ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 22-04-30
j.inst.Korean.electr.electron.eng.Vol.26,No.4,736~741,December 2022
https://doi.org/10.7471/ikeee.2022.26.4.736
213

R-LWE 암호화를 위한 근사 모듈식 다항식 곱셈기 최적화

Optimization of Approximate Modular Multiplier for R-LWE Cryptosystem

이 재 우*, 김 영 민*★

Jae-Woo Lee*, Youngmin Kim*★

Abstract

Lattice-based cryptography is the most practical post-quantum cryptography because it enjoys strong worst-case security, relatively efficient implementation, and simplicity. Ring learning with errors (R-LWE) is a public key encryption (PKE) method of lattice-based encryption (LBC), and the most important operation of R-LWE is the modular polynomial multiplication of rings. This paper proposes a method for optimizing modular multipliers based on approximate computing (AC) technology, targeting the medium-security parameter set of the R-LWE cryptosystem. First, as a simple way to implement complex logic, LUT is used to omit some of the approximate multiplication operations, and the 2's complement method is used to calculate the number of bits whose value is 1 when converting the value of the input data to binary. We propose a total of two methods to reduce the number of required adders by minimizing them. The proposed LUT-based modular multiplier reduced both speed and area by 9% compared to the existing R-LWE modular multiplier, and the modular multiplier using the 2's complement method reduced the area by 40% and improved the speed by 2%. appear. Finally, the area of the optimized modular multiplier with both of these methods applied was reduced by up to 43% compared to the previous one, and the speed was reduced by up to 10%.

요 약

격자 기반 암호화는 최악의 경우를 기반으로 한 강력한 보안, 비교적 효율적인 구현 및 단순성을 누리기 때문에 포스트 양자 암호화 방식 중 가장 실용적인 방식이다. 오류가 있는 링 학습(R-LWE)은 격자 기반 암호화(LBC)의 공개키암호화(Public Key Encryption: PKE) 방식이며, R-LWE의 가장 중요한 연산은 링의 모듈러 다항식 곱셈이다. 본 논문은 R-LWE 암호 시스템의 중간 보안 수준의 매개 변수 집합을 대상으로 하여 근사 컴퓨팅(Approximate Computing: AC) 기술을 기반으로 한 모듈러 곱셈기를 최적화하는 방법을 제안한다. 먼저 복잡한 로직을 간단하게 구현하는 방법으로 LUT을 사용하여 근사 곱셈 연산 중 일부의 연산 과정을 생략하고, 2의 보수 방법을 활용하여 입력 데이터의 값을 이진수로 변환 시 값이 1인 비트의 개수를 최소화하여 필요한 덧셈기의 개수를 절감하는 총 두 가지 방법을 제안한다. 제안된 LUT 기반의 모듈식 곱셈기는 기존 R-LWE 모듈식 곱셈기 대비 속도와 면적 모두 9%까지 줄어들었고, 2의 보수 방법을 적용한 모듈식 곱셈기는 면적을 40%까지 줄이고 속도는 2% 향상되는 것으로 나타났다. 마지막으로 이 두 방법을 모두 적용한 최적화된 모듈식 곱셈기의 면적은 기존대비 43%까지 감소하고 속도는 10%까지 감소하는 것으로 나타났다.

Key words : Approximate Computing(AC), Lattice-Based Cryptography(LBC), Ring-Learning With Errors(R-LWE), Polynomial multiplication, FPGA.

* School of Electronic & Electrical Eng. Hongik University
★ Corresponding author
E-mail : youngmin@hongik.ac.kr, Tel : +82-2-320-1665

※ Acknowledgment
This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2022-RS-2022-00156225) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation). This research was supported by the Basic Science Research Program, through the National Research Foundation of Korea (NRF), funded by the Ministry of Education(NRF-2020R1F1A1055251). The EDA tool was supported by the IC Design Education Center(IDEC), Korea.
Manuscript received Dec. 13, 2022; revised Dec. 20, 2022; accepted Dec. 27, 2022.

Ⅰ. 서론

양자 컴퓨터에 대한 개발이 활발히 진행되면서, 기존에 사용되던 RSA, DSA 등과 같은 공개키 암호(PKC) 시스템의 안전성에 대한 문제가 제기되고 있다[1-2].

포스트 양자 암호 기법의 하나인 격자 기반 암호화(LBC) 방식은 양자 컴퓨터 공격에 대응할 수 있는 가장 유망한 대안 중 하나로 알려져 있다[2-4]. LBC의 한 종류인 R-LWE(Ring Learning with Errors)은 어려운 격자 문제를 기반으로 광범위하게 조사되며 다항식 링에서의 모듈식 다항식 곱셈이 가장 큰 비중을 차지하며 매우 방대한 양의 연산을 필요로 한다. 따라서 R-LWE 암호화 시스템의 저전력 및 면적 효율적인 모듈식 다항식 곱셈기의 구현은 IOT 장치와 모바일 기기와 같은 크기와 자원이 제한된 애플리케이션에서 매우 중요하다[5-11].

본 논문은 모듈식 다항식 곱셈기를 최적화시키는 두 가지 방법을 제안한다. 첫 번째로는 입력 데이터를 이진수로 표현할 시 1의 개수가 적을수록 곱셈 연산에 효율적이기 때문에 1의 개수를 최소화하여 덧셈기를 적층시켜 곱셈 연산을 수행하는 방법을 제안한다. 두 번째로는 [12]의 모듈식 연산 곱셈기의 특정 구조인 곱셈 연산에서 사용되는 입력 데이터의 특정 범위에 따라 하나의 동일한 결과값을 갖는다는 점을 기반으로 LUT 기반의 모듈식 다항식 곱셈기로 최적화하는 방법을 제안한다. [12]의 모듈식 다항식 곱셈기에 본 논문이 제안하는 방법을 적용한 곱셈기를 Verilog HDL로 설계하고 Vivado 2021.1을 사용해 Artix-7 패밀리를 Target으로 하여 합성을 수행한다. 기존의 곱셈기[12]와의 성능을 각각 비교하였고, 제안하는 두 방법을 모두 적용한 모듈식 다항식 곱셈기의 성능 또한 알아보았다.

마지막으로, 제안하는 최적화 방법을 ASIC에도 적용해보기 위해 같은 회로를 Yosys 논리 합성 툴을 사용하여 합성 후 성능을 관찰하였다.

Ⅱ. 본론

1. AxMM(Approximate modular mulipiler)

LBC 방식 중 하나인 R-LWE 암호화 시스템은 링에 대한 다항식 곱셈 연산을 가장 중요시한다. 일반적으로 링 $Zq[x]/(n\times x+1)$을 사용하는데 여기서 n은 격자 차원을 나타내며 정수 2의 거듭제곱이고 q는 소수이다[9]. 또한, 각 요소는 차수가 n보다 작고, 계수는 q보다 작은 음이 아닌 정수이다. [12]의 다항식 곱셈은 SchoolBook

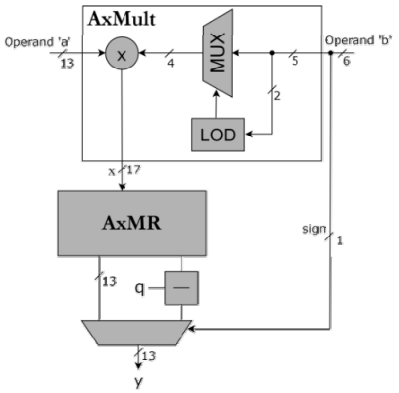


Fig. 1. The hardware design of approximate modular multiplier.
그림 1. 근사화 모듈식 곱셈기의 하드웨어 설계도

다항식 곱셈 알고리즘을 사용하여 입력 데이터를 곱하고, 모듈러 감소(Modular Reduction) 연산은 Barrett의 감소 알고리즘[14]을 q에 대하여 사용하여 모듈식 연산을 수행한다[10-14]. 그리고 입력 데이터는 중간 보안 수준의 R-LWE 매개변수 집합(n=256, q=7681, σ=4.51)[15]을 기반으로 한 가우시안 잡음 분포에서 샘플링이 되면서 다항식 곱셈을 위한 기존의 13비트 입력 데이터는 6비트(1개의 부호비트, 5개의 데이터비트)로 변환된다[11]. 따라서 13×13비트 근사 컴퓨팅 기반의 모듈식 다항식 곱셈기는 13×13비트의 부호 없는 표현 대신 1개의 부호 비트와 5개의 데이터 비트가 입력 데이터를 나타내기에 충분하다[11-12]. 따라서 그림 1과 같이 부호비트를 제외한 13×5비트 곱셈기로 대체할 수 있다[11-12].

그림 1에서 AxMult 블록의 LOD(Leading One Detector)는 입력 데이터[4:3]에서의 비트 '1'의 위치를 파악하여 한 비트의 절단을 수행한다. LOD의 출력 데이터가 1이면 b[4:1]를, 0이면 b[3:0]가 선택되어 Mux에서 출력된다. b[5]는 부호 비트로 마지막 연산에서 부호를 결정하는 데 사용된다.

AxMR 블록에서는 Barrett의 MR 알고리즘을 적용하여 모듈러 감소 연산을 수행한다. 본 논문은 그림 1의 AxMult 블록 부분에 대한 최적화 설계에만 집중한다.

2. 2's Complement Data Representation

곱셈기는 덧셈기를 이진수로 변환 시 1비트의 위치에 배치 후 적층하여 설계를 할 수 있는데 본 논문에서 제안하는 방법은 이와 유사하다. 그림 1의 AxMult에서 실질적인 곱셈은 13비트 a와 LOD를 통한 Mux 연산 후 선택된 Bit Length가 4인 b로 수행된다. 이때의 b를 b′

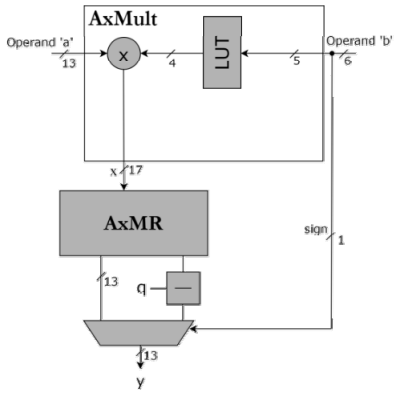


Fig. 2. The approximate modular multiplier proposed as LUT-based Method.
그림 2. LUT 기반의 방법으로 제안된 근사화 모듈식 곱셈기

이라고 가정한다. 본 논문이 제안하는 첫 번째 최적화 방법은 N 비트의 임의의 입력 데이터를 이진수로 표현했을 때, 1의 개수를 n이라 하고 $\frac{N}{2}$인 경우엔 2의 보수를 취하는 방법이다. 이 회로에서의 N은 4이므로 $2 < n$일 때 b′에 대하여 2의 보수를 취한다. 이 결과 $2 \geq n'$이라면 b를 제외한 다른 피연산자 a를 왼쪽으로 4비트 시프트(Shift) 연산 후 n'개의 뺄셈기를 해당 비트 위치에 설계한다. 여기서 n'은 b′를 2의 보수로 변환 후의 1의 개수이다.

하지만, 반대로 2의 보수를 취하였는데 $2 < n'$이라면 비트 내의 n을 줄일 수 없다는 의미기 때문에 기존의 b′를 n-1개의 덧셈기를 적층하여 설계한다.

예를 들어, b′의 값이 $1111_{(2)}$일 때는 위의 조건을 충족시키기 때문에 2의 보수로 변환하면 $0001_{(2)}$이 된다. 따라서 1개의 뺄셈기를 해당 비트 위치에 설계하여 곱셈기를 구현한다. 이처럼 위 조건을 충족시킨다면 2의 보수 방법을 적용하고, 그렇지 않다면 n-1개의 덧셈기를 적층하여 곱셈기를 구현한다.

3. LUT based Operand Manipulation

본 논문에서 제안하는 두 번째 방법은 LUT 추가이다. 5비트인 b에 대하여 AxMult의 LOD와 Mux 대신 총 32가지의 경우로 분류된 LUT로 대체하여 연산량을 줄일 수 있다. 이에 더불어, b의 Bit Length와 그림 1의 AxMult 블록에서 같은 규칙의 비트 형태를 보이는 b′의 구조를 통해 16가지 경우의 LUT로 감소시킬 수 있다. 자세한 설명은 다음과 같다.

우선, 그림 1의 AxMult 블록의 입력 데이터 b는 Mux에서 LOD의 출력이 1이면 b[4:1]를 0이면 b[3:0]가 선택된다. 여기서 Bit Length가 5에서 4로 감소하면서 값이 변환된다. 이때 특정 범위에서의 b 값이 입력되면 하나의 같은 결괏값을 갖는 구조가 되는데 이를 표 1로 정리하였다.

Table 1. Bit position of input data with the same result.
표 1. 결과값이 동일한 입력 데이터의 규칙

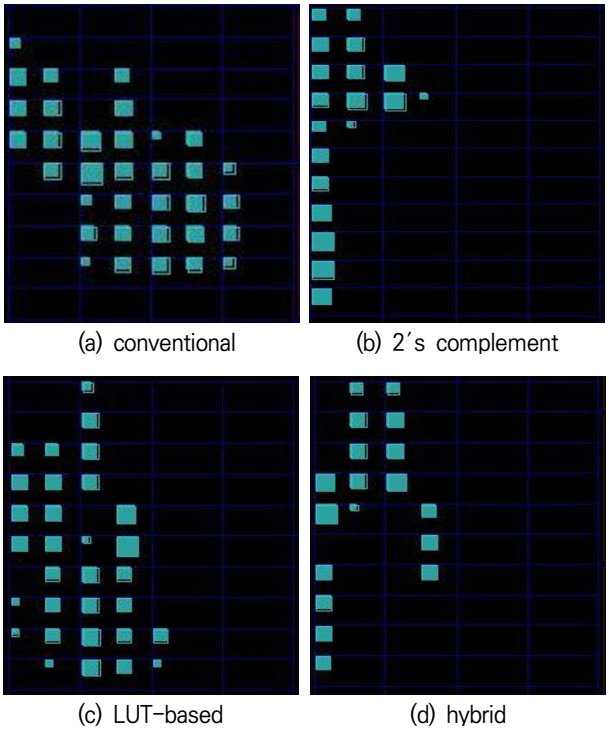
Input		Output
$1\_000x_{(2)}$	$1000_{(2)}$	$1000_{(2)}$
$1\_001x_{(2)}$	$1001_{(2)}$	$1001_{(2)}$
$1\_010x_{(2)}$	$1010_{(2)}$	$1010_{(2)}$
$1\_011x_{(2)}$	$1011_{(2)}$	$1011_{(2)}$
$1\_100x_{(2)}$	$1100_{(2)}$	$1100_{(2)}$
$1\_101x_{(2)}$	$1101_{(2)}$	$1101_{(2)}$
$1\_110x_{(2)}$	$1110_{(2)}$	$1110_{(2)}$
$1\_111x_{(2)}$	$1111_{(2)}$	$1111_{(2)}$

예를 들어, b의 값이 $1_000x_{(2)}$일 경우 Mux 연산 때문에 결과는 $1000_{(2)}$으로 같은 값이 출력된다 (여기서 x는 0 혹은 1이다). 이는 b의 값이 $1000_{(2)}$으로 입력될 때와도 같은 결괏값을 도출하는데 결국, 세 가지 경우의 입력 데이터가 하나의 동일한 값을 결괏값으로 갖게 된다. 이를 중점으로 제안된 방법은 5비트인 b에 대하여 총 AxMult의 LOD와 Mux 연산을 수행하지 않고 표 1의 총 16가지 경우의 LUT를 삽입하면서 Propagation Delay와 Logic Area를 감소시킨다. 아래의 그림 2는 본 방법을 적용한 근사화 모듈러 곱셈기의 회로도이다.

Ⅲ. 실험 및 결과

본 논문에서 제안하는 방법을 적용한 모든 근사 모듈식 다항식 곱셈기는 Verilog HDL을 이용해 설계하였으며, Xilinx 사의 Artix-7(xc7a25tcsg325-3) FPGA에 Vivado 2020.1 합성툴을 사용하여 논리 합성을 수행하였다.

우선, AC 회로가 포함된 그림 1의 A×MR 블록을 제외한 AxMult 블록에 집중하여 연구를 수행하였기 때문에 AC의 Relative error는 11.69%로 기존 모듈식 곱셈기와 Ⅱ.2절과 Ⅱ.3절에서 제안하는 방법을 적용한 모델에서 같다. 제안하는 방법을 적용한 곱셈기의 성능을 비교하기 위해 본 방법들을 적용하지 않은 일반적인 곱셈기를 사용한 [12]의 AxMM 논리 합성을 진행하였다. 그리고 Ⅱ.2와 Ⅱ.3절의 방법을 각각 적용하여 설계한 곱셈



(a) conventional (b) 2's complement

(c) LUT-based (d) hybrid

Fig. 3. Comparison of LUT assignment results for existing modular (a) and modular multiplier with two optimization methods in Artix-7 FPGA device (b-d).

그림 3. FPGA Artix-7 장치에서 두 가지 최적화 방법을 적용한 (b-d)와 기존 모듈식 곱셈기에 대한 LUT 할당 결과 비교

기, 마지막으로, 두 개의 방법을 모두 적용하여 설계한 Hybird 방식의 근사 모듈식 다항식 곱셈기의 논리 합성 결과를 각각 순서대로 표 2에 정리하였다.

그 결과, 방법 II.2를 적용하여 설계한 곱셈기는 범용성 곱셈기를 기반으로 한 근사 모듈식 다항식 곱셈기의 LUT 개수 대비 평균적으로 40% 정도까지 감소하여 우수한 결과를 나타냈다. 하지만 신호 전달 지연은 감소하지 않고 2% 정도 증가하는 것으로 보아 II.2절의 방법은 하드웨어의 면적 제한적인 경우에 매우 적합할 것으로 생각된다.

II.3의 방법을 적용한 곱셈기는 기존의 근사 모듈식 다항식 곱셈기[12] 대비 9%까지 LUT의 개수가 감소하였고, 신호 전달 지연 또한 9%까지 감소하였다. 하드웨어의 면적 면에서 II.2을 적용한 곱셈기와 성능을 비교하였을 때 개선 폭이 크진 않은 결과를 보였지만, 신호 전달 지연 면에서는 우수한 결과로 하드웨어의 속도가 중요한 경우라면 II.3절의 방법이 더 우수하다 판단된다.

마지막으로 hybrid 방식으로 설계한 곱셈기는 기존 곱셈기 대비 평균적으로 42%까지 LUT의 개수가 감소하였고, 신호 전달 지연 또한 33% 감소하면서, 각각의 방법을 적용하여 설계하였을 때보다 감소 폭이 큰 것을 관찰할 수 있었다.

그림 3은 Artix-7 FPGA 내의 Map Layout으로 (a)~(d)는 비율이 같으며 SLICEL와 LUT가 차지하는 Logic area이다. (b)와 (c)는 2의 보수 방법과 II.3절의 방법 각각을 적용하였을 때이며, (d)는 hybrid 모듈식 다항식 곱셈기로 기존의 모델(a)와 비교하여 하드웨어 면적이 감소하는 것을 쉽게 확인할 수 있다.

FPGA뿐만 아니라 ASIC로도 구현하였는데, 동일한 근사 모듈식 다항식 곱셈기를 Yosys라는 합성 툴을 사용하여 TSMC 0.18um Standard Cell Library로 합성을 진행하였다.

마찬가지로, II.2절과 II.3절의 방법으로 설계된 곱셈기 그리고 hybrid 방식의 근사 모듈식 다항식 곱셈기를 기존 모델[12]과 비교한 결과를 표 3에 정리하였다.

II.2절의 방법을 적용한 모델은 기존의 모델[12] 대비 Logic Area가 평균적으로 30%까지 감소하였고, 신호 전달 지연 또한 14%까지 감소하였다. 이는 하드웨어의 면적뿐만 아니라 신호 전달 지연까지 감소하여 ASIC로 합성 시 시간적인 부분까지 이점이 있다는 것을 확인할 수 있었다. II.3절의 방법을 적용한 모델 또한 기존의 모델 대비 Logic Area가 평균적으로 5%까지 감소하였고, 신호 전달 지연은 0.3%가 증가하는 것으로 나타났다. 신

Table 2. Result of proposed modular multiplier in FPGA.

표 2. FPGA에서의 제안된 모듈식 곱셈기 결과값

Approximate Modular Multiplier	Average				Minimum			
	Area		Delay		Area		Delay	
	# of LUT	normalized	ns	normalized	# of LUT	normalized	ns	normalized
Conventional	112	1	14.59	1	112	1	14.59	1
2's complement	68	0.60	14.92	1.02	62	0.55	12.19	0.83
LUT-based	103	0.91	13.54	0.92	103	0.91	13.54	0.92
Hybrid	**65**	**0.58**	**9.82**	**0.67**	**62**	**0.55**	**8.71**	**0.59**

Table 3. The result of modules synthesized with TSMC 0.18um standard cells.
표 3. TSMC 0.18um 표준 셀로 모듈을 합성한 결과

Approximate Modular Multiplier	Average				Minimum				NAND2X1 equivalent	
	Area		Delay		Area		Delay			
	μm^2	norm.	ns	norm.	μm^2	norm.	ns	norm.	EA	norm.
Conventional	15164	1.00	7.34	1.00	15164	1.00	7.34	1.00	82	1.00
2's complement	11016	0.70	6.32	0.86	8725	0.55	5.08	0.69	58	0.70
LUT-based	14988	0.95	7.36	1.003	14988	0.95	7.36	1.003	76	0.92
Hybrid	**11002**	**0.70**	**6.02**	**0.82**	**8090**	**0.52**	**4.72**	**0.64**	**56**	**0.68**

호 전달 지연 면에서 FPGA로 합성 시와는 상반되는 결과를 보였다. 마지막으로 hybrid 방식의 모델은 기존 모델 대비 Logic Area는 30%, 신호 전달 지연은 18%까지 감소하며 II.2, II.3절의 방법 각각을 적용하였을 때와 비교하여 가장 높은 성능을 나타냈다.

Ⅳ. 결론

이를 통해, 본 논문에서 제안하는 두 가지 방법들을 적용한 근사 모듈식 다항식 곱셈기를 FPGA뿐만 아니라 ASIC에서도 효율적으로 구현할 수 있음을 파악할 수 있었다.

격자 기반 암호화 방식 중 하나인 R-LWE은 모듈식 다항식 곱셈이 주 연산으로 많은 양의 연산이 요구된다. 따라서 최근 근사 컴퓨팅 기술과 결합한 근사 모듈식 곱셈기에 관한 연구가 활발히 진행되는데 본 논문은 근사 모듈식 곱셈기에 대한 두 가지의 하드웨어 면적 및 전력 효율적인 최적화 방법을 제안한다.

제안된 방법을 적용하여 설계된 근사 모듈식 곱셈기는 기존의 곱셈기 대비 LUT 소요 개수를 최대 45%까지 감소시켰고, 신호 전달 지연은 17%까지 FPGA Artix-7 모델에서 감소시켰다. 또한 FPGA뿐만 아니라 ASIC 0.18 Standard cell library를 사용하여 논리 합성을 수행하였는데 Hybrid 방식의 근사 모듈식 곱셈기에서 하드웨어 면적은 최대 48%까지 감소시켰고, 신호 전달 지연은 36%까지 감소시켰다. 향후 연산량 및 면적 효율적인 근사 모듈식 곱셈기에 관한 연구는 활발히 수행될 것으로 생각된다.

References

[1] Mavroeidis, Vasileios, et al., "The impact of quantum computing on present cryptography," *IJACSA,* vol.9, no.3, pp.405-414, 2018. DOI: 10.48550/arXiv.1804.00200

[2] Nejatollahi, Hamid, et al., "Post-quantum lattice-based cryptography implementations: A survey," *ACM Computing Surveys (CSUR),* vol.1, no.1, pp.1-41, 2019. DOI: 10.1145/3292548

[3] Liu, Dongsheng, et al., "A resource-efficient and side-channel secure hardware implementation of ring-LWE cryptographic processor," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol.66, no.4, pp.1474-1483, 2018. DOI: 10.1109/TCSI.2018.2883966

[4] Lyubashevsky, Vadim, Chris Peikert, and Oded Regev, "On ideal lattices and learning with errors over rings," *Annual international conference on the theory and applications of cryptographic techniques,* pp.1-23, 2010. DOI: 10.1007/978-3-642-13190-5_1

[5] Pöppelmann, Thomas, and Tim Güneysu, "Towards efficient arithmetic for lattice-based cryptography on reconfigurable hardware," *International conference on cryptology and information security in Latin America. Springer, Lecture Notes in,* pp.139-158, 2012. DOI: 10.1007/978-3-642-33481-8_8

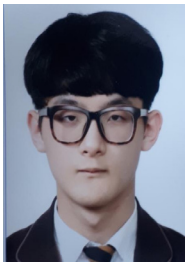
[6] Pöppelmann, Thomas, and Tim Güneysu, "Area optimization of lightweight lattice-based encryption on reconfigurable hardware," *IEEE international symposium on circuits and systems (ISCAS). IEEE,* pp.2796-2799, 2014. DOI: 10.1109/ISCAS.2014.6865754

[7] Khalid, Ayesha, et al., "Lattice-based cryptography for IoT in a quantum world: Are we ready?,"

IEEE 8th international workshop on advances in sensors and interfaces (IWASI), pp.194-199, 2019.
DOI: 10.1109/IWASI.2019.8791343
[8] Aysu, Aydin, Cameron Patterson, and Patrick Schaumont, "Low-cost and area-efficient FPGA implementations of lattice-based cryptography," *IEEE international symposium on hardware-oriented security and trust (HOST),* pp.81-86, 2013.
DOI: 10.1109/HST.2013.6581570
[9] Zhang, Xinmiao, and Keshab K. Parhi. "Reduced-complexity modular polynomial multiplication for R-LWE cryptosystems," *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* pp.7853-7857, 2021.
DOI: 10.1109/ICASSP39728.2021.9414005
[10] Liu, Zhe, et al., "Efficient Ring-LWE encryption on 8-bit AVR processors," *International Workshop on Cryptographic Hardware and Embedded Systems. Springer,* pp.663-682, 2015.
DOI: 10.1007/978-3-662-48324-4_33
[11] Liu, Weiqiang, et al., "Optimized schoolbook polynomial multiplication for compact lattice-based cryptography on FPGA," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* vol.27, no.10, pp.2459-2463, 2019.
DOI: 10.1109/TVLSI.2019.2922999
[12] Kundi, Dur E. Shahwar, et al., "AxMM: Area and power efficient approximate modular multiplier for R-LWE cryptosystem," *2020 IEEE International Symposium on Circuits and Systems (ISCAS),* pp.1-5, 2020.
DOI: 10.1109/ISCAS45731.2020.9180839
[13] Zhang, Yuqing, et al., "An efficient and parallel R-LWE cryptoprocessor," I*EEE Transactions on Circuits and Systems II: Express Briefs,* vol.67, no.5, pp.886-890, 2020.
DOI: 10.1109/TCSII.2020.2980387
[14] Barrett, Paul, "Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor," *Conference on the Theory and Application of Cryptographic Techniques. Springer,* pp.311-323, 1986.
DOI: 10.1007/3-540-47721-7_24
[15] Roy, Sujoy Sinha, et al., "Compact ring-LWE cryptoprocessor," *International workshop on cryptographic hardware and embedded systems. Springer*, pp.371-391, 2014.

BIOGRAPHY

Jae-Woo Lee (Member)



2022.2 : BS degree in Electronic and Electrical Engineering, Korea National University of Transportation.
2022.8~ : MS Program in Electronic & Electrical Engineering, Hongik University.

Youngmin Kim (Member)

1999.8 : BS degree in Electrical Engineering, Yonsei University.
2003 : MS degree in EE, Univ. of Michigan, Ann Arbor.
2007 : PhD degree in EE, Univ. of Michigan, Ann Arbor.
2007.10~2009.7 : Qualcomm, Senior Engineer.
2009.8~2015.2 : Assistant Professor at UNIST.
2015.3~2019.2 : Associate Professor at Kwangwoon University.
2019.3~current : Professor at Hongik University.