Multivariate Quadratic Polynomials in Public Key Cryptography

Christopher Wolf

Katholieke Universiteit Leuven
Dept. Electrical Engineering — ESAT/COSIC

Christopher.Wolf@esat.kuleuven.be
chris@Christopher-Wolf.de

DIAMANT/EIDMA symposium 2005

November 16, 2006, Mierlo, The Netherlands

Outline

Outline

Introduction
Motivation of this talk

- Asymmetric Cryptography is necessary for using the Internet in a secure manner, *e.g.*, e-Commerce applications, private communication, secure communication

Introduction
Motivation of this talk

- Asymmetric Cryptography is necessary for using the Internet in a secure manner, *e.g.*, e-Commerce applications, private communication, secure communication
- At present, mostly RSA (factoring), and $\mathbb{Z}_p$/ECC (discrete logarithm) are used for asymmetric cryptography

Introduction
Motivation of this talk

- Asymmetric Cryptography is necessary for using the Internet in a secure manner, *e.g.*, e-Commerce applications, private communication, secure communication
- At present, mostly RSA (factoring), and $\mathbb{Z}_p$/ECC (discrete logarithm) are used for asymmetric cryptography
- Both factoring and discrete logarithm are insecure under the assumption that quantum computer exist (algorithm of Shor), hence new schemes are needed (long-term security)

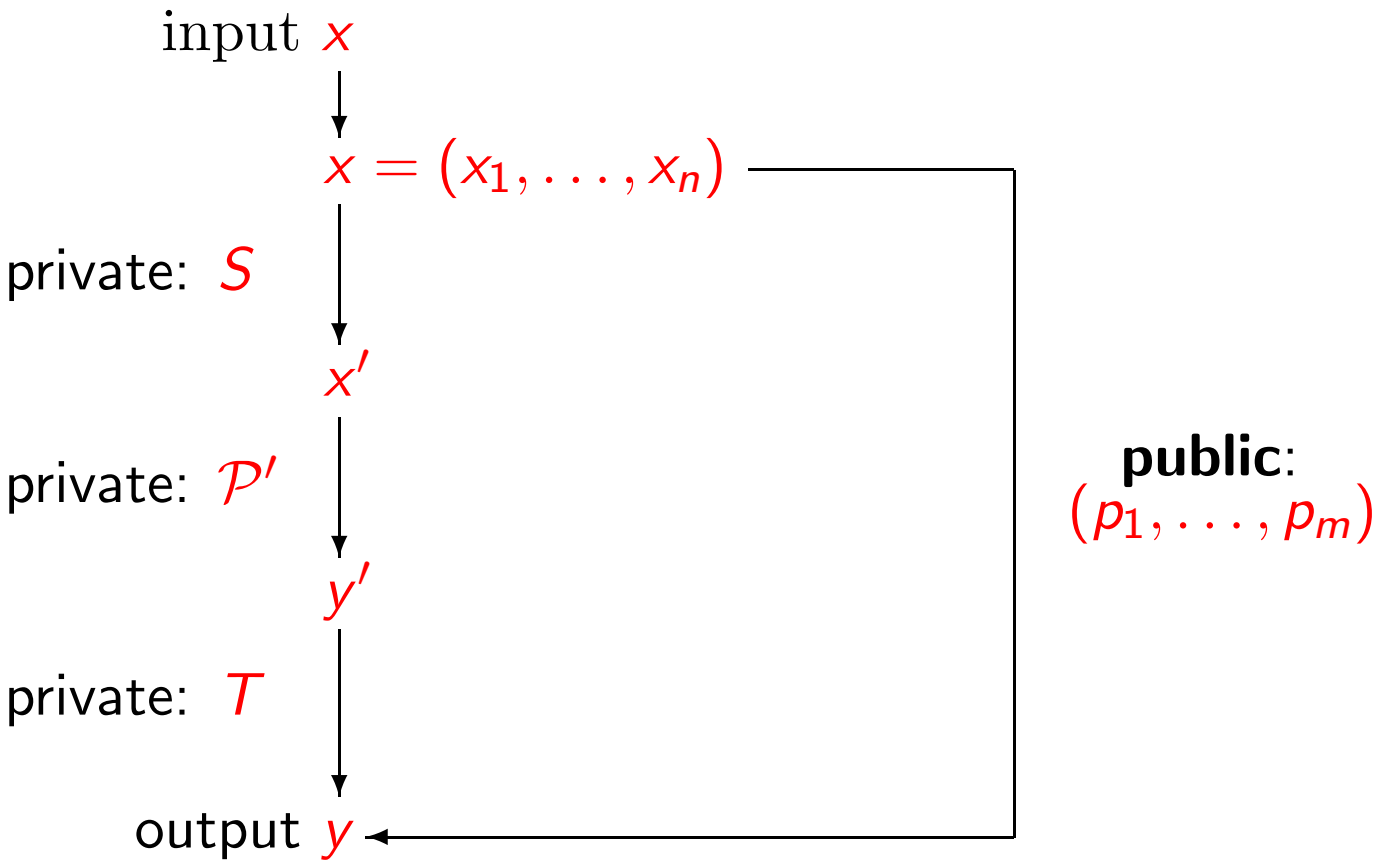
Introduction
$\mathcal{MQ}$-Schemes

- Multivariate Quadratic schemes are known since the 1980s — since then, some effort has been made to understand their security
- These schemes allow fast encryption and signature verification — often also fast decryption and signature generation
- With the current constructions, it is possible to achieve signatures as short as 128 bits
- All in all, they are a worthwhile research topic as there are still many open questions. However, they are not yet used in practice

Outline

Multivariate Quadratic Cryptography

Graphical Overview



$\mathcal{M}$ultivariate $\mathcal{Q}$uadratic Cryptography

Comparison with RSA

Encryption in RSA

$$y = x^e \pmod{n}$$

Encryption in $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic systems

$$\begin{cases} y_1 = x_1x_2 + x_1x_3 + x_1x_5 + x_2x_5 + x_2x_6 + x_3x_5 + x_5x_6 \pmod{p} \\ y_2 = x_1x_3 + x_2x_4 + x_3x_5 \pmod{p} \\ y_3 = x_1x_3 + x_1x_5 + x_2x_3 + x_3x_4 + x_3x_6 + x_5x_6 \pmod{p} \\ y_4 = x_1x_2 + x_3x_5 \pmod{p} \\ y_5 = x_1x_3 + x_1x_4 + x_1x_5 + x_2x_4 + x_3x_4 + x_3x_6 \pmod{p} \\ y_6 = x_1x_3 + x_1x_4 + x_2x_3 + x_2x_5 + x_3x_4 + x_4x_5 + x_4x_6 \pmod{p} \end{cases}$$

$\mathcal{M}$ultivariate $\mathcal{Q}$uadratic Cryptography

Overview

- Public key schemes based on problem of solving $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic polynomial equations and the Isomorphism of Polynomials problem
- Use polynomials over small finite fields $\mathbb{F}$, *e.g.*, GF(2), GF(128), or GF(256) — hence very suitable for 8-bit microprocessors
- Some schemes use extension fields $\mathbb{E}$ with dimension n over $\mathbb{F}$
- Secret key $(S, \mathcal{P}', T) \in \mathrm{AGL}_n(\mathbb{F}) \times \mathcal{MQ}_m(\mathbb{F}^n) \times \mathrm{AGL}_m(\mathbb{F})$
- Public key $\mathcal{P} \in \mathcal{MQ}_m(\mathbb{F}^n)$ with $\mathcal{P} = T \circ \mathcal{P}' \circ S$

Multivariate Quadratic Cryptography
Public Key

Public Key equations:

$$p_i(x_1, \ldots, x_n) := \sum_{1 \leq j \leq k \leq n} \gamma_{i,j,k} x_j x_k + \sum_{j=1}^{n} \beta_{i,j} x_j + \alpha_i$$

for $1 \leq i \leq m$ and coefficients $\alpha_i, \beta_{i,j}, \gamma_{i,j,k} \in \mathbb{F}$

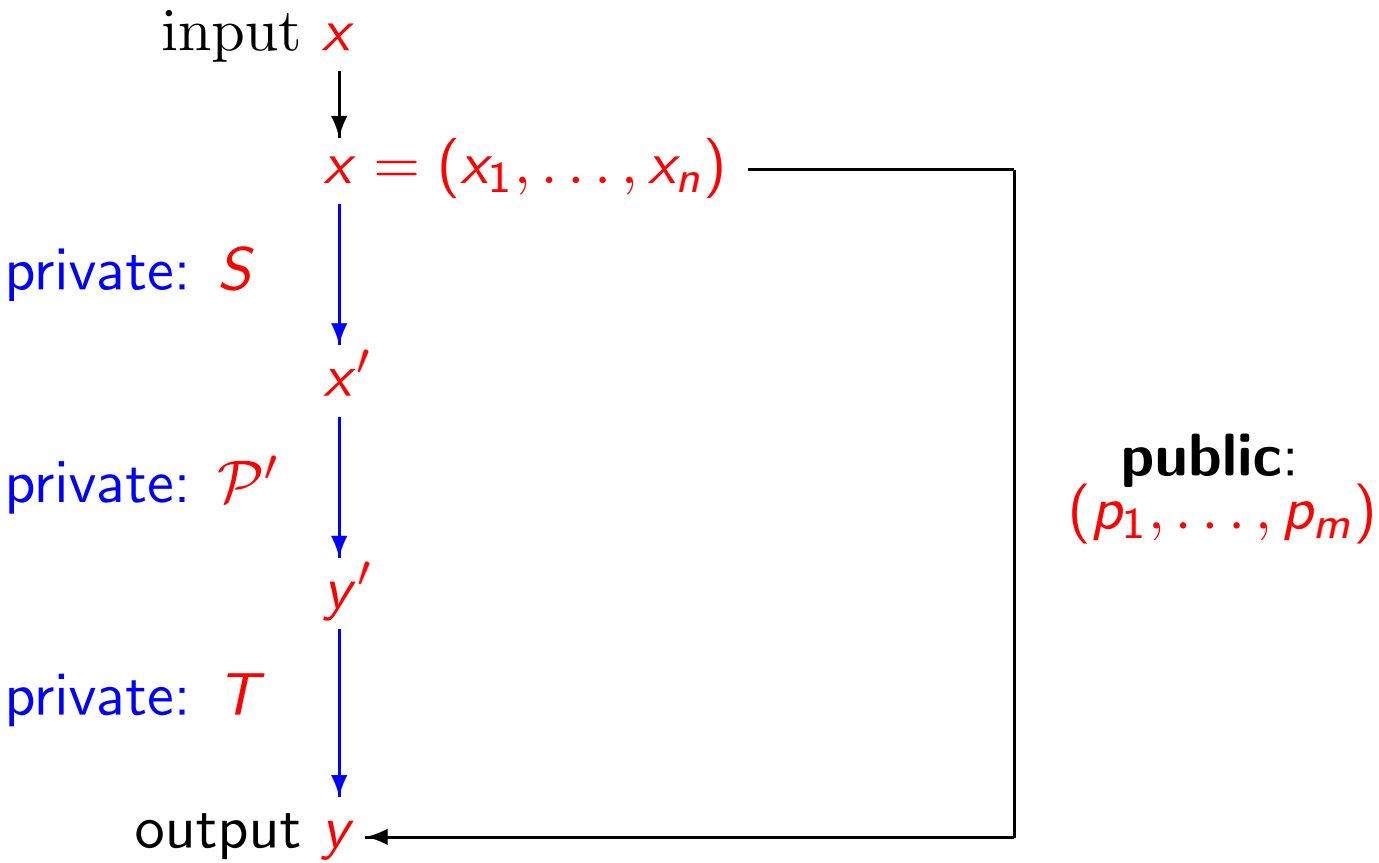
Notation: $\mathcal{P}(x) := (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n))$

Encryption: Compute $y \in \mathbb{F}^m$ for given $x \in \mathbb{F}^n$ by evaluating $y = \mathcal{P}(x)$. We now have cipher text y for the plain text x

Signature verification: Given pair $(x, y) \in \mathbb{F}^n \times \mathbb{F}^m$. Check if the equation $y \stackrel{?}{=} \mathcal{P}(x)$ holds

Multivariate Quadratic Cryptography

Private Key

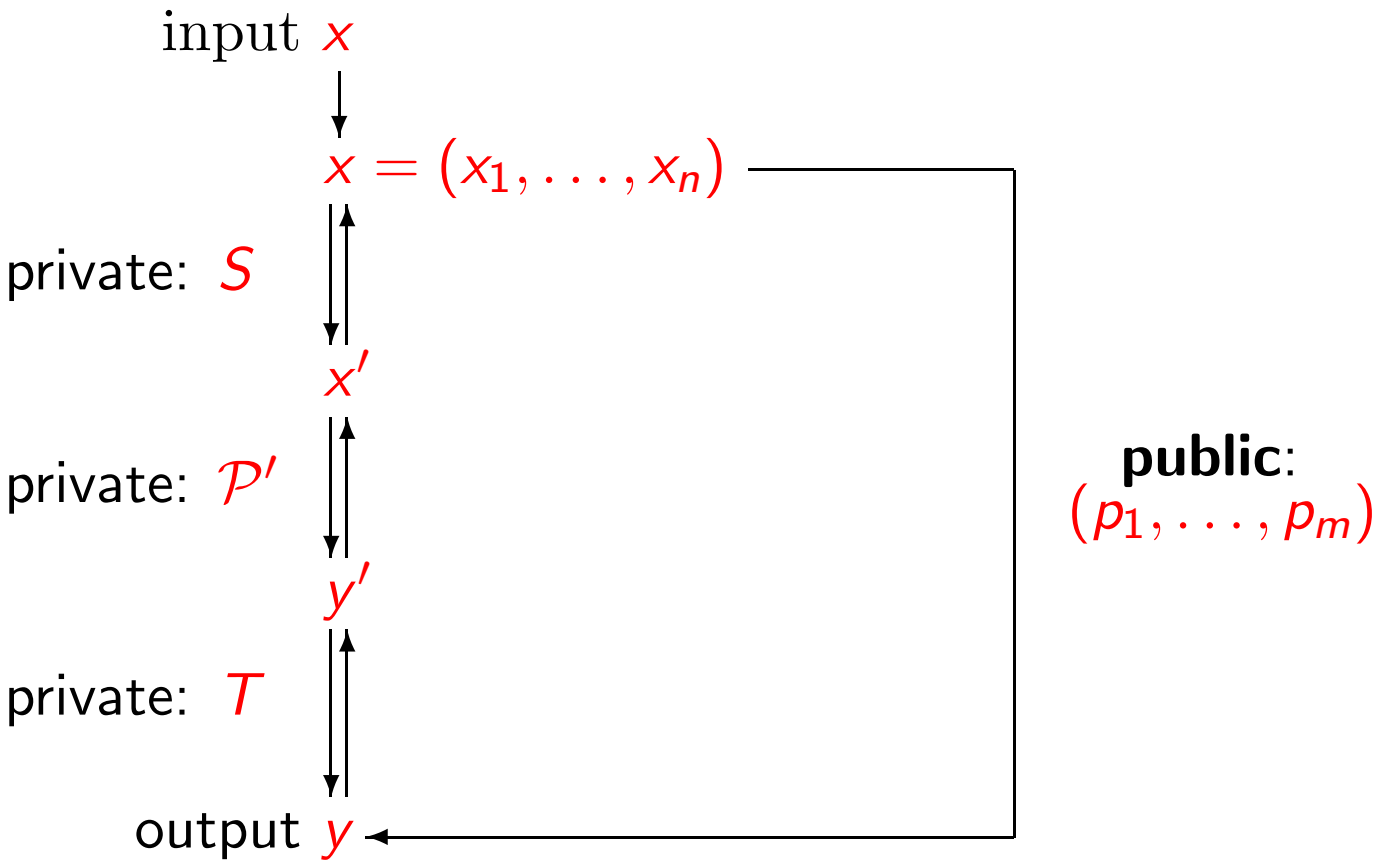


Multivariate Quadratic Cryptography
Private Key Computations

- **Inversion of affine transformations:**
  Let $S(x) = M_S x + v_s$ for $M_S \in \mathbb{F}^{n \times n}, v_s \in \mathbb{F}^n$. We require M_S being invertible and compute $S^{-1}(x') = M_S^{-1}(x' - v_s)$.
  Similar, we can invert $T(y') = y$ for given y
- **Inversion of $\mathcal{P}$':** *Different for each scheme, see later*
- **Signature generation:** invert each step for given $y \in \mathbb{F}^m$, publish the corresponding x as signature of y
- **Decryption:** unique inversion of $\mathcal{P}'$ may not be possible, hence, some redundancy $H := h(x)$ is used with $h(\cdot)$ a cryptographically secure hash function to pick the correct cleartext $x \in \mathbb{F}^n$ for given ciphertext $y \in \mathbb{F}^m$

Multivariate Quadratic Cryptography

Graphical Overview (2)



Outline

Basic Classes
Motivation 1/2

Allows to contract previously written paper into one taxonomy.

- **Unbalanced Oil and Vinegar (UOV)**
  Patarin (1997); Kipnis, Schmir (1998); Kipnis, Patarin, Goubin (1999); Courtois, Goubin, Meier, Tacier (2002); Braeken, Wolf, Preneel (2005); Ding, Schmidt (2005); Wolf, Preneel (2005)
- **Stepwise Triangular Systems (STS)**
  Coppersmith, Stern, Vaudenay (1993); Shamir (1993); Theobald (1995); Coppersmith, Stern, Vaudenay (1997); Moh (1999); Goubin, Courtois (2000); Ding, Yin (2004); Wang, Chang (2004); Kasahara, Sakai (2004); Wolf, Braeken, Preneel (2004); Yang, Chen (2004); Joux, Kunz-Jacques, Muller, Ricordel (2005); Kasahara, Sakai (2005); Wang, Hu, Lai, Chou, Yang (2005)

Basic Classes
Motivation 2/2

- **Matsumoto Imai Scheme A (MIA)**
  Matsumoto, Imai (1985); Matsumoto, Imai, Harashima, Miyakawa (1985); Matsumoto, Imai (1988); Patarin (1995); Patarin, Goubin (1997); Patarin, Goubin, Courtois (1998); Courtois, Goubin, Patarin (2000); Courtois, Goubin, Patarin (2001); Geiselmann, Steinwandt, Beth (2001); Felke (2001); Courtois, Goubin, Patarin (2002); Gilbert, Minier (2002); Ding (2004); Fouque, Granboulan, Stern (2005); Wolf, Preneel (2005)
- **Hidden Field Equations (HFE)**
  Patarin (1996); Kipnis, Shamir (1999); Courtois, Goubin, Patarin (2000); Courtois, Goubin, Patarin (2001); Daum (2001); Courtois (2002); Courtois, Daum, Felke (2003); Faugère, Joux (2003); Sidorenko, Gabidulin (2003); Felke (2004); Wolf (2004); Wolf, Preneel (2004); Ding, Schmidt (2005); Wolf, Preneel (2005)

Basic Classes

Unbalance Oil and Vinegar scheme (UOV)

Unbalanced Oil and Vinegar scheme. Uses vinegar and oil variables (v and o). We have $n = v + o$ and need $v = 2o \ldots 3o$ for a secure scheme. Moreover, we have $o = m$.
Central polynomials have the form

$$p'_i(x'_1, \ldots, x'_n) := \sum_{j=1}^{v} \sum_{k=1}^{n} \gamma'_{i,j,k} x'_j x'_k + \sum_{j=1}^{n} \beta'_{i,j} x'_j + \alpha'_i$$

for $1 \leq i \leq m$ and coefficients $\alpha'_i, \beta'_{i,j}, \gamma'_{i,j,k} \in \mathbb{F}$.
Note: These equations become linear if values are assigned to the vinegar variables $x'_1, \ldots, x'_v$

Basic Classes

STS — Overview

System $\mathcal{P}'$:

$$\begin{array}{rl}
\text{Step } 1 & \left\{ \begin{array}{llll} p'_1 & (x'_1, \ldots, x'_r) & & \\ & \vdots & & \\ p'_r & (x'_1, \ldots, x'_r) & & \end{array} \right. \\
\vdots & \\
\text{Step } l & \left\{ \begin{array}{llll} p'_{(l-1)r+1} & (x'_1, \ldots, x'_r, & \ldots, & x'_{(l-1)r+1}, \ldots, x'_{lr}) \\ & & \vdots & \\ p'_{lr} & (x'_1, \ldots, x'_r, & \ldots, & x'_{(l-1)r+1}, \ldots, x'_{lr}) \end{array} \right.
\end{array}$$

Basic Classes

Matsumoto Imai Scheme A (MIA)

For this scheme (Matsumoto Imai Scheme A, also C*), the central equations are over an extension field $\mathbb{E}$ of degree n. They have the form

$$P(X') := X'^{q^\lambda+1}$$

for $q := |\mathbb{F}|$ and some $\lambda \in \mathbb{N}$.
Between $\mathbb{F}^n$ and $\mathbb{E}$, we use a coefficient-wise bijection, *i.e.*, let the vector $a \in \mathbb{F}^n$ be $(a_1, \ldots, a_n)$ with $a_i \in \mathbb{F}$, and let the element $b \in \mathbb{E}$ have the form $b_{n-1}t^{n-1} + \cdots + b_1 t + b_0$ with $b_i \in \mathbb{F}$ and $i(t)$ the defining polynomial of $\mathbb{E}$.
As X'^{q^λ} is a linear equation over $\mathbb{F}$ for any $\lambda \in \mathbb{N}$ and so is X', their product leads to quadratic equations over $\mathbb{F}$.
To obtain a bijection, we also need $\gcd(q^n - 1, q^\lambda + 1) = 1$.

Basic Classes
Hidden Field Equations (HFE)

Hidden Field Equations. Use a similar idea as MIA, but exploit a different idea for the trapdoor. Note: no bijection anymore.
As for MIA, the central equations are over an extension field $\mathbb{E}$ of degree n. They have the form

$$P'(X') := \sum_{\substack{0\le i,j\le d \\ q^i+q^j\le d}} C'_{i,j} X'^{q^i+q^j} + \sum_{\substack{0\le k\le d \\ q^k\le d}} B'_k X'^{q^k} + A'$$

$$\text{where} \begin{cases} C'_{i,j} X^{q^i+q^j} & \text{for } C'_{i,j} \in \mathbb{E} \text{ are the quadratic terms,} \\ B'_k X^{q^k} & \text{for } B'_k \in \mathbb{E} \text{ are the linear terms, and} \\ A' & \text{for } A' \in \mathbb{E} \text{ is the constant term} \end{cases}$$

for $i, j \in \mathbb{N}$ and some degree $d \in \mathbb{N}$.

Basic Classes
Modifiers

Symbol	Long Name	Security
-	Minus	secure
+	Plus	mostly no effect
/	Subfield	insecure
$\perp$	Branching	insecure
f	fixing	open
h	homogenising	no effect
i	internal	open
m	masking	open
s	sparse	open
v	vinegar	slightly more secure

Examples: HFEv-, MIAi, MIAi+, UOV/, STS(UOV)

Outline

Practical Examples
Random Number Generation

Exploit the fact that $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic equations are difficult to solve, namely $\mathcal{NP}$-complete. Secure parameters would be

Seed [bit]	Parameter	$\mathcal{MQ}$-System [kByte]	Evaluation [ms]
259	$q = 128$, $m = n = 37$	23	< 1
469	$q = 128$, $m = n = 67$	134	< 1

The evaluation time has been computed for a PC. However, we only used "full" $\mathcal{MQ}$-systems for this proposal. Using specially designed equations, we could both reduce the number of variables and the size of these systems.

Practical Examples
Electronic Stamps

Need fast signature generation, fast signature verification. Large public keys are no problem as we would not change the public keys too often. Main concern: high through-put of messages and low signature expansion.

Hash [bit]	Parameter	Priv. Key [kByte]	Pub. Key [kByte]	Sign [ms]	Verify [ms]	Expansion [bit]
160	$q = 128$ $n = 67$ $r = 11$	7.8	112.3	< 1	< 1	237

Practical Examples
Electronic Stamps

The above parameters have been taken from Quartz. Note the low signature expansion rate. However, signature generation time now goes up to 5 seconds (extrapolation from Quartz).

Message [bit]	Parameter	Pub. Key [kByte]	Sign [ms]	Verify [ms]	Expansion [bit]
173	$q = 2$ $n = 173$ $r = 10$	310.2	5,000	< 5	10

Practical Examples
Quartz Signature Scheme

Quartz has been suggested as a signature scheme in the European NESSIE project. Below we summarise the parameter for its secure variation Quartz-7m.

Parameter	Priv. Key [kByte]	Pub. Key [kByte]	Sign [ms]	Verify [ms]	Signature [bit]
$q = 2$ $n = 107$ $r = 7$	3	71	10,000	< 1	128

Outline

Conclusions

- There are only 4 basic trapdoors for multivariate schemes known so far — and 3 of them are broken in their basic version
- However, they may be combined with several modifiers
- We know that some of the modified versions (*e.g.*, HFE- instead of HFE, MIA- instead of MIA) are much stronger. Hence, a more systematic study of this topic may be useful

Conclusions

- A general characteristic of $\mathcal{MQ}$-systems is that they allow several "tweaks" and trades, *e.g.*,
  - key size vs. generation time
  - signature size vs. generation time
  - key size vs. message expansion
- $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic signature schemes have been investigated since 2 decades by now. The theory is developed, we are now ready to do the step from concepts to products

Thank you for your attention!