Improved Lattice-Based Attack on Mersenne Low Hamming Ratio Search Problem

Mengce Zheng, Wei Yan

Zhejiang Wanli University; National University of Defense Technology

Sydney, Australia

July 16, 2024

Outline

1. Introduction
   1.1 Background
   1.2 Research Problem
2. Improved Attack
   2.1 Lattice
   2.2 Attack Strategy
   2.3 Success Probability
   2.4 Validating Experiments
3. Conclusion

1.1.1 BACKGROUND

AJPS Cryptosystem

- It was introduced by Aggarwal *et al.* at Crypto 2018
- A somewhat ring and noise scheme using elements of $\mathbb{Z}_p$
- Use Mersenne prime $p = 2^n - 1$ where n is a prime number

Interesting Features

- It is conjectured to resist against potential quantum attacks
- The advantage is simplicity in representation and computation
- Connection between integers modulo p and binary strings of length n

1.1.2 BACKGROUND

Key Information

- Integers in $\mathbb{Z}_p$ are mapped onto a set of n-bit strings
- Key generation involves random selection of f and g from $\mathbb{Z}_p$
- They relate to sparse binary strings with Hamming weight $w \approx \sqrt{n}$
- Another key h is defined as $f/g \pmod{p}$ ensuring g has an inverse
- It will relate to an n-bit string having an arbitrary Hamming weight

$$f,\ g \in \{0,\ 1,\ 2,\ \ldots,\ p-1\} \quad \rightleftharpoons \quad \underbrace{\cdots 0 \cdots \overbrace{1 \cdots 1 \cdots 1 \cdots 1}^{w \text{ ones}} \cdots 0 \cdots}_{n\text{-bit strings}}$$

Two Schemes

Single Bit Version

Two integers f and g each has a Hamming weight of w with a constraint $n > 4w^2$. The key pair $(\mathsf{pk}, \mathsf{sk})$ is $(h = f/g \pmod p),\ g)$.

Encryption

Choose a and b with a Hamming weight of w and encrypt one bit m through

$$c = (-1)^m \cdot (a \cdot h + b)$$

Decryption

Compute $d = \mathsf{Ham}(c \cdot g)$ and output '0' if $d \leq 2w^2$ or '1' otherwise. The core judgment is

$$c \cdot g = (-1)^m \cdot (a \cdot f + b \cdot g)$$

Two Schemes

Multiple Bits Version

Using above f, g and a random integer r modulo p leads to pk $:= (r, t) = (r, f \cdot r + g)$ and sk $:= f$. Besides, error correcting code $(\mathcal{E}, \mathcal{D})$ is required.

Encryption

Choose a, b_1, b_2 with a Hamming weight of w and encrypt multi-bit m to $(c_1, c_2) =$

$$(a \cdot r + b_1, (a \cdot t + b_2) \oplus \mathcal{E}(m))$$

Decryption

Output $\mathcal{D}((f \cdot c_1) \oplus c_2)$ as $f \cdot c_1$ and $a \cdot t + b_2$ exhibit a low Hamming distance through

$$f \cdot c_1 = (a \cdot t + b_2) - a \cdot g - b_2 + b_1 \cdot f$$

1.1.5 Hard Problems

Mersenne Low Hamming Ratio Search Problem (MLHRSP)

Consider an n-bit Mersenne prime $p = 2^n - 1$ and a positive integer w. Let f and g be two n-bit random strings characterized by a Hamming weight of w. The goal is to extract the values of f and g from the information provided by the equation $h = f/g \pmod p$ with a given h.

Mersenne Low Hamming Combination Search Problem (MLHCSP)

Consider an n-bit Mersenne prime $p = 2^n - 1$, a positive integer w, and a uniformly random n-bit string r. Let f and g be two n-bit random strings with a Hamming weight of w. The goal is to extract the values of f and g given $(r,\ t) = (r,\ f \cdot r + g \pmod p)$.

1.2.1 PREVIOUS ATTACKS

Beunardeau *et al.*'s Attack

When $f,\ g < \sqrt{p}$, $h = f/g \pmod{p}$ can be exploited to find them using a 2-dimensional lattice generated by basis matrix

$$\begin{pmatrix} 1 & h \\ 0 & p \end{pmatrix}.$$

Under Gaussian heuristic, recover a short vector (g, f) with 2^{-2w} probability.

More...

- A 3-dimensional lattice applies to the recovery of one bit m
- Similarly extending to attack on MLHCSP with $r, t = f \cdot r + g \pmod{p}$

1.2.2 Previous Attacks

Coron-Gini's Attack

It is a modified version of Beunardeau *et al.*'s attack on multi-bit AJPS and breaks the indistinguishability of ciphertexts (i.e., $m = 0$ and $m \neq 0$).

More...

- One has $\mathcal{E}(m) = 0$ for $m = 0$ and $c_1 = a \cdot r + b_1$, $c_2 = a \cdot t + b_2$
- Recovery of $a,\ b_1,\ b_2 < p^{2/3}$ through lattice reduction algorithm
- Success probability is $(2/3)^{3w} \approx 2^{-1.75w}$ outperforming original one

1.2.3 Our Contribution

Improved Lattice-Based Attack on MLHRSP

Let $p = 2^n - 1$ be an n-bit Mersenne prime and w be a positive integer. Let f and g bounded by $f \leq p^{\xi_1}$ and $g \leq p^{\xi_2}$, denote two unknown n-bit random strings with a Hamming weight of w. Given h satisfying $h = f/g \pmod p$, then f and g can be efficiently recovered if $\xi_1 + \xi_2 < 1$ (i.e., $f \cdot g < p$).

Improved Features

- Address unbalanced scenarios when $f < \sqrt{p} < g$ or $g < \sqrt{p} < f$
- Recognize unexplored advantage of lattice reduction algorithm
- Increase attack success probability from 2^{-2w} to $\sqrt{\pi}w^{3/2}/2 \times 2^{-2w}$

Lattice-Based Solving Strategy

Lattice Concepts

The set of all integer linear combinations of linearly independent vectors.

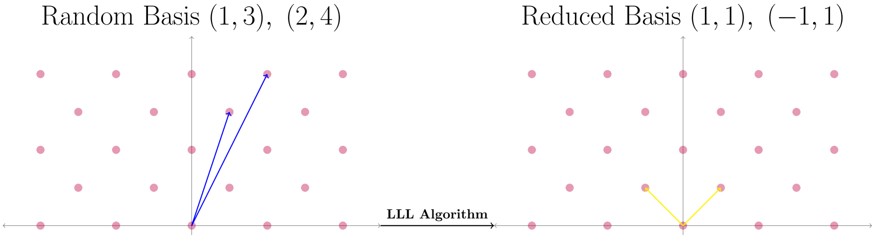
- Dimension: $\dim(\Lambda) = \omega$
- Basis vectors: $\vec{b}_1, \ldots, \vec{b}_\omega$
- Basis matrix: $B = (b_{ij})_{\omega \times \omega}$
- Determinant: $\det(\Lambda) = |\det(B)|$

$$\Lambda = \mathbb{Z}\vec{b}_1 + \cdots + \mathbb{Z}\vec{b}_\omega = \left\{ \sum_{i=1}^{\omega} z_i \vec{b}_i : z_i \in \mathbb{Z}, \vec{b}_i \in \mathbb{R}^\omega \right\}$$

Lattice-Based Solving Strategy

Lattice Reduction

- Lenstra, Lenstra, and Lovász proposed the famous LLL algorithm
- Output approximately shortest reduced vectors in polynomial time
- Lattice-based solving strategy is applied in public key cryptanalysis



2.1.3 Lattice-Based Solving Strategy

How to Find Small Modular Roots Using Lattice Reduction

1. Construct shift polynomials sharing common root modulo R
2. Transform their coefficient vectors into a lattice basis matrix B
3. Calculate short reduced vectors from ω-dimensional lattice $\Lambda(B)$
4. Transform output reduced vectors into integer equations system
5. Extract desired root over the integers using some simple methods

Asymptotic Solving Condition

$$\det(\Lambda) < R^{\omega} \quad \Longrightarrow \quad |\det(B)| < R^{\omega}$$

2.1.4 Target Modular Equation

Bivariate Equation

Derive a bivariate polynomial $f(x_1, x_2) := x_1 - hx_2$ from $h = f/g \pmod p$ and thus a bivariate modular equation:

$$f(x_1, x_2) \equiv 0 \pmod p,$$

with the root $(x_1^\star, x_2^\star) = (f, g)$. The upper bounds of desired root $(x_1^\star, x_2^\star)$ are $X_1 = p^{\xi_1}$ and $X_2 = p^{\xi_2}$ respectively.

Given parameters are as follows:

$$h, \quad p, \quad \xi_1, \quad \xi_2$$

2.2.1 Improved Strategy (1)

Shift Polynomials

Shift polynomials defined for a positive s and a non-negative i are

$$g_i(x_1, x_2) := x_2^{s-i} f^i(x_1, x_2) p^{s-i}, \quad 0 \le i \le s.$$

Therefore R indicated in the lattice-based solving strategy is p^s.

Improved Strategy

Shift Polynomials

Shift polynomials defined for a positive s and a non-negative i are

$$g_i(x_1, x_2) := x_2^{s-i} f^i(x_1, x_2) p^{s-i}, \quad 0 \leq i \leq s.$$

Therefore R indicated in the lattice-based solving strategy is p^s.

Coefficient Vectors

Transforming coefficient vectors of $g_i(X_1 x_1, X_2 x_2)$ into row vectors of B and the leading monomial of $g_i(x_1, x_2)$ is $x_1^i x_2^{s-i} p^{s-i}$.

Improved Strategy

Constructed Lattice

Regarding derived coefficient vectors as $\vec{b}_i$ for $i = 1, \ldots, \omega$ and generate

$$\Lambda = \left\{ \sum_{i=1}^{\omega} z_i \vec{b}_i : z_i \in \mathbb{Z} \right\}.$$

The lattice dimension ω is calculated as

$$\omega = \sum_{i=0}^{s} 1 = s + 1.$$

2.2.3 Improved Strategy (3)

Toy Example

$$
\begin{array}{c|ccc}
 & x_2^2 & x_1x_2 & x_1^2 \\
\hline
g_0 & p^2X_2^2 & 0 & 0 \\
g_1 & -hpX_2^2 & pX_1X_2 & 0 \\
g_2 & h^2X_2^2 & -2hX_1X_2 & X_1^2
\end{array}
$$

Improved Strategy

Toy Example

$$
\begin{array}{c|ccc}
 & x_2^2 & x_1x_2 & x_1^2 \\
\hline
g_0 & p^2X_2^2 & 0 & 0 \\
g_1 & -hpX_2^2 & pX_1X_2 & 0 \\
g_2 & h^2X_2^2 & -2hX_1X_2 & X_1^2
\end{array}
$$

Lattice Reduction

Matrix diagonals are $X_1^i X_2^{s-i} p^{s-i}$ for $0 \le i \le s$ and $\det(\Lambda) = p^{s_p} X_1^{s_1} X_2^{s_2}$ for $s_p = s_2 = \sum_{i=0}^{s}(s-i) = s(s+1)/2$ and $s_1 = \sum_{i=0}^{s} i = s(s+1)/2$.

Improved Strategy

Attack Bound

The solving condition $\det(\Lambda) < R^{\omega}$ with $R = p^s$ yields

$$(pX_1X_2)^{\frac{s(s+1)}{2}} < p^{s\cdot(s+1)}.$$

Simplify the exponents over p and obtain

$$\frac{1}{2} \cdot (1 + \xi_1 + \xi_2) < 1,$$

It further leads to

$$\boxed{\xi_1 + \xi_2 < 1, \quad (f \cdot g < p.)}$$

2.3.1 SUCCESS PROBABILITY

Previous Success Probability

Given f, g are both less than $\sqrt{p}$, namely their w many '1' bits are chosen from low $\lfloor n/2 \rfloor$ bits, the expression for Pr_1 is calculated as

$$\begin{aligned}\mathsf{Pr}_1 &= \frac{\binom{\lfloor n/2 \rfloor}{w}\binom{\lfloor n/2 \rfloor}{w}}{\binom{n}{w}\binom{n}{w}} \\ &= \left(\frac{\lfloor n/2 \rfloor!(n-w)!}{n!(\lfloor n/2 \rfloor - w)!}\right)^2 \\ &\approx 2^{-2w}.\end{aligned}$$

2.3.2 Success Probability

Our Success Probability

The w many '1' bits are chosen in a wider range and our Pr_2 is calculated as

$$\begin{aligned}
\mathrm{Pr}_2 &= \sum_{t=w}^{n-w} \frac{\binom{t}{w}\binom{n-t}{w}}{\binom{n}{w}\binom{n}{w}} = \frac{\binom{n+1}{2w+1}}{\binom{n}{w}\binom{n}{w}} \\
&= \frac{\binom{n+1}{2w+1}}{\binom{\lfloor n/2 \rfloor}{w}\binom{\lfloor n/2 \rfloor}{w}} \cdot \mathrm{Pr}_1 \\
&\approx \frac{\sqrt{\pi}}{2} w^{\frac{3}{2}} \cdot 2^{-2w} = \sqrt{\pi} w^{3/2} 2^{-2w-1}.
\end{aligned}$$

2.4. Experimental Results

Experiment Details

- Performed on a laptop computer running Ubuntu 22.04
- Conducted using `SageMath` mathematics software system
- Chose random parameters for generating experimental instances
- Provided source code at `https://github.com/MengceZheng/MLHRSP`

Time Comparison

- $n = 521, w = 10$: our improved attack succeeded in ≈ 0.2 s
- $n = 4253, w = 30$: our improved attack succeeded in ≈ 48 s
- $n = 11213, w = 50$: our improved attack succeeded in ≈ 2900 s

3. Conclusion

Improvements

- Expand vulnerable private key range and find more weak keys
- Increase success probability by considering unbalanced attack cases

Limitation

- Discard and resample f, g again if both of them fall within attack range

Future Work

- Explore how to incorporate a similar random partition technique
- Extend such improved lattice-based attack on MLHRSP to MLHCSP

Mengce Zheng

Sydney, Australia, July 16, 2024

mengce.zheng@gmail.com