Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

CrypTO CONFERENCE

Politecnico di Torino 1859

Telsy | A TIM ENTERPRISE BRAND

DISMA

Partial key exposure attacks on NIST rank-based candidates

Giuseppe D'Alconzo   Andre Esser   Andrea Gangemi   Carlo Sanna

CrypTO Conference 2025, Torino

Politecnico di Torino
Technology Innovation Institute

Motivation

- PQC schemes have been proven to not be leakage resistant [EMVW ’22, KM ’22][1,2]

- No scheme submitted to the new NIST call for digital signatures was investigated from this perspective

1 Andre Esser, Alexander May, Javier A. Verbel, and Weiqiang Wen. *Partial key exposure attacks on BIKE, rainbow and NTRU*, Crypto 2022.
2 Elena Kirshanova and Alexander May, *Decoding McEliece with a Hint–Secret Goppa Key Parts Reveal Everything*, SCN 2022.

Motivation

- PQC schemes have been proven to not be leakage resistant [EMVW ’22, KM ’22][1,2]

- No scheme submitted to the new NIST call for digital signatures was investigated from this perspective

We analyze the leakage resistance of (Round I) Rank-based candidates, that is RYDE, MiRitH and MIRA

1 Andre Esser, Alexander May, Javier A. Verbel, and Weiqiang Wen. *Partial key exposure attacks on BIKE, rainbow and NTRU*, Crypto 2022.
2 Elena Kirshanova and Alexander May, *Decoding McEliece with a Hint–Secret Goppa Key Parts Reveal Everything*, SCN 2022.

NIST Candidates, Round 1

Code-Based

CROSS
Enhanced pqsigRM
FuLeeca
LESS
MEDS
WAVE

Other

ALTEQ
eMLE-Sig 2.0
KAZ-SIGN
PREON
Xifrat1-Sign.I

Lattice-Based

EagleSign
EHTv4
HAETAE
HAWK
HuFu
Raccoon
SQUIRRELS

Symmetric-Based

AIMer
Ascon-Sign
FAEST
SPHINCS-alpha

MPC-in-the-Head

Biscuit
MIRA*
MiRitH*
MQOM
PERK
RYDE
SDitH

Isogeny-Based

SQIsign

Multivariate

3WISE
DME-Sign
HPPC
MAYO
PROV
QR-UOV
SNOVA
TUOV
UOV
VOX

NIST Candidates, Round 2

- CROSS
- FAEST
- HAWK
- LESS
- MAYO
- Mirath (merger of **MIRA**/**MiRitH**)
- MQOM
- PERK
- QR-UOV
- **RYDE**
- SDitH
- SNOVA
- SQIsign
- UOV

Methodology

- We answer the following questions:
  - *Erasure model*: given a n-bit *erased* secret key where t bits are leaked, what is the security of the remaining $n - t$ bits?
  - *Error model*: given a n-bit *erroneous* secret key where every bit is swapped with probability p, can we recover the secret key?

Methodology

- We answer the following questions:
  - *Erasure model*: given a n-bit *erased* secret key where t bits are leaked, what is the security of the remaining $n - t$ bits?
  - *Error model*: given a n-bit *erroneous* secret key where every bit is swapped with probability p, can we recover the secret key?

- Asymptotic leakage bounds (poly-time)

Methodology

- We answer the following questions:
  - *Erasure model*: given a n-bit *erased* secret key where t bits are leaked, what is the security of the remaining $n - t$ bits?
  - *Error model*: given a n-bit *erroneous* secret key where every bit is swapped with probability p, can we recover the secret key?

- Asymptotic leakage bounds (poly-time)

- Practical leakage bounds

RYDE, MiRitH and MIRA

Secret Keys and Witness

RYDE (Rank-SD):
a rank-r vector x over $\mathbb{F}_{2^m}$ of length n such that $Hx = s$

Secret Keys and Witness

RYDE (Rank-SD):
a rank-r vector x over $\mathbb{F}_{2^m}$ of length n such that $Hx = s$

MiRitH and MIRA (MinRank):
coefficients $\alpha_1, \dots, \alpha_k \in \mathbb{F}_{16}$ s.t. the matrix $E = M_0 + \sum_{i=1}^{k} \alpha_i M_i$ of dimension $m \times n$ on $\mathbb{F}_{16}$ has rank r

Secret Keys and Witness

RYDE (Rank-SD):
a rank-r vector x over $\mathbb{F}_{2^m}$ of length n such that $Hx = s$

MiRitH and MIRA (MinRank):
coefficients $\alpha_1, \dots, \alpha_k \in \mathbb{F}_{16}$ s.t. the matrix $E = M_0 + \sum_{i=1}^{k} \alpha_i M_i$ of dimension $m \times n$ on $\mathbb{F}_{16}$ has rank r

RYDE Witness (resp. MIRA):
coefficients $\beta_0, \dots, \beta_{r-1} \in \mathbb{F}_{q^m}$ of a q-polynomial constructed from the solution x ($\alpha_1, \dots, \alpha_k$)

q-polynomials [Ore '33][1]

Let $x = (x_1, \ldots, x_n)$ be a Rank-SD solution. Let U be the rank-r linear subspace generated by the support of x. The q-polynomial is defined as

$$L_U(X) = \prod_{u \in U} (X - u) = X^{q^r} + \sum_{i=0}^{r-1} \beta_i X^{q^i}$$

1 Oystein Ore. *On a special class of polynomials*. Transactions of the American Mathematical Society.

q-polynomials [Ore '33][1]

Let $x = (x_1, \dots, x_n)$ be a Rank-SD solution. Let U be the rank-r linear subspace generated by the support of x. The q-polynomial is defined as

$$L_U(X) = \prod_{u \in U} (X - u) = X^{q^r} + \sum_{i=0}^{r-1} \beta_i X^{q^i}$$

MIRA: x is the vector whose entries are the columns of E seen as elements of $\mathbb{F}_{q^m}$

1 Oystein Ore. *On a special class of polynomials*. Transactions of the American Mathematical Society.

The GRS Algorithm [GRS ’15][1]

- Aim to find a subspace $F \subset \mathbb{F}_{q^m}$ that contains $U = \mathrm{supp}(x)$

1 Philippe Gaborit, Olivier Ruatta, and Julien Schrek. *On the complexity of he rank syndrome decoding problem*. IEEE Transactions on Information Theory.

The GRS Algorithm [GRS ’15][1]

- Aim to find a subspace $F \subset \mathbb{F}_{q^m}$ that contains $U = \mathrm{supp}(x)$

- Strategy: choose a random F of dimension r' and suppose $\mathrm{U} \subset F$.
  Express every component x_i of x w.r.t. a basis of F, that is $x_i = \sum_{j=1}^{r'} \gamma_{i,j} f_j$ for some unknown coefficients $\gamma_{i,j} \in \mathbb{F}_2$ (nr'unknowns)

1 Philippe Gaborit, Olivier Ruatta, and Julien Schrek. *On the complexity of he rank syndrome decoding problem*. IEEE Transactions on Information Theory.

The GRS Algorithm [GRS '15][1]

- Aim to find a subspace $F \subset \mathbb{F}_{q^m}$ that contains $U = \text{supp}(x)$

- Strategy: choose a random F of dimension r' and suppose $\mathrm{U} \subset F$. Express every component x_i of x w.r.t. a basis of F, that is $x_i = \sum_{j=1}^{r'} \gamma_{i,j} f_j$ for some unknown coefficients $\gamma_{i,j} \in \mathbb{F}_2$ (nr' unknowns)

- The relation $Hx = s$ gives $n - k$ linear equations on $\mathbb{F}_{2^m}$, that can be embedded into $(n-k)m$ linear equations on $\mathbb{F}_2$

1 Philippe Gaborit, Olivier Ruatta, and Julien Schrek. *On the complexity of he rank syndrome decoding problem*. IEEE Transactions on Information Theory.

The GRS Algorithm [GRS '15][1]

- Aim to find a subspace $F \subset \mathbb{F}_{q^m}$ that contains $U = \mathrm{supp}(x)$

- Strategy: choose a random F of dimension r' and suppose $\mathrm{U} \subset F$.
  Express every component x_i of x w.r.t. a basis of F, that is $x_i = \sum_{j=1}^{r'} \gamma_{i,j} f_j$ for some unknown coefficients $\gamma_{i,j} \in \mathbb{F}_2$ (nr'unknowns)

- The relation $Hx = s$ gives $n - k$ linear equations on $\mathbb{F}_{2^m}$, that can be embedded into $(n-k)m$ linear equations on $\mathbb{F}_2$

- Choose $r' = \left\lceil \frac{m(n-k)}{n} \right\rceil$, solve the linear system and repeat the attack until the found solution x has rank r

1 Philippe Gaborit, Olivier Ruatta, and Julien Schrek. *On the complexity of he rank syndrome decoding problem*. IEEE Transactions on Information Theory.

The Erasure Model

Secret key 1 1 0 1 0 1 1 0 0 1 1 1 1 0 1 0 0 1 0

Erased key 1 ? 0 1 ? ? ? 0 0 ? 1 ? 1 0 ? 0 ? ? 0

The Erasure Model

Secret key 1 1 0 1 0 1 1 0 0 1 1 1 1 0 1 0 0 1 0

$$\mathbb{P}[1 \to ?] = \mathbb{P}[0 \to ?]$$

Erased key 1 ? 0 1 ? ? ? 0 0 ? 1 ? 1 0 ? 0 ? ? 0

Rank-SD attack

- Suppose we know t bits of a RYDE private key. Every bit gives one extra linear equation we can use to enhance the GRS attack

1 Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich. *A new algorithm for solving the rank syndrome decoding problem*, ISIT 2018.

Rank-SD attack

- Suppose we know t bits of a RYDE private key. Every bit gives one extra linear equation we can use to enhance the GRS attack

- We can take $r' = \left\lceil \frac{m(n-k)+t}{n} \right\rceil$ and proceed as before until the found solution has rank r

1 Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich. *A new algorithm for solving the rank syndrome decoding problem*, ISIT 2018.

Rank-SD attack

- Suppose we know t bits of a RYDE private key. Every bit gives one extra linear equation we can use to enhance the GRS attack

- We can take $r' = \left\lceil \frac{m(n-k)+t}{n} \right\rceil$ and proceed as before until the found solution has rank r

- The GRS algorithm has been improved in [AGHT '18][1] by exploiting the $\mathbb{F}_{2^m}$-linearity of the code. Our attack can easily be adapted to this modeling

1 Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich. *A new algorithm for solving the rank syndrome decoding problem*, ISIT 2018.

Impact on RYDE Parameters

- We achieve reduced complexity even ***without additional knowledge*** *f*or RYDE

Impact on RYDE Parameters

- We achieve reduced complexity even ***without additional knowledge*** *f*or RYDE

Exploit the ceiling: guess t bits such that we get the same number of equations and unknowns

Impact on RYDE Parameters

- We achieve reduced complexity even ***without additional knowledge*** for RYDE

Exploit the ceiling: guess t bits such that we get the same number of equations and unknowns

Reapply the attack for all 2^t possible choices to reduce the complexity of 9 and 6 bits for RYDE NIST-I and NIST-III (Round I) parameters respectively

RYDE (Round I) bounds

	Bit security		Erasure rate p	
	RYDE submission	This work	Polynomial	60-bit
NIST I	**147**	**138**	**0.61**	**0.71**
NIST III	**216**	**210**	**0.59**	**0.67**
NIST V	**283**	**283**	**0.64**	**0.69**

MinRank Attack

- Original instance: parameters (m, n, k, r) over $\mathbb{F}_{16}$

MinRank Attack

- Original instance: parameters (m, n, k, r) over $\mathbb{F}_{16}$

- New instance: parameters $(4m, 4n, 4k, 4r)$ over $\mathbb{F}_2$

MinRank Attack

- Original instance: parameters (m, n, k, r) over $\mathbb{F}_{16}$
- New instance: parameters $(4m, 4n, 4k, 4r)$ over $\mathbb{F}_2$
- Incorporate knowledge: parameters $(4m, 4n, 4k - t, 4r)$ over $\mathbb{F}_2$

MinRank Attack

- Original instance: parameters (m, n, k, r) over $\mathbb{F}_{16}$
- New instance: parameters $(4m, 4n, 4k, 4r)$ over $\mathbb{F}_2$
- Incorporate knowledge: parameters $(4m, 4n, 4k - t, 4r)$ over $\mathbb{F}_2$
- Solve the latter instance with any MinRank algorithm (e.g. Kernel-Search)

MinRank bounds

Erasure rate p, 2^{60} operations	MIRA	MiRitH "a"
NIST I	0.27	0.26
NIST III	0.14	0.18
NIST V	0.10	0.11

Partial Exposure of the q-polynomial

- Suppose to know t bits of the coefficients $\beta_0, \ldots, \beta_{r-1} \in \mathbb{F}_{q^m}$ of a q-polynomial

Partial Exposure of the q-polynomial

- Suppose to know t bits of the coefficients $\beta_0, \dots, \beta_{r-1} \in \mathbb{F}_{q^m}$ of a q-polynomial

- Recovering the unknown coefficients is equivalent to solving a MinRank instance of parameters $(mv, mv, mvr - t, (m-r)v)$ over $\mathbb{F}_2$ (for RYDE, $v = 1$; for MIRA, $v = 4$)

Partial Exposure of the q-polynomial

- Suppose to know t bits of the coefficients $\beta_0, \ldots, \beta_{r-1} \in \mathbb{F}_{q^m}$ of a q-polynomial

- Recovering the unknown coefficients is equivalent to solving a MinRank instance of parameters $(mv, mv, mvr - t, (m-r)v)$ over $\mathbb{F}_2$ (for RYDE, $v = 1$; for MIRA, $v = 4$)

- Solve the latter instance with any MinRank algorithm

Partial Exposure of the q-polynomial

- Suppose to know t bits of the coefficients $\beta_0, \ldots, \beta_{r-1} \in \mathbb{F}_{q^m}$ of a q-polynomial

- Recovering the unknown coefficients is equivalent to solving a MinRank instance of parameters $(mv, mv, mvr - t, (m-r)v)$ over $\mathbb{F}_2$ (for RYDE, $v = 1$; for MIRA, $v = 4$)

- Solve the latter instance with any MinRank algorithm

- Unique solution as long as $t > mvr - vr^2$

Bounds

Erasure rate p, 2^{60}operations	RYDE	MIRA
NIST I	0.21	0.14
NIST III	0.12	0.09
NIST V	0.09	0.08

The Error Model

Secret key x 1 1 0 1 0 1 1 0 0 1 1 1 1 0 1 0 0 1 0

Erroneous key $\tilde{x}$ 1 0 0 1 0 0 1 0 0 0 1 1 1 0 0 0 1 1 0

The Error Model

Secret key x 1 1 0 1 0 1 1 0 0 1 1 1 1 0 1 0 0 1 0

$$\mathbb{P}[1 \to 0] = \mathbb{P}[0 \to 1] = p$$

Erroneous key $\tilde{x}$ 1 0 0 1 0 0 1 0 0 0 1 1 1 0 0 0 1 1 0

The Error Model

Secret key x 1 1 0 1 0 1 1 0 0 1 1 1 1 0 1 0 0 1 0

$$\mathbb{P}[1 \to 0] = \mathbb{P}[0 \to 1] = p$$

Erroneous key $\tilde{x}$ 1 0 0 1 0 0 1 0 0 0 1 1 1 0 0 0 1 1 0

$$\tilde{x} = x + e$$

General Strategy (RYDE)

- Generic translation of the erasure attack to the error setting

General Strategy (RYDE)

- Generic translation of the erasure attack to the error setting
- We exploit the sparseness of e by guessing zeros in the error vector and then perform the erasure-enhanced (improved) GRS attack

General Strategy (RYDE)

- Generic translation of the erasure attack to the error setting
- We exploit the sparseness of e by guessing zeros in the error vector and then perform the erasure-enhanced (improved) GRS attack
- Polynomial-time recovery if $p = O\left(\frac{\log(nm)}{nm}\right)$

General Strategy (RYDE)

- Generic translation of the erasure attack to the error setting
- We exploit the sparseness of e by guessing zeros in the error vector and then perform the erasure-enhanced (improved) GRS attack
- Polynomial-time recovery if $p = O\left(\frac{\log(nm)}{nm}\right)$
- Similar attacks for MinRank schemes and q-polynomial setting. No polynomial regime

Conclusion and Open Questions

- Non-trivial polynomial time recovery for RYDE, plus an improvement of the best generic attack
- Efficient attack for MIRA and MiRitH as long as roughly 73-74% of the secret key material is leaked (NIST-I)
- Initiated the study of partial exposure of the witness in constructions following the MPC-in-the-Head paradigm

Conclusion and Open Questions

- Non-trivial polynomial time recovery for RYDE, plus an improvement of the best generic attack
- Efficient attack for MIRA and MiRitH as long as roughly 73-74% of the secret key material is leaked (NIST-I)
- Initiated the study of partial exposure of the witness in constructions following the MPC-in-the-Head paradigm
- **Can we design an algorithm that is able to exploit information on the witness as well as the secret key?**

THANKS! QUESTIONS?

https://eprint.iacr.org/2024/2070