On a class of left MQQs with degree invariant to parastrophy

Simona Samardjiska (joint work with Danilo Gligoroski)

Department of Telematics, NTNU, Norway
simonas@item.ntnu.no,danilog@item.ntnu.no

Norsk Kryptoseminar 2011 - Nov 9-10 Bergen

Introduction - Left Quasigroups

(Q, q) - a groupoid, a - fixed element of Q.
(Q, q) is called **left quasigroup** if the mapping $L_a : Q \to Q$

$$L_a x = q(a, x),$$

is a bijection for every $a \in Q$.

If Q is finite, $|Q|$ - **order** of (Q, q).

NTNU
Norwegian University of
Science and Technology

Introduction - Left Quasigroups

Parastrophe operation "$q_\backslash$": $q_\backslash(x,y)=z \Leftrightarrow q(x,z)=y$, defines a left quasigroup $(Q,q_\backslash)$.

Important identities:

$$q(x,q_\backslash(x,y))=y, \quad q_\backslash(x,q(x,y))=y,$$

(Q,q_1) and (Q,q_2) are **isotopic**,
if there exist bijections $\alpha,\beta,\gamma: Q\to Q$, s.t.

$$(\forall a,b\in Q) \quad \gamma(q_1(a,b))=q_2(\alpha(a),\beta(b)).$$

The isotopy is (α,β,γ).

NTNU
Norwegian University of
Science and Technology

Introduction - Left Quasigroups

Parastrophe operation "$q_\backslash$": $q_\backslash(x, y) = z \Leftrightarrow q(x, z) = y$, defines a left quasigroup $(Q, q_\backslash)$.

Important identities:

$$q(x, q_\backslash(x, y)) = y, \quad q_\backslash(x, q(x, y)) = y,$$

(Q, q_1) and (Q, q_2) are **isotopic**, if there exist bijections $\alpha, \beta, \gamma : Q \to Q$, s.t.

$$(\forall a, b \in Q) \quad \gamma(q_1(a, b)) = q_2(\alpha(a), \beta(b)).$$

The isotopy is (α, β, γ).

NTNU
Norwegian University of
Science and Technology

Introduction - Left Multivariate Quasigroups

Every left quasigroup (Q, q) of order 2^n:

$$\begin{aligned} & q(x,y) = z \Longleftrightarrow \\ & q(x_1,\ldots,x_n,y_1,\ldots,y_n) = \\ = \quad & (q^{(1)}(x_1,\ldots,x_n,y_1,\ldots,y_n),\ldots,q^{(n)}(x_1,\ldots,x_n,y_1,\ldots,y_n)). \end{aligned}$$

Each of the $q^{(s)}$ has a unique ANF form over $GF(2)$.

$$q^{(s)}(x_1,...,x_n,y_1,...,y_n) = \bigoplus_{\substack{j=(j_1,...,j_n)\in\mathbb{Z}_2^n \\ k=(k_1,...,k_n)\in\mathbb{Z}_2^n}} a_{jk} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n} y_1^{k_1} \cdots y_n^{k_n},$$

where $a_{jk} \in \mathbb{Z}_2$, x^0 is an empty string and $x^1 = x$.

NTNU
Norwegian University of
Science and Technology

Introduction - Left MQQs

If all $q^{(s)}$ are of degree 2 -

Left Multivariate Quadratic Quasigroups (MQQ)

- Suitable for symbolic computation
- Can be used in Multivariate Public Key cryptosystems

- Algorithms for construction
  - Gligoroski et al. (2008) - introduction of MQQ
  - Christov (2009) - characterization and algorithm for quadratic loops
  - Samardjiska et al. (2010) - characterization and algorithms for T-Multivariate Quasigroups and permutations of any degree
  - Chen et al. (2010)- algorithm for bilinear quadratic quasigroups

NTNU
Norwegian University of Science and Technology

Introduction - Left MQQs

If all $q^{(s)}$ are of degree 2 -

Left Multivariate Quadratic Quasigroups (MQQ)

- Suitable for symbolic computation
- Can be used in Multivariate Public Key cryptosystems

- Algorithms for construction
  - Gligoroski et al. (2008) - introduction of MQQ
  - Christov (2009) - characterization and algorithm for quadratic loops
  - Samardjiska et al. (2010) - characterization and algorithms for T-Multivariate Quasigroups and permutations of any degree
  - Chen et al. (2010)- algorithm for bilinear quadratic quasigroups

NTNU
Norwegian University of
Science and Technology

Introduction - Left MQQs

If all $q^{(s)}$ are of degree 2 -

Left Multivariate Quadratic Quasigroups (MQQ)

- Suitable for symbolic computation
- Can be used in Multivariate Public Key cryptosystems

- Algorithms for construction
  - Gligoroski et al. (2008) - introduction of MQQ
  - Christov (2009) - characterization and algorithm for quadratic loops
  - Samardjiska et al. (2010) - characterization and algorithms for T-Multivariate Quasigroups and permutations of any degree
  - Chen et al. (2010)- algorithm for bilinear quadratic quasigroups

NTNU
Norwegian University of
Science and Technology

Multivariate Public Key cryptosystems using MQQs

Typical scenario:

- Encryption: the (left) quasigroup q
- Decryption: the parastrophe $q_\backslash$:

$$q_\backslash(x, y) = z \Leftrightarrow q(x, z) = y.$$

Important:

- In the decryption process: The parastrophes are not in their ANF form
- Why? In general, time and space consuming!
  - Time: Can be difficult to find the ANF of the parastrophe
  - Space: Can have any degree and **exponentially** many terms

Multivariate Public Key cryptosystems using MQQs

Typical scenario:

- Encryption: the (left) quasigroup q
- Decryption: the parastrophe $q_\backslash$:

$$q_\backslash(x, y) = z \Leftrightarrow q(x, z) = y.$$

Important:

- In the decryption process: The parastrophes are not in their ANF form
- Why? In general, time and space consuming!
  - Time: Can be difficult to find the ANF of the parastrophe
  - Space: Can have any degree and **exponentially** many terms

NTNU
Norwegian University of
Science and Technology

Multivariate Public Key cryptosystems using MQQs

So, is this a problem?

- MQQ-sig: bilinear quasigroups of order 2^8
- MQQ-enc: left quasigroups of order 2^8

Crucial: The decryption can be made by

- Using lookup tables - **the Caley table of the quasigroup (i.e. the parastrophe)**
- Solving small systems of multivariate quadratic equations

NTNU
Norwegian University of
Science and Technology

Multivariate Public Key cryptosystems using MQQs

So, is this a problem?

- MQQ-sig: bilinear quasigroups of order 2^8
- MQQ-enc: left quasigroups of order 2^8

Crucial: The decryption can be made by

- Using lookup tables - **the Caley table of the quasigroup (i.e. the parastrophe)**
- Solving small systems of multivariate quadratic equations

NTNU
Norwegian University of
Science and Technology

But... what about other types of public key encryption like

Identity based encryption (IBE)?

Why IBE?

1. **The possibilities of IBE are enormous:**
   - No need for public key certificates - **public key = identity of its owner**
   - Revocation of public keys
   - Delegation of decryption keys
   - Generalization to more powerful HIBE, ABE, Functional encryption

NTNU
Norwegian University of
Science and Technology

But... what about other types of public key encryption like

Identity based encryption (IBE)?

Why IBE?

1. **The possibilities of IBE are enormous:**
   - No need for public key certificates -
     public key = identity of its owner
   - Revocation of public keys
   - Delegation of decryption keys
   - Generalization to more powerful HIBE, ABE, Functional encryption

NTNU
Norwegian University of
Science and Technology

But... what about other types of public key encryption like

Identity based encryption (IBE)?

Why IBE?

1. **The possibilities of IBE are enormous:**
   - No need for public key certificates -
     public key = identity of its owner
   - Revocation of public keys
   - Delegation of decryption keys
   - Generalization to more powerful HIBE, ABE, Functional encryption

NTNU
Norwegian University of
Science and Technology

Can we use quasigroups to create a Multivariate IBE scheme?

Why is that important?

2. So far only Boneh-Franklin and Boneh-Boyen schemes are practical!
   - based on computational and decisional bilinear Diffie-Hellman problem

3. **A multivariate IBE has not been proposed so far!**

NTNU
Norwegian University of
Science and Technology

Can we use quasigroups to create a Multivariate IBE scheme?

Why is that important?

2. So far only Boneh-Franklin and Boneh-Boyen schemes are practical!

- based on computational and decisional bilinear Diffie-Hellman problem

3. **A multivariate IBE has not been proposed so far!**

NTNU
Norwegian University of
Science and Technology

Can we use quasigroups to create a Multivariate IBE scheme?

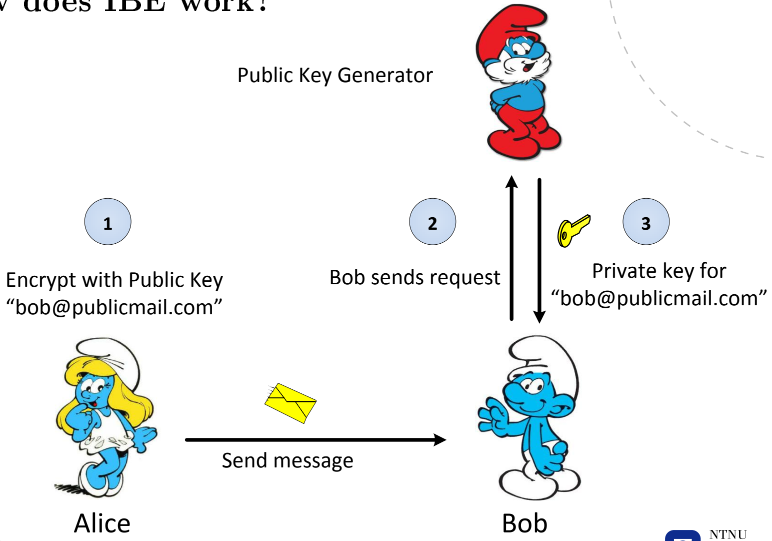
Why is that important?

2. So far only Boneh-Franklin and Boneh-Boyen schemes are practical!
   - based on computational and decisional bilinear Diffie-Hellman problem

3. **A multivariate IBE has not been proposed so far!**

NTNU
Norwegian University of
Science and Technology

How does IBE work?



Public Key Generator

1

Encrypt with Public Key
“bob@publicmail.com”

2

Bob sends request

3

Private key for
“bob@publicmail.com”

Send message

Alice

Bob

Motivation

- The private key s (for decryption) for user ID should have **explicit multivariate form!**
- The quasigroups used can be **of orders as big as** 2^{64}, 2^{128}, 2^{256}!

Natural first step:

To find a class of left MQQs such that:

- The left parastrophe can be easily represented
- The left parastrophe is also a left MQQ, i.e. is of degree 2

NTNU
Norwegian University of
Science and Technology

Motivation

- The private key s (for decryption) for user ID should have **explicit multivariate form!**
- The quasigroups used can be **of orders as big as** 2^{64}, 2^{128}, 2^{256}!

Natural first step:

To find a class of left MQQs such that:

- The left parastrophe can be easily represented
- The left parastrophe is also a left MQQ, i.e. is of degree 2

NTNU
Norwegian University of
Science and Technology

Construction of left quasigroups (SS 2010)

$x_1, \ldots, x_n, y_1, \ldots, y_n$ Boolean variables, $w > 1$.
$\mathbf{D_1}$, $\mathbf{D_2}$, $\mathbf{D}$ - nonsingular Bool. matrices, $\mathbf{c}$, $\mathbf{c_1}$, $\mathbf{c_2}$, $\mathbf{c_3}$, - Bool. vectors.
$\mathbf{A}$ and $\mathbf{B}$ - nonsingular upper triangular matrices of random affine Boolean expressions, such that:

- $\forall i = 1, \ldots, n$, $f_{ii} = 1$ and $g_{ii} = 1$, and
- $\forall i, j$, $i < j \leq n$, f_{ij} and g_{ij} depend only on $x_1, \ldots, x_n$, $y_{i+1}, \ldots, y_n$.

Then

$$\begin{aligned} &q(x_1, \ldots, x_n, y_1, \ldots, y_n) = \mathbf{A} \cdot (x_1, \ldots, x_n) + \mathbf{B} \cdot (y_1, \ldots, y_n) + \mathbf{c} \\ &q_1(x_1, \ldots, x_n, y_1, \ldots, y_n) = \\ &\qquad = \mathbf{D}(q(\mathbf{D}_1(x_1, \ldots, x_n) + \mathbf{c}_1, \mathbf{D}_2(y_1, \ldots, y_n) + \mathbf{c}_2)) + \mathbf{c}_3 \end{aligned}$$

define left MQQs (Q, q) and (Q, q_1) of order 2^n, $Q = \mathbb{Z}_2^n$.

NTNU
Norwegian University of
Science and Technology

The first modification

$$q(\mathbf{x},\mathbf{y}) = \mathbf{A}(\mathbf{x},\mathbf{y})\cdot\mathbf{x} + \mathbf{B}(\mathbf{x},\mathbf{y})\cdot\mathbf{y} + \mathbf{c} \qquad (SS2010)$$

$$\Downarrow \qquad \Downarrow \qquad \Downarrow$$

$$q(\mathbf{x},\mathbf{y}) = \mathbf{A}(\mathbf{x}) + \mathbf{B}(\mathbf{x})\cdot\mathbf{y} + \mathbf{c}$$

$\mathbf{A}(\mathbf{x})$ - vector of random quadratic Boolean expressions
$\mathbf{B}(\mathbf{x})$ - nonsingular upper triangular matrix, such that:

- $\forall i = 1,\ldots,n$, $b_{ii}(\mathbf{x}) = 1$, and
- $\forall i, j$, $i < j \le n$, $b_{ij}(\mathbf{x})$ random affine Boolean expressions of $x_1,\ldots,x_n$.

The parastrophe is

$$q_{\backslash}(\mathbf{x},\mathbf{y}) = \mathbf{B}^{-1}(\mathbf{x})\cdot\mathbf{y} + \mathbf{B}^{-1}(\mathbf{x})\cdot\mathbf{A}(\mathbf{x}) + \mathbf{B}^{-1}(\mathbf{x})\cdot\mathbf{c}$$

When is $q_\backslash(\mathbf{x}, \mathbf{y})$ quadratic?

$$q_\backslash(\mathbf{x}, \mathbf{y}) = \mathbf{B}^{-1}(\mathbf{x}) \cdot \mathbf{y} + \mathbf{B}^{-1}(\mathbf{x}) \cdot \mathbf{A}(\mathbf{x}) + \mathbf{B}^{-1}(\mathbf{x}) \cdot \mathbf{c}$$

$$\Downarrow \quad \Downarrow \quad \Downarrow$$

Iff

- $\mathbf{B}^{-1}(\mathbf{x})$ has elements - affine expressions, and
- $deg(\mathbf{B}^{-1}(\mathbf{x}) \cdot \mathbf{A}(\mathbf{x})) = 2.$

NTNU
Norwegian University of
Science and Technology

When are the elements of $\mathbf{B}^{-1}(\mathbf{x})$ affine expressions?

Iff

$\forall i, j,\ i \leq j \leq n$

$$\sum_{k=i}^{j} (\mathbf{x}^T B_{ik} \mathsf{B}_{kj}^T \mathbf{x} + \mathbf{x}^T B_{ik} \beta_{kj} + b_{ik} \mathsf{B}_{kj}^T \mathbf{x} + b_{ik} \beta_{kj}) = 0$$

where

- $\mathbf{B}(\mathbf{x}) : b_{ij}(\mathbf{x}) = \mathbf{x}^T \cdot B_{ij} + b_{ij}$, and B_{ij}, $\mathbf{x}$ column vectors,
- $\mathbf{B}^{-1}(\mathbf{x}) : \beta_{ij}(\mathbf{x}) = \mathbf{x}^T \cdot \mathsf{B}_{ij} + \beta_{ij}$, and B_{ij} column vector,

Construction

- expanded form, and
- backtracking algorithm,

NTNU
Norwegian University of
Science and Technology

When are the elements of $\mathbf{B}^{-1}(\mathbf{x})$ affine expressions?

Iff

$\forall i, j,\ i \leq j \leq n$

$$\sum_{k=i}^{j} (\mathbf{x}^T B_{ik} \mathsf{B}_{kj}^T \mathbf{x} + \mathbf{x}^T B_{ik} \beta_{kj} + b_{ik} \mathsf{B}_{kj}^T \mathbf{x} + b_{ik} \beta_{kj}) = 0$$

where

- $\mathbf{B}(\mathbf{x}) : b_{ij}(\mathbf{x}) = \mathbf{x}^T \cdot B_{ij} + b_{ij}$, and B_{ij}, $\mathbf{x}$ column vectors,
- $\mathbf{B}^{-1}(\mathbf{x}) : \beta_{ij}(\mathbf{x}) = \mathbf{x}^T \cdot \mathsf{B}_{ij} + \beta_{ij}$, and B_{ij} column vector,

Construction

- expanded form, and
- backtracking algorithm,

When are the elements of $\mathbf{B}^{-1}(\mathbf{x})$ affine expressions?

Iff

$\forall i, j,\ i \leq j \leq n$

$$\sum_{k=i}^{j} (\mathbf{x}^T B_{ik} \mathsf{B}_{kj}^T \mathbf{x} + \mathbf{x}^T B_{ik} \beta_{kj} + b_{ik} \mathsf{B}_{kj}^T \mathbf{x} + b_{ik} \beta_{kj}) = 0$$

where

- $\mathbf{B}(\mathbf{x}) : b_{ij}(\mathbf{x}) = \mathbf{x}^T \cdot B_{ij} + b_{ij}$, and B_{ij}, $\mathbf{x}$ column vectors,
- $\mathbf{B}^{-1}(\mathbf{x}) : \beta_{ij}(\mathbf{x}) = \mathbf{x}^T \cdot \mathsf{B}_{ij} + \beta_{ij}$, and B_{ij} column vector,

Construction

- expanded form, and
- backtracking algorithm,

Sufficient conditions

If $\forall i, j,\ i \leq j \leq n$

1. $\displaystyle\sum_{k=i}^{j} B_{ik}\mathsf{B}_{kj}^{T} = \mathbf{0}$
2. $\displaystyle\sum_{k=i}^{j} B_{ik}\beta_{kj} + b_{ik}\mathsf{B}_{kj}^{T} = \mathbf{0}$
3. $\displaystyle\sum_{k=i}^{j} b_{ik}\beta_{kj} = \mathbf{0}$

then the elements of $\mathbf{B}^{-1}(\mathbf{x})$ are affine expressions.

Still not good enough for construction!

NTNU
Norwegian University of
Science and Technology

Sufficient conditions

If $\forall i, j,\ i \leq j \leq n$

1. $$\sum_{k=i}^{j} B_{ik}\mathsf{B}_{kj}^{T} = \mathbf{0}$$
2. $$\sum_{k=i}^{j} B_{ik}\beta_{kj} + b_{ik}\mathsf{B}_{kj}^{T} = \mathbf{0}$$
3. $$\sum_{k=i}^{j} b_{ik}\beta_{kj} = \mathbf{0}$$

then the elements of $\mathbf{B}^{-1}(\mathbf{x})$ are affine expressions.

Still not good enough for construction!

NTNU
Norwegian University of
Science and Technology

Lemma

If $\forall i, j,\ i \leq j \leq n$

1. $$\beta_{ij} = b_{ij} + \sum_{m=1}^{j-i} \sum_{i<r_1<\cdots<r_m<j} b_{ir_1} b_{r_1 r_2} \ldots b_{r_m j}$$
2. $$\mathsf{B}_{ij} = B_{ij} + \sum_{m=1}^{j-i} \sum_{\substack{i < r_1 < \cdots < r_m < j \\ t \in \{1,\ldots,m\}}} b_{ir_1} \ldots B_{r_t r_{t+1}} \ldots b_{r_m j}$$
3. $$\sum_{m=1}^{j-i} \sum_{i<r_1<\cdots<r_m<j} B_{ir_1} b_{r_1 r_2} \ldots b_{r_{m-1} r_m} B^T_{r_m j} = \mathbf{0}$$

then the elements of $\mathbf{B}^{-1}(\mathbf{x})$ are affine expressions.

Theorem for construction

Let $q(\mathbf{x},\mathbf{y}) = \mathbf{A}(\mathbf{x}) + \mathbf{B}(\mathbf{x}) \cdot \mathbf{y} + \mathbf{c}$ where

- $\mathbf{B}(\mathbf{x}) : b_{ij}(\mathbf{x}) = \mathbf{x}^T \cdot B_{ij} + b_{ij}$, where B_{ij}, $\mathbf{x}$ column vectors,
- $\mathbf{A}(\mathbf{x}) : a_i(\mathbf{x})$ Boolean expressions.

If

- $B_{2k_1+1,2k_2} \neq \mathbf{0}$, $B_{2k_1+1,2k_2+1} = \mathbf{0}$, $B_{2k_1,2k_2+1} = \mathbf{0}$, $B_{2k_1,2k_2} = \mathbf{0}$,
- $b_{2k_1+1,2k_2} \neq 0$, $b_{2k_1+1,2k_2+1} \neq 0$, $b_{2k_1,2k_2} \neq 0$, $b_{2k_1,2k_2+1} = 0$,
- $a_{2k}(\mathbf{x})$ is affine and $a_{2k+1}(\mathbf{x})$ is quadratic,

Then q is a left MQQ with degree invariant to the parastrophe $\backslash$.

NTNU
Norwegian University of
Science and Technology

Example

Let $\mathbf{A}(\mathbf{x})$ be a vector of dimension 4 and let $\mathbf{B}(\mathbf{x})$ be 4×4 matrix given by

$$\mathbf{A}(\mathbf{x}) = \begin{bmatrix} 1 + x_3 + x_1x_3 + x_2x_3 + x_4 \\ 1 + x_4 \\ 1 + x_2 + x_4 + x_3x_4 \\ 1 + x_1 + x_4 \end{bmatrix},$$

$$\mathbf{B}(\mathbf{x}) = \begin{bmatrix} 1 & x_1 + x_2 + x_3 & 1 & 1 + x_1 + x_3 + x_4 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & x_1 + x_2 + x_4 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

and let

$$q(\mathbf{x}, \mathbf{y}) = \mathbf{D}(\mathbf{A}(\mathbf{D_1} \cdot \mathbf{x} + \mathbf{c_1}) + \mathbf{B}(\mathbf{D_1} \cdot \mathbf{x} + \mathbf{c_1}) \cdot \mathbf{D_2} \cdot \mathbf{y} + \mathbf{c_2} + \mathbf{c}) + \mathbf{c_3}.$$

NTNU
Norwegian University of
Science and Technology

Example

$$q(x_1,\dots,x_4,y_1,\dots,y_4) =$$

$$= \begin{bmatrix} 1+x_1+x_2+x_1x_2+x_3+x_1x_3+x_2x_3+x_4+x_1x_4+x_2x_4+y_1+ \\ +x_1y_1+x_4y_1+y_2+x_1y_2+x_2y_2+x_4y_2+x_1y_3+x_4y_3+x_2y_4 \\ 1+x_1x_2+x_3+x_1x_3+x_1x_4+x_2x_4+x_3x_4+y_1+x_1y_1+ \\ +x_4y_1+x_4y_2+x_1y_3+x_4y_3+x_1y_4 \\ x_1x_2+x_1x_3+x_1x_4+x_2x_4+x_3x_4+x_1y_1+x_4y_1+y_2+ \\ +x_4y_2+y_3+x_1y_3+x_4y_3+x_1y_4 \\ 1+x_1+x_3+x_2x_3+x_4+x_3x_4+x_1y_2+x_2y_2+y_4+x_1y_4+x_2y_4 \end{bmatrix}$$

is a Left MQQ of order 2^4.

NTNU
Norwegian University of
Science and Technology

Example

$$q_{\backslash}(x_1,\dots,x_4,y_1,\dots,y_4) =$$

$$= \begin{bmatrix} x_2 + x_1x_3 + x_1x_4 + x_2x_4 + y_1 + x_1y_1 + y_2 + x_4y_2 + y_3 + x_4y_4 \\ x_1 + x_1x_2 + x_3 + x_4 + x_1x_4 + x_2x_4 + x_3x_4 + y_1 + x_2y_1 + x_1y_2 + \\ + x_2y_2 + x_4y_2 + y_4 + x_1y_4 + x_2y_4 + x_4y_4 \\ 1 + x_1 + x_1x_2 + x_1x_3 + x_4 + x_3x_4 + y_1 + x_1y_1 + x_2y_1 + x_1y_2 + \\ + x_2y_2 + y_3 + x_1y_4 + x_2y_4 \\ 1 + x_1 + x_2 + x_1x_2 + x_3 + x_4 + x_1x_4 + x_2x_4 + x_3x_4 + x_2y_1 + x_1y_2 + \\ + x_2y_2 + x_4y_2 + y_4 + x_1y_4 + x_2y_4 + x_4y_4 \end{bmatrix}$$

is again a Left MQQ of order 2^4.

NTNU
Norwegian University of
Science and Technology

Thank you for your attention!

NTNU
Norwegian University of
Science and Technology