2023.11.13.(월) 연세대 동문회관 3층 그랜드볼룸

Recent Updates on SOLMAE

김 광조

세계암호학회(IACR) Fellow
국제사이버보안연구원(IRCS) 원장
KAIST 전산학부 명예교수
kkj@kaist.ac.kr
https://caislab.kaist.ac.kr/kkj

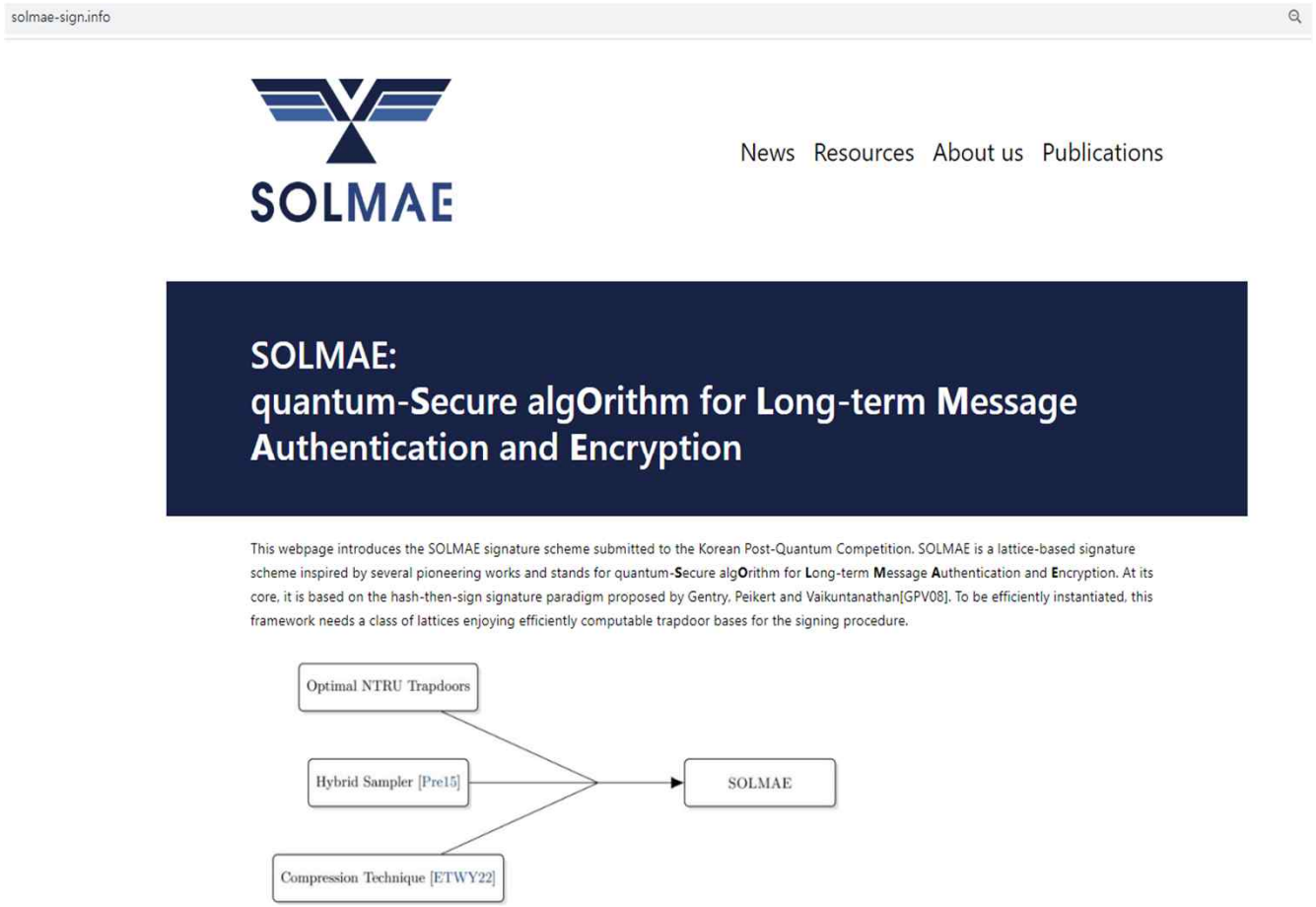
KAIST

IRCS 국제사이버보안연구원

Contents

Overview of SOLMAE

http://solmae-sign.info



✓ 국제사이버보안연구원, 한국형 양자내성 전자서명 방식 '솔매' 개발

https://www.boannews.com/media/view.asp?idx=119368&page=1&kind=3

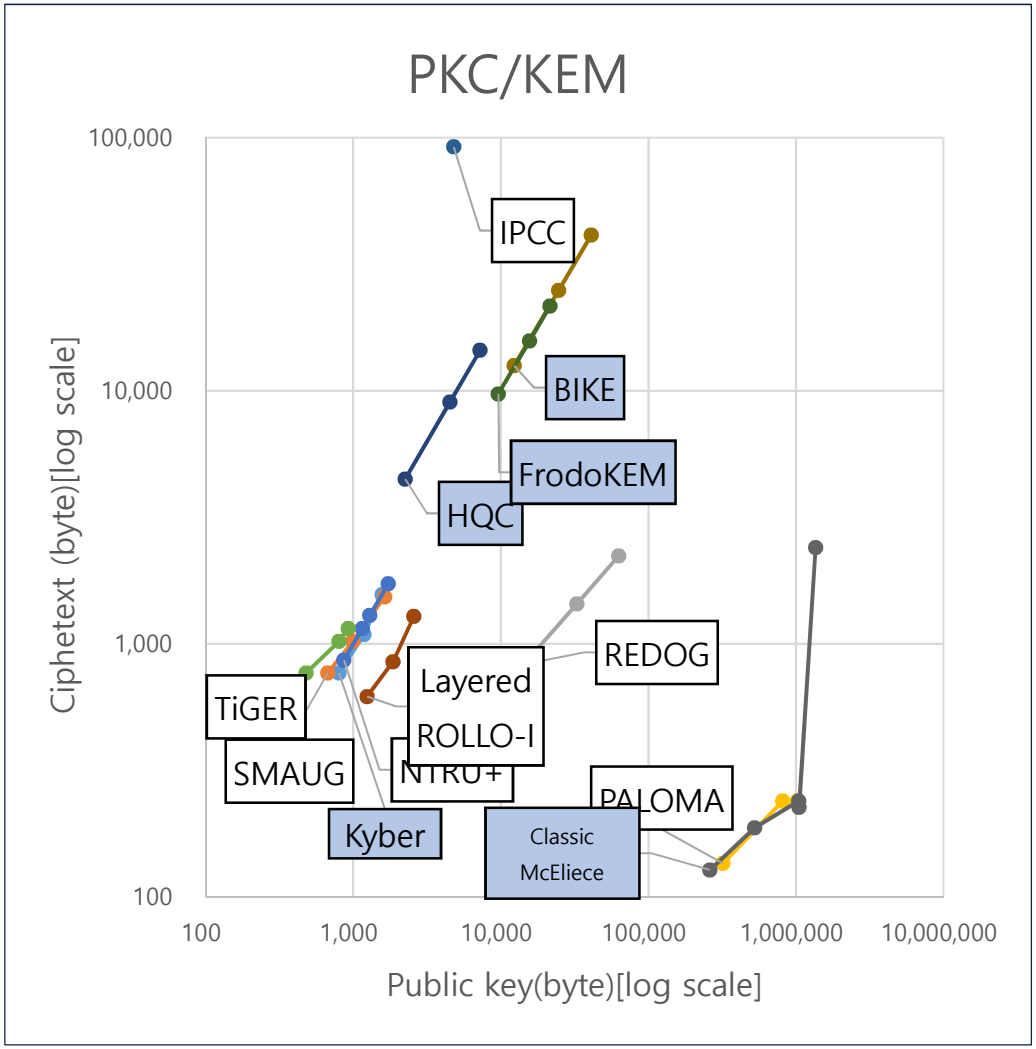
quantum-Secure algOrithm for Long-term Message Authentication and Encryption

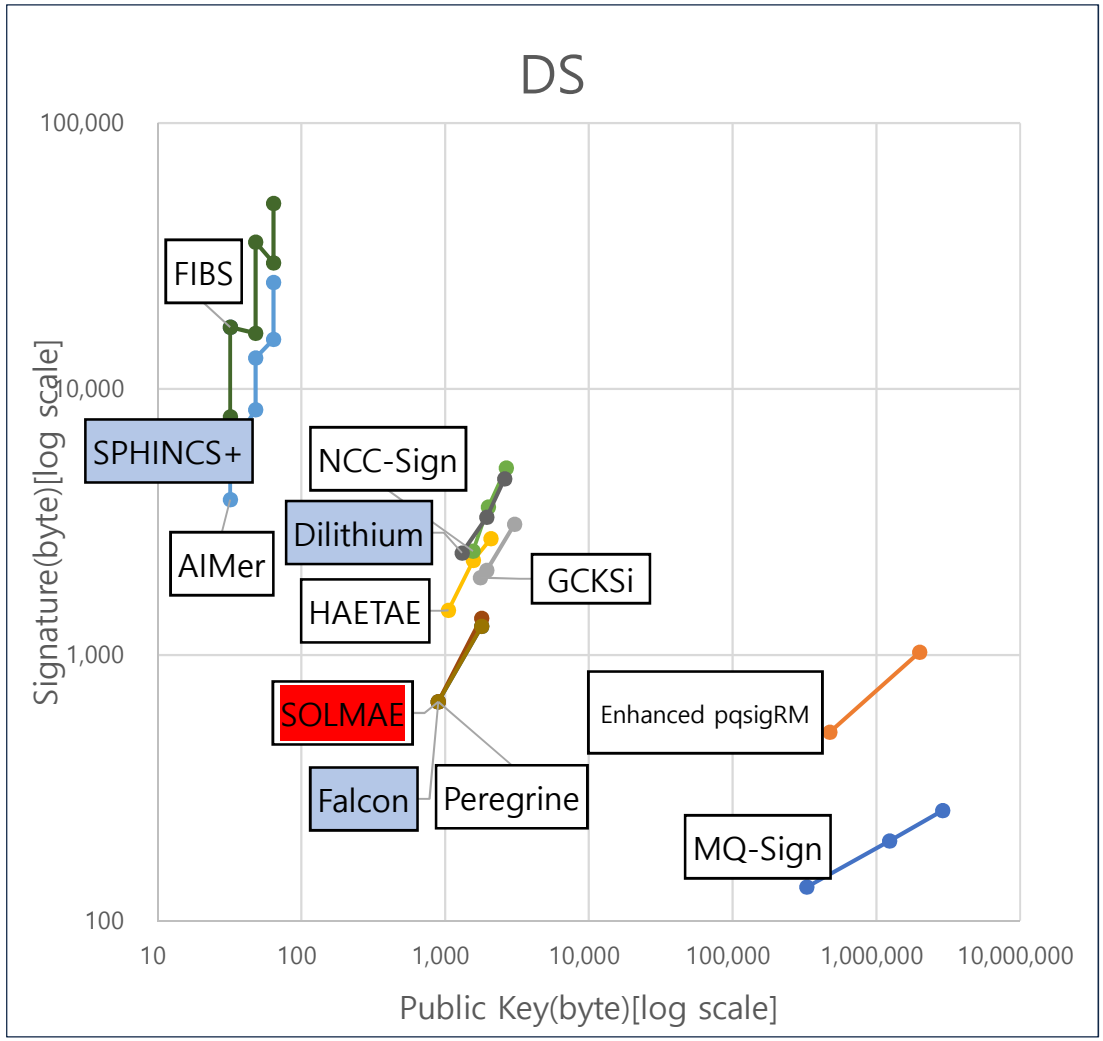
SOLMAE Team

- Korean PI
  - Kwangjo Kim (President@IRCS, Emeritus Prof.@KAIST), https://caislab.kaist.ac.kr/~kkj
- Member (7 persons)
  - Mehdi Tibouchi (NTT, Japan), https://www.normalesup.org/~tibouchi/
  - Thomas Espitau (PQshield, UK), https://espitau.github.io/
  - Alexandre Wallet (INRIA Rennes, France), https://awallet.github.io/
  - Yang Yu(Tsinghua University, China), https://yuyang-crypto.github.io/
  - Akira Takahashi(U. of Edinburgh, Scotland), https://akiratk0355.github.io/
  - Sylvain Guilley (Secure-IC, France), https://perso.telecom-paristech.fr/guilley/
  - Seungki Kim(U. of Cincinnati, USA), https://sites.google.com/view/seungki/home

Comparison of KpqC R1 Algorithms*

: NIST PQC Standard





*from KRnet2023 presentation by NSR

KAIST

IRCS 국제사이버보안연구원

SCIS2023, Riga Royal Hotel,
Kogura, Japan, Jan. 26 (Thu.) 2023

SOLMAE was proposed to KpqC Competition

Prof. Kwangjo Kim
IACR Fellow

Emeritus Professor@KAIST / President@IRCS

Acknowledgement : My travel to SCIS2023 was fully supported by Prof. Kouichi Kakurai, Kyushu Univ.

KAIST

IRCS 국제사이버보안연구원

1st RWPQC2023@Tokyo in Mar. 26, 2023

SOLMAE

https://rwpqc.org/

We are the **Real World PQC** workshop.

Our aim is to bring together the industry, academia and standardization bodies to think about the tasks we will encounter ahead of integrating post-quantum algorithms to the networks, protocols and systems we use today. Our aim will be informed by sharing knowledge about the latest advances of cryptanalysis, the state of different algorithms, and implementation concerns.

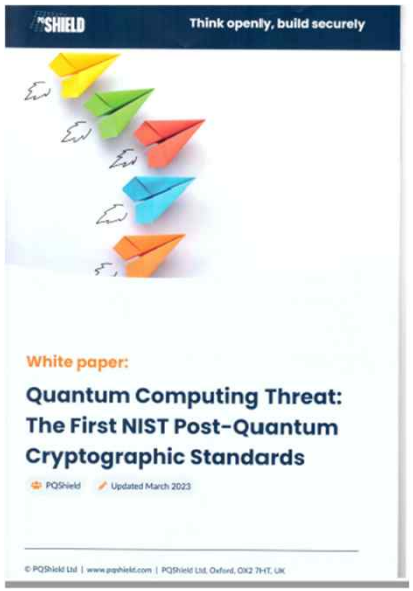
We believe it is very important to start organizing around this topic now as we begin to face the challenges of migrating our systems to post-quantum cryptography. Welcome to the first instantiation of our workshop!

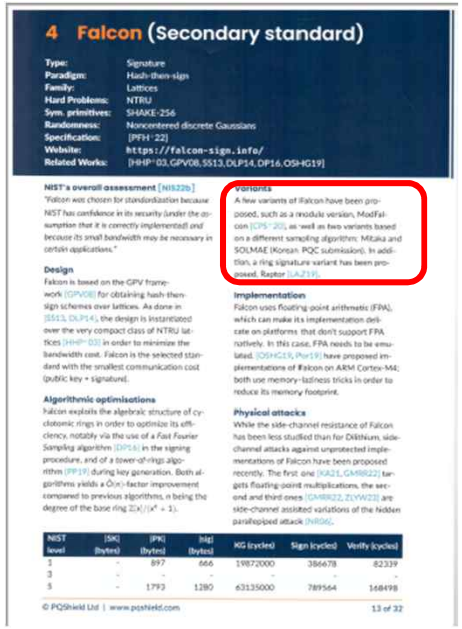
SCHEDULE

Activity
Workshop Kick-Off – Daniel Apon (MITRE)
Opening Remarks – Charles Clancy (MITRE)
Invited Talk #1 NIST and PQC – Dustin Moody (NIST)
Lessons Learned Talks of the selected candidates Kyber – Peter Schwabe (Max Planck Institute for Security and Privacy) Dilithium – Vadim Lyubashevsky (IBM Research) Falcon – Thomas Prest (PQShield) SPHINCS+ – Andreas Hülsing (Eindhoven University of Technology)
Coffee Break
Invited Talk #2 IETF Efforts in PQC – Douglas Stebila (University of Waterloo)
Roundtable #1 – Implementation and side channels Moderator: James Howe Participants: Thomas Pornin (NCC), Tobias Schneider (NXP), Daniel Genkin (Georgia Tech), Mélissa Rossi (ANSSI), Patrick Longa (Microsoft Research)
Lunch Break
Invited Talk #3 ANSSI's recommendations on the migration plan – Mélissa Rossi (ANSSI)
Roundtable #2 – Industry side discussion Moderator: Marc Manzano Participants: Carlos Aguilar (SandboxAQ), Rafael Misoczki (Meta), Craig Costello (Microsoft), Panos Kampanakis (AWS), Tancrède Lepoint (AWS), Scott Fluhrer (Cisco)
Coffee Break
Roundtable #3 – Current state of cryptanalysis Moderator: Daniel Apon Participants: Ward Beullens (IBM Research), Chloe Martindale (University of Bristol), Martin Albrecht (SandboxAQ, King's College London), Leo Ducas (CWI), Ray Perlner (NIST)
Invited Talk #4 The bright present and future of lattice-based zero-knowledge proofs – Vadim Lyubashevsky (IBM Research)
Recent Results / Lightning Talks: GlowingMoltenHotRealPQC (5 minute slots) Submissions closed: please see below for information. Moderator: Sofia Celi
Closing remarks – Sofia Celi (Brave)

RWC2023 by IACR was held Mar. 27-29, Tokyo, Japan

Prest's presentation@1st RWPQC





https://www.youtube.com/watch?v=J0QpSV2xSvM&t=17347s

KAIST

IRCS 국제사이버보안연구원

How SOLMAE was designed

Prof. Kwangjo Kim
IACR Fellow

President@ IRCS / Emeritus Professor@ KAIST

Key Features of RSA and SOLMAE

Table 1: Key Features of RSA and SOLMAE

Item	RSA	SOLMAE
Mathematics	Number Theory	Algebra
Basic operation	Mod. Exp.	Polynomial
Trapdoor	Mul. Inverse	NTRU
Verification	$Left = Right$	$Left \leq Right$
Gaussian sampling	No	Yes
Security assumption	Integer Fact.	SIS
Worst to avg. red.	No	Yes
Classical attack	No	No
Quantum attack	Yes	No

Comparison of SOLMAE and ECDSA

Table 3: Comparison of SOLMAE and ECDSA

		SOLMAE	ECDSA
Specification		512	P256r1
Size(Bytes)	pk	1,792	65
	sgn	1,375	32
Time	KeyGen(ms)	30.21	2.53
	Sign(μs)	288.2	2,582.8
	Verif(μs)	55.6	7,744.7

Chinese Standard Seminar (Online presentation)
Jul. 2(Sun.), 2023

How SOLMAE was developed to meet KpqC Competition

Prof. Kwangjo Kim

IACR Fellow

President@ IRCS / Emeritus Professor@ KAIST

Current Status of KpqC Standard Competition in Korea

IACR Fellow Kwangjo Kim

President@IRCS/Emeritus
Prof@KAIST
kkj@kaist.ac.kr

https://mp.weixin.qq.com/s/vsjRK24NPWWDKzz6ryTKoQ

✓ 家：越早 后量子公 究, 于中 得相 主 越有利*

* Domestic experts: The sooner you participate in post-quantum public key research, the more beneficial it will be for China to gain the relevant initiative.

KAIST

IRCS 국제사이버보안연구원

Comparison of SOLMAE vs. FALCON by Python

Theoretical and Empirical Analysis of FALCON and SOLMAE using their Python Implementation

Anonymous Authors

No Institute Given

Abstract. Since NIST has recently selected FALCON as one of quantum–resistant digital signatures which uses the hash-and-sign paradigm in the style of Gentry–Peikert–Vaikuntanathan framework and instantiated over NTRU lattices, SOLMAE as a variant of FALCON was submitted to KpqC standard competition by taking all the pros of FALCON and Mitaka and reducing their cons as much as possible.
In this paper, we suggest the asymptotic computational complexity of FALCON and SOLMAE take $\Theta(n \log n)$ in their `KeyGen`, `Sign` and `Verif` procedures simultaneously, but our computer experiments using their Python implementation exhibit empirically that `KeyGen` of FALCON–512 takes longer time than that of SOLMAE–512 by about a second while the other two procedures are running almost the same time. We show a sample execution of FALCON–512 and SOLMAE–512 with their real value are described in detail for the educational purpose to understand FALCON and SOLMAE easily. We also checked the Gaussian randomness of $\mathcal{N}$-`Sampler` and `UnifCrown` samplers used in SOLMAE only.

Keywords: Lattice-based cryptography · Hash-and-sign paradigm · NTRU trapdoors · Discrete Gaussian sampling · Python implementation

Introduction

When Shor [16] has proposed an efficient randomized algorithm on a hypothetical quantum computer in 1999 to integer factorization and discrete logarithm problems in a polynomial time, it was beyond our imagination building for the powerful computing environment at that time. Currently the threat of attacking the current (or classical) secure system by using the quantum computer is expected to be right at our fingertips due to the aggressive road map by IBM quantum computing. We are very concerned about so called *Harvest now, decrypt later* attack [17] which is a surveillance strategy that relies on the acquisition and long-term storage of currently unreadable encrypted data awaiting possible breakthroughs in decryption technology that would render it readable in the future.

Due to the substantial amount of research on quantum computers, large-scale quantum computers if built, can break many public-key cryptosystems based on the number–theoretic hard problems in use. In 2016, NIST [14] has initiated Post Quantum Cryptography(PQC) project to solicit, evaluate, and standardize one or more quantum-resistant cryptographic algorithms for Key Encapsulation Mechanism(KEM) and Digital Signature(DS) worldwide. After several rounds, NIST has finally selected CRYSTALS-Kyber for KEM and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for DS in 2022.

Influenced by this NIST PQC project, Korean cryptographic society led by KpqC task force [11] has called for soliciting Korean PQC standard candidates by the end of Oct. in 2022. By the due of submission, 7 candidates KEM and 8 candidates DS for KpqC competition were submitted and their details are available at https://kpqc.or.kr/.

SOLMAE [1] was submitted to KpqC Competition as one of DS candidate algorithms which is a lattice-based signature scheme inspired by several pioneering works based on the hash-then-sign signature paradigm proposed by Gentry, Peikert and Vaikuntanathan [6].

SOLMAE is inspired from FALCON's design. Some of the new theoretical foundations were laid out in the presentation of Mitaka [1]. At a high level, it removes the inherent technicality of the sampling procedure, and most of its induced complexity from an implementation standpoint, for *free*, that is with no loss of efficiency. This simplicity translates into faster operations while

[1] This is an acronym of quantum–Secure algOrithm for Long–term Message Authentication and Encryption.

8 Concluding Remarks

FALCON is claimed to have the advantage of providing short public keys and signatures as well as high–security levels; plagued by a contrived signing algorithm, not very fast for signing and hard to parallelize; very little flexibility in terms of parameter settings. However, SOLMAE has a simple, fast, parallelizable signing algorithm, with flexible parameters with its novel key generation algorithm.

In this paper, after giving a brief description of the specification of FALCON and SOLMAE, we found that their asymptotic computational complexity of `KeyGen`, `Sign` and `Verif` procedures take $\Theta(n \log n)$ simultaneously. Also, our computer experiments using their Python implementation exhibit empirically that `KeyGen` of FALCON–512 only takes longer time than that of SOLMAE–512 by about a second. But we can say that this is not an exact evaluation of their performance by Python implementation.

Further work such as elaborated analysis of computational complexity on FALCON and SOLMAE asymptotically is left to do next.

Acknowledgement

Omitted for anonymous submission.

References

1. 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. Advances in Cryptology, Proc. of EUROCRYPTO 2022, Part III pp. 222–253 (2022) 1, 8
2. Espitau, T., Tibouchi, M., Wallet, A., Yu, Y.: Shorter hash-and-sign lattice-based signatures. Advances in Cryptology, Proc. of CRYPTO 2022, Part II pp. 245–275 (2022) 8
3. Fouque, P.A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z.: Falcon: Fast-fourier lattice-based compact signatures over ntru, https://falcon-sign.info/ 5, 6, 12, 16
4. Fouque, P.A., Kirchner, P., Tibouchi, M., Wallet, A., Yu, Y.: Key recovery from gram-schmidt norm leakage in hash-and-sign signatures over ntru lattices. Cryptology ePrint Archive, Paper 2019/1180 (2019), https://eprint.iacr.org/2019/1180, https://eprint.iacr.org/2019/1180 6
5. G. E. P. Box, M.E.M.: A note on the generation of random normal deviatess. Ann. Math. Statist. pp. 610–611 (1958) 15
6. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Ladner, R.E., Dwork, C. (eds.) 40th ACM STOC. pp. 197–206. ACM Press (May 2008). https://doi.org/10.1145/1374376.1374407 1, 5
7. Goldreich, O., Goldwasser, S., Halevi, S.: Public-key cryptosystems from lattice reduction problems. Advances in Cryptology, Proc. of Crypto 1997 pp. 112–131 (1997) 5
8. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998. Lecture Notes in Computer Science, vol. 1423, pp. 267–288. Springer (1998) 4
9. Kim, K., Tibouchi, M., Espitau, T., Takashima, A., Wallet, A., Yu, Y., Guilley, S., Kim, S.: Solmae : Algorithm specification. Updated SOLMAE, IRCS Blog (2023), https://ircs.re.kr/?p=1714 7, 8, 9, 10, 14, 18
10. Kim, W.: Mathematical Statistics(in Korean). Minyoungsa, Seoul, Korea (2021) 15
11. KpqC: Korean post-quantum crytography (2020), https://kpqc.or.kr/ 1
12. Min, S., Yamamoto, G., Kim, K.: Weak property of malleability in ntrusign. Proc. of ACISP 2004, LNCS 3108 pp. 379–390 (2004) 5
13. Nguyen, P.Q., Regev, O.: Learning a parallelepiped: Cryptanalysis of ggh and ntru signatures. Journal of Cryptology **22**(2), 139–160 (2009) 5, 14
14. NIST: Post-quantum crytography (2016), https://csrc.nist.gov/projects/post-quantum-cryptography 1
15. Pornin, T., Prest, T.: More efficient algorithms for the NTRU key generation using the field norm. In: Lin, D., Sako, K. (eds.) PKC 2019, Part II. LNCS, vol. 11443, pp. 504–533. Springer, Heidelberg (Apr 2019). https://doi.org/10.1007/978-3-030-17259-6_17 5, 10

KAIST

IRCS 국제사이버보안연구원

Invited Talk to LG U+

2023
양자내성암호
기술 세미나

디지털 암호에서 양자내성 암호로의 변혁

| 일시_ 11월 1일 오후 2시
| 장소_ B1 인사이트홀
| 주최_ 김광조 교수
KAIST 명예교수
| 내용_ 암호의 발전 과정
양자내성암호의 활용

LG U+

2 Papers@Asiacrypt2023

25. Antrag: Annular NTRU Trapdoor Generation

Thomas Espitau, Thi Thu Quyen Nguyen, Chao Sun, Mehdi Tibouchi, Alexandre Wallet

PQShield, Inria Rennes, Osaka University, NTT Social Informatics Laboratories, Univ Rennes, Inria, CNRS, IRISA

Table 2. Practical parameter selection, power-of-two case

	$q = 12289$		$q = 3329$	
d	512	1024	512	1024
Quality α	1.15	1.23	1.23	1.48
Repetition rate M	3	4	4	4
Bit security (C/Q)	124/113	264/240	21/110	265/240
Verification key size (bytes)	896	1792	768	1536
Signature size (bytes)	646	1260	591	1176

Table 3. Practical parameter selection for ANTRAG, 3-smooth conductor case.

(a) Modulus $q = 12289$

d	648	768	864	972
Quality α	1.17	1.19	1.21	1.22
Repetition rate M	4	3	3	4
Bit security (C/Q)	166/151	196/178	222/201	251/227
Verification key size (bytes)	1134	1344	1512	1701
Signature size (bytes)	808	952	1069	1200

(b) Various moduli. For $d = 768, 864, 972$, the right column shows moduli of [14].

	$d = 648$		$d = 768$		$d = 864$		$d = 972$	
Modulus q	3889	9721	3329	18433	3727	10369	4373	17497
Quality α	1.32	1.19	1.39	1.16	1.40	1.23	1.40	1.18
Expected repetitions	4	4	4	3	4	3	4	4
Bit security (C/Q)	159/144	164/149	192/174	195/177	220/200	222/201	254/230	250/227
Verification key size (bytes)	972	1134	1152	1440	1296	1512	1580	1823
Signature size (bytes)	747	796	883	977	1000	1058	1133	1225

Table 4. Performance comparison with FALCON and MITAKA.

	FALCON [33]		MITAKA [14]		This paper	
d	512	1024	512	1024	512	1024
Quality α	1.17	1.17	2.04	2.33	1.15	1.23
Classical sec.	123	284	102	233	124	264
Key size (bytes)	896	1792	896	1792	896	1792
Sig. size (bytes)	666	1280	713	1405	646	1260
`keygen` speed (Mcycles)	—	—	—	—	15.4	55.2
`keygen` speed (ms)	4.7	13.8	*1657**	*6214**	5.7	20.5
`sign` speed (kcycles)	—	—	340	661	334	655
`sign` speed (μs)	204	412	127	246	124	243
`verif` speed (kcycles)	—	—	23	46	23	46
`verif` speed (μs)	21	43	9	17	9	17

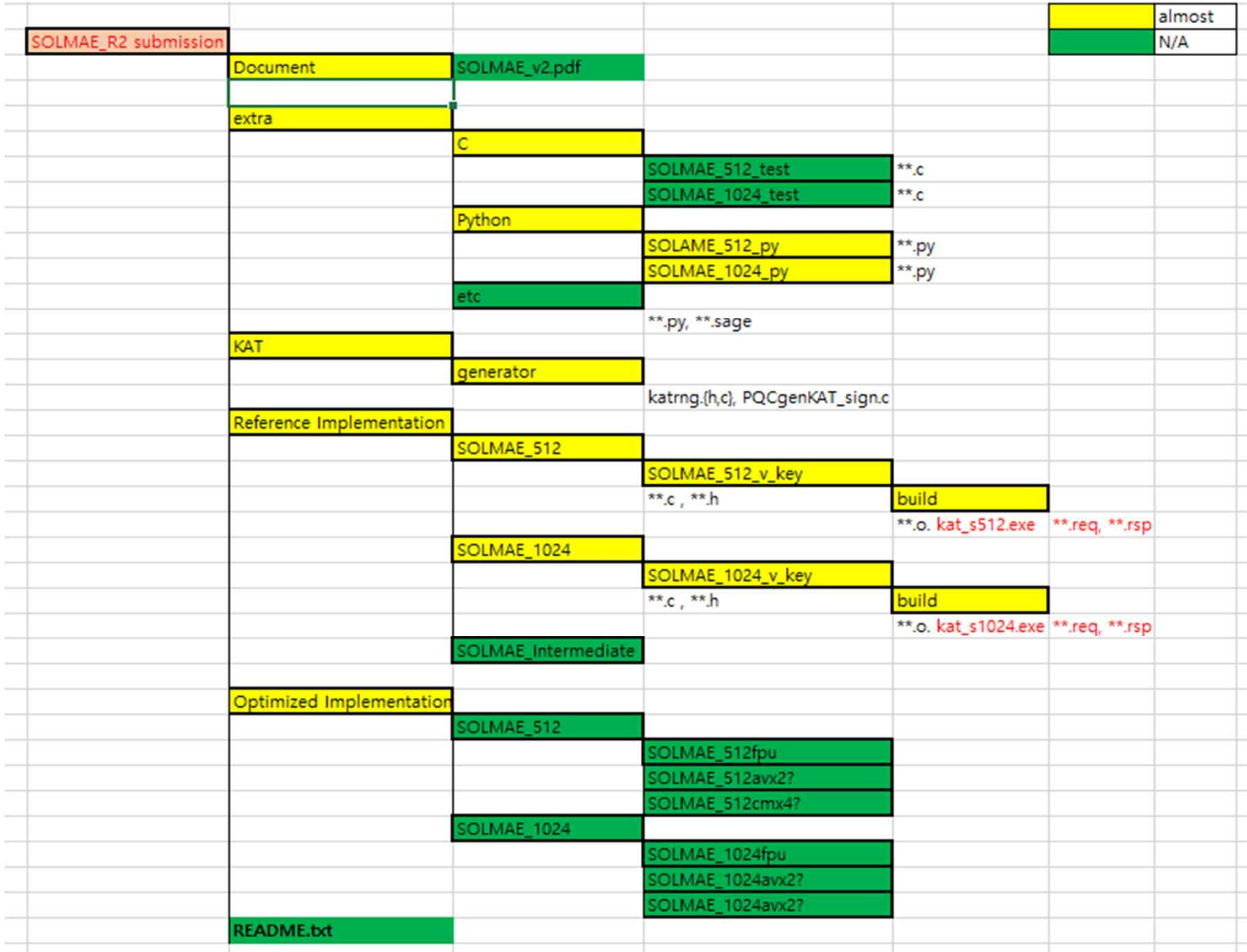
* Timings for the optimized SageMath implementation (excluding NTRUSolve), since no C implementation exists.

85. On Gaussian sampling, smoothing parameter and application to signatures

Thomas Espitau, Alexandre Wallet, Yang Yu

PQShield, France, Univ Rennes, Inria, CNRS, IRISA, Tsinghua University, Beijing, China

Deliverables of SOLMAE Round 2 (if OK)



Summary

- After Round 1 submission of SOLMAE package,
  The followings were done:
  1. SOLMAE web page (https://solmae-sign.info) was opened
  2. International (Japan and China) invited & domestic talks/ papers
  3. Python Implementation of SOLMAE(https://github.com/kjkim0410/SOLMAE_python_512) and comparison with FALCON

- 2 papers on SOLMAE accepted to Asiacrypt2023@China

- International reputations on SOLMAE are rapidly increasing

- Still lots of job are remaining!!