Breaking the Fukuoka MQ Challenges

Tung Chou*, Ruben Niederhagen*, and Bo-Yin Yang⋆

⋆Academia Sinica, Taipei, Taiwan
*Eindhoven University of Technology, the Netherlands

February 26, 2016

Fukuoka MQ Challenge:

For quadratic polynomials f_i ($i = 1, 2, \ldots, m$) of n variables over a finite field $\mathbb{F}$, consider the following polynomial system:

$$
\begin{aligned}
f_1(x_1, \ldots, x_n) &= \sum_{1 \le i \le j \le n} a_{ij}^{(1)} x_i x_j + \sum_{1 \le i \le n} b_i^{(1)} x_i + c^{(1)} &= d_1 \\
f_2(x_1, \ldots, x_n) &= \sum_{1 \le i \le j \le n} a_{ij}^{(2)} x_i x_j + \sum_{1 \le i \le n} b_i^{(2)} x_i + c^{(2)} &= d_2 \\
&\vdots \\
f_m(x_1, \ldots, x_n) &= \sum_{1 \le i \le j \le n} a_{ij}^{(m)} x_i x_j + \sum_{1 \le i \le n} b_i^{(m)} x_i + c^{(m)} &= d_m
\end{aligned}
$$

The goal is to find an answer $v = [v_1, \ldots, v_n]$ in $\mathbb{F}^n$ of the above system.

Fukuoka MQ Challenge:

This challenge has six types of systems: three of them are related to an encryption scheme with three different base fields, and other three are related to a signature scheme:

Type I:	Encryption,	$m = 2n$,	$\mathbb{F} = GF(2)$
Type II:	Encryption,	$m = 2n$,	$\mathbb{F} = GF(2^8)$
Type III:	Encryption,	$m = 2n$,	$\mathbb{F} = GF(31)$
Type IV:	Signature,	$n \approx 1.5m$,	$\mathbb{F} = GF(2)$
Type V:	Signature,	$n \approx 1.5m$,	$\mathbb{F} = GF(2^8)$
Type VI:	Signature,	$n \approx 1.5m$,	$\mathbb{F} = GF(31)$

Fukuoka MQ Challenge:

This challenge has six types of systems: three of them are related to an encryption scheme with three different base fields, and other three are related to a signature scheme:

Type I:	Encryption,	$m = 2n$,	$\mathbb{F} = \mathrm{GF}(2)$
Type II:	Encryption,	$m = 2n$,	$\mathbb{F} = \mathrm{GF}(2^8)$
Type III:	Encryption,	$m = 2n$,	$\mathbb{F} = \mathrm{GF}(31)$
Type IV:	Signature,	$n \approx 1.5m$,	$\mathbb{F} = \mathrm{GF}(2)$
Type V:	Signature,	$n \approx 1.5m$,	$\mathbb{F} = \mathrm{GF}(2^8)$
Type VI:	Signature,	$n \approx 1.5m$,	$\mathbb{F} = \mathrm{GF}(31)$

Breaking MQ Challenges with XL:

We solved two Type III challenges with extended linearization (XL):

- *Extend* the system by multiplying the equations with all monomials up to a certain degree D.
- *Linearize* the system by treating all monomials in the resulting system as individual variables.
- *Solve* the resulting linear system; the solution is also a solution for the MQ system.

We are using an adaptation *Coppersmith's block Wiedemann* (BW) algorithm to solve the linear system.

Breaking MQ Challenges with XL:

Number of variables (n)	34	35
Number of equations (m)	68	70
Runtime:	32d 18h 26min	48d 23h 32min
BW1:	26d 3h 31min	40d 9min
BW2 (Berlekamp-Massey):	6d 14h 53min	8d 23h 21min
BW3*:	2min	3min

Computation on a quad-socket AMD Opteron 6282 SE machine with 512GB memory.

*Adapted step in Coppersmith's block Wiedemann.

Breaking MQ Challenges with Gray Code enumeration:

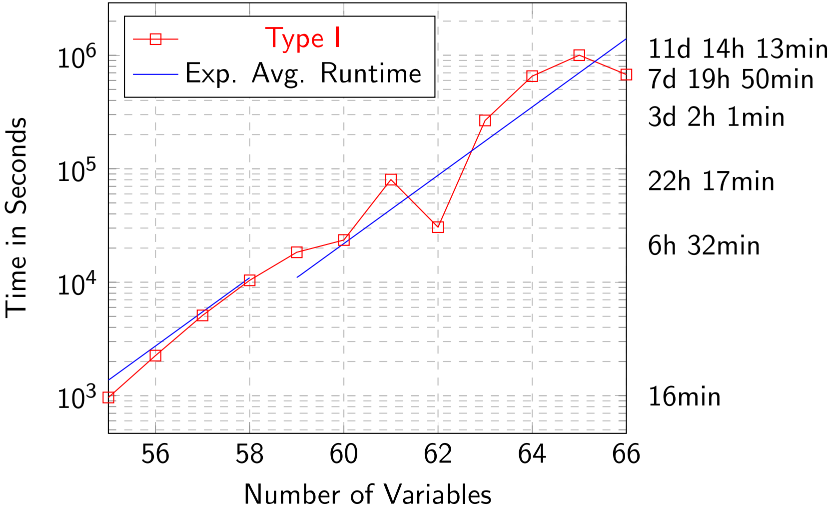
We solved several Type I and Type IV challenges (GF(2)) using an FPGA implementation of *Gray Code enumeration*.

Using Gray Code enumeration, only the first derivative needs to be added to the previous evaluation of an equation.

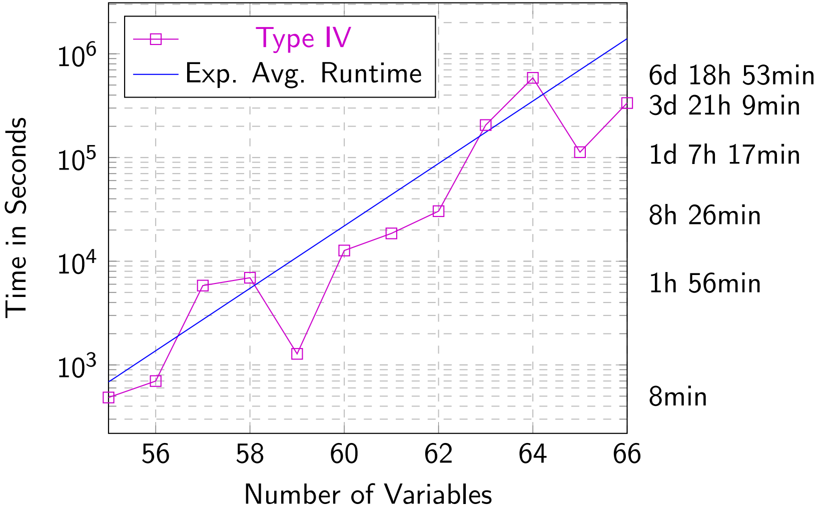
$\Longrightarrow$ Efficient "brute force" search.

We were using a cluster of 64–128 Spartan 6 FPGAs, each FPGA evaluating 1024 solution candidates in parallel at 200MHz.

Breaking MQ Challenges with Gray Code enumeration:



Breaking MQ Challenges with Gray Code enumeration:



More information:

`http://www.win.tue.nl/~tchou/mqchallenge/`

More information:

http://www.win.tue.nl/~tchou/mqchallenge/

There are many open challenges; join us in breaking them!

More information:
`http://www.win.tue.nl/~tchou/mqchallenge/`

There are many open challenges; join us in breaking them!

Thank you for your attention.