



# MQ Signatures for PKI

June 2017

**Alan Szepieniec,**  
Ward Beullens, Bart Preneel



# New Hope Key Exchange

- Post-Quantum KX based on RLWE
- USENIX 2016

# New Hope Key Exchange

- Post-Quantum KX based on RLWE
- USENIX 2016
  - Facebook Internet Defense Prize

# New Hope Key Exchange

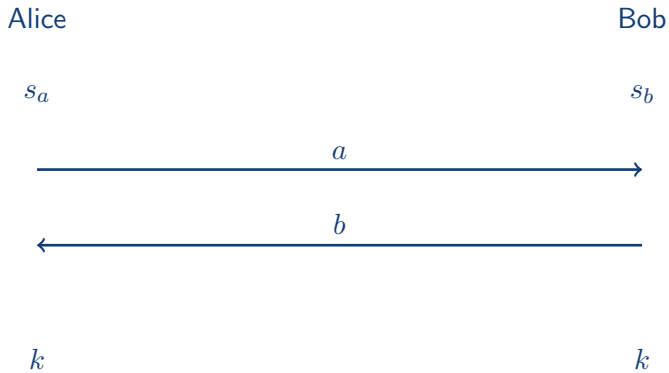
- Post-Quantum KX based on RLWE
- USENIX 2016
  - Facebook Internet Defense Prize
- Google Experiment
  - fraction of Chrome browsers use ECDH+NH

# New Hope Key Exchange

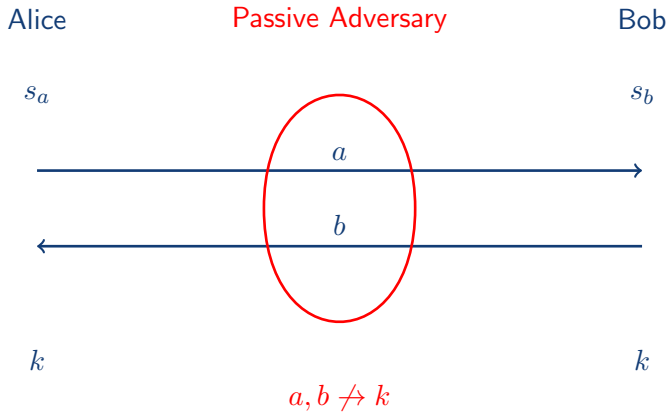
- Post-Quantum KX based on RLWE
- USENIX 2016
  - Facebook Internet Defense Prize
- Google Experiment
  - fraction of Chrome browsers use ECDH+NH

\o/

# Post-Quantum Key Exchange



# Post-Quantum Key Exchange





# Post-Quantum Key Exchange

Alice

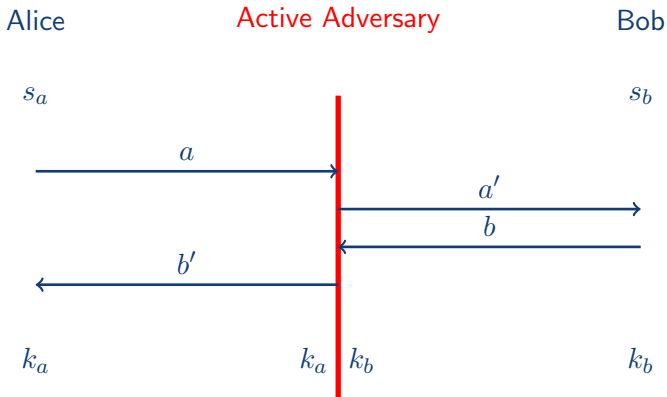
Active Adversary

Bob

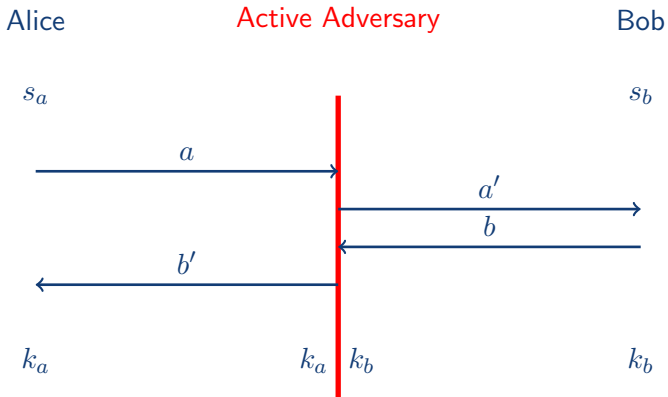
$s_a$

$s_b$

# Post-Quantum Key Exchange

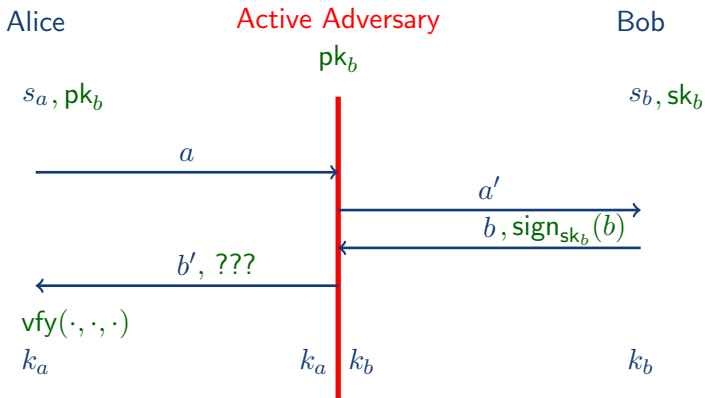


# Post-Quantum Key Exchange



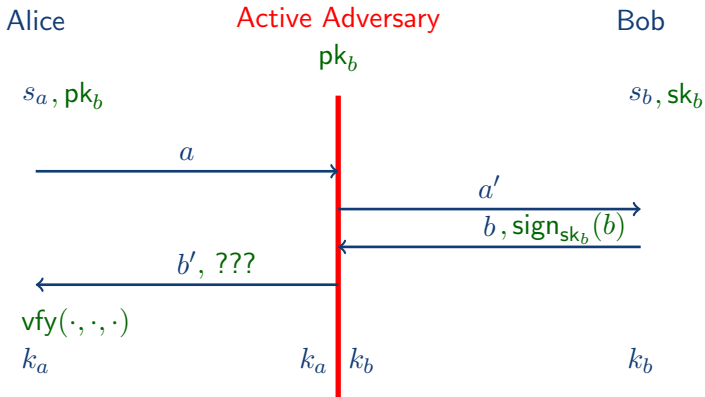
How to kill MitM?

# Post-Quantum Key Exchange



How to kill MitM? Signatures, of course!

# Post-Quantum Key Exchange



How to kill MitM? Signatures, of course!

Post-Quantum

# Public Key Infrastructure (PKI)

Alice

$b, \text{sign}_{sk_b}(b)$



# Public Key Infrastructure (PKI)

Alice

$b, \text{sign}_{sk_b}(b), pk_b$



# Public Key Infrastructure (PKI)

Alice

$b, \text{sign}_{sk_b}(b), pk_b, \text{sign}_{sk_c}(pk_b)$





# Public Key Infrastructure (PKI)

Alice

$b, \text{sign}_{sk_b}(b), pk_b, \text{sign}_{sk_c}(pk_b), pk_c$



# Public Key Infrastructure (PKI)

Alice

$pk_r$

$b, \text{sign}_{sk_b}(b), pk_b, \text{sign}_{sk_c}(pk_b), pk_c, \dots, \text{sign}_{sk_r}(pk_q)$

←

certificate

$\text{vfy}(\cdot, \cdot, \cdot)$

# Public Key Infrastructure (PKI)

Alice

$pk_r$

$b, \text{sign}_{sk_b}(b), pk_b, \text{sign}_{sk_c}(pk_b), pk_c, \dots, \text{sign}_{sk_r}(pk_q)$

←

certificate

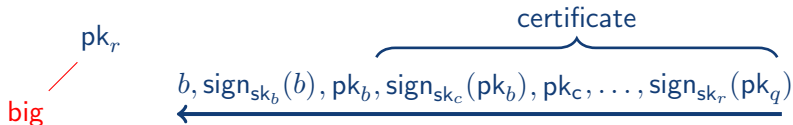
$\text{vfy}(\cdot, \cdot, \cdot)$

desirable properties

acceptable drawbacks

# Public Key Infrastructure (PKI)

Alice



$\text{vfy}(\cdot, \cdot, \cdot)$

desirable properties

acceptable drawbacks

# Public Key Infrastructure (PKI)

Alice

$pk_r$   
big

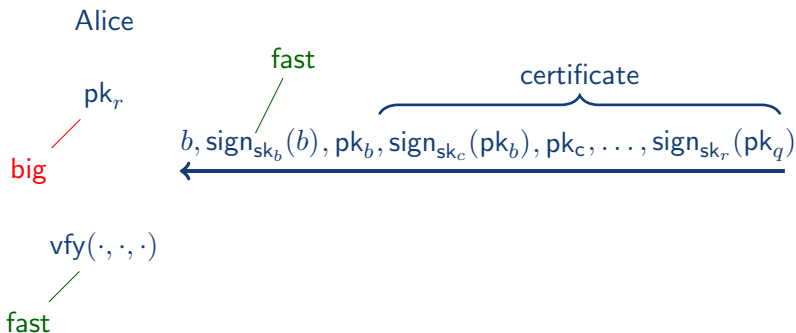
certificate  
 $b, \text{sign}_{sk_b}(b), pk_b, \text{sign}_{sk_c}(pk_b), pk_c, \dots, \text{sign}_{sk_r}(pk_q)$

$\text{vfy}(\cdot, \cdot, \cdot)$   
fast

desirable properties

acceptable drawbacks

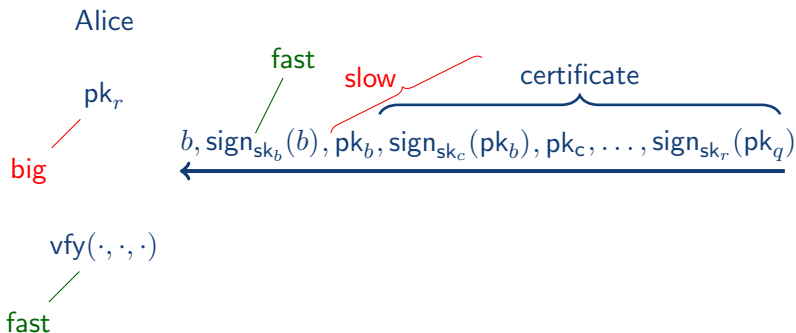
# Public Key Infrastructure (PKI)



desirable properties

acceptable drawbacks

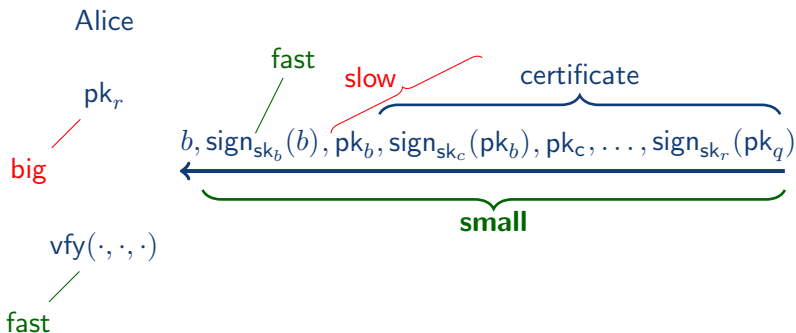
# Public Key Infrastructure (PKI)



desirable properties

acceptable drawbacks

# Public Key Infrastructure (PKI)

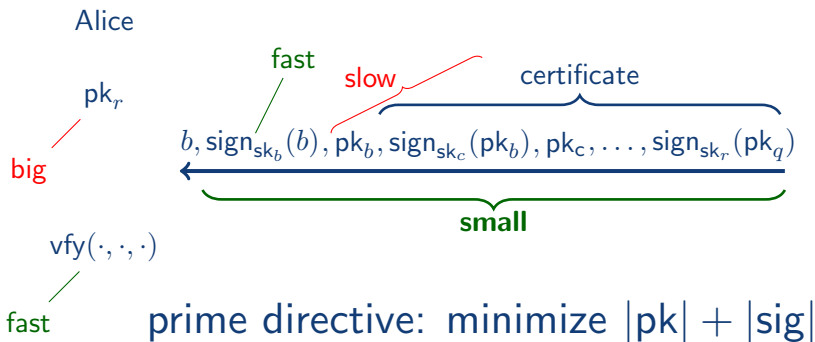


desirable properties

acceptable drawbacks



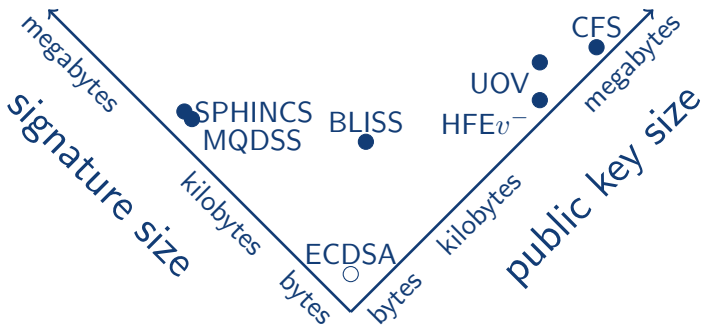
# Public Key Infrastructure (PKI)



desirable properties

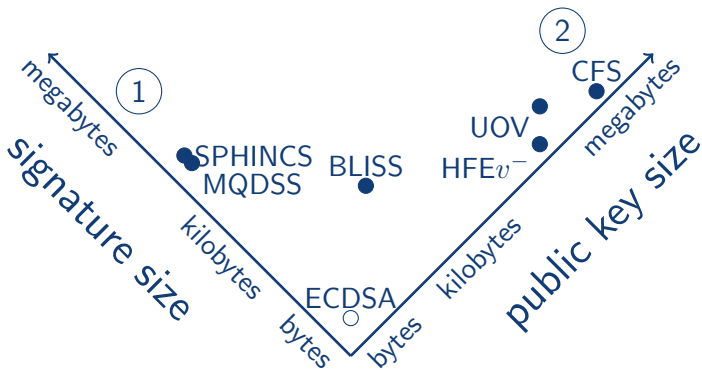
acceptable drawbacks

## Post-Quantum Signature Schemes



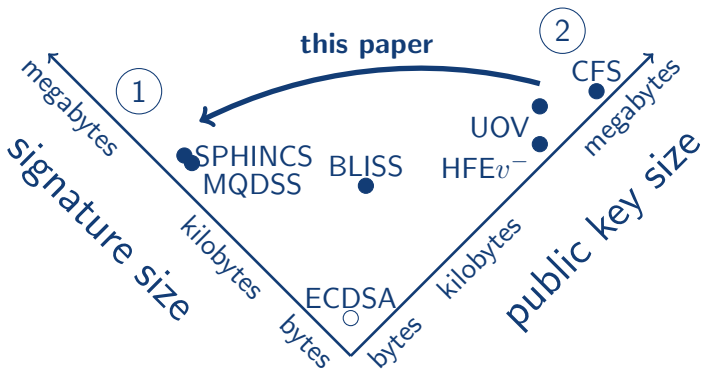
strategy: *transform MQ-signature schemes to shrink  $|pk| + |s|$*

## Post-Quantum Signature Schemes



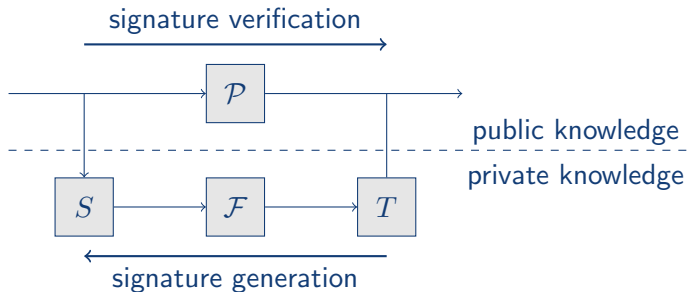
strategy: *transform MQ-signature schemes to shrink  $|pk| + |s|$*

# Post-Quantum Signature Schemes



strategy: *transform MQ-signature schemes to shrink  $|pk| + |s|$*

# MQ Signature Schemes



$$\mathcal{P}, \mathcal{F} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$$

$$\mathbf{s} \in \mathbb{F}_q^n$$

$$T, S \in \text{GL}(\mathbb{F}_q)$$

$$\text{vfy} : \mathcal{P}(\mathbf{s}) \stackrel{?}{=} H(d)$$

## Transformation

Step 1: replace  $\mathcal{P}(s) \stackrel{?}{=} H(d)$  with  $\mathbf{t}\mathcal{P}(s) \stackrel{?}{=} \mathbf{t}H(d)$  for  $\mathbf{t} \stackrel{\$}{\leftarrow} \mathbb{F}_q^{\alpha \times m}$

determine  $\mathbf{t} = H(s)$

transmit  $\mathcal{R}(\mathbf{x}) = \mathbf{t}\mathcal{P}(\mathbf{x})$  with  $s$  as part of signature

## Transformation

Step 1: replace  $\mathcal{P}(s) \stackrel{?}{=} H(d)$  with  $\mathbf{t}\mathcal{P}(s) \stackrel{?}{=} \mathbf{t}H(d)$  for  $\mathbf{t} \stackrel{\$}{\leftarrow} \mathbb{F}_q^{\alpha \times m}$

determine  $\mathbf{t} = H(s)$

transmit  $\mathcal{R}(\mathbf{x}) = \mathbf{t}\mathcal{P}(\mathbf{x})$  with  $s$  as part of signature

Step 2: authenticate  $\mathcal{R}(\mathbf{x})$  using linearly homomorphic MACs

## Transformation

Step 1: replace  $\mathcal{P}(s) \stackrel{?}{=} H(d)$  with  $\mathbf{t}\mathcal{P}(s) \stackrel{?}{=} \mathbf{t}H(d)$  for  $\mathbf{t} \stackrel{\$}{\leftarrow} \mathbb{F}_q^{\alpha \times m}$

determine  $\mathbf{t} = H(s)$

transmit  $\mathcal{R}(\mathbf{x}) = \mathbf{t}\mathcal{P}(\mathbf{x})$  with  $s$  as part of signature

Step 2: authenticate  $\mathcal{R}(\mathbf{x})$  using linearly homomorphic MACs

2a. define  $\hat{\mathcal{R}}(z), \hat{\mathcal{P}}(z)$  with same coefficients as  $\mathcal{R}(\mathbf{x}), \mathcal{P}(\mathbf{x})$



## Transformation

Step 1: replace  $\mathcal{P}(s) \stackrel{?}{=} H(d)$  with  $\mathbf{t}\mathcal{P}(s) \stackrel{?}{=} \mathbf{t}H(d)$  for  $\mathbf{t} \stackrel{\$}{\leftarrow} \mathbb{F}_q^{\alpha \times m}$

determine  $\mathbf{t} = H(s)$

transmit  $\mathcal{R}(\mathbf{x}) = \mathbf{t}\mathcal{P}(\mathbf{x})$  with  $s$  as part of signature

Step 2: authenticate  $\mathcal{R}(\mathbf{x})$  using linearly homomorphic MACs

2a. define  $\hat{\mathcal{R}}(z), \hat{\mathcal{P}}(z)$  with same coefficients as  $\mathcal{R}(\mathbf{x}), \mathcal{P}(\mathbf{x})$

2b. verify that  $\mathbf{t}\hat{\mathcal{P}}(z) = \hat{\mathcal{R}}(z)$  instead of  $\mathbf{t}\mathcal{P}(\mathbf{x}) = \mathcal{R}(\mathbf{x})$

$$\begin{array}{ccc} \mathcal{P}(\mathbf{x}) & \xrightarrow{\text{MAC}} & \hat{\mathcal{P}}(z) \\ \downarrow \mathbf{t} & & \downarrow \mathbf{t} \\ \mathbf{t}\mathcal{P}(\mathbf{x}) & \xrightarrow{\text{MAC}} & \mathbf{t}\hat{\mathcal{P}}(z) \end{array}$$

## Transformation

Step 1: replace  $\mathcal{P}(s) \stackrel{?}{=} H(d)$  with  $\mathbf{t}\mathcal{P}(s) \stackrel{?}{=} \mathbf{t}H(d)$  for  $\mathbf{t} \stackrel{\$}{\leftarrow} \mathbb{F}_q^{\alpha \times m}$

determine  $\mathbf{t} = H(\mathbf{s})$

transmit  $\mathcal{R}(\mathbf{x}) = \mathbf{t}\mathcal{P}(\mathbf{x})$  with  $\mathbf{s}$  as part of signature

Step 2: authenticate  $\mathcal{R}(\mathbf{x})$  using linearly homomorphic MACs

2a. define  $\hat{\mathcal{R}}(z), \hat{\mathcal{P}}(z)$  with same coefficients as  $\mathcal{R}(\mathbf{x}), \mathcal{P}(\mathbf{x})$

2b. verify that  $\mathbf{t}\hat{\mathcal{P}}(z) = \hat{\mathcal{R}}(z)$  instead of  $\mathbf{t}\mathcal{P}(\mathbf{x}) = \mathcal{R}(\mathbf{x})$

$$\begin{array}{ccc} \mathcal{P}(\mathbf{x}) & \xrightarrow{\text{MAC}} & \hat{\mathcal{P}}(z) \\ \downarrow \mathbf{t} & & \downarrow \mathbf{t} \\ \mathbf{t}\mathcal{P}(\mathbf{x}) & \xrightarrow{\text{MAC}} & \mathbf{t}\hat{\mathcal{P}}(z) \end{array}$$

2c. verify  $\mathbf{t}\hat{\mathcal{P}}(z_i) = \hat{\mathcal{R}}(z_i)$  in only  $\vartheta$  randomly chosen points

determine  $\{z_1, \dots, z_\vartheta\} = H(\mathcal{R}(\mathbf{x}))$

## Transformation

Step 1: replace  $\mathcal{P}(s) \stackrel{?}{=} H(d)$  with  $\mathbf{t}\mathcal{P}(s) \stackrel{?}{=} \mathbf{t}H(d)$  for  $\mathbf{t} \stackrel{\$}{\leftarrow} \mathbb{F}_q^{\alpha \times m}$

determine  $\mathbf{t} = H(\mathbf{s})$

transmit  $\mathcal{R}(\mathbf{x}) = \mathbf{t}\mathcal{P}(\mathbf{x})$  with  $\mathbf{s}$  as part of signature

Step 2: authenticate  $\mathcal{R}(\mathbf{x})$  using linearly homomorphic MACs

2a. define  $\hat{\mathcal{R}}(z), \hat{\mathcal{P}}(z)$  with same coefficients as  $\mathcal{R}(\mathbf{x}), \mathcal{P}(\mathbf{x})$

2b. verify that  $\mathbf{t}\hat{\mathcal{P}}(z) = \hat{\mathcal{R}}(z)$  instead of  $\mathbf{t}\mathcal{P}(\mathbf{x}) = \mathcal{R}(\mathbf{x})$

$$\begin{array}{ccc} \mathcal{P}(\mathbf{x}) & \xrightarrow{\text{MAC}} & \hat{\mathcal{P}}(z) \\ \downarrow \mathbf{t} & & \downarrow \mathbf{t} \\ \mathbf{t}\mathcal{P}(\mathbf{x}) & \xrightarrow{\text{MAC}} & \mathbf{t}\hat{\mathcal{P}}(z) \end{array}$$

2c. verify  $\mathbf{t}\hat{\mathcal{P}}(z_i) = \hat{\mathcal{R}}(z_i)$  in only  $\vartheta$  randomly chosen points

determine  $\{z_1, \dots, z_\vartheta\} = H(\mathcal{R}(\mathbf{x}))$

2d. Merkleize all  $\tau$  evaluations  $\hat{\mathcal{P}}(z_i)$

## Transformation

Step 1: replace  $\mathcal{P}(s) \stackrel{?}{=} H(d)$  with  $\mathbf{t}\mathcal{P}(s) \stackrel{?}{=} \mathbf{t}H(d)$  for  $\mathbf{t} \stackrel{\$}{\leftarrow} \mathbb{F}_q^{\alpha \times m}$

determine  $\mathbf{t} = H(\mathbf{s})$

transmit  $\mathcal{R}(\mathbf{x}) = \mathbf{t}\mathcal{P}(\mathbf{x})$  with  $\mathbf{s}$  as part of signature

Step 2: authenticate  $\mathcal{R}(\mathbf{x})$  using linearly homomorphic MACs

2a. define  $\hat{\mathcal{R}}(z), \hat{\mathcal{P}}(z)$  with same coefficients as  $\mathcal{R}(\mathbf{x}), \mathcal{P}(\mathbf{x})$

2b. verify that  $\mathbf{t}\hat{\mathcal{P}}(z) = \hat{\mathcal{R}}(z)$  instead of  $\mathbf{t}\mathcal{P}(\mathbf{x}) = \mathcal{R}(\mathbf{x})$

$$\begin{array}{ccc} \mathcal{P}(\mathbf{x}) & \xrightarrow{\text{MAC}} & \hat{\mathcal{P}}(z) \\ \downarrow \mathbf{t} & & \downarrow \mathbf{t} \\ \mathbf{t}\mathcal{P}(\mathbf{x}) & \xrightarrow{\text{MAC}} & \mathbf{t}\hat{\mathcal{P}}(z) \end{array}$$

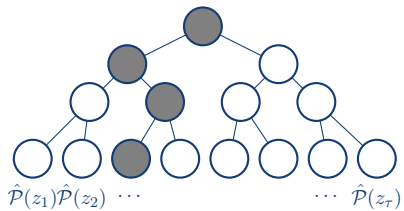
2c. verify  $\mathbf{t}\hat{\mathcal{P}}(z_i) = \hat{\mathcal{R}}(z_i)$  in only  $\vartheta$  randomly chosen points

determine  $\{z_1, \dots, z_\vartheta\} = H(\mathcal{R}(\mathbf{x}))$

2d. Merkleize all  $\tau$  evaluations  $\hat{\mathcal{P}}(z_i)$

new signature:  $(\mathbf{s}, \mathcal{R}(\mathbf{x}), \text{Merkle paths})$     new public key: *Merkle root*

# Merkle Tree



## Provable Security

$$\begin{aligned} \text{InSec}_{\text{NEW}}^{\text{EUF-CMA}}(t, Q) &\leq \text{InSec}_{\text{ORIGINAL}}^{\text{EUF-CMA}}(t + O(Q), Q) \\ &+ (2\tau - 1) \frac{Q+1}{2^\kappa} \\ &+ \left( \frac{n(n+1)}{2\tau} \right)^{\vartheta} (Q + 1) \\ &+ q^{-\alpha} (Q + 1) \end{aligned}$$

# Provable Security

$$\begin{aligned} \text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, Q) &\leq \text{InSec}_{\text{ORIGINAL}}^{\text{EUFCMA}}(t + O(Q), Q) && \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \text{original scheme} \\ &+ (2\tau - 1) \frac{Q+1}{2^\kappa} && \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \text{Merkle tree} \\ &+ \left( \frac{n(n+1)}{2\tau} \right)^{\vartheta} (Q+1) && \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \text{MAC polynomials} \\ &+ q^{-\alpha} (Q+1) && \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \text{lucky s} \end{aligned}$$





## Example Parameters

scheme	parameters	sec. lvl.	pk	s
UOVRand	$q = 256, n = 135, m = 45$	128	45.5 kB	1080
transformed	$\alpha = 16, \vartheta = 12, \tau = 2^{20}$	128	256 bits	21.3 kB
UOVRand	$q = 256, n = 210, m = 70$	192	169.9 kB	1 680 bits
transformed	$\alpha = 24, \vartheta = 19, \tau = 2^{20}$	192	384 bits	70.4 kB
UOVRand	$q = 256, n = 285, m = 95$	256	423.0 kB	2 280 bits
transformed	$\alpha = 32, \vartheta = 28, \tau = 2^{20}$	256	512 bits	166.3 kB

## Improvement

- idea: use *multiple* signatures
- $s_1, \dots, s_\sigma$  such that  $\mathcal{P}(s_i) = H(d||i)$

## Improvement

- idea: use *multiple* signatures
- $\mathbf{s}_1, \dots, \mathbf{s}_\sigma$  such that  $\mathcal{P}(\mathbf{s}_i) = \mathbf{H}(d\|i)$
- ... reduce  $\alpha$   $\longrightarrow$  fewer polynomials in  $\mathcal{R}$

## Improvement

- idea: use *multiple* signatures
- $\mathbf{s}_1, \dots, \mathbf{s}_\sigma$  such that  $\mathcal{P}(\mathbf{s}_i) = H(d\|i)$
- ... reduce  $\alpha \rightarrow$  fewer polynomials in  $\mathcal{R}$
- $|\mathbf{s}_i| = n \log_2 q$  whereas  $|\mathcal{R}_i(\mathbf{x})| = \frac{n(n+1)}{2} \log_2 q$
- $q^\alpha > 2^\kappa$  becomes  $q^{\alpha\sigma} > 2^\kappa$

## Security Proof Fails

$$\begin{aligned} \text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q}) &\leq \text{InSec}_{\text{ORIGINAL}}^{\text{EUFCMA}}(t + O(\hat{Q}), \hat{Q}) && \left. \vphantom{\text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q})} \right\} \text{original scheme} \\ &+ \Theta\left((2\tau - 1) \frac{(\hat{Q} + 1)^2}{2^\kappa}\right) && \left. \vphantom{\text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q})} \right\} \text{Merkle tree} \\ &+ \Theta\left(\left(\frac{n(n+1)}{2\tau}\right)^\vartheta (\hat{Q} + 1)^2\right) && \left. \vphantom{\text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q})} \right\} \text{MAC polynomials} \\ &+ \Theta\left(q^{-\sigma\alpha} (\hat{Q} + 1)^2\right) && \left. \vphantom{\text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q})} \right\} \text{lucky s} \end{aligned}$$

## Security Proof Fails

$$\begin{aligned} \text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q}) &\leq \text{InSec}_{\text{ORIGINAL}}^{\text{EUFCMA}}(t + O(\hat{Q}), \hat{Q}) && \left. \vphantom{\text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q})} \right\} \text{original scheme} \\ &+ \Theta\left((2\tau - 1) \frac{(\hat{Q} + 1)^2}{2^\kappa}\right) && \left. \vphantom{\text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q})} \right\} \text{Merkle tree} \\ &+ \Theta\left(\left(\frac{n(n+1)}{2\tau}\right)^\vartheta (\hat{Q} + 1)^2\right) && \left. \vphantom{\text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q})} \right\} \text{MAC polynomials} \\ &\cancel{+ \Theta\left(q^{-\sigma\alpha} (\hat{Q} + 1)^2\right)} && \left. \vphantom{\text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q})} \right\} \text{lucky s} \end{aligned}$$

## Security Proof Fails

$$\begin{aligned} \text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q}) &\leq \text{InSec}_{\text{ORIGINAL}}^{\text{EUFCMA}}(t + O(\hat{Q}), \hat{Q}) && \left. \vphantom{\text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q})} \right\} \text{original scheme} \\ &+ \Theta\left((2\tau - 1) \frac{(\hat{Q} + 1)^2}{2^\kappa}\right) && \left. \vphantom{\text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q})} \right\} \text{Merkle tree} \\ &+ \Theta\left(\left(\frac{n(n+1)}{2\tau}\right)^\vartheta (\hat{Q} + 1)^2\right) && \left. \vphantom{\text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q})} \right\} \text{MAC polynomials} \\ & ~~+ \Theta\left(q^{-\sigma\alpha} (\hat{Q} + 1)^2\right) && \left. \vphantom{\text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q})} \right\} \text{lucky s} \end{aligned}~~$$

rows of  $t$  are independent events ...

## Security Proof Fails

$$\begin{aligned} \text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q}) &\leq \text{InSec}_{\text{ORIGINAL}}^{\text{EUFCMA}}(t + O(\hat{Q}), \hat{Q}) && \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \text{original scheme} \\ &+ \Theta\left((2\tau - 1) \frac{(\hat{Q} + 1)^2}{2^\kappa}\right) && \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \text{Merkle tree} \\ &+ \Theta\left(\left(\frac{n(n+1)}{2\tau}\right)^\vartheta (\hat{Q} + 1)^2\right) && \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \text{MAC polynomials} \\ & ~~+ \Theta\left(q^{-\sigma\alpha} (\hat{Q} + 1)^2\right) && \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \text{lucky } s \end{aligned}~~$$

rows of  $\mathbf{t}$  are independent events ...

... but  $s_i$  are not!



## Security Proof Fails

$$\begin{aligned} \text{InSec}_{\text{NEW}}^{\text{EUFCMA}}(t, \hat{Q}) &\not\leq \text{InSec}_{\text{ORIGINAL}}^{\text{EUFCMA}}(t + O(\hat{Q}), \hat{Q}) \quad \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \text{original scheme} \\ &+ \Theta\left((2\tau - 1) \frac{(\hat{Q} + 1)^2}{2^\kappa}\right) \quad \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \text{Merkle tree} \\ &+ \Theta\left(\left(\frac{n(n+1)}{2\tau}\right)^\vartheta (\hat{Q} + 1)^2\right) \quad \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \text{MAC polynomials} \\ &\cancel{+ \Theta\left(q^{-\sigma\alpha} (\hat{Q} + 1)^2\right)} \quad \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \text{lucky } s \end{aligned}$$

rows of  $\mathbf{t}$  are independent events ...

... but  $s_i$  are not!

## Low-Dim Errors

- find  $\mathbf{s}_1, \dots, \mathbf{s}_\sigma$  such that  $\forall i. \mathbf{t} \mathcal{P}(\mathbf{s}_i) = \mathbf{t} \mathbf{H}(d \| i)$
- model  $\mathbf{t} \leftarrow \mathbf{H}(d \| \mathbf{s}_1 \| \dots \| \mathbf{s}_\sigma)$  as  $\mathbf{t} \leftarrow \mathbb{F}_q^{\alpha \times m}$

## Low-Dim Errors

- find  $\mathbf{s}_1, \dots, \mathbf{s}_\sigma$  such that  $\forall i. \mathbf{t}\mathcal{P}(\mathbf{s}_i) = \mathbf{t}\mathbf{H}(d\|i)$
- model  $\mathbf{t} \leftarrow \mathbf{H}(d\|\mathbf{s}_1\| \cdots \|\mathbf{s}_\sigma)$  as  $\mathbf{t} \stackrel{\$}{\leftarrow} \mathbb{F}_q^{\alpha \times m}$
- works if  $\mathbf{0} \neq \mathcal{P}(\mathbf{s}_i) - \mathbf{H}(d\|i) \in \ker \mathbf{t}$

## Low-Dim Errors

- find  $\mathbf{s}_1, \dots, \mathbf{s}_\sigma$  such that  $\forall i. \mathbf{t}\mathcal{P}(\mathbf{s}_i) = \mathbf{t}\mathbf{H}(d\|i)$
- model  $\mathbf{t} \leftarrow \mathbf{H}(d\|\mathbf{s}_1\| \cdots \|\mathbf{s}_\sigma)$  as  $\mathbf{t} \stackrel{\$}{\leftarrow} \mathbb{F}_q^{\alpha \times m}$
- works if  $\mathbf{0} \neq \mathcal{P}(\mathbf{s}_i) - \mathbf{H}(d\|i) \in \ker \mathbf{t}$
- *error space is low-dim  $\implies$  high success probability*

# AMQ Problem

## Definition

**AMQ Problem.** (Approximate Multivariate Quadratic)

Given:  $\mathcal{P} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m; \mathbf{y}_1, \dots, \mathbf{y}_\sigma \in \mathbb{F}_q^m$

Find:  $\mathbf{x}_1, \dots, \mathbf{x}_\sigma \in \mathbb{F}_q^n$

Such that:  $\dim \langle \{\mathcal{P}(\mathbf{x}_i) - \mathbf{y}_i\}_i \rangle \leq r$

# AMQ Problem

## Definition

**AMQ Problem.** (Approximate Multivariate Quadratic)

Given:  $\mathcal{P} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m; \mathbf{y}_1, \dots, \mathbf{y}_\sigma \in \mathbb{F}_q^m$

Find:  $\mathbf{x}_1, \dots, \mathbf{x}_\sigma \in \mathbb{F}_q^n$

Such that:  $\dim \langle \{\mathcal{P}(\mathbf{x}_i) - \mathbf{y}_i\}_i \rangle \leq r$

- exhaustive search:  $O(q^{m-r})$ ; Grover:  $O(q^{(m-r)/2})$
- $\text{AMQ}[m, n, \sigma, r] \leq \sigma \cdot \text{MQ}[m - r, n]$
- $\text{AMQ}[m, n, \sigma, r] \leq \text{AMQ}[m, n, \sigma + 1, r]$  (gets harder with  $\sigma$ )
- $\text{AMQ}[m, n, \sigma, r + 1] \leq \text{AMQ}[m, n, \sigma, r]$  (gets easier with  $r$ )
- $\text{AMQ}[m, n, \sigma = 1, r = 0] = \text{MQ}[m, n]$

## Example Parameters

scheme	parameters	sec. lvl.	pk	s
original HFE $v^-$	$q = 2, n = 98, m = 90$	80	56.8 kB	98 bits
transformed	$\alpha = 1, \sigma = 80, \vartheta = 7, \tau = 2^{20}$	80 ?	80 bits	4.4 kB
original HFE $v^-$	$q = 2, n = 133, m = 123$	120	139.2 kB	123 bits
transformed	$\alpha = 1, \sigma = 120, \vartheta = 11, \tau = 2^{20}$	120 ?	120 bits	9.4 kB
original HFE $v^-$	$q = 4, n = 141, m = 129$	128 (PQ)	288.4 kB	258 bits
transformed	$\alpha = 1, \sigma = 64, \vartheta = 13, \tau = 2^{20}$	128 ? (PQ)	256 bits	16.5 kB