

# M4GB: An Efficient Gröbner Basis Algorithm

Rusydi H. Makarim<sup>1,2</sup>    Marc Stevens<sup>2</sup>

<sup>1</sup>Mathematics Institute, University Leiden

<sup>2</sup>Cryptology Group, Centrum Wiskunde en Informatica (CWI)

ALGANT-DOC Meeting, 15th May 2017

M4GB: An  
Efficient  
Gröbner Basis  
Algorithm

Rusydi H.  
Makarim,  
Marc Stevens

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

- ➊ Introduction
- ➋ M4GB Algorithm
- ➌ Performance Comparison
- ➍ Solving MQ Challenges

# Table of Contents

- ➊ Introduction
- ➋ M4GB Algorithm
- ➌ Performance Comparison
- ➍ Solving MQ Challenges

# Problem

$\mathbb{F}[x_1, \dots, x_n]$  - a polynomial ring over a field  $\mathbb{F}$  together with an admissible monomial ordering  $<$ .

# Problem

$\mathbb{F}[x_1, \dots, x_n]$  - a polynomial ring over a field  $\mathbb{F}$  together with an admissible monomial ordering  $<$ .

## Problem (MQ-problem)

*Let  $n, m \in \mathbb{Z}_{>0}$ . Given  $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$  with  $f_i$  be quadratic polynomials, find a  $(a_1, \dots, a_n) \in \mathbb{F}^n$  such that  $f_i(a_1, \dots, a_n) = 0$  for all  $i = 1, \dots, m$ .*

# Notations

## Example

$$f = -15x^2 + 8xy - 13z^2 - 4x + 11z \in \mathbb{F}_{31}[x, y, z]$$

# Notations

## Example

$$f = -15x^2 + 8xy - 13z^2 - 4x + 11z \in \mathbb{F}_{31}[x, y, z]$$

- $\text{LM}(f) = x^2$  (the leading monomial of  $f$ )

# Notations

## Example

$$f = -15x^2 + 8xy - 13z^2 - 4x + 11z \in \mathbb{F}_{31}[x, y, z]$$

- $\text{LM}(f) = x^2$  (the leading monomial of  $f$ )
- $\text{LC}(f) = -15$  (the leading coefficient of  $f$ )



# Notations

## Example

$$f = -15x^2 + 8xy - 13z^2 - 4x + 11z \in \mathbb{F}_{31}[x, y, z]$$

- $\text{LM}(f) = x^2$  (the leading monomial of  $f$ )
- $\text{LC}(f) = -15$  (the leading coefficient of  $f$ )
- $\text{LT}(f) = -15x^2$  (the leading term of  $f$ )

# Notations

## Example

$$f = -15x^2 + 8xy - 13z^2 - 4x + 11z \in \mathbb{F}_{31}[x, y, z]$$

- $\text{LM}(f) = x^2$  (the leading monomial of  $f$ )
- $\text{LC}(f) = -15$  (the leading coefficient of  $f$ )
- $\text{LT}(f) = -15x^2$  (the leading term of  $f$ )
- $\text{Tail}(f) = 8xy - 13z^2 - 4x + 11z$  (the tail of  $f$ )

# Notations

## Example

$$f = -15x^2 + 8xy - 13z^2 - 4x + 11z \in \mathbb{F}_{31}[x, y, z]$$

- $\text{LM}(f) = x^2$  (the leading monomial of  $f$ )
- $\text{LC}(f) = -15$  (the leading coefficient of  $f$ )
- $\text{LT}(f) = -15x^2$  (the leading term of  $f$ )
- $\text{Tail}(f) = 8xy - 13z^2 - 4x + 11z$  (the tail of  $f$ )

# Polynomial Reduction

## Theorem

*Let  $G = (g_1, \dots, g_t)$  be a nonempty ordered finite subset of  $\mathbb{F}[x_1, \dots, x_n]$ . Then every polynomial  $f \in \mathbb{F}[x_1, \dots, x_n]$  can be written as*

$$f = q_1 g_1 + \dots + q_t g_t + r,$$

*where  $q_1, \dots, q_t, r \in \mathbb{F}[x_1, \dots, x_n]$  and either  $r = 0$  or none of terms of  $r$  is divisible by any of  $\text{LT}(g_1), \dots, \text{LT}(g_t)$ .*

# Polynomial Reduction

## Theorem

*Let  $G = (g_1, \dots, g_t)$  be a nonempty ordered finite subset of  $\mathbb{F}[x_1, \dots, x_n]$ . Then every polynomial  $f \in \mathbb{F}[x_1, \dots, x_n]$  can be written as*

$$f = q_1g_1 + \dots + q_tg_t + r,$$

*where  $q_1, \dots, q_t, r \in \mathbb{F}[x_1, \dots, x_n]$  and either  $r = 0$  or none of terms of  $r$  is divisible by any of  $\text{LT}(g_1), \dots, \text{LT}(g_t)$ .*

$$r \leftarrow \text{FULLREDUCE}(f, G)$$

# Gröbner basis

## Definition

Let  $I \neq \{0\}$  be an ideal of  $\mathbb{F}[x_1, \dots, x_n]$ . A finite subset  $G \subseteq I$  that generates  $I$  is a Gröbner basis of  $I$  if for all  $f \in I$ , there exists  $g \in G$  such that  $\text{LT}(g) \mid \text{LT}(f)$ .

# S-polynomial

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

## Definition

Let  $f, g \in \mathbb{F}[x_1, \dots, x_n]$  be nonzero polynomials and let  $x^\gamma = \text{LCM}(\text{LM}(f), \text{LM}(g))$ . The S-polynomial of  $f$  and  $g$  is defined as

$$\text{Spoly}(f, g) = \frac{x^\gamma}{\text{LT}(f)} \cdot f - \frac{x^\gamma}{\text{LT}(g)} \cdot g.$$

# Buchberger's Algorithm

**Input:** A finite ordered subset  $F \subseteq \mathbb{F}[x_1, \dots, x_n]$

**Result:** A Gröbner basis  $G$  such that  $\langle G \rangle = \langle F \rangle$

```
1  $P \leftarrow \{\{p, q\} : \forall p, q \in F \text{ and } p \neq q\}$ 
2  $G \leftarrow F$ 
3 while  $P \neq \{\}$  do
4    $\{p, q\} \leftarrow \text{SELECT}(P)$ 
5    $P \leftarrow P \setminus \{\{p, q\}\}$ 
6    $r \leftarrow \text{FULLREDUCE}(\text{Spoly}(p, q), G)$ 
7   if  $r \neq 0$  then
8      $P \leftarrow P \cup \{\{r, g\} : \forall g \in G\}$ 
9      $G \leftarrow G \cup \{r\}$ 
10 return  $G$ 
```



# Table of Contents

- ➊ Introduction
- ➋ M4GB Algorithm
- ➌ Performance Comparison
- ➍ Solving MQ Challenges

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

# Observations

M4GB: An  
Efficient  
Gröbner Basis  
Algorithm

Rusydi H.  
Makarim,  
Marc Stevens

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

# Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$  with *degrevlex* monomial ordering

# Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$  with *degrevlex* monomial ordering

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2$$

# Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$  with *degrevlex* monomial ordering

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2 \quad G = \{g_1, g_2, g_3\}$$

$$g_1 = x_1^2 x_2^3 + x_1 x_3^3 + x_4^2$$

$$g_2 = x_2^3 x_4 + x_2 x_3 + x_3 + 1$$

$$g_3 = x_1 x_2 x_3 + x_1 x_3$$

## Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$  with *degrevlex* monomial ordering

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2 \quad G = \{g_1, g_2, g_3\}$$

$$g_1 = x_1^2 x_2^3 + x_1 x_3^3 + x_4^2$$

$$g_2 = x_2^3 x_4 + x_2 x_3 + x_3 + 1$$

$$g_3 = x_1 x_2 x_3 + x_1 x_3$$

# Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$  with *degrevlex* monomial ordering

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2 \quad G = \{g_1, g_2, g_3\}$$

$$f = f - g_1 = x_1 x_2^3 x_4 + x_1^3 x_4 + x_2 x_3^2$$
$$g_1 = x_1^2 x_2^3 + x_1 x_3^3 + x_4^2$$
$$g_2 = x_2^3 x_4 + x_2 x_3 + x_3 + 1$$
$$g_3 = x_1 x_2 x_3 + x_1 x_3$$

# Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$  with *degrevlex* monomial ordering

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2 \quad G = \{g_1, g_2, g_3\}$$

$$f = f - g_1 = x_1 x_2^3 x_4 + x_1^3 x_4 + x_2 x_3^2$$
$$g_1 = x_1^2 x_2^3 + x_1 x_3^3 + x_4^2$$
$$g_2 = x_2^3 x_4 + x_2 x_3 + x_3 + 1$$
$$g_3 = x_1 x_2 x_3 + x_1 x_3$$



## Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$  with *degrevlex* monomial ordering

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2 \quad G = \{g_1, g_2, g_3\}$$

$$\begin{aligned} f &= f - g_1 = x_1 x_2^3 x_4 + x_1^3 x_4 + x_2 x_3^2 \\ g_1 &= x_1^2 x_2^3 + x_1 x_3^3 + x_4^2 \\ g_2 &= x_2^3 x_4 + x_2 x_3 + x_3 + 1 \\ g_3 &= x_1 x_2 x_3 + x_1 x_3 \end{aligned}$$

$$x_1 g_2 = x_1 x_2^3 x_4 + x_1 x_2 x_3 + x_1 x_3 + x_1$$

# Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$  with *degrevlex* monomial ordering

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2 \quad G = \{g_1, g_2, g_3\}$$

$$f = f - g_1 = x_1 x_2^3 x_4 + x_1^3 x_4 + x_2 x_3^2$$
$$g_1 = x_1^2 x_2^3 + x_1 x_3^3 + x_4^2$$
$$g_2 = x_2^3 x_4 + x_2 x_3 + x_3 + 1$$
$$g_3 = x_1 x_2 x_3 + x_1 x_3$$

$$x_1 g_2 = x_1 x_2^3 x_4 + x_1 x_2 x_3 + x_1 x_3 + x_1$$

## Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$  with *degrevlex* monomial ordering

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2$$

$$G = \{g_1, g_2, g_3\}$$

$$f = f - g_1 = x_1 x_2^3 x_4 + x_1^3 x_4 + x_2 x_3^2$$

$$g_1 = x_1^2 x_2^3 + x_1 x_3^3 + x_4^2$$

$$g_2 = x_2^3 x_4 + x_2 x_3 + x_3 + 1$$

$$g_3 = x_1 x_2 x_3 + x_1 x_3$$

$$x_1 g_2 = x_1 x_2^3 x_4 + x_1 x_2 x_3 + x_1 x_3 + x_1$$

## Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$  with *degrevlex* monomial ordering

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2$$

$$f = f - g_1 = x_1 x_2^3 x_4 + x_1^3 x_4 + x_2 x_3^2$$

$$G = \{g_1, g_2, g_3, g_4\}$$

$$g_1 = x_1^2 x_2^3 + x_1 x_3^3 + x_4^2$$

$$g_2 = x_2^3 x_4 + x_2 x_3 + x_3 + 1$$

$$g_3 = x_1 x_2 x_3 + x_1 x_3$$

$$g_4 = x_1 g_2 - g_3 = x_1 x_2^3 x_4 + 1$$

$$x_1 g_2 = x_1 x_2^3 x_4 + x_1 x_2 x_3 + x_1 x_3 + x_1$$

## Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$  with *degrevlex* monomial ordering

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2$$

$$G = \{g_1, g_2, g_3, g_4\}$$

$$f = f - g_1 = x_1 x_2^3 x_4 + x_1^3 x_4 + x_2 x_3^2$$

$$g_1 = x_1^2 x_2^3 + x_1 x_3^3 + x_4^2$$

$$g_2 = x_2^3 x_4 + x_2 x_3 + x_3 + 1$$

$$g_3 = x_1 x_2 x_3 + x_1 x_3$$

$$g_4 = x_1 g_2 - g_3 = x_1 x_2^3 x_4 + 1$$

$$x_1 g_2 = x_1 x_2^3 x_4 + x_1 x_2 x_3 + x_1 x_3 + x_1$$

## Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$  with *degrevlex* monomial ordering

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2$$

$$f = f - g_1 = x_1 x_2^3 x_4 + x_1^3 x_4 + x_2 x_3^2$$

$$f = f - g_4 = x_1^3 x_4 + x_2 x_3^2 + 1$$

$$G = \{g_1, g_2, g_3, g_4\}$$

$$g_1 = x_1^2 x_2^3 + x_1 x_3^3 + x_4^2$$

$$g_2 = x_2^3 x_4 + x_2 x_3 + x_3 + 1$$

$$g_3 = x_1 x_2 x_3 + x_1 x_3$$

$$g_4 = x_1 g_2 - g_3 = x_1 x_2^3 x_4 + 1$$

$$x_1 g_2 = x_1 x_2^3 x_4 + x_1 x_2 x_3 + x_1 x_3 + x_1$$

## Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$  with *degrevlex* monomial ordering

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2$$

$$f = f - g_1 = x_1 x_2^3 x_4 + x_1^3 x_4 + x_2 x_3^2$$

$$f = f - g_4 = x_1^3 x_4 + x_2 x_3^2 + 1$$

$$G = \{g_1, g_2, g_3, g_4\}$$

$$g_1 = x_1^2 x_2^3 + x_1 x_3^3 + x_4^2$$

$$g_2 = x_2^3 x_4 + x_2 x_3 + x_3 + 1$$

$$g_3 = x_1 x_2 x_3 + x_1 x_3$$

$$g_4 = x_1 g_2 - g_3 = x_1 x_2^3 x_4 + 1$$

$$x_1 g_2 = x_1 x_2^3 x_4 + x_1 x_2 x_3 + x_1 x_3 + x_1$$

$$r = x_1^3 x_4 + x_2 x_3^2 + 1$$

# M4GB Reduction

MULFULLREDUCE( $G, u, f$ )

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

```
1  $r \leftarrow 0$ 
2 forall  $t \in \text{Term}(f)$  do
3    $t' \leftarrow u \cdot t$ 
4   if  $\exists g \in G : \text{LT}(g) \mid t'$  then
5      $(G, g) \leftarrow$ 
6        $\text{GETREDUCTOR}(G, t')$ 
7      $r \leftarrow r - (t' / \text{LT}(g)) \cdot \text{Tail}(g)$ 
8   else
9      $r \leftarrow r + t'$ 
10 return  $(G, r)$ 
```



# M4GB Reduction

MULFULLREDUCE( $G, u, f$ )

GETREDUCTOR( $G, t$ )

```
1  $r \leftarrow 0$ 
2 forall  $t \in \text{Term}(f)$  do
3    $t' \leftarrow u \cdot t$ 
4   if  $\exists g \in G : \text{LT}(g) \mid t'$  then
5      $(G, g) \leftarrow$ 
6        $\text{GETREDUCTOR}(G, t')$ 
7        $r \leftarrow r - (t' / \text{LT}(g)) \cdot \text{Tail}(g)$ 
8   else
9      $r \leftarrow r + t'$ 
10 return  $(G, r)$ 
```

```
1 if  $\exists g \in G : \text{LM}(g) = \text{LM}(t)$  then
2    $\lfloor$  return  $(G, g)$ 
3  $h \leftarrow \text{SELECTREDUCTOR}(G, t)$ 
4  $(G, h) \leftarrow$ 
5    $\text{MULFULLREDUCE}(G, t / \text{LT}(h), \text{Tail}(h))$ 
6  $g \leftarrow t + h$ 
7 return  $(G \cup \{g\}, g)$ 
```

M4GB: An  
Efficient  
Gröbner Basis  
Algorithm

Rusydi H.  
Makarim,  
Marc Stevens

# M4GB (Simplified)

Introduction

**M4GB  
Algorithm**

Performance  
Comparison

Solving MQ  
Challenges

# Table of Contents

- ❶ Introduction
- ❷ M4GB Algorithm
- ❸ Performance Comparison
- ❹ Solving MQ Challenges

- Implemented using C++11

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

- Implemented using C++11
- Comparison with existing implementations
  - ① FGb C Interface - Implementation by Jean Charles Faugere<sup>1</sup>
  - ② Magma v2.20-6
  - ③ OpenF4 v1.0.1 - Open source implementation by Coladon, Vitse and Joux<sup>2</sup>.

---

<sup>1</sup>Available at <http://www-polsys.lip6.fr/~jcf/FGb/C/index.html>

<sup>2</sup>Available at <https://github.com/naotit/openf4>

- Implemented using C++11
- Comparison with existing implementations
  - ① FGb C Interface - Implementation by Jean Charles Faugere<sup>1</sup>
  - ② Magma v2.20-6
  - ③ OpenF4 v1.0.1 - Open source implementation by Coladon, Vitse and Joux<sup>2</sup>.
- Test cases
  - ① Dense polynomials with coefficients in  $\mathbb{F}_{31}$
  - ②  $m = 2n$  and  $m = n + 1$ .

---

<sup>1</sup>Available at <http://www-polsys.lip6.fr/~jcf/FGb/C/index.html>

<sup>2</sup>Available at <https://github.com/naotit/openf4>

# Benchmark for $m = 2n$

		Total CPU time (sec)			
$n$	$m$	OpenF4	FGb	Magma (projected)	M4GB
20	40	206	470	232.17	57
21	42	472	1002	500.26	170
22	44	1145	3118	1616.73	424
23	46	2274	6849	3184.82	1060
24	48	10293	64700	31167.61	2556
25	50	-	151653	77678.58	5575
26	52	-	360055	183628.74	15517
27	54	-	767543	409451.87	46548

		Memory (MB)			
20	40	4240	112	361.84	73
21	42	6640	165	577.34	121
22	44	14368	525	853.84	226
23	46	26135	918	1324.16	395
24	48	161945	1561	8872.94	663
25	50	-	2765	19718.78	1471
26	52	-	4607	25197	3328
27	54	-	8180	39844.84	6799

M4GB: An  
Efficient  
Gröbner Basis  
Algorithm

Rusydi H.  
Makarim,  
Marc Stevens

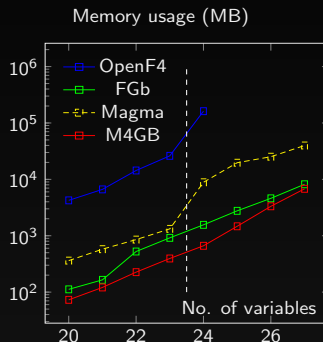
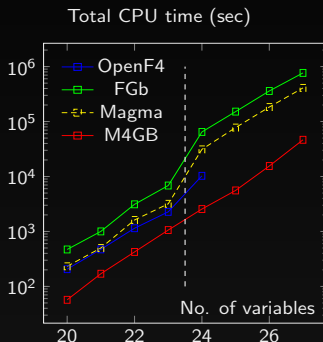
Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

# Graph for $m = 2n$





# Benchmark for $m = n + 1$

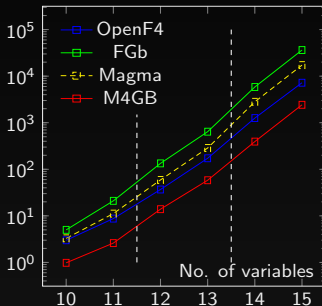
		Total CPU time (sec)			
$n$	$m$	OpenF4	FGb	Magma (projected)	M4GB
10	11	2.99	5	3.29	0.98
11	12	8.73	21	11.172	2.6
12	13	36.76	134	59.08	13.92
13	14	172.49	642	286.4	58.18
14	15	1258	5850	2810.75	393.19
15	16	7225	36361	17265.5	2424

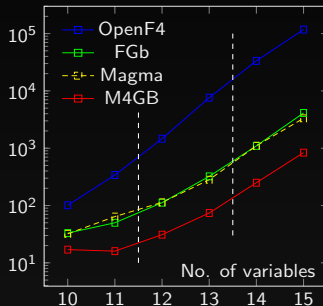
		Memory (MB)			
10	11	101	33	32.09	17
11	12	341	50	64.12	16
12	13	1463	112	113.59	31
13	14	7622	323	281.53	74
14	15	33460	1098	1104	250
15	16	117396	4118	3320	837

## Graph for $m = n + 1$

Total CPU time (sec)



Memory usage (MB)



# Table of Contents

- ➊ Introduction
- ➋ M4GB Algorithm
- ➌ Performance Comparison
- ➍ Solving MQ Challenges

M4GB: An  
Efficient  
Gröbner Basis  
Algorithm

Rusydi H.  
Makarim,  
Marc Stevens

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

- MQ-based public key and digital signature are candidates of post-quantum cryptography.
- Their security relies on the difficulty of finding a solution of an MQ problem.
- Need to understand its difficulty in practice

# Fukuoka MQ Challenge

- Started on 1st April 2015
- Six different type of challenges

# Fukuoka MQ Challenge

- Started on 1st April 2015
- Six different type of challenges
- Type I, II, and III are encryption-type parameter ( $m = 2n$ ) and coefficients in  $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$  respectively.

## Fukuoka MQ Challenge

- Started on 1st April 2015
- Six different type of challenges
- Type I, II, and III are encryption-type parameter ( $m = 2n$ ) and coefficients in  $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$  respectively.
- Type IV, V, and VI are signature-type parameter ( $n \approx 1.5m$ ) and coefficients in  $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$  respectively.

# Fukuoka MQ Challenge

- Started on 1st April 2015
- Six different type of challenges
- Type I, II, and III are encryption-type parameter ( $m = 2n$ ) and coefficients in  $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$  respectively.
- Type IV, V, and VI are signature-type parameter ( $n \approx 1.5m$ ) and coefficients in  $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$  respectively.
- Parameter Choice : Require at least **one month** for Magma 2.19-9 to solve using **Four 6-cores Intel(R) Xeon(R) CPU E5-4617 @ 2.9GHz** and **1TB of RAM**.



# Fukuoka MQ Challenge

- Started on 1st April 2015
- Six different type of challenges
- Type I, II, and III are encryption-type parameter ( $m = 2n$ ) and coefficients in  $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$  respectively.
- Type IV, V, and VI are signature-type parameter ( $n \approx 1.5m$ ) and coefficients in  $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$  respectively.
- Parameter Choice : Require at least **one month** for Magma 2.19-9 to solve using **Four 6-cores Intel(R) Xeon(R) CPU E5-4617 @ 2.9GHz** and **1TB of RAM**.

<https://www.mqchallenge.org>

# Solving Signature-type MQ Challenge

- Hybrid approach : trade-off between exhaustive search and computing Gröbner bases
- Idea :

- ① Select a random vector  $(a_1, \dots, a_{n-m}) \in \mathbb{F}_q^{n-m}$
- ② Construct a new system with  $n = m$

$$\tilde{F} = \{f(x_1, \dots, x_m, a_1, \dots, a_{n-m}) : \forall f \in F\}$$

- ③ Select  $k \in \{1, \dots, m\}$  and construct  $q^k$  subsystems from  $\tilde{F}$  by substituting  $k$  variables with all elements of  $\mathbb{F}_q^k$ .
- ④ Each subsystem generated can be solved in parallel.

# Computational Resources

A) Desktop machine with Intel(R) Core(TM) i7-2600K CPU @  
3.40GHz and 16GB RAM

# Computational Resources

- A) Desktop machine with Intel(R) Core(TM) i7-2600K CPU @ 3.40GHz and 16GB RAM
- B) NUMA machine with two nodes of Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz and 128GB RAM each.

# Solved Challenges

Type	$n/m$	Machine Used	# Node	Duration

# Solved Challenges

Type	$n/m$	Machine Used	# Node	Duration
V	24/16			
V	25/17			
V	27/18			

# Solved Challenges

Type	$n/m$	Machine Used	# Node	Duration
V	24/16	A	1	$\approx 9.3$ hours
V	25/17			
V	27/18			

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

# Solved Challenges

Type	$n/m$	Machine Used	# Node	Duration
V	24/16	A	1	$\approx 9.3$ hours
V	25/17	B	1	$\approx 46.33$ hours
V	27/18	B	2	$\approx 10.9$ days

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges



# Solved Challenges

Type	$n/m$	Machine Used	# Node	Duration
V	24/16	A	1	$\approx 9.3$ hours
V	25/17	B	1	$\approx 46.33$ hours
V	27/18	B	2	$\approx 10.9$ days
VI	24/16			
VI	25/17			
VI	27/18			
VI	28/19			

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

# Solved Challenges

Type	$n/m$	Machine Used	# Node	Duration
V	24/16	A	1	$\approx 9.3$ hours
V	25/17	B	1	$\approx 46.33$ hours
V	27/18	B	2	$\approx 10.9$ days
VI	24/16	A	1	$\approx 1.2$ hours
VI	25/17			
VI	27/18			
VI	28/19			

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

# Solved Challenges

Type	$n/m$	Machine Used	# Node	Duration
V	24/16	A	1	$\approx 9.3$ hours
V	25/17	B	1	$\approx 46.33$ hours
V	27/18	B	2	$\approx 10.9$ days
VI	24/16	A	1	$\approx 1.2$ hours
VI	25/17	B	1	$\approx 9.87$ hours
VI	27/18	B	1	$\approx 31.48$ hours
VI	28/19	B	2	$\approx 7.61$ days

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

M4GB: An  
Efficient  
Gröbner Basis  
Algorithm

Rusydi H.  
Makarim,  
Marc Stevens

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

<https://github.com/cr-marcstevens/m4gb>

M4GB: An  
Efficient  
Gröbner Basis  
Algorithm

Rusydi H.  
Makarim,  
Marc Stevens

Introduction

M4GB  
Algorithm

Performance  
Comparison

Solving MQ  
Challenges

Question ?