짧은 정수해 문제들 사이의 관계를 통한 암호시스템의 공격 가능성

구자현*, 노종선*
*서울대학교 전기정보공학부 뉴미디어통신공동연구소
*bravokoo@ccl.snu.ac.kr, *jsno@snu.ac.kr

Possibility of attacking cryptosystem through the relationship between short intger solution problems

Zahyun Koo*, Jong-Seon No*
*INMC, Department of ECE, Seoul National Univ.

요 약

본 논문은 환 상에서 정의된 짧은 정수해 문제 (RSIS)와 모듈상에서 정의된 짧은 정수해 문제 (MSIS)의 관계를 소개하고 이를 통해 암호 시스템의 공격 가능성에 대해 살펴본다. 두 문제 사이의 관계는 특정 매개변수들에 의해 성립되기에 암호시스템이 특정 매개변수들 사이의 관계를 만족하는지 확인하였다..

Ⅰ. 서 론

많은 암호시스템은 큰 정수의 소인수분해가 어렵다는 점을 기반으로 만들어진 RSA, 타원곡선을 기반으로 구성된 Elliptic Curve Cryptography (ECC) 등이 있다. 특히, 위 암호시스템들은 슈퍼컴퓨터로도 오랜 시간이 걸리기 때문에 안전하다는 평가를 받고 있다. 하지만 최근 양자컴퓨터의 개발로 인해 슈퍼컴퓨터로도 오랜 시간이 걸려야 풀 수 있는 문제들도 암호시스템을 위협할 만큼 빠른 시간안에 풀 수 있게 되었다. 이에 따라 많은 암호학자들은 양자컴퓨터에도 안전한 암호시스템을 구축하기 위해 많은 노력을 기울이고 있으며, 그 중에서 유력한 후보군으로는 격자 기반 암호, 부호 기반 암호, 그리고 다변수 다항식 기반 암호가 있다. 세 후보군 중에서 격자 기반 암호가 가장 유력한 차세대 암호시스템으로 고려되고 있다.

격자 기반 암호는 격자 상에서 정의된 문제인 Shortest Vector Problem (SVP), Shortest Independent Vector Problem (SIVP)등을 기반으로 만들어진 암호시스템이다. 하지만, 두 문제들은 1998년도 Ajtai에 의해 Short Integer Solution Problem (SIS)로 Reduction이 되며 ([1]), 2005년도 Regev에 의해 Learning with Error (LWE)로 Reduction이 되었다 ([2]). 이에 따라 최근 격자 기반 암호 시스템은 SIS문제와 LWE 문제를 기반으로 만들어지고 있는 추세이다. 하지만 두 문제를 기반으로 만드는 과정에서 Key의 크기가 크며, 비효율적인 측면이 있다. 이를 극복하기 위해 수학적인 구조인 환 (Ring) 과 모듈 (Module)을 도입하여 Ring-SIS (RSIS), Module-SIS (MSIS), Ring-LWE (R-LWE) 그리고 Module-LWE (M-LWE)를 정의하였다. 일반적으로 Module 상에서 정의된 문제가 Ring 상에서 정의된 문제보다 어렵다는 것이 알려져 있다. 따라서 많은 암호시스템은 Module상에서 정의된 문제 MSIS와 M-LWE 문제를 기반으로 만들어지며 Ring상에서 정의된 문제를 푸는 알고리즘의 존재성에 대해 고려하지 않아도 된다. 하지만, 최근 연구에서는 특정 매개변수에 대해 Ring 상에서 정의된 문제가 어렵다는 결과들이 있다.

본 논문에서는 MSIS와 RSIS 간의 관계를 소개하며, 이를 통해 암호시스템의 공격 가능성에 대하여 살펴본다. 특히, 두 문제의 관계를 통해 나타나는 특정 매개변수가 암호시스템과 부합하는지 확인을 한다. 이로 인해 Ring상에서 정의된 문제들을 푸는 알고리즘의 존재성에 대해 완벽하게 배제할 수 없음을 나타낸다.

Ⅱ. 본론

Ⅱ-1. RSIS문제와 MSIS 문제간의 관계

환(Ring)구조를 갖는 격자 상에서 정의된 문제인 Ring Short Integer Solution Problem (RSIS)문제는 다음과 같이 정의한다.

정의) ($RSIS_{q,m,\beta}$문제)
주어진 $a_1,...,a_m \in Z_q[X]/\langle X^n+1\rangle$ 를 균등분포에서 독립적으로 뽑았을 때, $\sum_{i=1}^{m} a_i \cdot z_i = 0 \bmod q$와 어떤 β에 대해 $0 < \| z \| \le \beta$ 를 만족하는
$z = (z_1,...,z_m) \in (Z[X]/\langle X^n+1\rangle)^m$을 찾는 문제이다

마찬가지로 모듈 (Module) 구조를 갖는 격자상에서 정의된 Module Short Integer Solution Problem (MSIS) 문제는 다음과 같이 정의한다.

정의) ($MSIS_{q,m,\beta}$문제)
주어진 $a_1,...,a_m \in (Z_q[X]/\langle X^n+1\rangle)^d$ 를 균등분포에서 독립적으로 뽑았을 때, $\sum_{i=1}^{m} a_i \cdot z_i = 0 \bmod q$와 어떤 β에 대해 $0 < \| z \| \le \beta$ 를 만족하는
$z = (z_1,...,z_m) \in (Z[X]/\langle X^n+1\rangle)^m$을 찾는 문제이다

일반적으로 MSIS 문제를 푸는 알고리즘이 존재한다면 RSIS 문제는 MSIS문제의 Rank가 1인 경우이기 때문에 자연스럽게 풀 수 있다. 다음 명제는 특정 매개변수에서는 RSIS 문제가 MSIS 문제보다 더 어렵다는 사실을 내포하고 있다 ([3]). 하지만 RSIS의 해들의 유계인 β에 대해 특정한 Constraint가 생기게 된다.

정리 ([3])) ($MSIS_{q^k,m^k,\beta'}$문제를 $RSIS_{q,m,\beta}$로 환원)

m과 $k>1$ 이 정수이고, q를 소수라 하자. 그리고 다음 조건을 만족하는 Module의 Rank d를 선택하자.

$$\sqrt{nm}\,q^{\frac{1}{m}} < \sqrt[2d-1]{q/(\sqrt{m})^{d-1}}$$

그리고 β를 다음과 같이 선택하자.

$$\sqrt{nm}\,q^{\frac{1}{m}} \le \beta < \sqrt[2d-1]{q/(\sqrt{m})^{d-1}}$$

이 때, 만약 $RSIS_{q,m,\beta}$를 푸는 알고리즘 A가 존재하면 $MSIS_{q^k,m^k,\beta'}$를 푸는 알고리즘 A'이 존재한다. 이 때, $\beta' = m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)}$ 이다.

Ⅱ-2. RSIS문제와 MSIS 문제간의 관계를 통한 암호시스템 공격 가능성.

일반적으로 암호시스템을 구성하는 방법은 다음과 같다.

주어진 문제 P를 기반으로 하는 암호시스템 A에 대해 만약 A를 푸는 알고리즘 T가 존재한다면 이 알고리즘 T를 이용하여 P를 푸는 알고리즘 T'을 만들 수 있다.

이 때, 암호시스템의 안전성을 위해 문제 P는 NP문제로 설정한다. 즉 암호시스템이 깨지게 되면 NP문제가 깨진다는 명제를 통해 암호알고리즘을 설계한다.

우리는 암호 알고리즘 중 [4]의 알고리즘인 RingCT V2.0을 통해 MSIS와 RSIS 간의 관계를 통한 공격가능성에 대하여 알아본다. RingCT V2.0 암호시스템이 사용하는 매개변수들은 다음과 같다.

Rank d	2	3
Modulus q	$\approx 2^{196}$	$\approx 2^{196}$
Instances 수 m	132	132
Ring Dimension n	2^{10}	2^{10}
Upper bound β	$\approx 2^{126}$	$\approx 2^{126}$
$\sqrt{nm}\,q^{\frac{1}{m}}$	≈ 1029.01	≈ 1029.01
$\sqrt[2d-1]{q/(\sqrt{m})^{d-1}}$	$\approx 2059.98\times 10^{16}$	$\approx 2378.26\times 10^{8}$

따라서 RingCT V2.0의 알고리즘에 대한 매개변수들은 위 정리의 매개변수의 조건들을 만족하게 된다. 특히, $k=2, d=2$ 에 대해서 RSIS의 유계인 γ에 대해 $132^{\frac{k}{2}(d-1)}\gamma^{k(2d-1)} = 2^{126}$을 풀면 $\gamma \approx 9293.93\times 10^2$가 나오게 된다. 즉, Modulus $\approx 2^{98}$, Instance = 132, Upper bound $\approx 9293.93\times 10^2$를 매개변수로 갖는 RSIS를 푸는 알고리즘이 존재할 때, RingCT V2.0을 푸는 알고리즘에 존재할 가능성이 생기게 된다. 따라서 RingCT V2.0이 더욱 안전하다는 것을 보이기 위해서는 RSIS를 푸는 알고리즘의 존재성을 완벽하게 배제할 수 없다.

Ⅲ. 결론

본 논문에서는 격자 상의 문제인 MSIS와 RSIS를 소개하였고 특정 매개변수에 대해서 두 문제 사이의 관계를 소개하였다. 일반적으로 MSIS문제가 RSIS문제 보다 어렵다고 알려져 있다, 이로 인해 MSIS기반으로 만든 문제는 RSIS를 푸는 알고리즘의 존재성에 대해 고려하지 않았다. 하지만 특정 매개변수에서는 RSIS문제가 MSIS문제보다 어려울 수 있기 때문에 MSIS를 기반으로 만든 문제들에 대해서도 RSIS 문제를 푸는 알고리즘의 존재성에 대해 고려해야할 필요가 있다.

ACKNOWLEDGMENT

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00400, 저사양 디바이스 대상 고효율 PQC 안전성 및 성능 검증 기술 개발)

참 고 문 헌

[1] Ajtai, Miklós. "Generating hard instances of the short basis problem." International Colloquium on Automata, Languages, and Programming. Springer, Berlin, Heidelberg, 1999.

[2] Regev, Oded. "On lattices, learning with errors, random linear codes, and cryptography." Journal of the ACM (JACM) 56.6 (2009): 1-40

[3] Koo, Zahyun, Jong-Seon No, and Young-Sik Kim. "Reduction From Module-SIS to Ring-SIS Under Norm Constraint of Ring-SIS." IEEE Access 8 (2020): 140998-141006.

[4] Torres, Wilson Alberto, et al. "Lattice RingCT V2. 0 with multiple input and multiple output wallets." Australasian Conference on Information Security and Privacy. Springer, Cham, 2019