# CROSS 암호 기반 문제 R-SDP 및 R-SDP(G)의 특성에 따른 효율성과 보안성

이창열, 손일권, 이원혁

한국과학기술정보연구원

{lcy253898, d2estiny, livezone}@kisti.re.kr

# Efficiency and Security of the CROSS-based Cryptographic Problems R-SDP and R-SDP(G) According to their Characteristics

ChangYeol Lee, IlKwon Sohn, Wonhyuk Lee

Korea Institute of Science and Technology Information

요 약

양자 컴퓨터의 발전으로 기존 공개키 암호체계의 보안이 위협받음에 따라, 양자내성암호로의 전환이 필수 과제로 부상하였다. 이에 대응하기 위해서 NIST의 추가 서명 알고리즘 후보로 제안된 CROSS는, 전통적인 코드 기반 암호의 높은 안전성은 유지하면서 실용성을 개선하기 위해서 기존의 SDP에 구조적 제한을 의도적으로 부가한 R-SDP와 R-SDP(G)를 통하여 해결한다. 본 논문은 CROSS의 기반 문제인 R-SDP와 R-SDP(G)에 의도적으로 부가된 '구조적 제한'이 암호 시스템에 미치는 보안성과 효율성 그리고 추가된 방식에 의해 발생할 수 있는 문제점에 대하여 분석한다.

## Ⅰ. 서 론

양자 컴퓨터의 가능성에 따라서 Shor's Algorithm과 Grover's Algorithm과 같은 강력한 알고리즘이 연구 되어 왔다. 특히 Shor's Algorithm은 공개키 암호의 구조에 대하여 다항 시간 내에 공격할 수 있으며, Grover's Algorithm은 대칭키 암호의 유효 보안 강도를 감소시키고 다양한 암호에 대한 공격을 가속화 할 수 있어, 현대 보안에 잠재적 위협이 되고 있다. 이러한 위협에 대응하기 위해, 양자 컴퓨터로부터 안전한 양자내성암호(Post-Quantum Cryptography, PQC)로의 전환은 필수적이다. 이에 미국 국립표준기술연구소(NIST)는 양자내성암호를 표준화 하고자 했으며, 그 결과로 KEM(Key Encapsulation Mechanism)으로 CRYSTALS-Kyber, HQC를, 디지털 서명으로는 CRYSTALS-Dilithium, FALCON, SPHINCS+를 표준으로 선정했다.

그러나 NIST는 표준으로 선정된 서명 알고리즘의 격자(Lattice) 기반 문제에 대한 높은 의존도를 낮추고 기반 문제를 다양화하고자 추가 서명 알고리즘 표준화 절차를 공모했다. 이 과정에서 제안되어 현재 2라운드 후보로 선정된 CROSS(Codes and Restricted Objects Signature Scheme)는, 코드 기반 암호(Code-based Cryptography)에 속한다[1]. 코드 기반 암호는 오랜 연구를 통해서 안전성을 신뢰받는 암호이지만, 키 및 서명의 크기가 크다 보니 상대적으로 느린 연산 속도라는 문제를 지니고 있다. 이를 해결하고자 CROSS는, 기존의 Syndrome Decoding Problem(SDP)에 의도적으로 구조적 제한을 가한 Restricted Syndrome Decoding Problem(R-SDP)와 Restricted Syndrome Decoding Problem with subgroup G(R-SDP(G))라는 사용한다. 이러한 방식은 SDP의 수학적 난이도는 보존하면서, 기존의 성능 문제를 해결하고 실질적인 공격에 대한 높은 보안 강도의 핵심 요소로 작용한다.

본 논문에서는 CROSS의 핵심 설계 요소인 의도적인 구조적 제한이 암호에 미치는 영향을 분석하고자 한다. 먼저 이러한 제한이 어떻게 실질적인 공격에 대한 높은 보안 강도를 향상 시키고, 계산 효율성과 프로토콜 간소화에 어떻게 기여하는지를 서술한다. 이와 동시에, 효율성을 위해 도입된 구조가 역설적으로 기반문제에 대한 공격 가능성을 제공하는 Trade-Off 관계를 조명하고, 실제 공격 사례를 소개하고자 한다. 이를 통해 R-SDP 및 R-SDP(G)를 기반한 CROSS가 가진 장점과 내재한 위험을 종합적으로 이해하는 것을 목표로 한다.

## Ⅲ.본론

CROSS 암호는 R-SDP와 R-SDP(G)의 수학적 난이도를 바탕으로 한 암호 알고리즘이다[]. R-SDP와 R-SDP(G) 모두 SDP의 NP-Complete의 수학적 난이도를 그대로 유지하면서 표 1과 같이 오류 벡터 e에 특정한 구조적 제한을 의도적으로 부가한다.

| 문제 이름 | 구조적 제한 |
|---|---|
| R-SDP | $E=\{g^i \mid i\in\{1,\ldots,z\}\}\subset F_p^*, e\in E^n$ |
| R-SDP(G) | $G=\langle a_1,\ldots,a_m\rangle, \text{for}\, a_i\in E^n, e\in G$ |

표 1 R-SDP와 R-SDP(G)의 구조적 제한

이러한 구조적 제한을 추가한 R-SDP와 R-SDP(G)는 향상된 보안 강도를 보인다. 이때 향상된 보안 강도란 이론적 난이도의 변화가 아닌, 실질적인 공격에 대한 난이도 증가에 기인한다. 이론적 난이도 관점에서 SDP와 R-SDP,R_SDP(G)는 모두 NP-Complete라는 동일한 난이도를 보이지만, 부가된 오류 벡터의 구조적 제한을 통해서 Information-Set Decoding(ISD)와 같은 가장 효율적인 공격 알고리즘의 성능을 저하시키는 핵심적인 역할을 한다[2]. 또한 오류 벡터 e를 구성하는 희소 벡터 m을 생성할 때, 최신 부분합 공격에 강한 내성을 갖도록 파라미터를 신중하게 선택한다. 이러한 요인들이 종합적으로 작용하여 기존 SDP보다 실질적인 공격에 대하여 더 높은 보안 강도를 보인다.

다음으로 암호화 및 복호화 과정에서 필요한 계산을 제거하거나 축소하여 계산의 효율성을 보인다.

먼저 일반적으로 사용하는 표준 코드 기반의 영지식 증명 프로토콜은 오류 벡터 e의 구조가 노출되지 않도록 하기위해서 순열 연산을 필수적으로 사용하여 암호를 구성해야 한다. 하지만 이러한 방식은 증명자가 매 라운드마다 비밀 벡터의 좌표를 무작위로 섞기 위해 새로운 순열을 생산하고, 순열에 대한 약속(commitment)을 전송해야 한다. 이러한 과정은 계산이 복잡하여 실질적인 성능저하의 주된 요인으로 작용한다. 반면 R-SDP와 R-SDP(G)을 기반으로 하는 영지식 증명 프로토콜의 경우 이러한 문제를 근본적으로 해결한다. 비밀 정보에 해당하는 고정된 오류 벡터 e를 사용하는 것이 아니라, 서명할 메시지로부터 매번 새로운 오류 벡터를 생성한다. 이처럼 서명할 때마다 새로운 변수를 생성하기 때문에 기존의 방식인 순열을 사용한 연산을 할 필요가 없어진다. 결과적으로, 계산 비용이 많이 필요한 순열 연산을 배제하면서도 같은 보안 강도를 유지하고, 한층 더 간결한 프로토콜이 구현 가능하다.

또한 R-SDP와 R-SDP(G)는 기반으로 하는 SDP에 비하여 본질적인 계산 효율성 측면에서 이점을 보인다. 이러한 이점의 근원은, 파라미터 값을 더 작게 설정해도 동일한 보안 강도를 달성할 수 있다는 점에 있다. 즉, 일반적으로 SDP를 구성하는 파라미터에 해당하는 패리티 검사 행렬(H), 오류 벡터(e) 그리고 신드롬의 값(s)을 크기를 감소시키는 것을 의미한다. 이처럼 객체의 크기가 줄어듦에 따라서 키 생성, 서명, 검증 과정에 필요한 행렬-벡터 곱셈과 같은 기본 연산의 부담이 직접적으로 줄어든다. 이러한 효율성은 CROSS가 다른 코드 방식 암호와 비교하여 같은 수준의 서명 크기를 가지면서 서명 속도가 빠르다는 특징으로 나타난다.

앞서 서술한 R-SDP와 R-SDP(G)에 대한 여러 장점에도 불구하고, 오류 벡터 e에 부가된 구조적 제한 자체가 잠재적 단점을 일으킬 수 있는 Trade-off 관계를 가진다. 구조적 제한은 단계적으로 부가되는데, 일반적인 SDP에서 첫 제약을 가한 방식이 R-SDP가 되고, 여기에 추가적인 $(G)$라는 대수적 구조를 더하여 R-SDP(G)가 된다. 이러한 구체적인 제약에 해당하는 대수적 구조가 새로운 공격 경로를 생성하는 단점으로 작용할 수 있다. 자세히 설명하자면, 일반 SDP나 R-SDP와 달리, R-SDP(G)의 오류 벡터는 반드시 $e = m \cdot G$ 라는 선형 결합으로 생성되어야 하는 제약을 갖는다. 이러한 추가 제약 $(G)$는 공격자에게 핵심 힌트로 작용하여, $(G)$의 구조를 통해서 공격할 기회를 제공하게 된다. 이에 대표적인 연구로 2024년 Ward Beullens 등은 $(G)$의 구조를 충돌 공격(Collision Attack)하는 방식을 발표했다[3]. 해당 논문의 공격은 $(G)$ 구조에 특화된 공격으로 $(G)$구조가 없는 R-SDP에는 적용할 수 없지만, R-SDP(G)의 경우 취약점으로 간주 된다ㄴ. 결과적으로 이러한 공격은 ISD 저항성만을 고려하는 것이 아닌, 추가적인 보안 분석을 요구하기 때문에 파라미터 설정을 더욱 복잡하게 만드는 요인으로 작용한다.

## Ⅲ. 결론

본 논문에서는 NIST의 추가 서명 알고리즘 후보인 CROSS의 핵심 요소, 즉 기반 문제에 의도적으로 가해진 구조적 제한이 가지는 영향에 대해 서술하였다. 본론의 내용과 같이, 구조적 제한을 통해서 실질적인 공격에 대하여 난이도를 증가 시키고 최신 공격에 대응할 수 있도로 파라미터 선택에 있어서 신중을 기해야 하는 것을 확인했다. 또한 코드 기반 암호의 고질적인 문제였던 키 크기와 서명 크기를 해결하여 연산 속도를 효과적으로 해결했으며, 연산 비용이 많이 사용해야 하는 순열 연산을 제거한 영지 증명 프로토콜을 만들어 서명 속도를 크게 향상시켰다.

하지만 이러한 추가적인 구조는 또 다른 분석 가능성이 제시될 수 있다. 특히 대수적 구조가 추가된 R-SDP(G)의 경우, 일반 SDP 문제에는 적용되지 않는 충돌 공격과 같은 새로운 공격이 가능하다는 문제가 존재하며, 이는 암호의 보안성에 위협이 될 수 있다.

결론적으로, CROSS는 구조적 제한이라는 독착적인 방법을 통해서 코드 기반 서명을 실용성을 보인 서명 알고리즘 후보임이 분명하다. 하지만 이러한 방식은, 양자내성암호로서의 안전성에 대한 문제가 될 수 있다. 향후 표준화 과정에서 이러한 구조적 특성에 대한 검증이 성공적으로 이루어 진다면, 신뢰성 있는 양자내성암호로 자리매김할 수 있을 것이다.

## ACKNOWLEDGMENT

본 연구는 2025년도 과학기술정보통신부의 제원으로 한국연구재단 양자컴퓨팅 기반 양자이득 도전 연구사업(RS-2023-00256221)의 지원을 받아 수행된 연구임

## 참 고 문 헌

[1] Baldi, Marco, et al. "Codes and Restricted Objects Signature Scheme." Submission to the NIST Post-Quantum Cryptography Standardization Process. Algorithm Specifications and Supporting Documentation. Version (2025).

[2] Stern, J. (1988, November). A method for finding codewords of small weight. In International colloquium on coding theory and applications (pp. 106-113). Berlin, Heidelberg: Springer Berlin Heidelberg.

[3]Beullens, Ward, Pierre Briaud, and Morten Øygarden. "A security analysis of restricted syndrome decoding problems." Cryptology ePrint Archive (2024).