Practical Key-Recovery Attack on MQ-Sign and More

Thomas Aulbach[1] Simona Samardjiska[2] Monika Trimoska[3]

PQCrypto 2024, Oxford, UK

[1]University of Regensburg, Regensburg, Germany

[2]Radboud Universiteit, Nijmegen, The Netherlands

[3]Eindhoven University of Technology, Eindhoven, The Netherlands

MQ-Sign Variants

MQ-Sign Variants in the KpqC Competition

MQ-Sign is a Uov-based signature scheme and submitted to the KpqC competition.

Round 1 Variants	$\mathcal{F}_{V,V}$	$\mathcal{F}_{O,V}$	Attack Type	Complexity
MQ-Sign-RR	random	random		
MQ-Sign-SR	sparse	random		
MQ-Sign-RS	random	sparse		
MQ-Sign-SS	sparse	sparse		

MQ-Sign Variants in the KpqC Competition

MQ-Sign is a Uov-based signature scheme and submitted to the KpqC competition.

Round 1 Variants	$\mathcal{F}_{V,V}$	$\mathcal{F}_{O,V}$	Attack Type	Complexity
MQ-Sign-RR	random	random		
MQ-Sign-SR	sparse	random		
MQ-Sign-RS	random	sparse		
MQ-Sign-SS	sparse	sparse		

- MQ-Sign-RR corresponds to standard Uov.

MQ-Sign Variants in the KpqC Competition

MQ-Sign is a Uov-based signature scheme and submitted to the KpqC competition.

Round 1 Variants	$\mathcal{F}_{V,V}$	$\mathcal{F}_{O,V}$	Attack Type	Complexity
MQ-Sign-RR	random	random		
MQ-Sign-SR	sparse	random		
MQ-Sign-RS	random	sparse		
MQ-Sign-SS	sparse	sparse		

- MQ-Sign-RR corresponds to standard Uov.
- Variants with sparse central maps $\mathcal{F}$ are developed to reduce key size.

MQ-Sign Variants in the KpqC Competition

MQ-Sign is a Uov-based signature scheme and submitted to the KpqC competition.

Round 1 Variants	$\mathcal{F}_{V,V}$	$\mathcal{F}_{O,V}$	Attack Type	Complexity
MQ-Sign-RR	random	random	-	-
MQ-Sign-SR	sparse	random	forgery attack	exp time
MQ-Sign-RS	random	sparse	key-recovery	poly time
MQ-Sign-SS	sparse	sparse	key-recovery	poly time

- MQ-Sign-RR corresponds to standard Uov.
- Variants with sparse central maps $\mathcal{F}$ are developed to reduce key size.
- We present attacks to every sparse variant.

MQ-Sign Key Structure

Unbalanced Oil and Vinegar Signature

Secret/central map (easy to invert):

$$\mathcal{F} = (\mathcal{F}^{(1)}, \ldots, \mathcal{F}^{(m)}) : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

Unbalanced Oil and Vinegar Signature

Secret/central map (easy to invert):

$$\mathcal{F} = (\mathcal{F}^{(1)}, \ldots, \mathcal{F}^{(m)}) : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

Secret/central polynomials (structured):

$$\mathcal{F}^{(k)}(x_1, \ldots, x_n) = \sum_{i \in V, j \in V} \gamma_{ij}^{(k)} x_i x_j + \sum_{i \in V, j \in O} \gamma_{ij}^{(k)} x_i x_j + \cancel{\sum_{i \in O, j \in O} \gamma_{ij}^{(k)} x_i x_j}$$

Unbalanced Oil and Vinegar Signature

Secret/central map (easy to invert):

$$\mathcal{F} = (\mathcal{F}^{(1)}, \ldots, \mathcal{F}^{(m)}) : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

Secret/central polynomials (structured):

$$\mathcal{F}^{(k)}(x_1, \ldots, x_n) = \sum_{i \in V, j \in V} \gamma_{ij}^{(k)} x_i x_j + \sum_{i \in V, j \in O} \gamma_{ij}^{(k)} x_i x_j + \cancel{\sum_{i \in O, j \in O} \gamma_{ij}^{(k)} x_i x_j}$$

Store the coefficients of the quadratic part of $\mathcal{F}^{(k)}$ in an upper triangular matrix $\mathbf{F^{(k)}}$

$$\mathbf{F^{(k)}} = \begin{pmatrix} \mathbf{F_1^{(k)}} & \mathbf{F_2^{(k)}} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} = \begin{pmatrix} \mathbf{F_V^{(k)}} & \mathbf{F_{O,V}^{(k)}} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}.$$

Unbalanced Oil and Vinegar Signature

Secret/central map (easy to invert):

$$\mathcal{F} = (\mathcal{F}^{(1)}, \ldots, \mathcal{F}^{(m)}) : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

Secret/central polynomials (structured):

$$\mathcal{F}^{(k)}(x_1, \ldots, x_n) = \sum_{i \in V, j \in V} \gamma_{ij}^{(k)} x_i x_j + \sum_{i \in V, j \in O} \gamma_{ij}^{(k)} x_i x_j + \cancel{\sum_{i \in O, j \in O} \gamma_{ij}^{(k)} x_i x_j}$$

Store the coefficients of the quadratic part of $\mathcal{F}^{(k)}$ in an upper triangular matrix $\mathbf{F^{(k)}}$

$$\mathbf{F^{(k)}} = \begin{pmatrix} \mathbf{F_1^{(k)}} & \mathbf{F_2^{(k)}} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} = \begin{pmatrix} \mathbf{F_V^{(k)}} & \mathbf{F_{O,V}^{(k)}} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}.$$

Secret linear transformation (invertible matrix):

$$\mathbf{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n, \quad \text{where we commonly have } \mathbf{S} = \begin{pmatrix} \mathbf{I_v} & \mathbf{S}_1 \\ \mathbf{0} & \mathbf{I_m} \end{pmatrix}$$

Unbalanced Oil and Vinegar Signature

Public key map (hard to invert):

$$\mathcal{P} = (\mathcal{P}^{(1)}, \ldots, \mathcal{P}^{(m)}) : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

Unbalanced Oil and Vinegar Signature

Public key map (hard to invert):

$$\mathcal{P} = (\mathcal{P}^{(1)}, \ldots, \mathcal{P}^{(m)}) : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

Public polynomials (seemingly random):

$$\mathcal{P}^{(k)}(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} p_{ij}^{(k)} x_i x_j$$

Unbalanced Oil and Vinegar Signature

Public key map (hard to invert):

$$\mathcal{P} = (\mathcal{P}^{(1)}, \ldots, \mathcal{P}^{(m)}) : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

Public polynomials (seemingly random):

$$\mathcal{P}^{(k)}(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} p_{ij}^{(k)} x_i x_j$$

Store the coefficients of the quadratic part of $\mathcal{P}^{(k)}$ in an upper triangular matrix $\mathbf{P^{(k)}}$

$$\mathbf{P^{(k)}} = \begin{pmatrix} \mathbf{P_1^{(k)}} & \mathbf{P_2^{(k)}} \\ \mathbf{0} & \mathbf{P_4^{(k)}} \end{pmatrix}$$

Unbalanced Oil and Vinegar Signature

Public key map (hard to invert):

$$\mathcal{P} = (\mathcal{P}^{(1)}, \ldots, \mathcal{P}^{(m)}) : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

Public polynomials (seemingly random):

$$\mathcal{P}^{(k)}(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} p_{ij}^{(k)} x_i x_j$$

Store the coefficients of the quadratic part of $\mathcal{P}^{(k)}$ in an upper triangular matrix $\mathbf{P^{(k)}}$

$$\mathbf{P^{(k)}} = \begin{pmatrix} \mathbf{P_1^{(k)}} & \mathbf{P_2^{(k)}} \\ \mathbf{0} & \mathbf{P_4^{(k)}} \end{pmatrix}$$

The public and secret polynomials follow the equation:

$$\mathcal{P} = \mathcal{F} \circ \mathbf{S}$$

Unbalanced Oil and Vinegar Signature

Public key map (hard to invert):

$$\mathcal{P} = (\mathcal{P}^{(1)}, \ldots, \mathcal{P}^{(m)}) : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

Public polynomials (seemingly random):

$$\mathcal{P}^{(k)}(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} p_{ij}^{(k)} x_i x_j$$

Store the coefficients of the quadratic part of $\mathcal{P}^{(k)}$ in an upper triangular matrix $\mathbf{P^{(k)}}$

$$\mathbf{P^{(k)}} = \begin{pmatrix} \mathbf{P_1^{(k)}} & \mathbf{P_2^{(k)}} \\ \mathbf{0} & \mathbf{P_4^{(k)}} \end{pmatrix}$$

The public and secret polynomials follow the equation:

$$\mathcal{P} = \mathcal{F} \circ \mathbf{S}$$

$$\text{resp. } \mathbf{P^{(k)}} = \mathbf{S}^\top \mathbf{F^{(k)}} \mathbf{S}$$

Unbalanced Oil and Vinegar Signature

Sign

- Build the target value $\mathbf{t} = \mathbf{H}(\mathbf{m}, \texttt{salt})$ from message $\mathbf{m}$.
- Compute $\mathbf{y} = \mathcal{F}^{-1}(\mathbf{t}) \in \mathbb{F}_q^n$, and $\mathbf{z} = \mathbf{S}^{-1}(\mathbf{y})$.
- The signature is given by $sig = (\mathbf{z}, \texttt{salt})$

Unbalanced Oil and Vinegar Signature

Sign

- Build the target value $\mathbf{t} = \mathbf{H}(\mathbf{m}, \texttt{salt})$ from message $\mathbf{m}$.
- Compute $\mathbf{y} = \mathcal{F}^{-1}(\mathbf{t}) \in \mathbb{F}_q^n$, and $\mathbf{z} = \mathbf{S}^{-1}(\mathbf{y})$.
- The signature is given by $sig = (\mathbf{z}, \texttt{salt})$

Verify

- Build the target value $\mathbf{t} = \mathbf{H}(\mathbf{m}, \texttt{salt})$ and evaluate $\mathbf{t}' = \mathcal{P}(\mathbf{z})$.
- Accept if $\mathbf{t} = \mathbf{t}'$, reject otherwise.

MQ-Sign Modifications

MQ-Sign design principle: sparse polynomials to reduce key size

MQ-Sign Modifications

MQ-Sign design principle: sparse polynomials to reduce key size

- Choose $\mathcal{F}_V^{(k)}(x_1, \ldots, x_n)$ sparse

$$\sum_{i \in V,\, j \in V} \gamma_{ij}^{(k)} x_i x_j \;\rightarrow\; \sum_{i=1}^{v} \gamma_i^{(k)} x_i x_{(i+k-1 \pmod{v})+1}$$

MQ-Sign Modifications

MQ-Sign design principle: sparse polynomials to reduce key size

- Choose $\mathcal{F}_V^{(k)}(x_1, \ldots, x_n)$ sparse

$$\sum_{i \in V,\, j \in V} \gamma_{ij}^{(k)} x_i x_j \rightarrow \sum_{i=1}^{v} \gamma_i^{(k)} x_i x_{(i+k-1 (\bmod v))+1}$$

$\Rightarrow$ From $\boxed{v \cdot (v+1)/2}$ to $\boxed{v}$ coefficients per polynomials.

MQ-Sign Modifications

MQ-Sign design principle: sparse polynomials to reduce key size

- Choose $\mathcal{F}_V^{(k)}(x_1, \ldots, x_n)$ sparse

$$\sum_{i \in V,\, j \in V} \gamma_{ij}^{(k)} x_i x_j \;\rightarrow\; \sum_{i=1}^{v} \gamma_i^{(k)} x_i x_{(i+k-1 (\bmod v))+1}$$

$\Rightarrow$ From $\boxed{v \cdot (v+1)/2}$ to $\boxed{v}$ coefficients per polynomials.

- Choose $\mathcal{F}_{OV}^{(k)}(x_1, \ldots, x_n)$ sparse

$$\sum_{i \in V,\, j \in O} \gamma_{ij}^{(k)} x_i x_j \;\rightarrow\; \sum_{i=1}^{v} \gamma_i^{(k)} x_i x_{(i+k-2 (\bmod m))+v+1}.$$

MQ-Sign Modifications

MQ-Sign design principle: sparse polynomials to reduce key size

- Choose $\mathcal{F}_V^{(k)}(x_1, \ldots, x_n)$ sparse

$$\sum_{i \in V,\, j \in V} \gamma_{ij}^{(k)} x_i x_j \;\rightarrow\; \sum_{i=1}^{v} \gamma_i^{(k)} x_i x_{(i+k-1 (\bmod v))+1}$$

$\Rightarrow$ From $\boxed{v \cdot (v+1)/2}$ to $\boxed{v}$ coefficients per polynomials.

- Choose $\mathcal{F}_{OV}^{(k)}(x_1, \ldots, x_n)$ sparse

$$\sum_{i \in V,\, j \in O} \gamma_{ij}^{(k)} x_i x_j \;\rightarrow\; \sum_{i=1}^{v} \gamma_i^{(k)} x_i x_{(i+k-2 (\bmod m))+v+1}.$$

$\Rightarrow$ From $\boxed{v \cdot o}$ to $\boxed{v}$ coefficients per polynomials.

MQ-Sign Modifications

MQ-Sign design principle: sparse polynomials to reduce key size

- Choose $\mathcal{F}_V^{(k)}(x_1, \ldots, x_n)$ sparse

$$\sum_{i \in V,\, j \in V} \gamma_{ij}^{(k)} x_i x_j \rightarrow \sum_{i=1}^{v} \gamma_i^{(k)} x_i x_{(i+k-1 (\bmod v))+1}$$

$\Rightarrow$ From $\boxed{v \cdot (v+1)/2}$ to $\boxed{v}$ coefficients per polynomials.

- Choose $\mathcal{F}_{OV}^{(k)}(x_1, \ldots, x_n)$ sparse

$$\sum_{i \in V,\, j \in O} \gamma_{ij}^{(k)} x_i x_j \rightarrow \sum_{i=1}^{v} \gamma_i^{(k)} x_i x_{(i+k-2 (\bmod m))+v+1}.$$

$\Rightarrow$ From $\boxed{v \cdot o}$ to $\boxed{v}$ coefficients per polynomials.

MQ-Sign Modifications

Translate sparse polynomial equations to matrix visualization

MQ-Sign Modifications

Translate sparse polynomial equations to matrix visualization

$$\mathcal{F}_V^{(1)} = \sum_{i=1}^{v} \gamma_i^{(1)} x_i x_{(i \bmod v)+1} \quad \rightarrow \quad \mathbf{F}_V^{(1)} = \begin{pmatrix} 0 & \gamma_1^{(1)} & 0 & \cdots & 0 \\ 0 & 0 & \gamma_2^{(1)} & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \gamma_{v-1}^{(1)} \\ \gamma_v^{(1)} & 0 & 0 & \cdots & 0 \end{pmatrix}$$

MQ-Sign Modifications

Translate sparse polynomial equations to matrix visualization

$$\mathcal{F}_V^{(1)} = \sum_{i=1}^{v} \gamma_i^{(1)} x_i x_{(i \bmod v)+1} \quad \rightarrow \quad \mathbf{F}_V^{(1)} = \begin{pmatrix} 0 & \gamma_1^{(1)} & 0 & \cdots & 0 \\ 0 & 0 & \gamma_2^{(1)} & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \gamma_{v-1}^{(1)} \\ \gamma_v^{(1)} & 0 & 0 & \cdots & 0 \end{pmatrix}$$

$$\mathcal{F}_V^{(2)} = \sum_{i=1}^{v} \gamma_i^{(2)} x_i x_{(i+1 \bmod v)+1} \quad \rightarrow \quad \mathbf{F}_V^{(2)} = \begin{pmatrix} 0 & 0 & \gamma_1^{(2)} & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \gamma_{v-2}^{(2)} \\ \gamma_{v-1}^{(2)} & 0 & 0 & \cdots & 0 \\ 0 & \gamma_v^{(2)} & 0 & \cdots & 0 \end{pmatrix}$$

$$\vdots$$

MQ-Sign Secret Key Size

Key size reduction due to sparsely chosen central polynomials

Round 1 variants	$\mathcal{F}_{V,V}$	$\mathcal{F}_{O,V}$	Secret key size at security level I
MQ-Sign-RR	random	random	282 177 Bytes
MQ-Sign-SR	sparse	random	164 601 Bytes
MQ-Sign-RS	random	sparse	133 137 Bytes
MQ-Sign-SS	sparse	sparse	15 561 Bytes

Table: Key size of the MQ-Sign variants for security level I with parameters $(q, v, m) = (2^8, 72, 46)$

Polynomial Time Key-Recovery Attack

Derive Linear Equations from Key Equation

The key equation $\mathcal{P} = \mathcal{F} \circ \mathbf{S}$ translates to the matrix equations $\mathbf{P}^{(\mathbf{k})} = \mathbf{S}^\top \mathbf{F}^{(\mathbf{k})} \mathbf{S}$,

Derive Linear Equations from Key Equation

The key equation $\mathcal{P} = \mathcal{F} \circ \mathbf{S}$ translates to the matrix equations $\mathbf{P}^{(\mathbf{k})} = \mathbf{S}^\top \mathbf{F}^{(\mathbf{k})} \mathbf{S}$, i.e.

$$\begin{aligned}
\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ \mathbf{0} & \mathbf{P}_4^{(k)} \end{pmatrix} &= \mathtt{Upper}\left(\begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{S}_1^\top & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{F}_1^{(k)} & \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{S}_1 \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \right) \\
&= \begin{pmatrix} \mathbf{F}_1^{(k)} & (\mathbf{F}_1^{(k)} + \mathbf{F}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathtt{Upper}\ (\mathbf{S}_1^\top \mathbf{F}_1^{(k)} \mathbf{S}_1 + \mathbf{S}_1^\top \mathbf{F}_2^{(k)}) \end{pmatrix}.
\end{aligned}$$

Derive Linear Equations from Key Equation

The key equation $\mathcal{P} = \mathcal{F} \circ \mathbf{S}$ translates to the matrix equations $\mathbf{P^{(k)}} = \mathbf{S}^\top \mathbf{F^{(k)}} \mathbf{S}$, i.e.

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ \mathbf{0} & \mathbf{P}_4^{(k)} \end{pmatrix} = \mathtt{Upper}\left(\begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{S}_1^\top & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{F}_1^{(k)} & \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{S}_1 \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \right)$$
$$= \begin{pmatrix} \mathbf{F}_1^{(k)} & (\mathbf{F}_1^{(k)} + \mathbf{F}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathtt{Upper}\,(\mathbf{S}_1^\top \mathbf{F}_1^{(k)} \mathbf{S}_1 + \mathbf{S}_1^\top \mathbf{F}_2^{(k)}) \end{pmatrix}.$$

From the two upper blocks we obtain the equations

$$\mathbf{P}_1^{(k)} = \mathbf{F}_1^{(k)} \quad \text{and} \quad \mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

Derive Linear Equations from Key Equation

The key equation $\mathcal{P} = \mathcal{F} \circ \mathbf{S}$ translates to the matrix equations $\mathbf{P^{(k)}} = \mathbf{S}^\top \mathbf{F^{(k)}} \mathbf{S}$, i.e.

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ \mathbf{0} & \mathbf{P}_4^{(k)} \end{pmatrix} = \mathtt{Upper}\left(\begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{S}_1^\top & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{F}_1^{(k)} & \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{S}_1 \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \right)$$
$$= \begin{pmatrix} \mathbf{F}_1^{(k)} & (\mathbf{F}_1^{(k)} + \mathbf{F}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathtt{Upper}\ (\mathbf{S}_1^\top \mathbf{F}_1^{(k)} \mathbf{S}_1 + \mathbf{S}_1^\top \mathbf{F}_2^{(k)}) \end{pmatrix}.$$

From the two upper blocks we obtain the equations

$$\mathbf{P}_1^{(k)} = \mathbf{F}_1^{(k)} \quad \text{and} \quad \mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$\Rightarrow$ System of linear equations in the entries of the secret $\mathbf{S_1}$

Derive Linear Equations from Key Equation

The key equation $\mathcal{P} = \mathcal{F} \circ \mathbf{S}$ translates to the matrix equations $\mathbf{P^{(k)}} = \mathbf{S}^\top \mathbf{F^{(k)}} \mathbf{S}$, i.e.

$$\begin{aligned}\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ \mathbf{0} & \mathbf{P}_4^{(k)} \end{pmatrix} &= \mathtt{Upper}\left(\begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{S}_1^\top & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{F}_1^{(k)} & \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{S}_1 \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \right) \\ &= \begin{pmatrix} \mathbf{F}_1^{(k)} & (\mathbf{F}_1^{(k)} + \mathbf{F}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathtt{Upper}\ (\mathbf{S}_1^\top \mathbf{F}_1^{(k)} \mathbf{S}_1 + \mathbf{S}_1^\top \mathbf{F}_2^{(k)}) \end{pmatrix}.\end{aligned}$$

From the two upper blocks we obtain the equations

$$\mathbf{P}_1^{(k)} = \mathbf{F}_1^{(k)} \quad \text{and} \quad \mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$\Rightarrow$ System of linear equations in the entries of the secret $\mathbf{S_1}$

$\Rightarrow$ But highly **underdetermined**, due to the secret coefficients in $\mathbf{F}_2^{(k)}$

Efficient Key-Recovery

In MQ-SIGN-RS and MQ-SIGN-SS the coefficients in $\mathbf{F_2^{(k)}} = \mathbf{F_{O,V}^{(k)}}$ are chosen sparsely. This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p_{1,v+1}^{(k)} & \cdots & p_{1,v+m}^{(k)} \\ \vdots & & \vdots \\ p_{v,v+1}^{(k)} & \cdots & p_{v,v+m}^{(k)} \end{pmatrix}}_{public} = \underbrace{\begin{pmatrix} p_{1,1}^{,(k)} & \cdots & p_{1,v}^{,(k)} \\ \vdots & & \vdots \\ p_{v,1}^{,(k)} & \cdots & p_{v,v}^{,(k)} \end{pmatrix}}_{public} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{secret} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\text{secret, but known structure}}$$

Efficient Key-Recovery

In MQ-Sign-RS and MQ-Sign-SS the coefficients in $\mathbf{F_2^{(k)}} = \mathbf{F_{O,V}^{(k)}}$ are chosen sparsely. This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p_{1,v+1}^{(k)} & \cdots & p_{1,v+m}^{(k)} \\ \vdots & & \vdots \\ p_{v,v+1}^{(k)} & \cdots & p_{v,v+m}^{(k)} \end{pmatrix}}_{public} = \underbrace{\begin{pmatrix} p_{1,1}^{,(k)} & \cdots & p_{1,v}^{,(k)} \\ \vdots & & \vdots \\ p_{v,1}^{,(k)} & \cdots & p_{v,v}^{,(k)} \end{pmatrix}}_{public} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{secret} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\text{secret, but known structure}}$$

Efficient Key-Recovery

In MQ-SIGN-RS and MQ-SIGN-SS the coefficients in $\mathbf{F_2^{(k)}} = \mathbf{F_{O,V}^{(k)}}$ are chosen sparsely. This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p_{1,v+1}^{(k)} & \cdots & p_{1,v+m}^{(k)} \\ \vdots & & \vdots \\ p_{v,v+1}^{(k)} & \cdots & p_{v,v+m}^{(k)} \end{pmatrix}}_{public} = \underbrace{\begin{pmatrix} p'^{(k)}_{1,1} & \cdots & p'^{(k)}_{1,v} \\ \vdots & & \vdots \\ p'^{(k)}_{v,1} & \cdots & p'^{(k)}_{v,v} \end{pmatrix}}_{public} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{secret} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\text{secret, but known structure}}$$

Efficient Key-Recovery

In MQ-Sign-RS and MQ-Sign-SS the coefficients in $\mathbf{F_2^{(k)}} = \mathbf{F_{O,V}^{(k)}}$ are chosen sparsely. This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p_{1,v+1}^{(k)} & \cdots & p_{1,v+m}^{(k)} \\ \vdots & & \vdots \\ p_{v,v+1}^{(k)} & \cdots & p_{v,v+m}^{(k)} \end{pmatrix}}_{public} = \underbrace{\begin{pmatrix} p_{1,1}^{,(k)} & \cdots & p_{1,v}^{,(k)} \\ \vdots & & \vdots \\ p_{v,1}^{,(k)} & \cdots & p_{v,v}^{,(k)} \end{pmatrix}}_{public} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{secret} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\text{secret, but known structure}}$$

Efficient Key-Recovery

In MQ-Sign-RS and MQ-Sign-SS the coefficients in $\mathbf{F_2^{(k)}} = \mathbf{F_{O,V}^{(k)}}$ are chosen sparsely. This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p_{1,v+1}^{(k)} & \cdots & p_{1,v+m}^{(k)} \\ \vdots & & \vdots \\ p_{v,v+1}^{(k)} & \cdots & p_{v,v+m}^{(k)} \end{pmatrix}}_{\textit{public}} = \underbrace{\begin{pmatrix} p'^{(k)}_{1,1} & \cdots & p'^{(k)}_{1,v} \\ \vdots & & \vdots \\ p'^{(k)}_{v,1} & \cdots & p'^{(k)}_{v,v} \end{pmatrix}}_{\textit{public}} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{\textit{secret}} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\text{secret, but known structure}}$$

Efficient Key-Recovery

In MQ-Sign-RS and MQ-Sign-SS the coefficients in $\mathbf{F}_2^{(\mathbf{k})} = \mathbf{F}_{\mathbf{O},\mathbf{V}}^{(\mathbf{k})}$ are chosen sparsely. This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p_{1,v+1}^{(k)} & \cdots & p_{1,v+m}^{(k)} \\ \vdots & & \vdots \\ p_{v,v+1}^{(k)} & \cdots & \color{red}{p_{v,v+m}^{(k)}} \end{pmatrix}}_{\textit{public}} = \underbrace{\begin{pmatrix} p_{1,1}^{\prime(k)} & \cdots & p_{1,v}^{\prime(k)} \\ \vdots & & \vdots \\ \color{red}{p_{v,1}^{\prime(k)}} & \color{red}{\cdots} & \color{red}{p_{v,v}^{\prime(k)}} \end{pmatrix}}_{\textit{public}} \underbrace{\begin{pmatrix} s_{11} & \cdots & \color{red}{s_{1m}} \\ \vdots & & \color{red}{\vdots} \\ s_{v1} & \cdots & \color{red}{s_{vm}} \end{pmatrix}}_{\textit{secret}} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & \color{red}{0} \end{pmatrix}}_{\text{secret, but known structure}}$$

- Collect linear equations for all $k \in \{1, \ldots, m\}$ polynomials.

Efficient Key-Recovery

In MQ-Sign-RS and MQ-Sign-SS the coefficients in $\mathbf{F}_2^{(\mathbf{k})} = \mathbf{F}_{\mathbf{O},\mathbf{V}}^{(\mathbf{k})}$ are chosen sparsely. This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p_{1,v+1}^{(k)} & \cdots & p_{1,v+m}^{(k)} \\ \vdots & & \vdots \\ p_{v,v+1}^{(k)} & \cdots & p_{v,v+m}^{(k)} \end{pmatrix}}_{\textit{public}} = \underbrace{\begin{pmatrix} p_{1,1}^{,(k)} & \cdots & p_{1,v}^{,(k)} \\ \vdots & & \vdots \\ p_{v,1}^{,(k)} & \cdots & p_{v,v}^{,(k)} \end{pmatrix}}_{\textit{public}} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{\textit{secret}} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\text{secret, but known structure}}$$

- Collect linear equations for all $k \in \{1, \ldots, m\}$ polynomials.
- Obtain system of $mv(m-1)$ equations in vm variables (can be divided into subsystems).

Efficient Key-Recovery

In MQ-Sign-RS and MQ-Sign-SS the coefficients in $\mathbf{F_2^{(k)}} = \mathbf{F_{O,V}^{(k)}}$ are chosen sparsely. This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p_{1,v+1}^{(k)} & \cdots & p_{1,v+m}^{(k)} \\ \vdots & & \vdots \\ p_{v,v+1}^{(k)} & \cdots & p_{v,v+m}^{(k)} \end{pmatrix}}_{public} = \underbrace{\begin{pmatrix} p_{1,1}^{,(k)} & \cdots & p_{1,v}^{,(k)} \\ \vdots & & \vdots \\ p_{v,1}^{,(k)} & \cdots & p_{v,v}^{,(k)} \end{pmatrix}}_{public} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{secret} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\text{secret, but known structure}}$$

- Collect linear equations for all $k \in \{1, \ldots, m\}$ polynomials.
- Obtain system of $mv(m-1)$ equations in vm variables (can be divided into subsystems).
- Once $\mathbf{S}$ is known, receive all central polynomials efficiently from $\mathbf{P^{(k)}} = \mathbf{S}^\top \mathbf{F^{(k)}} \mathbf{S}$.

Attack Summary

Key-Recovery Attack Summary:

- Compute secret key $(\mathcal{F}, \mathbf{S})$ directly from public key $\mathcal{P}$, no signing-oracle needed.

Attack Summary

Key-Recovery Attack Summary:

- Compute secret key $(\mathcal{F}, \mathbf{S})$ directly from public key $\mathcal{P}$, no signing-oracle needed.
- Works in seconds for all security levels.

Attack Summary

Key-Recovery Attack Summary:

- Compute secret key $(\mathcal{F}, \mathbf{S})$ directly from public key $\mathcal{P}$, no signing-oracle needed.
- Works in seconds for all security levels.
- Ikematsu et al.[1] generalized this attack to arbitrary $\mathbf{S}$.

[1] Ikematsu et al. *A security analysis on MQ-Sign.* In International Conference on Information Security Applications, 2023

Attack Summary

Key-Recovery Attack Summary:

- Compute secret key $(\mathcal{F}, \mathbf{S})$ directly from public key $\mathcal{P}$, no signing-oracle needed.
- Works in seconds for all security levels.
- Ikematsu et al.[1] generalized this attack to arbitrary $\mathbf{S}$.
- Together, this led to the removal of the variants MQ-Sign-RS and MQ-Sign-SS.

[1]Ikematsu et al. *A security analysis on MQ-Sign.* In International Conference on Information Security Applications, 2023

Forgery Attack with Reduced Complexity

Forgery Attack on MQ-Sign SR

Given: a target value $\mathbf{t} = H(d) \in \mathbb{F}_q^m$

Forgery Attack on MQ-Sign SR

Given: a target value $\mathbf{t} = H(d) \in \mathbb{F}_q^m$

Find: a signature $\mathbf{z} \in \mathbb{F}_q^n$, such that $\mathcal{P}(\mathbf{z}) = \mathbf{t}$ is fulfilled, i.e.

$$(\mathbf{z}_v, \mathbf{z}_o) \begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ \mathbf{0} & \mathbf{P}_4^{(k)} \end{pmatrix} \begin{pmatrix} \mathbf{z}_v \\ \mathbf{z}_o \end{pmatrix} = \mathbf{z}_v \mathbf{P}_1^{(k)} \mathbf{z}_v + \mathbf{z}_v \mathbf{P}_2^{(k)} \mathbf{z}_o + \mathbf{z}_o \mathbf{P}_4^{(k)} \mathbf{z}_o = t_k$$

has to hold for all $k \in \{1, \ldots, m\}$.

Forgery Attack on MQ-Sign SR

Given: a target value $\mathbf{t} = H(d) \in \mathbb{F}_q^m$

Find: a signature $\mathbf{z} \in \mathbb{F}_q^n$, such that $\mathcal{P}(\mathbf{z}) = \mathbf{t}$ is fulfilled, i.e.

$$(\mathbf{z}_v, \mathbf{z}_o) \begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ \mathbf{0} & \mathbf{P}_4^{(k)} \end{pmatrix} \begin{pmatrix} \mathbf{z}_v \\ \mathbf{z}_o \end{pmatrix} = \mathbf{z}_v \mathbf{P}_1^{(k)} \mathbf{z}_v + \mathbf{z}_v \mathbf{P}_2^{(k)} \mathbf{z}_o + \mathbf{z}_o \mathbf{P}_4^{(k)} \mathbf{z}_o = t_k$$

has to hold for all $k \in \{1, \ldots, m\}$.

Recall: the submatrices $\mathbf{P}_1^{(k)} = \mathbf{F}_1^{(k)}$ are chosen sparse in $\mathrm{MQ\text{-}S{\scriptsize IGN}\text{-}SR}$

Forgery Attack on MQ-Sign SR

Given: a target value $\mathbf{t} = H(d) \in \mathbb{F}_q^m$

Find: a signature $\mathbf{z} \in \mathbb{F}_q^n$, such that $\mathcal{P}(\mathbf{z}) = \mathbf{t}$ is fulfilled, i.e.

$$(\mathbf{z}_v, \mathbf{z}_o) \begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ \mathbf{0} & \mathbf{P}_4^{(k)} \end{pmatrix} \begin{pmatrix} \mathbf{z}_v \\ \mathbf{z}_o \end{pmatrix} = \mathbf{z}_v \mathbf{P}_1^{(k)} \mathbf{z}_v + \mathbf{z}_v \mathbf{P}_2^{(k)} \mathbf{z}_o + \mathbf{z}_o \mathbf{P}_4^{(k)} \mathbf{z}_o = t_k$$

has to hold for all $k \in \{1, \ldots, m\}$.

Recall: the submatrices $\mathbf{P}_1^{(k)} = \mathbf{F}_1^{(k)}$ are chosen sparse in $\mathrm{MQ\text{-}S{\scriptsize IGN}\text{-}SR}$

First: eliminate the non-sparse submatrices $\mathbf{P}_2^{(k)}$ and $\mathbf{P}_4^{(k)}$ by fixing $\mathbf{z}_o$ randomly, which gives

$$\mathbf{z}_v \mathbf{P}_1^{(k)} \mathbf{z}_v + \mathrm{lin}(\mathbf{z}_v) = \sum_{i=1}^{v} \alpha_i^k z_i z_{(i+k-1 (\bmod v))+1} + \mathrm{lin}(\mathbf{z}_v) = t_k.$$

Forgery Attack on MQ-Sign SR

Given: a target value $\mathbf{t} = H(d) \in \mathbb{F}_q^m$

Find: a signature $\mathbf{z} \in \mathbb{F}_q^n$, such that $\mathcal{P}(\mathbf{z}) = \mathbf{t}$ is fulfilled, i.e.

$$(\mathbf{z}_v, \mathbf{z}_o) \begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ \mathbf{0} & \mathbf{P}_4^{(k)} \end{pmatrix} \begin{pmatrix} \mathbf{z}_v \\ \mathbf{z}_o \end{pmatrix} = \mathbf{z}_v \mathbf{P}_1^{(k)} \mathbf{z}_v + \mathbf{z}_v \mathbf{P}_2^{(k)} \mathbf{z}_o + \mathbf{z}_o \mathbf{P}_4^{(k)} \mathbf{z}_o = t_k$$

has to hold for all $k \in \{1, \ldots, m\}$.

Recall: the submatrices $\mathbf{P}_1^{(k)} = \mathbf{F}_1^{(k)}$ are chosen sparse in MQ-Sign-SR

First: eliminate the non-sparse submatrices $\mathbf{P}_2^{(k)}$ and $\mathbf{P}_4^{(k)}$ by fixing $\mathbf{z}_o$ randomly, which gives

$$\mathbf{z}_v \mathbf{P}_1^{(k)} \mathbf{z}_v + \mathrm{lin}(\mathbf{z}_v) = \sum_{i=1}^{v} \alpha_i^k z_i z_{(i+k-1(\bmod v))+1} + \mathrm{lin}(\mathbf{z}_v) = t_k.$$

Key observation: the $\frac{m}{2}$ equations from polynomials with odd index k are bilinear in the sets $z_{odd} = \{z_1, z_3, \ldots, z_{v-1}\}$ and $z_{even} = \{z_2, z_4, \ldots, z_v\}$

Attack Strategy

$\Rightarrow$ Split the m equations in $m/2$ bilinear and $m/2$ quadratic equations.

Attack Strategy

$\Rightarrow$ Split the m equations in $m/2$ bilinear and $m/2$ quadratic equations.

$\Rightarrow$ Split the v variables into $z_{odd} = \{z_1, z_3, \ldots, z_{v-1}\}$ and $z_{even} = \{z_2, z_4, \ldots, z_v\}$.

Attack Strategy

$\Rightarrow$ Split the m equations in $m/2$ bilinear and $m/2$ quadratic equations.

$\Rightarrow$ Split the v variables into $z_{odd} = \{z_1, z_3, \ldots, z_{v-1}\}$ and $z_{even} = \{z_2, z_4, \ldots, z_v\}$.

Step 1: Enumerate z_{odd}

Attack Strategy

$\Rightarrow$ Split the m equations in $m/2$ bilinear and $m/2$ quadratic equations.

$\Rightarrow$ Split the v variables into $z_{odd} = \{z_1, z_3, \ldots, z_{v-1}\}$ and $z_{even} = \{z_2, z_4, \ldots, z_v\}$.

Step 1: Enumerate z_{odd}

- Randomly guess the $\frac{v}{2}$ variables in z_{odd}

Attack Strategy

⇒ Split the m equations in $m/2$ bilinear and $m/2$ quadratic equations.

⇒ Split the v variables into $z_{odd} = \{z_1, z_3, \dots, z_{v-1}\}$ and $z_{even} = \{z_2, z_4, \dots, z_v\}$.

Step 1: Enumerate z_{odd}

- Randomly guess the $\frac{v}{2}$ variables in z_{odd}
- Get a $\frac{v-m}{2}$-dimensional linear solution space for z_{even} in the $\frac{m}{2}$ bilinear equations

Attack Strategy

$\Rightarrow$ Split the m equations in $m/2$ bilinear and $m/2$ quadratic equations.

$\Rightarrow$ Split the v variables into $z_{odd} = \{z_1, z_3, \ldots, z_{v-1}\}$ and $z_{even} = \{z_2, z_4, \ldots, z_v\}$.

Step 1: Enumerate z_{odd}

- Randomly guess the $\frac{v}{2}$ variables in z_{odd}
- Get a $\frac{v-m}{2}$-dimensional linear solution space for z_{even} in the $\frac{m}{2}$ bilinear equations
- Problem: will most likely not yield a solution to the remaining $\frac{m}{2}$ quadratic (non-bilinear) equations (probability $\approx q^{-(\frac{v}{2}-(v-m))}$) $\rightarrow$ repeat until **Step 2** finds a solution

Attack Strategy

$\Rightarrow$ Split the m equations in $m/2$ bilinear and $m/2$ quadratic equations.

$\Rightarrow$ Split the v variables into $z_{odd} = \{z_1, z_3, \ldots, z_{v-1}\}$ and $z_{even} = \{z_2, z_4, \ldots, z_v\}$.

Step 1: Enumerate z_{odd}

- Randomly guess the $\frac{v}{2}$ variables in z_{odd}
- Get a $\frac{v-m}{2}$-dimensional linear solution space for z_{even} in the $\frac{m}{2}$ bilinear equations
- Problem: will most likely not yield a solution to the remaining $\frac{m}{2}$ quadratic (non-bilinear) equations (probability $\approx q^{-(\frac{v}{2}-(v-m))}$) $\rightarrow$ repeat until **Step 2** finds a solution

Step 2: Solve for z_{even}

Attack Strategy

$\Rightarrow$ Split the m equations in $m/2$ bilinear and $m/2$ quadratic equations.

$\Rightarrow$ Split the v variables into $z_{odd} = \{z_1, z_3, \ldots, z_{v-1}\}$ and $z_{even} = \{z_2, z_4, \ldots, z_v\}$.

Step 1: Enumerate z_{odd}

- Randomly guess the $\frac{v}{2}$ variables in z_{odd}
- Get a $\frac{v-m}{2}$-dimensional linear solution space for z_{even} in the $\frac{m}{2}$ bilinear equations
- Problem: will most likely not yield a solution to the remaining $\frac{m}{2}$ quadratic (non-bilinear) equations (probability $\approx q^{-(\frac{v}{2}-(v-m))}$) $\rightarrow$ repeat until **Step 2** finds a solution

Step 2: Solve for z_{even}

- Try to find an assignment to z_{even} that also validate the remaining $\frac{m}{2}$ equations

Attack Strategy

$\Rightarrow$ Split the m equations in $m/2$ bilinear and $m/2$ quadratic equations.

$\Rightarrow$ Split the v variables into $z_{odd} = \{z_1, z_3, \ldots, z_{v-1}\}$ and $z_{even} = \{z_2, z_4, \ldots, z_v\}$.

Step 1: Enumerate z_{odd}

- Randomly guess the $\frac{v}{2}$ variables in z_{odd}
- Get a $\frac{v-m}{2}$-dimensional linear solution space for z_{even} in the $\frac{m}{2}$ bilinear equations
- Problem: will most likely not yield a solution to the remaining $\frac{m}{2}$ quadratic (non-bilinear) equations (probability $\approx q^{-(\frac{v}{2}-(v-m))}$) $\rightarrow$ repeat until **Step 2** finds a solution

Step 2: Solve for z_{even}

- Try to find an assignment to z_{even} that also validate the remaining $\frac{m}{2}$ equations
- I.e. solve a quadratic system of $\frac{m}{2}$ equations in $\frac{v-m}{2}$ variables

Complexity of Forgery Attack on MQ-Sign SR

Security level	Parameters (q, v, m)	$C_{\mathrm{ENUM}(q,\frac{v}{2}-(v-m))}$	$C_{\mathrm{MQ}(q,\frac{v-m}{2},\frac{m}{2})}$	Complexity
I	$(2^8, 72, 46)$	2^{80}	2^{31}	2^{111}
III	$(2^8, 112, 72)$	2^{128}	2^{42}	2^{170}
V	$(2^8, 148, 96)$	2^{176}	2^{52}	2^{228}

Table: Theoretical complexity of the forgery attack.

- $C_{\mathrm{ENUM}(q,\frac{v}{2}-(v-m))}$ denote the cost of the enumeration.
- $C_{\mathrm{MQ}(q,\frac{v-m}{2},\frac{m}{2})}$ denote the cost of solving the remaining quadratic system .

Complexity of Forgery Attack on MQ-Sign SR

Security level	Parameters (q, v, m)	$C_{\mathrm{ENUM}(q, \frac{v}{2}-(v-m))}$	$C_{\mathrm{MQ}(q, \frac{v-m}{2}, \frac{m}{2})}$	Complexity
I	$(2^8, 72, 46)$	2^{80}	2^{31}	2^{111}
III	$(2^8, 112, 72)$	2^{128}	2^{42}	2^{170}
V	$(2^8, 148, 96)$	2^{176}	2^{52}	2^{228}

Table: Theoretical complexity of the forgery attack.

- $C_{\mathrm{ENUM}(q, \frac{v}{2}-(v-m))}$ denote the cost of the enumeration.
- $C_{\mathrm{MQ}(q, \frac{v-m}{2}, \frac{m}{2})}$ denote the cost of solving the remaining quadratic system .

$\Rightarrow$ We implemented the system solving step to validate the complexity estimates.

Impact and Open Research Questions

MQ-Sign in Competition Round 2

MQ-Sign advanced to the KpqC Competition Round 2

Round 1 Variants	Attack Type	Complexity	Round 2 Variants
MQ-Sign-RR	-	-	MQ-Sign-RR
MQ-Sign-SR	direct attack	exp time	MQ-Sign-LR[2]
MQ-Sign-RS	key-recovery	poly time	✗
MQ-Sign-SS	key-recovery	poly time	✗

[2]another sparse MQ-Sign variant with different structure

MQ-Sign in Competition Round 2

MQ-Sign advanced to the KpqC Competition Round 2

Round 1 Variants	Attack Type	Complexity	Round 2 Variants
MQ-Sign-RR	-	-	MQ-Sign-RR
MQ-Sign-SR	direct attack	exp time	MQ-Sign-LR[2]
MQ-Sign-RS	key-recovery	poly time	✗
MQ-Sign-SS	key-recovery	poly time	✗

⇒ The presented key-recovery attack - together with its generalization by Ikematsu et al. - led to the removal of the last two variants

[2] another sparse MQ-Sign variant with different structure

MQ-Sign in Competition Round 2

MQ-Sign advanced to the KpqC Competition Round 2

Round 1 Variants	Attack Type	Complexity	Round 2 Variants
MQ-Sign-RR	-	-	MQ-Sign-RR
MQ-Sign-SR	direct attack	exp time	MQ-Sign-LR[2]
MQ-Sign-RS	key-recovery	poly time	✗
MQ-Sign-SS	key-recovery	poly time	✗

⇒ The presented key-recovery attack - together with its generalization by Ikematsu et al. - led to the removal of the last two variants

⇒ Possible future work: cryptanalysis of MQ-Sign-LR

[2] another sparse MQ-Sign variant with different structure

The End

Takeaways

- Sparse polynomials can introduce vulnerabilities.
- Attacks do not exploit a general weakness, sparse polynomials are still interesting.
- It seems preferable to choose public polynomials sparse, instead of secret polynomials.

Questions?

Contact: thomas.aulbach@ur.de

Aulbach, Samardjiska, Trimoska:
Practical Key-Recovery on MQ-Sign and More
https://ia.cr/2023/432