Masked Computation of the Floor Function and Its Application to the FALCON Signature

Pierre-Augustin Berthet[1,3][0009−0005−5065−2730], Justine Paillet[2,3][0009−0009−6056−7766], and Cédric Tavernier[3][0009−0007−5224−492X]

[1] Télécom Paris, Palaiseau, France, berthet@telecom-paris.fr
[2] Université Jean-Monnet, Saint-Étienne, France,
justine.paillet@univ-st-etienne.fr
[3] Hensoldt SAS FRANCE, Plaisir, France,
<pierre-augustin.berthet,justine.paillet,cedric.tavernier>@hensoldt.net

Abstract. With the ongoing standardization of new POst-Quantum Cryptography (PQC) primitives by the National Institute of Standards and Technology (NIST), it is important to investigate the robustness of new designs to Side Channel Analysis (SCA). Amongst those future standards is Falcon, a lattice-based signature which relies of rational numbers. It thus requires an implementation using floating point arithmetic, which is harder to design well and secure. While recent work proposed a solution to mask the addition and the multiplication, some roadblocks remains, most noticeably how to protect the floor function. In this work we propose several method to protect the computation of the floor function. We provide mathematical proofs of our methods as well as formal security proof. We also discuss their application to the FALCON Signature.

Keywords: Floor Function · Floating-Point Arithmetic · Post-Quantum Cryptography · FALCON · Side-Channel Analysis · Masking

1 Introduction

With the rise of quantum computing, mathematical problems which were hard to solve with current technologies will be easier to breach. Amongst the concerned problem is the Discrete Logarithm Problem (DLP) which can be solved in polynomial times by the Shor quantum algorithm [21]. As much of the current asymmetric primitives rely on this problem and will be breach, new cryptographic primitves are studied. The National Institute of Standards and Technology (NIST) launched a post-quantum standardization process [5]. The finalists are CRYSTALS-Kyber [3,16], CRYSTALS-Dilithium [6,15], SPHINCS+ [2,17] and FALCON [19].

Another concern for the security of cryptographic primitives is their robustness to a Side-Channel opponent. Side-Channel Analysis (SCA) was first introduced by Paul Kocher [13] in the mid-1990. This new branch of cryptanalysis focuses on studying the impact of a cryptosystem on its surroundings. AS computations take time and energy, an opponent able of accessing the variation of one or both could find correlations between its physical observations and the data manipulated, thus resulting in a leakage and a security breach. Thus, the study of weaknesses in implementations of new primitives and the ways to protect them is an active field of research.

While they have been many works focusing on CRYSTALS-Dilithium and CRYSTALS-Kyber, summed up by Ravi et al. [20], FALCON is noticeably harder to protect. Indeed, the algorithm relies on floating-point arithmetic, for which there is little litterature on how to protect it.

Related Work Previous works have identified two main weaknesses within the signing process of Falcon : the pre-image computation and the Gaussian sampler. The pre-image computation was proved vulnerable by Karabulut and Aysu [12] using an ElectroMagnetic (EM) attack. Their work was later improved by Guerreau et al. [10]. To counter those attacks, Chen and Chen [4] propose a masked implementation of the addition and multiplication of FALCON. However, they did not delved into the second weakness of Falcon, the Gaussian sampler.
The Gaussian sampler is vulnerable to timing attacks, as shown by previous work [9,7,14,18]. A isochronous design was proposed by Howe et al. [11]. However, a successful single power analysis (SPA) was proposed by Guerreau et al. [10] and further improved by Zhang et al. [22]. There is currently no masking countermeasure for FALCON's Gaussian Sampler. Existing work [8] tends to re-write the Gaussian Sampler to remove the use of floating arithmetic, thus avoiding the challenge of masking the floor function.

Our Contribution In this work we further expand the countermeasure from Chen and Chen [4] and apply it to the Gaussian Sampler. We propose two generic methods to arithmetize the computation of the floor function, a necessary step towards its masking. Then we propose a hybrid method to effectively mask the floor function in the case of FALCON.

Relying on the previous work of Chen and Chen [4], we also verify the higher-order security of our method in the probing model. Our formal proofs rely on the Non-Interference (NI) security model first introduced by Barthe et al. [1].

Finally, we provide some performances of our methods and compare them with the reference unmasked implementation and the previous work of Chen and Chen [4]. The implementation is tested on a personal computer with an Intel-Core i7-11850H CPU.

2 Notation and Background

2.1 Notation

2.2 FALCON Sign

FALCON [19] is a Lattice-Based signature using the GPV framework over the NTRU problem. In this paper we will focus on the Gaussian Sampler used in the signature algorithm. For more details on the key generation or the verification, please refer to the reference paper [19].

The signature follows the Hash-Then-Sign strategy. The message m is salted with a random value r and then hashed into a challenge c. The remainder of the signature aims at building an instance of the SIS problem upon c and a public key h, *id est* finding $\boldsymbol{s} = (s_1, s_2)$ such as $s_1 + s_2 h = c$. To do so, the need to compute $\boldsymbol{s} = (\boldsymbol{t} - \boldsymbol{z})\mathbf{B}$, with $\boldsymbol{t}$ a pre-image vector and $\boldsymbol{z}$ provided by a Gaussian Sampler. Chen and Chen [4] focuses on masking the pre-image vector computation. In this work we intend to mask the Gaussian Sampler. The signature algorithm is detailled in Algorithm

2.3 Floor Function

2.4 Masking

3 Masking of the Floor Function

3.1 The B-Method

3.2 The T-Method

4 Application to FALCON

5 Performances

6 Conclusion

Acknowlegdments

References

1. Barthe, G., Belaïd, S., Dupressoir, F., Fouque, P.A., Grégoire, B., Strub, P.Y., Zucchini, R.: Strong non-interference and type-directed higher-order masking. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. p. 116–129. CCS '16, Association for Computing Machinery, New York, NY, USA (2016). https://doi.org/10.1145/2976749.2978427, https://doi.org/10.1145/2976749.2978427

2. Bernstein, D.J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J., Schwabe, P.: The sphincs+ signature framework. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. p. 2129–2146. CCS '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3319535.3363229, https://doi.org/10.1145/3319535.3363229
3. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehle, D.: Crystals - kyber: A cca-secure module-lattice-based kem. In: 2018 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 353–367 (April 2018). https://doi.org/10.1109/EuroSP.2018.00032
4. Chen, K.Y., Chen, J.P.: Masking floating-point number multiplication and addition of falcon: First- and higher-order implementations and evaluations. IACR Transactions on Cryptographic Hardware and Embedded Systems **2024**(2), 276–303 (Mar 2024). https://doi.org/10.46586/tches.v2024.i2.276-303, https://tches.iacr.org/index.php/TCHES/article/view/11428
5. Chen, L., Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R.A., Smith-Tone, D.: Report on post-quantum cryptography, vol. 12. US Department of Commerce, National Institute of Standards and Technology . . . (2016)
6. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: Crystals-dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems **2018**(1), 238–268 (Feb 2018). https://doi.org/10.13154/tches.v2018.i1.238-268, https://tches.iacr.org/index.php/TCHES/article/view/839
7. Espitau, T., Fouque, P.A., Gérard, B., Tibouchi, M.: Side-channel attacks on bliss lattice-based signatures: Exploiting branch tracing against strongswan and electromagnetic emanations in microcontrollers. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. p. 1857–1874. CCS '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3133956.3134028, https://doi.org/10.1145/3133956.3134028
8. Espitau, T., Fouque, P.A., Gérard, F., Rossi, M., Takahashi, A., Tibouchi, M., Wallet, A., Yu, Y.: Mitaka: A simpler, parallelizable, maskable variant of falcon. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology – EUROCRYPT 2022. pp. 222–253. Springer International Publishing, Cham (2022)
9. Groot Bruinderink, L., Hülsing, A., Lange, T., Yarom, Y.: Flush, gauss, and reload – a cache attack on the bliss lattice-based signature scheme. In: Gierlichs, B., Poschmann, A.Y. (eds.) Cryptographic Hardware and Embedded Systems – CHES 2016. pp. 323–345. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
10. Guerreau, M., Martinelli, A., Ricosset, T., Rossi, M.: The hidden parallelepiped is back again: Power analysis attacks on falcon. IACR Transactions on Cryptographic Hardware and Embedded Systems **2022**(3), 141–164 (Jun 2022). https://doi.org/10.46586/tches.v2022.i3.141-164, https://tches.iacr.org/index.php/TCHES/article/view/9697
11. Howe, J., Prest, T., Ricosset, T., Rossi, M.: Isochronous gaussian sampling: From inception to implementation. In: Ding, J., Tillich, J.P. (eds.) Post-Quantum Cryptography. pp. 53–71. Springer International Publishing, Cham (2020)
12. Karabulut, E., Aysu, A.: Falcon down: Breaking falcon post-quantum signature scheme through side-channel attacks. In: 2021 58th ACM/IEEE Design Automation Conference (DAC). pp. 691–696 (Dec 2021). https://doi.org/10.1109/DAC18074.2021.9586131
13. Kocher, P.C.: Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In: Koblitz, N. (ed.) Advances in Cryptology — CRYPTO '96. pp. 104–113. Springer Berlin Heidelberg, Berlin, Heidelberg (1996)

14. McCarthy, S., Howe, J., Smyth, N., Brannigan, S., O'Neill, M.: Bearz attack falcon: Implementation attacks with countermeasures on the falcon signature scheme. Cryptology ePrint Archive, Paper 2019/478 (2019), https://eprint.iacr.org/2019/478, https://eprint.iacr.org/2019/478
15. NIST: Module-lattice-based digital signature standard. NIST FIPS (2024). https://doi.org/10.6028/NIST.FIPS.204.ipd
16. NIST: Module-lattice-based key-encapsulation mechanism standard. NIST FIPS (2024). https://doi.org/10.6028/NIST.FIPS.203.ipd
17. NIST: Stateless hash-based digital signature standard. NIST FIPS (2024). https://doi.org/10.6028/NIST.FIPS.205.ipd
18. Pessl, P., Bruinderink, L.G., Yarom, Y.: To bliss-b or not to be: Attacking strongswan's implementation of post-quantum signatures. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. p. 1843–1855. CCS '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3133956.3134023, https://doi.org/10.1145/3133956.3134023
19. Prest, T., Fouque, P.A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z.: Falcon. Post-Quantum Cryptography Project of NIST (2020)
20. Ravi, P., Chattopadhyay, A., D'Anvers, J.P., Baksi, A.: Side-channel and fault-injection attacks over lattice-based post-quantum schemes (kyber, dilithium): Survey and new results. ACM Trans. Embed. Comput. Syst. **23**(2) (mar 2024). https://doi.org/10.1145/3603170, https://doi.org/10.1145/3603170
21. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review **41**(2), 303–332 (1999). https://doi.org/10.1137/S0036144598347011, https://doi.org/10.1137/S0036144598347011
22. Zhang, S., Lin, X., Yu, Y., Wang, W.: Improved power analysis attacks on falcon. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. pp. 565–595. Springer Nature Switzerland, Cham (2023)