임베디드 시스템을 위한 양자후암호화 FALCON 알고리즘의 FFT 연산 가속 연구

이용석, 남기빈, 주유연, 백윤흥
서울대학교 전기정보공학부, 서울대학교 반도체 공동연구소

yslee@sor.snu.ac.kr, kvnam@sor.snu.ac.kr, yyjoo@sor.snu.ac.kr, ypaek@snu.ac.kr

A Study on the FFT Acceleration of PQC FALCON for Embedded Systems

Yongseok Lee, Kevin Nam, You-yeon Joo, Yunheung Paek
Dept. of Electrical and Computer Engineering and Inter-University Semiconductor Research Center(ISRC), Seoul National University.

요 약

기존의 전자서명에서 활용되는 공개키 암호 시스템을 대체하기 위해 표준화가 진행중인 PQC FALCON 전자서명 알고리즘은 서버와 일반 컴퓨터 뿐만 아니라 임베디드 환경에서도 범용적으로 사용되는 방식이다. 따라서 임베디드 시스템에서도 올바른 데이터 전송을 위해서 PQC 알고리즘을 활용한 전자서명을 필수로 수행해야 한다. 하지만 PQC 알고리즘은 기존의 전자서명 알고리즘과 달리 더 많은 데이터와 연산 복잡도를 요구하고 있다. 특히 FALCON 알고리즘은 일반적인 임베디드 시스템에서 지원하지 않는 double-precision 부동소수점 연산을 필요로 한다. 이는 추가적인 clock cycle 을 발생시키는 요소로 전자서명 시간을 증가시키는 요인이다. 따라서 double-precision 을 지원하는 FPU HW 모듈을 설계하고, 특히 많은 시간이 소요되는 FFT/IFFT 함수를 가속하는 HW 모듈을 설계하려 하였다. 이를 통해 SW 대비 138 배 적은 clock cycle 결과를 보여주었다.

Ⅰ. 서 론

최근 양자컴퓨팅 기술이 점차 발달하면서 기존의 전자서명에서 활용되는 공개키암호시스템인 RSA 기술 등을 대체하기 위해 NIST 는 양자후암호화(PQC, Post Quantum Computing) 표준화를 진행하고 있다.[1-2] 이러한 전자서명 알고리즘은 서버와 일반 컴퓨터 뿐만 아니라 임베디드 환경에서도 범용적으로 사용되는 방식이다. 예를 들어 서버에서 임베디드 시스템에 데이터를 보내줄 경우, 이 데이터가 확인된 서버에 의해 보내진 올바른 데이터인지 아니면 다른 서버가 공격을 위해 보낸 변조된 데이터 정보인지 판단할 때 전자서명 알고리즘이 사용된다. 따라서 임베디드 시스템에서도 올바른 데이터 전송을 위해서 PQC 알고리즘을 활용한 전자서명을 수행해야 하는 것이다. 하지만 PQC 알고리즘은 양자컴퓨터에서도 안전하게 사용될 수 있도록 고안된 알고리즘으로, 기존의 전자서명 알고리즘과 달리 더 복잡한 연산과 데이터를 다루고 있다. 특히 FALCON 알고리즘의 경우 double-precision floating point 연산을 수행하는 특징이 있다.[3] 하지만 이는 임베디드 시스템 벤치마크에 주로 사용되는 cortex M4 등에서는 지원하지 않는 연산이다. 부동소수점 연산은 선택적으로 FPU 모듈을 탑재해 지원하지만, 오직 single-precision 을 지원하여 double-precision 연산을 위해서는 SW 적으로 추가적인 instruction 이 필요하다. 본 논문에서는 임베디드 시스템에서 이를 극복하기 위해 double-precision 을 지원하면서 FALCON 알고리즘에서 많은 시간이 소요되는 FFT/IFFT 연산을 가속하는 HW 를 설계하려 한다.

Ⅱ. 본론

본 논문에서는 FALCON 알고리즘에서 주로 사용되는 FFT/IFFT 연산을 가속하는 것을 목표로 하였다. FFT/IFFT 연산은 그림 1 에서 볼 수 있듯이 일반적으로 데이터 연산 복잡도가 큰 함수이다. 하지만 mul, add, div 함수가 반복적인 구조로 사용되는 butterfly 유닛 구조를 가지고 있어, HW 설계에 유리한 면이 있다. FALCON 알고리즘에서 사용되는 FFT/IFFT 함수는 double-precision 부동소수점 연산들로 이루어져 있다. 일반적으로 Cortex M4 등의 임베디드 시스템은 double-precision 부동소수점 연산을 위해 추가적인 연산이 필요하다. 따라서 이에 대해 HW 모듈로 온전히 가속하는 FPU 모듈을 지원한다면 HW 로 설계하는 장점을 더 가져갈 수 있을 것으로 분석하였다.

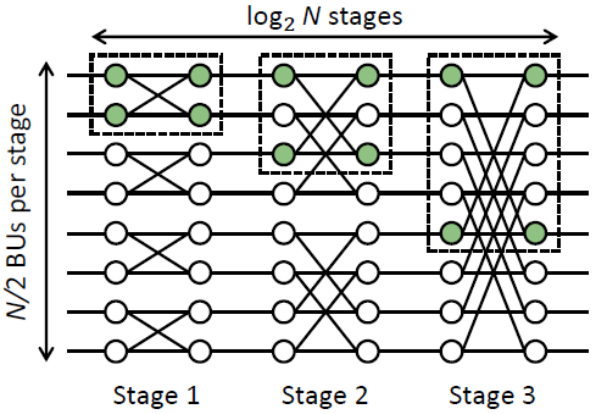

그림 1. 8 포인트 FFT 연산 그림 예시

표 1 에서 볼 수 있듯이 FALCON 전자서명 함수는 크게 ffSampling, FFT, IFFT 함수로 이루어져 있는데, cortex M4 에서 측정한 결과 연산시간 중 FFT/IFFT 함수가 27%정도의 비율을 차지한다. 수행시간 측정은 168MHz 동작속도로 진행하였고, 전체 소요 시간은 879ms 로 나타났다. 이 중 가장 많은 소요시간 비율을 차지하고 있는 ffSampling 함수 또한 내부적으로 FFT/IFFT 함수의 변형된 연산들이 포함되어 있다. 하지만 이는 랜덤 값을 사용하는 함수 등이 있어 본 연구에서는 목표로 하지 않았다. 본 논문에서는 double-precision 을 온전히 지원하지 않는 임베디드 시스템에서 FFT/IFFT 함수를 수행하는 FPU HW 로 대체하였을 경우 clock cycle 감소 효과가 어느정도 나타나는지 확인하는 것에 목표를 두고 설계하였다.

표 1. 전자서명 함수의 클럭 사이클 및 비율 분석

Function	Sub-function	Clock Cycle	Portion
crypto_sign	ffSampling	89099941	60.28%
	FFT	32984487	22.32%
	IFFT	7634106	5.16%
	etc	15714964	12.24%

본 논문에서 진행한 설계는 double-precision 부동소수점을 지원하는 mul, add, div 함수를 HW 로 설계하고, 이를 butterfly 유닛으로 구성하여 FFT/IFFT 함수를 연산할 수 있도록 하였다. 설계면적을 최소화 하기 위해 Single port RAM 을 주 연산 메모리로 할당하고, 이와 통신하며 HW 모듈이 연산을 수행하도록 구성하였다. 향후 임베디드 시스템에 추가적으로 연결되는 HW 모듈을 가정하여 연산 모듈들은 하나만 설계하고 이를 재사용하는 방식으로 하였다. 따라서 병렬적인 연산보다는 파이프라인 방식을 통해 latency 를 줄이는 방법을 사용하였다. 이는 하나의 스테이지 단위로 반복적으로 진행되는 butterfly 유닛에 효과적으로 적용 가능하였다.

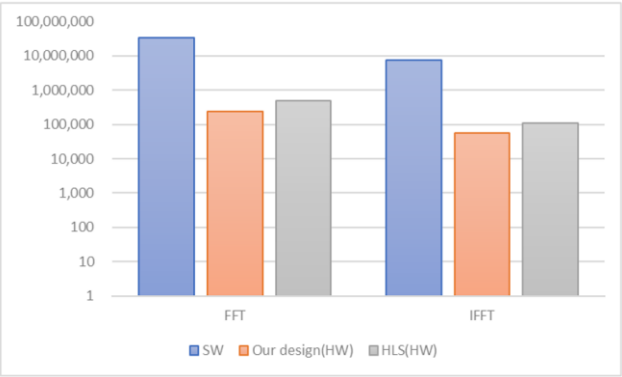

그림 2. Cortex M4(SW)수행, HLS(HW)설계 그리고 본 논문의 HW 설계결과에 대한 clock cycle 비교

실험결과 비교를 위해 Xilinx Vivado HLS 툴을 사용한 HW 설계결과도 비교하였다. 이는 본 연구에서 중점적으로 사용한 설계면적 최소화 기조를 유지하도록 제약을 주었다. 또한 임베디드 시스템인 cortex M4 환경에서 SW 수행한 결과 또한 비교하였다. 그림 2 를 보면 알 수 있듯이, FFT 연산과 IFFT 연산에서 모두 본 연구에서 설계한 HW 모듈이 더 낮은 clock cycle 을 보이는 것을 알 수 있다. 그래프의 왼쪽 축은 로그 스케일로 표현되어 있다.

같은 동작속도로 동작한다고 가정하였을 때, clock cycle 만을 비교한다면 기존의 SW 대비 본 연구의 HW 모듈은 약 138 배 더 낮은 clock cycle 을 기록하였다. 툴을 사용한 HLS(HW) 설계 모듈은 기존의 SW 대비 68 배 더 낮은 clock cycle 을 기록한 것으로 보아 본 연구의 결과물이 더 좋은 성능을 보이는 것을 확인할 수 있다.

Ⅲ. 결론

본 논문에서는 임베디드 시스템에서 성능 저하를 보이는 PQC FALCON 알고리즘의 FFT/IFFT 함수를 HW 로 가속한 결과를 보이고 있다. FALCON 알고리즘의 특징으로 double-precision 부동소수점 연산을 수행해야 하지만, cortex M4 처럼 일반적인 임베디드 시스템은 이를 지원하지 않아 추가적인 연산이 필요하였다. 이에 이를 따로 가속하는 전용 HW 모듈을 설계하였으며, 추후 임베디드 시스템에 추가하여 연산할 수 있도록 설계면적을 최소화하도록 하였다. 본 연구를 통해 추가적인 HW 로 가속하는 것이 효과적임을 확인하였으며, 향후 ffSampling 함수 등도 HW 모듈 설계를 통해 더 가속한다면 전체적인 FALCON 전자서명 알고리즘도 크게 가속될 수 있을 것이라 기대된다.

ACKNOWLEDGMENT

이 논문은 2022 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단 (NRF-2020R1A2B5B03095204), BK21 FOUR 정보기술 미래인재 교육연구단의 지원을 받아 수행된 연구임. 본 연구는 반도체 공동연구소 지원의 결과물임을 밝힙니다.

참 고 문 헌

[1] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2):303-332, 1999.

[2] NIST. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. https://www.federalregister.gov/documents/2016/12/20/2016-30615/announcing-request-for-nominations-for-public-key-post-quantum-cryptographic-algorithms. accessed:2022-02-10.

[3] PA Fouque, J Hoffstein, P Kirchner, V Lyubashevsky, T Pornin, T Prest, T Ricosset, G Seiler, W Whyte, and Z Zhang. Falcon: Fast-fourier latticebased compact signatures over ntru, specification v1. 2. NIST Post-Quantum Cryptography Standardization Round, 3, 2020.