AIMer

Seongkwang Kim[1] Jincheol Ha[2] Mincheol Son[2]
Byeonghak Lee[1] Dukjae Moon[1] Joohee Lee[3] Sangyub Lee[1]
Jihoon Kwon[1] Jihoon Cho[1] Hyojin Yoon[1] Jooyoung Lee[2]

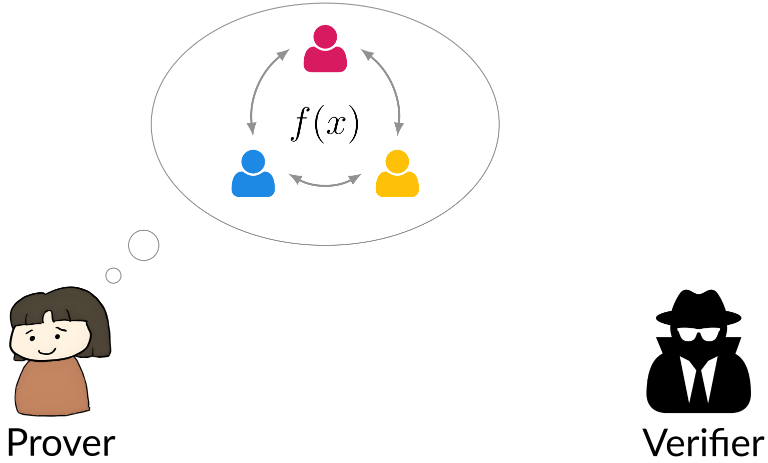
[1]Samsung SDS [2]KAIST [3]Sungshin Women's University

MPC-in-the-Head (MPCitH)

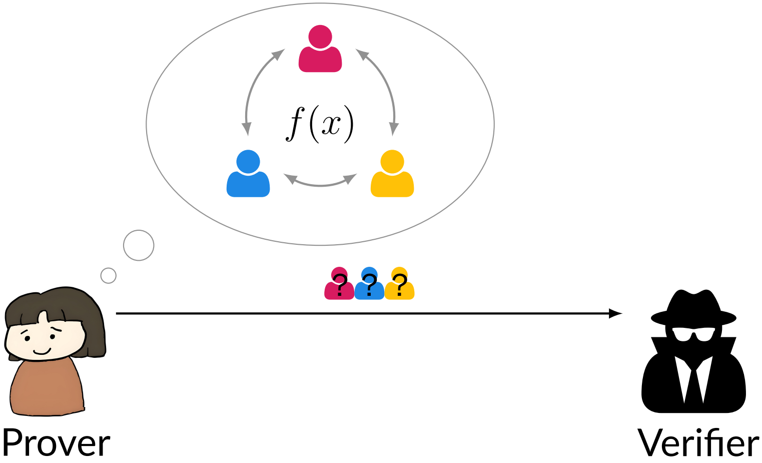
Prover

Verifier

MPC-in-the-Head (MPCitH)



MPC-in-the-Head (MPCitH)

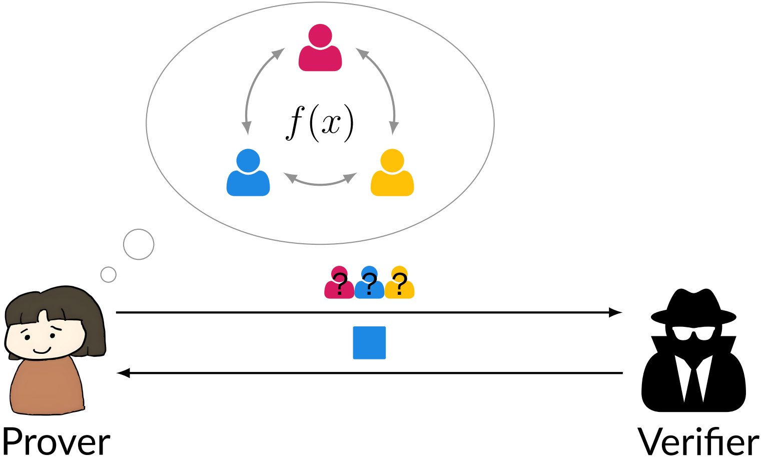


$f(x)$

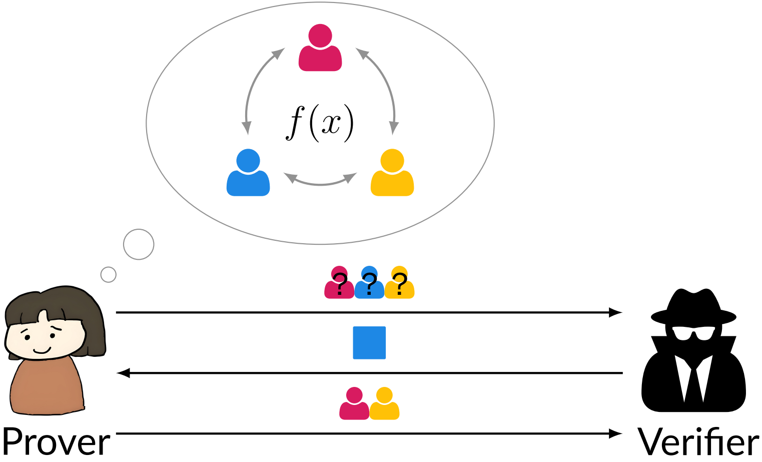
Prover

Verifier

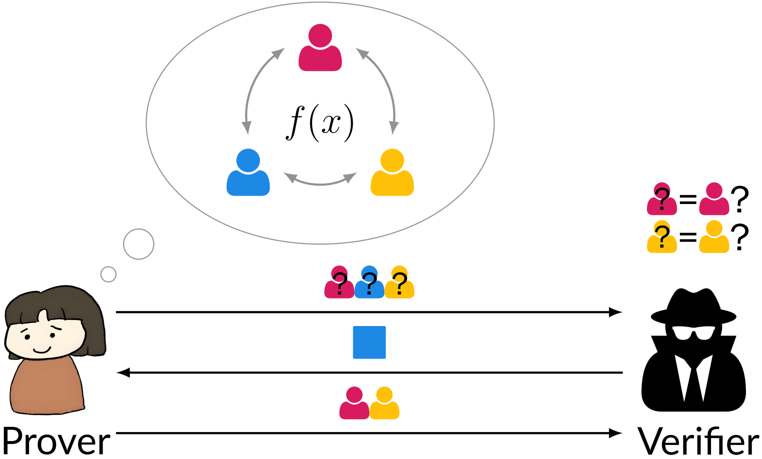
MPC-in-the-Head (MPCitH)



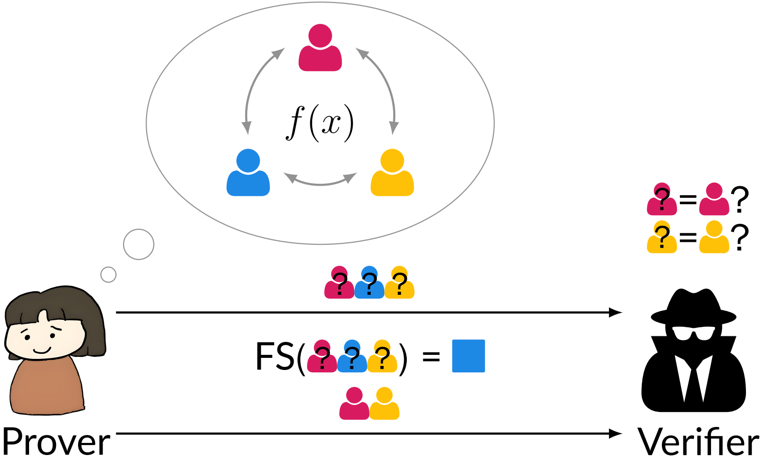
MPC-in-the-Head (MPCitH)



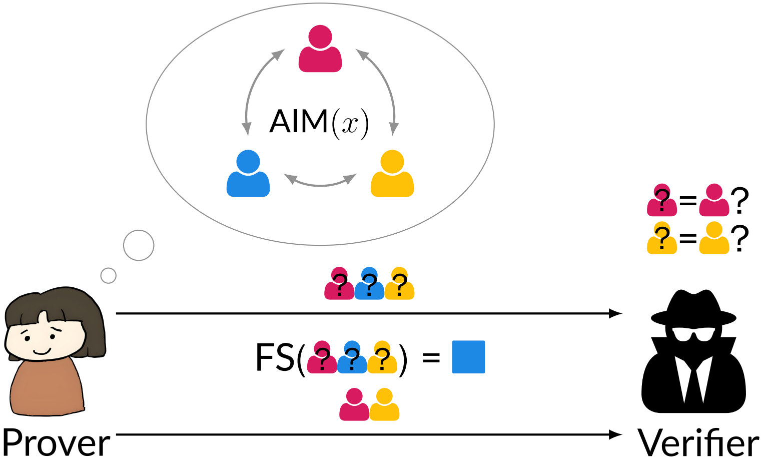
MPC-in-the-Head (MPCitH)



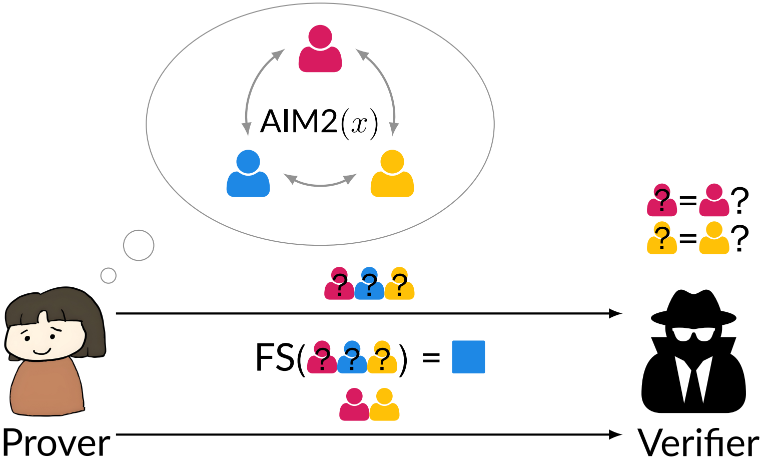
MPCitH-based Signature



AIMer v1.0



AIMer v2.0



AIM2(x)

? = ?

? = ?

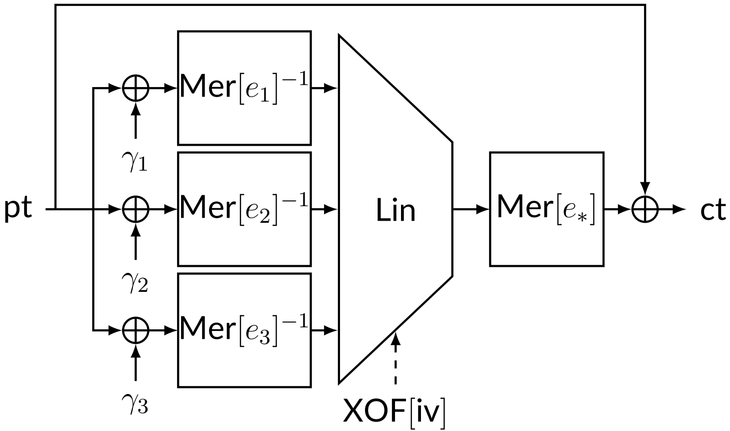
? ? ?

FS(? ? ?) = 🟦

Prover

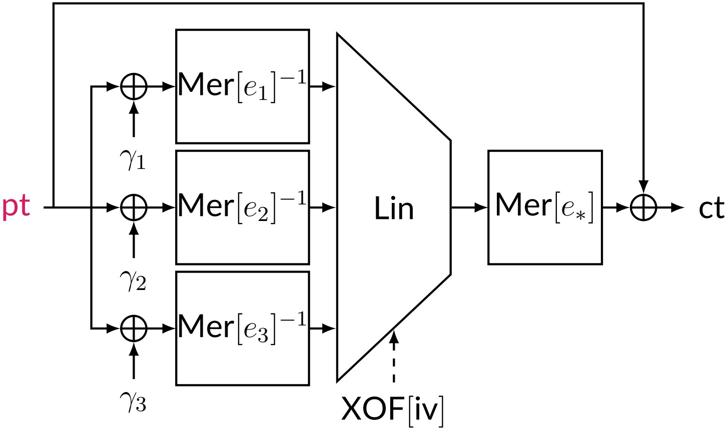
Verifier

AIM2



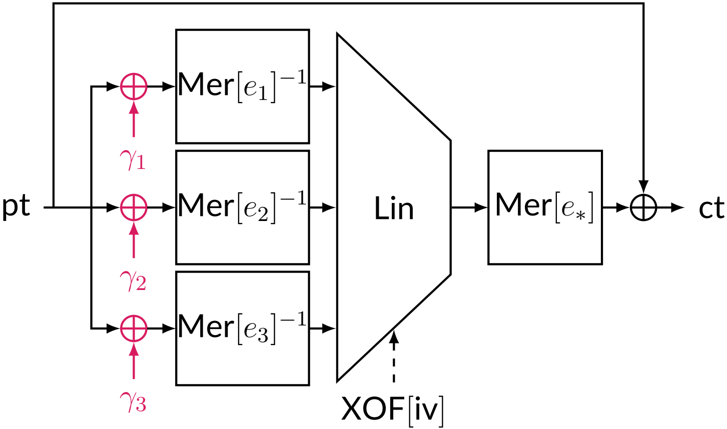
pt
γ_1
γ_2
γ_3
$\mathsf{Mer}[e_1]^{-1}$
$\mathsf{Mer}[e_2]^{-1}$
$\mathsf{Mer}[e_3]^{-1}$
Lin
XOF[iv]
$\mathsf{Mer}[e_*]$
ct

AIM2

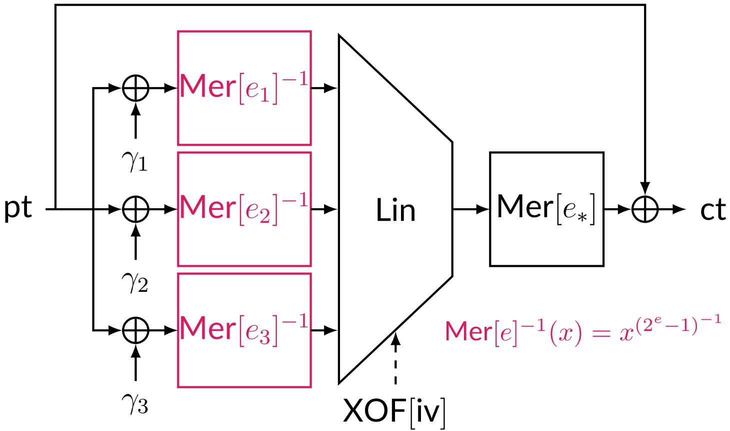


pt
γ_1
γ_2
γ_3
$\mathsf{Mer}[e_1]^{-1}$
$\mathsf{Mer}[e_2]^{-1}$
$\mathsf{Mer}[e_3]^{-1}$
Lin
XOF[iv]
$\mathsf{Mer}[e_*]$
ct

AIM2

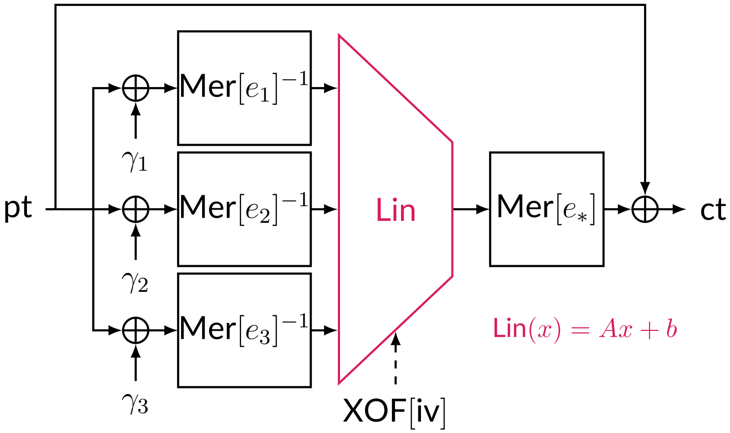

pt
γ_1
γ_2
γ_3
$\mathsf{Mer}[e_1]^{-1}$
$\mathsf{Mer}[e_2]^{-1}$
$\mathsf{Mer}[e_3]^{-1}$
Lin
XOF[iv]
$\mathsf{Mer}[e_*]$
ct

AIM2

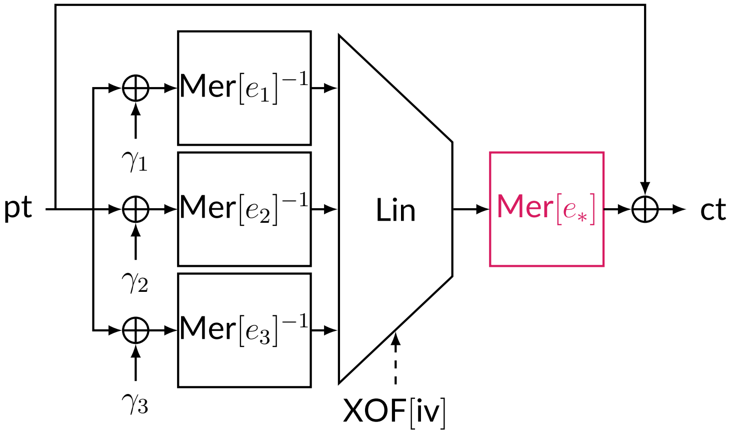


$\mathsf{Mer}[e]^{-1}(x) = x^{(2^e-1)^{-1}}$

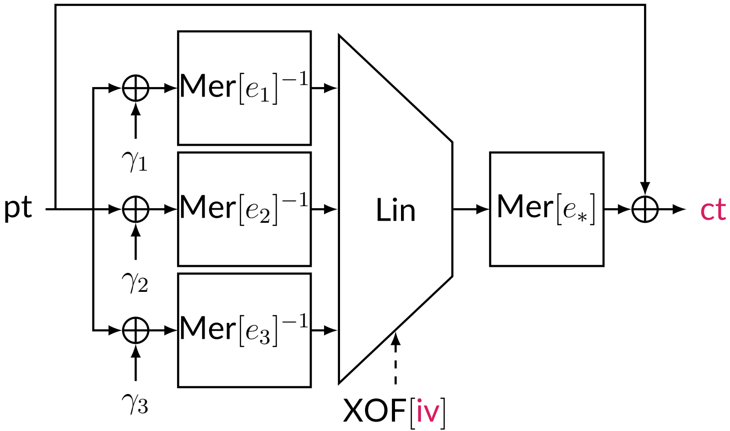
AIM2


pt
γ_1
γ_2
γ_3
Mer$[e_1]^{-1}$
Mer$[e_2]^{-1}$
Mer$[e_3]^{-1}$
Lin
XOF[iv]
Mer$[e_*]$
ct
Lin$(x) = Ax + b$

AIM2


pt
$\text{Mer}[e_1]^{-1}$
$\text{Mer}[e_2]^{-1}$
$\text{Mer}[e_3]^{-1}$
γ_1
γ_2
γ_3
Lin
XOF[iv]
$\text{Mer}[e_*]$
ct

AIM2


pt
γ_1
γ_2
γ_3
$\mathsf{Mer}[e_1]^{-1}$
$\mathsf{Mer}[e_2]^{-1}$
$\mathsf{Mer}[e_3]^{-1}$
Lin
XOF[iv]
$\mathsf{Mer}[e_*]$
ct

Merit 1: Novelty

Merit 1: Novelty

Merit 2: Multi-Scenario Implementation

Merit 2: Multi-Scenario Implementation

Done:

- C standalone
- AVX2
- ARM64
- ARM64 + SHA3 instr.
- Memory-reduced impl.
- ARM Cortex-M4

Merit 2: Multi-Scenario Implementation

Done:

- C standalone
- AVX2
- ARM64
- ARM64 + SHA3 instr.
- Memory-reduced impl.
- ARM Cortex-M4

To-do:

- liboqs
- OpenSSL
- OpenSSH

Merit 3: Performance & Security

Merit 3: Performance & Security

The security of AIMer only depends on symmetric primitives!

Merit 3: Performance & Security

The security of AIMer only depends on symmetric primitives!
AIMer enjoys balanced performance (all-rounder).

Scheme	Size (B)			Time (cycle)		
	sk	pk	sig	KeyGen	Sign	Verify
Dilithium						
Falcon						
SPHINCS+-f						
HAETAE						
NCC-Sign-tri						
MQ-Sign-LR						
AIMer-f						

SUPERCOP result (Zen 4), Category 1 or 2, median speed

Merit 3: Performance & Security

The security of AIMer only depends on symmetric primitives!

AIMer enjoys balanced performance (all-rounder).

Scheme	Size (B)			Time (cycle)		
	sk	pk	sig	KeyGen	Sign	Verify
Dilithium	2,528	1,312	2,420			
Falcon	1,281	897	666			
SPHINCS+-f	64	32	17.1K			
HAETAE	1,408	992	1,474			
NCC-Sign-tri	2,400	1,760	2,912			
MQ-Sign-LR	161K	328K	134			
AIMer-f	48	32	5,888			

SUPERCOP result (Zen 4), Category 1 or 2, median speed

Merit 3: Performance & Security

The security of AIMer only depends on symmetric primitives!

AIMer enjoys balanced performance (all-rounder).

Scheme	Size (B)			Time (cycle)		
	sk	pk	sig	KeyGen	Sign	Verify
Dilithium	2,528	1,312	2,420	62K	149K	70K
Falcon	1,281	897	666	15.6M*	331K*	63K*
SPHINCS+-f	64	32	17.1K	1.23M*	5.65M*	6.26M*
HAETAE	1,408	992	1,474	437K	1.13M	100K
NCC-Sign-tri	2,400	1,760	2,912	197K	295K	196K
MQ-Sign-LR	161K	328K	134	5.60M*	67K*	35K*
AIMer-f	48	32	5,888	40K	889K	898K

* Not intend to be constant-time

SUPERCOP result (Zen 4), Category 1 or 2, median speed

Merit 3: Performance & Security

The security of AIMer only depends on symmetric primitives!

AIMer enjoys balanced performance (all-rounder).

Scheme	Size (B)			Time (cycle)		
	sk	pk	sig	KeyGen	Sign	Verify
Dilithium	2,528	1,312	2,420	62K	149K	70K
Falcon	1,281	897	666	15.6M*	331K*	63K*
SPHINCS+-f	64	32	17.1K	1.23M*	5.65M*	6.26M*
HAETAE	1,408	992	1,474	437K	1.13M	100K
NCC-Sign-tri	2,400	1,760	2,912	197K	295K	196K
MQ-Sign-LR	161K	328K	134	101M	548K	693K
AIMer-f	48	32	5,888	40K	889K	898K

* Not intend to be constant-time

SUPERCOP result (Zen 4), Category 1 or 2, median speed

Merit 4: Active Research

Merit 4: Active Research

1. Evolving AIMer
   - Security reinforcement
   - Further optimization of implementation
   - Usability updates
   - Algorithmic improvement (sig. size 4.6KB/3.4KB)

Merit 4: Active Research

1. Evolving AIMer
   - Security reinforcement
   - Further optimization of implementation
   - Usability updates
   - Algorithmic improvement (sig. size 4.6KB/3.4KB)
2. Evolving MPCitH-based signatures
   - Hypercube method
   - SUF-CMA in the QROM
   - GGM tree optimization

Merit 5: Active Communication

Merit 5: Active Communication

- Communications with third-party
  - NIST submission
  - Talks (except KpqC events)
    - 2023 Ewha-KMS IWC
    - 2nd Oxford PQC Summit
    - ACM CCS 2023
    - The 5th NIST PQC Standardization Conference

Merit 5: Active Communication

- Communications with third-party
  - NIST submission
  - Talks (except KpqC events)
    - 2023 Ewha-KMS IWC
    - 2nd Oxford PQC Summit
    - ACM CCS 2023
    - The 5th NIST PQC Standardization Conference
- Cooperative attitude
  - Contribution to `mupq` (also planned for `pqm4`)
  - Resolving TIMECOP complaints
  - PQClean-friendly implementation
  - Response to the side-channel attack

Demerits

Demerits

1. Modest performance
    - Relatively large signature size
    - Not-so-fast sign/verify speed

Demerits

1. Modest performance
    - Relatively large signature size
    - Not-so-fast sign/verify speed
2. Relatively new primitive
    - AIM2 was proposed not a long time ago.

    * But multiple cryptanalysts have admitted that AIM2 is secure against state-of-the-art cryptanalytic techniques.

History: AIMer v0.9 (Oct. 2022)

History: AIMer v0.9 (Oct. 2022)

Algorithm		Implementation	Security
Symmetric	Protocol		
AIM	BN++	C standalone	Birthday-bound

History: AIMer v1.0 (Jun. 2023)

Algorithm		Implementation	Security
Symmetric	Protocol		
AIM	BN++ Merge hash Domain sep.	C standalone AVX2	Birthday-bound

History: AIMer v1.0 (Sep. 2023)

Algorithm		Implementation	Security
Symmetric	Protocol		
~~AIM~~	BN++	C standalone	Birthday-bound
Attack	Merge hash	AVX2	
AIM2	Domain sep.		

History: AIMer v2.0 (Feb. 2024)

Algorithm		Implementation	Security
Symmetric	Protocol		
~~AIM~~	BN++	C standalone	~~Birthday-bound~~
~~Attack~~	Merge hash	AVX2	Full-bound
AIM2	Domain sep.	ARM64	
	Half salt		
	Prehashing		

History: AIMer v2.1 (Aug. 2024)

Algorithm		Implementation	Security
Symmetric	Protocol		
~~AIM~~	BN++	C standalone	~~Birthday-bound~~
~~Attack~~	Merge hash	AVX2	Full-bound
AIM2	Domain sep.	ARM64 + SHA3	
	Half salt	ARM Cortex-M4	
	Prehashing	PQClean	
		Constrained mem.	
		TIMECOP	

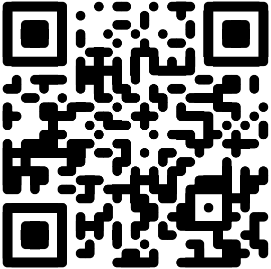
History: AIMer v?.? (Future work)

Algorithm		Implementation	Security
Symmetric	Protocol		
~~AIM~~ ~~Attack~~ AIM2	BN++ Merge hash Domain sep. Half salt Prehashing Hypercube method GGM tree opt. Semi-commitment	C standalone AVX2 ARM64 + SHA3 ARM Cortex-M4 PQClean Constrained mem. TIMECOP OpenSSH OpenSSL	~~Birthday-bound~~ Full-bound SUF-CMA QROM

Acknowledgement

- We appreciate …
  - Fukang Liu, Mohammad Mahzoun, Morten Øygarden, Willi Meier, Kaiyi Zhang, Qingju Wang, Yu Yu, Chun Guo, Hongrui Cui, and Markku-Juhani O. Saarinen for the symmetric cryptanalysis;
  - CryptoCraft lab in Hansung University (Prof. Hwajeong Seo) for the classical/quantum/M4 implementations;
  - SICADA lab in Kookmin University (Prof. Dong-Guk Han) for the side-channel analysis;
  - TU/e team for the valuable report;
  - Prof. Daniel Bernstein for helping incorporation to SUPERCOP;
  - pqm4 team for the initial ARM Cortex-M4 implementation;
  - KpqBench team for the performance and implementation security analysis.

Thank you!
Check out our website!



Attribution

- Illustrations at the very beginning was created using fontawesome latex package (`https://github.com/xdanaux/fontawesome-latex`).
- The picture of me at ACM CCS 2023 was taken by Mincheol Son.
- SUPERCOP result can be found in `https://bench.cr.yp.to/results-sign/amd64-hertz.html`.