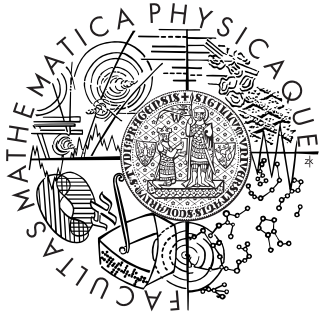
Quadratic quasigroups in public-key cryptography

Adam Christov

Charles University in Prague

Spring School of Algebra - March 2010



Motivation

- Security of the public-key schemes relies on just a small number of problems (factorization, discrete logarithm).

Motivation

- Security of the public-key schemes relies on just a small number of problems (factorization, discrete logarithm).
- Research on new cryptography schemes based on other classes of problems is important.

Motivation

- Security of the public-key schemes relies on just a small number of problems (factorization, discrete logarithm).
- Research on new cryptography schemes based on other classes of problems is important.
- **Danilo Gligoroski et al.** - presented schema which is using a special kind of quasigroups, the so-called *quadratic quasigroups*. This scheme is a specialization of general MQ-scheme (Matsumoto, Imai 1985), which relies on the problem of finding a solution of a system of multivariate quadratic equations.

Motivation

- Security of the public-key schemes relies on just a small number of problems (factorization, discrete logarithm).
- Research on new cryptography schemes based on other classes of problems is important.
- **Danilo Gligoroski et al.** - presented schema which is using a special kind of quasigroups, the so-called *quadratic quasigroups*. This scheme is a specialization of general MQ-scheme (Matsumoto, Imai 1985), which relies on the problem of finding a solution of a system of multivariate quadratic equations.
- In this talk I will show how this scheme works, then I will describe the quadratic quasigroups and loops.

General MQ-scheme

- **private key**: $(\mathscr{L}_1, \mathscr{L}_2, \mathscr{P})$.
  - $\mathscr{L}_1, \mathscr{L}_2$ are automorphisms of the vector space $\mathbb{F}_2^n$ (regular matrices)
  - $\mathscr{P}$ is an invertible map $\mathbb{F}_2^n \to \mathbb{F}_2^n$ represented by quadratic Boolean polynomials.

General MQ-scheme

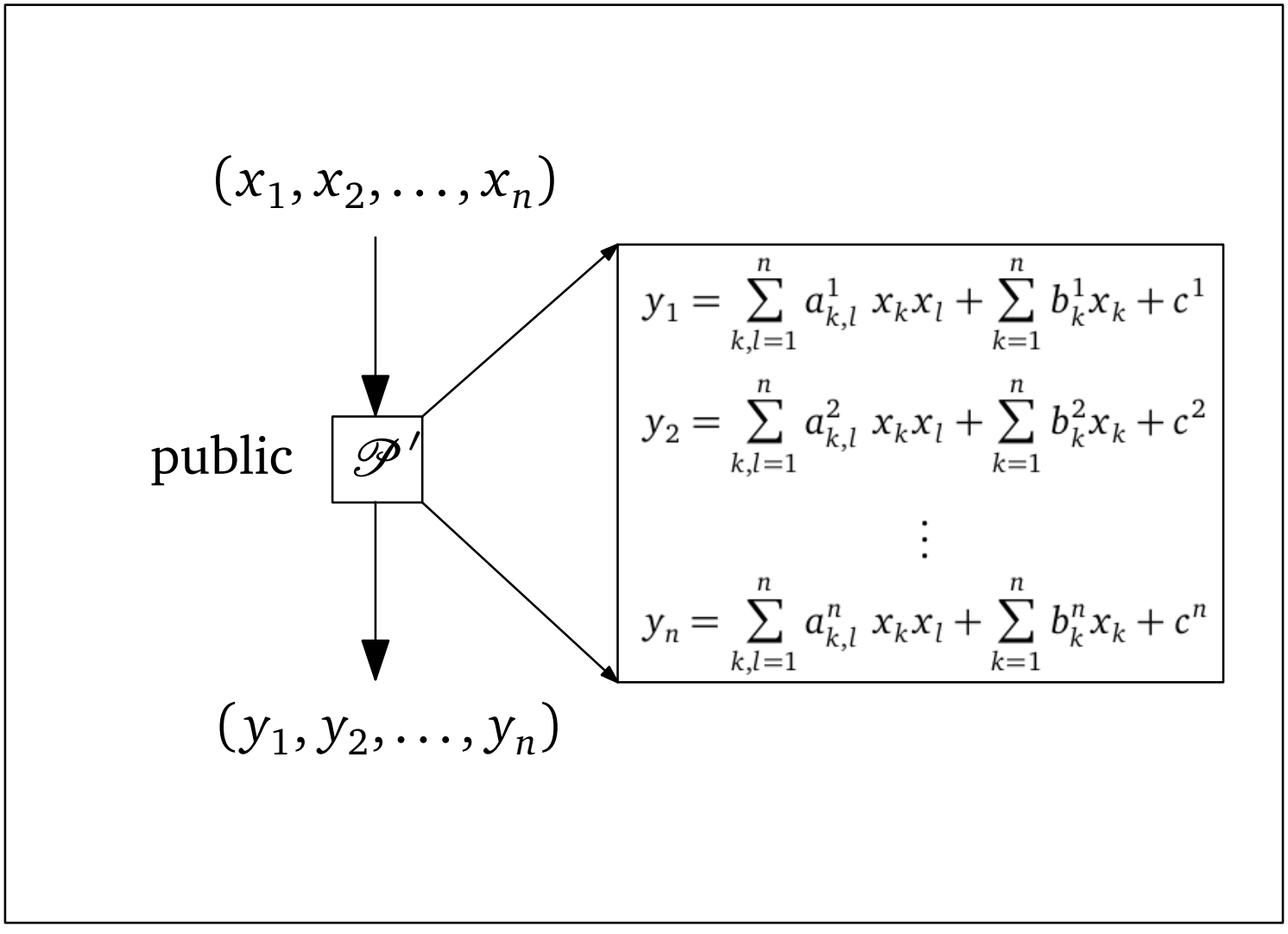
- **private key**: $(\mathscr{L}_1, \mathscr{L}_2, \mathscr{P})$.
  - $\mathscr{L}_1, \mathscr{L}_2$ are automorphisms of the vector space $\mathbb{F}_2^n$ (regular matrices)
  - $\mathscr{P}$ is an invertible map $\mathbb{F}_2^n \to \mathbb{F}_2^n$ represented by quadratic Boolean polynomials.
- **public key**: $\mathscr{P}' = \mathscr{L}_2 \circ \mathscr{P} \circ \mathscr{L}_1$.

Encryption and decryption

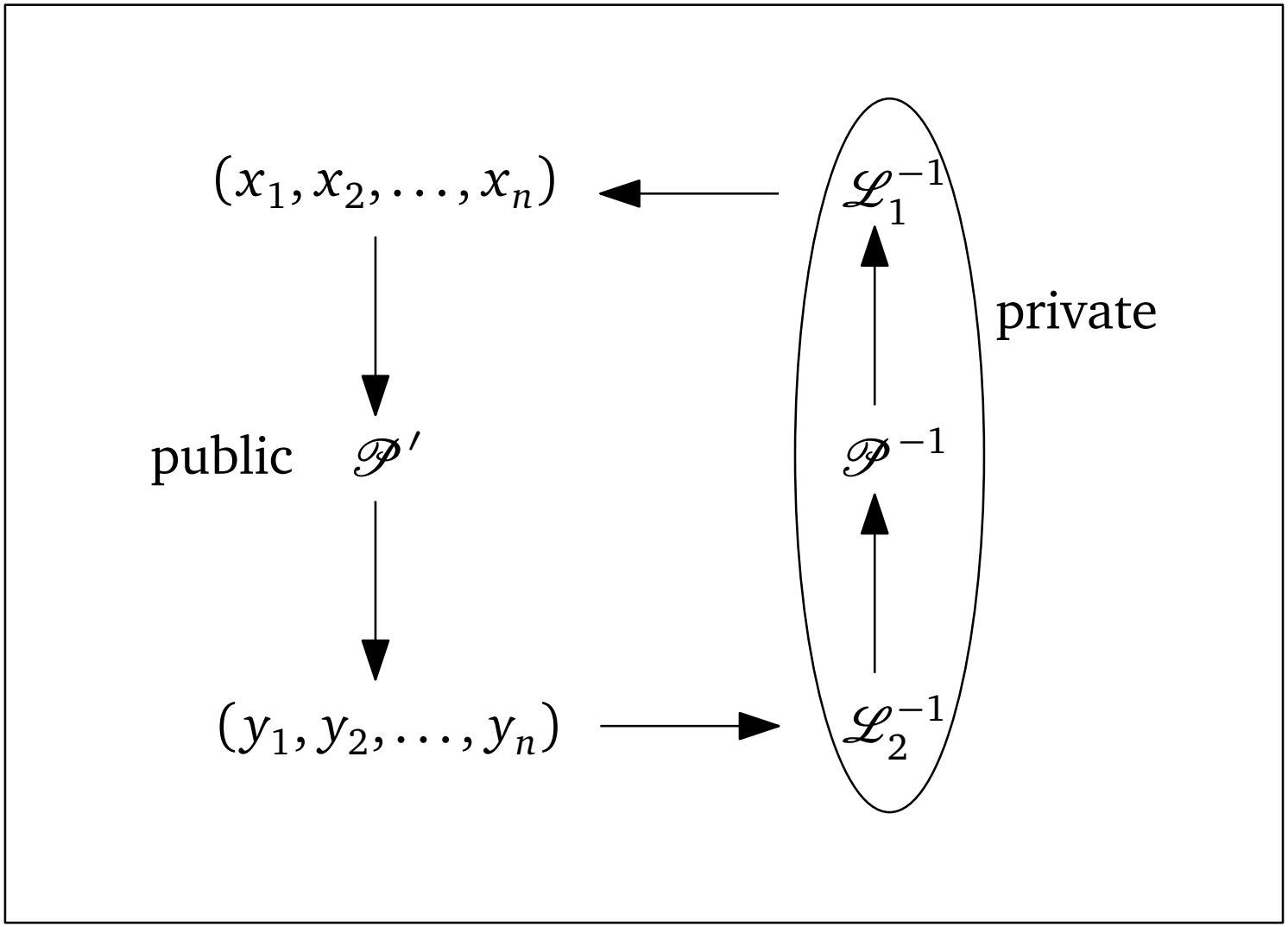
Secret message

$(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$

Encryption and decryption



Encryption and decryption



Quadratic quasigroup

Let $(\mathbb{F}_2^m, *)$ be a quasigroup upon the vector space $\mathbb{F}_2^m$.

$$
\begin{aligned}
* : \quad & \mathbb{F}_2^{2m} \to \mathbb{F}_2^m, \text{ neco} \\
* : \quad & (x_1, \ldots, x_m, y_1, \ldots, y_m) \mapsto (z_1, \ldots, z_m),
\end{aligned}
$$

where $(x_1, \ldots, x_m) * (y_1, \ldots, y_m) = (z_1, \ldots, z_m)$.

Quadratic quasigroup

Let $(\mathbb{F}_2^m, *)$ be a quasigroup upon the vector space $\mathbb{F}_2^m$.

$$\begin{aligned} * : \quad & \mathbb{F}_2^{2m} \to \mathbb{F}_2^m, \text{ neco} \\ * : \quad & (x_1, \ldots, x_m, y_1, \ldots, y_m) \mapsto (z_1, \ldots, z_m), \end{aligned}$$

where $(x_1, \ldots, x_m) * (y_1, \ldots, y_m) = (z_1, \ldots, z_m)$.

$$\begin{aligned} *_i : \quad & \mathbb{F}_2^{2m} \to \mathbb{F}_2 \\ *_i : \quad & (x_1, \ldots, x_m, y_1, \ldots, y_m) \mapsto z_i. \end{aligned}$$

$*_i$ is a boolean map. There exists corresponding boolean polynomial f_i such that

$$\mathbf{x} * \mathbf{y} = \Big(f_1(\mathbf{x}, \mathbf{y}), f_2(\mathbf{x}, \mathbf{y}), \ldots, f_m(\mathbf{x}, \mathbf{y}) \Big),$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^m$.

Quadratic quasigroup

Definiton

A quasigroup with an operation "$*$" on the set $\mathbb{F}_2^m$ is called *quadratic* if there exists quadratic polynomials $f_i \in \mathbb{F}_2[x_1, \ldots, x_m, y_1, \ldots, y_m], i = 1, \ldots, m$ of the order at most 2 such that

$$\mathbf{x} * \mathbf{y} = \Big(f_1(\mathbf{x}, \mathbf{y}), f_2(\mathbf{x}, \mathbf{y}), \ldots, f_m(\mathbf{x}, \mathbf{y}) \Big),$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^m$.

Quadratic quasigroup

Definiton

A quasigroup with an operation "$*$" on the set $\mathbb{F}_2^m$ is called *quadratic* if there exists quadratic polynomials $f_i \in \mathbb{F}_2[x_1, \ldots, x_m, y_1, \ldots, y_m], i = 1, \ldots, m$ of the order at most 2 such that

$$\mathbf{x} * \mathbf{y} = \Big(f_1(\mathbf{x}, \mathbf{y}), f_2(\mathbf{x}, \mathbf{y}), \ldots, f_m(\mathbf{x}, \mathbf{y}) \Big),$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^m$.

The map $\mathscr{P} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is constructed from quadratic quasigroups of order 2^5 in the following way:

Construction of the map $\mathscr{P}$

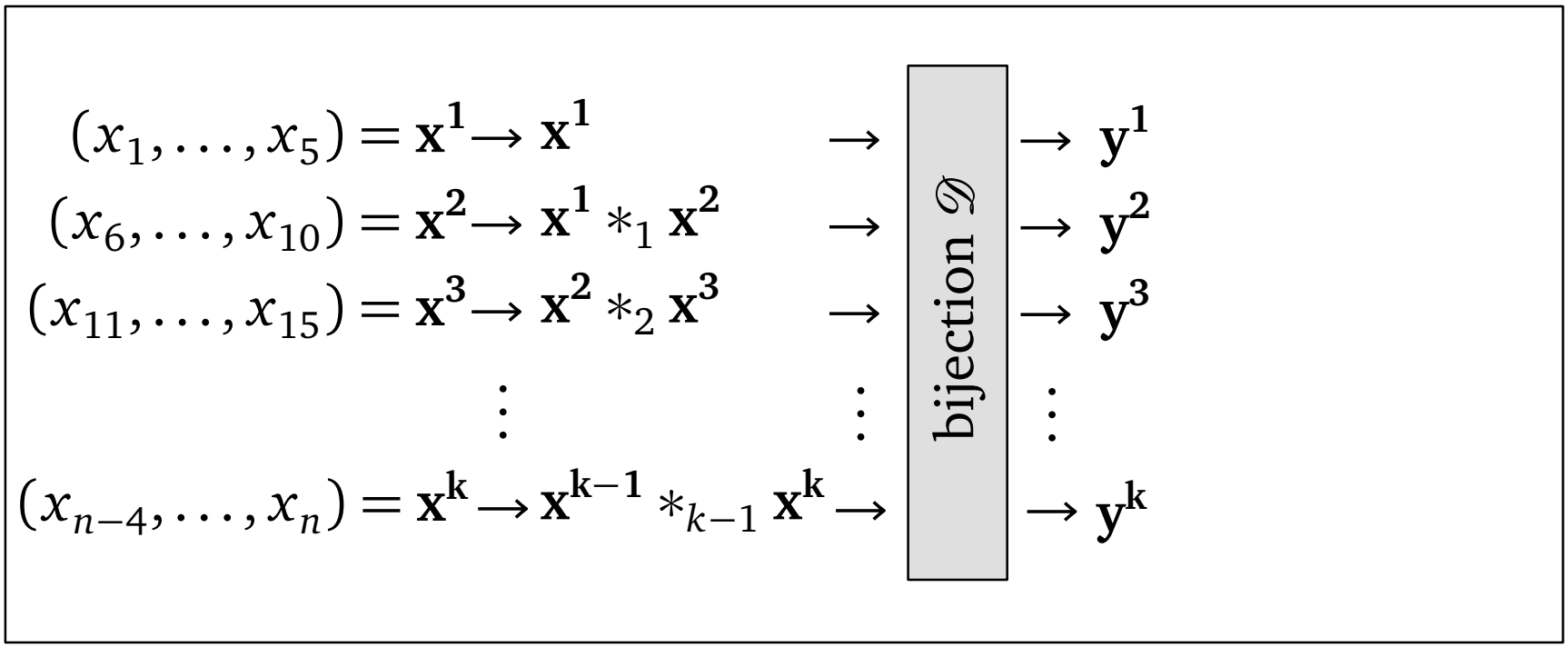
$$(x_1, \ldots, x_5) = \mathbf{x^1}$$
$$(x_6, \ldots, x_{10}) = \mathbf{x^2}$$
$$(x_{11}, \ldots, x_{15}) = \mathbf{x^3}$$

$$(x_{n-4}, \ldots, x_n) = \mathbf{x^k}$$

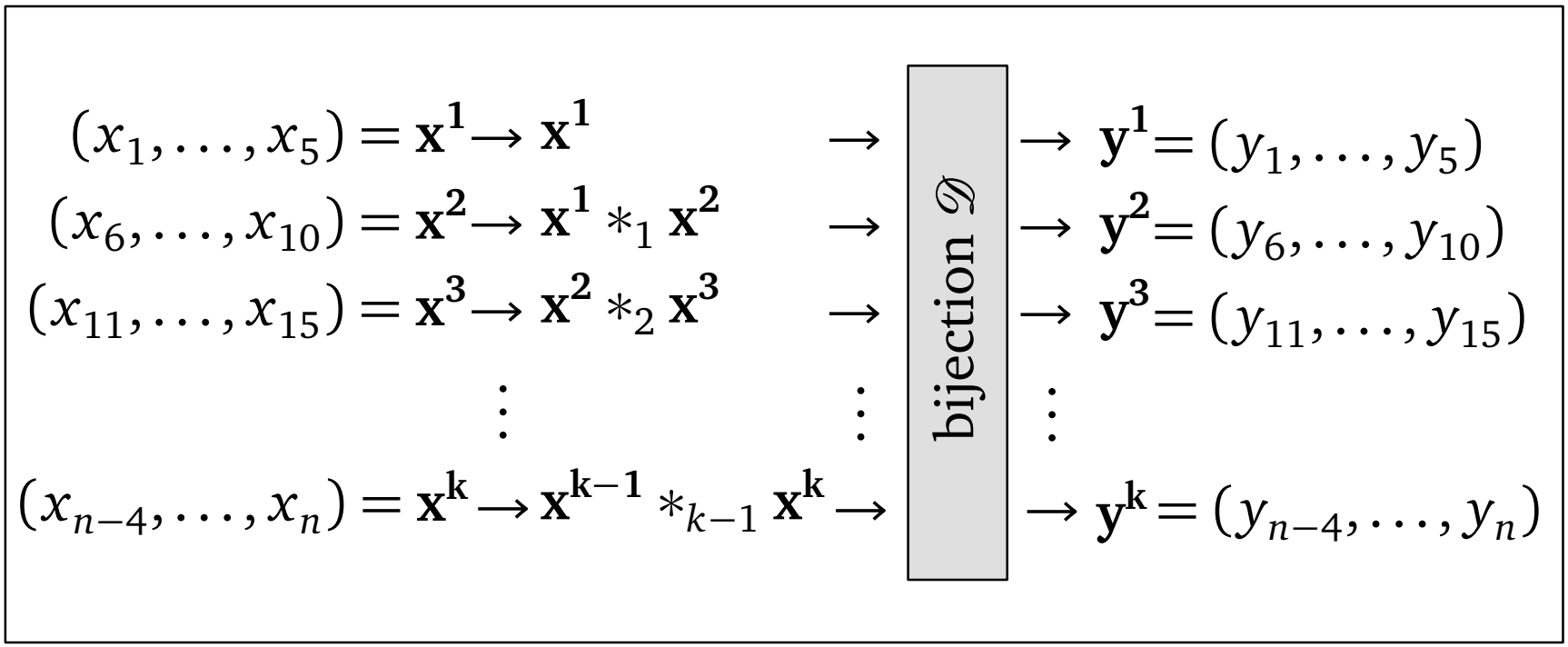
Construction of the map $\mathscr{P}$

$$
\begin{aligned}
(x_1, \ldots, x_5) &= \mathbf{x^1} \rightarrow \mathbf{x^1} \\
(x_6, \ldots, x_{10}) &= \mathbf{x^2} \rightarrow \mathbf{x^1} *_1 \mathbf{x^2} \\
(x_{11}, \ldots, x_{15}) &= \mathbf{x^3} \rightarrow \mathbf{x^2} *_2 \mathbf{x^3} \\
&\vdots \\
(x_{n-4}, \ldots, x_n) &= \mathbf{x^k} \rightarrow \mathbf{x^{k-1}} *_{k-1} \mathbf{x^k}
\end{aligned}
$$

Construction of the map $\mathscr{P}$



Construction of the map $\mathscr{P}$

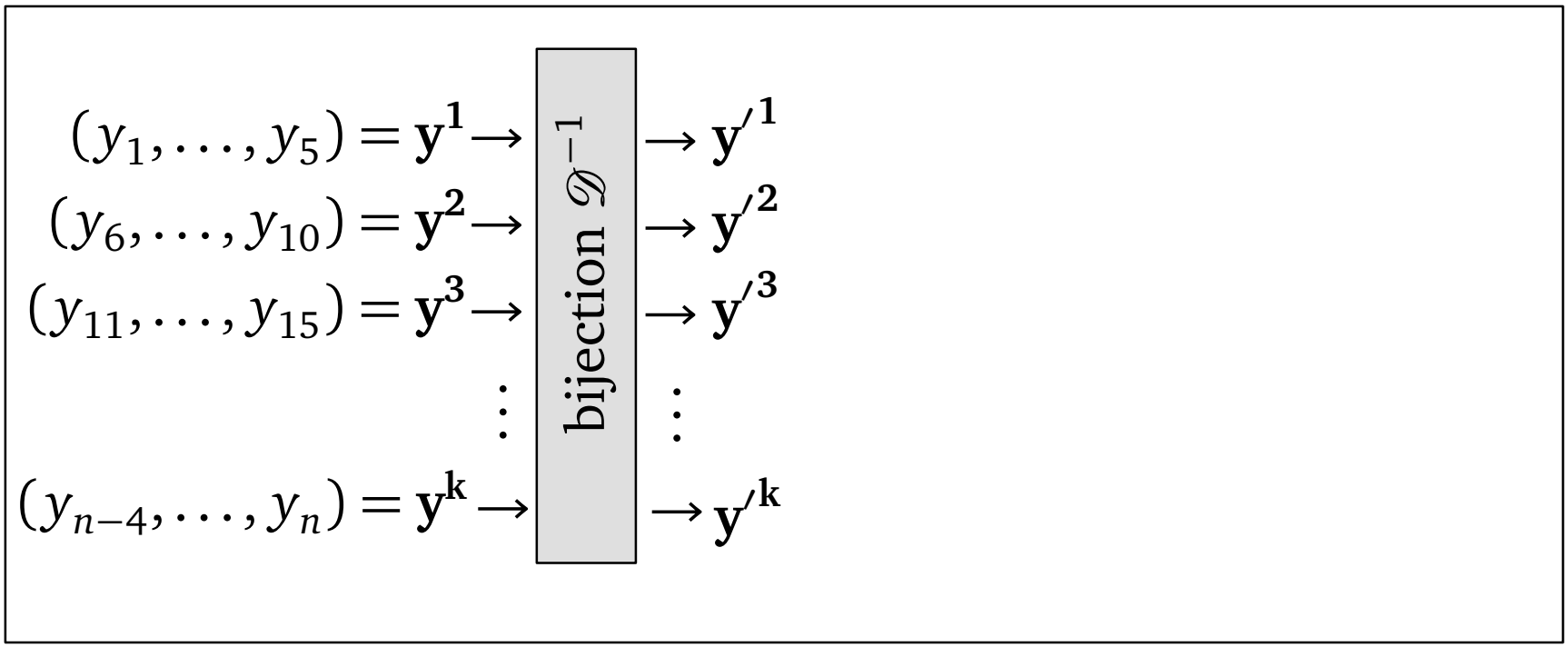


Inverting the map $\mathscr{P}$

$$(y_1, \ldots, y_5) = \mathbf{y^1}$$
$$(y_6, \ldots, y_{10}) = \mathbf{y^2}$$
$$(y_{11}, \ldots, y_{15}) = \mathbf{y^3}$$

$$(y_{n-4}, \ldots, y_n) = \mathbf{y^k}$$

Inverting the map $\mathscr{P}$



Inverting the map $\mathscr{P}$

$$
\begin{array}{rcl}
(y_1,\ldots,y_5)=\mathbf{y^1}\rightarrow & \text{bijection } \mathscr{D}^{-1} & \rightarrow \mathbf{y'^1}\rightarrow \mathbf{y'^1} = \mathbf{x^1} = (x_1,\ldots,x_5) \\
(y_6,\ldots,y_{10})=\mathbf{y^2}\rightarrow & & \rightarrow \mathbf{y'^2}\rightarrow \mathbf{x^1}\backslash_1\mathbf{y'^2} = \mathbf{x^2} = (x_6,\ldots,x_{10}) \\
(y_{11},\ldots,y_{15})=\mathbf{y^3}\rightarrow & & \rightarrow \mathbf{y'^3}\rightarrow \mathbf{x^2}\backslash_2\mathbf{y'^3} = \mathbf{x^3} = (x_{11},\ldots,x_{15}) \\
\vdots & \vdots & \vdots \quad \vdots \\
(y_{n-4},\ldots,y_n)=\mathbf{y^k}\rightarrow & & \rightarrow \mathbf{y'^k}\rightarrow \mathbf{x^{k-1}}\backslash_{k-1}\mathbf{y'^k} = (x_{n-4},\ldots,x_n)
\end{array}
$$

Properties of Gligoroski MQ-scheme

- Size of the keys (in KBytes):

n	Public key	Private key
140	168.7	9.8
160	251.6	11.3
200	490.8	14.8

Properties of Gligoroski MQ-scheme

- Size of the keys (in KBytes):

n	Public key	Private key
140	168.7	9.8
160	251.6	11.3
200	490.8	14.8

- Speed comparison (in 1000 cycles):

Algorithm	Sign	Verify
DSA 1024-bit	1041	1246
ECC 1024-bit	2147	4220
RSA 1024-bit	2939	99
MQQ 160-bit	10	140

Cryptanalysis of MQQ

- **M.S.E. Mohamed et al.**: Algebraic Cryptanalysis of MQQ Public Key Cryptosystem by MutantXL

Cryptanalysis of MQQ

- **M.S.E. Mohamed et al.**: Algebraic Cryptanalysis of MQQ Public Key Cryptosystem by MutantXL
- Possible improvement/modifications:

Cryptanalysis of MQQ

- **M.S.E. Mohamed et al.**: Algebraic Cryptanalysis of MQQ Public Key Cryptosystem by MutantXL
- Possible improvement/modifications:
  - Generate more complex quadratic quasigroups.

Cryptanalysis of MQQ

- **M.S.E. Mohamed et al.**: Algebraic Cryptanalysis of MQQ Public Key Cryptosystem by MutantXL
- Possible improvement/modifications:
  - Generate more complex quadratic quasigroups.
  - Use just left quadratic quasigroups.

Cryptanalysis of MQQ

- **M.S.E. Mohamed et al.**: Algebraic Cryptanalysis of MQQ Public Key Cryptosystem by MutantXL
- Possible improvement/modifications:
  - Generate more complex quadratic quasigroups.
  - Use just left quadratic quasigroups.
  - Exclude some polynomials to make MQQ non-injective. Can be still used for signing.

Decomposition of quadratic quasigroup

Let $(\mathbb{F}_2^n, *)$ be a quadratic quasigroup and $(f_1, \ldots, f_n)$ its representation.

$$f_1 = \sum_{k,l=1}^{n} a_{k,l}^1 \, x_k x_l + \sum_{k,l=1}^{n} m_{k,l}^1 \, x_k y_l + \sum_{k,l=1}^{n} b_{k,l}^1 \, y_k y_l + c^1$$

$$f_2 = \sum_{k,l=1}^{n} a_{k,l}^2 \, x_k x_l + \sum_{k,l=1}^{n} m_{k,l}^2 \, x_k y_l + \sum_{k,l=1}^{n} b_{k,l}^2 \, y_k y_l + c^2$$

$$\vdots$$

$$f_n = \sum_{k,l=1}^{n} a_{k,l}^n \, x_k x_l + \sum_{k,l=1}^{n} m_{k,l}^n \, x_k y_l + \sum_{k,l=1}^{n} b_{k,l}^n \, y_k y_l + c^n$$

Decomposition of quadratic quasigroup

Let $(\mathbb{F}_2^n, *)$ be a quadratic quasigroup and $(f_1, \ldots, f_n)$ its representation. Put $\mathbf{x} = (x_1, \ldots, x_n)$ a $\mathbf{y} = (y_1, \ldots, y_n)$.

$$
\begin{aligned}
f_1 &= \sum_{k,l=1}^{n} a_{k,l}^1 \, x_k x_l + \sum_{k,l=1}^{n} m_{k,l}^1 \, x_k y_l + \sum_{k,l=1}^{n} b_{k,l}^1 \, y_k y_l + c^1 \\
f_2 &= \sum_{k,l=1}^{n} a_{k,l}^2 \, x_k x_l + \sum_{k,l=1}^{n} m_{k,l}^2 \, x_k y_l + \sum_{k,l=1}^{n} b_{k,l}^2 \, y_k y_l + c^2 \\
&\vdots \\
f_n &= \sum_{k,l=1}^{n} a_{k,l}^n \, x_k x_l + \sum_{k,l=1}^{n} m_{k,l}^n \, x_k y_l + \sum_{k,l=1}^{n} b_{k,l}^n \, y_k y_l + c^n \\
&\quad \alpha(\mathbf{x}) \qquad \gamma(\mathbf{x}, \mathbf{y}) \qquad \beta(\mathbf{y}) \qquad \mathbf{c}
\end{aligned}
$$

Decomposition of quadratic quasigroup

Let $(\mathbb{F}_2^n, *)$ be a quadratic quasigroup and $(f_1, \ldots, f_n)$ its representation. Put $\mathbf{x} = (x_1, \ldots, x_n)$ a $\mathbf{y} = (y_1, \ldots, y_n)$.

$$
\begin{aligned}
f_1 &= \sum_{k,l=1}^{n} a_{k,l}^1 \, x_k x_l + \sum_{k,l=1}^{n} m_{k,l}^1 \, x_k y_l + \sum_{k,l=1}^{n} b_{k,l}^1 \, y_k y_l + c^1 \\
f_2 &= \sum_{k,l=1}^{n} a_{k,l}^2 \, x_k x_l + \sum_{k,l=1}^{n} m_{k,l}^2 \, x_k y_l + \sum_{k,l=1}^{n} b_{k,l}^2 \, y_k y_l + c^2 \\
&\vdots \\
f_n &= \sum_{k,l=1}^{n} a_{k,l}^n \, x_k x_l + \sum_{k,l=1}^{n} m_{k,l}^n \, x_k y_l + \sum_{k,l=1}^{n} b_{k,l}^n \, y_k y_l + c^n
\end{aligned}
$$

$$
\mathbf{x} * \mathbf{y} = \alpha(\mathbf{x}) + \gamma(\mathbf{x}, \mathbf{y}) + \beta(\mathbf{y}) + \mathbf{c}
$$

Decomposition of quadratic quasigroup

- γ is a *bilinear map* $\mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ represented by bilinear forms.

Decomposition of quadratic quasigroup

- γ is a *bilinear map* $\mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ represented by bilinear forms.
- Denote $\mathbf{o} = (0, 0, \ldots, 0)$. Then

$$R_{\mathbf{o}}(\mathbf{x}) = \mathbf{x} * \mathbf{o} = \alpha(\mathbf{x}) + \mathbf{c}, \quad \text{a} \quad L_{\mathbf{o}}(\mathbf{x}) = \mathbf{o} * \mathbf{y} = \beta(\mathbf{y}) + \mathbf{c}.$$

Decomposition of quadratic quasigroup

- γ is a *bilinear map* $\mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ represented by bilinear forms.
- Denote $\mathbf{o} = (0, 0, \ldots, 0)$. Then

$$R_{\mathbf{o}}(\mathbf{x}) = \mathbf{x} * \mathbf{o} = \alpha(\mathbf{x}) + \mathbf{c}, \quad \text{a} \quad L_{\mathbf{o}}(\mathbf{x}) = \mathbf{o} * \mathbf{y} = \beta(\mathbf{y}) + \mathbf{c}.$$

- α and β are bijective maps - *quadratic permutations*.

Decomposition of quadratic quasigroup

Theorem

For every quadratic quasigroup $(\mathbb{F}_2^n, *)$ there exist uniquely determined quadratic permutations α, β, a bilinear map γ and a vector $\mathbf{c}$, such that

$$\mathbf{x} * \mathbf{y} = \alpha(\mathbf{x}) + \gamma(\mathbf{x}, \mathbf{y}) + \beta(\mathbf{y}) + \mathbf{c},$$

for every $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$.

Decomposition of quadratic quasigroup

Let $(\mathbb{F}_2^n, *)$ be a quadratic quasigroup and $(f_1, \ldots, f_n)$ its representation. Put $\mathbf{x} = (x_1, \ldots, x_n)$ a $\mathbf{y} = (y_1, \ldots, y_n)$.

$$
\begin{aligned}
f_1 &= \sum_{k,l=1}^{n} a_{k,l}^1 \, x_k x_l + \sum_{k,l=1}^{n} m_{k,l}^1 \, x_k y_l + \sum_{k,l=1}^{n} b_{k,l}^1 \, y_k y_l + c^1 \\
f_2 &= \sum_{k,l=1}^{n} a_{k,l}^2 \, x_k x_l + \sum_{k,l=1}^{n} m_{k,l}^2 \, x_k y_l + \sum_{k,l=1}^{n} b_{k,l}^2 \, y_k y_l + c^2 \\
&\vdots \\
f_n &= \sum_{k,l=1}^{n} a_{k,l}^n \, x_k x_l + \sum_{k,l=1}^{n} m_{k,l}^n \, x_k y_l + \sum_{k,l=1}^{n} b_{k,l}^n \, y_k y_l + c^n
\end{aligned}
$$

$$
\mathbf{x} * \mathbf{y} = \alpha(\mathbf{x}) + \gamma(\mathbf{x}, \mathbf{y}) + \beta(\mathbf{y}) + \mathbf{c}
$$

Quadratic loop

- How do they look like?

Quadratic loop

Corollary

- Suppose that $(\mathbb{F}_2^n, *)$ is a quadratic loop with a unit $\mathbf{o}$.
- Then for every $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$

$$\mathbf{x} * \mathbf{y} = \mathbf{x} + \gamma(\mathbf{x}, \mathbf{y}) + \mathbf{y}.$$

- Such a loop is uniquely determined by the bilinear map γ.

Quadratic loop

Corollary

- Suppose that $(\mathbb{F}_2^n, *)$ is a quadratic loop with a unit $\mathbf{o}$.
- Then for every $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$

$$\mathbf{x} * \mathbf{y} = \mathbf{x} + \gamma(\mathbf{x}, \mathbf{y}) + \mathbf{y}.$$

- Such a loop is uniquely determined by the bilinear map γ.

- It is easy to generate γ for a small n.

Quadratic loops of order 8

- I generated all quadratic loops of order 8.
- The number of these loops is 4384.
- 13 main classes.
- Contains all groups except the cyclic one.