International Journal of Security and Its Applications
Vol.9, No.9 (2015), pp.45-54
http://dx.doi.org/10.14257/ijsia.2015.9.9.05

Design of a Robust Normal Distribution Sampler for Ring-Learning-With-Errors Cryptographic Scheme

Sangook Moon

Mokwon University, Daejeon, Korea
smoon@mokwon.ac.kr

Abstract

Due to the various characteristics from the pseudo random number generator or many kinds of deterministic devices such as arithmetic processing units, new principles and test schemes should be proposed for assessment of true random number generator. In this contribution, a novel viewpoint on designing a Normal distribution sampler applicable for implementing a homomorphic encryption system based on Ring-LWE crypto scheme is proposed. We suggest a Gaussian normal distribution sampler described with HDL to create uniformly distributed pseudo random numbers which will be used for generating non-symmetric key matrices and error matrices using an open-source AES cryptographic module. The implemented sampler can be conducted with high-speed clock frequency with its succinct critical delay paths as well.

Keywords: *Gaussian normal distribution sampler, lattice cryptography, security*

1. Introduction

With the upcoming visibility of spreading quantum computing algorithms in the near future, 3rd-generation cryptographic methods such as RSA, Elliptic curve cryptography (ECC) are in an unstable condition, which guarantee their cryptographic strength based on discrete logarithm problems or hard prime factorization [1-2] so that post-quantum cryptographic algorithms such as lattice cryptography have been drawing attention recently. Figure 1 shows why the cryptographic trend is changing from the 3rd generation cryptography to 4th.

The proof of security of lattice cryptography is based upon the shortest vector problem (SVP) and the closest vector problem (CVP). SVP and CVP leads to create the subset-sum problem, and then it succeed to the learning-with-errors (LWE) problem [3]. In 2013, C. Peikert and V. Lyubashevsky proposed the Ring-LWE, in which the key size are reduced to the complexity O(n) from O(n^2) [4].

The baseline of these proposals is the polynomial time algorithm which samples from a discrete Gaussian probability distribution over a lattice. With a vector $c \in R^n$, a width parameter s (>0), and a basis vector B, the sampling algorithm does not disclose any information about the input basis B since distribution D has been defined with no relationship to any specific basis vectors. This characteristic of zero-knowledge property explains the versatility in lattice based cryptography [5][6]. Ring-LWE cryptography uses polynomial multiplication with number theoretic transform (NTT) as its basic building block. In the present work, we use a modified Cooley-Tukey FFT algorithm to efficiently execute the polynomial multiplication to speed up lattice cryptographic applications and feed the parameters. This paper is an extended version of a work presented in a workshop [7].

ISSN: 1738-9976 IJSIA

2. The Ring-Learning-With-Errors Cryptosystem

We briefly introduce the basic clarification of the Ring-Learning-with-Errors (Ring-LWE) non-symmetric key cryptosystem.

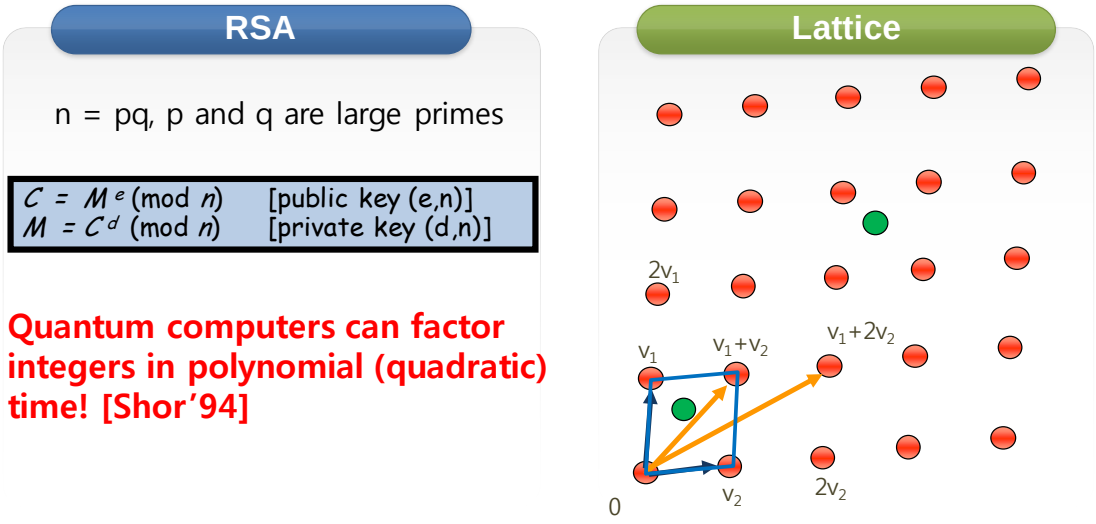

Figure 1. Why Lattice Cryptography is Chosen

2.1 Learning with Errors

Since the promoting result of Ajtai [8] who demonstrated a worst-case to average-case reduction among lattice problems, the theme of lattice based cryptography has been paid serious attention. It can be explained that the fundamental lattice problems are so highly adaptable that HIBE (hierarchical identity based encryption) or homomorphic encryption can be constructed [9]. Also it introduced some efficient non symmetric key encryption systems, digital signature, and hash functions as well [10]. An important benefit of these schemes is the fact that the quantum computing algorithms do not show superiority over the traditional cryptanalysis and that some of the schemes represent a proof of security which connects the hardness of breaking the crypto-scheme to the apparently intricate problem of dealing with a worst case lattice problem. This is a huge benefit to heuristic schemes such as NTRU (number theory R us) which is protected by patents [11]. Figure 2 represents how NTRU cryptosystem works [12].

However NTRU scheme showed vulnerability and the bit widths of the parameters grew larger against attacks. Consequently, while NTRU with bigger parameters are regarded as secure, the necessity of replacement cryptosystem has arisen.

The most serious critical problem of lattice based cryptography is the huge key sizes and subsequently inefficient vector calculation. This inefficiency brought out the idea of cyclic lattices which can be represented as $Z[x]/<f>$ for some primitive polynomial f of degree n. Many studies use the specific ring $R = Z_q[x]/<x^n + 1>$ for sufficient reasons [11].

Recently, the most well-known lattice based cryptography known as secure is the learning with errors (LWE) problem [13]. For the sake of attacking the decisional Ring-LWE problem, the attacker should determine if the samples $(a_1, b_1), \ldots, (a_m, b_m) \in R \times R$ in the ring $R = Z_q[x]/<x_n + 1>$ were picked uniformly random or if each coefficients of $b_i = a_i s + e_i$ with $s, e_1, \ldots, e_m$ from a normal distribution D_σ is very small. The distribution D_σ is called one dimensional discrete normal distribution on integer with standard deviation σ and 0 as the mean value. The probability that we

sample $x \in Z$ is $\rho_\sigma(x)/\rho_\sigma(Z)$ where $\rho_\sigma(x) = exp(-\frac{x^2}{2\sigma^2})$ and $\rho_\sigma(Z) = \sum_{k=-\infty}^{\infty} \rho_\sigma(k)$. Figure 3 shows how LWE crypto-scheme works. First we pick a random public key factor of a vector matrix A, which is defined in Z_q^{m*n} and then we select a secret key vector *s*, which is defined in Z_q^n. And then, we add an error factor of a vector *e*, which is defined in Z_q^m. When we unveil another public key factor of a vector by making $b = As + e$, *b* shows pseudo-randomness due to the characteristics of LWE.

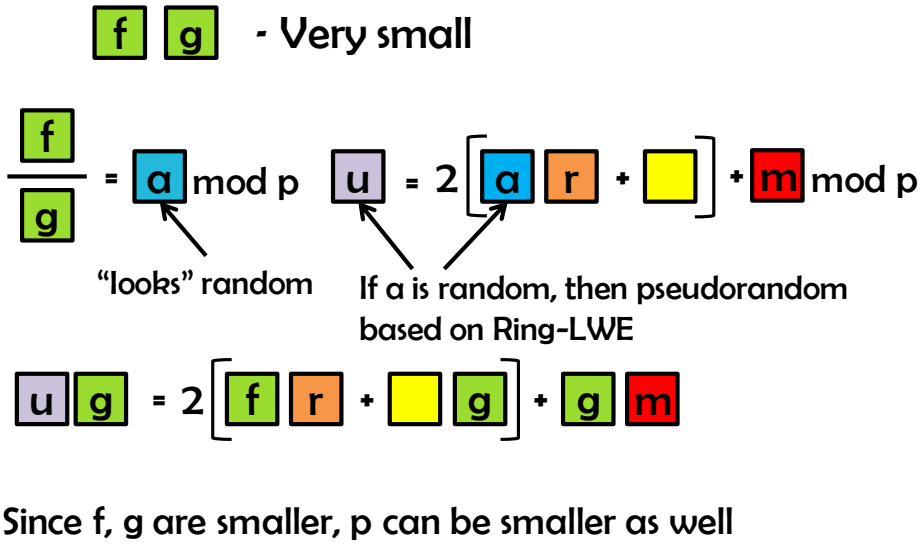

Figure 2. NTRU Cryptosystem

2.2 Ring-LWE

We can use the characteristics of the Ring-LWE problem to understand a reasonably reliable non-symmetric public key encryption method with a reduction to decisional Ring-LWE. The procedure and parameters were suggested by a few studies. Generate, encrypt, decrypt methods are described below, showing how the procedure work in Figure 4.

- *Generate* (*a*) : Pick *s*, $e \leftarrow D_\sigma$ and suppose $e = t - a*s \in R$.The public key is *t* and the secret key is *s* where *e* is just noise sample from Gaussian distribution and not required thereafter. We can designate the value of $a \in R$ as global constant or just taken uniformly random in this *generate* process.
- *Encrypt* (a, e, $m \in \{0,1\}^n$) : Pick the noise terms $e1, e2, e3 \leftarrow \in D_\sigma$. Suppose $\bar{m} = encode\ (m) \in R$, and outputs the encrypted text $c_1 = a \cdot e_1 + e_2, c_2 = t \cdot e_1 + e_3 + \bar{m} \in R^2$
- *Decrypt* ($c = [c_1, c_2], e$): Compute $decode\ (c_1 \cdot r_2 + c_2) \in \{0,1\}^n$

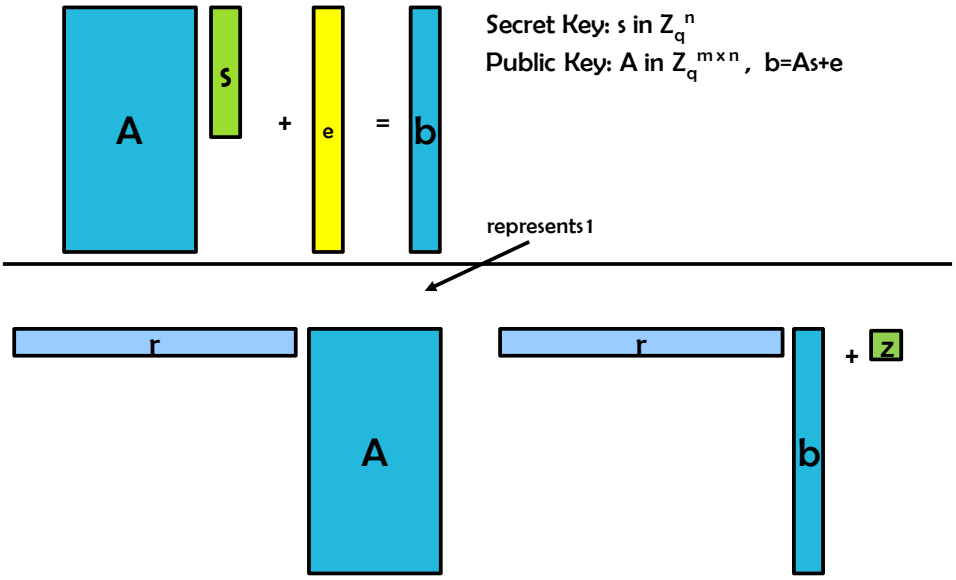

Figure 3. Public key encryption based on LWE

2.3 Security Presumption of Normal Sampling

$$R_q = Z_q[x] / < f > \quad (f(x) = x^n + 1, \quad q \equiv 1 \bmod 2n)$$
$$R_2 = Z_2[x] / < f > \quad (f(x) = x^n + 1)$$

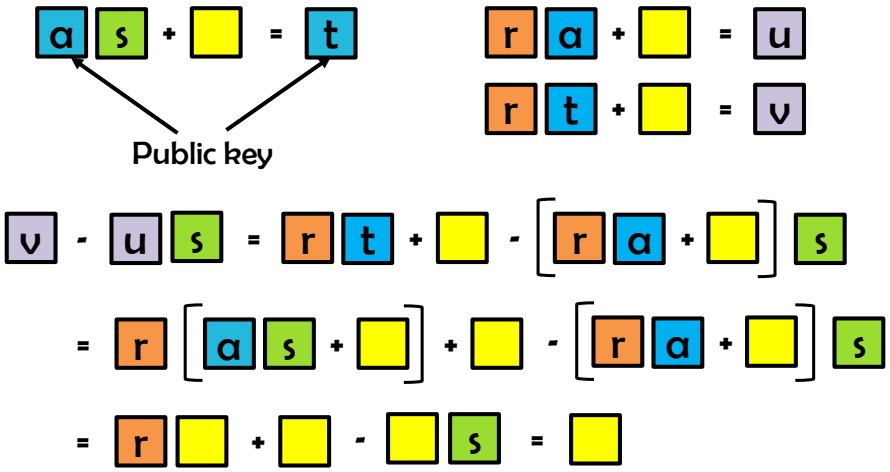

Figure 4. Ring-LWE Cryptosystem

It is general to limit the probability of both side's allowance of the Normal distribution for productivity and constructive reasons. For the bound of the tail, Peikert [6], who is one of the first to implement Ring-LWE cryptography suggested to confine the normal sampler from *upper* (-2*s*) to *upper* (+2*s*). However, they could not verify the proof of analysis for this specific period. Figure 5 shows how the Normal distribution transforms into uniform distribution according as the *s* increases. By experiment, the distribution shows a perfect uniform distribution when $s > 5m$.

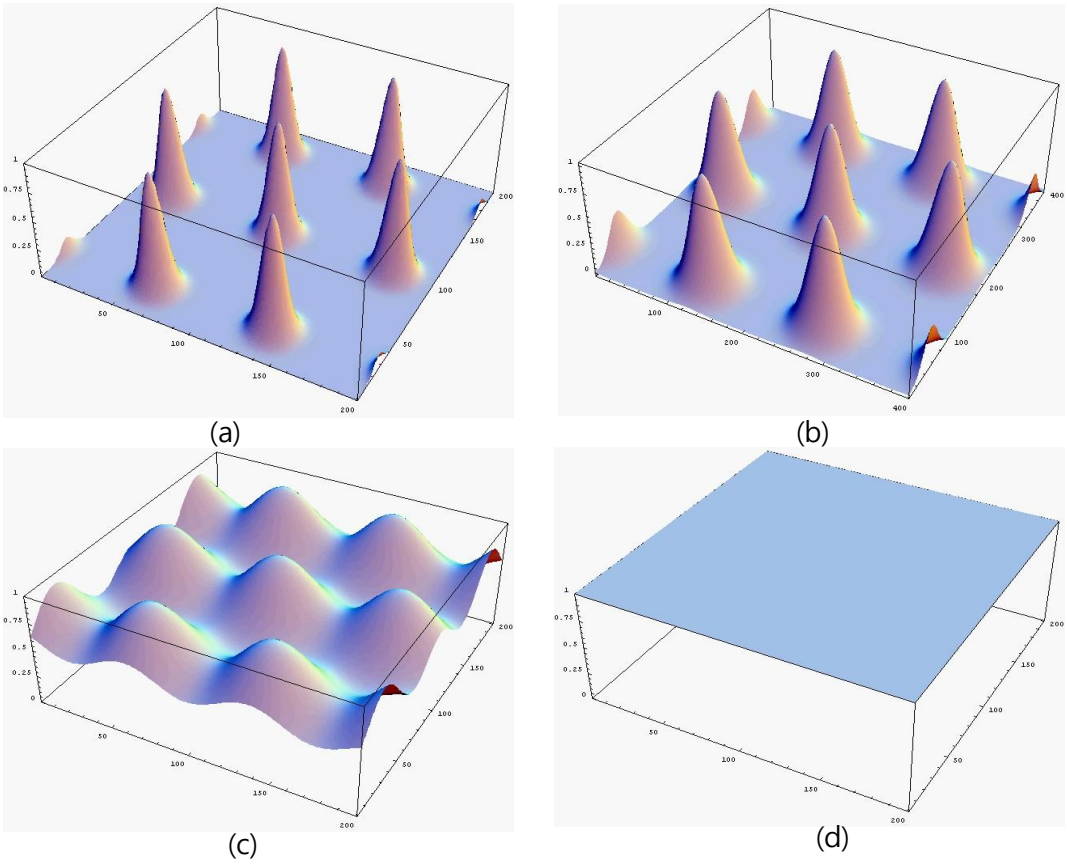

Figure 5. Normal Distribution Transforming into Uniform Distribution According as Standard Deviation Increases

3. Homomorphic Encryption Using Ring-LWE Encryption

Suppose we have a polynomial message $m \in R^2 = Z_2[x] < x^n + 1 >$ being transformed to a pair of encrypted polynomials $c \in R_q = Z_q[x] < x^n + 1 >$. The additive homomorphism can be obtained easily by coordinate based addition.

(Encrypt_Additive)

$c = (c_0, c_1)$ $\quad c_0 = a * s + 2 * e + m$

$\quad\quad\quad\quad\quad\quad c_1 = -a$

$$c_{add} = c + c' = (c_0 + c_0', c_1 + c_1')$$
$$= (a * s + 2 * e + m + a' * s + 2 * e' + m', -(a + a'))$$
$$= ((a + a') * s + 2 * (e + e') + m + m', -(a + a'))$$

(Decrypt_Additive)

With the encrypted message $c_{add} = (c_{add_0}, c_{add_1})$ $find\ c_{add_0} + c_{add_1} * s$

$$(a + a') * s + 2 * (e + e') + m + m' - (a + a') * s$$
$$= 2 * (e + e') + m + m' \cong m + m' (mod\ q)$$

(Encrypt_Multiplicative)

$c = (c_0, c_1)$ $\quad c_0 = a * s + 2 * e + m$

$\quad\quad\quad\quad\quad\quad c_1 = -a$

$c_{mul} = c * c' = (c_0 * c_0',\ c_0 * c_1' + c_0' * c_1,\ c_1 * c_1')$
$c_0{*}c_0' = (-a * a' * s^2 + (c_0 * a' + c_0' * a) * s$
$+2 * (2 * e * e' + e * m' + e' * m) + m * m'$
$c_1{*}c_1' = a * a$
$c_0{*}c_1' + c_0{*}c_1' = \cdots$

(**Decrypt_Multiplicative**)
With the encrypted message $c_{mul} = (c_{mul_0}, c_{mul_1}, c_{mul_2})$
$find\ c_{mul_0} + c_{mul_1} * s + c_{mul_2} * s^2$

$$c_{mul_0} + c_{mul_1} * s + c_{mul_2} * s^2 = (c_0 + c_1 * s) * (c_0' + c_1' * s) \cong m * m'\ (mod q)$$

4. Gaussians

The n-dimensional Gaussian operation $\rho : \mathbb{R}^n \to (0.1)$ is defined as

$$\rho(x) \triangleq exp(-\pi \cdot \|x\|^2) = exp(-\pi \cdot \langle x, x \rangle).$$

If we apply a nonsingular matrix B to obtain a linear transformation, we get the Gaussian operation

$$\rho B(x) \triangleq \rho(B^{-1}x) = exp(-\pi \cdot \langle B^{-1}x, B^{-1}x \rangle) = exp(-\pi \cdot x^t \sum^{-1} x)$$

where $\sum = BB^t > 0$. Since ρB can be discriminated only within $\sum$, we refer to it as $\rho_{\sqrt{\sum}}$ without losing generality.

Normalizing $\rho_{\sqrt{\sum}}$ by its whole area $\int \mathbb{R}^n \rho_{\sqrt{\sum}}(x)\, dx = \sqrt{det \sum}$ over $\mathbb{R}^n$, we acquire the Gaussian probability distribution function $D_{\sqrt{\sum}}$. It is simple to examine that a random variable x having distribution $D_{\sqrt{\sum}}$ can be mentioned as $\sqrt{\sum} \cdot z$, (z features spherical Gaussian distribution D_1) Thus, the random variable x has covariance as below.

$$\underset{x \sim D_{\sqrt{\sum}}}{E}[x, x^t] = \sqrt{\sum} \cdot \underset{z \sim D_1}{E}[z, z^t] \cdot \sqrt{\sum}^t = \sqrt{\sum} \cdot \frac{I}{2\pi} \cdot \sqrt{\sum} = \frac{\sum}{2\pi},$$

5. Gaussian on Lattices

Suppose $\Lambda \subset \mathbb{R}^n$ be a lattice, $c \in \mathbb{R}^n$, and suppose $\sum > 0$ be a symmetric matrix and $x^t \sum x > 0$ for all x which are not zeroes. The discrete Gaussian distribution $D_{\Lambda + c, \sqrt{\sum}}$ means that it sustains the coset $\Lambda + c$ within the Gaussian distribution $D_{\sqrt{\sum}}$. That indicates, for all $x \in \Lambda + c$, $D_{\Lambda + c, \sqrt{\sum}}(x) = \frac{\rho_{\sqrt{\sum}}(x)}{\rho_{\sqrt{\sum}}(\Lambda + c)} \propto \rho_{\sqrt{\sum}}(x)$.

Input: Probability matrix P, random number r, modulus q
Output: Sample value s

```
for col ← 0 to MAXCOL do
    d ← 2d + (r&1)
    r ← r ≫ 1
    for row ← MAXROW downto 0 do
        d ← d − P[row][col]
        if d = −1 then
            if (r&1) = 1 then
                return q − row
            else
                return row
return 0
```

Algorithm 1. Knuth-Yao Sampling Algorithm

The proposed Gaussian sampler seamlessly provides the parameters for the target Ring-LWE vector processor shown is Figure 6. There are a couple of memories in charge of dealing with instructions and data. We designed instructions specified for the target vector processor mostly dealing with single-instruction-multiple-data (SIMD). In the test prototype, there are four Ring-LWE processors at each vector slice. Since the bit-width scale is from kilo-bytes to mega-bytes, we need a sufficient data memory, which will be loaded to vector registers lanes. The ROM block stores the required parameters needed for number theoretic transform. There are four lanes of vector registers for vector pipelines, each with 1024/4=256 contents of 32-bit length registers. The background algorithm for implementing the Normal distribution sampling is adopted from Knuth-Yao [14].

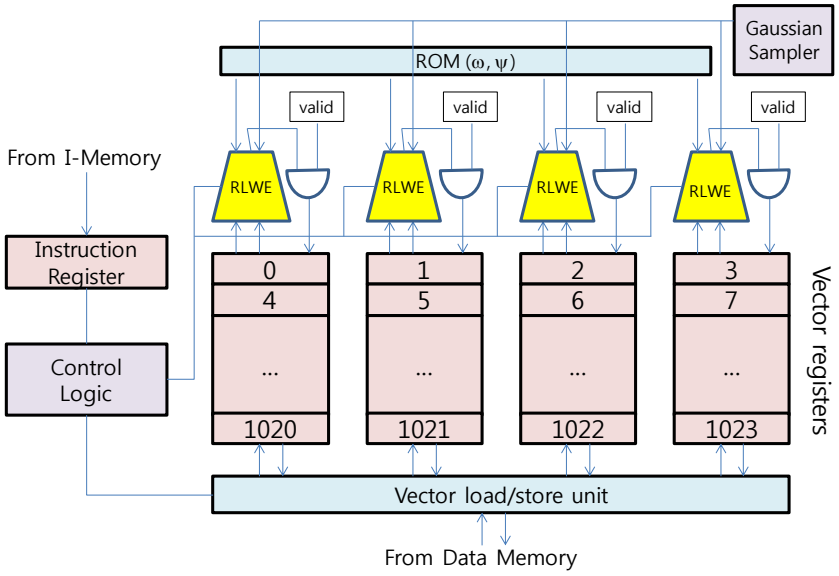

Figure 6. Target Ring-LWE Vector Processor

6. AES Block Cipher

AES (advanced encryption standard) enables both encrypting and decrypting using the same private key. This characteristic is a practical function when we intend to deliver data, but we should deal with limitations when we generate random numbers. One major factor must be considered. If an encryption algorithm holds a strong level of security, the

output bit stream with only one bit change in the input side will invert a tremendous number of bits showing uniformly distributed toggling ratio. To be sure, a strong level of homogeneity resides provided that the private key is kept secret. This characteristic is the point that we adopt the AES encryption algorithm as a random number generator. Figure 7 represents the encryption and decryption flow of AES cryptographic algorithm.

7. Conclusion

A new approach on designing a Gaussian sampler which is applicable to build a homomorphic encryption system based on Ring-LWE scheme is presented. Ring-LWE is an encryption scheme with small secret key size (O(n)) and small public key size (O(n)) as well Based on the hardness of subset-sum problems. In this work, we propose a Gaussian sampler designed with HDL to generate uniformly distributed pseudo-random numbers which will be used for public key vectors and error vectors using AES hardware implementation. The sampler can also be operated with high-speed clock frequency with its short critical delay path.

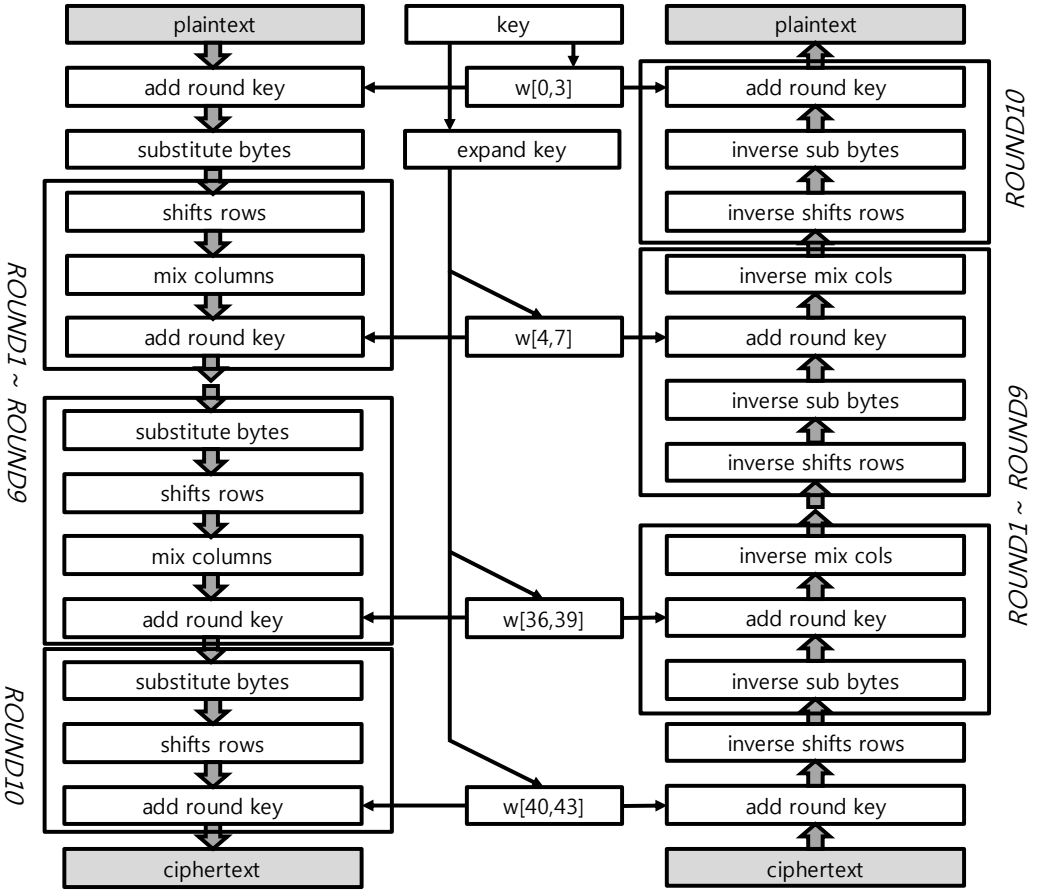

Figure 7. AES Algorithm Encryption and Decryption Flow

Acknowledgments

This research is supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2014R1A1A2A16053925)

References

[1] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits. Physical Review Letters, vol. 99, no. 25, **(2007).**
[2] E. Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O'Malley, D. Sank, A. Vainsencher, J. Wenner, T. White, Y. Yin, A. N. Cleland and John M. Martinis, "Computing prime factors with a Josephson phase qubit quantum processor", Nature Physics, vol. 8, **(2012),** pp. 719-723.
[3] V. Lyubashevsky, C. Peikert and O. Regev, "On ideal lattices and learning with errors over rings", Eurocrypt 2010, Lecture Notes in Computer Science, vol. 6110, **(2010),** pp. 1-23.
[4] V. Lyubashevsky, C. Peikert and O. Regev, "A toolkit for Ring-LWE cryptography", 2013, Lecture Notes in Computer Science, vol. 7881, **(2013),** pp. 35-54.
[5] C. Peikert, "An efficient and parallel Gaussian sampler for lattices", CRYPTO'10, **(2010)** August 15-19; Santa Barbara, California, USA.
[6] C. Gentry Peikert and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions", STOC 2008, **(2008)** May 17-20; Victoria(BC), Canada
[7] S. Moon, "A Gaussian sampler for Ring-LWE scheme reusing a cryptographic module", Advanced Science and Technology Letters, 109 (Security, Reliability and Safety 2015), **(2015),** pp. 5-9.
[8] M. Ajtai, "Generating hard instances of lattice problems", In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, **(1996)** May 22-24; Philadelphia, PA, USA
[9] S. Agrawal, D. Boneh and X. Boyen, "E_cient lattice (H)IBE in the standard model", In Henri Gilbert, editor, EUROCRYPT, volume 6110 of Lecture Notes in Computer Science, pp. 553-572, Springer, **(2010)**.
[10] Towards Practical Lattice-Based Public-Key Encryption on Reconfigurable Hardware Thomas Poppelmann and Tim Guneysu Horst Gortz Institute for IT-Security, Ruhr University Bochum, Germany, DEC, **(2014)**
[11] J. Ho_stein, J. Pipher, and J. Silverman, "NTRU: A ring-based public key cryptosystem", Algorithmic number theory, **(1998),** pp. 267-288.
[12] 2nd Bar-Ilan Winter School on Cryptography "Efficient Constructions", Vadim Lyubashevsky, Lattice-Based Cryptography and Applications , **(2012),** February 19-22.
[13] Z. Brakerski, A. Langlois, C. Peikert, O. Regev and D. Stehl_e, "Classical hardness of learning with errors", In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, STOC, **(2013),** pp. 575-584, ACM.
[14] D. E. Knuth and A. C. Yao, "The complexity of non-uniform random number generation", Algorithms and complexity: new directions and recent results, (**1976**), pp. 357-428.

Author

Sangook Moon, He received his Bachelor's degree, the Master's degree, and the Ph.D. degree in electronic engineering from Yonsei University, Seoul, Korea in 1995, 1997, and 2002, respectively. From 2002 to 2004, he was with Hynix Semiconductor, Seoul, Korea, where he developed Bluetooth baseband SoCs. Since 2004 he has been with the Department of Electronic Engineering at Mokwon University, Daejeon, Korea, where he currently serves as an Associate Professor. His research interests include computer architecture, embedded systems, SoCs, data encryption, and computer arithmetic.