Attacking ECDSA with Nonce Leakage by Lattice Sieving: Bridging the Gap with Fourier Analysis-based Attacks

Yiming Gao, Jinghui Wang, Honggang Hu and Binang He

University of Science and Technology of China

gym_2001@mail.ustc.edu.cn

December 10, 2024

Outline

1. Introduction
   - Contributions
2. Preliminaries
   - Lattice and Heuristic
   - ECDSA as HNP Instance
   - Solving HNP with Lattices
3. Improved Algorithms
   - New Lattice Construction
   - Improve Linear Predicate
   - Predicate for New Lattice
4. Hidden Number Problem with Erroneous Input
   - Theoretical Analysis
   - Modified Algorithms
5. Experiment
   - Compared with Other Lattice-based Attacks
   - New Records of Lattice-based Attack against ECDSA

Outline

1. Introduction
   - Contributions
2. Preliminaries
   - Lattice and Heuristic
   - ECDSA as HNP Instance
   - Solving HNP with Lattices
3. Improved Algorithms
   - New Lattice Construction
   - Improve Linear Predicate
   - Predicate for New Lattice
4. Hidden Number Problem with Erroneous Input
   - Theoretical Analysis
   - Modified Algorithms
5. Experiment
   - Compared with Other Lattice-based Attacks
   - New Records of Lattice-based Attack against ECDSA

Introduction to the Hidden Number Problem (HNP)

Background and Applications

- Investigate bit security of Diffie-Hellman
- Analyze the security of ECDSA with partial known nonce leakage

Algorithmic Approaches to Solving HNP

Lattice-based Attacks

- Better efficiency
- Fewer samples
- Perform poorly with hard instance and noisy data

Fourier Analysis-based Attacks

- Difficult instances, including erroneous input
- Larger sample size and computational time

Introduction

Key Questions

- Can lattice-based attacks be enhanced by utilizing more samples?
- Is there a smooth tradeoff that can be characterized between lattice-based and Fourier analysis-based algorithms?

A Solution

- Utilize more samples to improve lattice attack
- Address the case of 1-bit leakage and less than 1-bit leakage on a 160-bit curve

Main Contributions

Improved Algorithms for Solving the HNP

1. Use more samples to construct new lattice with a new parameter x, offering a dimension reduction of approximately $(\log_2 x)/l$
2. Prove the existence of a constant $c > 0$ which serves as a lower bound for the success probability of our algorithm
3. Propose an improved linear predicate with higher efficiency and prove its correctness
4. Design an interval reduction algorithm with expected time complexity $O(\log^2 x)$ instead of an exhaustive search complexity $O(x)$
5. Present a pre-screening technique to pre-select candidates

Main Contributions

Modified Algorithms for Handling Errors

1. Define HNP with erroneous input to handle practical scenarios in side-channel attacks
2. Demonstrate the effectiveness of our lattice construction, which offers a greater reduction in lattice dimension of more than $\log_2 x/l$
3. Extend our new algorithms and techniques for solving the HNP to address the case of erroneous input

New Records of Lattice-based Attacks against ECDSA

Recover the key for the ECDSA instance with 1-bit leakage and less than 1-bit on a 160-bit curve.

Comparison with Related Work

Table: Lattice-based Attacks Against ECDSA with Nonce Leakage

	Nonce leakage				
Modulus	4-bit	3-bit	2-bit	1-bit	<1-bit
112-bit	-	-	-	[2], Ours(faster)	Ours
128-bit	-	-	-	Ours	Ours
160-bit	-	-	[1,3]	Ours	Ours
256-bit	[1]	[1,3]	[2], Ours	-	-
384-bit	[1,3]	[2], Ours	-	-	-
512-bit	Ours	-	-	-	-

[1] On bounded distance decoding with predicate: Breaking the "lattice barrier" for the hidden number problem. (EUROCRYPT 2021)

[2] Improved attacks on (EC)DSA with nonce leakage by lattice sieving with predicate. (CHES 2023)

[3] Guessing bits: Improved lattice attacks on (EC)DSA with nonce leakage. (CHES 2022)

Outline

1. Introduction
   - Contributions
2. Preliminaries
   - Lattice and Heuristic
   - ECDSA as HNP Instance
   - Solving HNP with Lattices
3. Improved Algorithms
   - New Lattice Construction
   - Improve Linear Predicate
   - Predicate for New Lattice
4. Hidden Number Problem with Erroneous Input
   - Theoretical Analysis
   - Modified Algorithms
5. Experiment
   - Compared with Other Lattice-based Attacks
   - New Records of Lattice-based Attack against ECDSA

Lattice and Heuristic

- Let vectors $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_d\}$ be linearly independent row vectors in $\mathbb{Z}_d$, a full rank lattice $\mathcal{L}$ with basis vectors $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_d\}$ is

$$\mathcal{L} = \left\{ \sum_{i=1}^{d} k_i \mathbf{b}_i, k_i \in \mathbb{Z} \right\}$$

- The volume of the lattice is $\mathrm{Vol}(\mathcal{L}) = |\det(B)|$, where $B = [\mathbf{b}_1, \ldots, \mathbf{b}_d]^T$ is a basis matrix.

Gaussian Heuristic

The expected minimum vector length of a lattice $\mathcal{L}$ according to the Gaussian Heuristic, denoted by $\mathrm{GH}(\mathcal{L})$ is given by

$$\mathrm{GH}(\mathcal{L}) = \left(\Gamma\left(\frac{d}{2} + 1\right) \cdot \mathrm{Vol}(\mathcal{L}) \right)^{\frac{1}{d}} / \sqrt{\pi} \approx \sqrt{d/(2\pi e)} \cdot \mathrm{Vol}(\mathcal{L})^{\frac{1}{d}}$$

Lattice and Heuristic

Lattice Sieving

- Fastest SVP solving algorithm when lattice dimension > 70
- Output a database rather than a single vector

Assumption 1

When a 2-sieve algorithm terminates, it outputs a database L containing all vectors with norm $\leq \sqrt{4/3}\,\mathrm{GH}(\mathcal{L})$.

ECDSA as HNP Instance

Definition: HNP

Given an n-bit sized public modulu q, and there is a secret integer $\alpha \in \mathbb{Z}_q$, referred to the hidden number. For $i = 0, 1, \ldots, m-1$, t_i are uniformly random integers in $\mathbb{Z}_q$, and we are provided with the corresponding value a_i such that

$$|t_i \cdot \alpha - a_i|_q = k_i < q/2^l$$

The problem is to recover the hidden number α when m samples (t_i, a_i) are given.

- In a side-channel attack against ECDSA, the adversary may know l least significant bits of the nonce k
- ECDSA with nonce leakage can be regarded as a HNP instance

Sieving with Predicate

At EUROCRYPT 2021, Albrecht and Heninger extended the applicability of lattice-based attacks with their Sieving with Predicate (Sieve-Pred) algorithm.

Sieving with Predicate

1. Construct a lattice which may contains a short vector with the hidden number
2. Run lattice sieving algorithm and obtain a database full of short vectors
3. Run predicate algorithm (check if it is correct) on these vectors

- Albrecht and Heninger consider the expected squared norm $\mathbb{E}[\|\boldsymbol{v}\|^2]$
- The minimal lattice dimension can be estimated as the minimal integer d satisfying $\mathbb{E}\left[\|\boldsymbol{v}\|^2\right] \leq 4\,\mathrm{GH}^2(\mathcal{L})/3$.

Previous Lattice Construction

Albrecht and Heninger construct their lattice with recentering technique and elimination method:

$$\begin{bmatrix} q & 0 & \cdots & 0 & 0 & 0 \\ 0 & q & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & q & 0 & 0 \\ t'_1 & t'_2 & \cdots & t'_{m-1} & 1 & 0 \\ a'_1 & a'_2 & \cdots & a'_{m-1} & 0 & \tau \end{bmatrix}$$

- The target lattice vector becomes $\boldsymbol{v} = \pm(k'_1, \ldots, k'_{m-1}, k'_0, -\tau)$
- k'_0 is the new hidden number

Outline

1 Introduction
Contributions
2 Preliminaries
Lattice and Heuristic
ECDSA as HNP Instance
Solving HNP with Lattices
3 Improved Algorithms
New Lattice Construction
Improve Linear Predicate
Predicate for New Lattice
4 Hidden Number Problem with Erroneous Input
Theoretical Analysis
Modified Algorithms
5 Experiment
Compared with Other Lattice-based Attacks
New Records of Lattice-based Attack against ECDSA

New Lattice Construction

Main Idea

- In a large list of HNP samples (a'_i, t'_i), some samples have small t'_i
- Construct a new lattice using these samples:
  - Larger lattice determinant
  - Target vector norm remains (roughly) unchanged
- Enables dimension reduction while satisfying the attack condition: $\mathbb{E}\left[\|\boldsymbol{v}\|^2\right] \le 4\,\mathrm{GH}^2(\mathcal{L})/3$

Impact of Dimension Reduction

- State-of-the-art sieving algorithm for d-dimensional lattices: $2^{0.292d}$ time complexity
- Reducing lattice dimension significantly improves algorithm efficiency

New Lattice Construction

Hidden Number Decomposition

Motivated by Sun et al. [SETA22], we decompose the hidden number k_0' as $x \cdot \alpha_0 + \alpha_1$

New lattice:

$$\begin{bmatrix} q & 0 & \cdots & 0 & 0 & 0 \\ 0 & q & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & q & 0 & 0 \\ x \cdot t_1' & x \cdot t_2' & \cdots & x \cdot t_{m-1}' & y & 0 \\ a_1' & a_2' & \cdots & a_{m-1}' & 0 & \tau \end{bmatrix}$$

Samples Requirement

- Condition: $|t_i'| \leq q/(2^{l+4}x)$
- Cost: $2^{l+3}x$ times the original number of samples

New Lattice Construction

Advantage of Our Lattice Construction

- Larger lattice determinant
- Target vector norm remains (roughly) unchanged

Theorem 1: Lattice Dimension Reduction

For any positive integer x and the number of leaked bits l, the reduction of lattice dimension between our lattice and Albrecht and Heninger's lattice is given by

$$\frac{2\log x}{2l+3-\log(\pi e)} \approx \frac{\log x}{l}.$$

Success Probability Analysis

Our Work

- Theoretically analyzed success probability
- Proved a constant lower bound c under Assumption 1

Under Assumption 1, $\Pr(\|\boldsymbol{v}\|^2 \leq \mathbb{E}\left[\|\boldsymbol{v}\|^2\right])$ is the success probability of our algorithm.

Theorem 2: Lower Bound of Success Probability

Let $\boldsymbol{v}$ be the target vector of our lattice. For all $d \geq 3$, there exists a constant $c > 0$ such that $\Pr(\|\boldsymbol{v}\|^2 \leq \mathbb{E}\left[\|\boldsymbol{v}\|^2\right]) \geq c$.

Improve Linear Predicate

Predicate Algorithm

Purpose: To check if the candidate vector is correct.

Previous Predicates

- EUROCRYPT 2021 (Albrecht and Heninger):
  - Non-linear constraints
  - Time-consuming scalar multiplication on elliptic curves
- CHES 2023 (Xu et al.):
  - Linear predicate
  - Claimed higher efficiency than non-linear predicate

Improve Linear Predicate

Overview of Our Predicate

1. Operates on a 2-dimensional vector $\boldsymbol{v} = (v_0, v_1)$
2. Determines if the candidate vector satisfies linear conditions $|t_i \cdot \alpha' - a_i|_q < q/2^l$
3. If all conditions met, reveals hidden number; else, returns $\perp$

Improvements Compared to Xu's Predicate

- Use only the last two elements of a candidate vector
  - Avoid unnecessary vector inner products
- HNP samples used in step (2) are distinct from lattice construction samples
  - Inherently shorter vector $\boldsymbol{v}$ in sieving database
- Correct Xu's linear constraint, which is actually an identical equation

Predicate for New Lattice

Lattice Properties

- Transformed hidden number k_0' is decomposed as:

$$k_0' = \alpha_0 x + \alpha_1 \quad \text{where} \quad |\alpha_1| \leq x/2$$

- Target vector in our lattice only contains information about α_0

New Predicate Requirements

- Input: candidates of α_0
- Output: k_0' or $\perp$

Straightforward Approach

- Exhaustive search over all possible values of α_1
- Time complexity: $O(x)$
- Impractical for large x

Predicate for Our New Lattice

Our Proposed Solution

- Interval reduction algorithm
- Reduce complexity from $O(x)$ to $O(\log^2 x)$
- Predicate for New Lattice

Interval Reduction Algorithm

- Input: interval $[\mathrm{low}, \mathrm{high}]$ that may contain the hidden number k_0'
- Output: A set of intervals
- Then do exhaustive search on those intervals

Theorem 3: Predicate for New Lattice

The expected time complexity of Predicate for New Lattice is $O(\log^2 x)$.

Pre-screening Technique

Overview

- Eliminate majority of incorrect candidates before running interval reduction algorithm
- Involves only a few linear operations

Efficiency Improvements

- Does not increase sampling cost
- Experiment on HNP$(256, 2)$ with $x = 2^{15}$:
  - Interval reduction algorithm: 2590-fold speedup compared to exhaustive search
  - Combined with pre-screening technique: 3895-fold speedup

Outline

1. Introduction
    - Contributions
2. Preliminaries
    - Lattice and Heuristic
    - ECDSA as HNP Instance
    - Solving HNP with Lattices
3. Improved Algorithms
    - New Lattice Construction
    - Improve Linear Predicate
    - Predicate for New Lattice
4. Hidden Number Problem with Erroneous Input
    - Theoretical Analysis
    - Modified Algorithms
5. Experiment
    - Compared with Other Lattice-based Attacks
    - New Records of Lattice-based Attack against ECDSA

Handling Errors in Side-Channel Attacks

Challenges and Limitations for Lattice Attacks

- Errors in side-channel attacks lead to erroneous HNP samples
- Lattice-based attacks perform poorly with erroneous input
- Some works just assume error-free input
- Existing solutions lack detailed analysis and have limitations:
  - Rapid increase in lattice dimension with increasing error rate
  - non-linear predicate leads to high cost for searching sieving database

Comparison with Fourier Analysis-based Attacks

- Fourier analysis-based attacks demonstrate stronger robustness to errors
- Highlights a gap between lattice-based and Fourier-based approaches

Handling Errors in Side-Channel Attacks

Our Contributions

- Define HNP with erroneous input based on ECDSA nonce leakage model
- Demonstrate effectiveness of our new lattice construction
- Extend algorithms to enhance lattice's ability to handle errors
    - Linear predicate and pre-screening technique extended to handle erroneous input by calculating passing probability
    - Subsampling technique designed to guarantee interval reduction algorithm works in this case

As a result, we significantly narrow the gap between lattice-based attacks and Fourier analysis-based attacks

Theoretical Analysis

Definition of HNP with Erroneous Input

- Derived from ECDSA nonce leakage with errors
- Probability $1 - p$: obtain the correct value of k_{lsb}
- Probability p: obtain a random integer k'_{lsb} in $[0, 2^l - 1]$
- In the resulting HNP instance:
  - With probability $1 - p$: $|t_i\alpha - a_i|_q < q/2^l$
  - With probability p: $|t_i\alpha - a_i|_q$ is a random number in $\mathbb{Z}_q$

Lattice Construction

- same as before
- $\mathbb{E}\left[\|\boldsymbol{v}\|^2\right]$, τ changes with p

Effectiveness of Our Lattice Construction

Dimension Reduction

The lattice dimension compared to AH21 is reduced by

$$\frac{2\log x}{2l + 3 - \log(\pi e) - \log(1 + p \cdot (2^{2l} - 1))}$$

which is larger than that in Theorem 1.

Balancing Error Rate and Lattice Dimension

- The parameter x can be viewed as a balance to the error rate p
- p amplifies the target vector's squared magnitude by $1 + p(2^{2l} - 1)$
- x amplifies $\mathrm{GH}^2(\mathcal{L})$ by $x^{2/d}$
- For a higher error rate, increase x to keep the lattice dimension unchanged

Linear Predicate for Erroneous Input

Testing Hidden Number Candidates

- Compute $|t_i\alpha' - a_i|_q$ for each HNP sample (t_i, a_i) and candidate α'
- α' passes if the value is in $[0, q/2^l)$, fails otherwise
- With errors, a single failed test doesn't necessarily imply an incorrect candidate

Extended Linear Predicate

1. Collect $N = 2\log q$ samples
2. Count the number of passed samples M for α'
3. p_1: passing probability for $\alpha' = \alpha$; p_2: passing probability for $\alpha' \neq \alpha$
4. If $M > N(p_1 + p_2)/2$, conclude $\alpha' = \alpha$; otherwise, discard α'

Linear Predicate for Erroneous Input

Theorem 4: Correctness of Predicate for Erroneous Input

Our Predicate for Erroneous Input has an overwhelming success probability $1 - \mathrm{negl}(\log q)$.

Proof Sketch

We prove that both the probability of rejecting a correct hidden number (P_1) and accepting an incorrect candidate (P_2) are negligible:

- Define random variables X_i to represent whether a candidate α' passes the i-th sample.
- For P_1: Apply Chernoff bound to the sum $S_N = \sum_{i=1}^{N} X_i$ and show P_1 is exponentially small in $\log q$.
- For P_2: Similarly apply Chernoff bound to S_N with different parameters and show P_2 is also exponentially small in $\log q$.

Enhanced Pre-screening Technique for Erroneous Input

Pre-screening of Errorfree Input

- Use $\log q$ samples that satisfy $|t_i'| < q/(2^{l+3}x)$
- Compute $\left| |xt_i'\alpha_0 - a_i' + q/2|_q - q/2 \right|$ for each sample (t_i', a_i')
- A sample is non-compliant if the computed value exceeds $w + q/2^{l+4}$

Decision Strategy

- Goal: retain the correct hidden numbers, rather than eliminating all incorrect candidates
- Collect a set of samples instead of making a decision based on a single non-compliant sample
- Discard the hidden number candidate if more than threshold value samples are non-compliant

Sub-sampling Technique for Erroneous Input

Motivation

- The interval reduction algorithm requires error-free samples
- It may exclude the correct candidate with erroneous samples

Sub-sampling Technique Steps

1. Select $3 \log x/2$ samples to form a pool
2. Draw $\log x$ samples from the pool and apply interval reduction algorithm to the candidate α_0'
3. Repeat step 2 for γ times. If the hidden number is not found, reject the candidate

We could set success probability close to 1 by choosing parameter.

Outline

1. Introduction
    - Contributions
2. Preliminaries
    - Lattice and Heuristic
    - ECDSA as HNP Instance
    - Solving HNP with Lattices
3. Improved Algorithms
    - New Lattice Construction
    - Improve Linear Predicate
    - Predicate for New Lattice
4. Hidden Number Problem with Erroneous Input
    - Theoretical Analysis
    - Modified Algorithms
5. Experiment
    - Compared with Other Lattice-based Attacks
    - New Records of Lattice-based Attack against ECDSA

Key Recovery of ECDSA with Nonce Leakage

Implementation Enhancements

- Source code: https://github.com/JinghuiWW/ecdsa-leakage-attack
- Based on lattice sieving in g6k
- Preprocessing the lattice basis with BKZ-20

Classification of ECDSA Instances

- Instances are categorized into three classes based on the minimum lattice dimension d estimated via Albrecht and Heninger's lattice
  - Easy ($d \leq 100$)
  - Medium ($100 < d \leq 140$)
  - Hard ($d > 140$)
- x can be adjusted to achieve an optimal balance between time consumption and the number of available samples

Compared with Other Lattice-based Attacks

Curve	Leakage	d	x	CPU-seconds	s/r	Previous records
secp160r1	2	82	1	206s	52%	259s
		77	2^{10}	71s	58%	
secp192r1	2	99	1	10360s	60%	87500s
		94	2^{10}	2829s	69%	
secp256r1	4	66	1	7s	65%	15s
		64	2^{10}	5s	79%	
	3	87	1	634s	53%	924s
		84	2^{10}	359s	57%	
secp384r1	4	98	1	8154s	62%	11153s
		96	2^{10}	5583s	56%	

Table: Easy instances

Compared with Other Lattice-based Attacks

Curve	Leakage	d	x	Wall time	Mem GiB	Previous records
secp112r1	1	116	1	6min	35	260min
secp256r1	2	129	1	95min	219	466min
		124	2^{10}	31min	114	
secp384r1	3	130	1	128min	252	156min
		125	2^{15}	39min	132	

Table: Medium instances

New Records of Lattice-based Attack against ECDSA

4-bit Leakage

- Previous record: only achieved on a 384-bit curve
- Our algorithm: breaks ECDSA$(512, 4)$ using a 130-dimensional lattice

1-bit Leakage

- Previous lattice approaches: breaking ECDSA$(160, 1)$ considered exceptionally challenging
- Our work: first lattice attack on both 160-bit and 128-bit curves

Less than 1-bit Leakage

- Previous state-of-the-art: only Fourier-based attacks could handle less than 1-bit leakage
- Our work: first lattice-based attack results

New Records

Curve	Leakage	d	x	Samples	Wall time	Mem GiB
secp128r1	1	131	1	2^8	72min	294
		118	2^{15}	2^{26}	8min	53
secp160r1	1	144	2^{14}	2^{25}	824min	1939
		138	2^{25}	2^{36}	279min	850

(a) 1-bit leakage

Curve	Error rate	d	x	Samples	Wall time	Mem GiB
secp128r1	0.1	140	2^{20}	2^{31}	370min	1090
secp160r1	0.02	144	2^{14}	2^{25}	1009 min	1960

(b) Less than 1-bit leakage

Thanks for listening!