Improved Cryptanalysis of the AJPS Mersenne Based Cryptosystem

Jean-Sébastien Coron and **Agnese Gini**

University of Luxembourg

June 27, 2019
NutMiC

SNT
securityandtrust.lu
uni.lu
UNIVERSITÉ DU LUXEMBOURG

Timeline

- 2016 NIST calling for quantum-resistant cryptographic algorithms for new public-key crypto standards.
- 2017 Aggarwal, Joux, Prakash, Santha propose *A new public-key cryptosystem via Mersenne numbers*.
- 2017 Deadline submission to Round 1 NIST PQC "Competition": 69 accepted papers of 82, more than 40% lattice-based including *Mersenne-756839*.
- 2019 Round 2 candidates announced: 26 selected, $\sim$ 46% lattice-based not including *Mersenne-756839*.

Ring+Small Noise

- Let $\mathcal{R} := {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, where n is a prime and $p = 2^n - 1$ a Mersenne prime.

Ring+Small Noise

- Let $\mathcal{R} := {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, where n is a prime and $p = 2^n - 1$ a Mersenne prime.
- There is a bijection between integers mod p and strings of length n (up to $1^n \simeq 0^n$).

Ring+Small Noise

- Let $\mathcal{R} := {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, where n is a prime and $p = 2^n - 1$ a Mersenne prime.
- There is a bijection between integers mod p and strings of length n (up to $1^n \simeq 0^n$).
- Reducing mod p preserves low Hamming weight strings.

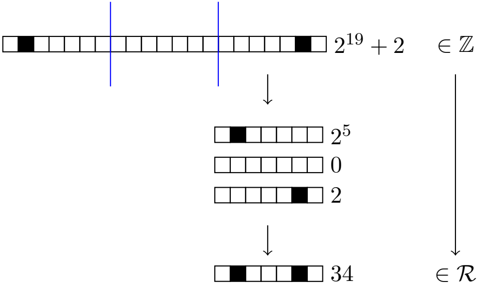
Ring+Small Noise

- Let $\mathcal{R} := \mathbb{Z}/_{p\mathbb{Z}}$, where n is a prime and $p = 2^n - 1$ a Mersenne prime.
- There is a bijection between integers mod p and strings of length n (up to $1^n \simeq 0^n$).
- Reducing mod p preserves low Hamming weight strings.

Ring+Small Noise

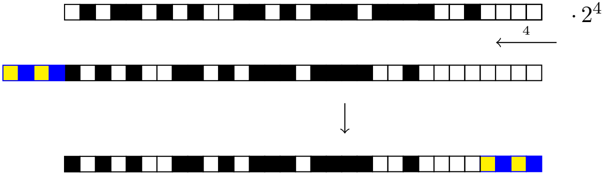
- Let $\mathcal{R} := {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, where n is a prime and $p = 2^n - 1$ a Mersenne prime.
- There is a bijection between integers mod p and strings of length n (up to $1^n \simeq 0^n$).
- Reducing mod p preserves low Hamming weight strings.

$n = 7, p = 2^7 - 1$



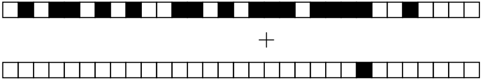
Ring+Small Noise

$n = 31, p = 2^{31} - 1$

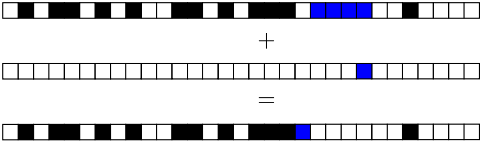


- $\mathsf{HW}(2^i \cdot A) = \mathsf{HW}(A)$

Ring+Small Noise



Ring+Small Noise



- $\mathsf{HW}(A + B) \leq \mathsf{HW}(A) + \mathsf{HW}(B)$
- $\mathsf{HW}(A \cdot B) \leq \mathsf{HW}(A)\mathsf{HW}(B)$
- $\mathsf{HW}(-B) = n - \mathsf{HW}(B)$

AJPS-2

Setup n, $p = 2^n - 1$ prime, $h = \lambda \in \mathbb{N}$, $(\mathcal{E}, \mathcal{D})$ error correcting code where $\mathcal{E}\colon \{0,1\}^h \to \{0,1\}^n$.

KeyGen
- $F, G \in \mathcal{R}$ random such that $\mathsf{HW}(F) = \mathsf{HW}(G) = h$
- $R \in \mathcal{R}$ random

$$pk = (R, F \cdot R + G) = (R, T) \quad \text{and} \quad sk = F$$

Encrypt Given $m \in \{0,1\}^h$:
- generate random A, B_1, $B_2 \in \mathcal{R}$ such that $\mathsf{HW}(A) = \mathsf{HW}(B_1) = \mathsf{HW}(B_2) = h$
- $(C_1, C_2) \coloneqq (A \cdot R + B_1, (A \cdot T + B_2) \oplus \mathcal{E}(m))$

Decrypt $m = \mathcal{D}((F \cdot C_1) \oplus C_2)$

AJPS-2

Setup n, $p = 2^n - 1$ prime, $h = \lambda \in \mathbb{N}$, $(\mathcal{E}, \mathcal{D})$ error correcting code where $\mathcal{E}\colon \{0,1\}^h \to \{0,1\}^n$.

KeyGen
- $F, G \in \mathcal{R}$ random such that $\mathsf{HW}(F) = \mathsf{HW}(G) = h$
- $R \in \mathcal{R}$ random

$$pk = (R, F \cdot R + G) = (R, T) \quad \text{and} \quad sk = F$$

Encrypt Given $m \in \{0,1\}^h$:

- generate random A, B_1, $B_2 \in \mathcal{R}$ such that $\mathsf{HW}(A) = \mathsf{HW}(B_1) = \mathsf{HW}(B_2) = h$
- $(C_1, C_2) \coloneqq (A \cdot R + B_1, (A \cdot T + B_2) \oplus \mathcal{E}(m))$

Decrypt $m = \mathcal{D}((F \cdot C_1) \oplus C_2)$

Note:

$$\begin{aligned} F \cdot C_1 =& A \cdot F \cdot R + F \cdot B_1 = A \cdot (T - G) + F \cdot B_1 \\ =& (A \cdot T + B_2) - A \cdot G - B_2 + B_1 \cdot F. \end{aligned}$$

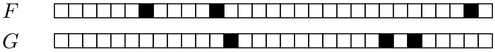
Mersenne Low Hamming Combination Search Problem (MLHCSP)

Let $p = 2^n - 1$ be an n-bit Mersenne prime, h be an integer, R be a uniformly random n-bit string and F, G having Hamming weight h. Given $(R, FR + G)$, find F, G.

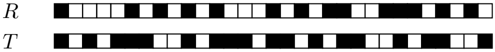
Mersenne Low Hamming Combination Search Problem (MLHCSP)

Let $p = 2^n - 1$ be an n-bit Mersenne prime, h be an integer, R be a uniformly random n-bit string and F, G having Hamming weight h. Given $(R, FR + G)$, find F, G.

$F = 2^{24} + 2^{19} + 2$ and $G = 2^{18} + 2^7 + 2^5$



$R = 2^{30} + 2^{25} + 2^{23} + 2^{21} + 2^{19} + 2^{15} + 2^{13} + 2^{11} + 2^{10} + 2^7 + 2^6 + 2^5 + 2^3 + 2$
$T = FR + G$



Weak-key Attack, Beunardeau *et al.*

Considers the lattice $\mathcal{L}$ generated by the rows of the matrix and $T = FR + G \mod p = FR + G + Kp$:

$$\begin{bmatrix} 1 & -R \\ 0 & p \end{bmatrix}$$

- $[0, T] - [F, G] = -F[1, -R] + K[0, p] \in \mathcal{L}$,
- if $F, G < \sqrt{p} \Rightarrow [0, T]$ is close to $\mathcal{L}$,
- if $F, G < \sqrt{p}$ this is a Closest Vector Problem in a lattice of dimension 2.
- This enables to recover F and G.

Weak-key Attack, Beunardeau *et al.*

Considers the lattice $\mathcal{L}$ generated by the rows of the matrix and $T = FR + G \mod p = FR + G + Kp$:

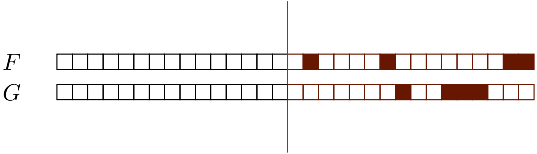
$$\begin{bmatrix} 1 & -R \\ 0 & p \end{bmatrix}$$

- $[0, T] - [F, G] = -F[1, -R] + K[0, p] \in \mathcal{L}$,
- if $F, G < \sqrt{p} \Rightarrow [0, T]$ is close to $\mathcal{L}$,
- if $F, G < \sqrt{p}$ this is a Closest Vector Problem in a lattice of dimension 2.
- This enables to recover F and G.

$$\mathcal{L}' = \begin{bmatrix} 2^{n/2} & 0 & T \\ 0 & 1 & -R \\ 0 & 0 & p \end{bmatrix}$$

- It contains a vector of norm $\simeq (\operatorname{vol} \mathcal{L}')^{1/3} \simeq 2^{\frac{n}{2}}$,
- $\|[2^{\frac{n}{2}}, F, G]\| \simeq 2^{\frac{n}{2}}$

- $\mathsf{HW}(F) = h \Rightarrow$ the probability that $F < 2^{\frac{n}{2}}$ is 2^{-h}.
- $\mathsf{HW}(G) = h \Rightarrow$ the probability that $G < 2^{\frac{n}{2}}$ is 2^{-h}.



We can recover the private key with probability 2^{-2h}.

- The previous attack is a weak key attack: recover sk from pk with probability 2^{-2h} over the public-keys.
- Beunardeau *et al.* showed that by using random partitions of the strings F and G, for any pk one can recover the secret F and G with complexity $\mathcal{O}(2^{2h})$.

Our New Attack

Assume that $m = 0$ and $\mathcal{E}(m) = 0$.

$$C_1 = A \cdot R + B_1$$
$$C_2 = A \cdot T + B_2 + \xcancel{\mathcal{E}(m)}$$

Our New Attack

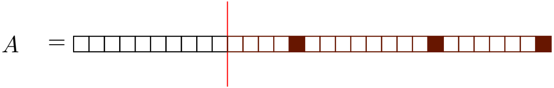
Assume that $m = 0$ and $\mathcal{E}(m) = 0$.

$$C_1 = A \cdot R + B_1$$
$$C_2 = A \cdot T + B_2 + \cancel{\mathcal{E}(m)}$$

$$\begin{bmatrix} 2^{\frac{2}{3}n} & 0 & C_1 & C_2 \\ 0 & 1 & -R & -T \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{bmatrix}$$

- $\mathcal{L}$ contains vectors of norm $\simeq (\mathrm{vol}\,\mathcal{L})^{\frac{1}{2}} \simeq 2^{\frac{2}{3}n}$,
- $\mathbf{s} = [2^{2n/3}, A, B_1, B_2] \in \mathcal{L}$,
- if $A, B_1, B_2 < 2^{\frac{2}{3}n} \Rightarrow \|\mathbf{s}\| \simeq 2^{\frac{2}{3}n}$,

- $\mathsf{HW}(A) = h \Rightarrow$ the probability that $A < 2^{\frac{2}{3}n}$ is $\left(\frac{2}{3}\right)^h$.



- $\mathsf{HW}(B_1) = h \Rightarrow$ the probability that $B_1 < 2^{\frac{2}{3}n}$ is $\left(\frac{2}{3}\right)^h$.
- $\mathsf{HW}(B_2) = h \Rightarrow$ the probability that $B_2 < 2^{\frac{2}{3}n}$ is $\left(\frac{2}{3}\right)^h$.

We can recover A, B_1, B_2 with probability $\left(\frac{2}{3}\right)^{3h}$.

Small summary

Beunardeau *et al.* weak-key attack:

- It recovers the secret key,
- $F, G < 2^{\frac{n}{2}}$,
- the probability is $\mathcal{O}(2^{-2h})$

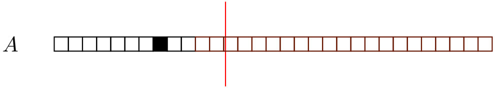
Our attack:

- It distinguishes between $m = 0$ and $m \neq 0$,
- $A, B_1, B_2 < 2^{\frac{2}{3}n}$,
- the probability is $\mathcal{O}\left(\left(\frac{2}{3}\right)^{3h}\right) \simeq \mathcal{O}(2^{-1.75h})$.

Using random partitions as in Beunardeau *et al.*, our attack complexity becomes $\mathcal{O}(2^{1.75h})$ instead of $\mathcal{O}(2^{2h})$

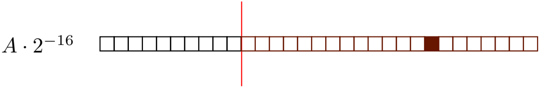
Case 1:

$n = 31$, $h = 1$. Suppose we sampled $B_1, B_2 < 2^{\frac{2}{3}n}$ and $A = 2^{23} > 2^{\frac{2}{3}n}$

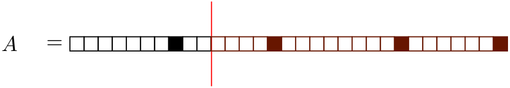


$A = 2^7 \cdot 2^{16} \Rightarrow s' = [2^{\frac{2}{3}n}, 2^7, B_1, B_2]$ is a candidate shortest vector of

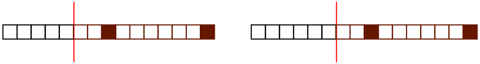
$$\begin{bmatrix} 2^{\frac{2}{3}n} & 0 & C_1 & C_2 \\ 0 & 1 & -R \cdot 2^{16} & -T \cdot 2^{16} \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{bmatrix}$$



Case 2:
Suppose $h = 4$



for any shift is not possible to recover A, B_1, B_2.
Split in 16+15 bits:



$a \to (x_1, x_2) = (129, 129)$ and

$$A = 129 \cdot 2^{16} + 129.$$

We have a representative of A of lower norm but higher dimension.

$\mathcal{L}_{\beta,P,Q,S} = \langle M_{\beta,P,Q,S} \rangle$, given $\beta \in \mathbb{Z} \setminus \{0\}$ and P, Q, S three interval-like partitions of $[n]$

$$\left[\begin{array}{c|c|cc|cc}
\beta & 0\,0\cdots 0 & 0\ \cdots\ 0 & C_1 \cdot 2^{-q_1} & 0\ \cdots\ 0 & C_2 \cdot 2^{-s_1} \\
\hline
0 & 1\,0\cdots 0 & 0\ \cdots\ 0 & -R \cdot 2^{p_k - q_1} & 0\ \cdots\ 0 & -T \cdot 2^{p_k - s_1} \\
0 & 0\,1\cdots 0 & 0\ \cdots\ 0 & -R \cdot 2^{p_{k-1} - q_1} & 0\ \cdots\ 0 & -T \cdot 2^{p_{k-1} - s_1} \\
0 & \ddots & 0\ \cdots\ 0 & -R \cdot 2^{p_2 - q_1} & 0\ \cdots\ 0 & -T \cdot 2^{p_2 - s_1} \\
0 & 0\,0\cdots 1 & 0\ \cdots\ 0 & -R \cdot 2^{p_1 - q_1} & 0\ \cdots\ 0 & -T \cdot 2^{p_1 - s_1} \\
\hline
0 & 0\,0\cdots 0 & 1\ \cdots\ 0 & -2^{q_\ell - q_1} & 0\ \cdots\ 0 & 0 \\
0 & 0\,0\cdots 0 & 0\ \ddots\ 0 & -2^{q_i - q_1} & 0\ \cdots\ 0 & 0 \\
0 & 0\,0\cdots 0 & 0\ \cdots\ 1 & -2^{q_2 - q_1} & 0\ \cdots\ 0 & 0 \\
0 & 0\,0\cdots 0 & 0\ \cdots\ 0 & p & 0\ \cdots\ 0 & 0 \\
\hline
0 & 0\,0\cdots 0 & 0\ \cdots\ 0 & 0 & 1\ \cdots\ 0 & -2^{s_j - s_1} \\
0 & 0\,0\cdots 0 & 0\ \cdots\ 0 & 0 & 0\ \ddots\ 0 & -2^{s_i - s_1} \\
0 & 0\,0\cdots 0 & 0\ \cdots\ 0 & 0 & 0\ \cdots\ 1 & -2^{s_2 - s_1} \\
0 & 0\,0\cdots 0 & 0\ \cdots\ 0 & 0 & 0\ \cdots\ 0 & p
\end{array}\right]$$

a) $\mathcal{L}_{\beta,P,Q,S}$ is full-rank lattice of dimension $d = k + \ell + j + 1$,

b) $\mathrm{vol}(\mathcal{L}_{\beta,P,Q,S}) \simeq 2^{(2+t)n}$ where $\beta = 2^{tn}$,

c) we have to ensure that structural vectors are not shorter than our target secret vector,

d) we expect the entries of the target vector to be about of the same size for a β-*lucky tuple* (P, Q, S).

a) $\mathcal{L}_{\beta,P,Q,S}$ is full-rank lattice of dimension $d = k + \ell + j + 1$,

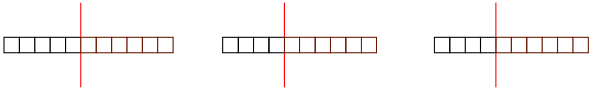
b) $\mathrm{vol}(\mathcal{L}_{\beta,P,Q,S}) \simeq 2^{(2+t)n}$ where $\beta = 2^{tn}$,

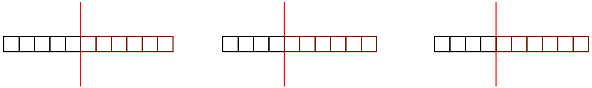
c) we have to ensure that structural vectors are not shorter than our target secret vector,

d) we expect the entries of the target vector to be about of the same size for a β-*lucky tuple* (P, Q, S).

Then $k = \ell = j$ is a good choice and in such a case

- $d = 3k + 1$
- if the norm of the target vector is less then $2^{\frac{2}{3k}n}$ we have a lucky tuple.





The success probability is roughly $(k \cdot 2n/3k \cdot 1/n)^{3h} \simeq 2^{-1.75h}$.

The number of (P, Q, S) to try before finding a lucky one is approximately

$$\mathcal{O}(2^{1.75h}).$$

h	n	$\log_2(\bar{y})$	$\log_2(\bar{Y})$
3	127	6.5	7.4
6	521	13.0	14.5
7	607	14.6	16.5
9	1279	14.9	16.4

Table : Average number $\bar{y}$ of partitions required to recover the secret values A, B_1, B_2, compared to the average number $\bar{Y}$ required for the original attack. We used 70 samples for $h = 3, 6, 7$, and 9 samples for $h = 9$.

Conclusions

- We described a variant of the Beunardeau *et al.* attack against AJPS-2, with complexity $\mathcal{O}(2^{1.75h})$ (instead of $\mathcal{O}(2^{2h})$) to break the indistinguishability of ciphertexts.
- AJPS is still a good post-quantum candidate, but it is important to work on cryptanalysis.

Conclusions

- We described a variant of the Beunardeau *et al.* attack against AJPS-2, with complexity $\mathcal{O}(2^{1.75h})$ (instead of $\mathcal{O}(2^{2h})$) to break the indistinguishability of ciphertexts.
- AJPS is still a good post-quantum candidate, but it is important to work on cryptanalysis.

Thanks for your attention!