- Mirath -

G. Adj, N. Aragon, S. Barbero, M. Bardet, E. Bellini, L. Bidoux,
J.J. Chi-Domínguez, V. Dyseryn, A. Esser, T. Feneuil, P. Gaborit, R. Neveu
M. Rivain, L. Rivera-Zamarripa, C. Sanna, J.P. Tillich, J. Verbel, F. Zweydinger

NIST Sixth PQC Standardization Conference (09/25)

Overview

Mirath results from the merge between the round 1 candidates **MIRA** and **MiRitH**

- Fiat-Shamir (FS) based signature along with a Zero-Knowledge Proof of Knowledge (PoK)
- PoK built using the Multi-Party Computation in the Head (MPCitH) paradigm
- PoK relies on the hardness of the MinRank problem

https://pqc-mirath.org

Agenda

1. Round 2 Updates
2. MinRank Problem
3. Scheme Overview
4. Sizes & Performances
5. Advantages & Limitations

Round 2 Updates

Round 2 Updates

New results since Round 1

- New modeling for MinRank [BFG+24]
- New MPCitH frameworks - **TCitH** [FR25] & **VOLEitH** [BBD+23]

Round 2 Updates

New results since Round 1

- ◇ New modeling for MinRank [BFG+24]
- ◇ New MPCitH frameworks - **TCitH** [FR25] & **VOLEitH** [BBD+23]

Modifications for Round 2

- ◇ v2.0.0 - Merge between **MIRA** and **MiRitH**
  Design update using the new modeling along with the new MPCitH frameworks
- ◇ v2.0.1 - Implementation update
- ◇ v2.1.0 - Implementation update & MPC Parameters fine-tuning

Round 2 Updates

Instance	Modeling	Proof System	Size (pk + sig.)
MIRA (round 1)	Annihilator q-polynomial	MPCitH	5.7 - 7.4 kB
MiRitH (round 1)	Kipnis-Shamir	MPCitH	5.7 - 7.9 kB
Mirath (round 2)	**Dual Support Decomposition**	**TCitH** (& VOLEitH)	**3.0 - 3.8 kB**

Table 1: Modifications for Mirath (sizes are given for NIST-1 security level)

MinRank Problem

MinRank Problem

MinRank Problem

Input

- Secret values $\mathbf{x} \in \mathbb{F}_q^k$ and $\mathbf{E} \in \mathbb{F}_q^{m \times n}$ such that $\text{rank}(\mathbf{E}) \leq r$
- Public values $(\mathbf{M}_i)_{i \in [0,k]} \in \mathbb{F}_q^{m \times n}$ such that $\mathbf{E} = \mathbf{M}_0 + \sum_{i=1}^{k} x_i \mathbf{M}_i$ and $\text{rank}(\mathbf{E}) \leq r$

Goal

- Find $\tilde{\mathbf{x}} \in \mathbb{F}_q^k$ such that $\tilde{\mathbf{E}} = \mathbf{M}_0 + \sum_{i=1}^{k} \tilde{x}_i \mathbf{M}_i$ and $\text{rank}(\tilde{\mathbf{E}}) \leq r$

Syndrome MinRank Problem

The **Syndrome MinRank** problem is **equivalent** to the **MinRank** problem

- Let $\mathsf{vec} : \mathbb{F}_q^{m \times n} \to \mathbb{F}_q^{mn}$ be the application vectorizing matrices by column-major order
- Let $\mathbf{H}$ and $\mathbf{G} = \begin{pmatrix} \mathsf{vec}(\mathbf{M}_1) \\ \vdots \\ \mathsf{vec}(\mathbf{M}_k) \end{pmatrix}$ be respectively the parity-check matrix and the generator matrix of the matrix code $\mathcal{C} = \langle \mathbf{M}_1, \cdots, \mathbf{M}_k \rangle$ along with $\mathbf{y}^\top = \mathbf{H}\mathsf{vec}(\mathbf{M}_0)^\top$

Syndrome MinRank Problem

The **Syndrome MinRank** problem is **equivalent** to the **MinRank** problem

- Let vec : $\mathbb{F}_q^{m\times n} \to \mathbb{F}_q^{mn}$ be the application vectorizing matrices by column-major order
- Let $\mathbf{H}$ and $\mathbf{G} = \begin{pmatrix} \text{vec}(\mathbf{M}_1) \\ \vdots \\ \text{vec}(\mathbf{M}_k) \end{pmatrix}$ be respectively the parity-check matrix and the generator matrix of the matrix code $\mathcal{C} = \langle \mathbf{M}_1, \cdots, \mathbf{M}_k \rangle$ along with $\mathbf{y}^\top = \mathbf{H}\text{vec}(\mathbf{M}_0)^\top$

$$\mathbf{E} = \mathbf{M}_0 + \sum_{i=1}^{k} x_i \mathbf{M}_i \quad \Leftrightarrow \quad \mathbf{H}\text{vec}(\mathbf{E})^\top = \mathbf{H}\text{vec}(\mathbf{M}_0)^\top = \mathbf{y}^\top$$

Syndrome MinRank Problem

Syndrome MinRank Problem

Input

- Secret value $\mathbf{E} \in \mathbb{F}_q^{m \times n}$ such that $\text{rank}(\mathbf{E}) \leq r$
- Public values $\mathbf{H} \in \mathbb{F}_q^{(mn-k) \times mn}$ and $\mathbf{y} \in \mathbb{F}_q^{mn-k}$

Goal

- Find $\tilde{\mathbf{E}} \in \mathbb{F}_q^{m \times n}$ such that $\mathbf{H}\text{vec}(\tilde{\mathbf{E}})^\top = \mathbf{y}^\top$ and $\text{rank}(\tilde{\mathbf{E}}) \leq r$

Syndrome MinRank Problem

Syndrome MinRank Problem

Input

- Secret value $\mathbf{E} \in \mathbb{F}_q^{m \times n}$ such that $\text{rank}(\mathbf{E}) \leq r$
- Public values $\mathbf{H} \in \mathbb{F}_q^{(mn-k) \times mn}$ and $\mathbf{y} \in \mathbb{F}_q^{mn-k}$

Goal

- Find $\tilde{\mathbf{E}} \in \mathbb{F}_q^{m \times n}$ such that $\mathbf{H}\text{vec}(\tilde{\mathbf{E}})^\top = \mathbf{y}^\top$ and $\text{rank}(\tilde{\mathbf{E}}) \leq r$

Mirath relies on the hardness of the (***unstructured***) Syndrome MinRank problem

Scheme Overview

Modeling

Mirath relies on the Dual Support Decomposition modeling for MinRank [BFG+24]

- Modeling based on the syndrome version of the MinRank problem
- Modeling checking the rank of $\mathbf{E}$ using matrix decomposition
- Updated MinRank parameter sets to minimize the witness size

Modeling

Mirath relies on the Dual Support Decomposition modeling for MinRank [BFG+24]

- ◇ Modeling based on the syndrome version of the MinRank problem
- ◇ Modeling checking the rank of $\mathbf{E}$ using matrix decomposition
- ◇ Updated MinRank parameter sets to minimize the witness size

Instance	Modeling	Witness Size (for NIST-1 security level)	
MIRA	Annihilator q-polynomial	$[k + rm] \cdot \log_2(q)$	**76 B**
MiRitH	Kipnis Shamir	$[k + r(n-r)] \cdot \log_2(q)$	**66 B**
Mirath	Dual Support Decomposition	$[rm + r(n-r)] \cdot \log_2(q)$	**41 B**

Table 2: Mirath modeling and resulting witness sizes

Modeling

Protocol Overview

Public Input

- An instance $(\mathbf{H}, \mathbf{y})$ of the Syndrome MinRank problem

Private Input

- Matrix $\mathbf{S} \in \mathbb{F}_q^{m \times r}$ and matrix $\mathbf{C}' \in \mathbb{F}_q^{r \times (n-r)}$

Protocol

1. Verify the rank of $\mathbf{E}$ by computing $\mathbf{E} = \mathbf{S} \cdot (\mathbf{I}_r \;\; \mathbf{C}')$
2. Verify that $\mathbf{E}$ is a solution by checking $\mathbf{H}\mathrm{vec}(\mathbf{E})^\top = \mathbf{y}^\top$

Proof System

MPCitH Frameworks

- Two recent improvements to the MPCitH paradigm - **TCitH** [FR25] & **VOLEitH** [BBD+23]
- TCitH and VOLEitH can be described using the PIOP formalism [Fen24]

Proof System

MPCitH Frameworks

- Two recent improvements to the MPCitH paradigm - **TCitH** [FR25] & **VOLEitH** [BBD+23]
- TCitH and VOLEitH can be described using the PIOP formalism [Fen24]

TCitH

- **5**-round protocol
- Computation over a small field
- Several protocol repetitions
- *Arguably* simpler

VOLEitH

- **7**-round protocol
- Computation over a large field
- One protocol execution
- Smaller signatures

Proof System

Mirath & TCitH vs VOLEitH

- TCitH and VOLEitH lead to comparable sizes for modeling with low multiplicative depth
- Mirath modeling features a small multiplicative depth $d = 2$

Proof System

Mirath & TCitH vs VOLEitH

- TCitH and VOLEitH lead to comparable sizes for modeling with low multiplicative depth
- Mirath modeling features a small multiplicative depth $d = 2$

Mirath Instantiation

- Mirath is instantiated with the **TCitH** framework (with a VOLEitH variant also described)
- Mirath uses the *one tree* optimization for GGM trees [BBM+24]

Sizes & Performances

Implementation

Implementation Updates

- Overall improvement of the performances of the scheme
- Update of symmetric primitives (AES/Rijndael for some PRG, AES/Rijndael variant for cmt)
- Reported constant-time issues have been fixed [ABB+25]

Implementation

Implementation Updates

- Overall improvement of the performances of the scheme
- Update of symmetric primitives (AES/Rijndael for some PRG, AES/Rijndael variant for cmt)
- Reported constant-time issues have been fixed [ABB+25]

Fine-Tuning Parameters

- MPC parameters updated based on the new performance profile of Mirath

Implementation

Implementation Updates

- Overall improvement of the performances of the scheme
- Update of symmetric primitives (AES/Rijndael for some PRG, AES/Rijndael variant for cmt)
- Reported constant-time issues have been fixed [ABB+25]

Fine-Tuning Parameters

- MPC parameters updated based on the new performance profile of Mirath

Benchmark & Ongoing Work

- Numbers reported for the fastest variant of the optimized implementation (avx2 & aes-ni)
- Ongoing work targeting additional performance improvements

Sizes & Performances

Mirath-1 Instance			|sk|	|pk|	|sig.|	Keygen	Sign	Verify
Mirath-1a (v2.0.0)	Short	$q = 16$	32 B	73 B	3.1 kB	0.2 M	166 M	123 M
Mirath-1a (v2.1.0)	Short	$q = 16$	32 B	73 B	3.2 kB	0.1 M	16 M	14 M
Mirath-1b (v2.1.0)	Short	$q = 2$	32 B	57 B	3.0 kB	0.6 M	24 M	18 M
Mirath-1a (v2.0.0)	Fast	$q = 16$	32 B	73 B	3.8 kB	0.2 M	11 M	9.8 M
Mirath-1a (v2.1.0)	Fast	$q = 16$	32 B	73 B	3.8 kB	0.1 M	5.9 M	3.3 M
Mirath-1b (v2.1.0)	Fast	$q = 2$	32 B	57 B	3.5 kB	0.5 M	9.8 M	5.5 M

Table 3: Sizes and performances (CPU cycles) of Mirath (TCitH) for NIST-1 security level

Sizes & Performances

Mirath-5 Instance			|sk|	|pk|	|sig.|	Keygen	Sign	Verify
Mirath-5a (v2.0.0)	Short	$q = 16$	64 B	147 B	12.5 kB	0.4 M	1415 M	712 M
Mirath-5a (v2.1.0)	Short	$q = 16$	64 B	147 B	13.1 kB	0.4 M	132 M	119 M
Mirath-5b (v2.1.0)	Short	$q = 2$	64 B	112 B	12.3 kB	1.9 M	155 M	132 M
Mirath-5a (v2.0.0)	Fast	$q = 16$	64 B	147 B	15.6 kB	0.4 M	87 M	65 M
Mirath-5a (v2.1.0)	Fast	$q = 16$	64 B	147 B	15.5 kB	0.4 M	40 M	28 M
Mirath-5a (v2.1.0)	Fast	$q = 2$	64 B	112 B	14.2 kB	2.0 M	70 M	52 M

Table 4: Sizes and performances (CPU cycles) of Mirath (TCitH) for NIST-5 security level

Comparison to other schemes

- Stay tuned till the end of the session -

Overview of MPCitH based Signatures using the ***PQ-SORT*** *benchmarking tool*

Advantages & Limitations

Advantages & Limitations

Advantages

- *Security* - Well established MinRank problem
  Conservative approach based on unstructured instances

Advantages & Limitations

Advantages

- *Security* - Well established MinRank problem
  Conservative approach based on unstructured instances
- *Parameters* - Adaptive and easily tunable parameters & Resilience against attacks

Advantages & Limitations

Advantages

- *Security* - Well established MinRank problem
  Conservative approach based on unstructured instances
- *Parameters* - Adaptive and easily tunable parameters & Resilience against attacks
- *Size* - Small public keys & Competitive signature size
  $|\text{pk+sig.}| \Rightarrow$ **3.0 - 3.2 kB** for Mirath, **3.7 kB** for ML-DSA, **7.8 kB** for SLH-DSA (for NIST-1 level)

Advantages & Limitations

Advantages

- *Security* - Well established MinRank problem
  Conservative approach based on unstructured instances
- *Parameters* - Adaptive and easily tunable parameters & Resilience against attacks
- *Size* - Small public keys & Competitive signature size
  $|\text{pk+sig.}| \Rightarrow$ **3.0 - 3.2 kB** for Mirath, **3.7 kB** for ML-DSA, **7.8 kB** for SLH-DSA (for NIST-1 level)

Limitations

- *Size* - Quadratic growth of signature sizes with respect to security level

Advantages & Limitations

Advantages

- *Security* - Well established MinRank problem
  Conservative approach based on unstructured instances
- *Parameters* - Adaptive and easily tunable parameters & Resilience against attacks
- *Size* - Small public keys & Competitive signature size
  $|\text{pk+ sig.}| \Rightarrow$ **3.0 - 3.2 kB** for Mirath, **3.7 kB** for ML-DSA, **7.8 kB** for SLH-DSA (for NIST-1 level)

Limitations

- *Size* - Quadratic growth of signature sizes with respect to security level
- *Performances* - Slower than lattice-based signature schemes
  But competitive with many other post-quantum signatures

Thank you for your attention.

References I

[ABB+25] Olivier Adjonyo, Sebastien Bardin, Emanuele Bellini, Gilbert Ndollane Dione, Mahmudul Faisal Al Ameen, Robert Merget, Frederic Recoules, and Yanis Sellami.
Systematic timing leakage analysis of nist pqdss candidates: Tooling and lessons learned.
arXiv preprint arXiv:2509.04010, 2025.

[BBD+23] Carsten Baum, Lennart Braun, Cyprien Delpech de Saint Guilhem, Michael Klooß, Emmanuela Orsini, Lawrence Roy, and Peter Scholl.
Publicly verifiable zero-knowledge and post-quantum signatures from VOLE-in-the-head.
In Helena Handschuh and Anna Lysyanskaya, editors, CRYPTO 2023, Part V, volume 14085 of LNCS, pages 581–615. Springer, Cham, August 2023.

[BBM+24] Carsten Baum, Ward Beullens, Shibam Mukherjee, Emmanuela Orsini, Sebastian Ramacher, Christian Rechberger, Lawrence Roy, and Peter Scholl.
One tree to rule them all: Optimizing ggm trees and owfs for post-quantum signatures.
In International Conference on the Theory and Application of Cryptology and Information Security, pages 463–493. Springer, 2024.

[BFG+24] Loïc Bidoux, Thibauld Feneuil, Philippe Gaborit, Romaric Neveu, and Matthieu Rivain.
Dual support decomposition in the head: Shorter signatures from rank SD and MinRank.
In Kai-Min Chung and Yu Sasaki, editors, ASIACRYPT 2024, Part II, volume 15485 of LNCS, pages 38–69. Springer, Singapore, December 2024.

References II

[Fen24] Thibauld Feneuil.
The polynomial-iop vision of the latest mpcith framework for signature schemes.
PQ Algebraic Cryptography Workshop, 2024.

[FR25] Thibauld Feneuil and Matthieu Rivain.
Threshold computation in the head: Improved framework for post-quantum signatures and zero-knowledge arguments.
Journal of Cryptology, 38(3):28, 2025.