HLS 를 활용한 FPGA 기반의 FALCON 알고리즘 서명 생성 하드웨어 가속 연구

이용석 [1], 이윤지 [1], 백윤흥 [1]
[1] 서울대학교 전기정보공학부, 서울대학교 반도체 공동연구소
yslee@sor.snu.ac.kr, yjlee@sor.snu.ac.kr, ypaek@snu.ac.kr

FPGA-based Hardware Acceleration for Signature Generation of FALCON using High Level Synthesis

Yongseok Lee[1], Yunji Lee[1], Yunheung Paek[1]
[1]Dept. of Electrical and Computer Engineering and Inter-University Semiconductor Research Center(ISRC), Seoul National University

요 약

최근 차세대 암호로 불리는 양자내성암호(PQC, Post Quantum Cryptography)는 양자 컴퓨터와 현재 사용하는 일반 컴퓨터 모두에서 내성을 갖는 암호이다. 그 중 FALCON 전자 서명 알고리즘은 표준화로 선정되며 초안 문서를 작성하는 중으로 차세대 암호로 주목받고 있다. 하지만 FALCON 알고리즘은 실수 연산을 사용하는 등 임베디드 환경에서 효율적인 성능을 보이지 못하고 있다. 이에 따라 임베디드 하드웨어 가속 연구들이 있으며, 그 중 HLS(High Level Synthesis)를 통한 FPGA 가속 연구들이 있다. 본 논문에서는 FALCON 전자서명 알고리즘에서 HLS 로 구현하는데 어려움이 있었던 서명 생성 함수에 대해 분석하고, 이를 소프트웨어/하드웨어 통합설계를 통해 HLS 로 구현하였다. 이는 기존 소프트웨어 대비 약 10 배 빠른 연산 속도를 보여주고 있다.

1. 서론

차세대 암호로 주목받고 있는 양자내성암호(PQC, Post Quantum Cryptography)는 양자 컴퓨터에서 취약성을 갖지 않도록 격자기반, 코드기반 등 다양한 보안성이 기반하여 고안된 알고리즘이다. 몇 년간 NIST(National Institute of Standard and Technology)에서 양자내성암호에 대한 표준화를 진행하고 있으며, 그 분야는 KEM(Key Encapsulation Mechanism) 그리고 DSA(Digital Signature Algorithm)으로 나눠져 있다. 2022 년에는 표준화 알고리즘으로 KEM 분야에서 Crystal-Kyber 를 선정하였으며, DSA 분야에서는 FALCON, Crystal-Dilithium, SPHINCS+를 선정하였다. 이후에도 다양성을 위해 표준화를 진행하고 있는 상태이다.

표준화 과정 중 후보 알고리즘들에 대한 평가 및 분석이 자유롭게 이뤄지며, 그 과정에서 분석한 결과들을 논문으로 발표하기도 하였다. 임베디드 소프트웨어 환경에서는 NIST 에서 추천하는 Cortex-M4 보드를 통한 연구들이 주로 진행되었으며, 임베디드 하드웨어 환경에서는 NIST 에서 추천하는 Xilinx Artix7 FPGA 보드에 대해 HLS(High Level Synthesis)[1] 혹은 핸드 코딩을 통한 RTL(Register Transfer Level) 연구[2,3]가 진행되었다.

하지만 FALCON 알고리즘은 표준화 후보로 등록된 지 오래되었고, 현재도 표준화 알고리즘으로 DSA 분야에서 선정되었지만, HLS 를 통한 FPGA 가속 연구는 부족한 실정이다. 기존 연구들은 FALCON 의 키 생성 과정과 서명 검증 과정을 HLS 를 통해 구현한 연구를 발표하는데 한계를 가지고 있다[4]. 이러한 이유는 FALCON 서명 생성과정에서 존재하는 알고리즘적 특성으로 인해 HLS 를 통한 단순 적용이 어렵기 때문이다. 따라서 본 논문에서는 FALCON 알고리즘의 전자서명 함수를 분석하고, 이를 HLS 에 적용하기 위해 소프트웨어/하드웨어 통합설계 방법을 제안한다.

본 논문에서 제안하는 HLS 방법은 FALCON 서명 생성 함수를 분석하여, 소프트웨어 파트와 하드웨어 파트를 구분하고, 실수 연산이 포함된 FFT/IFFT 연산 등을 하드웨어에서 연산하고, 정수 연산이 주로 있는 NTT/INTT 연산 등은 소프트웨어로 연산하며, 순환 함수 구조를 이루는 SamplerZ 함수는 소프트웨어/하드웨어 통합설계를 수행하는 방법을 적용하였다. 이

를 통해 FALCON 전자 서명 함수에 대한 HLS 수행을 진행하여 기존 소프트웨어 대비 약 10 배 빠른 연산 속도를 보여주었다.

2. 양자내성암호 FALCON 알고리즘

양자내성암호 중 FALCON 전자 서명 알고리즘은 표준화로 선택되어 표준화 문서 초안 작성 단계에 있다. 전자서명 과정은 키 생성, 서명 생성, 서명 검증 이렇게 세 과정으로 구성되어 있다. NIST 에서 제안하는 파라미터 구성은 아래 표 1 과 같이 FALCON-512 와 FALCON-1024 가 있으며, 각각 Security Level 1 과 5 를 나타내고 있다. Ring Degree 는 다항식의 차수를 나타내며 Modulus 는 정수 연산을 수행하는 NTT 의 경우 사용되는 q 값을 나타낸다.

표 1. FALCON 알고리즘 파라미터

Parameters	Ring Degree	Modulus	Security Level
FALCON-512	512	12,289	1
FALCON-1024	1,024	12,289	5

FALCON 의 특징 중 하나는 정수 연산과 실수 연산이 모두 존재한다는 점이다. NTT 연산의 경우 정수 연산을 수행하지만, FFT 연산 등 다른 함수에서는 실수 연산을 사용한다. 이는 알고리즘 특성상 서명 생성 과정에서 가우시안 분포를 샘플링 하고 검증하기 위해 실수 연산이 필요하기 때문이다. 그래서 정수 데이터와 실수 데이터 간의 타입 변환이 필요하다. 이러한 실수연산 때문에 FPU(Floating Point Unit)이 없는 임베디드 환경에서는 특히나 FALCON 연산이 비효율적인 상황이다. 이러한 문제로 FALCON 알고리즘에 대한 하드웨어 가속 논문들이 연구되고 있다.

3. HLS 를 활용한 하드웨어 가속 연구

본 논문에서는 Xilinx 사에서 제공하는 Vitis HLS(High Level Synthesis) 2021.1 버전의 기술을 활용하여 하드웨어 가속하는 연구를 수행한다. HLS 는 C/C++언어 등으로 작성된 소프트웨어 코드를 입력으로 받아 목표하는 FPGA 보드에 맞는 Verilog-HDL(Verilog Hardware Description Language) 코드를 생성하는 기술이다. HLS 를 수행하는 과정에서 FPGA 보드에 대한 제한사항과 더불어 연산 모듈 사이의 계층 구조, 인터페이스, 메모리 구성 등의 구조적인 제한사항을 고려할 수 있다. 또한 하드웨어 연산의 특성인 병렬성을 활용하기 위한 Loop-unrolling 과정에서 병렬화 개수를 조정하거나, RTL(Register Transfer Level)의 특성을 가지고 있는 하드웨어 특성으로 Low-level timing 을 조정하는 사항과 반복되는 연산에서 Iteration 을 제한하는 사항 등을 고려할 수 있다. 이처럼 설계자가 의도한 결과물을 도출하기 위해서는 HLS 를 수행하는 과정에서 다양한 제한 사항을 추가해야 하며, 이를 통해 서로 다른 결과를 얻을 수 있다.

Algorithm 1 SamplerZ

Input: Floating point values μ,
$\sigma' \in R$ such that $\sigma' \in [\sigma_{min}, \sigma_{max}]$
Output: An integer $z \in \mathbb{Z}$ sampled from a distribution very close to $D_{\mathbb{Z},\mu,\sigma'}$

1: $r \leftarrow \mu - \lfloor \mu \rfloor$
2: $ccs \leftarrow \sigma_{min}/\sigma'$
3: while do
4: $z_0 \leftarrow$ **GaussianSampler**() ▷ Gaussian sampling
5: $b \leftarrow$ UniformBits(8) & 0x1
6: $z \leftarrow b + (2 \cdot b - 1)z_0$
7: $x \leftarrow \frac{(z-r)^2}{2\sigma'^2} - \frac{z_0^2}{2\sigma_{max}^2}$
8: if(**BerExp**(x,ccs) = 1) ▷ Rejection sampling
9: return z + $\lfloor \mu \rfloor$

알고리즘 1. FALCON SamplerZ 함수 동작 수도코드

특히 FALCON 알고리즘의 서명 생성 과정은 순환 함수가 존재하는 특성이 있어, HLS 를 통한 하드웨어 구조 적용에 어려움이 있다. 서명 생성 과정에서 수행되는 순환 함수는 SamplerZ 함수이다. 이는 랜덤 값을 가지고 가우시안 분포를 생성하며, 이를 목표한 가우시안 분포와 얼마나 다른지 검증하는 단계로 이루어져 있다. 여기서 목표한 분포와 크게 다를 경우, 다시 랜덤 값을 받아와서 가우시안 분포를 생성하는 것부터 다시 시작하는 순환 구조를 가지고 있다. 이러한 특징은 HLS 적용에 많은 어려움을 야기하고 있었다.

기존 HLS 를 적용한 양자내성암호 연구들 에서도 FALCON 알고리즘의 서명 생성 과정을 다루지 못하고 있으며, 순환 함수가 없는 키 생성 및 서명 검증 과정에 대해서만 결과를 보여주고 있는 한계가 있다 [4]. 본 논문에서는 이를 해결하기 위해 SamplerZ 함수에 대해 소프트웨어/하드웨어 통합설계 방법을 제안한다. 램덤 값과 가우시안 표준편차를 생성하는 파트를 소프트웨어에서 수행하고, 이를 통한 가우시안 분포 생성 및 검증을 하드웨어에서 수행한다. 이를 통해 하드웨어에서 수행하는 연산은 외부 입력에 의해 수행되는 순차적인 연산들의 모임으로 구성할 수 있으며, 검증 결과를 통해 그 연산들을 단순 반복하는 방식으로 구성되게 된다.

4. FPGA 기반의 하드웨어 가속 방법

본 논문에서 제안하는 소프트웨어/하드웨어 통합설계 방법은 Cortex-M4 같은 임베디드 환경에서 소프트웨어로 FALCON 알고리즘을 수행할 때 어려움이 발생하는 FFT/IFFT 같은 실수 연산 들을 하드웨어 파트로 오프로딩하여 수행한다. 따라서 NTT/INTT 같은 정수 연산들은 소프트웨어에서 수행하는 것으로 구성하였다. 또한 SamplerZ 함수의 경우 소프트웨어/하드웨어 통합설계로 세부 연산을 분리하여 수행하며, 이를 통해 HLS 를 수행한 FPGA 결과를 얻을 수 있었다.

표 2. FPGA 하드웨어 합성 결과

	LUT	**FF**	**DSP**	**Clock Speed (MHz)**
Ours	11,522 (8.61%)	6,699 (2.49%)	49 (6.62%)	168

HLS 를 통해 Xilinx Artix7 FPGA 에서 합성된 결과는 표 2 와 같으며, 실수 연산에 해당하는 곱셈기, 덧셈기 등을 하나씩만 구성하도록 제한하여 임베디드 환경에 적합한 결과를 도출하려 하였다. 소프트웨어 동작 환경은 Cortex-M4 임베디드 보드로 168MHz 동작속도를 가진다. 표 3 에서 보여주는 소프트웨어 결과는 FALCON 서명 생성 함수를 Cortex-M4 임베디드 보드에서 수행한 결과이다. 표 3 에서 볼 수 있듯이 본 논문에서 제안하는 소프트웨어/하드웨어 통합설계 방법이 FALCON-512 그리고 FALCON-1024 파라미터에서 각각 40.1ms 와 83.2ms 로 기존 소프트웨어 연산 대비 약 10 배 정도 빠른 연산 결과를 보이고 있다.

표 3. Cortex-M4 소프트웨어 구현과 성능 비교

	Parameters	**Latency(ms)**	
M4 SW	FALCON-512	411.1	x10.25
	FALCON-1024	879.8	x10.57
Ours (SW+HW)	FALCON-512	**40.1**	-
	FALCON-1024	**83.2**	-

소프트웨어 연산과 이러한 성능 차이는 Cortex-M4 임베디드 보드가 가지는 한계로 실수 연산을 FPU 를 통해 직접적으로 지원하지 못하고 다른 명령어들의 조합으로 수행하는 단점이 있기 때문이다. 이에 FPGA 에서 수행하는 연산들은 실수 연산들을 주로 수행하며 전용 실수 곱셈기, 덧셈기, 나눗셈기 등을 구성하여 연산기 내부의 파이프라인 기법을 적용하여 가속하였다.

5. 결론

본 논문에서는 PQC DSA 알고리즘 중 하나인 FALCON 의 서명 생성 함수를 소프트웨어/하드웨어 통합설계 방법으로 가속하였다. 이는 기존 HLS 방법으로 FPGA 가속하는 연구에서 어려움으로 남아있는 서명 생성 함수를 소프트웨어/하드웨어 통합설계 방법으로 SamplerZ 함수 연산 플로우를 단순화하여 HLS 를 수행하는 방법으로 해결하였다. 또한 임베디드 하드웨어 환경에 맞게 실수 연산 모듈 등을 하나씩 구성하여 FPGA 자원을 효율적으로 사용했다. 그러면서도 연산 성능은 소프트웨어 대비 약 10 배 정도 빠른 결과를 보여주었다. 따라서 향후 FALCON 알고리즘 연구에 좋은 기여가 될 것으로 기대된다.

ACKNOWLEDGEMENT

이 논문은 2023 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구이며 (IITP-2023-RS-2023-00256081), 2024 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구이며 (RS-2023-00277326), 2024 년도 BK21 FOUR 정보기술 미래인재 교육연구단에 의하여 지원되었음. 본 연구는 IDEC 에서 EDA Tool 을 지원받아 수행하였음.

참고문헌

[1] Nguyen, Duc Tri, et al. “A High-Level Synthesis Approach to the Software/Hardware Codesign of NTT-Based Post-Quantum Cryptography Algorithms,” 2019 International Conference on Field-Programmable Technology (ICFPT), IEEE, pp.1-4, 2019. DOI: 10.1109/ICFPT47387.2019.00070

[2] Beckwith, Luke, et al. "Hardware Accelerators for Digital Signature Algorithms Dilithium and FALCON," IEEE Design & Test, IEEE, pp.1-7, 2023. DOI: 10.1109/MDAT.2023.3305156

[3] Karabulut, Emre, et al. "A Hardware-Software Co-Design for the Discrete Gaussian Sampling of FALCON Digital Signature," Cryptology ePrint Archive, Paper 2023/908, pp.1-6, 2023. Available: https://eprint.iacr.org/2023/908

[4] Soni, Deepraj, et al. “Hardware Architectures for Post-Quantum Digital Signature Schemes,” Springer, Cham, pp.1-170, 2021. Available: https://doi.org/10.1007/978-3-030-57682-0