A QC-LDPC code-based public-key cryptosystem resistant to reaction attacks

Paolo Santini

Università Politecnica delle Marche
p.santini@pm.univpm.it

Code-Based Cryptography Workshop 2018

Fort Lauderdale, Florida, USA
April 5-6, 2018

Code-based cryptography

- The use of codes for cryptographic purposes was initiated by McEliece in 1978, proposing a cryptosystem based on Goppa codes.
- The main drawback of code-based cryptosystems is represented by the dimension of the public key.
- In the binary case, the smallest key sizes are reached when quasi-cyclic (QC) sparse codes are used.

- R. McEliece, "Public-Key System Based on Algebraic Coding Theory," DSN Progress Report 44, pp. 114–116, 1978.
- M. Baldi, F. Chiaraluce: "Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes," In: Proc. IEEE ISIT 2007, pp. 2591-2595, Nice, 2007.
- R. Misoczki, J-P. Tillich, N. Sendrier, P.S.L.M. Barreto : "MDPC-McEliece: new McEliece variants from moderate density parity-check codes," In: IEEE International Symposium on Information Theory (ISIT2013), pp. 2069-2073, Istanbul, 2013.

Reaction attacks on sparse codes

- Low-density parity-check (LDPC) codes and moderate-density parity-check (MDPC) codes use decoders that are usually characterized by a small (but non negligible) decoding failure rate (DFR).

Reaction attacks on sparse codes

- Low-density parity-check (LDPC) codes and moderate-density parity-check (MDPC) codes use decoders that are usually characterized by a small (but non negligible) decoding failure rate (DFR).
- The decryption failure probability depends on the structure of the secret key: an opponent can estimate such a probability by observing Bob's reactions during decryption of known ciphertexts.

- Q. Guo, T. Johansson, P. Stankovski, "A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors," Advances in Cryptology ASIACRYPT 2016, vol. 10031 of Springer LNCS, pp. 789–815.
- T. Fabšič, V. Hromada, P. Stankovski, P. Zajac, Q. Guo, T. Johansson, "A Reaction Attack on the QC-LDPC McEliece Cryptosystem," PQCrypto 2017, vol. 10346 of Springer LNCS, pp. 51–68.

Avoiding reaction attacks

- Different ideas have been proposed, in order to avoid reaction attacks:
  - use of ephemeral keys;
  - choice of the system parameters in order to achieve negligible DFR values;
  - use of decoding strategies that do not leak information about the secret key;

- N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J. Deneuville, P. Gaborit, S. Gueron, T. Guneysu, C. A. Melchor, R. Misoczki, E. Persichetti, N. Sendrier, J. P. Tillich, and G. Zemor: "BIKE: first round submission to the NIST post-quantum cryptography call," November 2017.
- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini: "LEDAkem: first round submission to the NIST post-quantum cryptography call," November 2017.
- J.-P-Tillich," The decoding failure probability of MDPC codes," 2018.
- H. Bartz and G. Liva, "On decoding schemes for the MDPC-McEliece Cryptosystem," CoRR, vol. abs/1801.05659, 2018.

Avoiding reaction attacks

- Different ideas have been proposed, in order to avoid reaction attacks:
  - use of ephemeral keys;
  - choice of the system parameters in order to achieve negligible DFR values;
  - use of decoding strategies that do not leak information about the secret key;
  - decoding with indistinguishable parity check matrices (with respect to reaction attacks).

- N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J. Deneuville, P. Gaborit, S. Gueron, T. Guneysu, C. A. Melchor, R. Misoczki, E. Persichetti, N. Sendrier, J. P. Tillich, and G. Zemor: "BIKE: first round submission to the NIST post-quantum cryptography call," November 2017.
- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini: "LEDAkem: first round submission to the NIST post-quantum cryptography call," November 2017.
- J.-P-Tillich," The decoding failure probability of MDPC codes," 2018.
- H. Bartz and G. Liva, "On decoding schemes for the MDPC-McEliece Cryptosystem," CoRR, vol. abs/1801.05659, 2018.

Parity check matrix of a monomial code

- A monomial code is a QC code whose parity check matrix is in the form

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_{0,0} & \mathbf{H}_{0,1} & \cdots & \mathbf{H}_{0,n_0} \\ \mathbf{H}_{1,0} & \mathbf{H}_{1,1} & \cdots & \mathbf{H}_{1,n_0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{H}_{r_0-1,0} & \mathbf{H}_{r_0-1,1} & \cdots & \mathbf{H}_{r_0-1,n_0-1} \end{bmatrix}$$

  with each $\mathbf{H}_i$ being a circulant with size p and weight 1.
- It can be easily shown that at least $r_0 + 1$ rows in $\mathbf{H}$ are linearly dependent on the other rows, hence the code has dimension $k \geq (n_0 - r_0)p + r_0 + 1 = k_0 p + r_0 + 1$.

Exponent matrix

- Considering the homomorphism between size-p binary circulant matrices and polynomials in $\mathbb{F}_2[x]/(x^p - 1)$, each circulant block $\mathbf{H}_{i,j}$ can be represented as $x^{w_{i,j}}$.
- The exponents of the monomial can be grouped in a matrix $\mathbf{W}$, named *exponent matrix*, which is a compact representation of $\mathbf{H}$

$$\mathbf{W} = \begin{bmatrix} w_{0,0} & w_{0,1} & \cdots & w_{0,n_0-1} \\ w_{1,0} & w_{1,1} & \cdots & w_{1,n_0-1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{r_0-1,0} & w_{r_0-1,1} & \cdots & w_{r_0-1,n_0-1} \end{bmatrix}$$

Key generation

Secret Key

- $r \times n$ parity check matrix $\mathbf{H}$;
- $k \times k$ scrambling matrix $\mathbf{S}$.

Public key

- Let $\mathbf{G}$ be a generator matrix for the secret code.
- The public key is $\mathbf{G}' = \mathbf{S} \cdot \mathbf{G}$.

Key generation

Secret Key

- $r \times n$ parity check matrix $\mathbf{H}$;
- $k \times k$ scrambling matrix $\mathbf{S}$.

Public key

- Let $\mathbf{G}$ be a generator matrix for the secret code.
- The public key is $\mathbf{G}' = \mathbf{S} \cdot \mathbf{G}$.

Reducing the public key size

When a secure CCA2 conversion is used, $\mathbf{G}'$ can be in systematic form.

- K. Kobara, H. Imai, "Semantically secure McEliece public-key cryptosystems — conversions for McEliece PKC," PKC 2001, vol. 1992 of Springer LNCS, pp. 19–35, 2001.

Encryption and decryption

Encryption

- Alice generates a length-n vector $\mathbf{e}$ with weight t.
- She encrypts a k-bit message $\mathbf{u}$ as

$$\mathbf{x} = \mathbf{u} \cdot \mathbf{G}' + \mathbf{e}$$

Encryption and decryption

Encryption

- Alice generates a length-n vector $\mathbf{e}$ with weight t.
- She encrypts a k-bit message $\mathbf{u}$ as

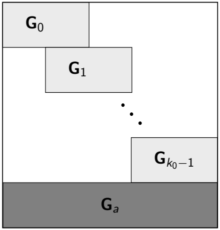
$$\mathbf{x} = \mathbf{u} \cdot \mathbf{G}' + \mathbf{e}$$

Decryption

- Bob computes $\mathbf{s} = \mathbf{H} \cdot \mathbf{x}^T = \mathbf{H} \cdot \mathbf{e}^T$.
- He decodes $\mathbf{s}$, corrects $\mathbf{e}$ and recovers $\mathbf{u}$.

A particular choice - Generator matrix

- The matrix $\mathbf{G}$ can have the following structure

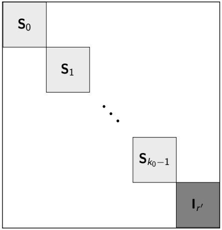


- Each matrix $\mathbf{G}_i$ has size $p \times (r_0+1)p$ and is in QC form.
- $\mathbf{G}_a$ contains additional $r' = n - k - r_0 p$ rows, needed in order to compensate the rank deficiency. These rows do not depend on the parity check matrix entries.

▶ M. Baldi, G. Cancellieri, and F. Chiaraluce, "Sparse generator matrices for some families of quasi-cyclic low-density parity-check codes," in Proc. 22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 247-251,2014.

A particular choice - Scrambling matrix

- The scrambling matrix $\mathbf{S}$ has the following structure

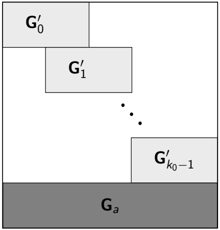


- Each matrix $\mathbf{S}_i$ is a dense circulant of size p.
- The presence of the identity $\mathbf{I}_{r'}$ is due to $\mathbf{G}_a$.

▶ M. Baldi, P. Santini, and G. Cancellieri, "Post-quantum cryptography based on codes: State of the art and open challenges," in 2017 AEIT International Annual Conference, pp. 1-6, 2017.

A particular choice - Public key

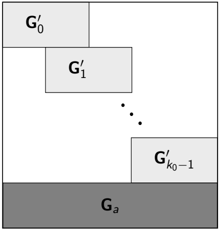
- With these choices $\mathbf{G}'$ has the following structure



  with $\mathbf{G}'_i = \mathbf{S}_i \cdot \mathbf{G}_i$.
- The block $\mathbf{G}_a$ is not part of the public key.

A particular choice - Public key

- With these choices $\mathbf{G}'$ has the following structure



  with $\mathbf{G}'_i = \mathbf{S}_i \cdot \mathbf{G}_i$.
- The block $\mathbf{G}_a$ is not part of the public key.

Public key size

With blocks $\mathbf{G}'_i$ in systematic form, the public key size is

$$KS = k_0 r_0 p$$

Distance spectrum

- Given two ones at positions v_1 and v_2, the corresponding cyclic distance is

$$\delta(v_1, v_2) = \min \{\pm(v_1 - v_2) \mod p\}$$

- The distance spectrum of a circulant matrix $\mathbf{A}$ is the set of distances produced by couples of ones in a row of $\mathbf{A}$.
- We say that a distance d has multiplicity $\mu(d)$ if there are $\mu(d)$ distinct couples of ones at distance d.

- Q. Guo, T. Johansson, P. Stankovski, "A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors," Advances in Cryptology ASIACRYPT 2016, vol. 10031 of Springer LNCS, pp. 789–815.

Distance spectrum

- Given two ones at positions v_1 and v_2, the corresponding cyclic distance is

$$\delta(v_1, v_2) = \min\{\pm(v_1 - v_2) \mod p\}$$

- The distance spectrum of a circulant matrix $\mathbf{A}$ is the set of distances produced by couples of ones in a row of $\mathbf{A}$.
- We say that a distance d has multiplicity $\mu(d)$ if there are $\mu(d)$ distinct couples of ones at distance d.
- The decoding failure rate (DFR) depends on the number of common distances between $\mathbf{e}$ and $\mathbf{H}$.

- Q. Guo, T. Johansson, P. Stankovski, "A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors," Advances in Cryptology ASIACRYPT 2016, vol. 10031 of Springer LNCS, pp. 789–815.

Relation between distance spectrum and DFR

- We can write $\mathbf{e} = [\mathbf{e}_0, \cdots, \mathbf{e}_{n_0-1}]$ and $\mathbf{s} = [\mathbf{s}_0, \cdots, \mathbf{s}_{r_0-1}]$, with $\mathbf{s}_j = \sum_{i=0}^{n_0-1} \mathbf{H}_{j,i} \cdot \mathbf{e}_i^T$.
- Common distances between $\mathbf{e}$ and $\mathbf{H}$ cause cancellations in the computation of the blocks $\mathbf{s}_j$.

Relation between distance spectrum and DFR

- We can write $\mathbf{e} = [\mathbf{e}_0, \cdots, \mathbf{e}_{n_0-1}]$ and $\mathbf{s} = [\mathbf{s}_0, \cdots, \mathbf{s}_{r_0-1}]$, with $\mathbf{s}_j = \sum_{i=0}^{n_0-1} \mathbf{H}_{j,i} \cdot \mathbf{e}_i^T$.
- Common distances between $\mathbf{e}$ and $\mathbf{H}$ cause cancellations in the computation of the blocks $\mathbf{s}_j$.

Observation #1

The DFR depends on the syndrome weight.

Relation between distance spectrum and DFR

- We can write $\mathbf{e} = [\mathbf{e}_0, \cdots, \mathbf{e}_{n_0-1}]$ and $\mathbf{s} = [\mathbf{s}_0, \cdots, \mathbf{s}_{r_0-1}]$, with $\mathbf{s}_j = \sum_{i=0}^{n_0-1} \mathbf{H}_{j,i} \cdot \mathbf{e}_i^T$.
- Common distances between $\mathbf{e}$ and $\mathbf{H}$ cause cancellations in the computation of the blocks $\mathbf{s}_j$.

Observation #1

The DFR depends on the syndrome weight.

Observation #2

Since the whole error vector contributes to the computation of every syndrome block, an opponent cannot know the positions of blocks where cancellations occurred.

Distance spectrum for monomial codes

- The distances in $\mathbf{H}$ are uniquely defined by $\mathbf{W}$.
- Distances can only be defined when considering two different columns in $\mathbf{W}$.
- Let $\lambda_{i,j}(\mathbf{W})$ be the set of distances between the i-th and j-th columns of $\mathbf{W}$: the distance spectrum $\mathbf{\Lambda}(\mathbf{W})$ is defined as the array containing all the sets $\lambda_{i,j}(\mathbf{W})$.

Distance spectrum for monomial codes

- The distances in $\mathbf{H}$ are uniquely defined by $\mathbf{W}$.
- Distances can only be defined when considering two different columns in $\mathbf{W}$.
- Let $\lambda_{i,j}(\mathbf{W})$ be the set of distances between the i-th and j-th columns of $\mathbf{W}$: the distance spectrum $\mathbf{\Lambda}(\mathbf{W})$ is defined as the array containing all the sets $\lambda_{i,j}(\mathbf{W})$.
- Example: for $p = 13$ and $\mathbf{W} = \begin{bmatrix} 1 & 4 & 5 \\ 3 & 11 & 0 \end{bmatrix}$

$$\mathbf{\Lambda}(\mathbf{W}) = \begin{bmatrix} - & \{3,5\} & \{3,4\} \\ \{3,5\} & - & \{1,2\} \\ \{3,4\} & \{1,2\} & - \end{bmatrix}$$

Recovering the secret key

- The knowledge of the spectrum $\mathbf{\Lambda}(\mathbf{W})$ can be used to build a matrix $\hat{\mathbf{H}} = \mathbf{\Pi} \cdot \mathbf{H}$, with $\mathbf{\Pi}$ being a permutation matrix.
- $\hat{\mathbf{H}}$ can be used to decode intercepted cyphertexts:
  1. the opponent computes

$$\begin{aligned}\hat{\mathbf{s}} &= \hat{\mathbf{H}} \cdot \mathbf{x}^T = \\ &= \mathbf{\Pi} \cdot \mathbf{H} \left(\mathbf{u} \cdot \mathbf{G}' + e\right)^T = \\ &= \mathbf{\Pi} \cdot \mathbf{H} \cdot \mathbf{e}^T\end{aligned}$$

  2. decoding of $\hat{\mathbf{s}}$ through $\hat{\mathbf{H}}$ returns $\mathbf{e}$.

Recovering the secret key

- The knowledge of the spectrum $\mathbf{\Lambda}(\mathbf{W})$ can be used to build a matrix $\hat{\mathbf{H}} = \mathbf{\Pi} \cdot \mathbf{H}$, with $\mathbf{\Pi}$ being a permutation matrix.
- $\hat{\mathbf{H}}$ can be used to decode intercepted cyphertexts:
  1. the opponent computes

$$\begin{aligned}\hat{\mathbf{s}} &= \hat{\mathbf{H}} \cdot \mathbf{x}^T = \\ &= \mathbf{\Pi} \cdot \mathbf{H} \left(\mathbf{u} \cdot \mathbf{G}' + e\right)^T = \\ &= \mathbf{\Pi} \cdot \mathbf{H} \cdot \mathbf{e}^T\end{aligned}$$

  2. decoding of $\hat{\mathbf{s}}$ through $\hat{\mathbf{H}}$ returns $\mathbf{e}$.
- Let $\hat{\mathbf{W}}$ be the exponent matrix associated to $\hat{\mathbf{H}}$: this matrix can be reconstructed from the distance spectrum $\mathbf{\Lambda}(\mathbf{W})$.

Reconstructing the exponent matrix

$\mathcal{G} \leftarrow$ graph with node 0
for $j \in \{0, 1, \cdots, n_0 - 1\}, d \in \lambda_{0,j}(\mathbf{H})$ **do**
    for $b \in \{0, 2, \cdots, 2r_0 - 2\}$ **do**
        $z_j^{(b)} = (j-1)p + [(p-d) \mod p]$
        $z_j^{(b+1)} = (j-1)p + d$
        Augment $\mathcal{G}$ with nodes $z_j^{(b)}$, $z_j^{(b+1)}$
        Augment $\mathcal{G}$ with edges $\left(0, z_j^{(b)}\right)$, $\left(0, z_j^{(b+1)}\right)$
for $i \in \{1, \cdots, n_0 - 2\}, j \in \{i+1, \cdots, n_0\}$ **do**
    for $b_i \in \{0, 1, \cdots, 2r_0 - 1\}, b_j \in \{0, 1, \cdots, 2r_0 - 1\}$ **do**
        if $\delta\left(z_i^{(b_i)}, z_j^{(b_j)}\right) \in \lambda_{i,j}$ **then**
            Augment $\mathcal{G}$ with edge $\left(z_i^{(b_i)}, z_j^{(b_j)}\right)$

Graph properties

- The algorithm builds the graph associated to the matrix $\hat{\mathbf{W}}$ having all zeros in the first column; this matrix can be called the *standard form* of $\mathbf{W}$ and denoted as $\mathbf{W}^*$.

Graph properties

- The algorithm builds the graph associated to the matrix $\hat{\mathbf{W}}$ having all zeros in the first column; this matrix can be called the *standard form* of $\mathbf{W}$ and denoted as $\mathbf{W}^*$.
- Every row of $\mathbf{W}^*$ is identified by a size-n_0 clique in $\mathcal{G}$ which contains the node 0, and corresponds to at least two cliques $\zeta = \{z_0, z_1, \cdots, z_{n_0-1}\}$ and $\zeta^* = \left\{z_0^*, z_1^*, \cdots, z_{n_0-1}^*\right\}$, such that

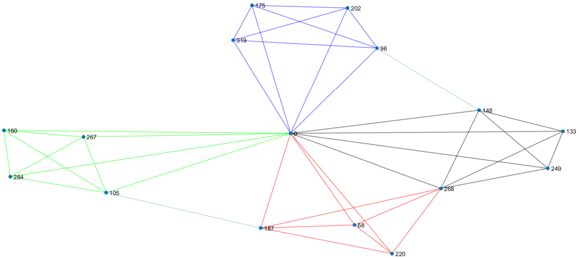
$$z_i^* = p\left\lfloor \frac{z_i}{p} \right\rfloor + [(p - z_i) \mod p]$$

Graph properties

- The algorithm builds the graph associated to the matrix $\hat{\mathbf{W}}$ having all zeros in the first column; this matrix can be called the *standard form* of $\mathbf{W}$ and denoted as $\mathbf{W}^*$.
- Every row of $\mathbf{W}^*$ is identified by a size-n_0 clique in $\mathcal{G}$ which contains the node 0, and corresponds to at least two cliques $\zeta = \{z_0, z_1, \cdots, z_{n_0-1}\}$ and $\zeta^* = \left\{z_0^*, z_1^*, \cdots, z_{n_0-1}^*\right\}$, such that
$$z_i^* = p\left\lfloor \frac{z_i}{p} \right\rfloor + [(p - z_i) \mod p]$$
- The graph $\mathcal{G}$ cannot contain an edge between two nodes z_i and z_j such that $\left\lfloor \frac{z_i}{p} \right\rfloor = \left\lfloor \frac{z_j}{p} \right\rfloor$: the maximum number of size-n_0 cliques in the graph is equal to p^{n_0-1}.

Graph properties

Example of the graph $\mathcal{G}$ associated to a code with $n_0 = 5$, $r_0 = 2$, $p = 67$, with exponent matrix $\mathbf{W} = \begin{bmatrix} 47 & 18 & 6 & 46 & 63 \\ 2 & 3 & 55 & 21 & 2 \end{bmatrix}$.



A special class of monomial codes

Exponent matrix generation

1. choose p as a prime;
2. randomly pick $\mathbf{y} = \left[y_0, y_1, \cdots, y_{\lceil \frac{p}{2} \rceil - 1}\right]$, with $y_i \in \mathbb{N}, y_i \in [0; p-1]$;
3. randomly pick a permutation $\mathbf{s} = [s_0, s_1, \cdots, s_{p-1}]$ of the vector $[0, 1, \cdots, p-1]$;
4. randomly pick a permutation $\mathbf{q} = \left[q_0, q_1, \cdots, q_{\lceil \frac{p}{2} \rceil - 1}\right]$ of the vector $\left[0, 1, \cdots, \left\lfloor \frac{p}{2} \right\rfloor\right]$;
5. for $i = 0, 1, \cdots, p$, compute the i-th column of $\mathbf{W}$ as

$$\mathbf{y}^T + s_i \mathbf{q}^T \mod p$$

Associated graph properties

- **Theorem:** all the exponent matrices constructed with the previous procedure satisfy the property

$$\lambda_{i,j}(\mathbf{W}) = \left\{0, 1, 2, \cdots, \left\lfloor \frac{p}{2} \right\rfloor \right\}, \ \ \forall i, j$$

Associated graph properties

- **Theorem:** all the exponent matrices constructed with the previous procedure satisfy the property

$$\lambda_{i,j}(\mathbf{W}) = \left\{0, 1, 2, \cdots, \left\lfloor \frac{p}{2} \right\rfloor \right\}, \ \ \forall i, j$$

- Any two nodes $z_i \geq 0$ and $z_j > 0$ such that $\left\lfloor \frac{z_i}{p} \right\rfloor \neq \left\lfloor \frac{z_j}{p} \right\rfloor$ are connected by an edge: the associated graph has $p^{n_0 - 1}$ cliques of size n_0.

Associated graph properties

- **Theorem:** all the exponent matrices constructed with the previous procedure satisfy the property

$$\lambda_{i,j}(\mathbf{W}) = \left\{0, 1, 2, \cdots, \left\lfloor \frac{p}{2} \right\rfloor \right\}, \ \forall i, j$$

- Any two nodes $z_i \geq 0$ and $z_j > 0$ such that $\left\lfloor \frac{z_i}{p} \right\rfloor \neq \left\lfloor \frac{z_j}{p} \right\rfloor$ are connected by an edge: the associated graph has p^{n_0-1} cliques of size n_0.

Indistinguishable secret keys

The distance spectrum is the same for all the secret exponent matrices.

Secret key cardinality

- The i-th column of $\mathbf{W}^*$ can be expressed as

$$\mathbf{w}_i^* = v_i^* \mathbf{q}^T \mod p$$

  where $v_0^* = 0$ and $\left[v_1^*, v_2^*, \cdots, v_{p-1}^*\right]$ corresponds to a permutation of the integers $\{1, 2, \cdots, p-1\}$.
- The vector $\mathbf{q}^T$ is a permutation of the integers in $\left[0, 1, \cdots, \left\lfloor \frac{p}{2} \right\rfloor\right]$: different configurations of $\mathbf{q}$ result in row permuted versions of $\mathbf{W}^*$.

Secret key cardinality

- The i-th column of $\mathbf{W}^*$ can be expressed as

$$\mathbf{w}_i^* = v_i^* \mathbf{q}^T \mod p$$

where $v_0^* = 0$ and $\left[v_1^*, v_2^*, \cdots, v_{p-1}^*\right]$ corresponds to a permutation of the integers $\{1, 2, \cdots, p-1\}$.

- The vector $\mathbf{q}^T$ is a permutation of the integers in $\left[0, 1, \cdots, \left\lfloor \frac{p}{2} \right\rfloor\right]$: different configurations of $\mathbf{q}$ result in row permuted versions of $\mathbf{W}^*$.
- The number of standard exponent matrices is equal to $N_W = (p-1)!$.

Secret key cardinality

- **Theorem:** let $\mathbf{W}^{(0)}$ and $\mathbf{W}^{(1)}$ be two exponent matrices generated according to the previous procedure, with $\mathbf{v}^{(1)} \neq \mathbf{v}^{(1)}$, and let $\mathbf{W}^{*(0)}$ and $\mathbf{W}^{*(1)}$ be their corresponding matrices in standard form. Then, $\mathbf{W}^{*(0)}$ and $\mathbf{W}^{*(1)}$ cannot be row permuted versions of the same matrix.

Secret key cardinality

- **Theorem:** let $\mathbf{W}^{(0)}$ and $\mathbf{W}^{(1)}$ be two exponent matrices generated according to the previous procedure, with $\mathbf{v}^{(1)} \neq \mathbf{v}^{(1)}$, and let $\mathbf{W}^{*(0)}$ and $\mathbf{W}^{*(1)}$ be their corresponding matrices in standard form. Then, $\mathbf{W}^{*(0)}$ and $\mathbf{W}^{*(1)}$ cannot be row permuted versions of the same matrix.

- Only one matrix, among all the possible $N_W = (p-1)!$ ones, is a parity check matrix of the public code.

Secret key cardinality

- **Theorem:** let $\mathbf{W}^{(0)}$ and $\mathbf{W}^{(1)}$ be two exponent matrices generated according to the previous procedure, with $\mathbf{v}^{(1)} \neq \mathbf{v}^{(1)}$, and let $\mathbf{W}^{*(0)}$ and $\mathbf{W}^{*(1)}$ be their corresponding matrices in standard form. Then, $\mathbf{W}^{*(0)}$ and $\mathbf{W}^{*(1)}$ cannot be row permuted versions of the same matrix.

- Only one matrix, among all the possible $N_W = (p-1)!$ ones, is a parity check matrix of the public code.

Brute-force equivalent security

The opponent cannot obtain information about the secret key: the only way of distinguishing the secret key is testing all possible candidates, whose number is equal to N_W.

System parameters

Proposed parameters require a number of operations $\geq 2^{\lambda}$, $\lambda \in \{80, 128, 256\}$, to run attacks on a classical computer.

λ	**p**	$\mathbf{n_0}$	$\mathbf{r_0}$	**t**	$\mathbf{N_W}$	K_s(kB)
80	103	103	52	84	2^{538}	34.14
128	137	137	69	132	2^{773}	80.36
256	257	257	129	261	2^{1684}	530.45

Conclusions and future works

- The proposed system achieves security against known reaction attacks, even with a non negligible DFR.
- The resulting key sizes are smaller than the ones of Goppa codes, but still too large with respect to other QC codes based systems.

Thanks for the attention