

Updates on AlMer

KpqC 9th Workshop

Seongkwang Kim¹ Jincheol Ha² Mincheol Son²
Byeonghak Lee¹ Dukjae Moon¹ Joohee Lee³ Sangyub Lee¹
Jihoon Kwon¹ Jihoon Cho¹ Hyojin Yoon¹ Jooyoung Lee²

¹Samsung SDS

²KAIST

³Sungshin Women's University

Summary of AIMer



Novel Design



Usability



Global
Communication



Symm. Prim.
Assumption



Balanced
Performance



Active Research

History: AlMer v0.9 (Oct. 2022)

History: AlMer v0.9 (Oct. 2022)

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

History: AlMer v1.0 (Jun. 2023)

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

History: AlMer v1.0 (Sep. 2023)

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

History: AlMer v2.0 (Feb. 2024)

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

History: AlMer v2.1 (Aug. 2024)

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

History: AlMer 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	Birth-day-bound Full-bound SUF-CMA QROM

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: Security

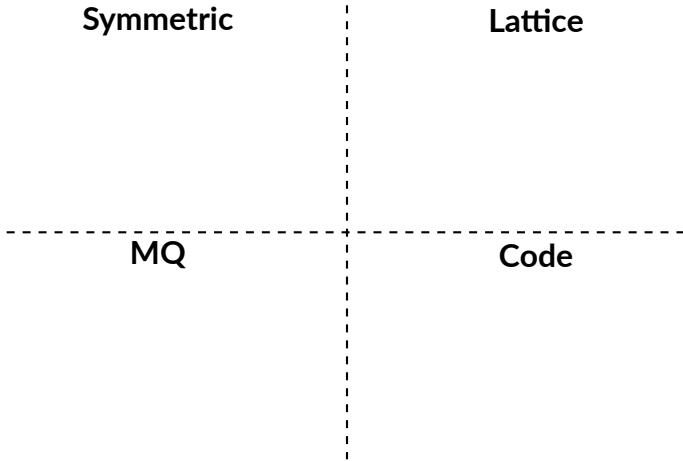
Merit 3: Security

Symmetric

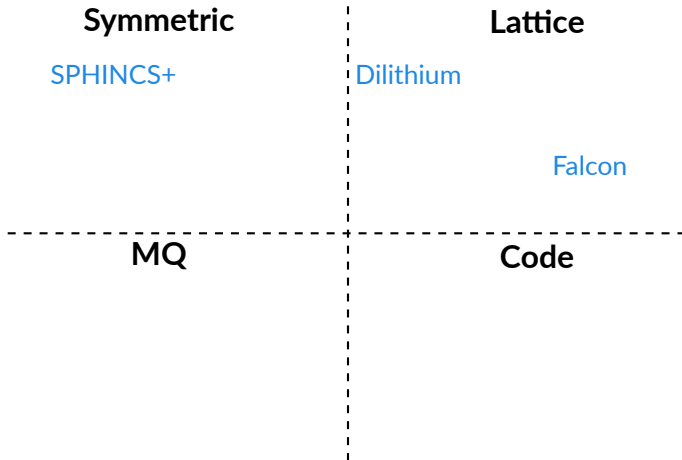
Lattice

MQ

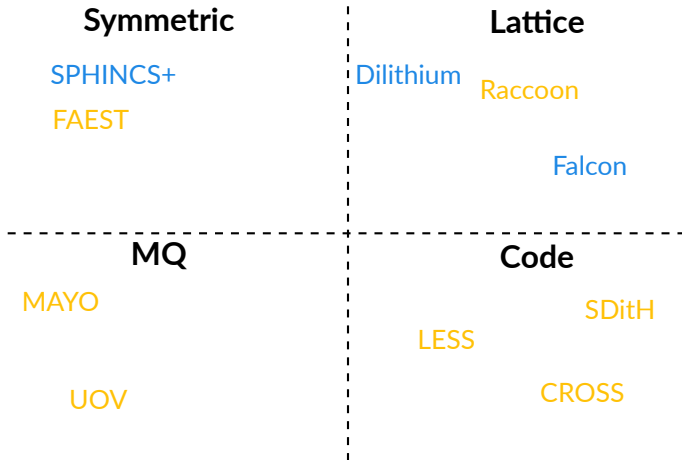
Code



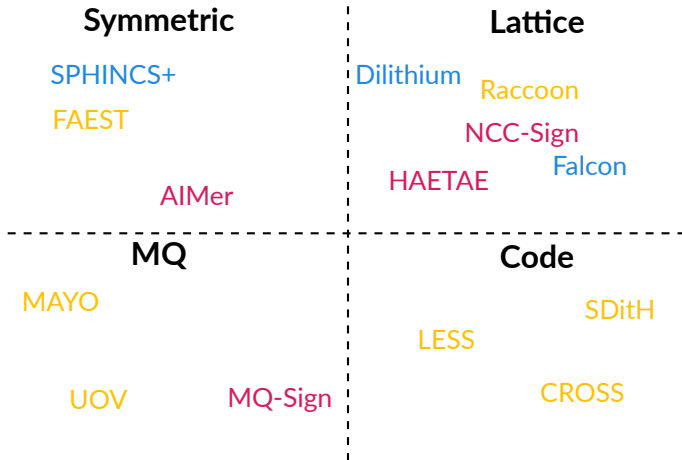
Merit 3: Security



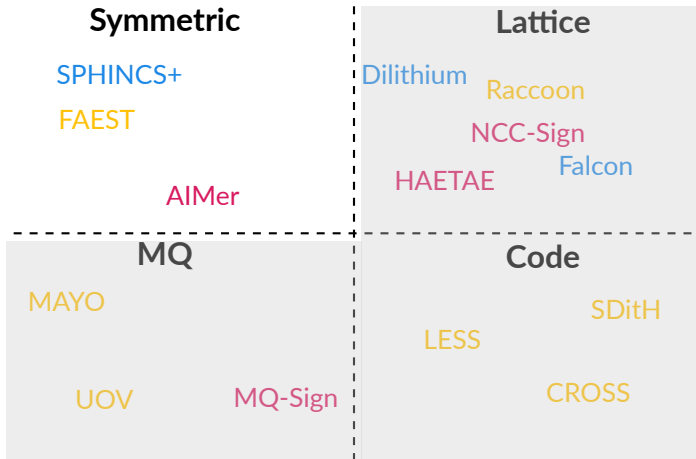
Merit 3: Security



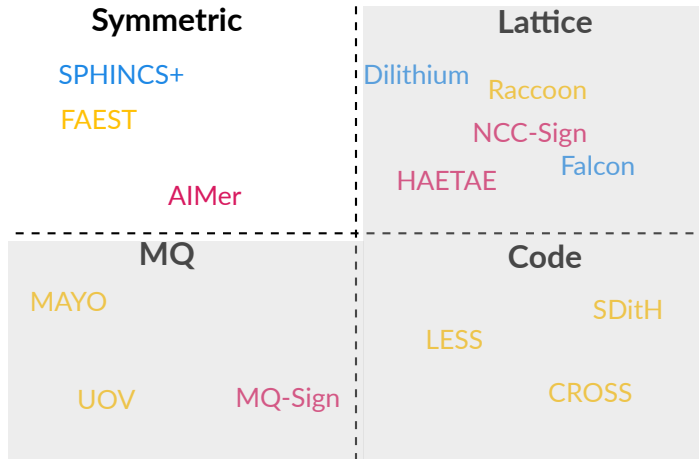
Merit 3: Security



Merit 3: Security



Merit 3: Security



The security of AIMer **only** depends on symmetric primitives!

Merit 4: Performance

Merit 4: Performance

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 4: Performance

AlMer 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			
AlMer-f	48	32	5,888			

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

Merit 4: Performance

AlMer 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*
AlMer-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: Performance

AlMer 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
AlMer-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 5: Active Research

Merit 5: Active Research

1. Evolving AlMer

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

Merit 5: Active Research

1. Evolving AlMer

- 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 6: Active Communication

Merit 6: 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

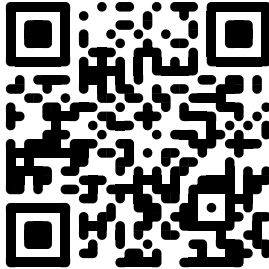
Merit 6: Active Communication

- 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 (we also PRed to pqm4)
 - Resolving TIMECOP complaints
 - PQCclean-friendly implementation
 - Response to the side-channel attack

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 fontawesome5 (<https://fontawesome.com/>) free version latex package.
- 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>.