AIMer v2.0

Seongkwang Kim[1], J. Cho[1], J. Ha[2], J. Kwon[1], B. Lee[1], J. Lee[3], J. Lee[2], S. Lee[1], D. Moon[1], M. Son[2], and H. Yoon[1].

[1]Samsung SDS, [2]KAIST, [3]Sungshin Women's University.

Poster QR

What is AIMer?

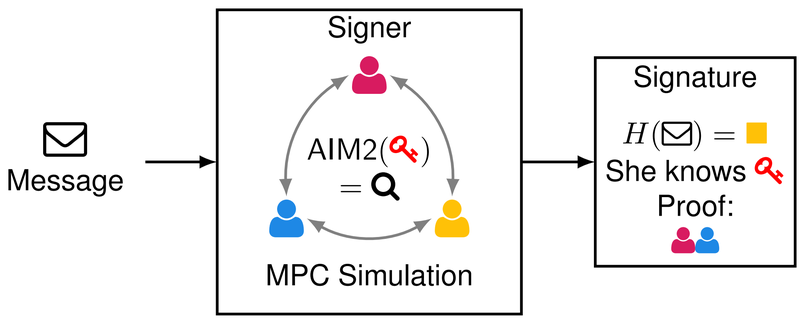


Fig. Diagram of how AIMer works†

AIMer is a signature scheme obtained from a zero-knowledge proof of preimage knowledge for a certain one-way function. AIMer consists of two parts: a non-interactive zero-knowledge proof of knowledge (NIZKPoK) system, and a one-way function AIM2. The security of both parts solely depends on the security of the underlying symmetric primitives.

NIZKPoK in AIMer

- Highly-engineered BN++
- Efficient for large fields
- Memory-saving verification

Symmetric Primitive AIM2

- Efficiently provable in BN++
- With in-depth algebraic analysis
- Previous weakness addressed

Improvements in Version 2.0

Change of specification

- Symmetric primitive: AIM → AIM2
- Prehashing now supported
- Halved salt size
- Reduced number of parameter sets

Change of Implementation

- More readable reference code
- Additional ARM64 implementation
- No OpenSSL dependency
- Up to **29%** faster signing than v1.0
- Up to **96%** less memory in verification

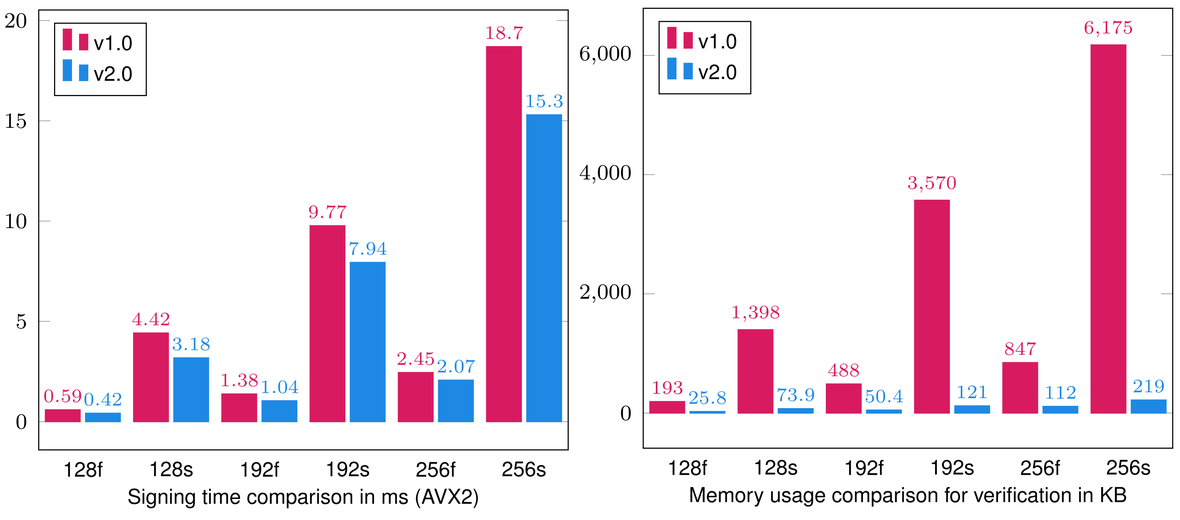
Editorial change

- Improved EUF-CMA security proof
- Implementation-friendly specification

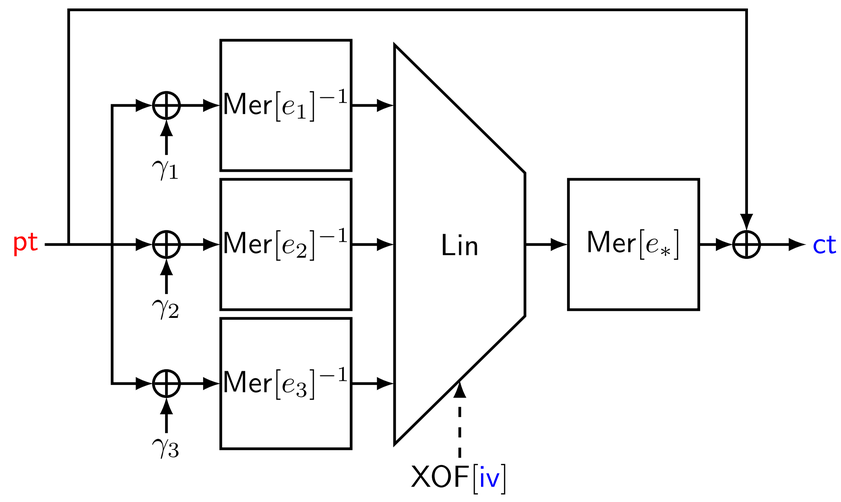
Implementation Results

- Benchmark highlights: signing time of (aimer128f, aimer128s)
  - AVX2: **(0.42ms, 3.18ms)** on Intel Xeon E5-1650 v3 (Haswell) @ 3.50 GHz
  - ARM64: **(1.77ms, 14.1ms)** on ASUS Tinker Board 2S, ARM Cortex-A72 @ 2.0 GHz
- A memory-centered implementation turned out to **run well on ARM Cortex-M4**.
- For more results, scan the QR code below!

Parameters	pk size (bytes)	sk size (bytes)	Sig. size (bytes)
aimer128f	32	48	5,888
aimer128s	32	48	4,160
aimer192f	48	72	13,056
aimer192s	48	72	9,120
aimer256f	64	96	25,120
aimer256s	64	96	17,056



AIM2



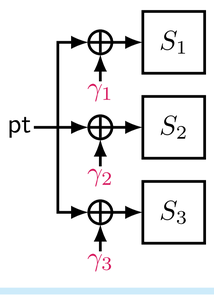
Symmetric primitive AIM is characterized by its parallel structure and Mersenne S-boxes, which are designed to minimize the signature size [3]. However, there have been some analyses on AIM (see the next box), we devise a new symmetric primitive AIM2 to mitigate all the recent cryptanalysis while maintaining the design strengths of AIM [4]. In AIMer version 2.0, we use AIM2 whose security is reinforced by following revisions:

Inverse Mersenne S-box

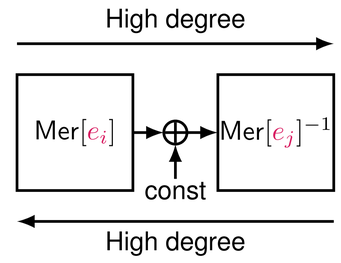
$$\mathrm{Mer}[e]^{-1}(x) = x^{\bar{e}}$$
$$\bar{e} = e^{-1} \pmod{2^n - 1}$$

- No low-degree system in λ variables
- Inherit all the strength of Mersenne S-box

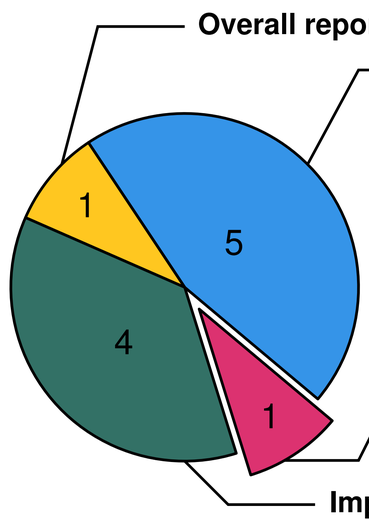
Constant addition to inputs



Increasing exponents



(Third-Party) Analyses on AIMer



Overall report [1]

Security analysis on AIM
- Algebraic analysis [6]
- Fast exhaustive search [5]
- Grover's search [2]

First-party analysis on AIM2 [4]
- **Presentation on TODAY 15:40!**

Implementation and performance analysis
- Clean implementation
- Optimized implementation
- ARM-Cortex M4 implementation

Future Work

Work in progress

- Implementing AIMer on ARM Cortex-M4 in an optimized form (est. Q3 2024)
  - Preliminary result: **memory usage** $\leq$ **110 KB** for all parameter sets
- Improving the puncturable PRF in the NIZKPoK and adopting AES-based PRG (est. Q3 2024)
  - Preliminary result: signature size **4.8 KB (128f), 3.6 KB (128s)**

Future Works

- Plan to apply Hypercube method
- Plan to prove the QROM security of AIMer

KEY REFERENCES

[1] Jolijn Cottaar et al. *Report on evaluation of KpqC candidates*. Cryptology ePrint Archive, Paper 2023/1853. 2023.

[2] Kyungbae Jang et al. *Quantum Implementation of AIM: Aiming for Low-Depth*. Cryptology ePrint Archive, Paper 2023/337. 2023.

[3] Seongkwang Kim et al. "AIM: Symmetric Primitive for Shorter Signatures with Stronger Security". In: *ACM CCS '23*. Association for Computing Machinery, 2023, pp. 401–415.

[4] Seongkwang Kim et al. *Efficacy and Mitigation of the Cryptanalysis on AIM*. Cryptology ePrint Archive, Paper 2023/1474. 2024.

[5] Fukang Liu et al. "Algebraic Attacks on RAIN and AIM Using Equivalent Representations". In: *IACR ToSC* 2023.4 (2023), pp. 166–186.

[6] Kaiyi Zhang et al. "Algebraic Attacks on Round-Reduced Rain and Full AIM-III". In: *ASIACRYPT 2023*. Ed. by Jian Guo and Ron Steinfeld. Springer, 2023, pp. 285–310.

† This diagram was created by using fontawesome icons.

ACKNOWLEDGEMENT AND PARTNERS

- KpqC committee
- Prof. Hwajeong Seo in Hansung University
- Prof. Dong-Guk Han in Kookmin University

MORE INFORMATION

AIMer Website

Seongkwang Kim
Samsung SDS
Security Algorithm Lab
sk39.kim@samsung.com

Posted in the 5th NIST PQC Standardization Conference (11th April 2024, 14:30 EST)