Hardware 기반 Crystals-Kyber의 효율적인 NTT Core 설계 및 경량화

정병욱, 윤동욱, 지장현, 김호원

부산대학교

jbu0828@gmail.com, donk1879@gmail.com, jjh0819@gmail.com, howonkim@gmail.com

Efficient NTT Core design and lightweighting of Hardware-based Crystals-Kyber

ByeongUk Jeong, DongWook Yun, JangHyun Ji, HoWon Kim

Pusan National Univ

요 약

양자 컴퓨터의 발전으로 기존 통신 프로토콜 및 네트워크에서 사용되어 오고 있는 공개키 암호 RSA와 ECC 기반 암호화 시스템의 기밀성과 무결성이 무력화 될 수 있다. 이에 대응하기 위해 양자내성암호의 필요성이 높아지고 있으며, 향후 저사양 임베디드 환경에서 활용하기 위해 하드웨어 기반 양자내성암호 Crystals-Kyber를 FPGA상에서 구현하였다. 구현에 있어 연산에 가장 많이 사용되는 Modular Reduction과 연산 오버헤드가 가장 높은 NTT/INTT 연산에 대한 효율적인 제어 및 최적화 기법에 대해 설명한다. 또한 본 논문의 결과물을 KAT(Known Answer Test)기반으로 키 생성 및 암복호화에 대해 검증하였다.

Ⅰ. 서 론

양자 컴퓨터의 발전으로 기존 컴퓨터에서 사용되어 오고 있는 공개키 암호화 방식인 RSA나 ECC 기반 암호화 시스템이 쉽게 해결될 우려가 있다. 이로 인해 기존 통신 프로토콜 또는 네트워크에서의 기밀성과 무결성이 저해될 수 있다. 이에 대응하여, 2016년에 미국 국립표준기술연구소(NIST)에서 양자 이후 암호 표준화 연구를 시작했으며, 최근 3라운드 최종 후보 결과로 격자 기반 KEM(Key Establishment Mechanism)에 Crystals Kyber가 선택되어 표준화 진행 중이다. 따라서 양자 컴퓨팅에 대응하는 양자 내성 암호화의 필요성이 증가하고 있으며, 본 논문에서 하드웨어 기반으로 경량화된 환경에서 고속화 연산이 가능한 구조를 제안하며, Crystals-Kyber에서 연산 오버헤드가 가장 높은 NTT(Number Theoretic Transform)에 대해 효율적으로 제어가 가능한 구조를 설명한다.

Ⅱ. 배경 지식

1) Crystals-Kyber

Crystals-Kyber는 MLWE(Module Learning With Error)를 기반으로 격자 공간상에서 가장 짧은 벡터를 찾는 문제 SVP(Shortest Vector Problem)와 주어진 벡터와 가장 가까운 벡터를 찾는 CVP(Closet Vector Problem) 문제를 이용하며, 격자 공간상에 작은 오류값을 더함으로써 기존의 수학적 해법으로는 해결하기 어려운 알고리즘이다. 그러므로 기존 및 양자 컴퓨터에서의 보안성을 제공하는 알고리즘이다.

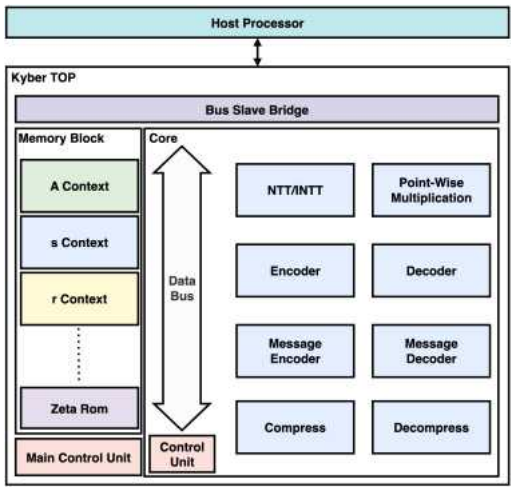
2) NTT/INTT

NTT는 신호처리에서의 FFT(Fast Fourier Transform) 특징을 이용한 알고리즘이다. NTT에서는 FFT의 Twiddle Factor와 유사한 Root of Unity를 사용하는데, 이는 다항식을 NTT 도메인으로 변환하기 위해 각 차수에 해당하는 계수와 곱에 사용되는 요소이다.

기존의 두 다항식의 곱셈은 모든 계수에 대해 곱셈 연산을 수행하여 $O(n^2)$의 계산 복잡도를 가지는데 NTT 도메인으로 변환하게 되면 각 차수에 해당하는 계수만 곱셈 연산을 수행한다. 또한 NTT 도메인으로 변환하는데 발생하는 곱셈 연산에 의해 총 계산 복잡도는 $O(n \log n)$으로 곱셈 연산 오버헤드를 효과적으로 줄일 수 있다.

Ⅲ. 본론

본 논문에서 설명하는 Hardware기반 Crystals-Kyber의 전체 구조는 [그림 1]과 같다. Host Processor에서 SHA3와 SHAKE 함수와 관련된 Rejection/CBD Sampling과 같은 전처리 수행을 소프트웨어를 통해 진행되었으며, AXI Bus 인터페이스를 이용하여 Memory Block에 각 기능 연산을 수행하기 위한 A, s, e, message 등을 입력받는 구조이다. 이후 각 기능들은 내부 Control Unit을 통해 Key Generation, Encryption, Decryption 동작을 위한 연산을 결정한다.

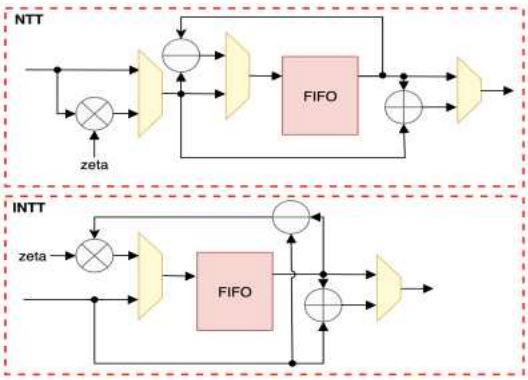


[그림 1] Crystals-Kyber 모듈 전체 구조도

본 논문에서 제안하는 하드웨어 경량화를 위해 Modular Reduction과 NTT/INTT 설계 구조에 대해서 설명한다. NIST에 제출된 Crystals-Kyber의 모델 구조에 따르면 Modular Reduction을 위해 다항식 덧셈과 뺄셈 연산 수행 시 Barrett Reduction을 다항식 곱셈 연산 수행 시 Montgomery Reduction을 따른다. 하지만 이를 하드웨어 구현 시

곱셈기와 덧셈기를 통해 구현되는데, 이는 하드웨어 자원량에서 많은 오버헤드가 발생한다. 이에 본 논문에서는 다항식 덧셈과 뺄셈 연산에 대한 Reduction은 단순 비교기를 활용하여 구현하였다. 이는 곱셈기를 사용하는 Barrett Reduction에 비해 상당한 자원량을 절약할 수 있다. 그리고 다항식 곱셈 연산에 대한 Montgomery Reduction을 대신하여 Dadda Reduction 기법을 활용하였다. Dadda Reduction은 q를 다항식으로 치환하여 재귀적으로 분해하여 덧셈을 수행한다. 하드웨어서 Bit shift 연산에는 자원 소요가 되지 않으며, 곱셈기를 대신하기 때문에 하드웨어 자원량을 최소화할 수 있다.[3, 4]

[그림 2]는 NTT와 INTT 연산 모듈에 대한 구조도이다. Crystals-Kyber의 경우 NTT/INTT 변환을 위해 총 7-Stage로 구성되어 있다. 각 Stage를 별도로 구현하여 Pipeline 구조를 적용시켰으며, 데이터 입출력을 효율적으로 제어하기 위해 FIFO(First In First Out)를 사용하였다. 입출력에 대응하는 다항식의 각 계수를 순차적으로 입력받으며 각 Stage별에 해당하는 입력 개수의 절반 만큼을 FIFO에 저장된다. 나머지 절반이 입력될 때 FIFO에서 출력하여 덧셈과 뺄셈을 수행한다. 이때 출력은 다음 Stage에 순차적으로 입력을 주기 위해 덧셈 값은 바로 출력으로 내보내고 뺄셈 값은 다시 FIFO에 저장해두었다가, 덧셈의 출력이 완료된 이후 FIFO에 저장된 뺄셈 값을 출력한다. 이를 통해 NTT/INTT 변환을 위한 제어 로직에 단순화 효과를 주며, 변환하는 데 발생하는 Latency를 최소화할 수 있다.



[그림 2] FIFO기반 NTT/INTT 연산 구조도

본 논문에서 제안하는 Crystals-Kyber 모듈을 구현하기 위해 Xilinx Zynq UltraScale+ ZU3EG MPSoC 칩이 내장된 보드를 사용하였으며, 칩에서 지원하는 PS(Processing System) 및 운영체제 Ubuntu 20.04 LTS를 이용하였다. Xilinx사의 Vivado 툴을 사용하여 블록 디자인을 구현하였으며 [표 1]은 이에 따른 하드웨어 자원 사용량을 나타낸 것이다.

[표 1] Crystals-Kyber 구현에 따른 하드웨어 자원사용량

	LUT	FF	BRAM	DSP
Utilized	10,719	8,538	41.5	22
Available	70,560	141,120	216	360
Percent	15.2%	6%	19.2%	6.1%

또한 Crystals-Kyber의 각 기능들에 대한 검증을 위해 KAT(Known Answer Test)기반 검증 소프트웨어를 구성하였으며, [그림 3]에서 Key Generation, Encryption, Decryption 기능들에 대한 검증 결과를 나타낸 것이다.

[그림 3] 각 기능들에 대한 검증 결과

Ⅳ. 결론

본 논문에서는 FPGA 보드 운영환경에서 순수 소프트웨어와 하드웨어 기반 가속기를 사용 시에 따른 성능 측정을 수행하였다. [그림 4]에서 전처리 수행에 따라서 NTT 이전 작업과 이후 작업에 대해 발생하는 Latency를 측정하여 두 작업의 차를 통해 성능 비교를 하였다. 하드웨어 기반 가속기 사용 시 각 기능별로 Key Generation은 5,904 Cycle, Encryption은 7,022 Cycle, Decryption은 5,494 Cycle로 소프트웨어 성능 대비 약 48~79배 성능 향상을 보인다.

[그림 4] 각 기능별 SW/HW 성능 비교

본 연구에서는 향후 양자 컴퓨터 발전에 대응하기 위해 하드웨어 기반 Crystals-Kyber를 구현하였다. 이는 저사양 IoT 디바이스 환경에서 데이터에 대한 기밀성과 무결성을 보장하여 높은 보안성을 제공하며, 향후 하드웨어 기반 양자 내성 암호 설계에 기여할 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 IDEC에서 EDA Tool를 지원받아 수행하였습니다.

참 고 문 헌

[1] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Specification document (update from August 2021). 2021-08-04

[2] XING, Yufei; LI, Shuguo. A compact hardware implementation of CCA-secure key exchange mechanism CRYSTALS-KYBER on FPGA.IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021, 328-356.

[3]YAMAN, Ferhat, et al. A hardware accelerator for polynomial multiplication operation of CRYSTALS-KYBER PQC scheme. In:2021 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2021. p. 1020-1025.

[4] 엄용준. "재구성형 Crystals-KYBER 양자내성암호 아키텍처." 국내석사학위논문 인하대학교 대학원, (2023)