A Secure and Efficient Implementation of the FALCON BaseSampler Against Side-Channel Attack

Hyunseo Choi
Dept. of Electronic Engineering
Hanyang University
Seoul, Republic of Korea
hyun123456a@hanyang.ac.kr

Jaesang Noh
Dept. of Electronic Engineering
Hanyang University
Seoul, Republic of Korea
darkelzm@hanyang.ac.kr

Seunghwan Lee
Dept. of Electronic Engineering
Hanyang University
Seoul, Republic of Korea
kr3951@hanyang.ac.kr

Dong-Joon Shin
Dept. of Electronic Engineering)
Hanyang University
Seoul, Republic of Korea
djshin@hanyang.ac.kr

***Abstract*—With the advent of quantum computing threatening the existing public-key cryptosystems, the U.S. National Institute of Standards and Technology (NIST) has been leading the standardization effort for Post-Quantum Cryptography. FALCON, one of the digital signature algorithms selected in this process, is notable for its high efficiency. However, its core component, the BaseSampler, is known to be vulnerable to Simple Power Analysis (SPA).**

In this paper, we propose a new implementation method of the FALCON BaseSampler to counteract this vulnerability. Our approach involves modifying the existing RCDT and altering the specific operation that causes an underflow. Through practical experiments conducted with ChipWhisperer and Cortex-M4 board, we verify that the proposed countermeasure effectively establishes robustness against the known vulnerability.

***Index Terms*—Post-Quantum Cryptography, FALCON Side-Channel Attack, Countermeasure.**

I. Introduction

The advent of quantum computing, particularly with the development of Shor's algorithm, has compromised the security of traditional public-key cryptosystems like RSA and Elliptic Curve Cryptography (ECC). [1] To address this critical vulnerability, the U.S. National Institute of Standards and Technology (NIST) is spearheading a global effort to develop and standardize new cryptographic algorithms that are resistant to quantum attacks. [2]

Among the algorithms selected through this rigorous process is FALCON [3], a digital signature scheme that is poised for future standardization. FALCON is gaining significant attention within the cryptographic community, primarily due to its exceptional efficiency and the remarkably compact size of its signatures and public keys, making it a highly promising solution for the post-quantum era.

However, even when a cryptographic algorithm is theoretically secure, its practical implementation can be vulnerable to side-channel attacks, which exploit physical information leakage like power consumption. FALCON provides a clear example of this vulnerability; a weakness has been identified through power analysis of its BaseSampler, a fundamental component for the Gaussian sampling in the signature generation process [4].

In this paper, we introduce a novel implementation of the FALCON BaseSampler for counteracting this side-channel attack. Furthermore, we substantiate the security of the proposed countermeasure through practical simulations conducted using the ChipWhisperer platform.

II. Side-Channel Vulnerability of FALCON BaseSampler

Algorithm 1: FALCON BaseSampler

Output: $z^+ \in \{0, \cdots, 18\}$
1 u←UniformBits(72)
2 $z^+ \leftarrow 0$
3 **for** $i \leftarrow 0, \cdots, 17$ **do**
4 $\quad z^+ \leftarrow z^+ + [\![u < \text{RCDT}[i]]\!]$
5 **end**
6 **return** z^+

The BaseSampler is structured as shown in Algorithm 1, where $[\![N]\!]$ denotes 1 if the condition is true and 0 otherwise. The critical part to focus on is the comparison operation in line 4. This comparison is implemented as a subtraction, which causes an underflow when the comparison condition is true. This underflow makes the eight most significant bits (MSBs) in register flipped to all ones. Conversely, when the comparison condition is false, no such change occurs. This discrepancy in behavior directly affects the power waveform, allowing an

attacker to determine with high probability whether z^+ is zero through Simple Power Analysis (SPA). By leveraging this leaked information about $z^+ = 0$, an attacker can filter a large number of signatures and ultimately recover the private key using the hidden parallelpiped attack [4].

III. Countermeasure

As discussed in Section 2, the FALCON BaseSampler has a vulnerability such that a difference in the power waveform is caused by an underflow. To mitigate this vulnerability, we have designed the following countermeasure.

First, we modify the existing RCDT to the new version shown in Table I. Subsequently, the original code is changed to adopt the new addition operation, as detailed in the pseudocode in Algorithm 2. This design ensures that the output is identical to the original implementation, ensuring that a 1-bit overflow occurs when $u < \text{RCDT}[i]$ is false, while no overflow occurs when it is true.

Algorithm 2: Pseudocode of BaseSampler Countermeasure

Output: $z^+ \in \{0, \cdots, 18\}$

$u \leftarrow$UniformBits(72)
$z^+ \leftarrow 18$
for $i \leftarrow 0, \cdots, 17$ **do**
  $u \leftarrow u + \text{RCDT}[i]$
  $u \leftarrow u >> 24$
  $z^+ \leftarrow z^+ - u$
end
return z^+

TABLE I
FALCON RCDT Modified For Countermeasure

6031371	13708370	13035516
11218132	15196351	8529020
14516786	3108022	14040575
16068234	12355639	6731034
16607867	9654539	12640399
16746677	3713809	9126559
16773083	2272211	8951066
16776798	9113	5413924
16777184	8333172	8690646
16777214	3932748	16511893
16777215	15544538	3132931
16777215	16739167	7665375
16777215	16776344	10638950
16777215	16777200	4231491
16777215	16777214	13673088
16777215	16777214	16748390
16777215	16777214	16777016
16777215	16777214	16777213

IV. Experiment

To confirm the effectiveness of the proposed countermeasure, an experiment is conducted by measuring the power waveforms of the BaseSampler. The power traces were captured using ChipWhisperer and a Cortex-M4 board.

First, 10,000 traces are collected using the original FALCON BaseSampler. Upon calculating the correlation between the traces with $z^+ = 0$ and the remaining traces, we can see a significant correlation spike in the initial sample points, as depicted by the solid line in Fig 1. However, when our countermeasure is applied, the correlation (shown as the dashed line) is relatively stable across all sample points compared to the original, which shows its robustness against SPA.

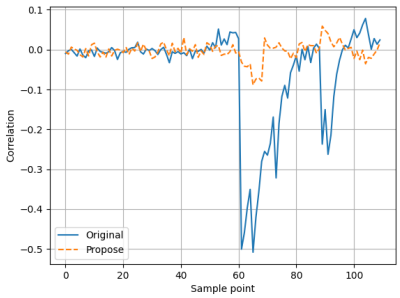

Fig. 1. Correlation Comparison of FALCON BaseSamplers

V. Conclusion

In FALCON BaseSampler, the subtraction implemented for the comparison operation causes an 8-bit underflow. This creates a significant difference in the power waveform between power traces with $z^+ = 0$ and all others, resulting in a vulnerability to power analysis. To address this issue, a countermeasure is proposed, which modifies the RCDT and replaces the subtraction with addition. It is confirmed that the proposed method effectively reduces the correlation between the power traces.

This research demonstrates that by slightly modifying the FALCON BaseSampler, it is possible to achieve robustness against SPA while producing identical output values. Furthermore, by verifying its robustness with an actual low-end ChipWhisperer, we are able to show the practical effectiveness of this countermeasure.

Acknowledgment

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. RS-2024-00409492)

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.
[2] G. Alagic, G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, C. Miller, *et al.*, "Status report on the third round of the nist post-quantum cryptography standardization process," 2022.
[3] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang, *et al.*, "Falcon: Fast-fourier lattice-based compact signatures over ntru," *Submission to the NIST's post-quantum cryptography standardization process*, vol. 36, no. 5, pp. 1–75, 2018.
[4] M. Guerreau, A. Martinelli, T. Ricosset, and M. Rossi, "The hidden parallelepiped is back again: Power analysis attacks on falcon," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 141–164, 2022.