Post-Quantum

Cryptography Conference

Update on the NIST standardization of additional signature schemes

In this presentation, Mr. Andrew Regenscheid, a distinguished expert from the U.S. National Institute of Standards and Technology (NIST), will take you on a deep dive into NIST's standardization efforts for additional signature schemes. In October 2024, NIST announced 14 Second-Round candidates chosen from 40 First-Round submissions, including CROSS, LESS, and even MAYO, which might bring a bit of flavor to the new algorithms. These algorithms were selected based on rigorous evaluations of security, performance, and unique algorithm characteristics, reflecting NIST's ongoing commitment to diversifying post-quantum cryptographic standards. Dr. Moody will discuss each selected scheme's potential, addressing key innovations and the next steps in the standardization process.

Andrew Regenscheid

Manager Cryptographic Technology Group at NIST

January 15 and 16, 2025 - Austin, TX (US) | Online

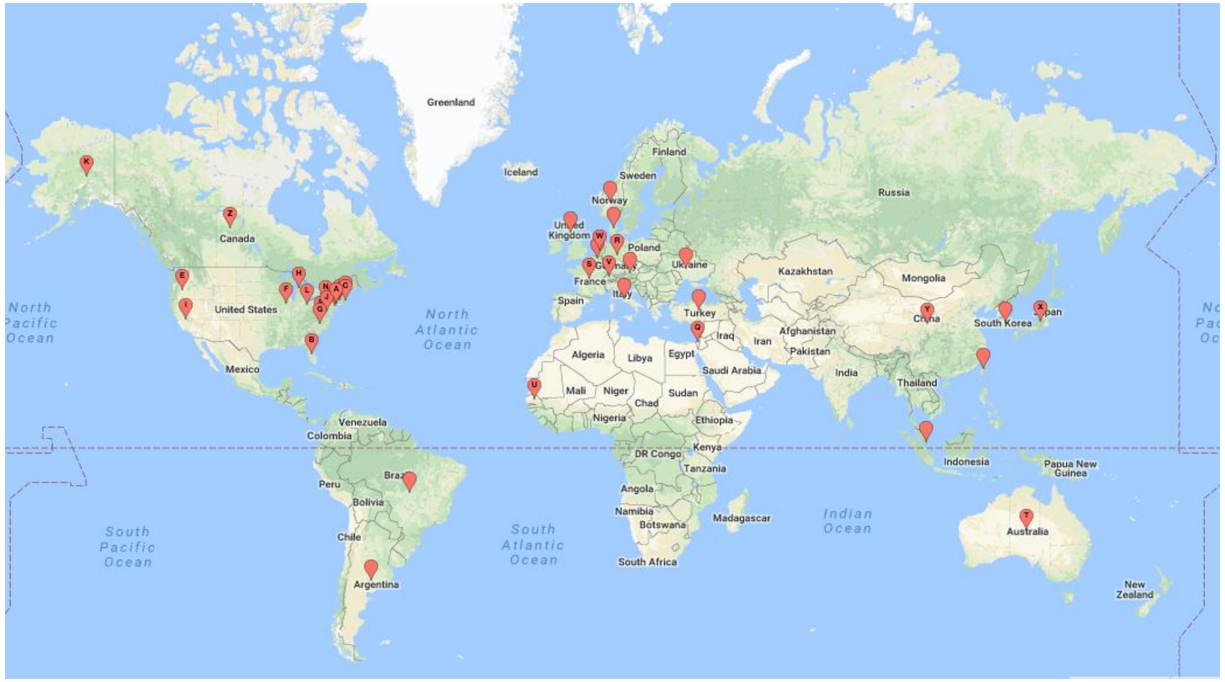
Update on the NIST standardization of Additional Signature Schemes

Andy Regenscheid
Cryptographic Technology Group, NIST

Tuesday, October 3rd, 2023

NIST PQC Standards – Milestones and Timeline

NIST



2010-2015– NIST PQC project team builds & First PQC Conference

2016– Determined criteria and requirements, Call for proposals

2017– Received 82 submissions, ***69 First Round candidates***

2018– 1st NIST PQC Standardization Conference

2019 – Announced ***26 Second Round candidates***
Released NISTIR 8240
Held the 2nd NIST PQC Standardization Conference

2020– Announced ***7 finalists & 8 alternate candidates***
Released NISTIR 8309

2021– Hold 3rd NIST PQC Standardization Conference

2022– ***Announced Initial Selections for Standardization & 4th Round Candidates***
Held 4th NIST PQC Standardization Conference

2023 Released draft standards and call for public comments

2024- Released Final Standards

The first Set of NIST PQC Standards

FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard (Based on CRYSTALS-Kyber)	FIPS 204 Module-Lattice-Based Digital Signature Standard (Based on CRYSTALS-Dilithium)	FIPS 205 Stateless Hash-Based Digital Signature Standard (Based on SPHINCS+)	FIPS 206 FFT-Over-NTRU-Lattice-Based Digital Signature Standard (Based on FALCON, under development)
• A module learning with errors (MLWE)-based key encapsulation mechanism (KEM) • Good performance in different platforms • An algorithm for key establishment in security protocols	• A lattice-based digital signature algorithm based on the Fiat-Shamir paradigm • Good performance, simple implementation, moderate public-key and signature size, suitable for general applications	• Not require to keep track of any state between signatures • Solid security, signatures are longer compared with ML-DSA	• Hash and sign paradigm • Smaller bandwidth and fast verification but more complicated implementation

Published August 2024! (FIPS 203, 204, 205)

Onramp for Additional Digital Signature Schemes

Why has NIST called for additional post-quantum signatures?

- NIST is primarily interested in additional general-purpose signature schemes that are ***not*** based on structured lattices
- NIST may also be interested in signature schemes that have short signatures and fast verification
- Any lattice signature would need to significantly outperform CRYSTALS-Dilithium and FALCON and/or ensure substantial additional security properties

Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process

Updated October 2022 to reflect that IP statements can be accepted digitally.

Table of Contents

Authority: This work is being initiated pursuant to NIST's responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107–347.

Onramp Process

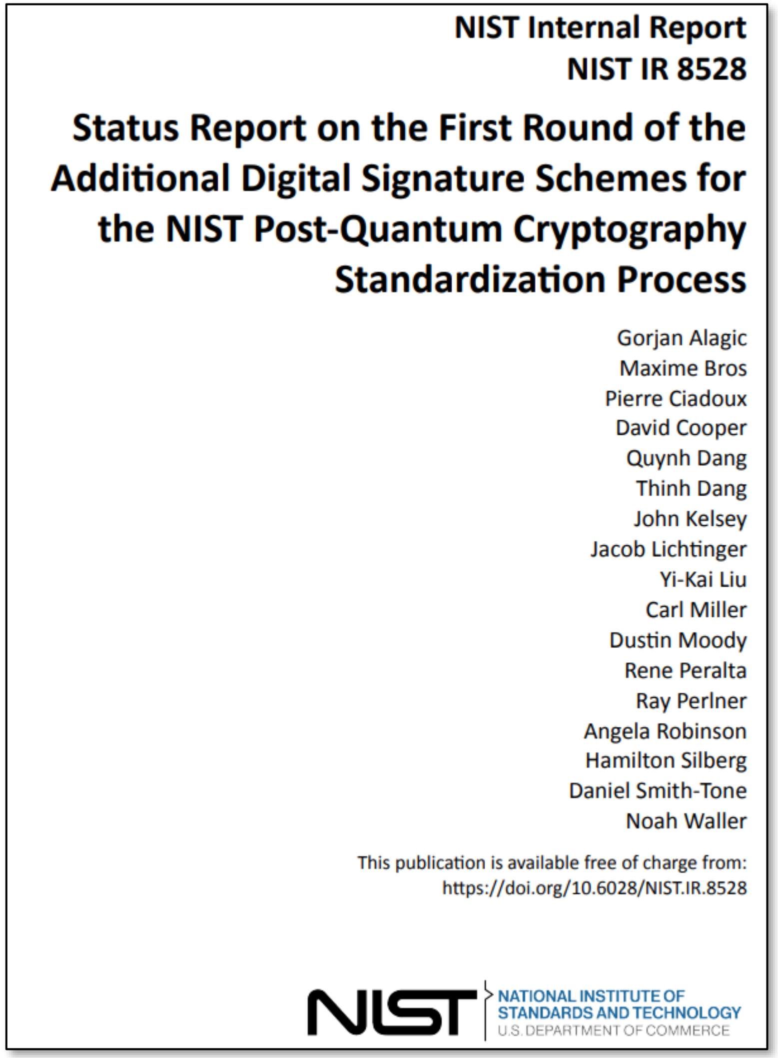
July 2022
- Announced new Call for Proposals

Sept. 2022
- CFP Published

June 2023
- Deadline for Submissions
- Announced 40 First-Round Candidates

April 2024
- 5th PQC Standardization Conference

Oct. 2024
- Announced 14 Second-Round Candidates



NIST Internal Report
NIST IR 8528

Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process

Gorjan Alagic
Maxime Bros
Pierre Ciadoux
David Cooper
Quynh Dang
Thinh Dang
John Kelsey
Jacob Lichtinger
Yi-Kai Liu
Carl Miller
Dustin Moody
Rene Peralta
Ray Perlner
Angela Robinson
Hamilton Silberg
Daniel Smith-Tone
Noah Waller

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8528

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Submission Teams

- 50 submissions received by the deadline

- 262 distinct submitters
  - There are 4 submitters who each have 4 submissions
  - There are 6 submitters who each have 3 submissions
  - There were 278 distinct submitters back in 2017
  - 45 people submitted in 2017 and 2023

- As of 2023, we had submitters from 5 continents and 28 countries

Countries

Australia
Austria
Belgium
Canada
China
Denmark
Finland
France
Germany
India
Israel
Japan
Malaysia
Mexico
Netherlands
Norway
Portugal
Senegal
Singapore
Slovakia
South Korea
Spain
Sweden
Switzerland
Taiwan
United Arab Emirates
United Kingdom
United States

First Round Additional Signatures

Multivariate		MPC in-the-head				Lattice	Code	Symmetric	Isogeny	Others
UOV	*Other*	*MinRank*	*SD/Rank-SD*	*PKP*	*MQ*					
Mayo	~~3wise~~	Mira*	Ryde	Perk	~~Biscuit~~	~~EagleSign~~	Cross	~~Aimer~~	SQIsign	~~Alteq~~
~~PROV~~	~~DMEsign~~	MiRitH*	SDitH		MQOM	~~EHT~~	~~E. Pqsign-rm~~	~~Ascon-Sign~~		~~eMLE-Sig 2.0~~
QR-UOV	~~HPPC~~					~~HAETAE~~	~~Fuleeca~~	FAEST		~~KAZ~~
SNOVA						Hawk	LESS	~~SPHINC-α~~		~~Preon~~
~~TUOV~~						~~HuFu~~	~~MEDS~~			~~Xifrat~~
UOV						~~Racoon~~	~~Wave~~			
~~VOX~~						~~Squirrels~~				

* Merged into Mirath

Second Round Candidates

Multivariate	MPC in-the-head				Lattice	Code	Symmetric	Isogeny
UOV	*MinRank*	*SD/Rank-SD*	*PKP*	*MQ*				
Mayo	**Mirath**	**Ryde**	**Perk**	**MQOM**	**Hawk**	**Cross**	**FAEST**	**SQIsign**
QR-UOV		**SDitH**				**LESS**		
SNOVA								
UOV								

Multivariate– UOV-Based Schemes

NIST

Quadratic Polynomial Systems

UOV-based schemes rely on solving multivariate quadratic equations, where the system is constructed such that knowledge of hidden structure (***oil*** and ***vinegar*** variables) allows efficient generation of signatures.

Hash-and-Sign Paradigm

These schemes use a hash function to map a message to a specific point in the quadratic system's range and sign by finding a pre-image using the secret ***oil*** subspace of the system's domain.

Unbalanced Design

The system is "unbalanced" because the number of ***oil*** variables is smaller than the number of ***vinegar*** variables, which is required for security against certain attacks.

Pros

- Very short signature (200B)
- Very fast
- 20+ years of cryptanalysis

Cons

- Very large public keys (~200kB for UOV) unless additional structure is added (as in MAYO, QR-UOV, SNOVA)
- Unnatural security assumption due to UOV trapdoor

Selected UOV-Based Schemes

UOV: A foundational multivariate cryptosystem offering very fast signing and verification with small signatures, but at the cost of large public key sizes

MAYO: UOV variant that dramatically reduces public key size by using a smaller quadratic map (mini-UOV) to generate efficient and compact signatures

QR-UOV: Employs quotient rings to achieve significantly smaller public keys than UOV while maintaining competitive performance

SNOVA: Simplified version of NOVA scheme, a UOV variant that uses non-commutative rings to achieve dramatically reduced public key sizes and fast operations, though some parameter sets were affected by cryptanalysis

Multivariate Schemes (UOV)– Performance

Scheme	Parameters	Public Key (bytes)	Sig. (bytes)	Sign (cycles)	Verify (cycles)
UOV	III-classic	1,225,440	200	299,316	241,588
MAYO	three	2,656	577	1,663,666	610,010
QR-UOV	III-(31, 246, 87, 3)	71,007	232	153,006,000	5,349,000
	III-(127, 228, 78, 3)	71,915	292	1,555,131,000	524,886,000
	III-(7, 1100, 140, 10)	55,173	489	98,376,000	47,636,000
	III-(31, 890, 100, 10)	34,423	643	573,433,000	232,156,000
SNOVA	(56, 25, 2)	31,266	168	964,716	507,009
	(49, 11, 3)	6,006	286	1,365,463	1,004,519
	(37, 8, 4)	4,112	376	1,188,690	544,395

MPC in-the-head Schemes

Zero-Knowledge Proofs (ZKPs)

MPCitH schemes leverage secure Multi-Party Computation (MPC) protocols to construct Zero-Knowledge Proofs, enabling a prover to demonstrate knowledge of a solution to a hard problem without revealing it.

Fiat-Shamir Paradigm

These schemes transform interactive ZKPs into non-interactive digital signatures by applying the Fiat-Shamir heuristic, eliminating the need for direct interaction with the verifier.

Hard Computational Problems

The underlying security of MPCitH schemes relies on well-established hard problems (e.g., MinRank, Syndrome Decoding, or Multivariate Quadratic equations).

Pros

- Small public keys
- Flexible designs that can be adapted to different mathematical problems

Cons

- Computationally expensive
- Complicated implementations and specifications
- Moderately large signatures
- Recent optimizations were unknown at time of submission resulting in rapidly changing designs

Selected MPCitH Categories

- **MinRank**
  - Based on the MinRank problem, which involves finding a linear combination of matrices with a minimal rank, making it computationally challenging.
  - ***2nd Round Candidates:*** **Mirath**
- **Syndrome Decoding/Rank Syndrome Decoding**
  - Based on decoding problems in linear codes: solving Hamming-Weight-constrained or rank-constrained linear systems, both known to be NP-hard.
  - ***2nd Round Candidates:*** **Ryde, SDitH**
- **Permuted Kernel Problem**
  - Relies on proving knowledge of a permutation that satisfies certain kernel equations. Solving for such a permutation is believed to be computationally hard.
  - ***2nd Round Candidates:*** **Perk**
- **MQ (Multivariate Quadratic Equations)**
  - Based on solving systems of quadratic equations over finite fields, a well-studied NP-hard problem.
  - ***2nd Round Candidates:*** **MQOM**

MPCitH Schemes– Performance

Scheme	Parameters	Public Key (bytes)	Sig. (bytes)	Sign (cycles)	Verify (cycles)
MIRA (Mirath)	192S	121	11,779	119,700,000	116,200,000
	192F	121	15,540	107,200,000	107,000,000
MiRitH (Mirath)	hypercube-IIIb short	205	13,136	71,813,403	75,999,541
	IIIb short	205	13,136	242,531,804	204,853,275
	hypercube-IIIb fast	205	18,459	18,384,614	15,550,479
	IIIb fast	205	18,459	24,538,474	22,470,437
RYDE	192S	131	12,933	49,600,000	44,800,000
	192F	131	16,380	12,200,000	10,700,000
SDitH	gf251-L3-hyp	180	19,544	46,600,000	44,300,000
	gf256-L3-hyp	180	19,544	26,200,000	22,900,000
	gf251-L3-thr	180	25,964	11,100,000	1,500,000
	gf256-L3-thr	180	25,964	16,200,000	5,700,000
PERK	III-short3	230	14,300	80,000,000	64,000,000
	III-fast3	230	18,800	15,000,000	12,000,000
MQOM	L3-gf31-short	73	13,846	108,000,000	102,000,000
	L3-gf251-short	92	14,266	69,500,000	65,600,000
	L3-gf31-fast	73	16,669	56,300,000	51,300,000
	L3-gf251-fast	92	17,252	32,900,000	29,600,000

Selected Lattice Scheme– HAWK

- **Lattice-based hash-and-sign signature scheme that has some similarities to Falcon**
  - The public key is the Gram matrix (basis vector lengths and inner products) for a bad basis for the integer lattice
  - The secret key gives a transformation mapping between the bad basis and the standard basis for the integer lattice
  - To sign, a message is hashed and interpreted as a rational linear combination of bad basis vectors, **h**.
  - The standard basis is then used to find an element in the lattice that is sufficiently close to **h** without leaking information about the secret key
- **Comparison to Falcon**
  - Falcon uses the Fast Fourier Transform to sign messages
  - HAWK relies on the one more shortest vector problem (omSVP) and search module lattice isomorphism problem (smLIP) over the integer lattice
  - HAWK can be implemented without floating point arithmetic

Pros

- Strong performance
- Avoids problematic floating point arithmetic

Cons

- Performance similar to Falcon
- Security relies on omSVP and smLIP problems – not as well studied as more conventional lattice problems

Lattice Scheme (HAWK)– Performance

Scheme	Parameters	Public Key (bytes)	Sig. (bytes)	Sign (cycles)	Verify (cycles)
HAWK	512-Cat1	1,024	555	85,372	148,224
	1024-Cat5	2,440	1,221	180,816	302,861
Falcon	512-Cat1	897	666	1,009,764	81,036
	1024-Cat5	1,793	1,280	2,053,080	160,596
ML-DSA	ML-DSA-65-Cat3	1,952	3,309	529,106	179,424
	ML-DSA-87-Cat5	2,592	4,627	642,192	279,936

Code-Based Schemes

CROSS

- Fiat-Shamir transform on a interactive zero-knowledge proof of knowledge (ZKPoK) identification protocol
- Two variants based on Syndrome Decoding Problems:
  - **R-SDP–** Restricted Syndrome Decoding Problem
  - **R-SDP(G)–** Restricted Syndrome Decoding Problem with subgroup **G**
- ‘Small’ and ‘Fast’ variants

LESS

- Fiat-Shamir transform on an interactive ZKPoK of the solution to a computational code equivalence problem
- Security based on Linear Equivalence Problem (LEP)
- New variant used Canonical Form LEP to reduce signature size
- ‘Balanced’ and ‘Short Signature’ variants

Pros

- Smaller signatures than SLH-DSA
- ***CROSS*** – faster signing than SLH-DSA
- ***LESS*** – small signatures (~3KB) proposed

Cons

- ***LESS*** – Large public keys
- ***LESS*** – Slow signature verification
- Mathematical problems are relatively new- more analysis is needed for confidence

Code-Based Schemes– Performance

Scheme	Parameters	Public Key (bytes)	Sig. (bytes)	Sign (cycles)	Verify (cycles)
CROSS	R-SDP(G) 3 balanced	59	23,380	2,630,000	1,530,000
	R-SDP 3 balanced	91	28,222	4,970,000	2,890,000
LESS	3s	70,144	13,722	2,984,300,000	3,075,100,000
	3b	35,020	17,203	2,446,900,000	2,521,400,000
SLH-DSA	SHAKE-192s	48	16,224	8,091,419,556	6,465,506
	SHAKE-192f	48	35,664	386,861,992	19,876,926

Other Schemes

NIST

FAEST

- Vector Oblivious Linear Evaluation in the Head (VOLEitH) framework
- Fiat-Shamir transform to an interactive ZKPoK on signing key shares
- Unforgeability relies only on the security of symmetric-key cipher– AES

Pros
- Very small public keys
- Competitive performance

Cons
- Slower than lattice-based schemes
- VOLEitH relatively new, and algorithm changes expected

SQISign

- Fiat-Shamir transform to ZK/sigma identification protocol
- Security based on difficulty of finding isogenies between supersingular elliptic curves
- Uses different assumptions and techniques than SIKE

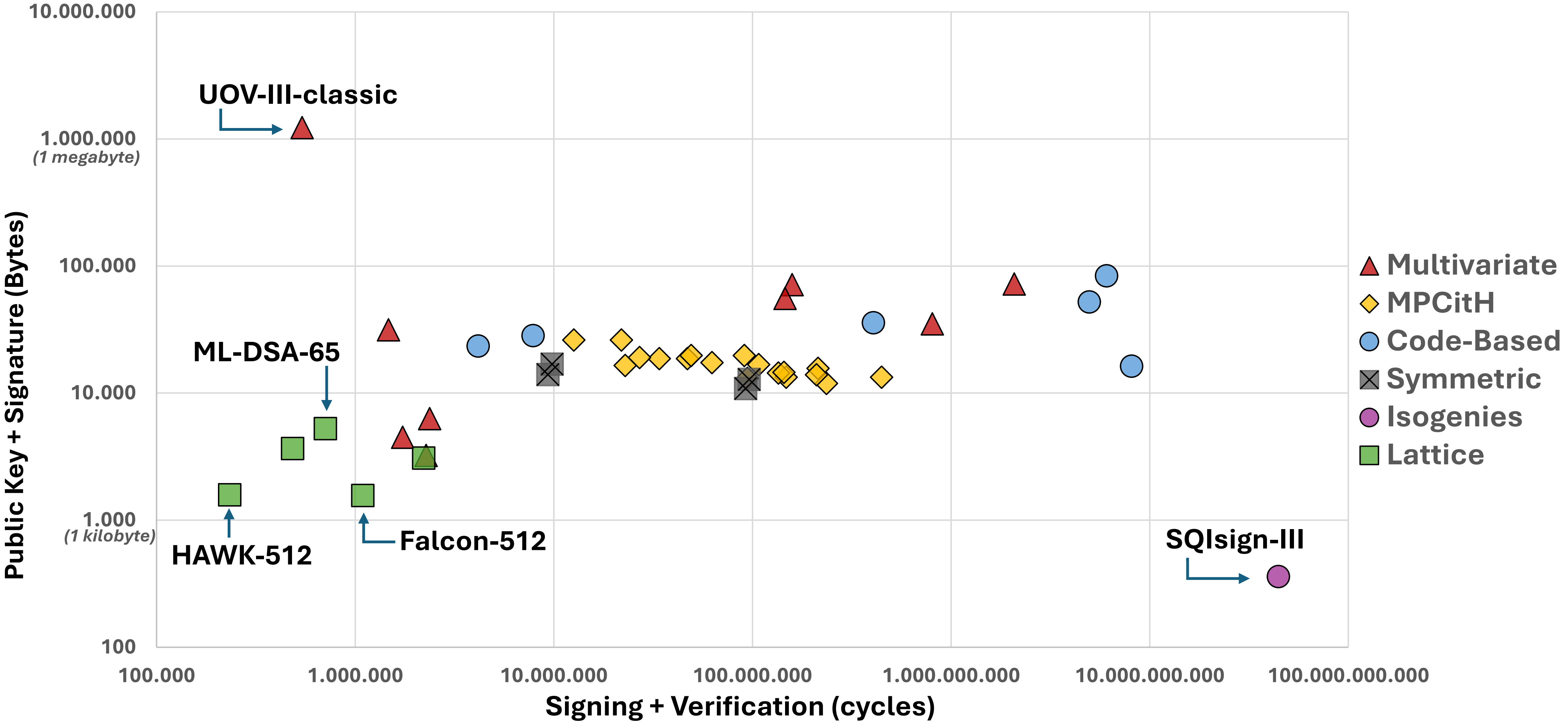
Pros
- Very small signatures and public keys

Cons
- Very slow performance (but improvements expected)
- New design– more analysis needed

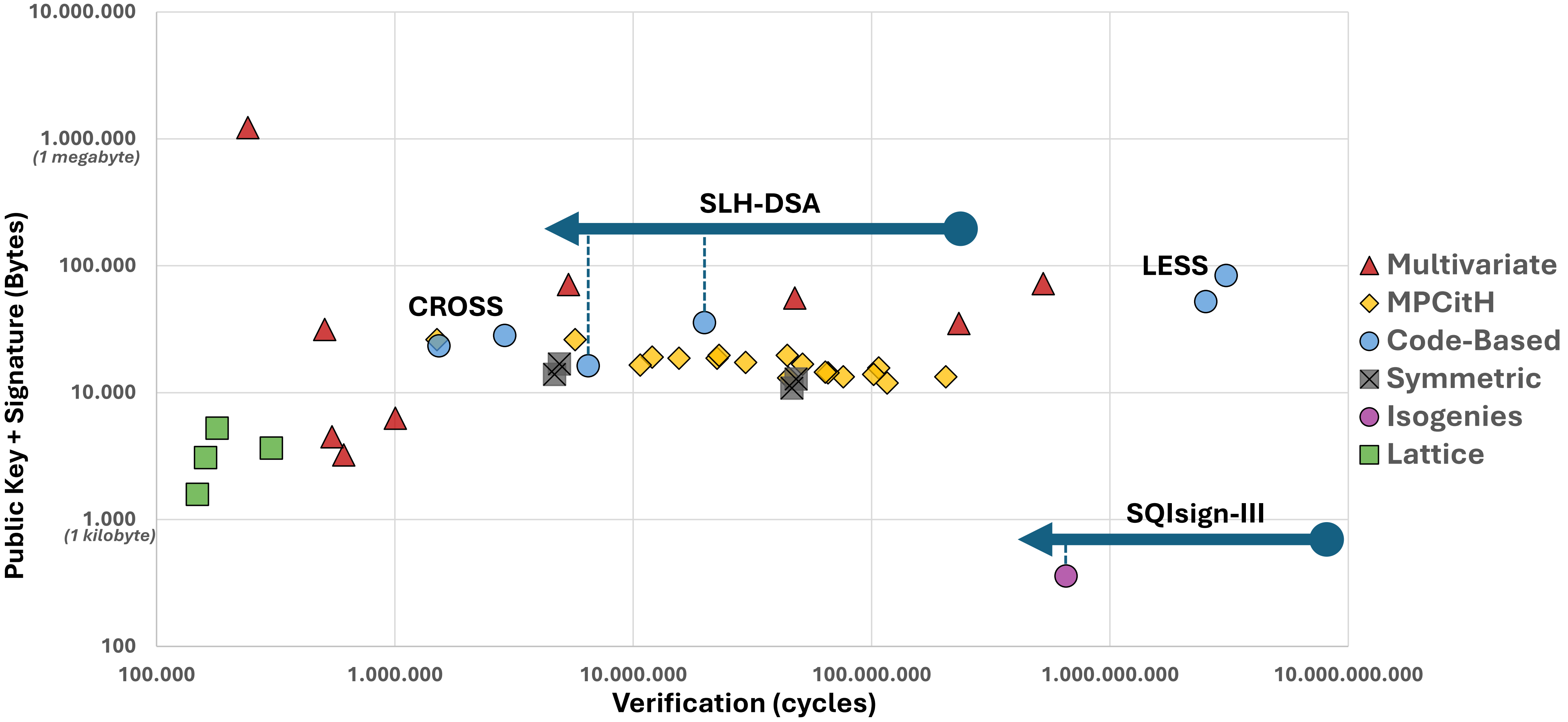
Other Schemes– Performance

Scheme	Parameters	Public Key (bytes)	Sig. (bytes)	Sign (cycles)	Verify (cycles)
FAEST	EM-192s	48	10,824	46,150,000	46,300,000
	192s	64	12,744	47,950,000	48,275,000
	EM-192f	48	13,912	4,675,000	4,675,000
	192f	64	16,792	4,900,000	4,900,000
SQIsign	III	96	263	43,760,000,000	654,000,000

Performance Summary (log scale)

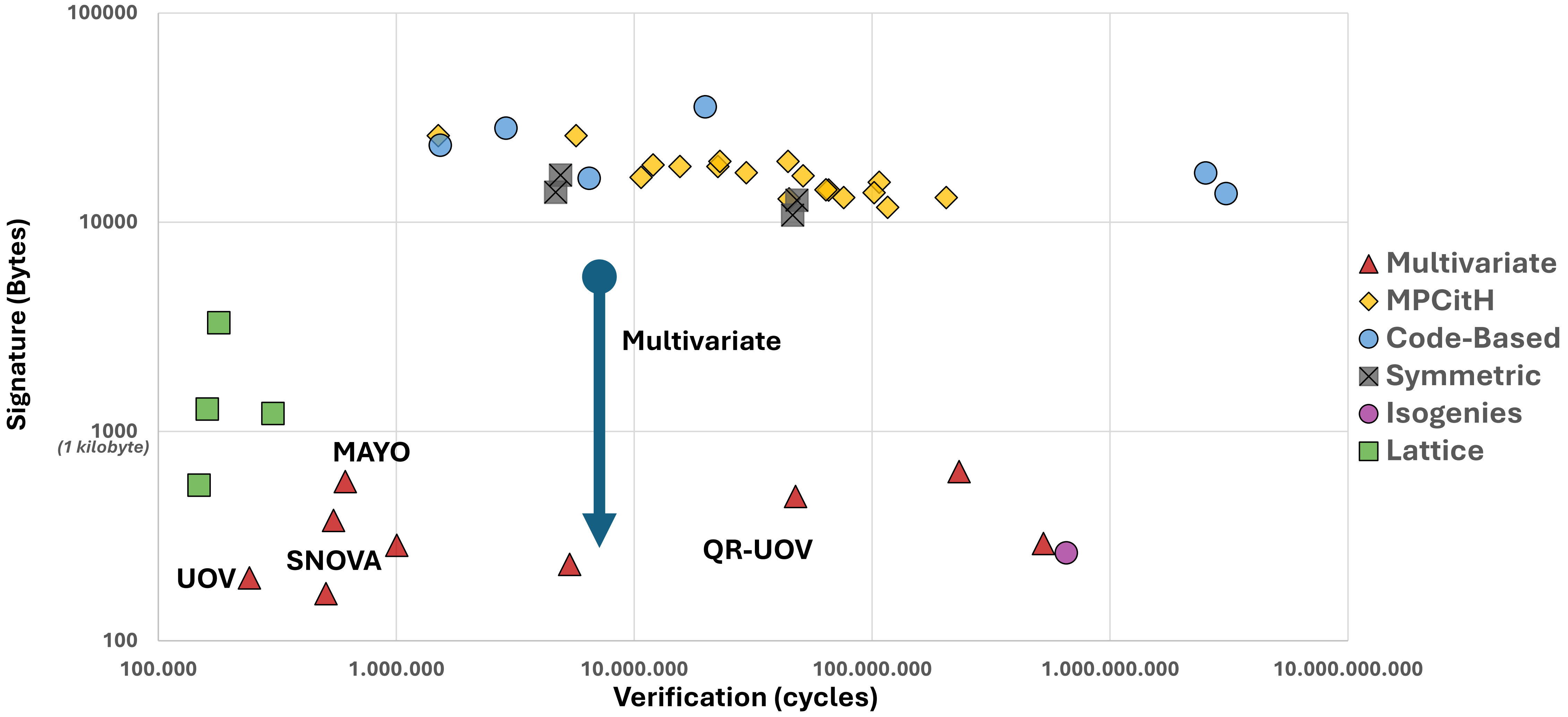


Performance Summary– Verification (log scale)



Performance Summary– Signature Size (log scale)

NIST

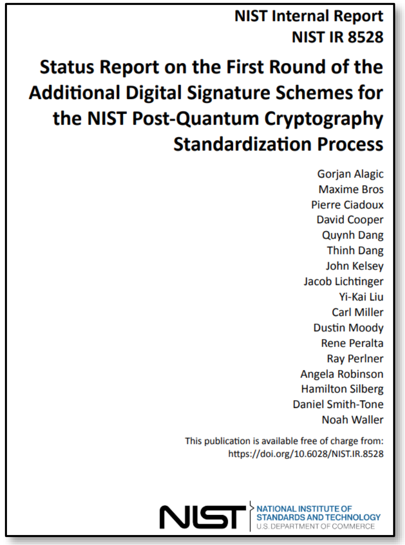


NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Next Steps

PQC Project Next Steps

- Ongoing evaluation of 2nd Round Additional Signature Candidates
  - Tweaks must be submitted to NIST by February 5 (*extended*)
  - 3rd round planned for 2026
- Sixth NIST PQC Standardization Conference
  - September 2025 (tentative)
  - In-person, DC-region
- ML-KEM, ML-DSA, & SLH-DSA finalized on August 2024
  - Draft FN-DSA (Falcon) standard under development
- NIST plans to make 4th round KEM selection soon
  - Classic McEliece
  - BIKE
  - HQC
  - ~~SIKE~~

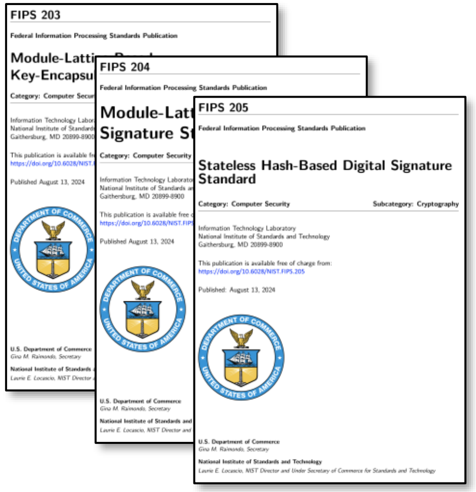

NIST Internal Report
NIST IR 8528

Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process

Gorjan Alagic
Maxime Bros
Pierre Ciadoux
David Cooper
Quynh Dang
Thinh Dang
John Kelsey
Jacob Lichtinger
Yi-Kai Liu
Carl Miller
Dustin Moody
Rene Peralta
Ray Perlner
Angela Robinson
Hamilton Silberg
Daniel Smith-Tone
Noah Waller

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8528

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE



Questions

Contact Information

Andrew Regenscheid, Cryptographic Technology Group

Email: Andrew.Regenscheid@nist.gov

NIST PQC standardization

www.nist.gov/pqcrypto

Sign up for ***pqc-forum*** mailing list

Email: pqc-comments@nist.gov

NCCoE PQC Migration Project

www.nccoe.nist.gov/applied-cryptography

Request to join Community of Interest

Email: applied-crypto-pqc@nist.gov