2023 KpqC Winter Camp

Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature and Fast Verification for Post-Quantum Cryptography

2023년 2월 24일

노종선, 조진규[1], 김영식[2], 이용우, 이위직[3]
서울대학교[1], 조선대학교[2], 삼성전자[3]

Coding and Cryptography Lab.
Dept. of ECE, Seoul National University

Outline

I. 개요

II. Enhanced pqsigRM

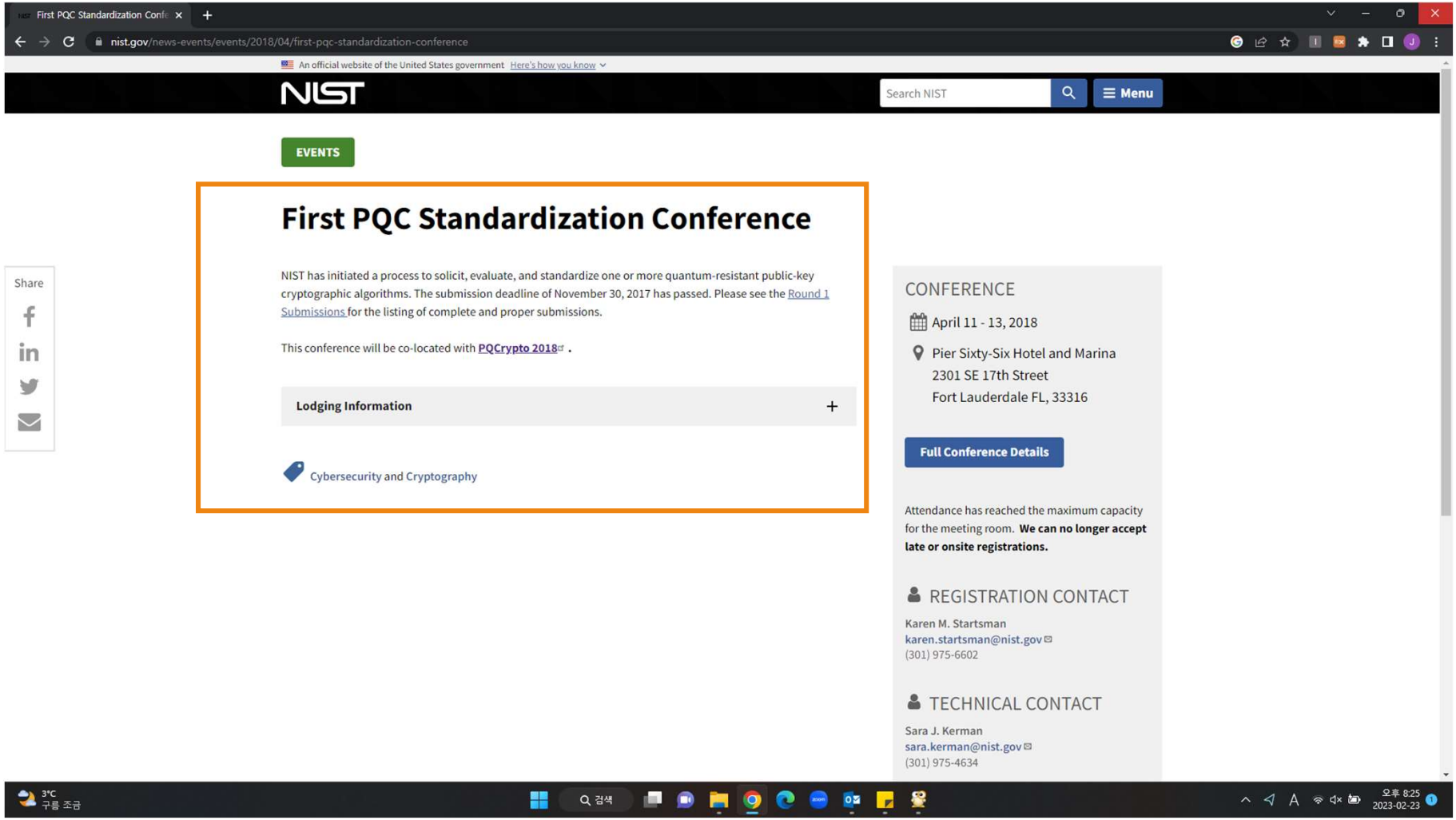
III. 결론

Outline

I. 개요

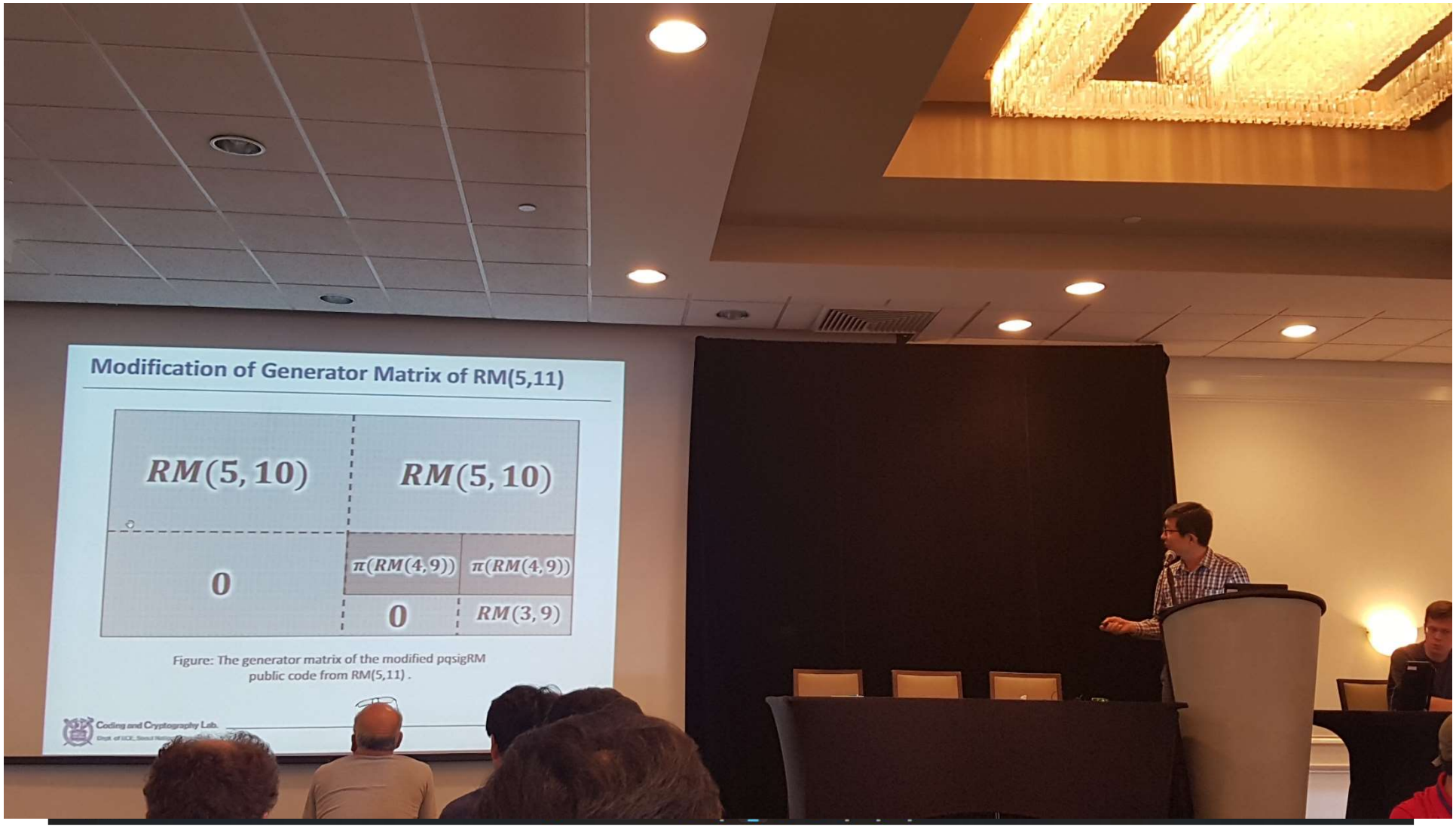
II. Enhanced pqsigRM

III. 결론


First PQC Standardization Conf
nist.gov/news-events/events/2018/04/first-pqc-standardization-conference
An official website of the United States government Here's how you know
NIST
Search NIST
Menu
EVENTS
First PQC Standardization Conference
NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. The submission deadline of November 30, 2017 has passed. Please see the Round 1 Submissions for the listing of complete and proper submissions.
This conference will be co-located with PQCrypto 2018 .
Lodging Information
Cybersecurity and Cryptography
Share
CONFERENCE
April 11 - 13, 2018
Pier Sixty-Six Hotel and Marina
2301 SE 17th Street
Fort Lauderdale FL, 33316
Full Conference Details
Attendance has reached the maximum capacity for the meeting room. We can no longer accept late or onsite registrations.
REGISTRATION CONTACT
Karen M. Startsman
karen.startsman@nist.gov
(301) 975-6602
TECHNICAL CONTACT
Sara J. Kerman
sara.kerman@nist.gov
(301) 975-4634
3°C
구름 조금
검색
오후 8:25
2023-02-23


PIER 66


PQCrypto 2018
The Ninth
International Conference on
Post-Quantum Cryptography
April 9-11, 2018
Fort Lauderdale, Florida
Invited Speakers
SALON A
ISARA
CSPi
IDQ
Infineon
Microsoft Research
intel


Modification of Generator Matrix of RM(5,11)
$RM(5,10)$
$RM(5,10)$
0
$\pi(RM(4,9))$
$\pi(RM(4,9))$
0
$RM(3,9)$
Figure: The generator matrix of the modified pqsigRM public code from RM(5,11) .
Coding and Cryptography Lab.

부호 기반 암호

- 미국의 NIST 에서 진행하는 포스트 양자 암호 표준화 프로젝트
  - 1라운드에 제출되었던 64개의 알고리즘 중 4라운드에는 8개의 알고리즘

    Signatures: CRYSTALS-Dilithium, FALCON, SPHINCS+

    KEM/Encryption: CRYSTALS-KYBER (BIKE, Classic McEliece, HQC, SIKE)
  - **부호 기반 암호**의 비중이 **두번째로 많음** (1라운드: 19개, 4라운드: 3개)

	Signatures		KEM/Encryption		Overall	
	1R	4R	1R	4R	1R	4R
Lattice-based	5	2	21	1	26	3
Code-based	2	-	17	(3)	19	(3)
Multi-variate	7	-	2	-	9	-
Hash/symmetric based	3	1	-	-	3	1
Other	2	-	5	(1)	7	(1)
Total	19	3	45	1(+4)	64	4(+4)

표 1. NIST PQC 표준화 과정 1 라운드와 4라운드 알고리즘 수

* 괄호는 대안 알고리즘

부호 기반 암호

- 부호 기반 암호
  - 포스트 양자 암호 중 격자 기반 암호 다음으로 가장 큰 비중을 차지.
  - 다양한 오류 정정 부호를 사용하며 부호 이론에 기반.
    - Goppa 부호, Quasi-cyclic 부호, Reed-Muller (RM) 부호, Low Density Parity Check (LDPC) 부호, …
  - 40년 이상 동안 깨지지 않은 전통적인 보안성
  - 행렬 연산의 간단한 연산 과정
  - 키 크기가 상당히 크다는 단점

Ex) McEliece 공개키 암호, CFS 전자 서명, …

NIST PQC: Classic McEliece, BIKE, HQC, …

부호 기반 암호

- 부호 기반 암호 시스템의 기본적인 구조
  - 메시지 m과 오류 e 에 대해서 어떤 랜덤한 부호의 생성 행렬 G ($k \times n$ 행렬)를 이용
  - 부호어 mG 를 생성하고 오류를 더해서 암호문 $c = mG + e$ 를 생성.
  - 여기에 생성행렬의 dual 부호인 패리티 체크 행렬 H ($(n-k) \times n$ 행렬) 를 곱하여서

$$s = cH^T = mGH^T + eH^T = eH^T$$

즉, $s = eH^T$ 형태의 신드롬 s 와 H 의 식으로도 나타냄.

부호 기반 암호

- 신드롬 복호 문제 (Syndrome Decoding Problem)에 기반
  - $He^T = s^T$ 에서 $wt(e) \leq t$ 를 만족하는 오류 벡터 e를 구하는 문제
    - H: 랜덤한 부호의 패리티 체크 행렬
    - s: 랜덤한 신드롬 벡터
    - t: 부호의 오류 정정 능력
    - $wt(e)$: e의 Hamming 무게
  - NP-complete 문제

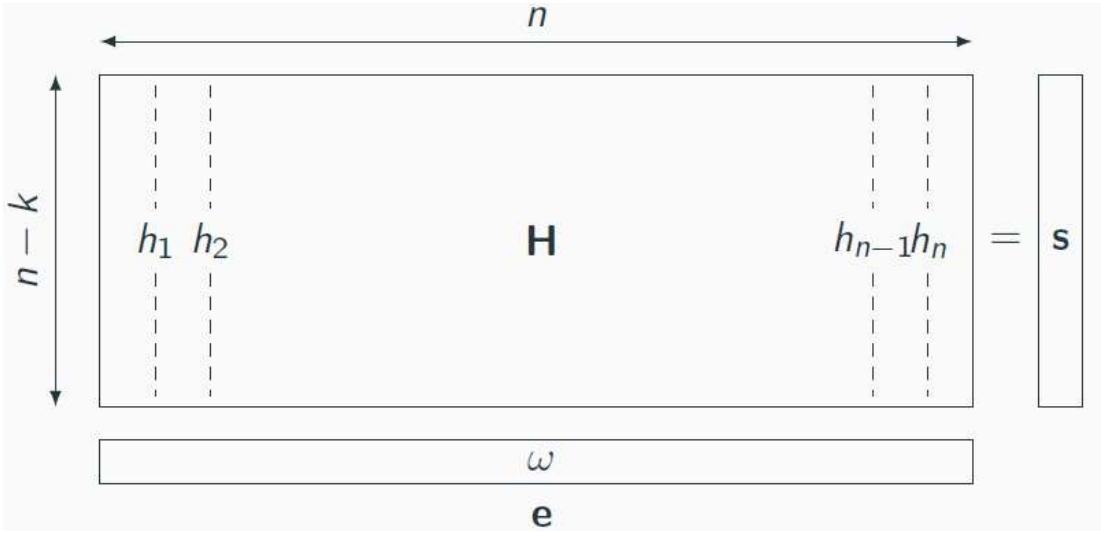


그림 1. 신드롬 복호 문제

전자서명 시스템

- 전자 서명 시스템의 세 가지 과정

1) 키 생성 : 공개키 pk와 비밀키 sk를 생성 (**In:** security 파라미터 λ, **Out:** pk, sk)

2) 서명 : Alice는 메시지 m에 비밀키 sk를 사용하여 서명 σ를 생성

(**In:** m, sk , **Out:** σ)

3) 검증 : Bob은 메시지 m 과 서명 σ을 갖고 있고, 공개키 pk를 사용하여 서명이 맞는지 검증

(**In:** m ,σ, pk, **Out:** 검증 결과 YES/NO)

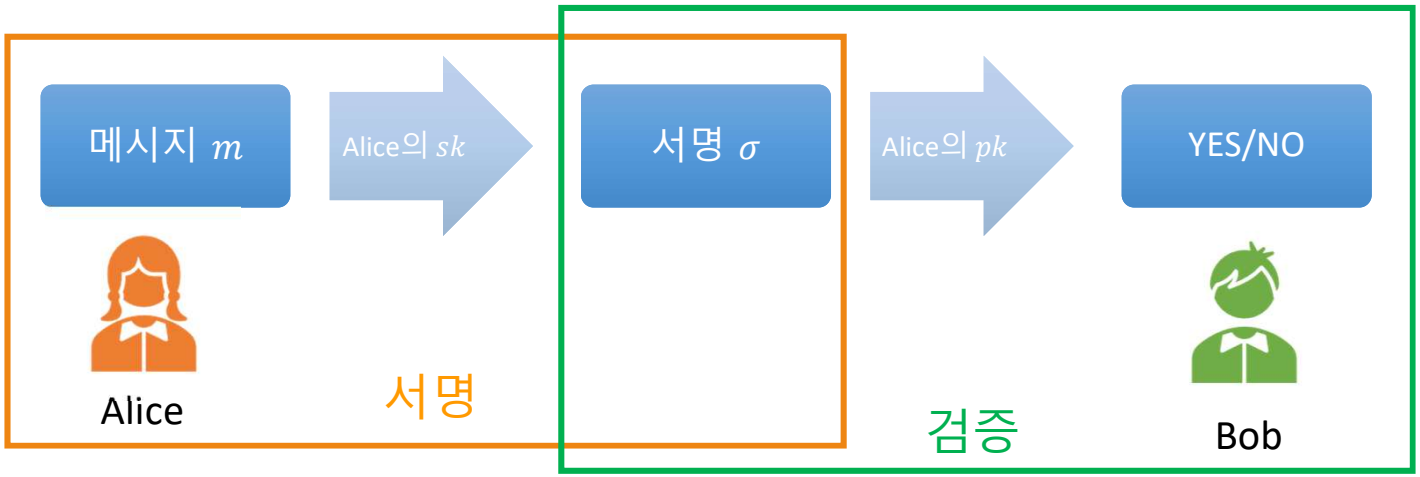


그림 2. 전자 서명 시스템

CFS 전자서명 시스템

- CFS (Courtois, Finiasz, Sendrier, 2001) 전자 서명
  - 가장 저명한 부호 기반의 전자 서명 시스템 중 하나
  - 작은 Hamming 무게를 갖는 오류를 찾을 때까지 반복해서 복호 과정 진행
  - 초기 모델은 high rate Goppa 부호 사용
    - 복호 가능한 신드롬을 찾을 확률이 매우 낮고
    - 공개키, 비밀키 크기가 매우 크다는 단점

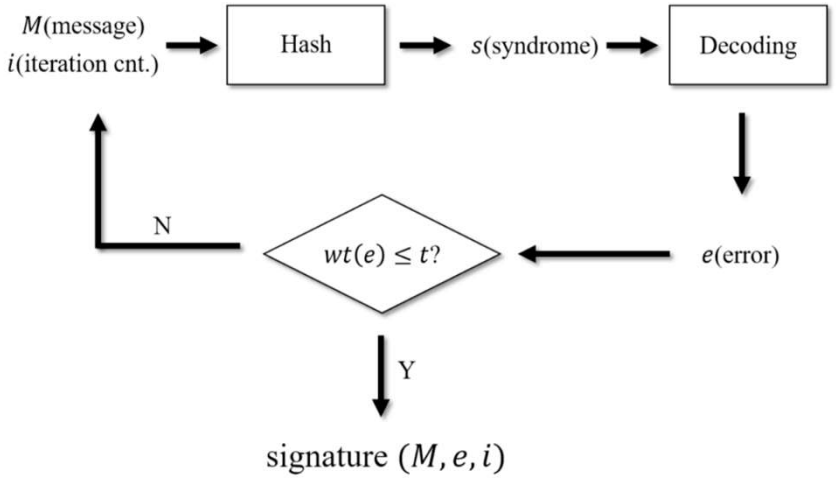


그림 3. CFS 전자서명 시스템의 서명 과정 [1]

[1] N. T. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," in *International Conference on the Theory and Application of Cryptology and Information Security*, 2001, pp. 157-174: Springer.

RM 부호

- RM 부호
  - 두개의 정수 r, m 으로 정의

    ⇒ 길이 $n = 2^m$, 차원 $k_r = \sum_{i=0}^{r} \binom{m}{i}$, 최소 거리 $d_{min} = 2^{m-r}$인 이진 선형 부호
  - Boolean 함수 $v_0, v_1, \ldots, v_m$ 들의 r차 선형 결합으로 표현 가능

$$G_r = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_m \\ v_1 v_2 \\ v_1 v_3 \\ \vdots \\ v_{m-1} v_m \\ \vdots \\ v_1 \cdots v_r \\ v_1 \cdots v_{r-1} v_{r+1} \\ \vdots \\ v_{m-r+1} \cdots v_m \end{pmatrix}$$

RM 부호

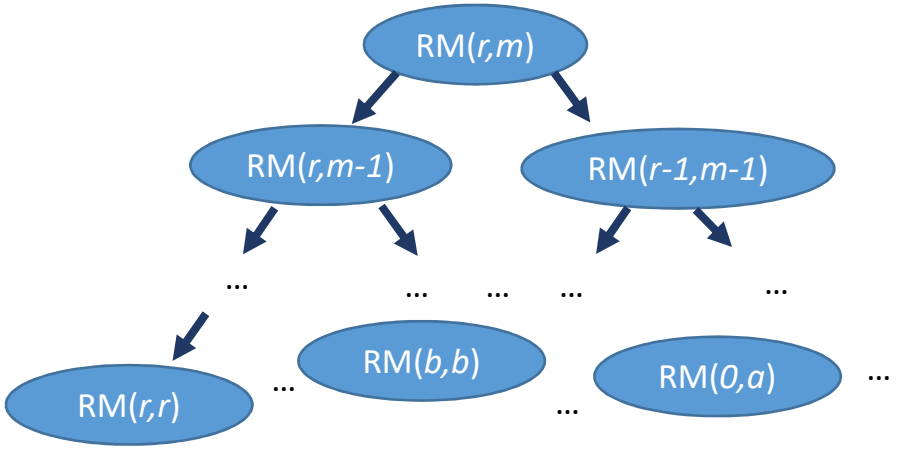
- RM 부호의 재귀적인 성질
  - 재귀적인 형태의 생성행렬
    - $G_{RM(r,m)} = \begin{pmatrix} G_{RM(r,m-1)} & G_{RM(r,m-1)} \\ 0 & G_{RM(r-1,m-1)} \end{pmatrix} =$

$$\begin{pmatrix} G_{RM(r,m-2)} & G_{RM(r,m-2)} & G_{RM(r,m-2)} & G_{RM(r,m-2)} \\ 0 & G_{RM(r-1,m-2)} & 0 & G_{RM(r-1,m-2)} \\ & 0 & G_{RM(r-1,m-2)} & G_{RM(r-1,m-2)} \\ & & 0 & G_{RM(r-2,m-2)} \end{pmatrix}$$

  - $(U, U+V)$ 구조
    - $RM_{(r,m)} \coloneqq \{(u|u+v) | u \in \mathrm{RM}_{(r,m-1)}, v \in \mathrm{RM}_{(r-1,m-1)}\}$
    - 앞 부분이 U, 뒷 부분이 $U+V$ 형태가 되는 부호가 됨

RM 부호

- RM 부호의 재귀적인 성질
  - 재귀적인 구조 끝에는 아래의 두 가지 형태가 남게 됨
  - $G_{\mathrm{RM}_{(0,a)}} \coloneqq \{(0,\dots,0),(1,\dots,1)\}$
  - $G_{\mathrm{RM}_{(b,b)}} \coloneqq \begin{pmatrix} 1 \\ v_1 \\ \dots \\ v_b \\ \dots \\ v_1 v_2 \dots v_b \end{pmatrix}$



RM 부호

- RM 부호의 재귀적 복호 과정
  - 재귀적인 성질을 이용하면 Dumer의 방식 대로 [2] 효율적인 복호를 할 수 있게 된다.
  - $RM_{(r,m)}$의 복호는 $RM_{(r,m-1)}$ 과 $RM_{(r-1,m-1)}$을 재귀적으로 복호함으로써 복호
  - $(U, U+V)$ 구조에서 V 부분을 먼저 복호하고, 그 다음에 U 부분을 복호하는 구조
  - $RM_{(0,m)}$과 $RM_{(r,r)}$ 부분은 최단 거리 복호 과정으로 복호

Algorithm 2 Recursive decoding of RM code [10]

function RECURSIVEDECODING($\mathbf{y}, r, m$)
  if $r = 0$ **then**
    Perform MD decoding on RM$(0, m)$
  else if $r = m$ **then**
    Perform MD decoding on RM(r, r)
  else
    $(\mathbf{y}'|\mathbf{y}'') \leftarrow \mathbf{y}$
    $\mathbf{y}^{\mathbf{v}} = \mathbf{y}' \cdot \mathbf{y}''$
    $\hat{\mathbf{v}} \leftarrow$ RECURSIVEDECODING$(\mathbf{y}^{\mathbf{v}}, r-1, m-1)$
    $\mathbf{y}^{\mathbf{u}} \leftarrow (\mathbf{y}' + \mathbf{y}'' \cdot \hat{\mathbf{v}})/2$
    $\hat{\mathbf{u}} \leftarrow$ RECURSIVEDECODING$(\mathbf{y}^{\mathbf{u}}, r, m-1)$
    Output $(\hat{\mathbf{u}}|\hat{\mathbf{u}} \cdot \hat{\mathbf{v}})$
  end if
end function

[2] I. Dumer, “Recursive decoding and its performance for low-rate Reed-Muller codes,” IEEE Trans. Inf. Theory, vol. 50, no. 5, pp. 8 11-823, May 2004.

RM 부호

- RM 부호 기반 CFS 알고리즘
  - 재귀적 복호 알고리즘을 사용하면 모든 주어진 신드롬에 대해 복호 가능 (작은 해밍 무게에서)

    ⇒ 전자 서명에서 사용하기 적합
  - 하지만, RM 부호의 구조에 대한 키 복구 공격에는 취약
    - Minder-Shokrollahi 공격, Chizhov-Borodin 공격, 제곱 부호 공격
  - **Proposed :** Enhanced pqsigRM은 이런 공격들도 모두 막아내는 RM 부호 기반 CFS 전자 서명

Dual 부호, hull

- Dual 부호의 정의 및 특징

  정의) (n, k) 부호 C에 대한 dual 부호 $C^{\perp}$은

  - $C^{\perp} = \{x \in \mathbb{F}_q^n | \langle x, c \rangle = 0, \forall c \in C\}$

  - $\dim(C) + \dim(C^{\perp}) = n$
  - $(C^{\perp})^{\perp} = C$
  - $C \cdot (C^{\perp})^T = 0$
  - 어떤 부호에서 생성 행렬의 dual 부호 : 패리티 체크 행렬

- Hull

  - $hull(C) = C \cap C^{\perp}$
  - RM 부호에서는 hull을 이용하는 공격이 존재 (e.g. Minder-Shokrollahi 공격)

Outline

I. 개요

II. Enhanced pqsigRM

III. 결론

Enhanced pqsigRM

- **pqsigRM**은 RM부호를 변형하고 CFS 스킴에 적용하여 2017년에 NIST PQC 1라운드에서 발표됨.
- 그 후 pqc-forum 등에서 제기되었던 공격법들을 해결하여 2020년에 **Modified pqsigRM**으로 개선.
- 키 크기와 서명 과정을 최소화 하여 2022년에 **Enhanced pqsigRM**으로 개선.

	Original pqsigRM [3] (2017)	Modified pqsigRM [4] (2020)	Enhanced pqsigRM [5] (2022)
키 생성 방식	열 puncturing 및 추가	부분적 permutation, 행 추가 및 대체	부분적 permutation, 행 추가 및 대체
복호 과정	랜덤하지 않음	랜덤화됨	랜덤화됨
공격법	Hull을 이용해서 puncturing 찾는 공격	없음	없음

표 2. pqsigRM 알고리즘의 개선 과정

[3] W. Lee, Y. S. Kim, Y. W. Lee, and J. S. No, ‘‘Post quantum signature scheme based on modified Reed–Muller code pqsigRM,’’ in First Round Submission to the NIST Postquantum Cryptography Call, Nov. 2017.

[4] Y. W. Lee, W. Lee, Y. S. Kim, and J. S. No, “Modified pqsigRM: RM code-based signature scheme,” *IEEE Access*, *8*, 177506-177518, 2020.

[5] J. Cho, J. S. No, Y. W. Lee, Z. Koo, and Y. S. Kim, “Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature and Fast Verification for Post-Quantum Cryptography.” *Cryptology ePrint Archive, 2022.*

Enhanced pqsigRM

- 부분적으로 permute된 RM 부호

1) RM 부호의 재귀적인 성질을 이용해 생성행렬을 아래와 같이 나눔

2) 첫번째 줄의 4개의 행렬들에 각각 permutation σ_p^1를 가함.

3) 마지막 줄의 행렬에 permutation σ_p^2 를 가함.

- 키 복구 공격 방지.
- 이때, hull의 dimension을 크게 설정해주어 hull을 이용하는 공격 방지.

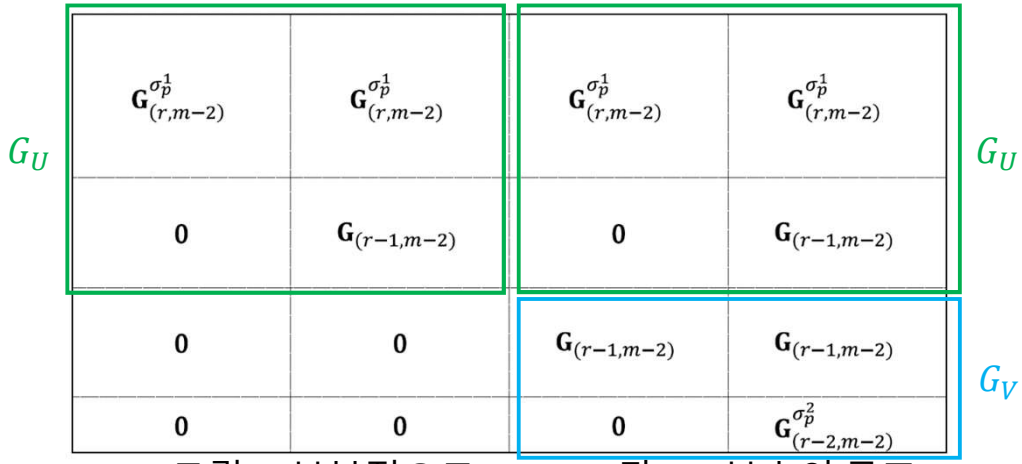


그림 3. 부분적으로 permute된 RM 부호의 구조

Enhanced pqsigRM

$$\mathbf{G}_U = \begin{bmatrix} \mathbf{G}_{(r,m-2)}^{\sigma_p^1} & \mathbf{G}_{(r,m-2)}^{\sigma_p^1} \\ \mathbf{0} & \mathbf{G}_{(r-1,m-2)} \end{bmatrix},$$

$$\mathbf{G}_V = \begin{bmatrix} \mathbf{G}_{(r-1,m-2)} & \mathbf{G}_{(r-1,m-2)} \\ \mathbf{0} & \mathbf{G}_{(r-2,m-2)}^{\sigma_p^2} \end{bmatrix}$$

$$\mathbf{G}_U^{\perp} = \begin{bmatrix} \mathbf{G}_{(r,m-2)}^{\perp\sigma_p^1} & \mathbf{0} \\ \mathbf{G}_{(r-1,m-2)}^{\perp} & \mathbf{G}_{(r-1,m-2)}^{\perp} \end{bmatrix}$$

- $(U, U+V)$ 부호가 높은 차원의 hull을 가지려면, $\dim(U^{\perp} \cap V)$가 큰 값을 가져야 함[6]
- 부분적으로 permute된 RM 부호에서 $U^{\perp} \cap V$ 는 위의 식에서 빨간 박스끼리의 교집합 중 일부가 되고, 이것의 차원은 아래와 같음

$$\min\left(\dim\left(RM_{(r-1,m-2)}\right), \dim\left(RM_{(m-r-2,m-2)}\right)\right) = \sum_{i=0}^{\min(r-1,m-r-2)} \binom{m-2}{i}$$

- [6] T. Debris-Alazard, N. Sendrier, and J.-P. Tillich, ``The problem with the SURF scheme," 2017, *arXiv:1706.08065*.

Enhanced pqsigRM

$$\mathbf{G}_U = \begin{bmatrix} \mathbf{G}_{(r,m-2)}^{\sigma_p^1} & \mathbf{G}_{(r,m-2)}^{\sigma_p^1} \\ \mathbf{0} & \mathbf{G}_{(r-1,m-2)} \end{bmatrix},$$

$$\mathbf{G}_V = \begin{bmatrix} \mathbf{G}_{(r-1,m-2)} & \mathbf{G}_{(r-1,m-2)} \\ \mathbf{0} & \mathbf{G}_{(r-2,m-2)}^{\sigma_p^2} \end{bmatrix}$$

$$\mathbf{G}_U^{\perp} = \begin{bmatrix} \mathbf{G}_{(r,m-2)}^{\perp\sigma_p^1} & \mathbf{0} \\ \mathbf{G}_{(r-1,m-2)}^{\perp} & \mathbf{G}_{(r-1,m-2)}^{\perp} \end{bmatrix}$$

- 그 이유는,
  - $RM_{(r,m)}$의 dual : $RM_{(m-r-1,m)}$
  - $r' \leq r$이면, $RM_{(r',m)} \subseteq RM_{(r,m)}$
- 그 부분의 차원 값은 크게 설정해주고, 빨간 박스와 상관 없는 부분에만 permutation σ_p^1, σ_p^2를 적용.

Enhanced pqsigRM

- Modified RM 부호

  - 부분적으로 permute된 RM 부호에 추가로 세 가지 변형

1) $\mathrm{RM}(r,r)$들을 랜덤한 부호들로 대체

   - RM 부호에서 재귀적 구조를 끝까지 반복해보면, 첫번째 2^r개의 행은 $\mathrm{RM}(r,r)$들이 2^{m-r}번 반복되는 구조가 됨.
   - 이 $\mathrm{RM}(r,r)$들을 2^{m-r}개의 반복되는 랜덤한 $(2^r, k_{rep})$ 부호들로 대체

✓ $k_{rep} = 2^r - 2$
: 대체 전보다 행의 수는 2 감소

✓ $k_{ap} = 2$

✓ 기존의 RM 부호보다 전체 행의 수는 1 증가

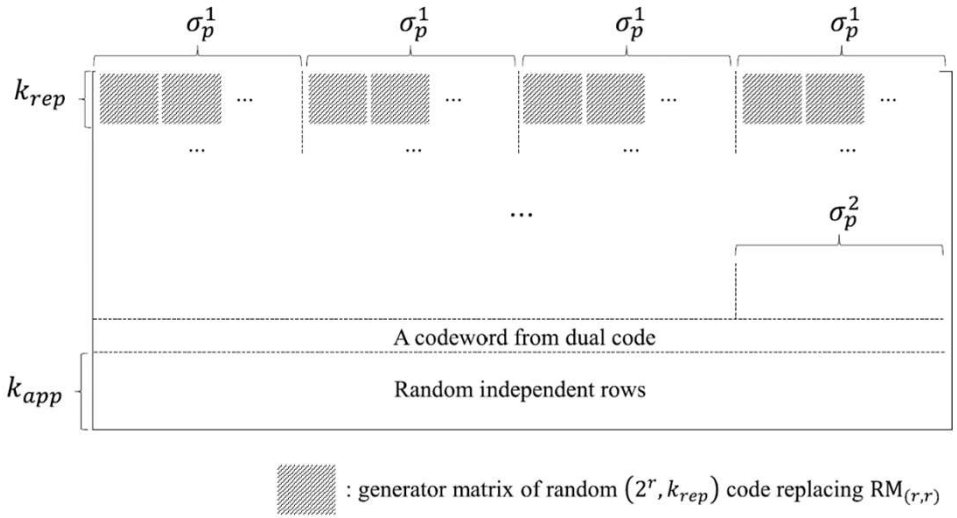


그림 4. 개선된 RM 부호의 구조

Enhanced pqsigRM

- 이때, 이 랜덤한 $(2^r, k_{rep})$ 부호의 dual 부호는 홀수의 Hamming 무게를 갖고 0이 아닌 부호어를 최소 한 개 이상 포함.
- 부분적 permute만 하면, 그 dual 부호가 짝수의 Hamming 무게를 가지는데
  ⇒ 그렇지 않고 랜덤해 보이도록 하기 위함.

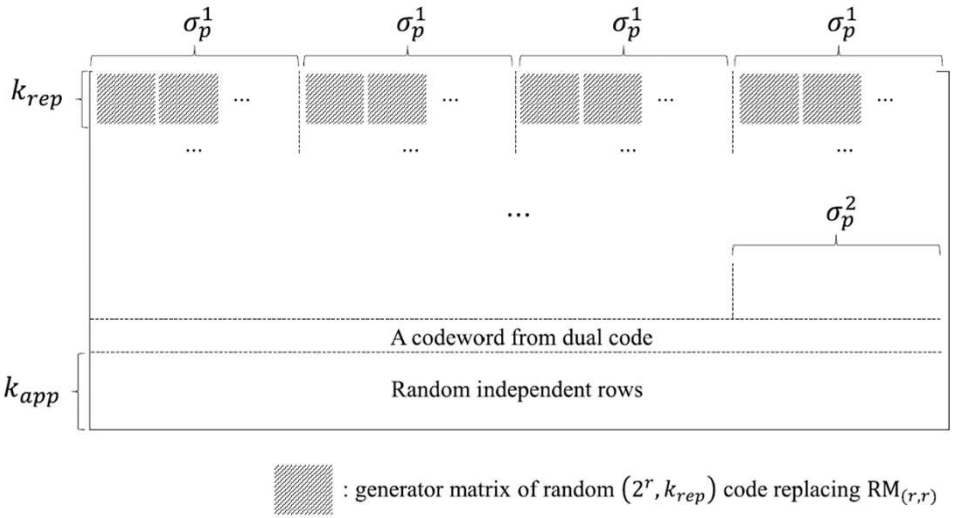


그림 4. 개선된 RM 부호의 구조

Enhanced pqsigRM

- Modified RM 부호

2) 랜덤한 행들 추가

- k_{app}만큼의 랜덤한 독립 행들 추가
- 이때, 부호는 홀수의 Hamming 무게를 갖고 0이 아닌 부호어를 최소 한 개 이상 포함.
- 부분적 permute만 하면, 그 부호가 짝수의 Hamming 무게를 가짐
  => 그렇지 않고 랜덤해 보이도록
- 랜덤 부호와의 구별성 문제를 더 강화
  - ✓ 더 이상 $(U, U+V)$ 부호는 아니게 되지만, $(U, U+V)$ 부호를 포함하고 있기 때문에 $(U, U+V)$ 부호의 복호 알고리즘은 사용가능

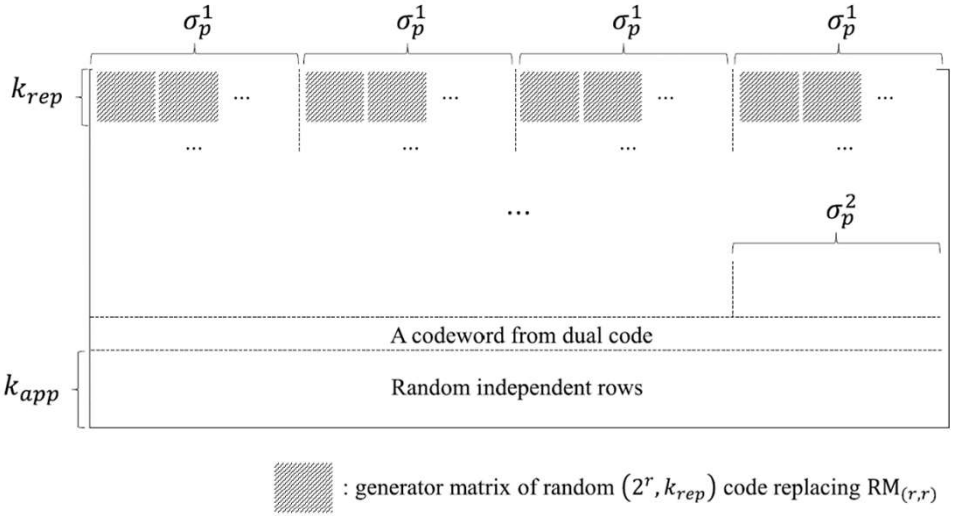


그림 4. 개선된 RM 부호의 구조

Enhanced pqsigRM

- Modified RM 부호

3) Dual 부호의 부호어 추가

- Dual 부호 중에서 랜덤하게 부호어 한 줄을 추가
- 부분적 permute 만 하면, hull의 Hamming 무게가 4의 배수가 됨
  => (랜덤 부호의 hull처럼) 임의의 짝수를 가지도록 하기 위함
- Hull을 한 줄 생성해주는 효과

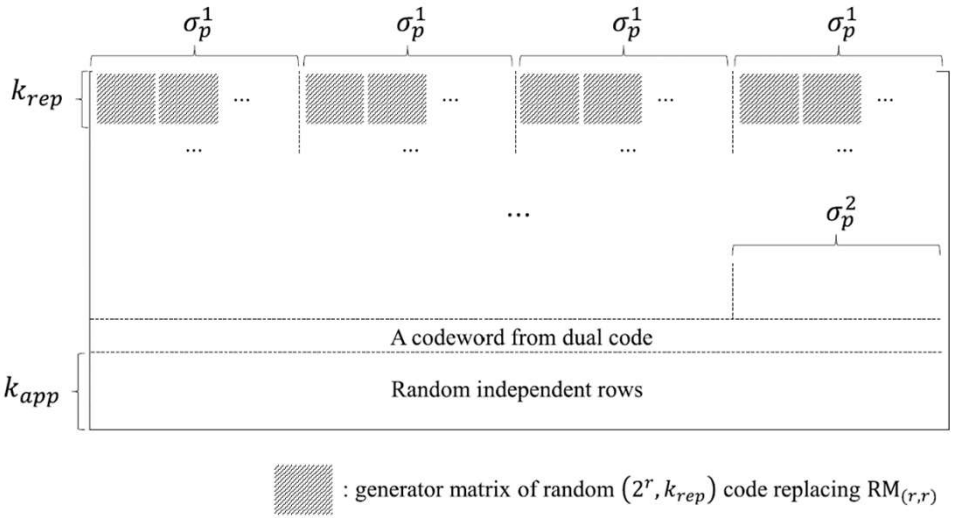


그림 4. 개선된 RM 부호의 구조

Enhanced pqsigRM

- Modified RM 부호의 복호 과정
  - 기본적으로 RM 부호의 재귀적인 성질을 이용한 재귀적 복호 과정을 거침
  - σ_p^1, σ_p^2 : Permutation 위치를 알면 복호 가능

1) RM(r,r)들을 2^{m-r}개의 반복되는 랜덤한 $(2^r, k_{rep})$ 부호로 대체
   - 작은 부호라서 최단 거리 복호 방법으로 복호 가능

2) k_{app}만큼의 랜덤한 독립 행들 추가

3) Dual 부호에서 랜덤한 부호어 한 줄 추가
   - 2), 3)의 추가되는 행들에 대해서는 received 벡터에 C_{app} (추가되는 행들의 집합)에 속하는 부호어들을 더하면서 오류의 최대 무게보다 작아질 때까지 반복

Enhanced pqsigRM 전자 서명

- Enhanced pqsigRM 전자 서명
  - CFS 전자 서명 방식에 modified RM 부호의 패리티 체크 행렬을 사용
- DOOM(Decoding One Out of Many) 문제
  - Enhanced pqsigRM의 안전성은 신드롬 복호 문제의 변형인 DOOM 문제에 기반
- 키 교환 공격
  - 신드롬에 hashing을 해줌으로써 키 교환 공격으로부터 안전해짐
- EUF-CMA 안전성
  - 공개키가 구별 불가능하다는 가정 하에 EUF-CMA 안전성을 증명함
- NIST SP 800-22 (랜덤 비트 생성 테스트) 통과
  - 공개키가 랜덤 시퀀스와 구별 불가능하다는 것을 실험적으로 확인함

Security

- DOOM(Decoding One Out of Many) 문제

  - Instance: (n, k) 선형 부호의 패리티 체크 행렬 $H \in \mathbb{F}_2^{(n-k)\times n}$, 신드롬 $s_1, s_2, \ldots, s_q$, 정수 w.

  - Output: $(e, i) \in \mathbb{F}_2^n \times [1, q]$

    - 이때 $wt(e) \leq w, He^T = {s_i}^T$

  - Enhanced pqsigRM의 안전성은 신드롬 복호 문제에서 확장된 DOOM 문제에 기반

Security

- EUF-CMA (Existential Unforgeability under Chosen Message Attack) 안전성

1) Challenger는 유효한 공개키, 비밀키를 만들고 Attacker에게 공개키를 제공
2) Attacker는 메세지들을 골라서 물어볼 수 있고 그에 대한 유효한 서명 값을 받음
3) Attacker가 유효한 메시지-서명 짝(물어보지 않은 새로운 짝)을 찾아내면 공격이 성립

- Enhanced pqsigRM의 EUF-CMA 안전성은 아래의 두가지 문제로 reduce 됨.

1) Modified RM 부호의 구별성 문제
2) 고차원 hull을 갖는 DOOM 문제

- Enhanced pqsigRM은 공개키가 구별 불가능하다는 가정 하에 EUF-CMA 안전성을 증명함

Enhanced pqsigRM

- Enhanced pqsigRM 전자 서명

  - Modified pqsigRM에서 몇가지 추가 개선
    - Systematic한 parity check matrix를 사용하여 공개키를 T로 사용. (공개키 감소)
    - 비밀키를 필요한 부분만 추출하여 크기 최소화.
    - 신드롬 생성시 해시 함수를 두 번이 아니라 한 번만 사용하여 서명 과정 간소화.

- **Key generation**
  - $\mathbf{G}$: $k \times n$ generator matrix of modified RM codes
  - $\mathbf{H}$: $(n-k) \times n$ parity check matrix of modified RM codes
  - $\mathbf{Q} \xleftarrow{\$} F_2^{n \times n}$
  - $\mathbf{H_{sys}} = (\mathbf{I}|\mathbf{T}) \leftarrow \mathbf{S_{sys}HQ}$
  - Public key: $\mathbf{T}$
  - Secret key: $\mathbf{Q}$, σ_p^1, σ_p^2, $k_{rep} \times 2^r$ (repeated) replacing codes, $k_{app} \times n$ appending codes, and $1 \times n$ padding dual code codeword
- **Signing**
  - $\mathbf{m}$: Message, $i \hookleftarrow \{0,1\}^{\lambda_0}$: Counter
  - $\mathbf{s} \leftarrow h(\mathbf{m}|i)$: Syndrome
  - $\mathbf{s'}^T \leftarrow \mathbf{S_{sys}}^{-1}\mathbf{s}^T$
  - $\mathbf{e'} \leftarrow \text{Decode}(\mathbf{s'}; \mathbf{H})$
  - $\mathbf{e}^T \leftarrow \mathbf{Q}^{-1}\mathbf{e'}^T$
  - Signature: $(\mathbf{m}, \mathbf{e}, \mathbf{i})$
- **Verification**
  - If $wt(e) \leq w$ and $\mathbf{H_{sys}}e^T = h(\mathbf{m}|i)$, return ACCEPT
  - Else, return REJECT

그림 5. Enhanced pqsigRM의 전자 서명 스킴

Enhanced pqsigRM

- Systematic한 공개키 생성
  - Modified pqsigRM : $H' = SHQ$: $(n-k) \times n$ 행렬
  - Enhanced pqsigRM : $H'_{sys} = (I|T) \Rightarrow T : (n-k) \times k$ 행렬
  - n이 같다는 가정 하에, systematic한 공개키 크기를 최대한 작게 하려면 k가 0 또는 n에 가깝게 유지되어야 함.
  - 아래의 Lemma를 토대로 r 값을 통해 k 값을 조절할 수 있음.

Lemma) RM 부호에서는 모든 r, r', m 값에 대해 아래의 식을 만족한다. $(r' \leq r)$

$$RM(r', m) \subseteq RM(r, m)$$

Enhanced pqsigRM

- Enhanced pqsigRM
  - Systematic한 공개키 사용
    - 공개키 크기 감소: $(n-k)n \Rightarrow (n-k)k$
  - 기존의 같은 security level에 대해 각각 **절반 정도로** 공개키 크기 감소 가능

	Modified pqsigRM			Enhanced pqsigRM	
(r, m)	(5, 11)	(6, 12)	(6, 13)	**(6, 12)**	**(6, 13)**
n	2048	4096	8192	4096	8192
k	1025	2511	4097	2511	4097
Security level	80	128	256	128	256
Bit security	83	130	259	130	259
공개키 크기(MB)	0.25	0.77	4.00	**0.47**	**2.00**

표 3. Modified pqsigRM 과 Enhanced pqsigRM 파라미터 비교

Enhanced pqsigRM

- 비밀키 최소화
  - Modified pqsigRM : 행렬 S, H, Q 전체
  - Enhanced pqsigRM : $Q, \sigma_p^1, \sigma_p^2, k_{rep} \times 2^r$ 행렬 (랜덤 부호 대체 부분), $k_{app} \times n$ 행렬 (랜덤 부호 추가 부분), $1 \times n$ 행렬 (dual 부호 추가 부분), S는 제거 (HQ를 systematic하게 만드는 unique한 S_{sys}를 쓰면 됨: 비밀키 X)
- 신드롬 간소화
  - Modified pqsigRM : $h(h(m|SHQ)i)$
  - Enhanced pqsigRM : $h(m|i)$

Parameters

- (r, m) 설정 ⇒ (n, k) 결정
  - n : 부호의 길이
    - $n = 2^m$
  - k : 부호의 차원
    - $k = \sum_{i=0}^{r} \binom{m}{i} + 1$
    - Modified RM 부호의 차원은 기존의 RM 부호의 차원보다 1 큰 값

	Enhanced pqsigRM	
(r, m)	(6, 12)	(6, 13)
n	4096	8192
k	2511	4097
w	495	1370
p	≥386	≥562
k_{rep}	62	62
k_{app}	2	2

표 3. Enhanced pqsigRM 파라미터 값

Parameters

- w: 오류의 최대 Hamming 무게
  - 여러 개의 랜덤한 값들에 대해 복호를 해보고 약 80% 정도의 확률로 w가 얼마 안 쪽으로 들어오는지 실험적으로 측정

	Enhanced pqsigRM	
(r, m)	(6, 12)	(6, 13)
n	4096	8192
k	2511	4097
w	495	1370
p	≥386	≥562
k_{rep}	62	62
k_{app}	2	2

표 3. Enhanced pqsigRM 파라미터 값

Parameters

- p: Partial permutation 횟수
  - $0 \leq p \leq \frac{n}{4}$
  - $p = 0$: Permutation 아예 하지 않은 것
  - $p = \frac{n}{4}$: Full permutation
  - p 값이 작을수록 decoding iteration이 적게 필요해져서 좋지만,
  - 무한정 줄이게 되면 기존의 RM 부호와 너무 비슷해지는 문제가 존재.
  - 따라서 특정 범위 내에서 사용하게 됨

	Enhanced pqsigRM	
(r, m)	(6, 12)	(6, 13)
n	4096	8192
k	2511	4097
w	495	1370
p	≥386	≥562
k_{rep}	62	62
k_{app}	2	2

표 3. Enhanced pqsigRM 파라미터 값

Parameters

- p 값의 범위 설정
  - 공개 키의 hull이 기존의 RM 부호에 속하고 그 차원 값이 크면, Minder-Shokrollahi 공격과 같은 공격을 당하게 됨
  - 따라서 이런 공격을 막으려면, $hull(C_{pub}) \setminus RM_{r,m}$ 이 전체 hull 중에 큰 비중을 차지해야 함

	Enhanced pqsigRM	
(r, m)	(6, 12)	(6, 13)
n	4096	8192
k	2511	4097
w	495	1370
p	≥386	≥562
k_{rep}	62	62
k_{app}	2	2

표 3. Enhanced pqsigRM 파라미터 값

Parameters

- p 값의 범위 설정
  - **목표 :** Full permutation을 했을 때 만큼의 $\dim(hull(C_{pub}) \setminus RM_{r,m})$ 값이 유지되는 최대한 작은 p 값을 찾는 것.
  - 실험적으로 구해본 결과, p 값이 증가함에 따라 $\dim(hull(C_{pub}) \setminus RM_{r,m})$ 값도 증가하고 어느 순간 saturate 하게 됨.

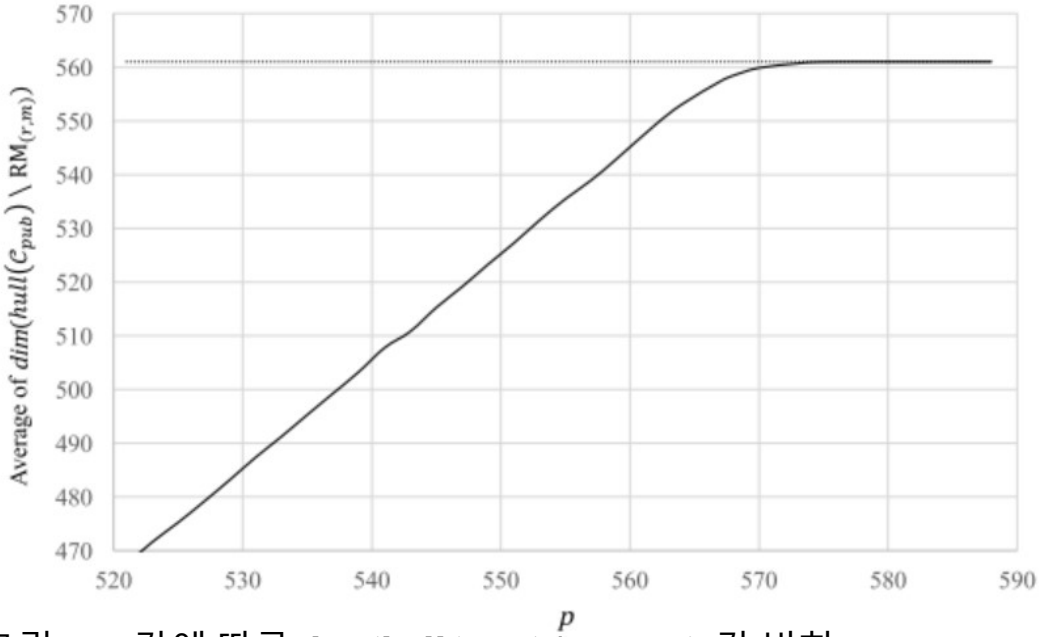


그림 6. p 값에 따른 $\dim(hull(C_{pub}) \setminus RM_{r,m})$ 값 변화 (EnhpqsigRM-613)

	Enhanced pqsigRM	
(r, m)	(6, 12)	(6, 13)
n	4096	8192
k	2511	4097
w	495	1370
p	≥386	≥562
k_{rep}	62	62
k_{app}	2	2

표 3. Enhanced pqsigRM 파라미터 값

Parameters

- k_{rep}
  - $k_{rep} = 2^r - 2$
  - Modified RM 부호를 만들 때, RM(r, r)들을 2^{m-r}개의 반복되는 랜덤한 $(2^r, k_{rep})$ 부호로 대체하는 k 값
  - 대체하기 전에 비해 k 값이 2만큼 감소하는 셈
- k_{ap}
  - $k_{ap} = 2$
  - Modified RM 부호를 만들 때, 랜덤한 독립 행들을 추가해주는 k 값

	Enhanced pqsigRM	
(r, m)	(6, 12)	(6, 13)
n	4096	8192
k	2511	4097
w	495	1370
p	≥386	≥562
k_{rep}	62	62
k_{app}	2	2

표 3. Enhanced pqsigRM 파라미터 값

Parameters

- Enhanced pqsigRM은 부호 기반 전자 서명 중 공개키 크기와 서명 길이가 **가장 작음**.
- NIST 4 라운드 암호시스템들에 비해 서명 길이는 **가장 작고** 공개키 사이즈는 매우 큼 (공개키는 한번만 보내고 서명은 서명할 때마다 보내기 때문에 **큰 장점**).

Security level		Parallel-CFS	Wave (Asiacrypt 2019)	Durandal (Eurocrypt 2019)	Enhanced pqsigRM	Classic McEliece (KEM)
128	공개키 크기(MB) 서명 길이(byte)	2.7×10^5 59	3.10 1647	0.015 4060	**0.47** **512**	0.26
256	공개키 크기(MB) 서명 길이(byte)	9.4×10^{15} 155	12.43 3293	X	**2.00** **1024**	1.04

표 4. 다른 부호 기반 알고리즘들과의 파라미터 크기 비교

Security level		Crystals-Dilithium	Falcon	Sphincs+
128	공개키 크기(byte) 서명 길이(byte)	1312 2420	897 666	32 7856
256	공개키 크기(byte) 서명 길이(byte)	2592 4595	1793 1280	64 29792

표 5. NIST 4 라운드 전자 서명들의 파라미터 크기

Verification Time

- Enhanced pqsigRM의 verification time 비교
  - 128 bit security: Verification time이 Crystals-Dilithium의 약 5배
  - 256 bit security: Crystals-Dilithium의 약 10배.

Security	Enhanced pqsigRM	Verification Cycles				
		Avg	Median	Crystals-Dilithium	Falcon	Sphincs+
128	Enh-pqsigRM-612	1,740,417	1,717,366	327,362	82,340	308,774
256	Enh-pqsigRM-613	8,260,745	8,094,462	871,609	168,498	696,980

Table 2. NIST 4라운드 finalist들과의 verification cycle 비교

Other Parameters

- 각 security level에 따른 비밀키 크기, 키 생성 cycle 수, 서명 cycle 수는 아래와 같음.

Security	Enhanced pqsigRM	비밀키 크기 (byte)	키 생성 cycle 수		서명 cycle 수	
			Avg	Med	Avg	Med
128	Enh-pqsigRM-612	10,736	2,626,460,531	2,643,729,770	4,738,459	4,337,129
256	Enh-pqsigRM-613	22,512	23,046,351,332	22,863,327,573	60,863,577	26,116,121

표 6. Enhanced pqsigRM의 비밀키 크기, 키 생성 cycle 수, 서명 cycle 수

NIST Comment 반영

- NIST PQC 4라운드 컨퍼런스에 Enhanced pqsigRM 알고리즘을 제출하여 아래의 두가지 comment를 받음

  1) $n-k$가 너무 작으면 information set 이 작아져서 information set decoding을 이용한 forgery attack에서 문제

  - k가 작을수록 유리

  2) Minimum weight codeword들을 찾을 수 있는 확률을 고려

  - k, d_{min} 클수록 유리.

  • Information set decoding에 의해 weight w인 error vector를 decoding할 확률: (Minimum weight codeword들을 찾을 수 있는 확률과 동일)

$$\frac{\binom{n-k}{w}}{\binom{n}{w}} = \frac{(n-k)(n-k-1)\dots(n-k-w+1)}{n\,(n-1)\,(n-2)\dots\,(n-w+1)} \approx \left(\frac{n-k}{n}\right)^{w}$$

NIST Comment 반영

- NIST comment를 고려하여 파라미터 값을 조정하면, 128-bit security에 Enh-pqsigRM-613을, 256-bit security에 Enh-pqsigRM-715를 사용해야 함.
- 공개키 크기 및 서명 길이
  - 공개키 크기는 매우 크고
  - 서명 길이는 128 bit security의 경우 : Crystals-Dilithium의 **1/2배**

    256 bit security의 경우 : Crystals-Dilithium의 **2배**

Security level		Enhanced pqsigRM	Crystals-Dilithium	Falcon	Sphincs+
128	공개키 크기(byte)	**2,000,000**	1312	897	32
	서명 길이(byte)	**1024**	2420	666	7856
256	공개키 크기(byte)	**32,000,000**	2592	1793	64
	서명 길이(byte)	**8192**	4595	1280	29792

표 7. NIST comment까지 고려한 Enhanced pqsigRM의 공개키와 서명 길이 비교

NIST Comment 반영

- Verification cycles
  - 128 bit security의 경우 : Crystals-Dilithium의 **25배 (**개선 중)

    256 bit security의 경우 : 새로 측정 중 (파라미터 값이 많이 커지다 보니 segment error 가 생겨서 코드의 연산 구조를 수정 중).

Security	Enhanced pqsigRM	Verification Cycles				
		Avg	Median	Crystals-Dilithium	Falcon	Sphincs+
128	Enh-pqsigRM-613	8,260,745	8,094,462	327,362	82,340	308,774

표 8. NIST comment까지 고려한 Enhanced pqsigRM의 검증 cycle 수

NIST Comment 반영

- 128 bit security에 따른 비밀키 크기, 키 생성 cycle 수, 서명 cycle 수는 아래와 같음.

Security	Enhanced pqsigRM	비밀키 크기 (byte)	키 생성 cycle 수		서명 cycle 수	
			Avg	Med	Avg	Med
128	Enh-pqsigRM-613	22,512	23,046,351,332	22,863,327,573	60,863,577	26,116,121

표 6. Enhanced pqsigRM의 비밀키 크기, 키 생성 cycle 수, 서명 cycle 수

Outline

I. 개요

II. Enhanced pqsigRM

III. 결론

Conclusion

- Enhanced pqsigRM은 CFS 알고리즘을 개선한 포스트 양자 부호 기반 전자 서명 시스템이며 부호 기반 전자 서명 중 가장 좋은 파라미터 값을 가짐.
- 또한 NIST 1 라운드와 pqc-forum을 통해 다양한 토론 과정을 거치며 그 안전성을 개선하였고 아직까지 유효한 공격법이 제안된 것이 없음.
- 추가적으로 NIST 4 라운드 컨퍼런스에 알고리즘을 제출하여 comment를 받았고 파라미터 값을 좀 더 안전하도록 수정함.
- NIST 4 라운드 암호시스템들에 비해 서명 길이는 가장 작지만, 공개키 크기는 매우 크다는 문제점.
- 개선하기 위한 방안을 계속해서 연구 중.

Thank you!