

# Public key cryptosystem design based on MRHS problem

Milan Vojvoda   **Pavol Zajac**<sup>1</sup>

CECC 2025, Budapest, Hungary

---

<sup>1</sup>This research was supported in part by the NATO Science for Peace and Security Programme under Project G5985, and in part by the Slovak Scientific Grant Agency, Grant Number VEGA 1/0105/23.

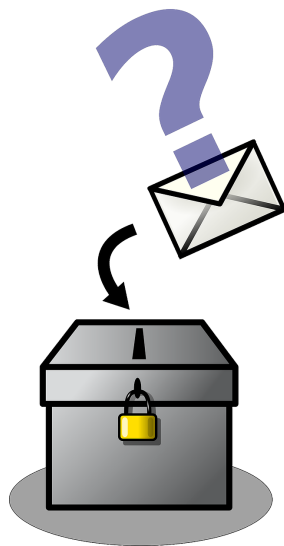
# Outline

---

- ① Motivation: Post-quantum cryptography
- ② New trapdoor function proposal
- ③ New trapdoor function analysis
  - One-way problem
  - Trapdoor
- ④ Conclusions

# One-way trapdoor function

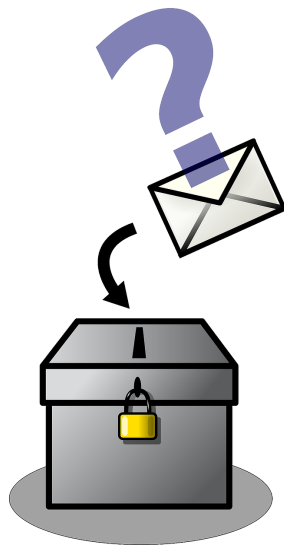
---



- Notion of a one-way trapdoor function is a basis of public key cryptography:
  - **Easy** to compute  $x \rightarrow y$  in one direction
  - **Difficult** to compute in the opposite direction,  $y \not\rightarrow x$
  - Unless we know some **trapdoor** information:  $y, t \rightarrow x$

# One-way trapdoor function : RSA

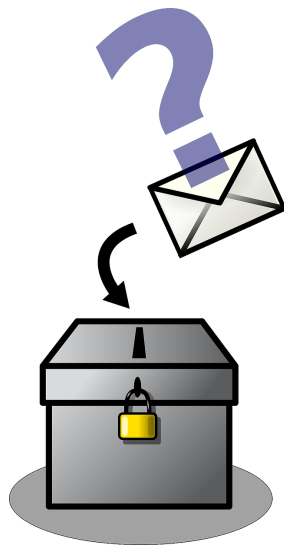
---



- Easy to understand: classical RSA
  - Easy: compute  $c = m^e \bmod n$
  - Difficult: compute  $m = c^{1/e} \bmod n$
  - Trapdoor: easy if you know  $n = p \cdot q$
- Quantum computer = future trapdoor
- Can we create easy to understand quantum-resistant one-way trapdoor function?

# One-way trapdoor function : McEliece

---



- Quantum resistant: McEliece cryptosystem
  - Easy: compute  $c = mG + e$
  - Difficult: compute  $m$  from  $c$  (find errors  $e$ )
  - Trapdoor: hidden structure  $G = S \cdot G' \cdot P$
- Which trapdoor codes are suitable?

# Main problem

---

- ① Take a random matrix  $\mathbf{M} \in \mathbb{F}_2^{(n \times mk)}$ ,  $n < km$ , and input  $\mathbf{x} \in \mathbb{F}_2^n$ .
- ② Compute  $\mathbf{v} = \mathbf{xM}$ , and split it into  $m$  blocks of length  $k$ :

$$\mathbf{v} = \mathbf{xM} = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m).$$

- ③ Output sequence  $\mathbf{y} = (\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_m)$  with  $\mathbf{y}_i \in \mathbb{F}_2^k \setminus \{\mathbf{v}_i\}$ .

## Problem

*How difficult is to compute original  $\mathbf{x}$  given  $\mathbf{y}$ ?*

# MRHS version of the problem

---

- MRHS formulation:

- ① Let  $\mathbf{M} = (\mathbf{M}_1 \mathbf{M}_2 \cdots \mathbf{M}_m)$ .

- ② Find solution of MRHS system  $\{\mathbf{xM}_i \in \mathbb{F}_2^k \setminus \{\mathbf{v}_i\}\}$ .

$$\begin{aligned}
 (x_1, x_2, x_3, x_4) \cdot & \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \\
 \in & \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}
 \end{aligned}$$

## $l$ -XOR-SAT version of the problem

---

MRHS instance

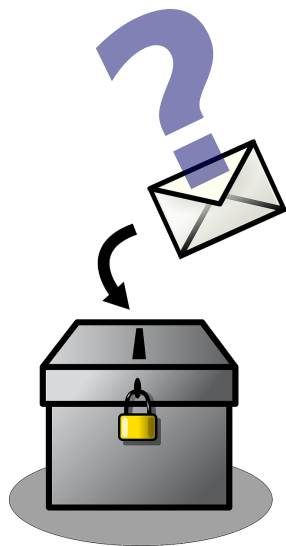
$$\begin{aligned}
 (x_1, x_2, x_3, x_4) \cdot & \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \\
 \in & \begin{Bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{Bmatrix} \times \begin{Bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{Bmatrix} \times \begin{Bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{Bmatrix} \times \begin{Bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{Bmatrix}
 \end{aligned}$$

can be written as 2-XOR-SAT instance:

$$\{x_1 \vee x_2\} \wedge \{x_3 \vee x_4\} \wedge \{(x_1 + x_3 + 1) \vee (x_4 + 1)\} \wedge \{(x_1 + x_2) \vee (x_3 + x_4 + 1)\}$$

# New One-way trapdoor function

---



- One-way trapdoor function based on MRHS system
  - Easy: compute  $\mathbf{y}$  with  $\mathbf{y}_i \neq \mathbf{xM}_i$
  - Difficult: compute  $\mathbf{x}$  from  $\mathbf{y}$
  - Trapdoor: hidden easy version of the MRHS problem
- Which instances are easy and which hard?
- Can we sufficiently mask easy instances?

## Difficult version of the problem

---

- 1 Let  $\mathbf{M} = (\mathbf{M}_1 \mathbf{M}_2 \cdots \mathbf{M}_m)$ .
- 2 Find solution of MRHS system  $\{\mathbf{x} \mathbf{M}_i \in \mathbb{F}_2^k \setminus \{\mathbf{v}_i\}\}$ .
  - $\mathbf{M}$  should be a random matrix,
  - $k$  should be small (for efficiency), sufficient:  $k = 2$
  - Ratio  $n/m$  is important:
    - $m$  small: too few constraints, false solutions,
    - $m$  large: too many constraints, can provide extra information,
  - Most difficult cases: 1 expected solution on average
  - For  $k = 2$ :

$$2^n \cdot \left(\frac{3}{4}\right)^m = 1 \Leftrightarrow m = \frac{n}{\log_2(3/4)} \approx 2.4n$$

## Difficult version of the problem

---

- ① Let  $\mathbf{M} = (\mathbf{M}_1\mathbf{M}_2 \cdots \mathbf{M}_m)$ .
- ② Find solution of MRHS system  $\{\mathbf{x}\mathbf{M}_i \in \mathbb{F}_2^k \setminus \{\mathbf{v}_i\}\}$ .
  - Problem 1: How to choose  $n$ ?
  - Basic attack: use linear algebra and restrict  $n$  variables into  $3^{n/2}$  choices...
  - Thus:  $n > 1.26\lambda$ ,  $m > 3\lambda$
  - $\lambda = 128$  gives  $n = 162$ ,  $n = 384$  (ct size 768 bits)

### Problem

*Are there more efficient solving methods for random instances?*

## Easy version of the problem

---

- ① Let  $\mathbf{M} = (\mathbf{M}_1\mathbf{M}_2 \cdots \mathbf{M}_m)$  be a **sparse matrix**.
- ② Find solution of MRHS system  $\{\mathbf{x}\mathbf{M}_i \in \mathbb{F}_2^k \setminus \{\mathbf{v}_i\}\}$ .
  - If each column of  $\mathbf{M}$  has a single 1: produces 2-SAT problem, which is in P:
    - method of syllogisms: transitive closure of an implication graph;
  - Can be solved efficiently even with higher density of 1's:
    - bit-flipping methods, genetic algorithms, ...

### Problem

*How can we mask sparse instances of the problem?*

# Proposed trapdoor

---

- 1 Let  $\mathbf{M} = (\mathbf{M}_1\mathbf{M}_2 \cdots \mathbf{M}_m)$  be a **sparse matrix** (secret).
- 2 Let  $\mathbf{R} \in \mathbb{F}^{(n \times n)}$  be a random (dense) matrix (secret).
- 3 Our trapdoor:  $\mathbf{P} = \mathbf{R}\mathbf{M}$  (public).
- 4 Trapdoor one-way function proposal:
  - Sender uses dense matrix  $\mathbf{P}$  to compute  $\mathbf{y}$  with  $\mathbf{y}_i \neq \mathbf{x}\mathbf{P}_i$ .
  - Recipient uses  $\mathbf{M}$  to solve the MRHS system  $\mathbf{y}_i \neq \mathbf{u}\mathbf{M}_i$ , and uses  $\mathbf{x} = \mathbf{u}\mathbf{R}^{-1}$  to change the basis of solution to reconstruct original  $\mathbf{x}$  (proof:  $\mathbf{y}_i \neq \mathbf{u}\mathbf{R}^{-1}\mathbf{R}\mathbf{M}_i$ ).

## Problem

*Can the adversary factor matrix  $\mathbf{P}$  into  $\mathbf{P} = \mathbf{R} \cdot \mathbf{M}$ ?*

## Summary

---

- We have proposed a one-way trapdoor function based on masked sparse MRHS equations.
- Problem 1: Exactly how difficult are random (dense) instances of the problem (on classical and quantum computers)?
- Problem 2: Can trapdoor matrix be factored into dense and sparse component?
- Problem 3: Can trap-doored instances be solved efficiently without the knowledge of the matrix factorization?

Thank you for your attention. Questions? Comments?