KpqC 코드기반 알고리즘 안전성 분석

Jon-Lark Kim

November 14, 2023

Department of Mathematics

Sogang University, S. Korea

Contents

KpqC 코드기반 알고리즘 안전성 분석

1. BBB+, BBC+ 알고리즘

1. BBB+, BBC+ 알고리즘

●BBB+ 알고리즘

- 랭크 거리 기반 코드에 적용할 수 있는 랭크 거리 코드 복호화 문제 알고리즘.
- 2020년 EUROCRYPT 2020에 소개된 An Algebraic Attack on Rank Metric Code-Based Cryptosystem[1] 논문에서 M. Bardet et al.에 의해 제안됨.
- T. Lange et al.이 해당 논문에서 소개된 decoding을 사용하면 Layered ROLLO-1와 REDOG 암호 알고리즘의 계산 복잡도가 감소한다고 제안함.
- 랭크 거리 복호화 문제를 다변수 방정식 시스템으로 변경하고, Grobner-basis 방법을 사용하여 해를 찾는 원리를 이용함.
- 코드와 오류의 길이, 차원, 랭크 등에 따라 regularity의 degree를 찾는 것이 중요함.

---

1) M. Bardet, P. Briaud, M. Bros, P. Gaborit, V. Neiger, O. Ruatta, & J. P. Tillich, (2020, May). An algebraic attack on rank metric code-based cryptosystems. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 64-93). Cham: Springer International Publishing.

1. BBB+, BBC+ 알고리즘

●BBB+ 알고리즘

- $m\binom{N-l-1}{t}+1 \geq \binom{N}{t}$ 조건을 만족하는 경우의 complexity는 다음과 같음.

$$\mathcal{O}\left(\left(\frac{((m+N)t)^t}{t!}\right)^\omega\right)$$

- $m\binom{N-l-1}{t}+1 \geq \binom{N}{t}$ 조건을 만족하지 않는 경우의 complexity는 다음과 같음.

$$\mathcal{O}\left(\left(\frac{((m+N)t)^{t+1}}{(t+1)!}\right)^\omega\right)$$

1. BBB+, BBC+ 알고리즘

●BBC+ 알고리즘

- BBB+를 개선하여 M. Bardet et al.이 새롭게 제안한 랭크 거리 코드 복호화 알고리즘
- 2020년 ASIACRYPT 2020에 소개된 Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems[2] 논문에서 M. Bardet et al.에 의해 제안됨.
- T. Lange et al.이 해당 논문에서 소개된 decoding을 사용하면 Layered ROLLO-1와 REDOG 암호 알고리즘의 계산 복잡도가 감소한다고 제안함.
- 다양한 조건에 따라 BBC+-1, BBC+-2, BBC+-3, BBC+-4의 4가지 식이 존재하며 각각은 최종 방정식 시스템의 크기와 매개변수에 의존함.

---

2) M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. Perlner, D. Smith-Tone, J. P. Tillich, and J. Verbel, 2020. Improvements of algebraic attacks for solving the rank decoding and MinRank problems. In *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part I 26* (pp. 507-536). Springer International Publishing.

1. BBB+, BBC+ 알고리즘

●BBC+ 알고리즘

- 시스템을 선형화 하기 위해 방정식에 일부 homogeneous 방정식을 곱하는 과정에서 q=2인 경우에 더 작은 b 값에서 오는 homogeneous 방정식을 고려해야 함.

- 이를 위해 아래와 같이 세 가지 표기법을 사용함. (BBC+-3, BBC+-4에 사용)

$$A_b := \sum_{j=1}^{b} \binom{N}{t} \binom{ml+1}{j},$$

$$B_b := \sum_{j=1}^{b} \left(m \binom{N-l-1}{t} \binom{ml+1}{j} \right) \text{ and}$$

$$C_b := \sum_{j=1}^{b} \left((-1)^{s+1} \binom{N}{t+s} \binom{m+s-1}{s} \binom{ml+1}{j-s} \right).$$

1. BBB+, BBC+ 알고리즘

●BBC+ 알고리즘

- BBC+-1의 complexity는 다음과 같음.

$$\mathcal{O}\left(m\binom{N-\ell-1}{t}\binom{N}{t}^{\omega-1}\right)$$

- BBC+-2의 complexity는 다음과 같음.

$$\mathcal{O}\left(q^{jt}m\binom{N-\ell-1}{t}\binom{N-j}{t}^{\omega-1}\right)$$

- BBC+-3의 complexity는 다음과 같음.

$$\mathcal{O}\left((m\ell+1)(t+1)A_b^2\right)$$

- BBC+-4의 complexity는 다음과 같음.

$$\mathcal{O}\left((B_b+C_b)A_b^{\omega-1}\right)$$

1. BBB+, BBC+ 알고리즘

●T. Lange et al. 이 적용한 BBC+ 알고리즘 코드

- T. Lange et al.은 2023년 8월 9일 on the security of REDOG 문서와 2023년 9월 5일 Analysis of Layered-ROLLO-1 문서를 통해 BBC+ 알고리즘을 적용한 경우의 cost를 계산하여 제시함.
- 그들이 제공한 sage 파일에서 C_b에 해당하는 식은 다음과 같이 쓰여 있음.

```
def C_b(NF,RF,MF,KF,b):
    return sum(sum((-1)^s+i * binomial(NF, RF+s) * binomial(MF + s - 1, s) *
```

- 그러나, C_b에 해당하는 식의 원래 형태는 다음과 같음.

$$C_b := \sum_{j=1}^{b} \left((-1)^{s+1} \binom{N}{t+s} \binom{m+s-1}{s} \binom{ml+1}{j-s} \right).$$

- 따라서 다음과 같이 변경하였음.

```
def C_b(NF,RF,MF,KF,b):
    return sum(sum((-1)^(s+1) * binomial(NF, RF+s) * binomial(MF + s - 1, s)
```

2. Layered ROLLO-1

2. Layered ROLLO-1

●Layered ROLLO-1 파라미터 연구

- T. Lange et al.은 2023년 9월 5일 Analysis of Layered-ROLLO-1 문서에서 각 security level별 cost를 다시 계산하여 공지하였으나, 해당 식에 오류를 발견한 Layered-ROLLO-1 연구팀이 아래와 같이 식을 수정하여 다시 계산하였음.

$$C_b := \sum_{j=1}^{b} \sum_{i=1}^{j} \left((-1)^{i+1} \binom{n}{r+i} \binom{m+i-1}{i} \binom{mk+1}{j-i} \right)$$

For the latter, it leads to a complexity of

$$\mathcal{O}\left((B_b + C_b) A_b^{\omega-1}\right)$$

[ASIACRYPT 2020]

```
def C_b(NF,RF,MF,KF,b):
    return sum(sum((-1)^s+i * binomial(NF, RF+s) * binomial(MF + s - 1, s) * binomial(MF * KF
```

Corrected

[Tange, et.al,

```
#Wrong point
def C_b(NF,RF,MF,KF,b):
    return sum(sum((-1)^(s+1)* binomial(NF, RF+s) * binomial(MF + s - 1, s) * binomial(MF
```

2. Layered ROLLO-1

●Layered ROLLO-1 파라미터 연구

- 아래의 표는 Layered-ROLLO-1 연구팀이 식을 수정하여 다시 계산한 결과는 BBC+(corrected)로, 기존에 T. Lange et al.이 제시한 결과는 BBC+(announced)로 표기한 결과임.

- 기존에 T. Lange et al.이 BBC+알고리즘을 적용한 경우가 가장 cost가 작게 나와 해당 값을 기입하였으며, Layered-ROLLO-1 팀은 동일한 알고리즘을 수정하여 재계산한 결과를 제시하였음.

security level	new (q, n_1, n_2, m, r, d)	BBC+(announced)	BBC+(corrected)
modified-128	(2,37,61,67,6,2)	93.68	113.78
modified-192	(2,43,71,79,7,3)	106.28	154.71
modified-256	(2,53,103,97,7,3)	114.1	167.81
new-128	(2,37,61,67,7,2)	102.14	186.82
new-192	(2,43,71,79,9,3)	119.1	318.49
new-256	(2,53,103,97,12,3)	152.07	854.29

2. Layered ROLLO-1

●Layered ROLLO-1 파라미터 연구

- 본 연구팀은 BBC+ 알고리즘 이외에도 다른 알고리즘에 대한 결과들을 계산하여 결과를 분석해 보았음.

- 계산 결과 BBC+가 항상 최소 cost를 보이지 않았으므로, BBC+의 결과와 최소 cost를 보이는 알고리즘과 이에 해당하는 결과를 계산한 것은 아래와 같음.

security level	new (q, n_1, n_2, m, r, d)	BBC+ (layered)	lowest cost
modified-128	(2,37,61,67,6,2)	113.78	113.78 (BBC+)
modified-192	(2,43,71,79,7,3)	154.71	154.71 (BBC+)
modified-256	(2,53,103,97,7,3)	167.81	162.79 (BBB+)
new-128	(2,37,61,67,7,2)	186.82	151.14 (BBB+)
new-192	(2,43,71,79,9,3)	318.49	200.46 (BBB+)
new-256	(2,53,103,97,12,3)	854.29	271.44 (BBB+)

2. Layered ROLLO-1

●Layered ROLLO-1 파라미터 연구

- 결과적으로, 올바르게 수정한 식을 사용하여 계산한 BBC+ 알고리즘의 cost 결과값이 T. Lange et al.의 결과보다 좋게 나타났음.
- 또한, BBC+ 알고리즘이 항상 최소의 cost값이 나타나지 않는다는 것을 확인할 수 있었음. Layered-ROLLO-1 팀이 제시한 new-128, new-192, new-256의 경우 BBB+ 알고리즘으로 계산한 cost가 더 작게 나타났음.
- 그럼에도 불구하고, 제시된 security level은 만족하는 것으로 나타났음.
- 각 파라미터를 조정하여 암호시스템의 securit를 확인하는 경우, BBC+ 뿐만 아니라 다른 랭크 거리 코드에 대한 복호화 알고리즘의 복잡도를 전부 고려하여 최솟값을 확인하는 것이 필요함.

3. PALOMA

3. PALOMA

●PALOMA의 복호화 방법 연구

- PALOMA 암호 알고리즘은 extended version을 구현하여 복호화 알고리즘으로서 사용하고 있음.
- Patterson decoding 알고리즘은 irreducible Goppa code를 복호화 하는 알고리즘으로 separable Goppa code를 복호화하기 위해 기존의 알고리즘을 수정한 extended를 구현하여 사용함.
- Irreducible Goppa code를 복호화하는 또 다른 알고리즘으로 Berlekamp-Massey 알고리즘이 있음. 해당 알고리즘은 Classic McEliece 암호 알고리즘에 사용되고 있으며, BCH 코드와 Reed-Solomon 코드 등의 복호화에도 사용하고 있음.
- 기존 논문들 중 Berlekamp-Massey algorithm을 사용하여 binary separable Goppa code를 복호화한 결과가 있으며, irreducible Goppa code와 separable Goppa code를 McEliece Cryptosystem에 적용해서 비교해 본 결과가 있음.
- 따라서 Berlekamp-Massey 알고리즘의 적용 또한 고려해 볼 필요가 있음.

●Binary separable Goppa code의 특성과 다항식 $g(X)$

- PALOMA 암호시스템은 separable Goppa code 생성을 위해 separable polynomial $g(X)$를 상수 시간 내에 생성함. 생성 방법은 다음과 같음

  ① 기저로 사용하는 $\mathbb{F}_{2^{13}}$ 필드에서 임의의 $n+t$개의 원소를 랜덤하게 추출함.

  ② 추출한 $n+t$개의 원소들 중 앞의 n개는 support set으로 두고, 뒤의 t개의 원소를 선택하여, t개의 원소들을 근으로 갖는 degree가 t인 Goppa polynomial g(X)를 생성함.

- 이 경우, $g(X)$의 근이 되는 t 개의 α_j들이 어떻게 선택되는지에 따라 다음과 같은 문제가 발생할 수 있음.
  - 예를 들어, t 개의 α_j들이 모두 conjugate한 원소들이라고 가정
  - 이러한 경우, $g(X)$가 어떤 α_j의 minimal polynomial과 동일하게 됨.
  - Minimal polynomial $g(X)$가 $\mathbb{F}_2$에서 irreducible polynomial이 되므로, 기존의 classic Goppa code의 generator로 사용할 수 있어 결과적으로 기존 Goppa Code에 대한 문제로 reduce가 가능함.

- 위와 같이 α_j들이 서로 conjugate해 지는 경우 reduce가 가능하므로 이 경우를 고려하여 $g(X)$를 선택해야 함.

4. REDOG

4. REDOG

●REDOG에 대한 복호화 실패 연구

- T. Lange et al.은 2023년 8월 9일 on the security of REDOG 문서에서 λ-dimensional subspace 문제와 복호화 실패 문제를 지적하였음.

- REDOG 암호시스템에서 key generation 과정 중 λ-dimensional subspace $\Lambda \subset \mathbb{F}_{q^m}$을 선택한 뒤 $S^{-1} \in GL_{n-k}(\Lambda)$가 만족하도록 S를 선택해야 하는데, 본 연구팀이 제시한 파라미터 중 일부는 $GL_{n-k}(\Lambda)$이 실제로 $GL_{n-k}(\mathbb{F}_{q^m})$ 의 subgroup이 되지 않아 문제가 발생함.

- 이를 해결하기 위해 m이 Λ의 차원을 의미하는 λ의 배수가 되도록 다음과 같이 조정하여 해결할 수 있음.

security level	original_parameter $(n,k,l,q,m,r,\lambda,t_1,t_2)$	new_parameter $(n,k,l,q,m,r,\lambda,t_1,t_2)$
128	(44, 8, 37, 2, 83, 18, 3, 9, 3)	(44, 8, 37, 2, 84, 18, 3, 9, 3)
192	(58, 10, 49, 2, 109, 24, 3, 12, 4)	(58, 10, 49, 2, 111, 24, 3, 12, 4)
256	(72, 12, 61, 2, 135, 30, 3, 15, 5)	(72, 12, 61, 2, 135, 30, 3, 15, 5)

●REDOG에 대한 파라미터 연구 – 본 연구팀의 방법

- 2023년 7월 13일에 제시된 오류 벡터 $e = (e_1, e_2)$에 대한 선택에 대한 문제에 대한 해결방안으로 본 연구팀은 $rk(e_1) = t_1 \leq \frac{r}{2}$, $rk(e_2) = t_2 \leq \frac{r}{2\lambda}$를 만족하도록 선택하는 것을 제안하였음.

- 그러나, Lange et al.의 계산은 잘못된 수식에 근거한 것이므로 해당 파라미터들에 대해 본 연구팀이 다시 계산하였으며 그 결과는 다음과 같음.

- Lange et al.이 계산한 cost는 Lange_cost로, 본 연구팀이 다시 계산한 cost는 recompute_cost로 표기하였으며 같은 파라미터를 사용하여 식을 수정한 결과를 표기하였음.

security level	parameter $(n, k, l, q, m, r, \lambda, t_1, t_2)$	Lange_cost	recomput_cost
128	(44, 8, 37, 2, 84, 18, 3, 9, 3)	114.8425	229.7623(BBB+)
192	(58, 10, 49, 2, 111, 24, 3, 12, 4)	143.3622	324.8804(BBB+)
256	(72, 12, 61, 2, 135, 30, 3, 15, 5)	173.2914	422.5785(BBB+)

●REDOG에 대한 파라미터 연구 – Lange et al.의 제안

- 2023년 8월 9일 T. Lange et al.은 파라미터 t_1, t_2를 설정하는 새로운 방법을 제시하였으며, 그들이 제시한 방법이 본 연구팀이 제시한 방법보다 cost가 크게 나타난다고 제안하였음.

- 그러나, Lange et al.의 계산은 잘못된 수식에 근거한 것이므로 해당 파라미터들에 대해 본 연구팀이 다시 계산하였으며 그 결과는 다음과 같음.

- Lange et al.이 계산한 cost는 Lange_cost로, 본 연구팀이 다시 계산한 cost는 recompute_cost로 표기하였으며 같은 파라미터를 사용하여 식을 수정한 결과를 표기하였음.

security level	parameter $(n, k, l, q, m, r, \lambda, t_1, t_2)$	Lange_cost	recomput_cost
128	(44, 8, 37, 2, 83, 18, 3, 15, 1)	128.3841	229.4455(BBB+)
192	(58, 10, 49, 2, 109, 24, 3, 21, 1)	163.9988	324.2406(BBB+)
256	(72, 12, 61, 2, 135, 30, 3, 27, 1)	199.0283	422.5785(BBB+)

5. 결론

5. 결론

●KpqC 공모전에 제안된 코드 기반 암호시스템

- Enhanced pqsigRM
  - NIST PQC competition이 진행될 때부터 제안되어 왔음.
  - 여러 번의 수정을 거치며 저널에도 게제되는 등 현재까지 유효한 attack이 없는 것으로 판명됨.
  - 서명 기법 알고리즘으로서 암호화 및 복호화 알고리즘과는 다소 차이가 있어 비교가 어려움.

- Modified Layered-ROLLO-1
  - 2023년 4월 첫 공격이 제시된 이후로 Lange et al.과 Pellegrini가 몇 번에 걸쳐 다양한 방식의 공격 제안.
  - 여러 번의 수정을 통해 security level을 만족하는 파라미터 제안
  - 알고리즘의 key size가 기존의 다른 알고리즘들에 비해 현저히 작아, 추가적인 검증을 통해 안전성을 확보하는 것이 필요해 보임.

5. 결론

●KpqC 공모전에 제안된 코드 기반 암호시스템

- PALOMA
  - Hamming 거리를 사용한 Classic McEliece 암호시스템과 비교하여 속도가 다소 빠른 등 장점이 존재함.
  - 그러나 키 사이즈가 크고, irreducible polynomial이 아닌 separable polynomia을 사용한 점 등에서 다양한 방면으로의 검증이 필요해 보임.
  - 비밀키 $g(X)$를 선택하는 과정에서 서로 conjugate한 근을 선택하는 경우 구조가 단순해질 수 있어 이에 대한 후속 연구가 필요함.

- REDOG
  - Lange et al.이 제안한 decoding failure와 λ-dimensional subspace에 대한 문제가 있었음.
  - 현재 해당 문제들에 대한 이론적인 해결 방법을 제시하였음.
  - 이에 해당하는 부분을 실질적인 코드로 구현해야 하는 작업이 필요함.
  - 코드 구현 과정을 진행하며 안전성을 추가로 검증해야 함.

감사합니다