Masking Floating-Point Number Multiplication and Addition of Falcon

Keng-Yu Chen, Jiun-Peng Chen

October 16th, 2024

IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN 2569-2925, Vol. 2024, No. 2, pp. 276–303. DOI:10.46586/tches.v2024.i2.276-303

Masking Floating-Point Number Multiplication and Addition of Falcon

First- and Higher-order Implementations and Evaluations

Keng-Yu Chen[1] and Jiun-Peng Chen[1,2]

[1] National Taiwan University, Taipei, Taiwan, r11921066@ntu.edu.tw
[2] Academia Sinica, Taipei, Taiwan, jpchen@ieee.org

Accepcted by Cryptographic Hardware and Embedded Systems (CHES) 2024

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Probing Model

To theoretically evaluate the security of our design, we consider the probing model [ISW03].

Probing Model

To theoretically evaluate the security of our design, we consider the probing model [ISW03].

- The t-probing model assumes that an adversary is able to peek any t intermediate values in the algorithm.

Probing Model

To theoretically evaluate the security of our design, we consider the probing model [ISW03].

- The t-probing model assumes that an adversary is able to peek any t intermediate values in the algorithm.
- To be secure in t-probing model, $n \geq t + 1$, and any share cannot be combined with each other.

Probing Model

To theoretically evaluate the security of our design, we consider the probing model [ISW03].

- The t-probing model assumes that an adversary is able to peek any t intermediate values in the algorithm.
- To be secure in t-probing model, $n \geq t + 1$, and any share cannot be combined with each other.
- It is complicated to prove t-probing security for a large composition of small gadgets. The concept of non-interference is convenient in this case.

Non-Interference Security

t-Non-Interference (t-NI) Security (from [Bar+16])

A gadget is t-Non-Interference (t-NI) secure if every set of t intermediate values can be simulated by no more than t shares of each of its inputs.

t-Strong Non-Interference (t-SNI) Security (from [Bar+16])

A gadget is t-Strong-Non-Interference (t-SNI) secure if for every set of t_I internal intermediate values and t_O of its output shares with $t_I + t_O \leq t$, they can be simulated by no more than t_I shares of each of its inputs.

Non-Interference Security

For $t = n - 1$, if a gadget is t-NI or t-SNI secure, and if any $n - 1$ input shares are uniformly and independently distributed, then it is t-probing secure.

Non-Interference Security

For $t = n - 1$, if a gadget is t-NI or t-SNI secure, and if any $n - 1$ input shares are uniformly and independently distributed, then it is t-probing secure.

Moreover,

Non-Interference Security

For $t = n - 1$, if a gadget is t-NI or t-SNI secure, and if any $n - 1$ input shares are uniformly and independently distributed, then it is t-probing secure.

Moreover,

- t-SNI is stronger than t-NI by definition.

Non-Interference Security

For $t = n - 1$, if a gadget is t-NI or t-SNI secure, and if any $n - 1$ input shares are uniformly and independently distributed, then it is t-probing secure.

Moreover,

- t-SNI is stronger than t-NI by definition.
- A composition of t-NI gadgets may not be t-NI, so we insert t-SNI gadgets to make it t-NI or t-SNI.

Non-Interference Security

For $t = n - 1$, if a gadget is t-NI or t-SNI secure, and if any $n - 1$ input shares are uniformly and independently distributed, then it is t-probing secure.

Moreover,

- t-SNI is stronger than t-NI by definition.
- A composition of t-NI gadgets may not be t-NI, so we insert t-SNI gadgets to make it t-NI or t-SNI.

All the gadgets/algorithms in our paper are proven either t-NI or t-SNI secure.

Gadgets/Algorithms in Our Work

Algorithm	**Security**	**Algorithm**	**Security**
SecAnd	t-SNI	SecOr	t-SNI
SecMult	t-SNI	SecNonzero	t-SNI
SecAdd	t-NI	SecFprUrsh	t-SNI
A2B	t-SNI	SecFprNorm64	t-NI
B2A	t-SNI	SecFPR	t-SNI
B2A_{Bit}	t-SNI	SecFprMul	t-SNI
RefreshMasks	t-NI	SecFprAdd	t-SNI
Refresh	t-SNI		

Table: List of gadgets/algorithms in our work with $n = t + 1$ shares

Test Vector Leakage Assessment (TVLA)

For practical security validation, we apply the Test Vector Leakage Assessment (TVLA) methodology [GJR+11].

Test Vector Leakage Assessment (TVLA)

For practical security validation, we apply the Test Vector Leakage Assessment (TVLA) methodology [GJR+11].
A tester records two sets of traces where

Test Vector Leakage Assessment (TVLA)

For practical security validation, we apply the Test Vector Leakage Assessment (TVLA) methodology [GJR+11].

A tester records two sets of traces where

- Set 1: fixed input

Test Vector Leakage Assessment (TVLA)

For practical security validation, we apply the Test Vector Leakage Assessment (TVLA) methodology [GJR+11].

A tester records two sets of traces where

- Set 1: fixed input
- Set 2: random input

Test Vector Leakage Assessment (TVLA)

For practical security validation, we apply the Test Vector Leakage Assessment (TVLA) methodology [GJR+11].

A tester records two sets of traces where

- Set 1: fixed input
- Set 2: random input

The Welch's t-test is then applied on the two sets.

Test Vector Leakage Assessment (TVLA)

For practical security validation, we apply the Test Vector Leakage Assessment (TVLA) methodology [GJR+11].

A tester records two sets of traces where

- Set 1: fixed input
- Set 2: random input

The Welch's t-test is then applied on the two sets.

By convention, the leakage is significant if the t-value exceeds ± 4.5.

Test Vector Leakage Assessment (TVLA)

For practical security validation, we apply the Test Vector Leakage Assessment (TVLA) methodology [GJR+11].

A tester records two sets of traces where

- Set 1: fixed input
- Set 2: random input

The Welch's t-test is then applied on the two sets.

By convention, the leakage is significant if the t-value exceeds ± 4.5.

Our TVLA result shows no leakage in the 2-shared version in 10,000 traces, and no leakage in the 3-shared version in 100,000 traces.

Table of Contents

Performance Evaluation on ARM Cortex-M4

	Algorithm	Cycles		
		Unmasked	**2 Shares**	**3 Shares**
SecFprMul	**Total**	**308**	**7134** (**23**$\times$)	**36388** (**118**$\times$)
	128-bit A2B	-	1619	19253
	64-bit SecNonzero	-	389	1350
	Two 16-bit SecNonzero	-	662	2012
	SecFPR	-	3362	10813
	#randombytes	-	333	2005
SecFprAdd	**Total**	**487**	**17154** (**35**$\times$)	**48291** (**99**$\times$)
	Three 64-bit SecAdd	-	6990	16956
	Two 16-bit B2A	-	88	332
	16-bit A2B	-	146	2267
	SecFprUrsh	-	1112	3214
	SecFprNorm64	-	2846	7270
	SecFPR	-	3362	10813
	#randombytes	-	849	2691

Performance Evaluation on ARM Cortex-M4

	Algorithm	Cycles		
		Unmasked	2 Shares	3 Shares
SecFprMul	**Total**	**308**	**7134** (**23**$\times$)	**36388** (**118**$\times$)
	128-bit A2B	-	1619	19253
	64-bit SecNonzero	-	389	1350
	Two 16-bit SecNonzero	-	662	2012
	SecFPR	-	3362	10813
	#randombytes	-	333	2005
SecFprAdd	**Total**	**487**	**17154** (**35**$\times$)	**48291** (**99**$\times$)
	Three 64-bit SecAdd	-	6990	16956
	Two 16-bit B2A	-	88	332
	16-bit A2B	-	146	2267
	SecFprUrsh	-	1112	3214
	SecFprNorm64	-	2846	7270
	SecFPR	-	3362	10813
	#randombytes	-	849	2691

Performance Evaluation on General Purpose CPU

We also test the time for signing one message on Intel-Core i9-12900 KF.

Security Level	**Unmasked**	**2 Shares**	**3 Shares**
Falcon-512	246.56	1905.55 (7.7×)	6137.25 (24.9×)
Falcon-1024	501.62	3819.76 (7.6×)	12287.29 (24.5×)

Table: Time (in microseconds) for signing a message on Intel-Core i9-12900KF CPU.

Table of Contents

Conclusion

In this paper,

Conclusion

In this paper,

- We present the first masking scheme for floating-point number multiplication and addition to protect the pre-image vector computation of FALCON.

Conclusion

In this paper,

- We present the first masking scheme for floating-point number multiplication and addition to protect the pre-image vector computation of FALCON.
- We design novel gadgets SecNonzero, SecFprUrsh, and SecFprNorm64.

Conclusion

In this paper,

- We present the first masking scheme for floating-point number multiplication and addition to protect the pre-image vector computation of FALCON.
- We design novel gadgets SecNonzero, SecFprUrsh, and SecFprNorm64.
- All our masked gadgets are proven either t-NI or t-SNI secure.

Conclusion

In this paper,

- We present the first masking scheme for floating-point number multiplication and addition to protect the pre-image vector computation of FALCON.
- We design novel gadgets SecNonzero, SecFprUrsh, and SecFprNorm64.
- All our masked gadgets are proven either t-NI or t-SNI secure.
- Our design pass the TVLA test in 10,000 (for 2-shared) or 100,000 (for 3-shared) traces.

Conclusion

In this paper,

- We present the first masking scheme for floating-point number multiplication and addition to protect the pre-image vector computation of FALCON.
- We design novel gadgets SecNonzero, SecFprUrsh, and SecFprNorm64.
- All our masked gadgets are proven either t-NI or t-SNI secure.
- Our design pass the TVLA test in 10,000 (for 2-shared) or 100,000 (for 3-shared) traces.
- Our countermeasure when compared to the unmasked reference implementation is much slower. Improved SecAdd and A2B can reduce the cost.

Reference I

[ISW03] Yuval Ishai, Amit Sahai, and David Wagner. "Private Circuits: Securing Hardware against Probing Attacks". In: *CRYPTO 2003*. Ed. by Dan Boneh. Vol. 2729. LNCS. Springer, Heidelberg, Aug. 2003, pp. 463–481. DOI: 10.1007/978-3-540-45146-4_27.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. "Trapdoors for hard lattices and new cryptographic constructions". In: *40th ACM STOC*. Ed. by Richard E. Ladner and Cynthia Dwork. ACM Press, May 2008, pp. 197–206. DOI: 10.1145/1374376.1374407.

[GJR+11] Benjamin Jun Gilbert Goodwill, Josh Jaffe, Pankaj Rohatgi, et al. "A testing methodology for side-channel resistance validation". In: *NIST non-invasive attack testing workshop*. Vol. 7. 2011, pp. 115–136.

[Cor+15] Jean-Sébastien Coron et al. "Conversion from Arithmetic to Boolean Masking with Logarithmic Complexity". In: *FSE 2015*. Ed. by Gregor Leander. Vol. 9054. LNCS. Springer, Heidelberg, Mar. 2015, pp. 130–149. DOI: 10.1007/978-3-662-48116-5_7.

[Bar+16] Gilles Barthe et al. "Strong Non-Interference and Type-Directed Higher-Order Masking". In: *ACM CCS 2016*. Ed. by Edgar R. Weippl et al. ACM Press, Oct. 2016, pp. 116–129. DOI: 10.1145/2976749.2978427.

[DP16] Léo Ducas and Thomas Prest. "Fast fourier orthogonalization". In: *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*. 2016, pp. 191–198.

Reference II

[Din+17] A. Adam Ding et al. "Towards Sound and Optimal Leakage Detection Procedure". In: *Smart Card Research and Advanced Applications - 16th International Conference, CARDIS 2017, Lugano, Switzerland, November 13-15, 2017, Revised Selected Papers*. Ed. by Thomas Eisenbarth and Yannick Teglia. Vol. 10728. Lecture Notes in Computer Science. Springer, 2017, pp. 105–122. DOI: 10.1007/978-3-319-75208-2_7. URL: https://doi.org/10.1007/978-3-319-75208-2%5C_7.

[Bar+18] Gilles Barthe et al. "Masking the GLP Lattice-Based Signature Scheme at Any Order". In: *EUROCRYPT 2018, Part II*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10821. LNCS. Springer, Heidelberg, Apr. 2018, pp. 354–384. DOI: 10.1007/978-3-319-78375-8_12.

[BCZ18] Luk Bettale, Jean-Sébastien Coron, and Rina Zeitoun. "Improved High-Order Conversion From Boolean to Arithmetic Masking". In: *IACR TCHES* 2018.2 (2018). https://tches.iacr.org/index.php/TCHES/article/view/873, pp. 22–45. ISSN: 2569-2925. DOI: 10.13154/tches.v2018.i2.22-45.

[Sch+19] Tobias Schneider et al. "Efficiently Masking Binomial Sampling at Arbitrary Orders for Lattice-Based Crypto". In: *PKC 2019, Part II*. Ed. by Dongdai Lin and Kazue Sako. Vol. 11443. LNCS. Springer, Heidelberg, Apr. 2019, pp. 534–564. DOI: 10.1007/978-3-030-17259-6_18.

Reference III

[Pre+20] Thomas Prest et al. *FALCON*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions. National Institute of Standards and Technology, 2020.

[KA21] Emre Karabulut and Aydin Aysu. "FALCON Down: Breaking FALCON Post-Quantum Signature Scheme through Side-Channel Attacks". In: *2021 58th ACM/IEEE Design Automation Conference (DAC)*. 2021, pp. 691–696. DOI: 10.1109/DAC18074.2021.9586131.

[Gue+22] Morgane Guerreau et al. "The Hidden Parallelepiped Is Back Again: Power Analysis Attacks on Falcon". In: *IACR TCHES* 2022.3 (2022), pp. 141–164. DOI: 10.46586/tches.v2022.i3.141-164.

[Zha+23] Shiduo Zhang et al. "Improved Power Analysis Attacks on Falcon". In: *EUROCRYPT 2023, Part IV*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14007. LNCS. Springer, Heidelberg, Apr. 2023, pp. 565–595. DOI: 10.1007/978-3-031-30634-1_19.

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents