Post-Quantum

Cryptography Conference

NIST standardization of additional signature schemes

Dustin Moody

Mathematician & Project Lead, Post-Quantum Cryptography at NIST

The Onramp

NIST Standardization of Additional Signature Schemes

Dustin Moody
Computer Security Division

Tuesday, October 3rd, 2023

THE STORY SO FAR

2016: NIST ANNOUNCES PROCESS FOR STANDARDIZING PQC KEMS AND SIGNATURES

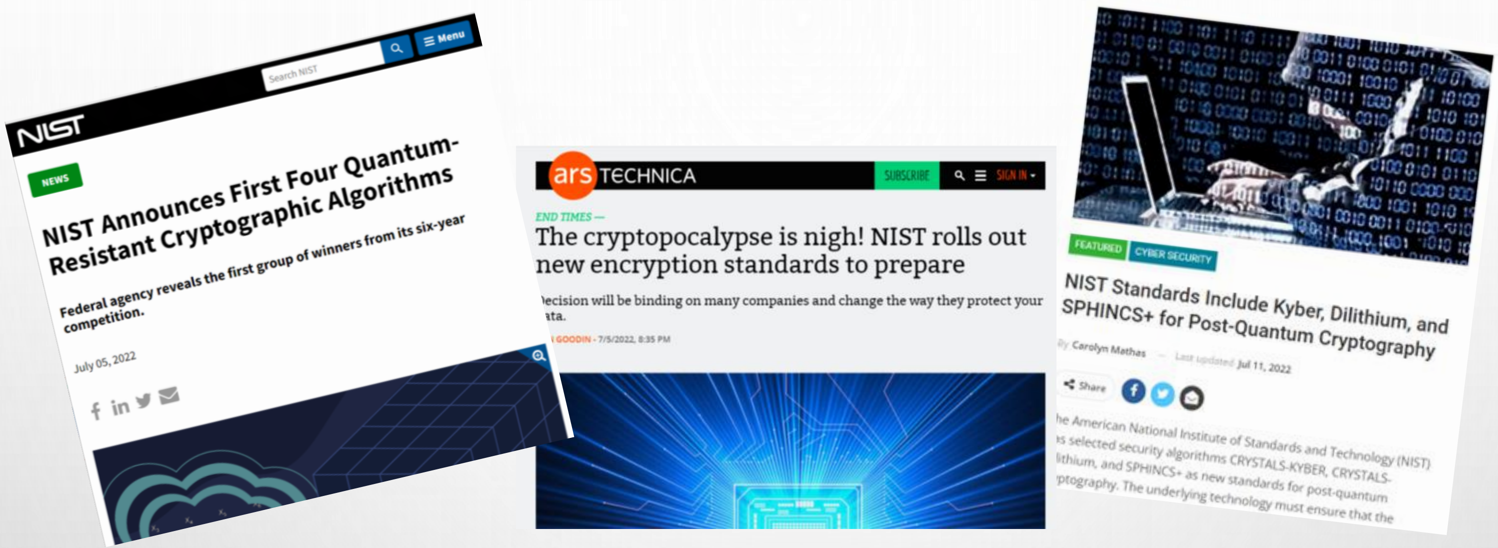
2017: INITIAL SUBMISSIONS (64 ACCEPTED: 19 SIGS + 45 KEMS)

2019: 2ND ROUND START (26 SCHEMES: 9 SIGS + 17 KEMS)

2020: 3RD ROUND START (7 FINALISTS, 8 ALTERNATES):

	Finalists	Alternates
KEM	Kyber, NTRU, Saber, Classic McEliece	Bike, FrodoKEM, HQC, NTRUPrime, SIKE
Signature	Dilithium, Falcon, Rainbow	GeMSS, Picnic, SPHINCS+

ROUND 3 RESULTS



3^{rd} round selection (KEM)	3^{rd} round selection (Signatures)
CRYSTALS-Kyber	**CRYSTALS-Dilithium, Falcon, SPHINCS+**

See NISTIR 8413, *Status Report on the 3rd Round of the NIST PQC Standardization Process*, for the rationale on the selections

4^{th} round candidates (all KEMs) evaluated for 18-24 months

- ClassicMcEliece, BIKE, HQC, ~~SIKE~~

THE SIGNATURES

- <u>CRYSTALS-DILITHIUM</u>
  - DIGITAL SIGNATURE BASED ON STRUCTURED LATTICES
  - GOOD ALL-AROUND PERFORMANCE AND SECURITY, RELATIVELY SIMPLE IMPLEMENTATION
  - NIST RECOMMENDS IT BE THE PRIMARY SIGNATURE ALGORITHM USED
- <u>FALCON</u>
  - DIGITAL SIGNATURE BASED ON STRUCTURED LATTICES
  - SMALLER BANDWIDTH, BUT MUCH MORE COMPLICATED IMPLEMENTATION
  - THE FALCON STANDARD WILL COME OUT AFTER THE OTHERS
- <u>SPHINCS+</u>
  - DIGITAL SIGNATURE BASED ON STATELESS HASH-BASED CRYPTOGRAPHY
  - SOLID SECURITY, BUT PERFORMANCE NOT AS GOOD IN COMPARISON TO DILITHIUM/FALCON

THE STATE OF THE SIGNATURES

- CRYPTANALYTIC RESULTS DURING THE 3RD ROUND CREATED SOME CONCERNS
  - **GEMSS** BROKEN IN NOVEMBER 2020 BY TAO, PETZOLDT, AND DING
  - BEULLENS POSTED AN ATTACK ON **RAINBOW**
    - BREAKS CATEGORY 1 PARAMETERS IN “A WEEKEND ON A LAPTOP”

- IN JAN 2021, NIST ASKED FOR FEEDBACK ON TWO TOPICS:
  - STANDARDIZING SPHINCS+ AFTER 3RD ROUND
  - INTRODUCING A MECHANISM TO CONSIDER NEW SIGNATURE SCHEMES

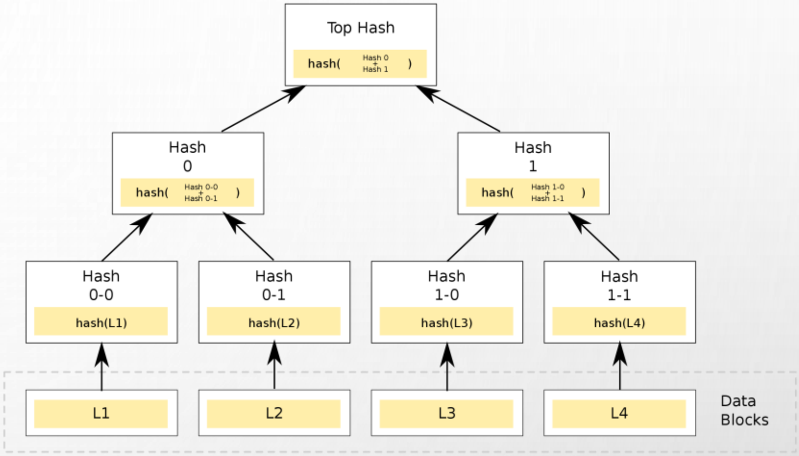
	Finalists	**Alternates**
Signatures	Dilithium, Falcon, ~~Rainbow~~	~~GeMSS~~, Picnic, SPHINCS+

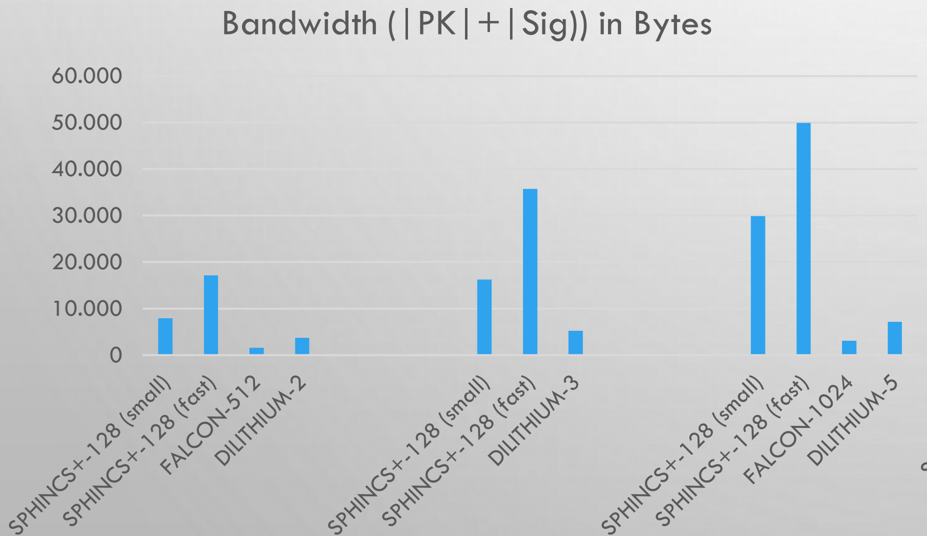
STANDARDIZATION

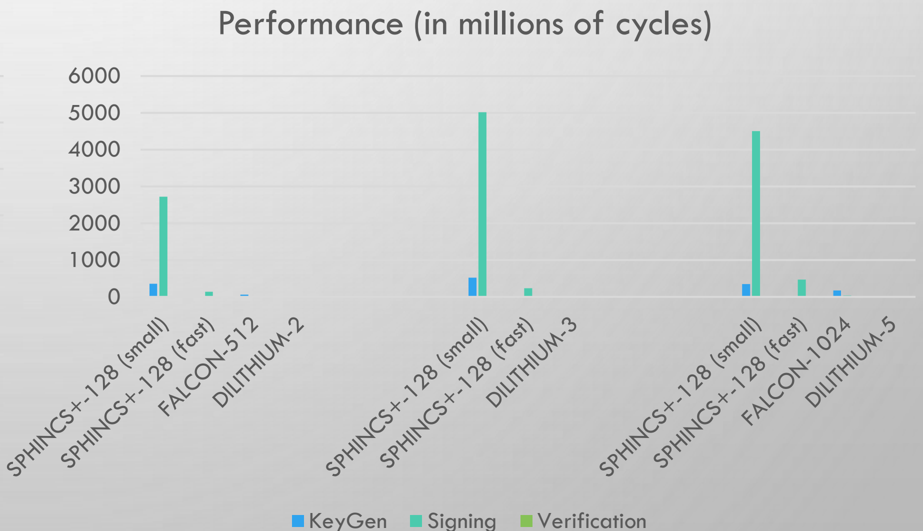
NIST

SPHINCS+

- SELECTED FOR ITS SOLID SECURITY
- BASED ON A DIFFERENT SET OF ASSUMPTIONS FROM LATTICES
- PERFORMANCE NOT GREAT







AN ON-RAMP FOR SIGNATURES

NIST

- Scope:
  - 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.
- The more mature the scheme, the better.
- NIST will decide which (if any) of the received schemes to focus attention on
- Currently ongoing

No on-ramp for KEMs currently planned.

TIMELINE

NIST

July 2022 - Call for Additional Signatures announced

August 2022 – Submission requirements and evaluation criteria published

March 1, 2023 – Preliminary submission deadline for early review

March 31, 2023 – Feedback given back to submitters

June 1, 2023 – Final deadline for submission

July 17, 2023 – Accepted submissions posted on our webpage

www.nist.gov/pqcrypto

TIMELINE


Initial call
Round 1
Round 2
Round 3
Round4
2017
2018
2020
2022
≈ 2024 ?
Initial call
Round 1
2022
2023

SUBMISSION NUMBERS

- 17 Preliminary submissions
- 50 submissions received by the final deadline
  - There were 23 signatures (and 59 KEMs) submitted in 2017
- 40 submissions accepted into the 1st Round
- 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

GEOGRAPHY

- In 2017, we had submitters from
  - 6 continents and 26 countries
- In 2023, we have submitters from
  - 5 continents and 28 countries

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

THE CANDIDATES

- 40 Submissions accepted into the 1st Round

Multivariate		MPC in-the-head				Lattice	Code	Symmetric	Isogeny	Other
UOV	Other	MinRank	SD/Rank-SD	PKP	MQ					
Mayo	3wise	Mira	RYDE	Perk	MQOM	EagleSign	Enh. Pqsig-rm	Aimer	SQIsign	Alteq
PROV	DMEsign	MiRitH	SDitH		Biscuit	EHT	Fuleeca	Ascon-sign		eMLE-Sig 2.0
QR-UOV	HPPC					HAETAE	LESS	FAEST		KAZ
SNOVA						Hawk	MEDS	SPHINCS-alpha		Preon
TUOV						HuFu	Wave			Xifrat
UOV						Raccoon	Cross			
Vox						Squirrels				
7	3	2	2	1	2	7	6	4	1	5
10		7								
40										

SOME ATTACKS

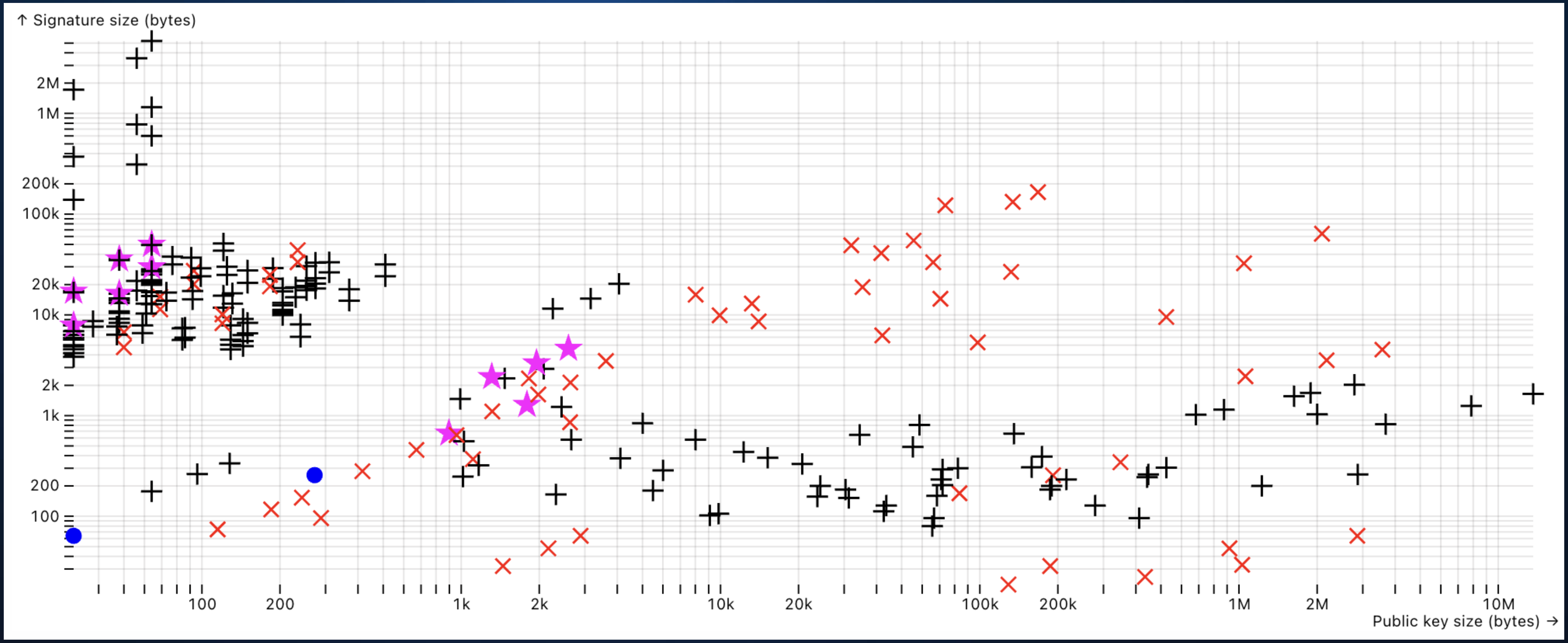
NIST

- Some reported attacks and implementation bugs

Multivariate		MPC in-the-head				Lattice	Code	Symmetric	Isogeny	Other
UOV	Other	MinRank	SD/Rank-SD	PKP	MQ					
Mayo	3wise	Mira	RYDE	Perk	MQOM	EagleSign	Enh. Pqsig-rm	Aimer	SQIsign	Alteq
PROV	DMEsign	MiRitH	SDitH		Biscuit	EHT	Fuleeca	Ascon-sign		eMLE-Sig 2.0
QR-UOV	HPPC					HAETAE	LESS	FAEST		KAZ
SNOVA						Hawk	MEDS	SPHINCS-alpha		Preon
TUOV						HuFu	Wave			Xifrat
UOV						Raccoon	Cross			
Vox						Squirrels				
7	4	2	3	1	1	7	5	4	1	5
11		7								
40										

KEY/SIGNATURE SIZES

- The PQ Signature Zoo (by Thom Wiggers of PQShield)



CATEGORIES

Broad categories of the candidates

- Multivariate
- MPC-in-the-head
- Lattice
- Code-based
- Symmetric-based
- Isogeny
- Other….

MULTIVARIATE BASED-CRYPTO

NIST

$$F\_q[x_1, x_2, \dots, x_n]$$

$$\begin{cases} x_1 + 2x_3 \\ 2x_1 + 2x_2 \\ x_1 + x_2 \end{cases}$$

$$\begin{cases} f_1(x_1, x_2, \dots, x_n) \\ f_2(x_1, x_2, \dots, x_n) \\ \vdots \\ f_m(x_1, x_2, \dots, x_n) \end{cases}$$

$$\begin{cases} x_1^2 + x_2^2 + x_2x_3 + 2x_3^2 \\ x_1x_2 + x_2^2 + x_2x_3 + x_3^2 \\ x_1^2 + x_1x_2 + x_1x_3 + x_2x_3 \end{cases}$$

Multivariate Quadratic (MQ)

- Multivariate signatures typically have large public keys and very small signatures
- Verification is quite fast

MULTIVARIATE BASED-CRYPTO

NIST

$F\_q[x_1, \ldots$

$f_1(x_1, x_2, \ldots, x$

$f_2(x_1, x_2, \ldots, x$

$\vdots$

$f_m(x_1, x_2, \ldots, x$

<u>Multivariate Signatures</u>

Mayo
PROV
QR-UOV
SNOVA
TUOV
UOV
Vox

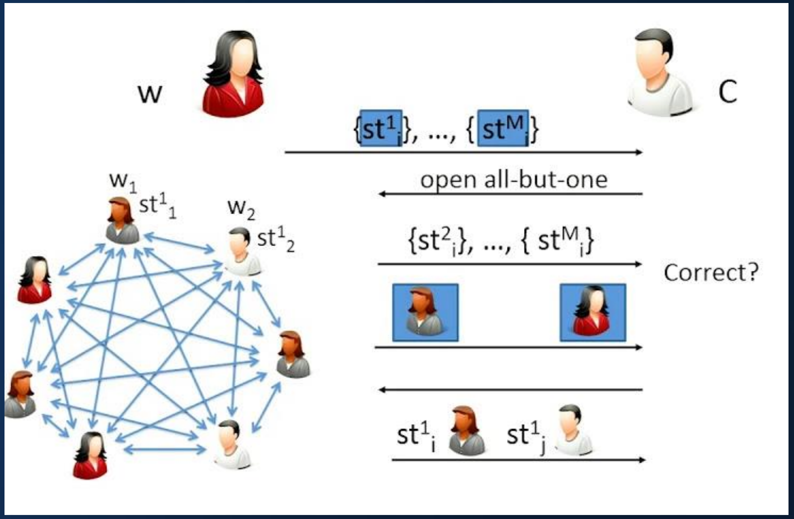
$_3$

MQ)

- Multivariate signatures typically have large public keys and very small signatures
- Verification is quite fast

MPC-IN-THE-HEAD

1. Choose a hard problem
2. Construct a zero-knowledge proof using MPC-in-the-head techniques
3. Use the Fiat-Shamir transform



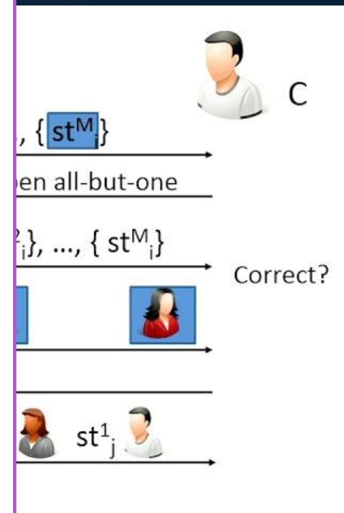
- MPC-in-the-head signatures is a newer area of research
- Key sizes and performance depend on the underlying problem

MPC-IN-THE-HEAD

1. C
2. Constru using M
3. Use

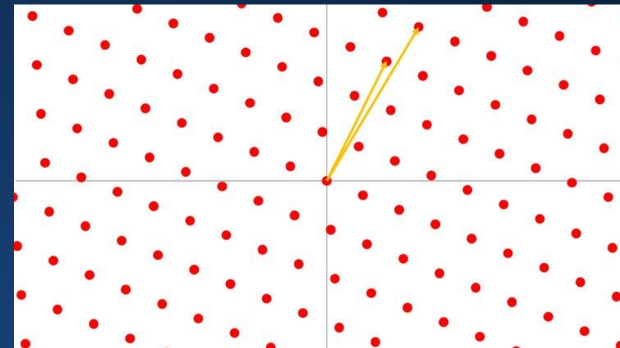
<u>MPC-in-the-Head Signatures</u>

Minrank: Mira, MiRitH
Syndrome-decoding: RYDE, SDitH
Permuted Kernel: Perk
Multivariate Quadratic: MQOM, Biscuit

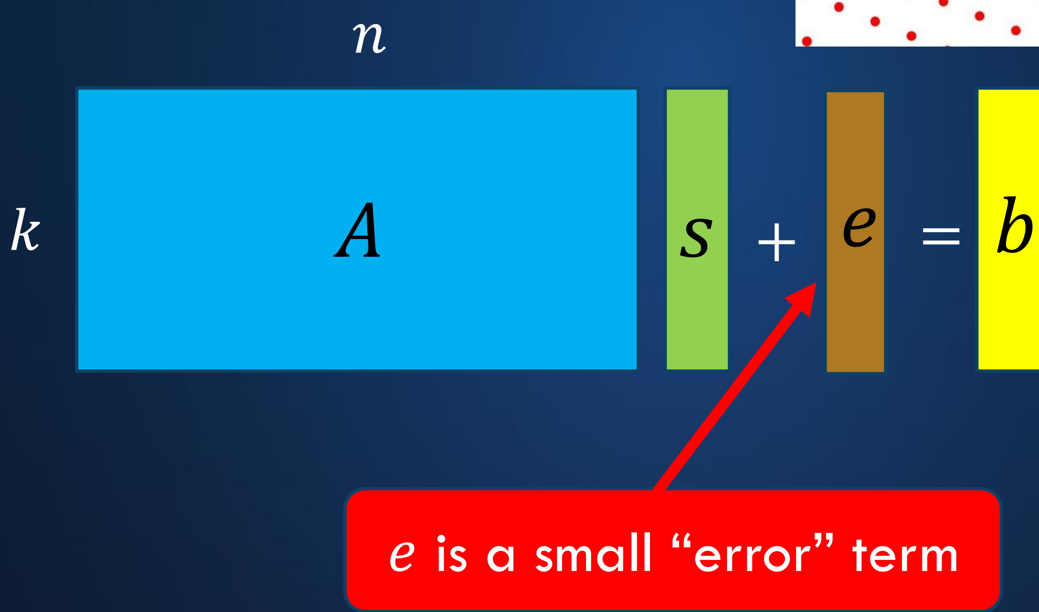


- MPC-in-the-head signatures is a newer area of research
- Key sizes and performance depend on the underlying problem

LATTICES



NIST



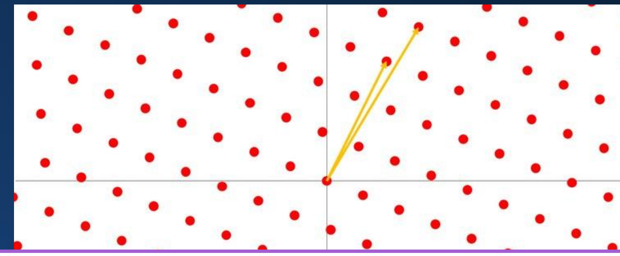
All entries in $\mathbb{F}_q$

$$As + e = b$$

Given $(A, b) \rightarrow$ Find s

- Lattice-based algorithms typically have balanced public key and signature sizes, and are very efficient
- Algebraic structure is often introduced to make the sizes smaller

LATTICES



NIST

<u>Lattice Signatures</u>

EagleSign
EHT
Fusion
HAETAE
Hawk
HuFu
Raccoon
Squirrels

k

ries in $\mathbb{F}_q$

$- \boldsymbol{e} = \boldsymbol{b}$

$\boldsymbol{b})$ → **Find** $\boldsymbol{s}$

- Lattice-based algorithms typically have balanced public key and signature sizes, and are very efficient
- Algebraic structure is often introduced to make the sizes smaller

Code-based

Repetition Code

1. Sender sends 3 copies of the message
2. Receiver decodes by taking most frequent bit for each position

1001001 1001001 1001001 → Noisy channel → 1001101 1001001 0001001

$$
\begin{aligned}
\mathbf{y} &= \mathbf{x}G' + \mathbf{e} \\
&= (1,1,0,1)\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} + (0,0,0,0,1,0,0) \\
&= (0,1,1,0,0,1,0) + (0,0,0,0,1,0,0) \\
&= (0,1,1,0,1,1,0).
\end{aligned}
$$

- Code-based schemes often have balanced public key and signature size
- Algebraic structure is often introduced to make the sizes smaller
- There have been more code-based encryption schemes than signatures

Code-based

1. Send
2. Rece

1001001 10010 … 1 0001001

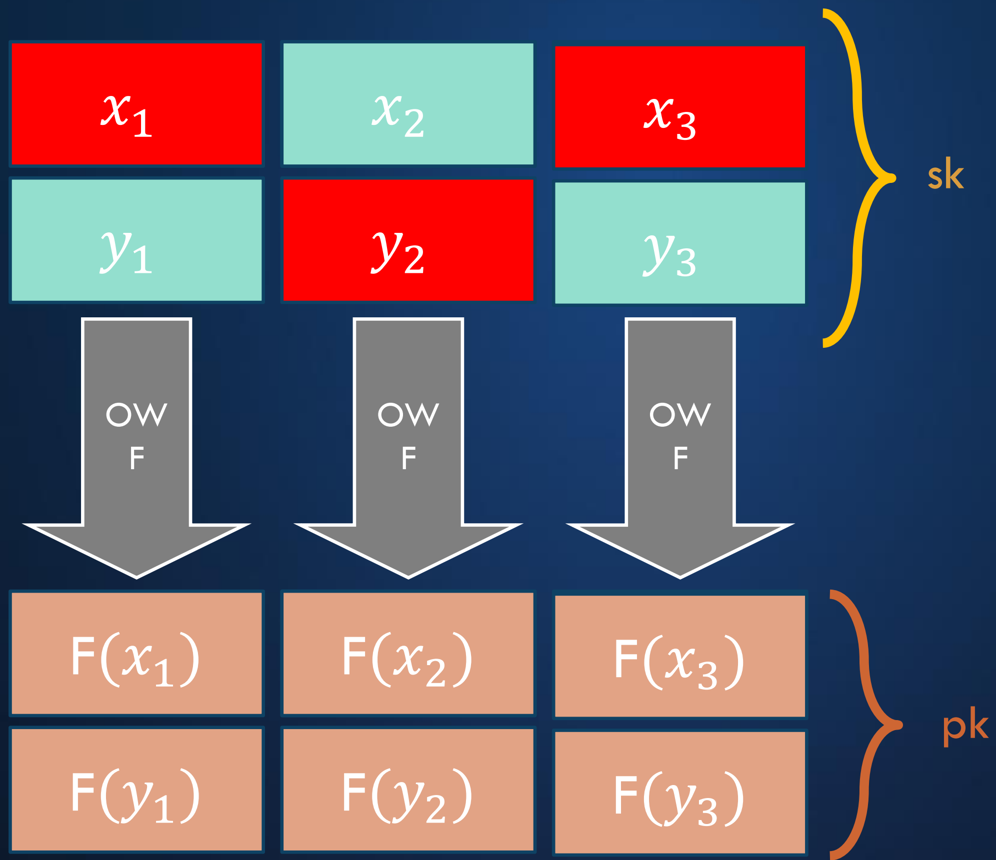
Code-based Signatures

Enhanced Pqsig-rm
Fuleeca
LESS
MEDS
WAVE
Cross

$= (0,1,1,0,1,1,0).$

- Code-based schemes often have balanced public key and signature size
- Algebraic structure is often introduced to make the sizes smaller
- There have been more code-based encryption schemes than signatures

SYMMETRIC-BASED



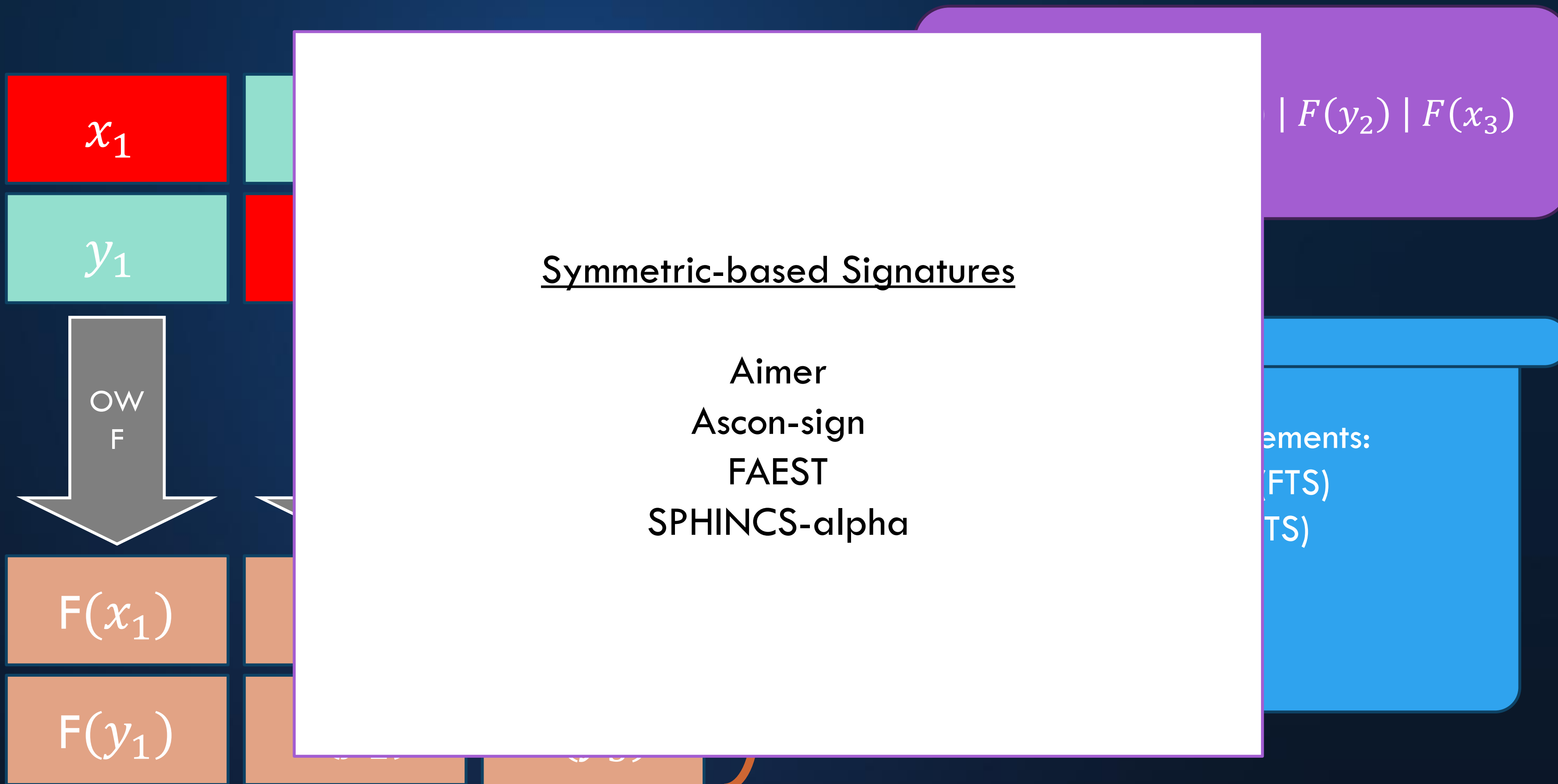
$$\text{Sign}(010) = F(x_1)\,|\,F(y_2)\,|\,F(x_3)$$

A LOT of improvements:

- Merkle trees (FTS)
- Winternitz (OTS)
- etc.
- SPHINCS+

- Symmetric-based schemes often have small public keys, but large signatures
- Security analysis of underlying symmetric primitive often well-studied

SYMMETRIC-BASED



<u>Symmetric-based Signatures</u>

Aimer

Ascon-sign

FAEST

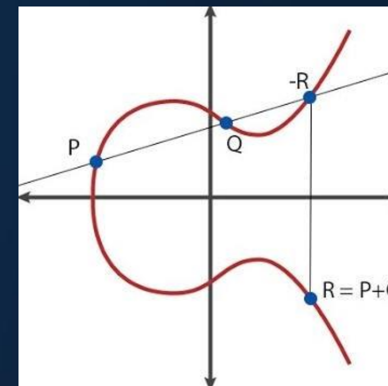
SPHINCS-alpha

- Symmetric-based schemes often have small public keys, but large signatures
- Security analysis of underlying symmetric primitive often well-studied

ISOGENY-BASED

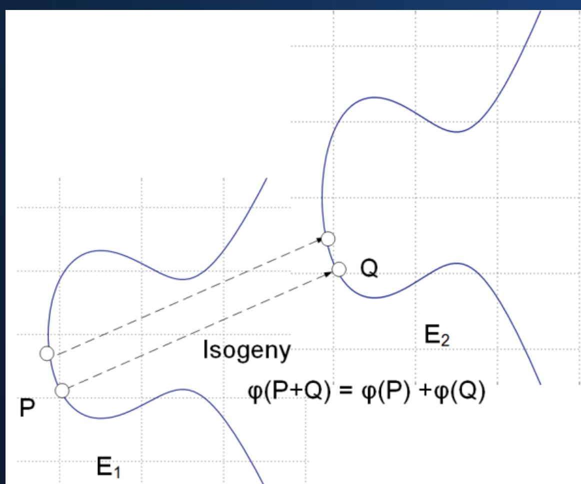
NIST

Abelian group



Elliptic curve

$y = x^3 + ax + b$ → Points in $\mathbb{F}_q$ →



An isogeny ϕ between curves E_1 and E_2 is a group homomorphism $E_1 \longrightarrow E_2$.
(usually defined by its kernel)

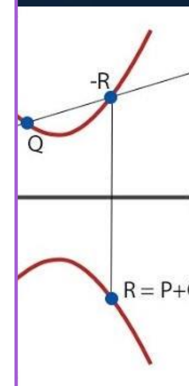
- While SIKE was broken, many isogeny schemes were not affected
- Isogeny-based schemes typically have quite small key/signature/ciphertext sizes
- They are about an order of magnitude slower than other candidates

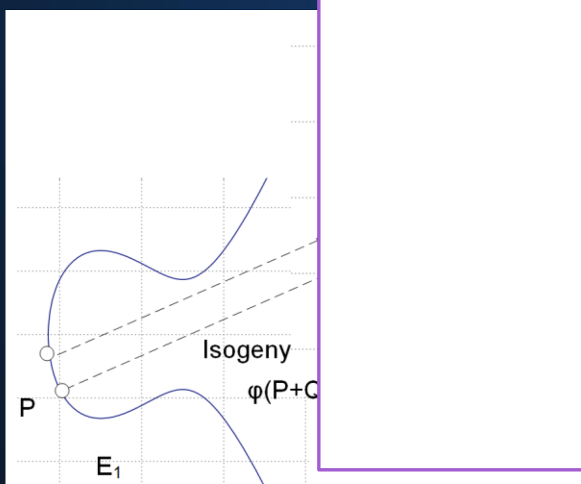
ISOGENY-BASED

group

Elliptic curv

$y = x^3 + ax$





Isogeny-based Signatures

SQIsign

Other

Alteq
eMLE-Sig 2.0
Preon
Xifrat

and E_2 is

$\to E_2$.

nel)

- While SIKE was broken, many isogeny schemes were not affected
- Isogeny-based schemes typically have quite small key/signature/ciphertext sizes
- They are about an order of magnitude slower than other candidates

FUTURE STANDARDIZATION

NIST

- Before standardization, candidates must have had sufficient time for evaluation and testing
  - We expect there will be multiple rounds, which will take years
- Likely outcome: at most 2 candidates selected for standardization
- We do not expect any of the onramp candidates to replace Dilithium (ML-DSA) as the main signature algorithm for most applications

READY, SET, GO!

- THE ONRAMP IS JUST BEGINNING
- PLEASE EVALUATE THE CANDIDATES
- STANDARDIZATION NOT FOR AWHILE

- CHECK OUT WWW.NIST.GOV/PQCRYPTO
  - SIGN UP FOR THE PQC-FORUM FOR ANNOUNCEMENTS & DISCUSSION
  - SEND E-MAIL TO PQC-COMMENTS@NIST.GOV

Post-Quantum Cryptography Conference

PKI Consortium