- RYDE -

N. Aragon, M. Bardet, L. Bidoux, J.J. Chi-Domínguez, V. Dyseryn, T. Feneuil,
P. Gaborit, A. Joux, R. Neveu, M. Rivain, J.P. Tillich, A. Vinçotte

NIST Sixth PQC Standardization Conference (09/25)

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY
CryptoExperts WE INNOVATE TO SECURE YOUR BUSINESS
Inria
litis
SORBONNE UNIVERSITÉ
TII Technology Innovation Institute
UNIVERSITÉ DE ROUEN NORMANDIE
xlim INSTITUT DE RECHERCHE

Overview

RYDE is a digital signature scheme named after the **R**ank S**Y**ndrome **DE**coding problem

- 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 Rank Syndrome Decoding problem (RSD)

https://pqc-ryde.org

Agenda

1 Round 2 Updates

2 RSD Problem

3 Scheme Overview

4 Sizes & Performances

5 Advantages & Limitations

Round 2 Updates

Round 2 Updates

New results since Round 1

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

Round 2 Updates

New results since Round 1

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

Modifications for Round 2

- v2.0.0 - Design update using the new modeling along with new MPCitH frameworks
- v2.0.1 - Implementation update
- v2.1.0 - Implementation update & Parameters fine-tuning

Round 2 Updates

RYDE Instance	Modeling	Proof System	Size (pk + sig.)
Round 1	Annihilator q-polynomial	MPCitH	6.1 - 7.6 kB
Round 2	**Dual Support Decomposition**	**TCitH** (& VOLEitH)	**3.2 - 3.7 kB**

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

RSD Problem

Rank Metric

RYDE relies on **code-based cryptography** in the **rank metric** setting

$$\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n \quad \Leftrightarrow \quad \mathbf{M}_{\mathbf{x}} = \begin{bmatrix} x_{1,1} & \cdots & x_{n,1} \\ \vdots & \ddots & \vdots \\ x_{1,m} & \cdots & x_{n,m} \end{bmatrix} \in \mathbb{F}_q^{m \times n}$$

Rank Metric

RYDE relies on **code-based cryptography** in the **rank metric** setting

$$\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n \qquad \Leftrightarrow \qquad \mathbf{M_x} = \begin{bmatrix} x_{1,1} & \cdots & x_{n,1} \\ \vdots & \ddots & \vdots \\ x_{1,m} & \cdots & x_{n,m} \end{bmatrix} \in \mathbb{F}_q^{m \times n}$$

- *Supp*$(\mathbf{x}) = \langle x_1, \ldots, x_n \rangle_{\mathbb{F}_q}$
- $w_R(\mathbf{x}) = \text{rank}(\mathbf{M_x})$

RSD Problem

Rank Syndrome Decoding Problem

Input

- Secret value $\mathbf{x} \in \mathbb{F}_{q^m}^n$ such that $w_R(\mathbf{x}) = r$
- Public values $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ and $\mathbf{y} \in \mathbb{F}_{q^m}^{n-k}$ such that $\mathbf{x}\mathbf{H}^\top = \mathbf{y}$

Goal

- Find $\tilde{\mathbf{x}} \in \mathbb{F}_{q^m}^n$ such that $\tilde{\mathbf{x}}\mathbf{H}^\top = \mathbf{y}$ and $w_R(\tilde{\mathbf{x}}) = r$

RSD Problem

Rank Syndrome Decoding Problem

Input

- Secret value $\mathbf{x} \in \mathbb{F}_{q^m}^n$ such that $w_R(\mathbf{x}) = r$
- Public values $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ and $\mathbf{y} \in \mathbb{F}_{q^m}^{n-k}$ such that $\mathbf{x}\mathbf{H}^\top = \mathbf{y}$

Goal

- Find $\tilde{\mathbf{x}} \in \mathbb{F}_{q^m}^n$ such that $\tilde{\mathbf{x}}\mathbf{H}^\top = \mathbf{y}$ and $w_R(\tilde{\mathbf{x}}) = r$

RYDE relies on the hardness of the RSD problem (***without*** *cyclic structure*)

Scheme Overview

Modeling

RYDE v2 relies on the Dual Support Decomposition modeling for RSD [BFG+24]

- Natural modeling checking the weight of $\mathbf{x}$ using matrix decomposition
- Updated RSD parameter sets to minimize the witness size

Modeling

RYDE v2 relies on the Dual Support Decomposition modeling for RSD [BFG+24]

- Natural modeling checking the weight of $\mathbf{x}$ using matrix decomposition
- Updated RSD parameter sets to minimize the witness size

RYDE Instance	Modeling	Witness Size (for NIST-1 security level)	
Round 1	Annihilator q-polynomial	$[(r-1)m + km] \cdot \log_2(q)$	**93 B**
Round 2	Dual Support Decomposition	$[(r-1)m + r(n-r)] \cdot \log_2(q)$	**45 B**

Table 2: RYDE modeling and resulting witness sizes

Modeling

Protocol Overview

Public Input

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

Private Input

- Coefficients $\mathbf{s}' \in \mathbb{F}_{q^m}^{(r-1)}$ of a basis $\mathbf{s} = (\mathbf{1} \;\; \mathbf{s}')$ of the support of $\mathbf{x}$
- Coefficients $\mathbf{C}' \in \mathbb{F}_q^{r \times (n-r)}$ of the support decomposition of $\mathbf{x}$ with respect to $\mathbf{s}$

Protocol

1. Verify the weight of $\mathbf{x}$ by computing $\mathbf{x} = \mathbf{s} \cdot (\mathbf{I}_r \;\; \mathbf{C}')$
2. Verify that $\mathbf{x}$ is a solution by checking $\mathbf{x}\mathbf{H}^\top = \mathbf{y}$

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

RYDE & TCitH vs VOLEitH

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

Proof System

RYDE & TCitH vs VOLEitH

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

RYDE Instantiation

- RYDE is instantiated with the **TCitH** framework (with a VOLEitH variant also described)
- RYDE 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

- RSD parameters updated for NIST-5 security level based on performance considerations
- MPC parameters updated based on the new performance profile of RYDE

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

- RSD parameters updated for NIST-5 security level based on performance considerations
- MPC parameters updated based on the new performance profile of RYDE

Benchmark & Ongoing Work

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

Sizes & Performances

RYDE-1 Instance		|sk|	|pk|	|sig.|	Keygen	Sign	Verify
Round 1	Short	32 B	86 B	6.0 kB	33 K	23 M	20 M
Round 2 (v2.1.0)	Short	32 B	69 B	3.2 kB	34 K	18 M	15 M
Round 1	Fast	32 B	86 B	7.5 kB	33 K	5.4 M	4.4 M
Round 2 (v2.1.0)	Fast	32 B	69 B	3.6 kB	34 K	7.0 M	2.8 M
Round 2 (v2.1.0)	Faster	32 B	69 B	5.0 kB	34 K	1.7 M	0.9 M

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

Sizes & Performances

RYDE-5 Instance		|sk|	|pk|	|sig.|	Keygen	Sign	Verify
Round 1	Short	64 B	188 B	22.9 kB	72 K	106 M	95 M
Round 2 (v2.1.0)	Short	64 B	133 B	12.7 kB	67 K	141 M	131 M
Round 1	Fast	64 B	188 B	29.2 kB	72 K	26 M	23 M
Round 2 (v2.1.0)	Fast	64 B	133 B	14.8 kB	67 K	29 M	24 M
Round 2 (v2.1.0)	Faster	64 B	133 B	20.9 kB	67 K	7.3 M	6.6 M

Table 4: Sizes and performances (CPU cycles) of RYDE (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* - Standard code-based assumption in the rank metric setting
  Conservative approach that does not rely on cyclic structure

Advantages & Limitations

Advantages

- *Security* - Standard code-based assumption in the rank metric setting
  Conservative approach that does not rely on cyclic structure
- *Parameters* - Adaptive and easily tunable parameters & Resilience against attacks

Advantages & Limitations

Advantages

- *Security* - Standard code-based assumption in the rank metric setting
  Conservative approach that does not rely on cyclic structure
- *Parameters* - Adaptive and easily tunable parameters & Resilience against attacks
- *Size* - Small public keys & Competitive signature size
  $|\text{pk+ sig.}| \Rightarrow$ **3.2 kB** for RYDE, **3.7 kB** for ML-DSA, **7.8 kB** for SLH-DSA (for NIST-1 level)

Advantages & Limitations

Advantages

- *Security* - Standard code-based assumption in the rank metric setting
  Conservative approach that does not rely on cyclic structure
- *Parameters* - Adaptive and easily tunable parameters & Resilience against attacks
- *Size* - Small public keys & Competitive signature size
  $|\text{pk} + \text{sig.}| \Rightarrow$ **3.2 kB** for RYDE, **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* - Standard code-based assumption in the rank metric setting
  Conservative approach that does not rely on cyclic structure
- *Parameters* - Adaptive and easily tunable parameters & Resilience against attacks
- *Size* - Small public keys & Competitive signature size
  $|\text{pk} + \text{sig.}| \Rightarrow$ **3.2 kB** for RYDE, **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.