workshop de Teses, Dissertações e Trabalhos de Iniciação Científica do Instituto de Computação da Universidade Estadual de Campinas [Ortiz et al. 2015b].

## 2. Aspectos da Amostragem Gaussiana Discreta

A distribuição Gaussiana unidimensional sobre os inteiros com centro $c \in \mathbb{R}$ e desvio padrão $\sigma \in \mathbb{R}^+$, denotada por $\mathcal{D}_{\mathbb{Z},\sigma,c}$, é definida na Equação 1.

$$\mathcal{D}_{\mathbb{Z},\sigma,c}(x) = \frac{\rho_{\sigma,c}(x)}{\sum_{y=-\infty}^{\infty} \rho_{\sigma,c}(y)}, \text{ com } \rho_{\sigma,c}(x) := \frac{1}{\sigma\sqrt{2\pi}} \exp\left(\frac{-(x-c)^2}{2\sigma^2}\right) \tag{1}$$

Tendo em vista que o intervalo de amostragem definido na Equação 1 é infinito, algoritmos em máquinas finitas são capazes somente de amostrar elementos de distribuições

Gaussianas estatisticamente próximas da ideal. Neste sentido, as amostragens ocorrem no intervalo $[c - t\sigma, c + t\sigma] \cap \mathbb{Z}$, com $t$ o comprimento da cauda da distribuição. Portanto, a cauda da distribuição, ou seja, a área correspondente a $|x| > t\sigma$, é ignorada, relativamente a uma precisão $2^{-\lambda}$. Comumente, o corte de cauda empregado em primitivas criptográficas corresponde a $t = 13{,}2$, de forma que, para todo $\sigma \geq 1$, a massa correspondente à região da cauda é negligenciável, tal que

$$1 - \frac{S_\sigma(13, 2\sigma)}{S_\sigma(\infty)} < 2^{-128},$$

com $S_\sigma$ a função cumulativa $S_\sigma(b) = \sum_{k=-b+1}^{b-1} \rho_{\sigma,0}(k)$ para $b \geq 1$ [Saarinen 2016].

Em um esquema criptográfico, tanto os parâmetros da distribuição como a distância estatística são determinados por cálculos oriundos da demonstração de segurança do esquema. Habitualmente, a distância estatística carece de um valor inferior a $2^{-\lambda}$, com $\lambda$ o nível de segurança. Para tal, a implementação de um método de amostragem Gaussiana sobre os inteiros deve considerar precisão mínima de $\lambda$ bits para as operações com ponto flutuante. Ademais, a precisão em bits define a dimensão das tabelas de consulta, impactando nos custos espacial e temporal dos algoritmos. Assim, além de resistentes a ataques por canais laterais, tais implementações devem ser eficientes.

## 3. Resultados Experimentais

A Figura 1 é uma representação do escopo desta dissertação. Tendo em vista reticulados NTRU e um esquema HIBE [Mochetti and Dahab 2014], nossas contribuções consistem na implementação de métodos para a amostragem de pontos de um reticulado que, por sua vez, requerem um oráculo para amostragem de inteiros, assim como criptossistemas baseados no problema Ring-LWE. A amostragem em ambos os casos segue uma função Gaussiana. Nesta seção, todas as implementações estão em linguagem C++ e utilizam a biblioteca NTL [Shoup 2016] para geração de valores aleatórios e para operações com vetores e matrizes. Além disso, as implementações tem como alvo um processador Ivy Bridge Intel®Core™i5-3570 @ 3.40 GHz e 8 GB de memória física e de *swap*.

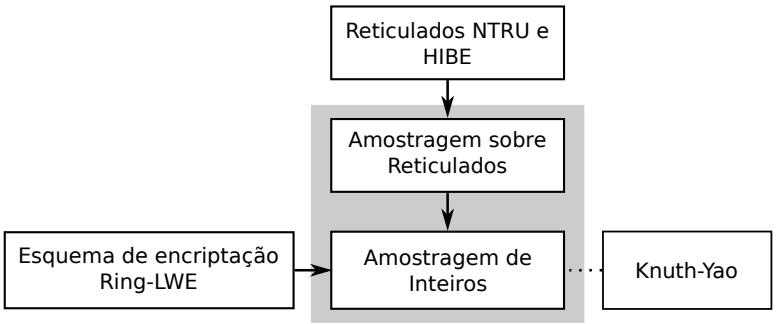


**Figura 1. Amostragem Gaussiana para esquemas sobre reticulados.**

Para a amostragem sobre os inteiros, com base em experimentos realizados com o algoritmo Knuth-Yao e o método discreto de Ziggurat, o método Knuth-Yao apresenta tempos de execução com uma ordem de magnitude menor do que os obtidos para o Ziggurat. Portanto, implementações com tempo constante para o Knuth-Yao foram propostas

para o esquema de encriptação baseado no problema Ring-LWE, bem como para métodos de amostragem de pontos de um reticulado. Implementações com tempo constante são resistentes a ataques por canais laterais de tempo, mas com tempos de execução superiores aos reportados em implementações com tempo variante. Tal acréscimo deve-se à necessidade de forçar a execução do algoritmo para o pior caso, bem como à inserção de novas instruções para que os caminhos de execução tenham todos o mesmo tamanho.

### 3.1. Esquema de Encriptação Ring-LWE

Para o esquema Ring-LWE, os parâmetros da distribuição Gaussiana são fixos, diferentemente de alguns métodos para amostragem sobre reticulados que requerem inteiros amostrados conforme uma função Gaussiana distinta a cada iteração. Neste sentido, tabelas de consulta podem ser calculadas e definidas estaticamente para acesso futuro na fase de amostragem.

De forma geral, o método Knuth-Yao consiste em processar uma matriz de probabilidades binária, que representa a parte negativa da distribuição Gaussiana. Assim, a matriz de probabilidades contém uma grande região nula “mais à esquerda"que permite o emprego de técnicas de compactação. Uma dessas técnicas é o armazenamento decimal das linhas da matriz binária. Além disso, a visitação de tais bits pode ser feita linha-a-linha em vez de bit-a-bit, uma vez que os pesos de Hamming das linhas da matriz são conhecidos. Nesta implementação, atribuições e desvios condicionais são substituídos por funções com tempo constante compostas de operadores aritméticos e lógicos.

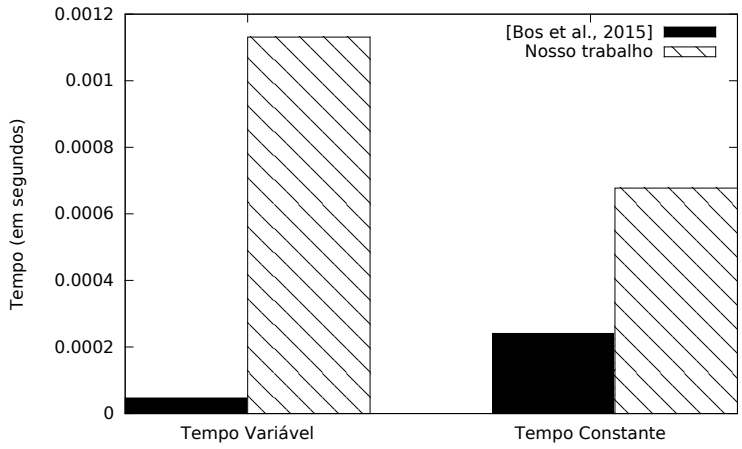


**Figura 2. Comparação entre métodos para amostragem Gaussiana de inteiros.**

Na literatura, Bos et al. apresentam um trabalho similar, onde uma implementação do método da transformação inversa é aplicada ao esquema assimétrico Ring-LWE [Lyubashevsky et al. 2012]. Na Figura 2, resultados em termos de tempo de execução, em segundos, são apresentados para a implementação do método da transformação inversa [Bos et al. 2015] e para o algoritmo Knuth-Yao. Em suma, nossa implementação com tempo constante é até quatro vezes menos eficiente que a implementação respectiva de Bos et al.. Apesar disso, nossa implementação requer menos bits para armazenamento das tabelas de consulta, uma diferença de 1852 bits quando $\sigma = 8/\sqrt{2\pi}$.

### 3.2. Amostragem Gaussiana sobre Reticulados

Para amostragem em reticulados, o esquema HIBE proposto por Mochetti e Dahab e reticulados NTRU são abordados. A base curta, que gera o reticulado $q$-ário do esquema HIBE [Mochetti and Dahab 2014], permite o uso de quatro algoritmos para amostragem Gaussiana: o amostrador Gaussiano usual, como apresentado em [Lyubashevsky and Prest 2015]; o método de Klein [Gentry et al. 2008], que produz vetores com normas menores e, portanto, melhores; o método de Peikert [Peikert 2010] que, em contraste com o custo quadrático do método de Klein, tem custo quase-linear apesar de produzir saídas piores; e o amostrador Gaussiano compacto [Lyubashevsky and Prest 2015], que requer somente uma fração da base de Gram-Schmidt presente na memória.

| | **Conjuntos de Parâmetros** $(n, m, q)$ | | | |
|---|---|---|---|---|
| **Algoritmo** | $(2, 12, 13)$ | $(4, 35, 11)$ | $(16, 111, 499)$ | $(64, 133, 1019)$ |
| AMOSTRADOR-GAUSSIANO | $0,06$ | $1,02$ | $51,81$ | $471,86$ |
| AG-COMPACTO | $0,05$ | $0,79$ | $53,81$ | $775,39$ |
| KLEIN | $0,06$ | $1,02$ | $44,11$ | $786,92$ |
| PEIKERT | $0,07$ | $0,73$ | $13,43$ | $86,27$ |

**Tabela 1. Tempos de execução em segundos para a fase de amostragem Gaussiana sobre reticulados para o esquema HIBE.**

A Tabela 1 apresenta resultados dos tempos de execução, em segundos, para a fase de amostragem de tais métodos. Neste caso, os conjuntos de parâmetros são fictícios. Um conjunto de parâmetros real com nível de segurança de $128$ bits é $(n, q) = (128, 2083)$ tal que $\mathbf{B} \in \mathbb{Z}^{mn \times mn}$ é uma base curta para o reticulado $\Lambda_q^{\perp}(\mathbf{B})$. Para o esquema HIBE, todos os métodos para amostragem de pontos de um reticulado possuem uma fase de pré-computação de forma a gerar e ortogonalizar ou inverter a base curta que gera o reticulado em questão. A ortogonalização é calculada utilizando o método usual de Gram-Schmidt. A fim de justificar tais escolhas de conjuntos de parâmetros, quando $(n, m, q) = (64, 133, 1019)$, o tempo despendido pelo algoritmo de Peikert na fase de pré-computação e na amostragem é de, aproximadamente, $42$ horas e requer cerca de $17{,}33$ GB de espaço em memória.

Por outro lado, para reticulados NTRU, a base $\mathbf{B}$ que gera o reticulado é composta por blocos de bases isométricas, tal que

$$\mathbf{B}_{f,g,F,G} = \left[\begin{array}{c|c} \mathcal{A}(f) & \mathcal{A}(g) \\ \hline \mathcal{A}(F) & \mathcal{A}(G) \end{array}\right],$$

sendo que para cada $p \in \mathbb{Z}_N[x]$, $\mathcal{A}(p)$ denota uma matriz $N \times N$ cuja $i$-ésima linha é dada pelos coeficientes de $x^{i-1}p(x) \mod (x^N + 1)$. Ainda, $q$ é um inteiro positivo e $f$, $g$, $F$, $G$ são polinômios no anel $\mathbb{Z}_N[x]$ tais que $fG - gF = q \mod (x^N + 1)$.

Neste caso, os métodos OGS-EM-BLOCOS [Lyubashevsky and Prest 2015] e AMOSTRADOR-HÍBRIDO [Ducas and Prest 2015] usufruem dessa estrutura da base curta a fim de computar eficientemente a ortogonalização de Gram-Schmidt e a amostragem de pontos do reticulado, respectivamente.

| | **Dimensão** $(N)$ | | | |
|---|---|---|---|---|
| **Algoritmo** | **128** | **256** | **512** | **1024** |
| GERAÇÃO-DE-CHAVES | $0,10$ | $0,44$ | $2,20$ | $11,02$ |
| OGS-EM-BLOCOS | $0,11$ | $0,45$ | $2,37$ | $7,43$ |
| PRÉ-COMPUTAÇÃO-KLEIN | $3,60$ | $17,15$ | $97,46$ | $505,39$ |
| PRÉ-COMPUTAÇÃO-PEIKERT | $3,19$ | $5,60$ | $20,94$ | $82,37$ |
| AMOSTRADOR-HÍBRIDO | $15,58$ | $72,38$ | $373,23$ | $2042,71$ |

**Tabela 2. Tempos de execução em segundos para o método híbrido com variação no valor de $N$.**

Na Tabela 2, a primeira amostragem sobre o reticulado NTRU tem a penalidade de todos os algoritmos, a saber GERAÇÃO-DE-CHAVES para geração da base do reticulado, OGS-EM-BLOCOS para sua ortogonalização, PRÉ-COMPUTAÇÃO-KLEIN e PRÉ-COMPUTAÇÃO-PEIKERT como fases preparatórias para a amostragem propriamente dita e, então, o AMOSTRADOR-HÍBRIDO. Nas amostragens seguintes, o único custo associado é o de execução do procedimento AMOSTRADOR-HÍBRIDO. Neste cenário, os conjuntos de parâmetros refletem os valores adotados na literatura e, no pior caso, quando $N = 1024$, a amostragem pode consumir cerca de $34$ minutos.

| **Dimensão** $(N)$ | **Knuth-Yao** | **Método Híbrido** | **Proporção** $(\%)$ |
|---|---|---|---|
| 128 | 0,0013 | 1564,60 | 0,0085 |
| 256 | 0,0021 | 7261,47 | 0,0029 |
| 512 | 0,0037 | 37446,08 | 0,0010 |
| 1024 | 0,0068 | 204856,22 | 0,0003 |

**Tabela 3. Proporção do tempo, em segundos, consumida pelo algoritmo Knuth-Yao no método híbrido.**

A Tabela 3 ilustra a proporção do tempo de execução do método híbrido consumida pela tarefa de amostragem Gaussiana sobre os inteiros. Neste experimento, o método híbrido [Ducas and Prest 2015] é executado cem vezes, uma vez que há diferença na latência para amostragem do primeiro vetor e para a amostragem dos seguintes. Além disso, a amostragem de cada vetor sobre o reticulado NTRU requer que um polinômio com dimensão $N$ seja gerado, tal que suas coordenadas são inteiros amostrados pelo algoritmo Knuth-Yao. Então, a proporção se torna ínfima com o crescimento do valor de $N$, posto que o tempo de execução do método híbrido cresce na proporção aproximada $5/2$ em relação ao crescimento da dimensão $N$.

Em ambos os casos, para reticulados NTRU e para o esquema HIBE, não há na literatura trabalhos similares que permitam uma comparação justa de desempenho. Apesar de serem passíveis de otimizações algorítmicas, os resultados para as implementações dos métodos de Klein e de Peikert, e para os métodos compacto e híbrido dão uma noção inicial da penalidade associada com a tarefa de amostragem Gaussiana sobre reticulados. O código-fonte de todas as implementações mencionadas pode ser encontrado em repositórios públicos no GitHub no endereço `https://github.com/jnortiz`.

## Referências

[Agrawal et al. 2010] Agrawal, S., Boneh, D., and Boyen, X. (2010). Efficient Lattice (H)IBE in the Standard Model. In Gilbert, H., editor, *Advances in Cryptology – EUROCRYPT 2010*, volume

6110 of *LNCS*, pages 553–572. Springer Berlin Heidelberg.

[Alkim et al. 2015] Alkim, E., Ducas, L., Pöppelmann, T., and Schwabe, P. (2015). Post-quantum key exchange - a new hope. Cryptology ePrint Archive, Report 2015/1092. `http://eprint.iacr.org/`.

[Boneh et al. 2014] Boneh, D., Gentry, C., Gorbunov, S., Halevi, S., Nikolaenko, V., Segev, G., Vaikuntanathan, V., and Vinayagamurthy, D. (2014). Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits. In Nguyen, P. and Oswald, E., editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 533–556. Springer Berlin Heidelberg.

[Boneh et al. 2011] Boneh, D., Sahai, A., and Waters, B. (2011). Functional Encryption: Definitions and Challenges. In Ishai, Y., editor, *Theory of Cryptography*, volume 6597 of *LNCS*, pages 253–273. Springer Berlin Heidelberg.

[Bos et al. 2015] Bos, J. W., Costello, C., Naehrig, M., and Stebila, D. (2015). Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem. In *Security and Privacy (SP), 2015 IEEE Symposium on*, pages 553–570.

[Bruinderink et al. 2016] Bruinderink, L. G., Hülsing, A., Lange, T., and Yarom, Y. (2016). Flush, Gauss, and Reload – A Cache Attack on the BLISS Lattice-Based Signature Scheme. Cryptology ePrint Archive, Report 2016/300. `http://eprint.iacr.org/`.

[Buchmann et al. 2014] Buchmann, J., Cabarcas, D., Göpfert, F., Hülsing, A., and Weiden, P. (2014). Discrete Ziggurat: A Time-Memory Trade-Off for Sampling from a Gaussian Distribution over the Integers. In Lange, T., Lauter, K., and Lisoněk, P., editors, *Selected Areas in Cryptography – SAC 2013*, volume 8282 of *LNCS*, pages 402–417. Springer Berlin Heidelberg.

[Ducas et al. 2013] Ducas, L., Durmus, A., Lepoint, T., and Lyubashevsky, V. (2013). *Advances in Cryptology – CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, chapter Lattice Signatures and Bimodal Gaussians, pages 40–56. Springer Berlin Heidelberg, Berlin, Heidelberg.

[Ducas and Prest 2015] Ducas, L. and Prest, T. (2015). A Hybrid Gaussian Sampler for Lattices over Rings. Cryptology ePrint Archive, Report 2015/660. `http://eprint.iacr.org/`.

[Gentry et al. 2008] Gentry, C., Peikert, C., and Vaikuntanathan, V. (2008). Trapdoors for Hard Lattices and New Cryptographic Constructions. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, pages 197–206, New York, NY, USA. ACM.

[Hoffstein et al. 2010] Hoffstein, J., Howgrave-Graham, N., Pipher, J., and Whyte, W. (2010). Practical Lattice-Based Cryptography: NTRUEncrypt and NTRUSign. In Nguyen, P. Q. and Vallée, B., editors, *The LLL Algorithm*, Information Security and Cryptography, pages 349–390. Springer Berlin Heidelberg.

[Hoffstein et al. 2014] Hoffstein, J., Pipher, J., Schanck, J. M., Silverman, J. H., and Whyte, W. (2014). *Applied Cryptography and Network Security: 12th International Conference, ACNS 2014, Lausanne, Switzerland, June 10-13, 2014. Proceedings*, chapter Practical Signatures from the Partial Fourier Recovery Problem, pages 476–493. Springer International Publishing, Cham.

[Knuth and Yao 1976] Knuth, D. and Yao, A. (1976). *Algorithms and Complexity: New Directions and Recent Results*, chapter The Complexity of Nonuniform Random Number Generation. Academic Press, New York, j. f. traub edition.

[Lyubashevsky et al. 2010] Lyubashevsky, V., Peikert, C., and Regev, O. (2010). On Ideal Lattices and Learning with Errors over Rings. In Gilbert, H., editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer Berlin Heidelberg.

[Lyubashevsky et al. 2012] Lyubashevsky, V., Peikert, C., and Regev, O. (2012). On Ideal Lattices and Learning with Errors Over Rings. Cryptology ePrint Archive, Report 2012/230. `http://eprint.iacr.org/`.

[Lyubashevsky and Prest 2015] Lyubashevsky, V. and Prest, T. (2015). Quadratic Time, Linear Space Algorithms for Gram-Schmidt Orthogonalization and Gaussian Sampling in Structured Lattices. Cryptology ePrint Archive, Report 2015/257. `http://eprint.iacr.org/`.

[Mochetti and Dahab 2014] Mochetti, K. and Dahab, R. (2014). Ideal Lattice-based (H)IBE Scheme. Technical Report IC-14-18, Institute of Computing, University of Campinas.

[O'Neill 2010] O'Neill, A. (2010). Definitional Issues in Functional Encryption. Cryptology ePrint Archive, Report 2010/556. `http://eprint.iacr.org/`.

[Ortiz et al. 2015a] Ortiz, J. N., Aranha, D. F., and Dahab, R. (2015a). Implementação em Tempo Constante de Amostragem de Gaussianas Discretas. In *XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, SBSeg 2015 (full papers)*, Florianópolis, SC.

[Ortiz et al. 2015b] Ortiz, J. N., Aranha, D. F., and Dahab, R. (2015b). Implementação em Tempo Constante de Amostragem de Gaussianas Discretas. In *X Workshop de Teses, Dissertações e Trabalhos de Iniciação Científica, WTD 2015*, Campinas, SP.

[Peikert 2010] Peikert, C. (2010). An Efficient and Parallel Gaussian Sampler for Lattices. In *Proceedings of the 30th Annual Conference on Advances in Cryptology*, CRYPTO'10, pages 80–97, Berlin, Heidelberg. Springer-Verlag.

[Regev 2005] Regev, O. (2005). On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC '05, pages 84–93, New York, NY, USA. ACM.

[Saarinen 2016] Saarinen, M.-J. O. (2016). Arithmetic Coding and Blinding for Lattice Cryptography. Cryptology ePrint Archive, Report 2016/276. `http://eprint.iacr.org/`.

[Shoup 2016] Shoup, V. (2016). Number Theory Library (NTL). Website. `http://www.shoup.net/ntl/` - Último acesso em 13 de julho de 2016.

[Stehlé and Steinfeld 2011] Stehlé, D. and Steinfeld, R. (2011). *Advances in Cryptology – EUROCRYPT 2011, Tallinn, Estonia, May 15-19, 2011. Proceedings*, chapter Making NTRU as Secure as Worst-Case Problems over Ideal Lattices, pages 27–47. Springer Berlin Heidelberg, Berlin, Heidelberg.