코드 기반 KpqC & NIST 추가 서명 공모전 출품작 설계사상 분석

Part II

이형태

중앙대학교 소프트웨어학부

October 22, 2024

Target Algorithms (at The 8th KpqC Workshop in July 2024)

- KpqC 2라운드 진출 코드 기반 암호 기법
  - **PALOMA**
  - **REDOG**

- NIST Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process

설계 방식	코드 기반 전자서명
Hash-and-Sign 기반	**Enhanced pqsigRM**
	FuLeeca
	Wave
비 Hash-and-Sign 기반	**CROSS**
	LESS
	MEDS
코드+MPC-in-the-Head	RYDE
	SDitH

Underlying Assumption I: Syndrome Decoding Problem

Syndrome Decoding Problem

Given $\mathbf{H} \in \mathbb{F}_p^{(n-k)\times n}$, $t \in \mathbb{N}$, and $\mathbf{s} \in \mathbb{F}_p^{n-k}$, decide if there exists an $\mathbf{e} \in \mathbb{F}_p^n$ such that $wt(\mathbf{e}) \leq t$ and $\mathbf{e}\mathbf{H}^\mathsf{T} = \mathbf{s}$.

Restricted Syndrome Decoding Problem (R-SDP)

Given $g \in \mathbb{F}_p^*$ of order z, $\mathbf{H} \in \mathbb{F}_p^{(n-k)\times n}$, $\mathbf{s} \in \mathbb{F}_p^{n-k}$, and $\mathbb{E} = \{g^i | 1 \leq i \leq z\}$, decide if there exists an $\mathbf{e} \in \mathbb{E}^n$ such that $\mathbf{e}\mathbf{H}^\mathsf{T} = \mathbf{s}$.

Restricted Syndrome Decoding Problem with Subgroups (R-SDP(G))

Let $G = \langle \mathbf{a}_1, \ldots, \mathbf{a}_m \rangle$ for $\mathbf{a}_i \in \mathbb{E}^n$, $\mathbf{H} \in \mathbb{F}_p^{(n-k)\times n}$, $\mathbf{s} \in \mathbb{F}_p^{n-k}$. Does there exist a vector $\mathbf{e} \in G$ with $\mathbf{e}\mathbf{H}^\mathsf{T} = \mathbf{s}$?

- It is known that R-SDP and R-SDP(G) are NP-complete.

Underlying Assumption II: Code Equivalence Problem

(Linear) Code Equivalence Problem

Let $\mathbf{G}, \mathbf{G}' \in \mathbb{F}_q^{k \times n}$ be two generator matrices for linear codes C and C', respectively. Decide if the two codes are linearly equivalent, i.e., if there exist two matrices $\mathbf{S} \in GL_k(q)$ and $\mathbf{Q} \in M_n(q)$ such that $\mathbf{G}' = \mathbf{SGQ}$.

- Hardness of the Linear Code Equivalence Problem
  - The linear code equivalence problem is NOT NP-complete.
  - However, it is believed that the linear code equivalence problem is intractable under many instances for about 40 years.

Summary of Code-Based Signature Schemes in Previous Presentation

Table 1: Feature Comparison of Code-Based Signatures in Previous Talk

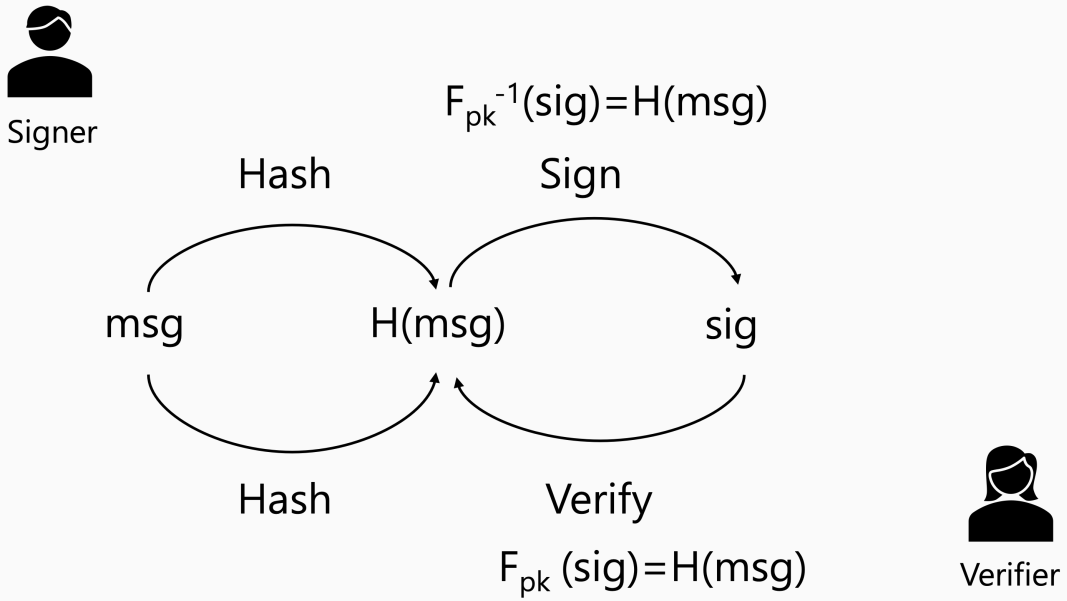
Scheme	Design	Underlying Assumption	Security
LESS [BBB+23a]	ZK+FS	CEP	
CROSS [BBB+23b]	ZK+FS	R-SD	
Enhanced pqsigRM [NCL+22]	Hash-and-Sign	SD	Broken [DLV24]
FuLeeca [RMB+23]	Hash-and-Sign	SD (Lee metric)	Broken [vWH24]

Target Algorithms (Today)

- KpqC 2라운드 진출 코드 기반 암호 기법
  - PALOMA
  - REDOG
- NIST Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process

설계 방식	코드 기반 전자서명
Hash-and-Sign 기반	Enhanced pqsigRM
	FuLeeca
	Wave
비 Hash-and-Sign 기반	CROSS
	LESS
	MEDS
코드+MPC-in-the-Head	**RYDE**
	SDitH

서명 설계 방법 I: Hash-and-Sign



- Easy to compute F_{pk}, but hard to compute F_{pk}^{-1}
- Insert a trapdoor in the public key
- Short signature, large public key
- RSA-Based: RSA-PSS
- **Code-Based**: **CFS**, **Enhanced pqsigRM**, **FuLeeca**, **Wave**

* Figures in this slide referred to [Feb24].

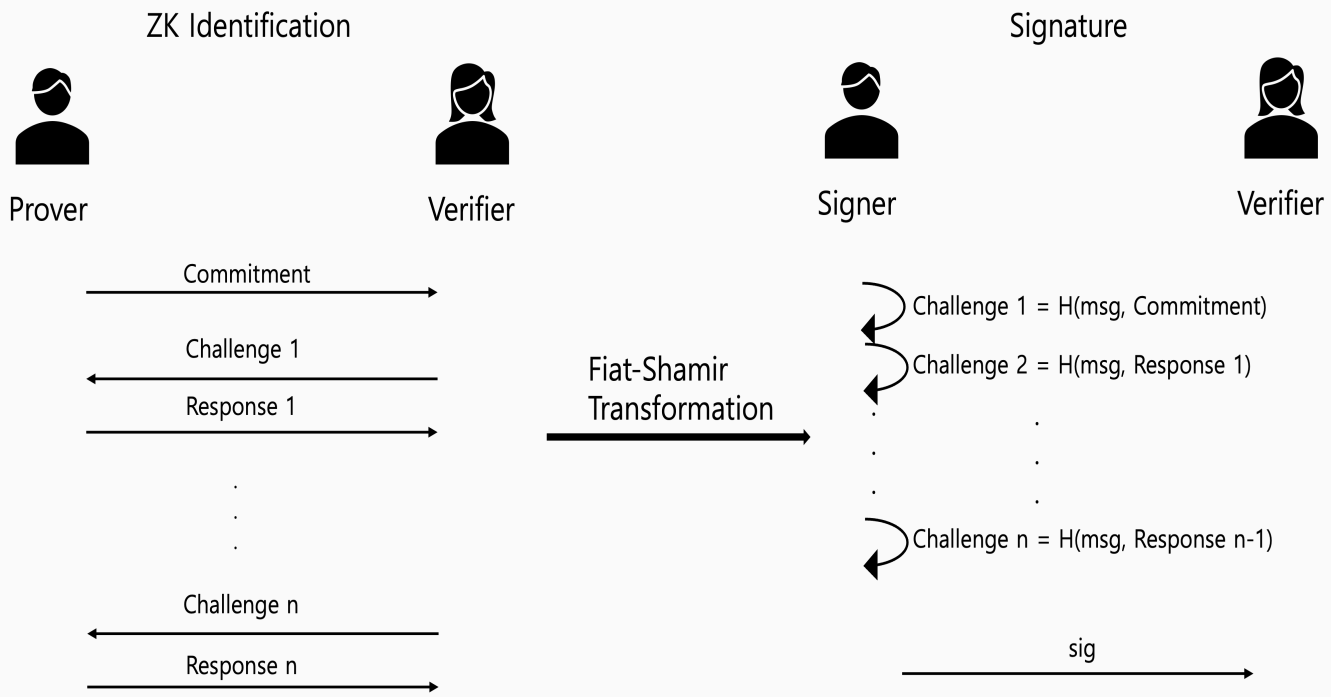
Wave [BCC+23]

- Follow the GPV framework
- Based on the hardness of the general syndrome decoding problem
- Provide a new trapdoor in code-based cryptography over permuted and generalized $(U, U + V)$ code
- Provide an efficient decoding algorithm for their setting

Table 2: Performance of Wave

Security	Sizes (Bytes)			Cycles (Mega Cycles)			
	Sig	SK	PK	KeyGen	Sign	Verify I	Verify II
128	$\leq$ 822	18,900	3,677,390	14,468	1,160	205	1.2
192	$\leq$ 1,249	27,630	7,867,598	47,222	3,507	464	2.5
256	$\leq$ 1,644	36,360	13,632,308	108,642	7,936	813	4.3

서명 설계 방법 II: ZK+Fiat-Shamir 변환



- Apply Fiat-Shamir transformation [FS86] to the ZK identification scheme
- Repeat several times to reduce the soundness error
- Large signature, short public key
- DL-Based: Schnorr signature
- **Code-Based**: **CROSS**, **LESS**, **MEDS**

* Figures in this slide referred to [Feb24].

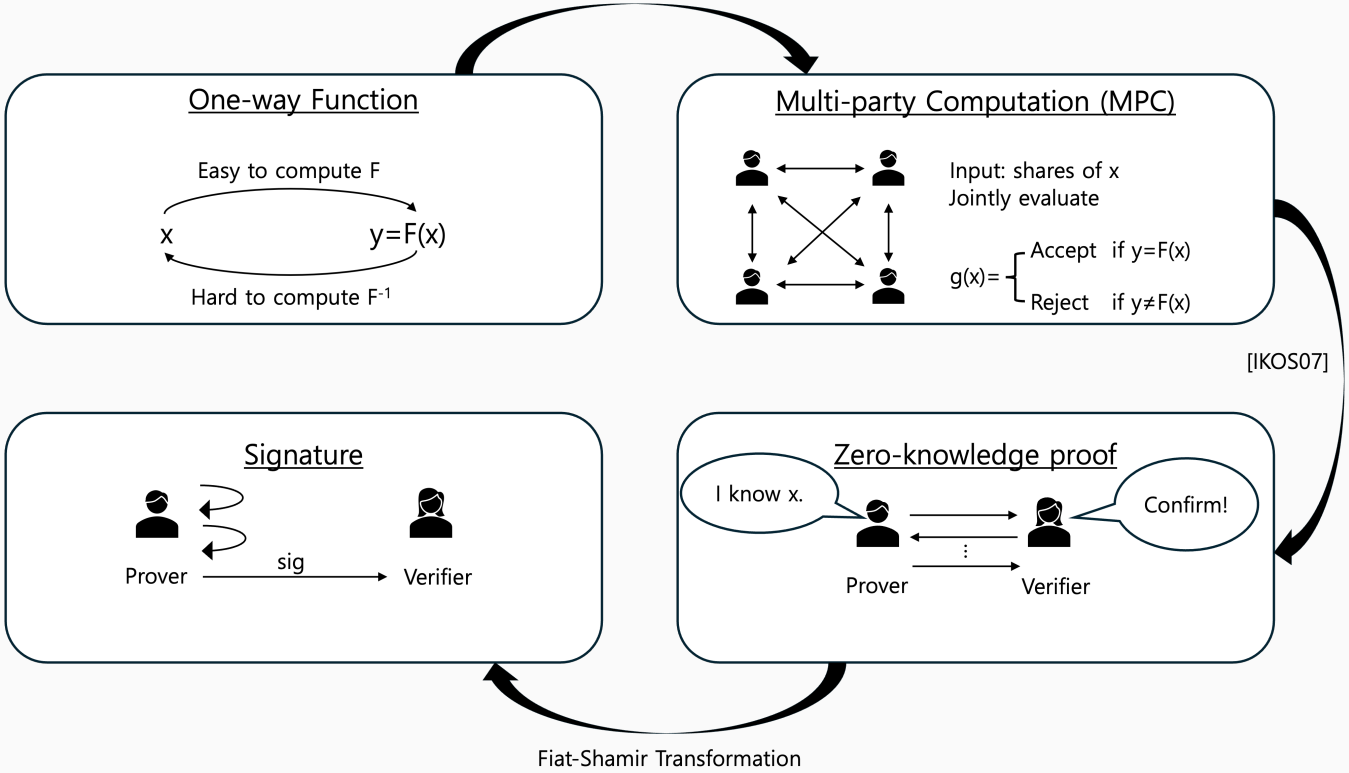
MEDS [CNP+23]

- Propose 3-pass ZK proof for the matrix code equivalence problem with rank metric codes
- Soundness error: $1/2$
- Repeat t times where $(1/2)^t \leq 2^{-\lambda}$ for the security parameter λ
- Present additional optimization techniques

Table 3: Performance of MEDS

Security	Parameter	Sizes (Bytes)			Cycles (Mega Cycles)		
		Sig	SK	PK	KeyGen	Sign	Verify
NIST I	MEDS9923	9,896	1,828	9,923	1.90	518.05	515.36
	MEDS13220	12,976	2,416	13,220	2.51	88.90	87.48
NIST III	MEDS41711	41,080	4,420	41,711	9.80	1467.00	1461.77
	MEDS55604	54,736	5,872	55,604	12.82	203.83	200.37
NIST V	MEDS134180	132,528	9,968	134,180	44.75	1629.84	1612.57
	MEDS167717	165,464	12,444	167,717	55.83	961.80	938.89

서명 설계 방법 III: MPC-in-the-Head+Fiat-Shamir 변환



- Transform a multi-party computation protocol into a ZK protocol [IKOS07] and then transform the ZK protocol into a signature scheme [FS86]
- 9 Submissions in Additional NIST Call: **AIMer**, Biscuit, FAEST, MIRA, MiRitH, MQOM, PERK, **RYDE**, **SDitH**

KpqC

Code-Based

* Figures in this slide referred to [Feb24].

RYDE [ABB+23]

- Follow the MPC-in-the-head paradigm
- Based on the hardness of the rank syndrome decoding problem
- Design an MPC protocol using threshold linear secret sharing scheme
- Propose a new linear secret sharing technique so called hypercube optimization
- Use the systematic form of the parity check matrix

Table 4: Performance of RYDE

Security	Parameter	Sizes (Bytes)			Cycles (Mega Cycles)		
		Sig	SK	PK	KeyGen	Sign	Verify
NIST I	RYDE-128F	7,446	32	86	0.033	5.4	4.4
	RYDE-128S	5,956	32	86	0.033	23.4	20.1
NIST III	RYDE-192F	16,380	48	131	0.048	12.2	10.7
	RYDE-192S	12,933	48	131	0.049	49.6	44.8
NIST V	RYDE-256F	29,134	64	188	0.072	26.0	22.7
	RYDE-256S	22,802	64	188	0.072	105.5	94.9

SDitH [FJR22]

- Follow the MPC-in-the-head paradigm
- Based on the hardness of the general syndrome decoding problem
- Use the systematic form of the parity check matrix

Table 5: Performance of SDitH

Instance	Size (KB)			Cycles (Mega Cycles)		
	Sig	SK	PK	KeyGen	Sign	Verify
SDitH-gf256-L1-thr	8,260	404	120	3.2	5.1	1.6
SDitH-gf256-L3-thr	19,206	616	183	3.9	14.8	4.9
SDitH-gf256-L5-thr	33,448	812	234	7.1	30.5	10.2
SDitH-gf251-L1-thr	10,424	404	120	1.7	4.4	0.6
SDitH-gf251-L3-thr	25,603	616	183	1.9	11.7	1.5
SDitH-gf251-L5-thr	45,160	812	234	3.7	23.9	3.2

Summary I: Feature Comparison

Table 6: Feature Comparison of Recent Code-Based Signatures

Scheme	Design	Underlying Assumption	Security
LESS [BBB+23a]	ZK+FS	CEP	
CROSS [BBB+23b]	ZK+FS	R-SD	
MEDS [CNP+23]	ZK+FS	CEP (Rank metric)	
Wave [BCC+23]	Hash-and-Sign	SD	
RYDE [ABB+23]	MPC-in-the-Head	SD (Rank metric)	
SDitH [FJR22]	MPC-in-the-Head	SD	
Enhanced pqsigRM [NCL+22]	Hash-and-Sign	SD	Broken [DLV24]
FuLeeca [RMB+23]	Hash-and-Sign	SD (Lee metric)	Broken [vWH24]

Summary II: Performance Comparison

Table 7: Performance comparison of Recent Secure Code-Based Signatures (for NIST Security Category I)

Scheme	Sizes (Bytes)			Cycles (Mega Cycles)		
	Sig	SK	PK	KeyGen	Sign	Verify
LESS	13,700	32	8,400	3.4	878.7	890.8
CROSS	8,665	16	**38**	0.03	**3.08**	**2.11**
MEDS	9,896	1,828	9,923	1.90	518.05	515.36
Wave	$\leq$ **822**	18,900	**3,677,390**	14,468	**1,160**	205
RYDE	7,446	32	86	0.03	5.4	4.4
SDitH	10,424	404	120	3.2	5.1	**1.6**

Thank you for your attention!

Questions?

References I

[ABB+23] N. Aragon, M. Bardet, L. Bidoux, J. -J. Chi-Dominguez, V. Dyseryn, T. Feneuil, P. Gaborit, A. Joux, M. Rivain, J. -P. Tillich, and A. Vincotte, RYDE specifications, NIST Additional Signatures, Round 1 Submission, 2023.

[BBB+23a] M. Baldi, A. Barenghi, L. Beckwith, J.-f. Biasse, A. Esser, K. Gaj, K. Mohajerani, G. Pelosi, E. Persichetti, M.-J. O. Saarinen, P. Santini, and R. Wallace, LESS: Linear equivalence signature scheme, NIST Additional Signatures, Round 1 Submission, 2023.

[BBB+23b] M. Baldi, A. Barenghi, S. Bitzer, P. Karl, F. Manganiello, A. Pavoni, G. Pelosi, P. Santini, J. Schupp, F. Slaughter, A. Wachter-Zeh, and V. Weger, CROSS: Codes and restricted objects signature scheme, NIST Additional Signatures, Round 1 Submission, 2023.

[BCC+23] G. Banegas, K. Carrier, A. Chailloux, A. Couvreur, T. Debris-Alazard, P. Gaborit, P. Karpman, J. Loyer, R. Niederhagen, N. Sendrier, B. Smith, and J. Tillich, Wave, NIST Additional Signature, Round 1 Submission, 2023.

[CNP+23] T. Chou, R. Niederhagen, E. Persichetti, T. H. Randrianarisoa, K. Reijnders, S. Samardjiska, and M. Trimoska, MEDS: Matrix Equivalence Digital Signature, NIST Additional Signatures, Round 1 Submission, 2023.

[DLV24] T. Debris-Alazard, P. Loisel, and V. Vasseur, Exploiting signature leakeages: Breaking Enhanced pqsigRM, ePrint Archive, 2024/1134.

[Feb24] T. Feneuil, Constructions for digital signature Part I: Introduction to MPC-in-the-Head, NIST PQC Seminar, 2024.

References II

[FJR22] T. Feneuil, A. Joux, and M. Rivain, Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs, CRYPTO 2022.

[IKOS07] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, Zero-knowledge from secure multiparty computation, STOC, 2007.

[KJKK24] D.-C. Kim, C.-Y. Jeon, Y. Kim, and M. Kim, PALOMA: Binary seperable Goppa-based KEM, KpqC 2 Round Submission, 2024.

[KHL+24] J.-L. Kim, J. Hong, T. S. C. Lau, Y. Lim, C. H. Tan, T. F. Prabowo, and B.-S. Won, REDOG, KpqC 2 Round Submission, 2024.

[NCL+22] J.-S. No, J. Cho, Y. Lee, Z. Koo, and Y.-S. Kim, Enhanced pqsigRM: Code-based digital signature scheme with short signature and fast verification for post-quantum cryptography, KpqC Call for Proposals, Round 1 Submission, 2022.

[RMB+23] S. Ritterhoff, G. Maringer, S. Bitzer, V. Weger, P. Karl, T. Schambeger, J. Schupp, and A. W.-Zeh, FuLeeca: A Lee-based signature scheme, NIST PQC Additional Signature, 2023.

[vWH24] W. van Woerden and F. Hörmann, FuLeakage: Breaking FuLeeca by learning attacks, Crypto 2024.