A Short, Fast, Post-quantum Multivariate Digital Signature Scheme

Anindya Ganguly, Angshuman Karmakar, **Nitin Saxena**
CSE, IIT Kanpur

IIT-ISM Dhanbad
(virtual)

April-2024


Malicious person
Insecure channel
Party A
Party B

Enigma

Homomorphic encryption

Post-quantum cryptography

Playfair cipher

Public key cryptography

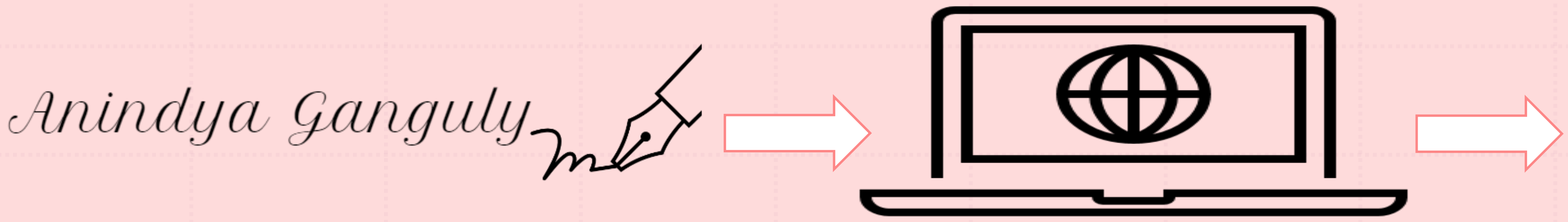
Computations on encrypted data

Quantum cryptography

Computational power

Mathematically (hard?) problems

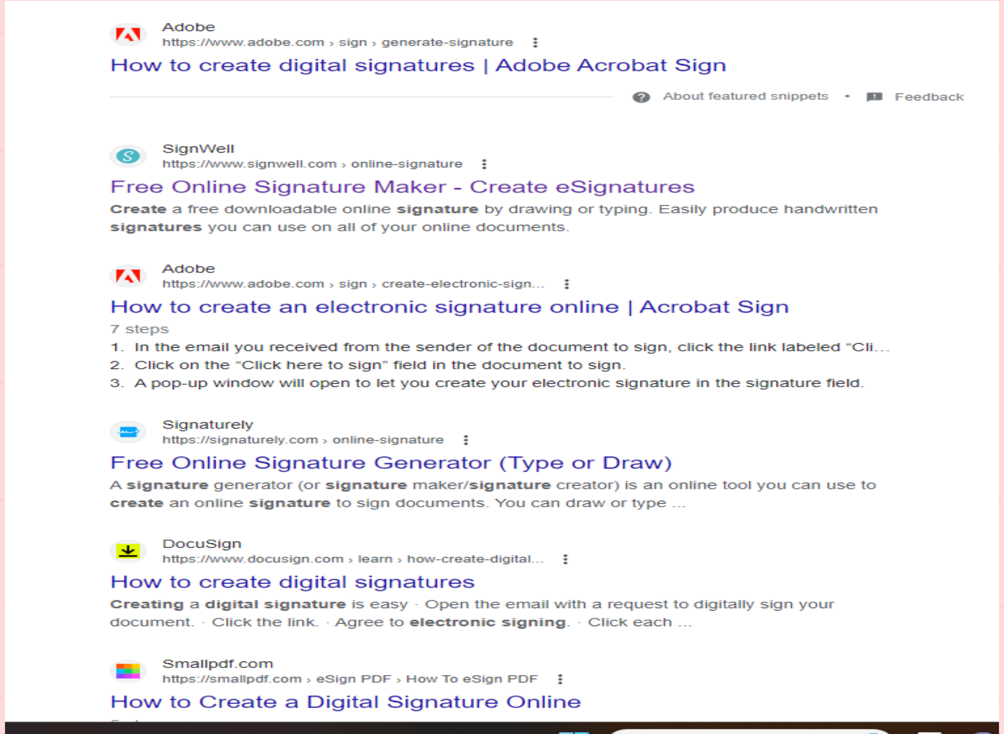
Digital Signature



01011110100 ···

anindya_signature.png

Offline signatures are widely utilized for signing a variety of documents, such as contracts, checks, and legal forms



Adobe
https://www.adobe.com › sign › generate-signature
How to create digital signatures | Adobe Acrobat Sign

About featured snippets • Feedback

SignWell
https://www.signwell.com › online-signature
Free Online Signature Maker - Create eSignatures
Create a free downloadable online **signature** by drawing or typing. Easily produce handwritten **signatures** you can use on all of your online documents.

Adobe
https://www.adobe.com › sign › create-electronic-sign...
How to create an electronic signature online | Acrobat Sign
7 steps
1. In the email you received from the sender of the document to sign, click the link labeled "Cli...
2. Click on the "Click here to sign" field in the document to sign.
3. A pop-up window will open to let you create your electronic signature in the signature field.

Signaturely
https://signaturely.com › online-signature
Free Online Signature Generator (Type or Draw)
A **signature** generator (or **signature** maker/**signature** creator) is an online tool you can use to **create** an online **signature** to sign documents. You can draw or type ...

DocuSign
https://www.docusign.com › learn › how-create-digital...
How to create digital signatures
Creating a **digital signature** is easy · Open the email with a request to digitally sign your document. · Click the link. · Agree to **electronic signing**. · Click each ...

Smallpdf.com
https://smallpdf.com › eSign PDF › How To eSign PDF
How to Create a Digital Signature Online

- ❑ The ease of copying a digitized handwritten signature makes it susceptible to forgery.
- ❑ Digital signature provides *integrity* : message authentication, non-repudiation

Signature schemes: Wide applications

- Social Media/ UPI
- Legal docs/ degree certificates
- Electronic voting m/c
- NFT/ Blockchain

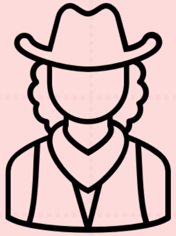
- Authentication/ Data privacy
- Protection against alteration
- Non-repudiated transfer of information
- Unobstructed channel of communication

Digital Signature: Math modelling

KeyGen()

- Generate $s, VK \leftarrow^{\$} \mathcal{K}$

Secret key s



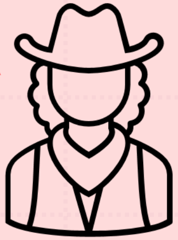
Signer

Output:

$\sigma \leftarrow Sign\ (M, s)$

Transmit σ

Verification key VK



Verifier

Output:

$\{0,1\} \leftarrow Verf\ (M, \sigma, VK)$

Motivation for multivariate

- ❑ **Design a secure signature scheme** →

- ❑ Quantum algorithms can efficiently solve problems, e.g. like IFP, DL
- ❑ Lattices are crypto-friendly quantum-safe constructions
- ❑ Research community needs diversity in hardness assumptions
- ❑ Multivariate construction offers short signature size
- ❑ Recent NIST submission has eleven multivariate candidates

Motivation for multivariate

- ❑ Design a secure signature scheme
- ❑ Lattices are crypto-friendly quantum-safe constructions
- ❑ Multivariate construction offers short signature size

- ❑ **Quantum algorithms can efficiently solve problems, e.g. like IF, DL**
- ❑ Research community needs diversity in hardness assumptions
- ❑ Recent NIST submission has eleven multivariate candidates

Motivation for multivariate

- ❑ Design a secure signature scheme
- ❑ **Lattices are crypto-friendly quantum-safe constructions**
- ❑ Multivariate construction offers short signature size

- ❑ Quantum algorithms can efficiently solve problems, e.g. like IFP, DL
- ❑ Research community needs diversity in hardness assumptions
- ❑ Recent NIST submission has eleven multivariate candidates

Motivation for multivariate

- ❑ Design a secure signature scheme
- ❑ Lattices are crypto-friendly quantum-safe constructions
- ❑ Multivariate construction offers short signature size

- ❑ Quantum algorithms can efficiently solve problems, e.g. like IFP, DL
- ❑ **Research community needs diversity in hardness assumptions**
- ❑ Recent NIST submission has eleven multivariate candidates

Motivation for multivariate

- ❑ Design a secure signature scheme
- ❑ Lattices are crypto-friendly quantum-safe constructions
- ❑ **Multivariate construction offers short signature size**

- ❑ Quantum algorithms can efficiently solve problems, e.g. like IFP, DL
- ❑ Research community needs diversity in hardness assumptions
- ❑ Recent NIST submission has eleven multivariate candidates

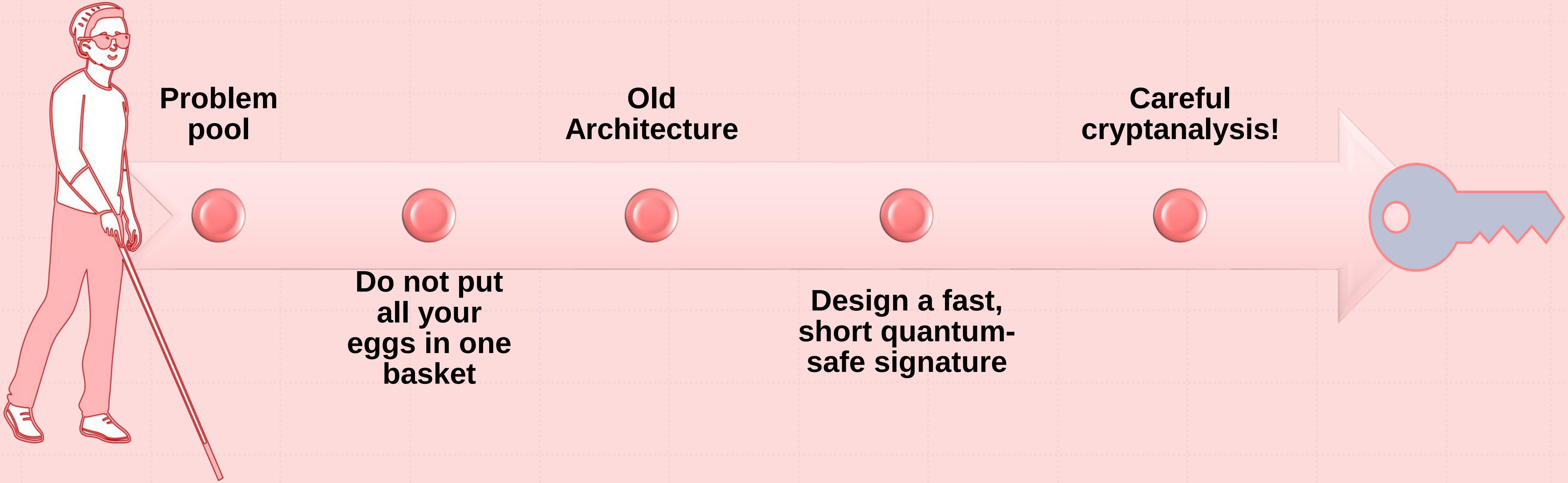
Motivation for multivariate

- ❑ Design a secure signature scheme
- ❑ Quantum algorithms can efficiently solve problems, e.g. like IFP, DL
- ❑ Lattices are crypto-friendly quantum-safe constructions
- ❑ Research community needs diversity in hardness assumptions
- ❑ Multivariate construction offers short signature size
- ❑ **Recent NIST submission has eleven multivariate candidates**

VDOO: Cause of Happiness

- **New design element:** introduced diagonal layers
- **Fastest:** size of linear system is **small**, so Gaussian Elimination is efficient
- **Secure:** against all existing classical and quantum attacks
- **Shortest:** **96 bytes,** which is one of the **smallest** signature size (including SPHINCS+, Dilithium, and Falcon)

Roadmap for Signature Design



Cryptography from Hard Problems

Problem pool

Hard problems	Example	Importance and drawbacks
Classical cryptography	RSA, ECDH, ECDSA, EdDSA	Small key and signature size. But **quantum-insecure**
Lattice-based cryptography	Crystals-dilithium , Falcon, NTRU	**Large key size and signature size**. Fast. Most crypto friendly
Multivariate cryptography	~~Rainbow~~, UOV, Mayo	Small signature, **large key size**, simple construction
Hash-based cryptography	SPHNICS+, XMSS	Small public key size, **large signature** size and **slow**
Code-based cryptography	BIKE, Classical McEliece	Complex structure. **Syndrome decoding; slow**
Isogeny-based cryptography	~~SIKE~~, SQISign	Small signature and public key size but significantly **slow**

Don’t Put All Your Eggs In One Basket

Multivariate Cryptography

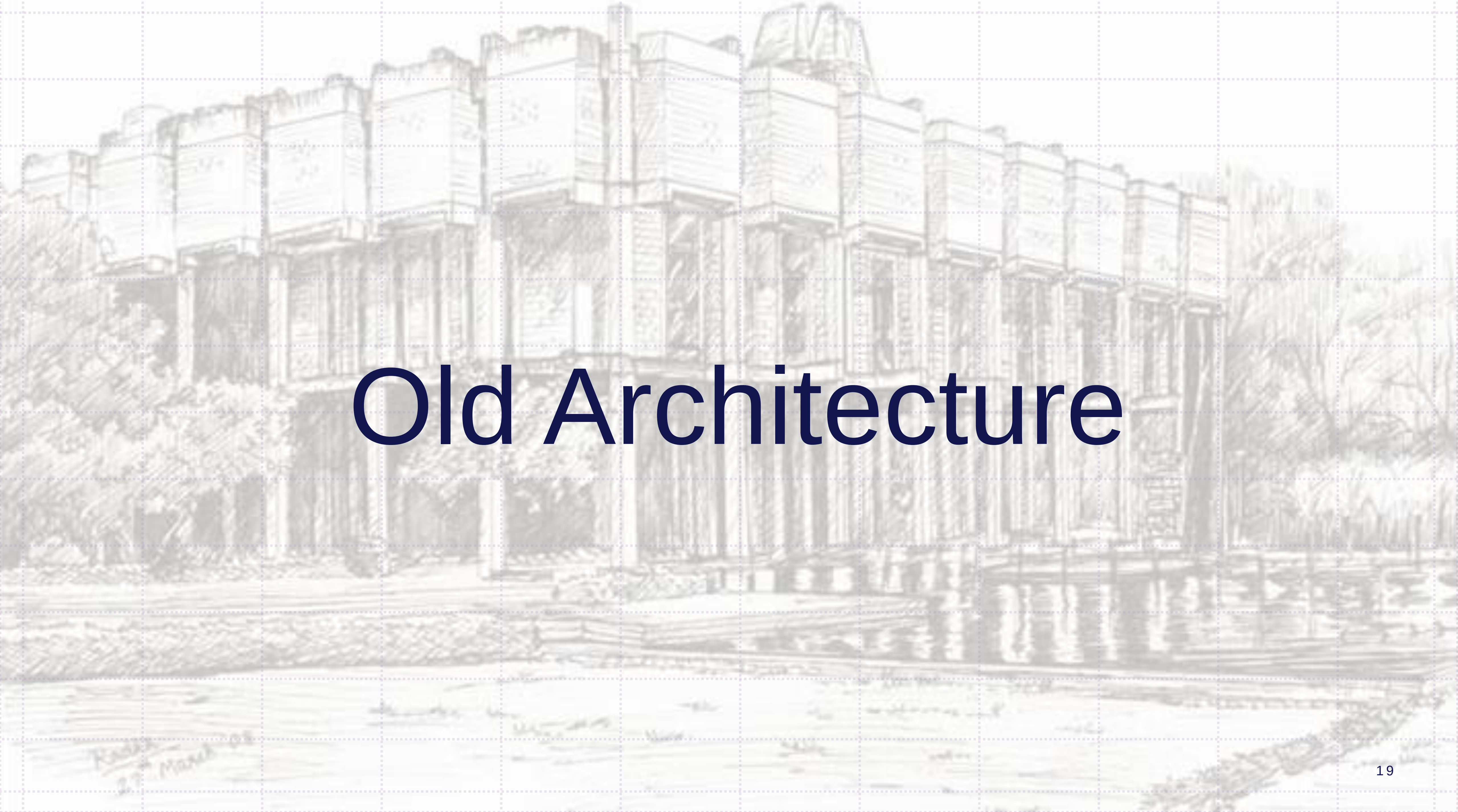
NP-hard

Multivariate Quadratic (MQ) Problem

- Given a quadratic system of m **homogeneous equations** and n **variables**, find a solution in **polynomial time**.

Constructions based on MQ

~~**Hidden Field Equation**~~ [Patarin-96; Tao,Petzoldt,Ding-21]
Oil-Vinegar-based construction [Kipnis,Patarin,Goubin-99]
ZKP-based construction (5-round identification, MPCitH) [CHR+, Fen-22]



Old Architecture

Oil-Vinegar map

Quadratic map $\mathcal{F} :: (f^{(1)}, \cdots, f^{(m)}): \mathbb{F}_q^n \to \mathbb{F}_q^m$

$$\boldsymbol{f^{(1)}(x_1, \cdots, x_v, \cdots, x_n) :: \sum_{i=1}^{v} \sum_{j=1}^{v} \alpha_{i,j}^{(1)} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{i,j}^{(1)} x_i x_j = t_1}$$

$$\boldsymbol{f^{(2)}(x_1, \cdots, x_v, \cdots, x_n) :: \sum_{i=1}^{v} \sum_{j=1}^{v} \alpha_{i,j}^{(2)} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{i,j}^{(2)} x_i x_j = t_2}$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\boldsymbol{f^{(m)}(x_1, \cdots, x_v, \cdots, x_n) :: \sum_{i=1}^{v} \sum_{j=1}^{v} \alpha_{i,j}^{(m)} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{i,j}^{(m)} x_i x_j = t_m}$$

Oil-Vinegar map

Quadratic map $\mathcal{F}$ :: $(f^{(1)}, \cdots, f^{(m)}): \mathbb{F}_q^n \to \mathbb{F}_q^m$

$$f^{(1)}(x_1, \cdots, x_v, \cdots, x_n) \;::\; \sum_{i=1}^{v}\sum_{j=1}^{v} \alpha_{i,j}^{(1)} x_i x_j + \sum_{i=1}^{v}\sum_{j=v+1}^{n} \beta_{i,j}^{(1)} x_i x_j = t_1$$

$$f^{(2)}(x_1, \cdots, x_v, \cdots, x_n) \;::\; \sum_{i=1}^{v}\sum_{j=1}^{v} \alpha_{i,j}^{(2)} x_i x_j + \sum_{i=1}^{v}\sum_{j=v+1}^{n} \beta_{i,j}^{(2)} x_i x_j = t_2$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$f^{(m)}(x_1, \cdots, x_v, \cdots, x_n) \;::\; \sum_{i=1}^{v}\sum_{j=1}^{v} \alpha_{i,j}^{(m)} x_i x_j + \sum_{i=1}^{v}\sum_{j=v+1}^{n} \beta_{i,j}^{(m)} x_i x_j = t_m$$

Oil-Vinegar map

Quadratic map $\mathcal{F} :: (f^{(1)}, \cdots, f^{(m)}) \colon \mathbb{F}_q^n \to \mathbb{F}_q^m$

$$f^{(1)}(x_1, \cdots, x_v, \cdots, x_n) \;::\; \sum_{i=1}^{v}\sum_{j=1}^{v} \cancel{\alpha_{i,j}^{(1)}}\, \cancel{x_i}\, \cancel{x_j} + \sum_{i=1}^{v}\sum_{j=v+1}^{n} \cancel{\beta_{i,j}^{(1)}}\, \cancel{x_i}\, x_j \;=\; t_1$$

$$f^{(2)}(x_1, \cdots, x_v, \cdots, x_n) \;::\; \sum_{i=1}^{v}\sum_{j=1}^{v} \cancel{\alpha_{i,j}^{(2)}}\, \cancel{x_i}\, \cancel{x_j} + \sum_{i=1}^{v}\sum_{j=v+1}^{n} \cancel{\beta_{i,j}^{(2)}}\, \cancel{x_i}\, x_j \;=\; t_2$$

$$\vdots \qquad \vdots \qquad \vdots$$

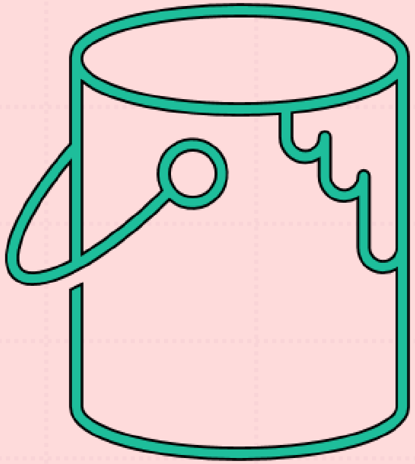
$$\vdots \qquad \vdots \qquad \vdots$$

$$f^{(m)}(x_1, \cdots, x_v, \cdots, x_n) \;::\; \sum_{i=1}^{v}\sum_{j=1}^{v} \cancel{\alpha_{i,j}^{(m)}}\, \cancel{x_i}\, \cancel{x_j} + \sum_{i=1}^{v}\sum_{j=v+1}^{n} \cancel{\beta_{i,j}^{(m)}}\, \cancel{x_i}\, x_j \;=\; t_m$$

Construct an Oil-Vinegar Polynomial

Vinegar × Vinegar

Vinegar × Oil



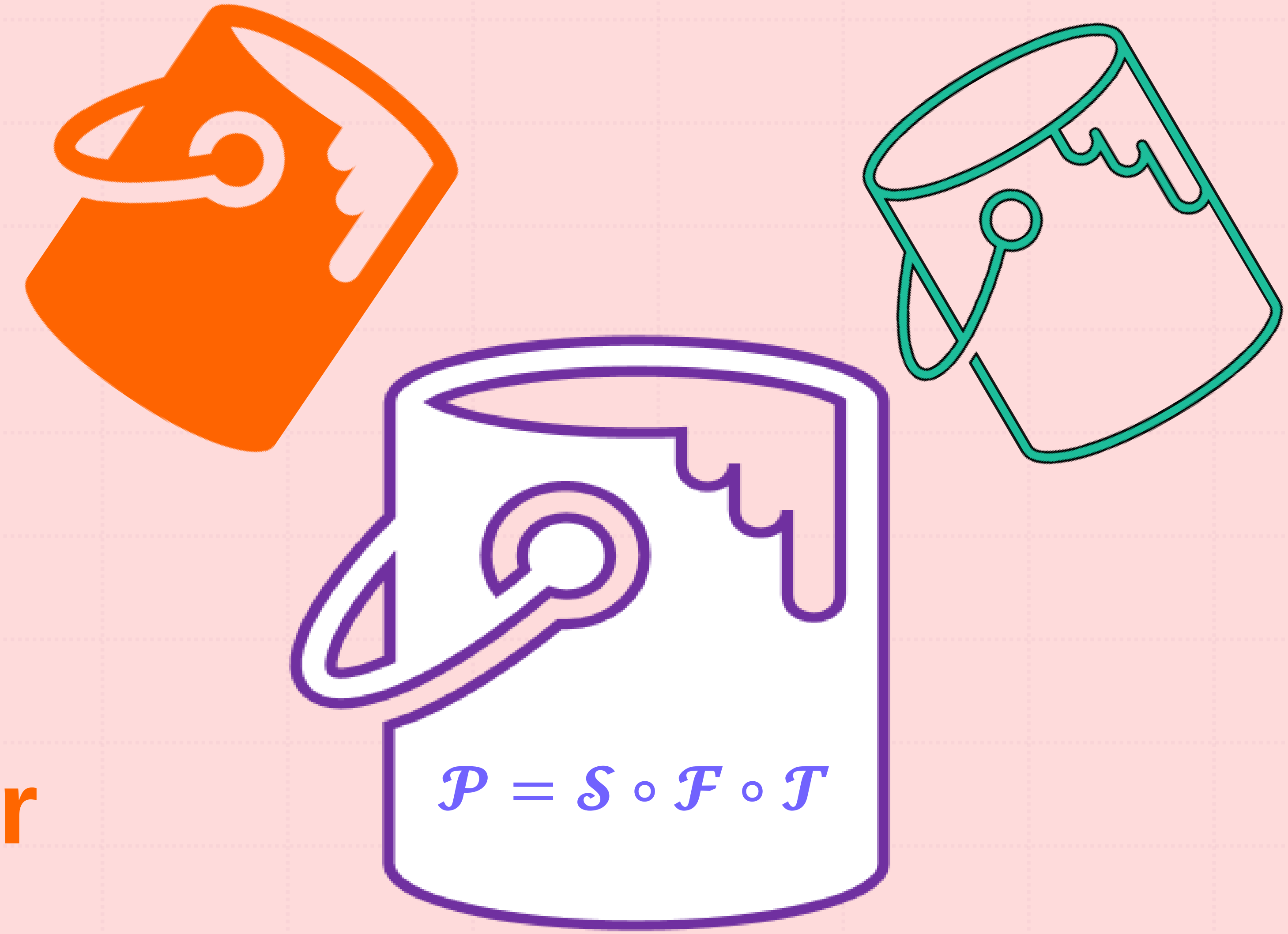
No Oil × Oil terms

Vinegar

Oil

Variables Bucket

Construct a (random) Multivariate Polynomial



Vinegar

Oil

Variables mixed randomly

Multivariate Signature Scheme

Private Key:

- ❑ invertible linear map

$\mathcal{S} : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^m, \quad \mathcal{T} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$

- ❑ quadratic map $\mathcal{F} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$

$$\boldsymbol{d} = \mathcal{H}(\boldsymbol{msg})$$

➔ Signature Generation ➔

$$\boldsymbol{d} \in \mathbb{F}_q^m \Longrightarrow_{\mathcal{S}^{-1}} \boldsymbol{w} \in \mathbb{F}_q^m \Longrightarrow_{\mathcal{F}^{-1}} \boldsymbol{y} \in \mathbb{F}_q^n \Longrightarrow_{\mathcal{T}^{-1}} \boldsymbol{x} \in \mathbb{F}_q^n$$

Multivariate Signature Scheme

Private Key:

- invertible linear map

$\mathcal{S} : \mathbb{F}_q^m \to \mathbb{F}_q^m, \ \mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$

- quadratic map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$

$d = \mathcal{H}(msg)$

➔ Signature Generation ➔

$$d \in \mathbb{F}_q^m \Longrightarrow_{\mathcal{S}^{-1}} w \in \mathbb{F}_q^m \Longrightarrow_{\mathcal{F}^{-1}} y \in \mathbb{F}_q^n \Longrightarrow_{\mathcal{T}^{-1}} x \in \mathbb{F}_q^n$$

Multivariate Signature Scheme

Private Key:

- invertible linear map

  $\mathcal{S}: \mathbb{F}_q^m \to \mathbb{F}_q^m, \quad \mathcal{T}: \mathbb{F}_q^n \to \mathbb{F}_q^n$

- quadratic map $\mathcal{F}: \mathbb{F}_q^n \to \mathbb{F}_q^m$

$\boldsymbol{d = \mathcal{H}(msg)}$ ➔ **Signature Generation** ➔

$$d \in \mathbb{F}_q^m \Longrightarrow_{\mathcal{S}^{-1}} w \in \mathbb{F}_q^m \Longrightarrow_{\mathcal{F}^{-1}} y \in \mathbb{F}_q^n \Longrightarrow_{\mathcal{T}^{-1}} x \in \mathbb{F}_q^n$$

Multivariate Signature Scheme

Private Key:

- invertible linear map

  $\mathcal{S} : \mathbb{F}_q^m \to \mathbb{F}_q^m, \ \mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$

- quadratic map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$

$\boldsymbol{d = \mathcal{H}(msg)}$

➔ Signature Generation ➔

$$\boldsymbol{d} \in \mathbb{F}_q^m \Longrightarrow_{\mathcal{S}^{-1}} \boldsymbol{w} \in \mathbb{F}_q^m \Longrightarrow_{\mathcal{F}^{-1}} \boldsymbol{y} \in \mathbb{F}_q^n \Longrightarrow_{\mathcal{T}^{-1}} \boldsymbol{x} \in \mathbb{F}_q^n$$

Signature $= \boldsymbol{x}$

$\boldsymbol{d = \mathcal{H}(msg)}$

$\boldsymbol{d' = \mathcal{P}(x)}$

🡐 Verification 🡐

$\boldsymbol{d \overset{?}{=} d'}$

Verification/Public Key:

$\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^m$

VDOO: Design Rationale

Diagonal Layer

Vinegar Variables: First randomly fix $\boldsymbol{x_1, x_2, \cdots, x_v \in_U \mathbb{F}_q}$

$$\boldsymbol{f_1(x_1, x_2, \cdots, x_{v+1}) = x_{v+1} \cdot l_1(x_1, x_2, \cdots, x_v) + g_1(x_1, x_2, \cdots, x_v)}$$

l_i is **linear** and
g_i is **quadratic**

$$\boldsymbol{f_2(x_1, x_2, \cdots, x_{v+2}) = x_{v+2} \cdot l_2(x_1, x_2, \cdots, x_{v+1}) + g_2(x_1, x_2, \cdots, x_{v+1})}$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\boldsymbol{f_d(x_1, x_2, \cdots, x_{v+d}) = x_{v+d} \cdot l_d(x_1, x_2, \cdots, x_{v+d-1}) + g_d(x_1, x_2, \cdots, x_{v+d-1})}$$

Why Diagonal Layer?

Diagonal Layer

$$\gamma_1^{(1)} x_1 + c_1 = t_1$$

$$\gamma_2^{(2)} x_2 + c_2 = t_2$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\gamma_N^{(N)} x_N + c_N = t_N$$

Time Complexity: $\boldsymbol{O(N)}$

Oil Layer

$$\gamma_1^{(1)} x_1 + \gamma_2^{(1)} x_2 + \cdots + \gamma_N^{(1)} x_N = t_1$$

$$\gamma_1^{(2)} x_1 + \gamma_2^{(2)} x_2 + \cdots + \gamma_n^{(2)} x_N = t_2$$

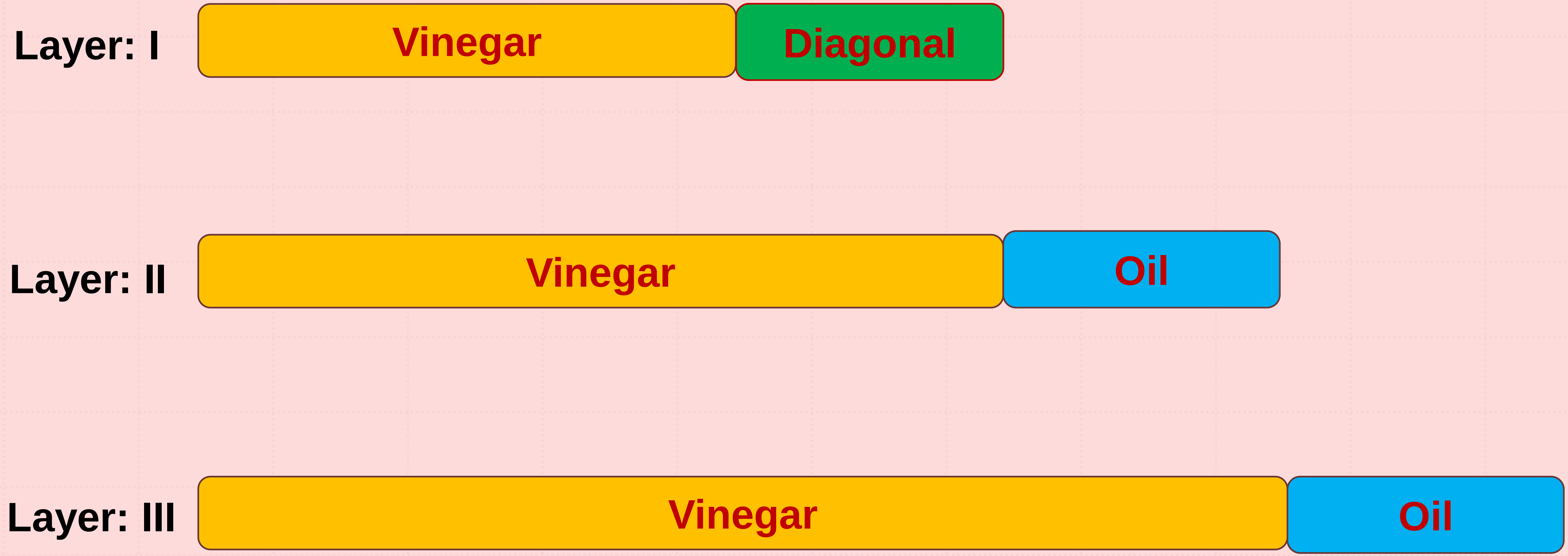
$$\vdots \qquad \vdots \qquad \vdots$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\gamma_1^{(N)} x_1 + \gamma_2^{(N)} x_2 + \cdots + \gamma_N^{(N)} x_N = t_N$$

Time Complexity: $\boldsymbol{O(N^3)}$

Design Rationale



Design Rationale

Goal: **Find $x \in \mathbb{F}_q^n$, from $t = \mathcal{F}(x)$; $t \in \mathbb{F}_q^m$**

Layer: I $x_1, x_2, \cdots, x_v$ | $x_{v+1}, \cdots, x_{v+d}$

$$\gamma_{v+1}^{(1)} x_{v+1} + c_1 = t_1$$

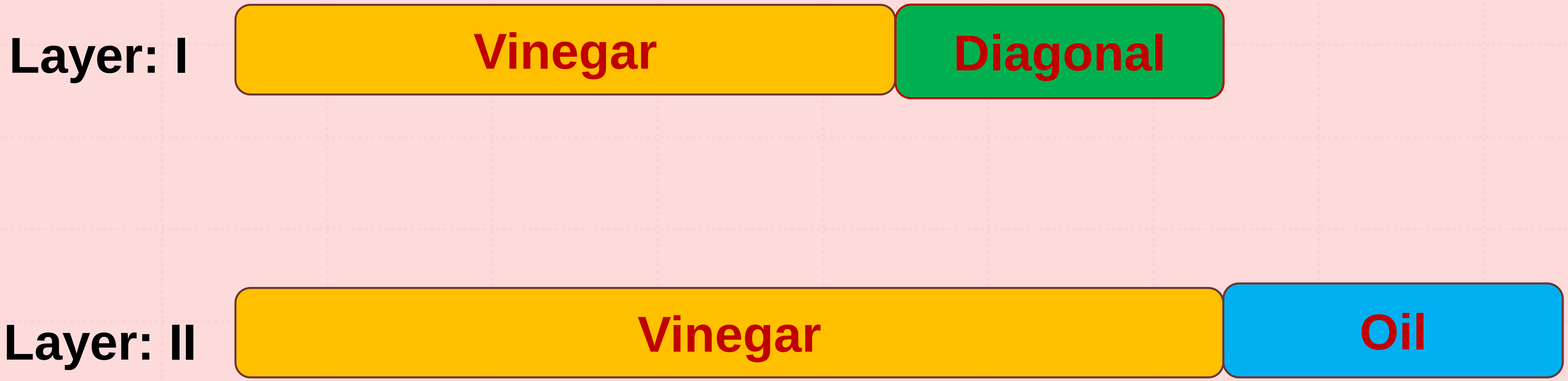
$$\gamma_{v+2}^{(2)} x_{v+2} + c_2 = t_2$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\gamma_n^{(d)} x_{v+d} + c_d = t_d$$

Design Rationale



Design Rationale

Layer: II

$x_1, x_2, \cdots, x_v, \cdots, x_{v+d}$	$x_{v+d+1}, \cdots, x_{v+d+o_1}$

$$\gamma_{v+d+1}^{(d+1)} x_{v+d+1} + \gamma_{v+d+2}^{(d+1)} x_{v+d+2} + \cdots + \gamma_{v+d+o_1}^{(d+1)} x_{v+d+o_1} = t_{d+1}$$

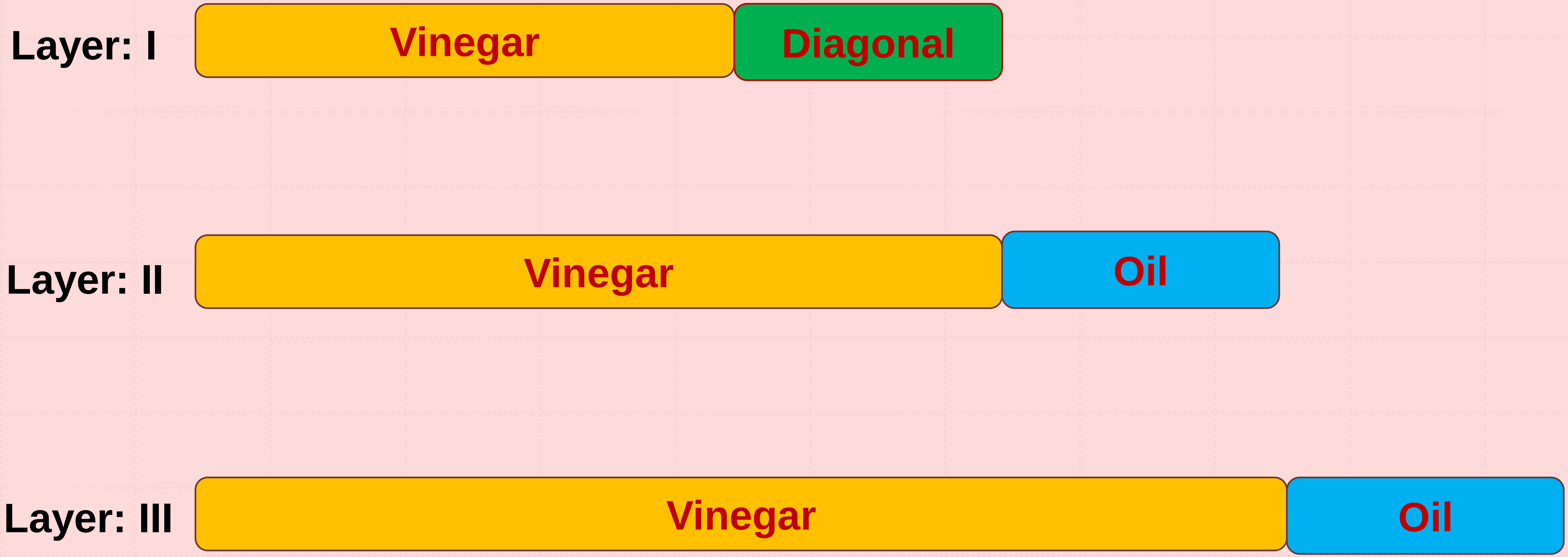
$$\gamma_{v+d+1}^{(d+2)} x_{v+d+1} + \gamma_{v+d+2}^{(d+2)} x_{v+d+2} + \cdots + \gamma_{v+d+o_1}^{(d+2)} x_{v+d+o_1} = t_{d+2}$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\gamma_{v+d+1}^{(d+o_1)} x_{v+d+1} + \gamma_{v+d+2}^{(d+o_1)} x_{v+d+2} + \cdots + \gamma_{v+d+o_1}^{(d+o_1)} x_{v+d+o_1} = t_{d+o_1}$$

Design Rationale



Design Rationale

Layer: III $x_1, x_2, \cdots, x_v, \cdots, x_{v+d}, \cdots, x_{v+d+o_1}$ $x_{v+d+o_1+1}, \cdots, x_n$

$$\gamma^{(d+o_1+1)}_{v+d+o_1+1} x_{v+d+o_1+1} + \gamma^{(d+o_1+1)}_{v+d+o_1+2} x_{v+d+o_1+2} + \cdots + \gamma^{(d+o_1+1)}_{n} x_n = t_{d+o_1+1}$$

$$\gamma^{(d+o_1+2)}_{v+d+o_1+1} x_{v+d+o_1+1} + \gamma^{(d+o_1+2)}_{v+2} x_{v+d+o_1+2} + \cdots + \gamma^{(d+o_1+2)}_{n} x_n = t_{d+o_1+2}$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\gamma^{(m)}_{v+d+o_1+1} x_{v+d+o_1+1} + \gamma^{(m)}_{v+d+o_1+2} x_{v+d+o_1+2} + \cdots + \gamma^{(m)}_{n} x_n = t_m$$

Parameters

Security Level	Parameters (q, v, d, o_1, o_2) + salt	Signature Size (B)	Public Key (KB)
SL-1 (128-bit)	(16,60,30,34,36)	96	236
SL-3 (192-bit)	(256,100,30,40,40)	226	2437
SL-5 (256-bit)	(256,120,50,60,70)	316	8127

Chen, L., Moody, D., Liu, Y.: NIST post-quantum cryptography standardization. Transition 800, 131A (2017)

Careful Cryptanalysis

Structural attacks -- Forgery

1. Kipnis-Shamir attack [KS98]
2. Intersection attack [Beullens-21]
   - Simple attack [Beu22]
3. Rectangular min-rank attack [Beu21]
   - Combine (simple + rectangular min-rank) attack [Beu22]

Find an equivalent composition

$$\mathcal{P} = \mathcal{S}' \circ \mathcal{F}' \circ \mathcal{T}'$$

Structural attacks -- Forgery

1. Kipnis-Shamir attack [KS98]
2. Intersection attack [Beullens-21]
   - Simple attack [Beu22]
3. Rectangular min-rank attack [Beu21]
   - Combine (simple + rectangular min-rank) attack [Beu22]

Find an oil vector

VDOO is Secure

Parameter set	Simple attack	Combine attack	Intersection attack
Security level-I (128-bit)	*134*	136	141
Security level-III (192-bit)	207	*194*	229
Security level-V (256-bit)	270	*264*	293

Provable Security?

- Traditional MQ signature algorithms often depend on *ad-hoc* assumptions.
- While UOV Problem is well understood.
- The *EUF-CMA security of VDOO* signature scheme reduces to its EUF-KOA security.
- EUF-KOA security of VDOO scheme reduces to the *hardness of UOV problem (+ VDOO problem)*.
- Implying: VDOO is EUF-CMA secure.

EUF-CMA:: Existential Unforgeability under Chosen Message Attack
EUF-KOA:: Existential Unforgeability under Key Only Attack

Comparison

VDOO is Short and Fast

Algorithm	Sign size (B)	Public key size (KB)	Computational bottleneck in signing
VDOO	**96**	**238**	$GE_{(16,34)}+GE_{(16,36)}$
Mayo	387	1	$GE_{(16,65)}$
Rainbow	128	861	$GE_{(256,32)}+GE_{(256,48)}$
Unbalanced Oil-Vinegar	134	335	$GE_{(256,64)}$
QR-UOV	331	21	$GE_{(7,100)}$
TUOV	80	65	$GE_{(16,64)}+GE_{(16,32)}$

$GE_{(q,m)}$: Gaussian elimination of a system of m equations over $\mathbb{F}_q$

w.r.t. SL-1 parameters

Shortest among Standardized Signatures

Algorithms	Signature size (B)	Public Key size (B)
VDOO	**96**	**23813**
Crystals Dilithium	2420	1312
Falcon	666	897
SPHINCS+	7856	32

w.r.t. SL-1 parameters

At the End…

Conclusion

1. VDOO offers 96 Bytes for 128-bit security level
2. Gaussian elimination is faster for VDOO central polynomial
3. No classical and quantum attacks are known
4. Thus, useful for practical purpose.

Future Scope

1. Can we further reduce public key size?
2. Can we prove the security in Quantum Random Oracle?
3. Implementation package?
4. Physical/ side-channel attacks?

Anindya Ganguly
CSE, IITK
anindyag@cse.iitk.ac.in

Angshuman Karmakar
CSE, IITK
angshuman@cse.iitk.ac.in

Nitin Saxena
CSE, IITK
nitin@cse.iitk.ac.in

Any Questions?

Anindya Ganguly
CSE, IITK
anindyag@cse.iitk.ac.in

Angshuman Karmakar
CSE, IITK
angshuman@cse.iitk.ac.in

Nitin Saxena
CSE, IITK
nitin@cse.iitk.ac.in

Thank You!