Attacks on the Mersenne-based AJPS cryptosystem

Koen de Boer [1], L. Ducas [1], S. Jeffery [1,2], R. de Wolf [1,2,3]

[1]Centrum Wiskunde en Informatica, Amsterdam

[2]QuSoft, Amsterdam

[3]University of Amsterdam

April 9, 2018

Overview

May '17

Aggarwal, Joux, Prakash, Santha [AJPS17]

- Propose *potentially quantum-safe* public-key cryptosystem based on Mersenne numbers and NTRU [HPS98].

Overview

May '17

Aggarwal, Joux, Prakash, Santha [AJPS17]

- Propose *potentially quantum-safe* public-key cryptosystem based on Mersenne numbers and NTRU [HPS98].
- Consider but dismiss Meet-in-the-Middle and lattice attacks.

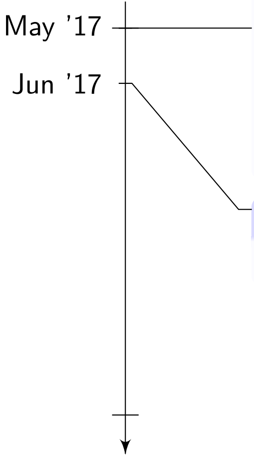
Overview

May '17

Aggarwal, Joux, Prakash, Santha [AJPS17]

- Propose *potentially quantum-safe* public-key cryptosystem based on Mersenne numbers and NTRU [HPS98].
- Consider but dismiss Meet-in-the-Middle and lattice attacks.
- Hope that 'brute force' is the optimal attack.

Overview



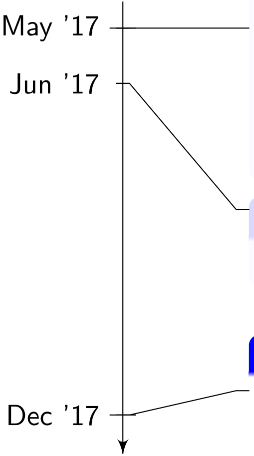
Aggarwal, Joux, Prakash, Santha [AJPS17]

- Propose *potentially quantum-safe* public-key cryptosystem based on Mersenne numbers and NTRU [HPS98].
- Consider but dismiss Meet-in-the-Middle and lattice attacks.
- Hope that 'brute force' is the optimal attack.

Beunardeau, Connolly, Géraud, Naccache [BCGN17]

Describe an experimental lattice-reduction attack.

Overview



Aggarwal, Joux, Prakash, Santha [AJPS17]

- Propose *potentially quantum-safe* public-key cryptosystem based on Mersenne numbers and NTRU [HPS98].
- Consider but dismiss Meet-in-the-Middle and lattice attacks.
- Hope that 'brute force' is the optimal attack.

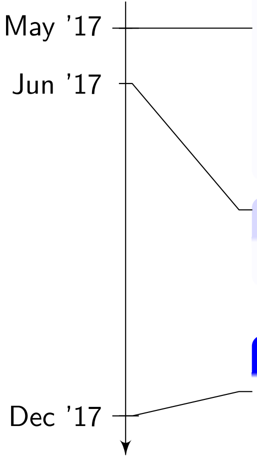
Beunardeau, Connolly, Géraud, Naccache [BCGN17]

Describe an experimental lattice-reduction attack.

Our contribution

- Meet-in-the-Middle attack

Overview



Aggarwal, Joux, Prakash, Santha [AJPS17]

- Propose *potentially quantum-safe* public-key cryptosystem based on Mersenne numbers and NTRU [HPS98].
- Consider but dismiss Meet-in-the-Middle and lattice attacks.
- Hope that 'brute force' is the optimal attack.

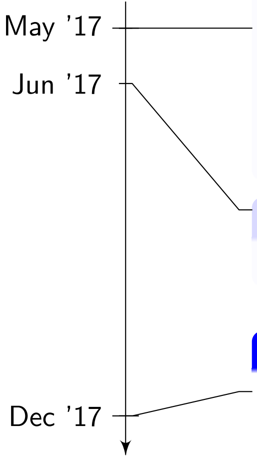
Beunardeau, Connolly, Géraud, Naccache [BCGN17]

Describe an experimental lattice-reduction attack.

Our contribution

- Meet-in-the-Middle attack
- Analysis of the lattice-attack of Beunardeau et al.

Overview



Aggarwal, Joux, Prakash, Santha [AJPS17]

- Propose *potentially quantum-safe* public-key cryptosystem based on Mersenne numbers and NTRU [HPS98].
- Consider but dismiss Meet-in-the-Middle and lattice attacks.
- Hope that 'brute force' is the optimal attack.

Beunardeau, Connolly, Géraud, Naccache [BCGN17]

Describe an experimental lattice-reduction attack.

Our contribution

- **Meet-in-the-Middle attack** ← **this talk**
- Analysis of the lattice-attack of Beunardeau et al.

Table of Contents

1 The Mersenne-number based AJPS-cryptosystem

2 Meet-in-the-Middle attack on the AJPS cryptosystem
- Example: Subset-sum problem
- MITM in the AJPS-cryptosystem

The AJPS cryptosystem

- Set $R = \mathbb{Z}/N\mathbb{Z}$, where $N = 2^n - 1$ with n prime.

The AJPS cryptosystem

- Set $R = \mathbb{Z}/N\mathbb{Z}$, where $N = 2^n - 1$ with n prime.
- Each element in R can be uniquely identified by its binary representation in $\{0,1\}^n \backslash \{1^n\}$.

$a \in R$	bin. rep.	$\lvert a \rvert$
0	0...000	0
1	0...001	1
2	0...010	1
3	0...011	2
$\vdots$	$\vdots$	$\vdots$
$2^n - 2$	1...110	$n - 1$

The AJPS cryptosystem

- Set $R = \mathbb{Z}/N\mathbb{Z}$, where $N = 2^n - 1$ with n prime.
- Each element in R can be uniquely identified by its binary representation in $\{0,1\}^n \backslash \{1^n\}$.
- For $a \in R$, set $|a| :=$ the Hamming weight of the binary representation of a.

$a \in R$	bin. rep.	$\lvert a \rvert$
0	0...000	0
1	0...001	1
2	0...010	1
3	0...011	2
⋮	⋮	⋮
$2^n - 2$	1...110	$n-1$

The AJPS cryptosystem

- Set $R = \mathbb{Z}/N\mathbb{Z}$, where $N = 2^n - 1$ with n prime.
- Each element in R can be uniquely identified by its binary representation in $\{0,1\}^n \backslash \{1^n\}$.
- For $a \in R$, set $|a| :=$ the Hamming weight of the binary representation of a.

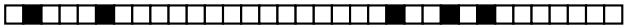
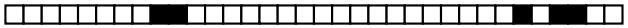
$a \in R$	bin. rep.	$\|a\|$
0	0...000	0
1	0...001	1
2	0...010	1
3	0...011	2
$\vdots$	$\vdots$	$\vdots$
$2^n - 2$	1...110	$n - 1$

The AJPS cryptosystem

- Set $R = \mathbb{Z}/N\mathbb{Z}$, where $N = 2^n - 1$ with n prime.
- Each element in R can be uniquely identified by its binary representation in $\{0,1\}^n \backslash \{1^n\}$.
- For $a \in R$, set $|a| :=$ the Hamming weight of the binary representation of a.
- Set $w = \lfloor \sqrt{n}/2 \rfloor$.

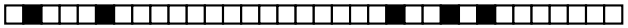
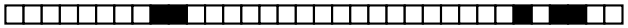
The AJPS cryptosystem

- Set $R = \mathbb{Z}/N\mathbb{Z}$, where $N = 2^n - 1$ with n prime.
- Each element in R can be uniquely identified by its binary representation in $\{0,1\}^n \backslash \{1^n\}$.
- For $a \in R$, set $|a| :=$ the Hamming weight of the binary representation of a.
- Set $w = \lfloor \sqrt{n}/2 \rfloor$.
- Choose $f, g \in R$ such that $|f| = |g| = w$ and g invertible.

$f =$  , $g =$ 

The AJPS cryptosystem

- Set $R = \mathbb{Z}/N\mathbb{Z}$, where $N = 2^n - 1$ with n prime.
- Each element in R can be uniquely identified by its binary representation in $\{0,1\}^n \backslash \{1^n\}$.
- For $a \in R$, set $|a| :=$ the Hamming weight of the binary representation of a.
- Set $w = \lfloor \sqrt{n}/2 \rfloor$.
- Choose $f, g \in R$ such that $|f| = |g| = w$ and g invertible.
- Set $h = f/g$. Public key is $\boldsymbol{h}$ and secret key $\boldsymbol{g}$.

$f =$  , $\boldsymbol{g} =$ 

$\boldsymbol{h} = \frac{f}{\boldsymbol{g}} =$ 

The AJPS cryptosystem

- Set $R = \mathbb{Z}/N\mathbb{Z}$, where $N = 2^n - 1$ with n prime.
- Each element in R can be uniquely identified by its binary representation in $\{0,1\}^n \backslash \{1^n\}$.
- For $a \in R$, set $|a| :=$ the Hamming weight of the binary representation of a.
- Set $w = \lfloor \sqrt{n}/2 \rfloor$.
- Choose $f, g \in R$ such that $|f| = |g| = w$ and g invertible.
- Set $h = f/g$. Public key is $\boldsymbol{h}$ and secret key $\boldsymbol{g}$.

The Mersenne Low Hamming Ratio Problem

The AJPS cryptosystem

- Set $R = \mathbb{Z}/N\mathbb{Z}$, where $N = 2^n - 1$ with n prime.
- Each element in R can be uniquely identified by its binary representation in $\{0,1\}^n \backslash \{1^n\}$.
- For $a \in R$, set $|a| :=$ the Hamming weight of the binary representation of a.
- Set $w = \lfloor \sqrt{n}/2 \rfloor$.
- Choose $f, g \in R$ such that $|f| = |g| = w$ and g invertible.
- Set $h = f/g$. Public key is $\boldsymbol{h}$ and secret key $\boldsymbol{g}$.

The Mersenne Low Hamming Ratio Problem

- Given $\boldsymbol{h} \in R$, which is quotient of two elements of low Hamming wt.

The AJPS cryptosystem

- Set $R = \mathbb{Z}/N\mathbb{Z}$, where $N = 2^n - 1$ with n prime.
- Each element in R can be uniquely identified by its binary representation in $\{0,1\}^n \backslash \{1^n\}$.
- For $a \in R$, set $|a| :=$ the Hamming weight of the binary representation of a.
- Set $w = \lfloor \sqrt{n}/2 \rfloor$.
- Choose $f, g \in R$ such that $|f| = |g| = w$ and g invertible.
- Set $h = f/g$. Public key is $\boldsymbol{h}$ and secret key $\boldsymbol{g}$.

The Mersenne Low Hamming Ratio Problem

- Given $\boldsymbol{h} \in R$, which is quotient of two elements of low Hamming wt.
- Find $f, g \in R$ with $|f| = |g| = w$ such that $\boldsymbol{h} = f/g$.

The AJPS cryptosystem

- Set $R = \mathbb{Z}/N\mathbb{Z}$, where $N = 2^n - 1$ with n prime.
- Each element in R can be uniquely identified by its binary representation in $\{0,1\}^n \backslash \{1^n\}$.
- For $a \in R$, set $|a| :=$ the Hamming weight of the binary representation of a.
- Set $w = \lfloor \sqrt{n}/2 \rfloor$.
- Choose $f, g \in R$ such that $|f| = |g| = w$ and g invertible.
- Set $h = f/g$. Public key is $\boldsymbol{h}$ and secret key $\boldsymbol{g}$.

The Mersenne Low Hamming Ratio Problem

- Given $\boldsymbol{h} \in R$, which is quotient of two elements of low Hamming wt.
- Find $f, g \in R$ with $|f| = |g| = w$ such that $\boldsymbol{h} = f/g$.

Brute force attack: Guess a $g \in R$ with $|g| = w$, check whether $|g\boldsymbol{h}| = w$. time: $\binom{n}{w}$.

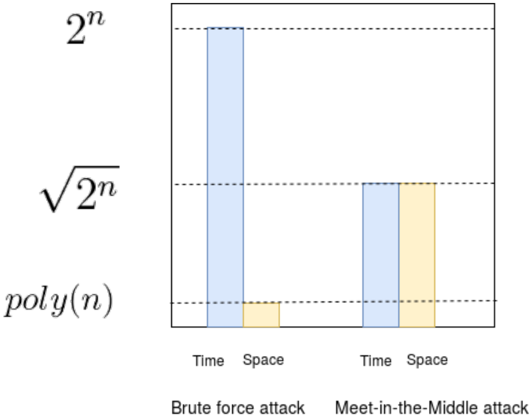
Table of Contents

1 The Mersenne-number based AJPS-cryptosystem

2 Meet-in-the-Middle attack on the AJPS cryptosystem
- Example: Subset-sum problem
- MITM in the AJPS-cryptosystem

Meet-in-the-Middle attack

Improved time complexity, at the cost of greater space complexity.



MITM in the subset-sum problem

Subset-sum problem

Given $z_1, \ldots, z_n \in \mathbb{Z}$
Find $I \subseteq \{1, \ldots, n\}$ such that $\sum_{i \in I} z_i = 0$.

$\mathbf{z_1}$	**6**
z_2	2
$\mathbf{z_3}$	**−1**
z_4	10
z_5	9
$\mathbf{z_6}$	**−5**

MITM in the subset-sum problem

Subset-sum problem

Given $z_1, \ldots, z_n \in \mathbb{Z}$
Find $I \subseteq \{1, \ldots, n\}$ such that $\sum_{i \in I} z_i = 0$.

- For all $I_1 \subseteq \{1, \ldots, n/2\}$, store I_1 in the bucket $L\left[\sum_{i \in I_1} z_i\right]$.

z_1	6
z_2	2
z_3	-1
z_4	10
z_5	9
z_4	-5

i	$L[i]$

MITM in the subset-sum problem

Subset-sum problem

Given $z_1, \ldots, z_n \in \mathbb{Z}$
Find $I \subseteq \{1, \ldots, n\}$ such that $\sum_{i \in I} z_i = 0$.

- For all $I_1 \subseteq \{1, \ldots, n/2\}$, store I_1 in the bucket $L\left[\sum_{i \in I_1} z_i\right]$.

z_1	6
z_2	2
z_3	-1
z_4	10
z_5	9
z_4	-5

i	$L[i]$
6	$\{1\}$

MITM in the subset-sum problem

Subset-sum problem

Given $z_1, \ldots, z_n \in \mathbb{Z}$
Find $I \subseteq \{1, \ldots, n\}$ such that $\sum_{i \in I} z_i = 0$.

- For all $I_1 \subseteq \{1, \ldots, n/2\}$, store I_1 in the bucket $L\left[\sum_{i \in I_1} z_i\right]$.

z_1	6
z_2	2
z_3	-1
z_4	10
z_5	9
z_4	-5

i	$L[i]$
6	$\{1\}$
8	$\{1, 2\}$

MITM in the subset-sum problem

Subset-sum problem

Given $z_1, \ldots, z_n \in \mathbb{Z}$
Find $I \subseteq \{1, \ldots, n\}$ such that $\sum_{i \in I} z_i = 0$.

- For all $I_1 \subseteq \{1, \ldots, n/2\}$, store I_1 in the bucket $L\left[\sum_{i \in I_1} z_i\right]$.

z_1	6
z_2	2
z_3	-1
z_4	10
z_5	9
z_4	-5

i	$L[i]$
6	$\{1\}$
8	$\{1, 2\}$
7	$\{1, 2, 3\}$

MITM in the subset-sum problem

Subset-sum problem

Given $z_1, \ldots, z_n \in \mathbb{Z}$
Find $I \subseteq \{1, \ldots, n\}$ such that $\sum_{i \in I} z_i = 0$.

- For all $I_1 \subseteq \{1, \ldots, n/2\}$, store I_1 in the bucket $L\left[\sum_{i \in I_1} z_i\right]$.

z_1	6
z_2	2
z_3	-1
z_4	10
z_5	9
z_4	-5

i	$L[i]$
-1	$\{3\}$
1	$\{2, 3\}$
2	$\{2\}$
5	$\{1, 3\}$
6	$\{1\}$
7	$\{1, 2, 3\}$
8	$\{1, 2\}$

MITM in the subset-sum problem

Subset-sum problem

Given $z_1, \ldots, z_n \in \mathbb{Z}$
Find $I \subseteq \{1, \ldots, n\}$ such that $\sum_{i \in I} z_i = 0$.

- For all $I_1 \subseteq \{1, \ldots, n/2\}$, store I_1 in the bucket $L\left[\sum_{i \in I_1} z_i\right]$.
- For every $I_2 \subseteq \{n/2+1, \ldots, n\}$ do

z_1	6
z_2	2
z_3	-1
z_4	10
z_5	9
z_4	-5

i	$L[i]$
-1	$\{3\}$
1	$\{2,3\}$
2	$\{2\}$
5	$\{1,3\}$
6	$\{1\}$
7	$\{1,2,3\}$
8	$\{1,2\}$

MITM in the subset-sum problem

Subset-sum problem

Given $z_1, \ldots, z_n \in \mathbb{Z}$
Find $I \subseteq \{1, \ldots, n\}$ such that $\sum_{i \in I} z_i = 0$.

- For all $I_1 \subseteq \{1, \ldots, n/2\}$, store I_1 in the bucket $L\left[\sum_{i \in I_1} z_i\right]$.
- For every $I_2 \subseteq \{n/2+1, \ldots, n\}$ do
  - Check whether the bucket $L\left[-\sum_{i \in I_2} z_i\right]$ is non-empty.

z_1	6
z_2	2
z_3	-1
z_4	10
z_5	9
z_4	-5

i	$L[i]$
-1	$\{3\}$
1	$\{2,3\}$
2	$\{2\}$
5	$\{1,3\}$
6	$\{1\}$
7	$\{1,2,3\}$
8	$\{1,2\}$

$-\sum_{i \in \{4\}} z_i = -10$

MITM in the subset-sum problem

Subset-sum problem

Given $z_1, \ldots, z_n \in \mathbb{Z}$
Find $I \subseteq \{1, \ldots, n\}$ such that $\sum_{i \in I} z_i = 0$.

- For all $I_1 \subseteq \{1, \ldots, n/2\}$, store I_1 in the bucket $L\left[\sum_{i \in I_1} z_i\right]$.
- For every $I_2 \subseteq \{n/2+1, \ldots, n\}$ do
  - Check whether the bucket $L\left[-\sum_{i \in I_2} z_i\right]$ is non-empty.

z_1	6
z_2	2
z_3	-1
z_4	10
z_5	9
z_4	-5

i	$L[i]$
-1	$\{3\}$
1	$\{2,3\}$
2	$\{2\}$
5	$\{1,3\}$
6	$\{1\}$
7	$\{1,2,3\}$
8	$\{1,2\}$

$-\sum_{i \in \{4\}} z_i = -10$
$-\sum_{i \in \{5\}} z_i = -9$

MITM in the subset-sum problem

Subset-sum problem

Given $z_1, \ldots, z_n \in \mathbb{Z}$
Find $I \subseteq \{1, \ldots, n\}$ such that $\sum_{i \in I} z_i = 0$.

- For all $I_1 \subseteq \{1, \ldots, n/2\}$, store I_1 in the bucket $L\left[\sum_{i \in I_1} z_i\right]$.
- For every $I_2 \subseteq \{n/2+1, \ldots, n\}$ do
  - Check whether the bucket $L\left[-\sum_{i \in I_2} z_i\right]$ is non-empty.
  - If it is, output I_2 and a $I_1 \in L\left[-\sum_{i \in I_2} z_i\right]$.

z_1	6
z_2	2
z_3	-1
z_4	10
z_5	9
z_6	-5

i	$L[i]$
-1	$\{3\}$
1	$\{2, 3\}$
2	$\{2\}$
5	$\mathbf{\{1, 3\}}$
6	$\{1\}$
7	$\{1, 2, 3\}$
8	$\{1, 2\}$

$-\sum_{i \in \{4\}} z_i = -10$
$-\sum_{i \in \{5\}} z_i = -9$
$-\sum_{i \in \{6\}} z_i = 5$

MITM in the subset-sum problem

Subset-sum problem

Given $z_1, \ldots, z_n \in \mathbb{Z}$
Find $I \subseteq \{1, \ldots, n\}$ such that $\sum_{i \in I} z_i = 0$.

- For all $I_1 \subseteq \{1, \ldots, n/2\}$, store I_1 in the bucket $L\left[\sum_{i \in I_1} z_i\right]$.
- For every $I_2 \subseteq \{n/2+1, \ldots, n\}$ do
  - Check whether the bucket $L\left[-\sum_{i \in I_2} z_i\right]$ is non-empty.
  - If it is, output I_2 and a $I_1 \in L\left[-\sum_{i \in I_2} z_i\right]$.

$\mathbf{z_1}$	**6**
z_2	2
$\mathbf{z_3}$	**−1**
z_4	10
z_5	9
$\mathbf{z_6}$	**−5**

Output: $\{1, 3\} \cup \{6\}$

MITM in the AJPS-cryptosystem

The Mersenne Low Hamming Ratio Problem

- Given $\boldsymbol{h} \in R$, which is quotient of two elements of low Hamming wt.
- Find $f, g \in R$ with $|f| = |g| = w$ such that $\boldsymbol{h} = f/g$.

MITM in the AJPS-cryptosystem

The Mersenne Low Hamming Ratio Problem

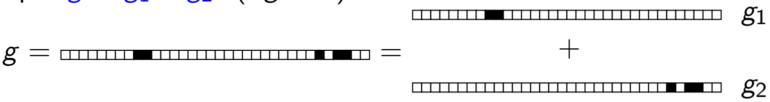
- Given $\boldsymbol{h} \in R$, which is quotient of two elements of low Hamming wt.
- Find $f, g \in R$ with $|f| = |g| = w$ such that $\boldsymbol{h} = f/g$.

- Split $g = g_1 + g_2$. ($\boldsymbol{h}g = f$)

The Mersenne Low Hamming Ratio Problem

- Given $\boldsymbol{h} \in R$, which is quotient of two elements of low Hamming wt.
- Find $f, g \in R$ with $|f| = |g| = w$ such that $\boldsymbol{h} = f/g$.

- Split $g = g_1 + g_2$. ($\boldsymbol{h}g = f$)



MITM in the AJPS-cryptosystem

The Mersenne Low Hamming Ratio Problem

- Given $\boldsymbol{h} \in R$, which is quotient of two elements of low Hamming wt.
- Find $f, g \in R$ with $|f| = |g| = w$ such that $\boldsymbol{h} = f/g$.

- Split $g = g_1 + g_2$. $(\boldsymbol{h}g = f)$

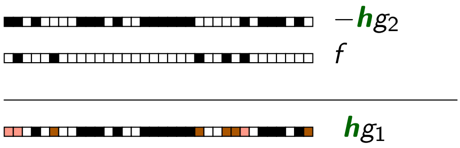
MITM in the AJPS-cryptosystem

The Mersenne Low Hamming Ratio Problem

- Given $\boldsymbol{h} \in R$, which is quotient of two elements of low Hamming wt.
- Find $f, g \in R$ with $|f| = |g| = w$ such that $\boldsymbol{h} = f/g$.

- Split $g = g_1 + g_2$. ($\boldsymbol{h}g = f$)

- Then $hg_1 = -hg_2 + f$

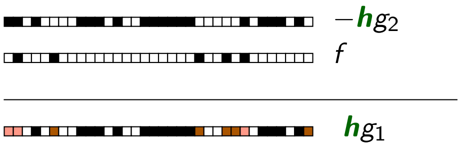


MITM in the AJPS-cryptosystem

The Mersenne Low Hamming Ratio Problem

- Given $\boldsymbol{h} \in R$, which is quotient of two elements of low Hamming wt.
- Find $f, g \in R$ with $|f| = |g| = w$ such that $\boldsymbol{h} = f/g$.

- Split $g = g_1 + g_2$. ($\boldsymbol{h}g = f$)
- Then $hg_1 = -hg_2 + f$



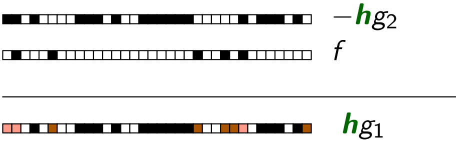
- Heuristically, assume $-hg_2$ is random.

MITM in the AJPS-cryptosystem

The Mersenne Low Hamming Ratio Problem

- Given $\boldsymbol{h} \in R$, which is quotient of two elements of low Hamming wt.
- Find $f, g \in R$ with $|f| = |g| = w$ such that $\boldsymbol{h} = f/g$.

- Split $g = g_1 + g_2$. ($\boldsymbol{h}g = f$)
- Then $hg_1 = -hg_2 + f$



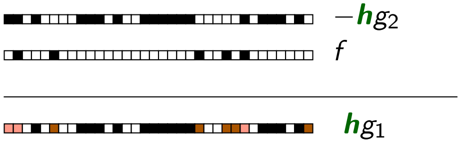
- Heuristically, assume $-hg_2$ is random.
- Then $\Delta_{Hamm}(-hg_2, hg_1) \leq 2w + c\sqrt{w}$ with error probability $\leq e^{-c/8}$.

MITM in the AJPS-cryptosystem

The Mersenne Low Hamming Ratio Problem

- Given $\boldsymbol{h} \in R$, which is quotient of two elements of low Hamming wt.
- Find $f, g \in R$ with $|f| = |g| = w$ such that $\boldsymbol{h} = f/g$.

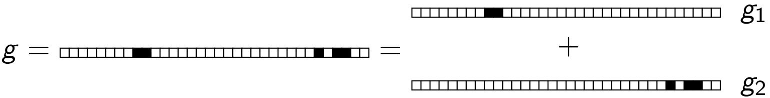
- Split $g = g_1 + g_2$. ($\boldsymbol{h}g = f$)
- Then $hg_1 = -hg_2 + f$



- Heuristically, assume $-hg_2$ is random.
- Then $\Delta_{Hamm}(-hg_2, hg_1) \leq 2w + c\sqrt{w}$ with error probability $\leq e^{-c/8}$.
- Informally: $-hg_2 \approx hg_1$.

MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.

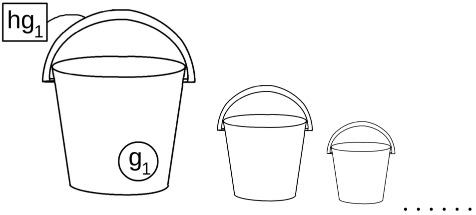


MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, store $\{g_1\}$ into the bucket $L[hg_1]$.

Hash Table L:

Key	Bucket
$hg_1 \rightarrow$	$\{g_1\}$
$hg_1' \rightarrow$	$\{g_1'\}$
$\vdots$	$\vdots$

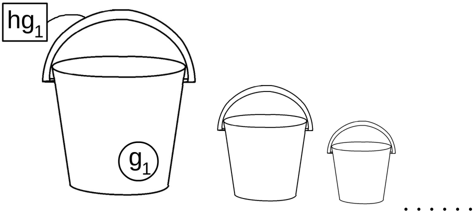


MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, store $\{g_1\}$ into the bucket $L[hg_1]$.
- For all g_2, do

Hash Table L:

Key	Bucket
$hg_1 \rightarrow$	$\{g_1\}$
$hg'_1 \rightarrow$	$\{g'_1\}$
$\vdots$	$\vdots$

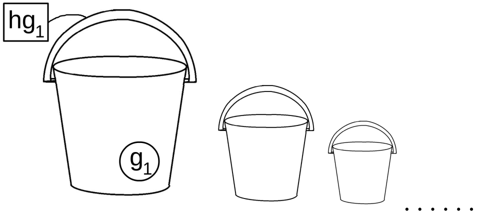


MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, store $\{g_1\}$ into the bucket $L[hg_1]$.
- For all g_2, do
  - Find $t \approx -hg_2$, such that $L[t]$ is non-empty.

Hash Table L:

Key	Bucket
$hg_1 \rightarrow$	$\{g_1\}$
$hg_1' \rightarrow$	$\{g_1'\}$
$\vdots$	$\vdots$

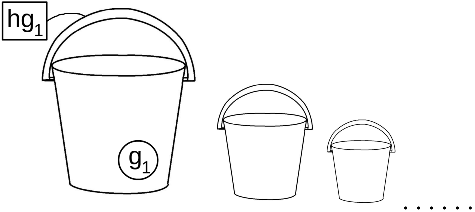


MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, store $\{g_1\}$ into the bucket $L[hg_1]$.
- For all g_2, do
  - Find $t \approx -hg_2$, such that $L[t]$ is non-empty.
  - If such t exists, pick $g_1 \in L[t]$ and output $g_1 + g_2$.

Hash Table L:

Key	**Bucket**
$\boldsymbol{hg_1} \rightarrow$	$\{\boldsymbol{g_1}\}$
$hg_1' \rightarrow$	$\{g_1'\}$
$\vdots$	$\vdots$



MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, store $\{\boldsymbol{g_1}\}$ into the bucket $\boldsymbol{L}[\boldsymbol{hg_1}]$.
- For all g_2, do
  - Find $t \approx -hg_2$, such that $L[t]$ is non-empty.
  - If such t exists, pick $g_1 \in L[t]$ and output $g_1 + g_2$.

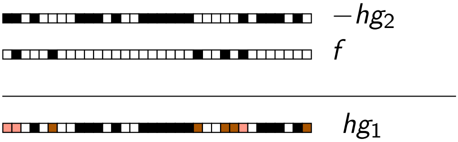
Hash Table L:

Key	**Bucket**
$\boldsymbol{hg_1} \rightarrow$	$\{\boldsymbol{g_1}\}$
$hg_1' \rightarrow$	$\{g_1'\}$
$\vdots$	$\vdots$

Problem: There are **many** $t \approx -hg_2$, and most of the buckets $L[t]$ are empty

Locality Sensitive Hashing

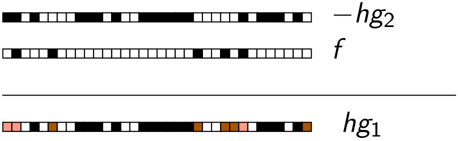
$hg_1 = -hg_2 + f$



Locality Sensitive Hashing

Locality Sensitive Hashing

$hg_1 = -hg_2 + f$

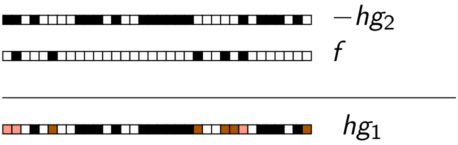


Locality Sensitive Hashing

Construct the 'hash' function $\mathcal{H} : \{0,1\}^n \to \{0,1\}^k$, sending $b_n \cdots b_1 \mapsto b_{k+i} \cdots b_i$.

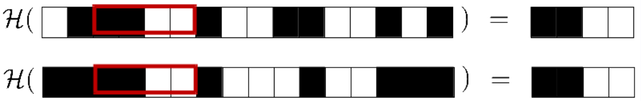
Locality Sensitive Hashing

$hg_1 = -hg_2 + f$



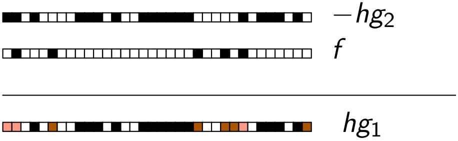
Locality Sensitive Hashing

Construct the 'hash' function $\mathcal{H} : \{0,1\}^n \to \{0,1\}^k$, sending $b_n \cdots b_1 \mapsto b_{k+i} \cdots b_i$.



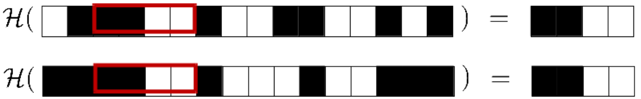
Locality Sensitive Hashing

$hg_1 = -hg_2 + f$



Locality Sensitive Hashing

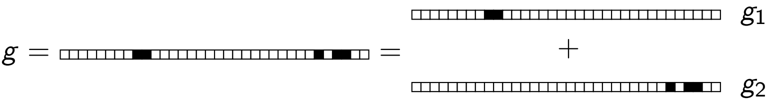
Construct the 'hash' function $\mathcal{H} : \{0,1\}^n \to \{0,1\}^k$, sending $b_n \cdots b_1 \mapsto b_{k+i} \cdots b_i$.



Hope: $\mathcal{H}(hg_1) = \mathcal{H}(-hg_2)$

MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.



MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, $\{\boldsymbol{g_1}\}$ into the bucket $\boldsymbol{L}[\boldsymbol{\mathcal{H}(hg_1)}]$.

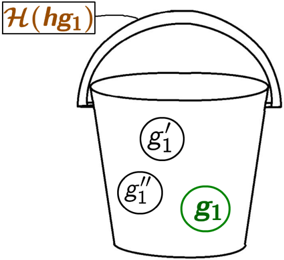
Hash Table L:

Key	**Bucket**
$\boldsymbol{\mathcal{H}(hg_1)} \rightarrow$	$\{g_1', g_1'', \boldsymbol{g_1}, \ldots\}$
$\mathcal{H}(hg_1''') \rightarrow$	$\{g_1''', \ldots\}$
$\vdots$	$\vdots$

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, $\{\boldsymbol{g_1}\}$ into the bucket $\boldsymbol{L}[\boldsymbol{\mathcal{H}(hg_1)}]$.

Hash Table L:

Key	Bucket
$\boldsymbol{\mathcal{H}(hg_1)} \rightarrow$	$\{g_1', g_1'', \boldsymbol{g_1}, \ldots\}$
$\mathcal{H}(hg_1''') \rightarrow$	$\{g_1''', \ldots\}$
$\vdots$	$\vdots$

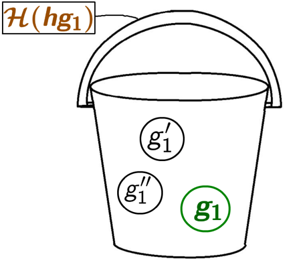


MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, $\{\boldsymbol{g_1}\}$ into the bucket $\boldsymbol{L}[\mathcal{H}(\boldsymbol{hg_1})]$.
- For all g_2 do

Hash Table L:

Key	**Bucket**
$\mathcal{H}(\boldsymbol{hg_1}) \rightarrow$	$\{g_1', g_1'', \boldsymbol{g_1}, \ldots\}$
$\mathcal{H}(hg_1''') \rightarrow$	$\{g_1''', \ldots\}$
$\vdots$	$\vdots$

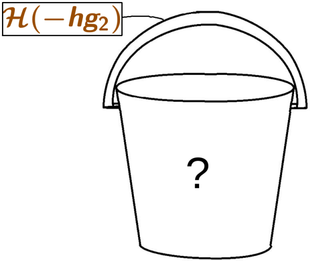


MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, $\{\boldsymbol{g_1}\}$ into the bucket $\boldsymbol{L}[\mathcal{H}(\boldsymbol{hg_1})]$.
- For all g_2 do
  - Check whether $\boldsymbol{L}[\mathcal{H}(-\boldsymbol{hg_2})]$ is non-empty.

Hash Table L:

Key	**Bucket**
$\mathcal{H}(\boldsymbol{hg_1}) \rightarrow$	$\{g_1', g_1'', \boldsymbol{g_1}, \ldots\}$
$\mathcal{H}(hg_1''') \rightarrow$	$\{g_1''', \ldots\}$
$\vdots$	$\vdots$

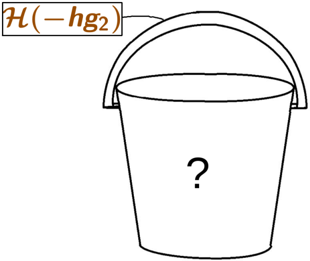


MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, $\{\boldsymbol{g_1}\}$ into the bucket $\boldsymbol{L}[\boldsymbol{\mathcal{H}(hg_1)}]$.
- For all g_2 do
  - Check whether $\boldsymbol{L}[\boldsymbol{\mathcal{H}(-hg_2)}]$ is non-empty.
  - If so, then check if some $g_1 \in L[\mathcal{H}(-hg_2)]$ satisfies $|h(g_1 + g_2)| = w$.

Hash Table L:

Key	**Bucket**
$\boldsymbol{\mathcal{H}(hg_1)} \rightarrow$	$\{g_1', g_1'', \boldsymbol{g_1}, \ldots\}$
$\mathcal{H}(hg_1''') \rightarrow$	$\{g_1''', \ldots\}$
$\vdots$	$\vdots$



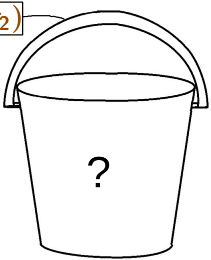
MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, $\{g_1\}$ into the bucket $L[\mathcal{H}(hg_1)]$.
- For all g_2 do
  - Check whether $L[\mathcal{H}(-hg_2)]$ is non-empty.
  - If so, then check if some $g_1 \in L[\mathcal{H}(-hg_2)]$ satisfies $|h(g_1 + g_2)| = w$.
  - If so, output $g_1 + g_2$.

Hash Table L:

Key	Bucket
$\mathcal{H}(hg_1) \rightarrow$	$\{g_1', g_1'', g_1, \ldots\}$
$\mathcal{H}(hg_1''') \rightarrow$	$\{g_1''', \ldots\}$
$\vdots$	$\vdots$

$\mathcal{H}(-hg_2)$



MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, $\{\boldsymbol{g_1}\}$ into the bucket $\boldsymbol{L}[\mathcal{H}(\boldsymbol{hg_1})]$.
- For all g_2 do
  - Check whether $\boldsymbol{L}[\mathcal{H}(-\boldsymbol{hg_2})]$ is non-empty.
  - If so, then check if some $g_1 \in L[\mathcal{H}(-hg_2)]$ satisfies $|h(g_1 + g_2)| = w$.
  - If so, output $g_1 + g_2$.

Difficulties:

MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, $\{\boldsymbol{g_1}\}$ into the bucket $\boldsymbol{L}[\boldsymbol{\mathcal{H}(hg_1)}]$.
- For all g_2 do
  - Check whether $\boldsymbol{L}[\boldsymbol{\mathcal{H}(-hg_2)}]$ is non-empty.
  - If so, then check if some $g_1 \in L[\mathcal{H}(-hg_2)]$ satisfies $|h(g_1 + g_2)| = w$.
  - If so, output $g_1 + g_2$.

Difficulties:

- 'false positives': non-close elements in the bucket

MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, $\{\boldsymbol{g_1}\}$ into the bucket $\boldsymbol{L}[\mathcal{H}(\boldsymbol{hg_1})]$.
- For all g_2 do
  - Check whether $\boldsymbol{L}[\mathcal{H}(-\boldsymbol{hg_2})]$ is non-empty.
  - If so, then check if some $g_1 \in L[\mathcal{H}(-hg_2)]$ satisfies $|h(g_1 + g_2)| = w$.
  - If so, output $g_1 + g_2$.

Difficulties:

- 'false positives': non-close elements in the bucket
- 'false negatives': close element in 'wrong' bucket

MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, $\{g_1\}$ into the bucket $L[\mathcal{H}(hg_1)]$.
- For all g_2 do
  - Check whether $L[\mathcal{H}(-hg_2)]$ is non-empty.
  - If so, then check if some $g_1 \in L[\mathcal{H}(-hg_2)]$ satisfies $|h(g_1 + g_2)| = w$.
  - If so, output $g_1 + g_2$.

Difficulties:

- 'false positives': non-close elements in the bucket
- 'false negatives': close element in 'wrong' bucket

Solution: Choose the block size of $\mathcal{H}$ to be $\log_2 \binom{n/2}{w/2}$. Repeat algorithm over randomized $\mathcal{H}$.

MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, $\{g_1\}$ into the bucket $L[\mathcal{H}(hg_1)]$.
- For all g_2 do
    - Check whether $L[\mathcal{H}(-hg_2)]$ is non-empty.
    - If so, then check if some $g_1 \in L[\mathcal{H}(-hg_2)]$ satisfies $|h(g_1 + g_2)| = w$.
    - If so, output $g_1 + g_2$.

Difficulties:

- 'false positives': non-close elements in the bucket
- 'false negatives': close element in 'wrong' bucket

Solution: Choose the block size of $\mathcal{H}$ to be $\log_2 \binom{n/2}{w/2}$. Repeat algorithm over randomized $\mathcal{H}$. Using a combinatorial heuristic, this works.

MITM in the AJPS-cryptosystem

- Split a possible $g = g_1 + g_2$ in two parts, where $g_1 \in \{0,1\}^{n/2} \times 0^{n/2}$ and $g_2 \in 0^{n/2} \times \{0,1\}^{n/2}$.
- For all g_1, $\{g_1\}$ into the bucket $L[\mathcal{H}(hg_1)]$.
- For all g_2 do
  - Check whether $L[\mathcal{H}(-hg_2)]$ is non-empty.
  - If so, then check if some $g_1 \in L[\mathcal{H}(-hg_2)]$ satisfies $|h(g_1 + g_2)| = w$.
  - If so, output $g_1 + g_2$.

Difficulties:

- 'false positives': non-close elements in the bucket
- 'false negatives': close element in 'wrong' bucket

Solution: Choose the block size of $\mathcal{H}$ to be $\log_2 \binom{n/2}{w/2}$. Repeat algorithm over randomized $\mathcal{H}$. Using a combinatorial heuristic, this works.

This algorithm breaks the AJPS system in time $\binom{n/2}{w/2} \approx n^{\sqrt{n}/8}$

Overview

Attack	Authors	Running time	
		Classical	Quantum

Overview

Attack	Authors	Running time	
		Classical	Quantum
Brute force	AJPS	$n^{\frac{\sqrt{n}}{4}}$	$n^{\frac{\sqrt{n}}{8}}$

Overview

Attack	Authors	Running time	
		Classical	Quantum
Brute force	AJPS	$n^{\frac{\sqrt{n}}{4}}$	$n^{\frac{\sqrt{n}}{8}}$
Meet in the Middle	Our work	$n^{\frac{\sqrt{n}}{8}}$	$n^{\frac{\sqrt{n}}{12}}$

Overview

Attack	Authors	Running time	
		Classical	Quantum
Brute force	AJPS	$n^{\frac{\sqrt{n}}{4}}$	$n^{\frac{\sqrt{n}}{8}}$
Meet in the Middle	Our work	$n^{\frac{\sqrt{n}}{8}}$	$n^{\frac{\sqrt{n}}{12}}$
Lattice attack	BCGN	$2^{\sqrt{n}}$?	$2^{\sqrt{n}/2}$?

Overview

Attack	Authors	Running time	
		Classical	Quantum
Brute force	AJPS	$n^{\frac{\sqrt{n}}{4}}$	$n^{\frac{\sqrt{n}}{8}}$
Meet in the Middle	Our work	$n^{\frac{\sqrt{n}}{8}}$	$n^{\frac{\sqrt{n}}{12}}$
Lattice attack	BCGN	$2^{\sqrt{n}}$?	$2^{\sqrt{n}/2}$?
	Our analysis	$2.01^{\sqrt{n}}$	$2.01^{\sqrt{n}/2}$

Open Questions

- We analyzed the lattice attack of Beunardeau et al. over randomly chosen keys.

Open Questions

- We analyzed the lattice attack of Beunardeau et al. over randomly chosen keys.
  Are there specific ‘weak’ keys for this lattice attack?

Open Questions

- We analyzed the lattice attack of Beunardeau et al. over randomly chosen keys.
  Are there specific 'weak' keys for this lattice attack?
- Aggarwal et al. improved their cryptosystem [AJPS17], allowing to encrypt more bits.

Open Questions

- We analyzed the lattice attack of Beunardeau et al. over randomly chosen keys.
  Are there specific 'weak' keys for this lattice attack?
- Aggarwal et al. improved their cryptosystem [AJPS17], allowing to encrypt more bits.
  What is the security of this improved system?

Main lesson

Main lesson

Collisions don't need to be exact to apply a Meet-in-the-Middle attack

References

D. Aggarwal et al. *A New Public-Key Cryptosystem via Mersenne Numbers*. Cryptology ePrint Archive, Report 2017/481. http://eprint.iacr.org/2017/481. 2017.

A. Ambainis. "Quantum Search with Variable Times". In: *Theory of Computing Systems* 47.3 (2010), pp. 786–807. ISSN: 1433-0490. DOI: 10.1007/s00224-009-9219-1.

M. Beunardeau et al. "On the Hardness of the Mersenne Low Hamming Ratio Assumption". In: *Progress in Cryptology – LATINCRYPT 2017*. Available at http://eprint.iacr.org/2017/522. 2017.

J. Hoffstein, J. Pipher, and J. H. Silverman. "NTRU: A ring-based public key cryptosystem". In: *International Algorithmic Number Theory Symposium*. Springer. 1998, pp. 267–288.