동형암호를 위한 FPGA 기반의 하드웨어 가속기에 관한 연구 동향

이용석*, 백윤흥*
*서울대학교 전기정보공학부, 서울대학교 반도체 공동연구소
yslee@sor.snu.ac.kr, ypaek@snu.ac.kr

Research Trend on FPGA-based Hardware Accelerator for Homomorphic Encryption

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

요 약

최근 개인 정보 보호를 위해 주목 받고 있는 동형암호 알고리즘은 암호화된 상태로 덧셈과 곱셈 연산이 가능하여, 연산을 위한 복호화 과정 없이 데이터에 대한 가공이 가능하다. 따라서 이러한 동형암호 알고리즘이 개인 정보 보호를 위한 방법으로 떠오르고 있으며, 특히 완전동형암호 알고리즘의 경우 덧셈과 곱셈 연산을 모두 지원하며, 유효 연산 횟수에도 제한이 없어 응용 분야에서 널리 활용될 것으로 예상된다. 그러나, 완전동형암호 알고리즘의 경우 암호문의 크기가 평문대비 크게 증가하고, 다항식으로 구성된 암호문의 덧셈 및 곱셈 연산도 복잡하여 이에 대한 가속이 필요한 실정이다. 이에 FPGA 기반의 동형암호 가속기 개발이 많이 연구되고 있으며, 이를 통해 동형암호 연산의 특징을 이해하고 가속기 연구 동향을 알아보려 한다.

1. 서론

최근 전 세계적으로 개인 정보 보호에 대한 관심이 높아지면서, 데이터 암호화에 대한 관심이 많아지고 있다. 특히 암호화된 상태로 연산이 가능한 동형암호의 경우 과거에 연산량이 비현실적으로 많아서 정보 보호에 응용이 어려웠던 것과 달리, 현대에는 동형암호 알고리즘의 발달 및 하드웨어를 통한 동형암호 연산 가속 기술의 발달로 동형암호를 응용하려는 관심 또한 많아지고 있는 경향이 있다[1].

동형암호 알고리즘의 발달은 다음과 같이 세 가지로 구분할 수 있다[2]. 첫 번째는 덧셈과 곱셈 연산 중 하나만 수행할 수 있는, 연산에 부분적인 동형암호(Partially Homomorphic Encryption, PHE)로 1976 년도에 발표된 RSA 와 1999 년도에 발표된 Paillier 알고리즘이 있다. 이는 덧셈 혹은 곱셈 연산 하나에 대해 암호화된 상태로 연산이 가능하고, 이를 복호화 하면 암호화하지 않은 데이터를 연산한 것과 같은 결과를 보여준다. 두 번째는 암호화된 상태로 덧셈과 곱셈 연산 모두 수행이 가능하지만, 암호화된 상태로 연산 가능한 유효 횟수에 제한이 있는, 횟수에 부분적인 동형암호(Somewhat Homomorphic Encryption, SWHE)로 2005 년도에 발표된 BNG 알고리즘이 있다. 이는 덧셈과 곱셈 연산이 모두 가능하였지만, 유효한 연산 횟수에 제한이 있어서 연산 횟수를 증가시키기 위해서는 암호화 알고리즘 파라미터를 조정하여 암호문의 크기 및 연산량이 증가하는 한계가 존재하였다. 이러한 연산 횟수에 대한 한계로 응용 분야 적용에 제한이 있었다. 마지막으로 앞서 소개한 부분적인 동형암호 알고리즘들의 장점을 결합한 것이 완전동형암호(Fully Homomorphic Encryption, FHE)로 2009 년도에 발표된 Gentry 와 2017 년도에 발표된 CKKS 알고리즘이 대표적이다. 이는 암호화된 상태로 덧셈과 곱셈 연산을 모두 수행 가능한 것은 물론, 유효 연산 횟수에 대한 제한도 없이 지속적인 연산이 가능하여 여러 응용분야에 적용 가능할 것으로 기대되는 알고리즘이다. 특히 CKKS 알고리즘은 2018 년도 Bootstrapping 이라는 기법을 활용한 논문과 RNS 기법을 활용한 논문을 발표하며 지속적인 동형암호 알고리즘의 발전을 추구하고 있다. 게다가 알고리즘의 발전과 더불어 최근에는 동형암호 연산을 위한 전용 하드웨어 가속기가 많이 연구되고 있으며, 이러한 동형암호 가속기 중 특히 FPGA 기반 연구 동향에 대해 알아보려 한다.

2. 동형암호 연산

본 논문에서는 동형암호 알고리즘 중 최근 하드웨어 가속기로 많이 연구되고 있는 CKKS 알고리즘에 대한 연산을 살펴보려 한다. 동형암호 연산과정 중 암호문에 대한 연산을 주로 다루며, 이러한 암호문(ciphertext)는 다항식 $\boldsymbol{P(x)}$로 구성되어 있다. 이를 수식으로 나타내면 아래 수식 (1)과 같다.

$$\boldsymbol{ciphertext = P(x) = \sum_{i=0}^{N} a_i x^i, (N = 2^{17})} \quad (1)$$

따라서 동형암호 알고리즘에서 암호문의 덧셈은 두 다항식의 덧셈을 나타내고, 암호문의 곱셈은 두 다항식의 곱셈을 나타낸다고 볼 수 있다. 그리고 최근의 CKKS 알고리즘은 RNS(Residue Number System)기반으로 구성되어 다항식 연산 중에 나머지를 계산하는 modulus 연산이 필수적으로 수행되는 구조를 가지고 있다.

3. FPGA 기반의 하드웨어 가속기

본 논문의 2 장에서 살펴본 동형암호의 특징으로 최근의 CKKS 알고리즘은 다항식을 이루는 하나의 큰 계수에 대해 연산하는 방식이 아닌, RNS 기반으로 여러 작은 정수로 나눠진 계수를 연산하는 방식으로 동형암호 연산이 구성되어 있음을 알 수 있다. 이러한 연산 방식은 RNS 로 나눠진 작은 계수들에 대해 독립적인 연산이 수행될 수 있다는 큰 특징이 있다. 따라서 이러한 특징으로 FPGA 기반의 하드웨어 가속기를 개발한다면 병렬성을 효율적으로 활용한 연산이 가능할 것으로 기대되고, 이에 대한 최근 연구들이 그 결과를 보이고 있다.

먼저 동형암호 연산에서 자주 사용되는 modulus 연산에 대한 가속기 개발 연구가 있다[3]. 이는 FPGA 에서 제공되는 연산 블록인 DSP(Digital Signal Processing) 슬라이스를 활용하여 최소한의 자원 및 latency 로 modulus 연산을 수행하는 최적화 방법을 제안하고 있다. 그 방법으로 Barrett 최적화 방식을 사용하였으며, 내부 정수 곱셈기를 필요 결과비트에 따라 다르게 구성하여 최적화 하였다. 또한 modulus 를 통해 나누는 수가 2 의 거듭제곱으로 표현이 가능한 solinas 정수인 경우, 곱셈기와 덧셈기가 필요한 DSP 슬라이스 대신 덧셈기와 쉬프트 연산을 통해 정수 곱셈이 가능하다는 것을 보여주어 특별한 나누는 수에 대한 최적화 방법도 제안하였다.

또한 동형암호의 암호문 곱셈 연산에서 주로 사용되는 NTT(Number Theoretic Transform)을 FPGA 기반으로 가속하는 연구도 있다[4]. 이는 두 개의 다항식에 대한 곱셈 연산을 수행하는 경우, 두 다항식 계수들의 컨볼루션 연산으로 곱셈 연산을 치환하고, 이를 DFT(Discrete Fourier Transform)와 유사한 연산 방식으로 정수에 대해 연산을 수행하는 것이다. 이러한 방식은 기존 DFT 연산처럼 복잡한 Butterfly Unit 연산이 수행된다. 하지만 동형암호 연산에서는 다항식의 계수가 상당히 크기 때문에 하나의 스테이지를 연산한 후 발생하는 중간 연산 데이터에 대한 처리가 중요한 이슈이다. 이 논문에서는 이러한 중간 연산 데이터의 입출력 및 관리를 위해 전체 파이프라인 방식으로 NTT 연산을 구현하였다. 이는 연산 순서 조정을 위한 재배열 모듈이 포함되어 회로 복잡도를 증가시키지만, 데이터가 큰 동형암호 연산을 위한 방법으로 새로운 방향성을 제시하였다.

4. 결론

본 논문에서는 암호화된 상태로 연산이 가능한 동형암호 알고리즘의 응용에서 어려움 중 하나인 연산 속도를 가속하기 위한 FPGA 기반의 하드웨어 가속기 연구들의 동향을 살펴보았다. 특히 다항식 곱셈에 대한 연구들이 주로 이루어지고 있으며, 아직 동형암호를 응용하기 위해서는 많은 연구들이 남아있는 것으로 생각된다. 앞으로도 이러한 동형암호 가속기에 대한 연구가 지속된다면, 동형암호 알고리즘을 통한 헬스케어 정보 및 DNA 분석 시스템에 응용할 수 있을 것으로 기대된다.

ACKNOWLEDGEMENT

이 논문은 2021 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구이며 (No.2018-0-00230, (IoT 총괄/1 세부) IoT 디바이스 자율 신뢰보장 기술 및 글로벌 표준기반 IoT 통합보안 오픈 플랫폼 기술개발 [TrusThingz 프로젝트]), (No.2020-0-00325, 클라우드 엣지 전주기 데이터 안정성을 위한 추적성 보장 기술 개발), 2021 년도 BK21 FOUR 정보기술 미래인재 교육연구단의 지원을 받았으며, 2021 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2020R1A2B5B03095204).

참고문헌

[1] Salavi, et al. "A survey of various cryptographic techniques: From traditional cryptography to fully homomorphic encryption." Innovations in Computer Science and Engineering. Springer, Singapore, 2019. 295-305.

[2] Alharbi, et al. "Survey on Homomorphic Encryption and Address of New Trend." Int. J. Adv. Comput. Sci. Appl 11.7 (2020): 618-626.

[3] Kim, Sunwoong, et al. "FPGA-based Accelerators of Fully Pipelined Modular Multipliers for Homomorphic Encryption." 2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig). IEEE, 2019.

[4] Kim, Sunwoong, et al. "Hardware architecture of a number theoretic transform for a bootstrappable rns-based homomorphic encryption scheme." 2020 IEEE 28th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM). IEEE, 2020.