KU LEUVEN

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

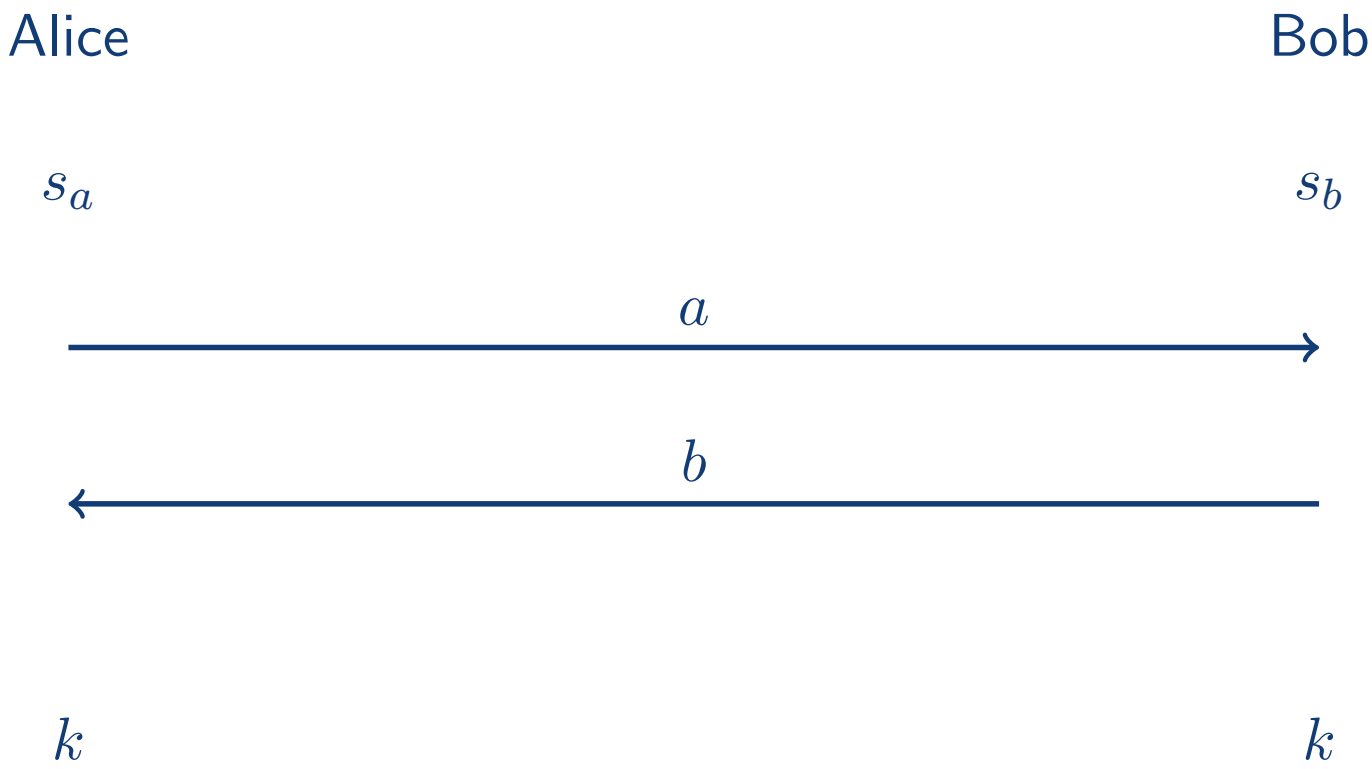
- Post-Quantum KX based on RLWE
- USENIX 2016
  - Facebook Internet Defense Prize
- Google Experiment
  - fraction of Chrome browsers use ECDH+NH

New Hope Key Exchange

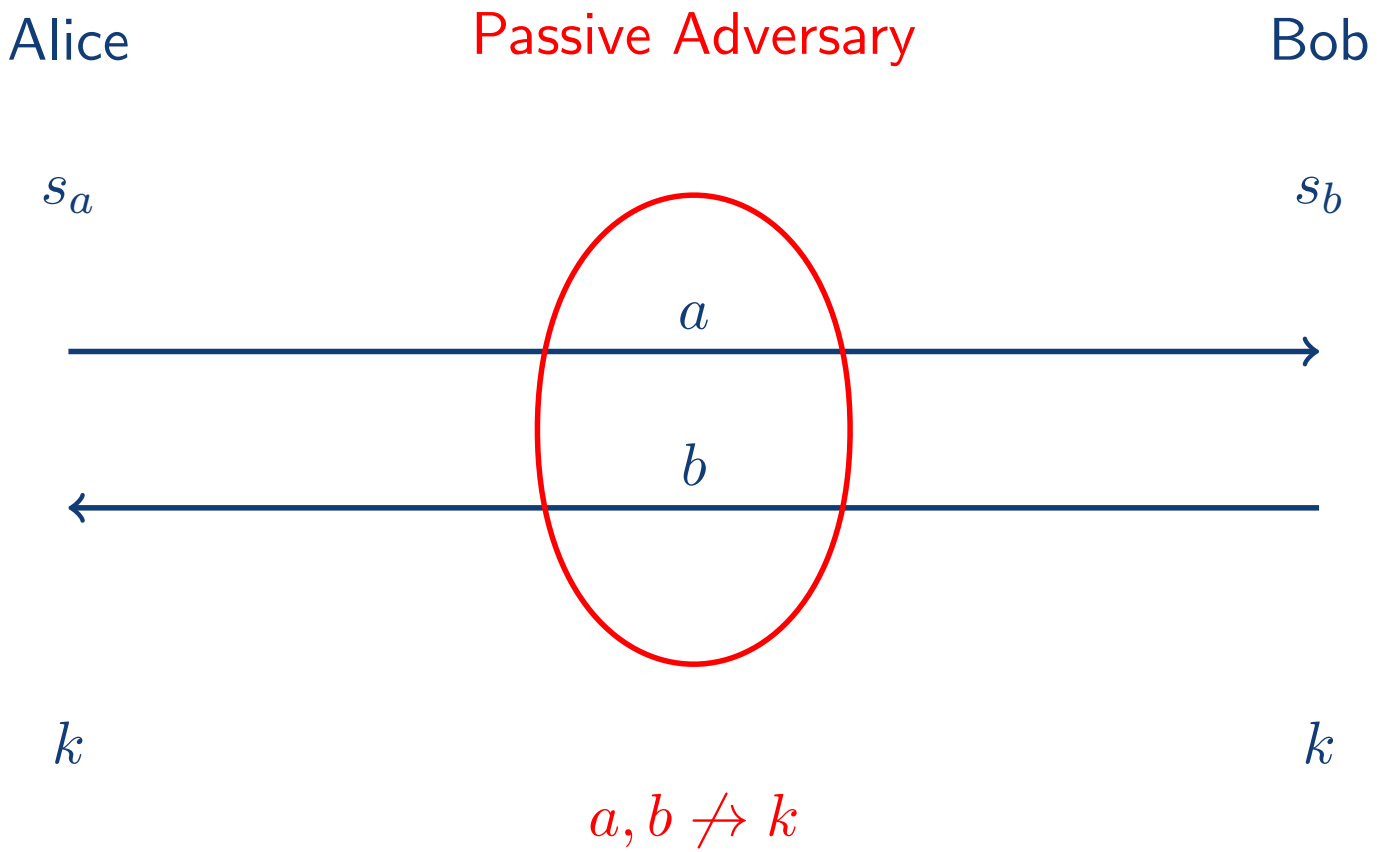
- Post-Quantum KX based on RLWE
- USENIX 2016
  - Facebook Internet Defense Prize
- Google Experiment
  - fraction of Chrome browsers use ECDH+NH

$$\backslash o /$$

Post-Quantum Key Exchange



Post-Quantum Key Exchange

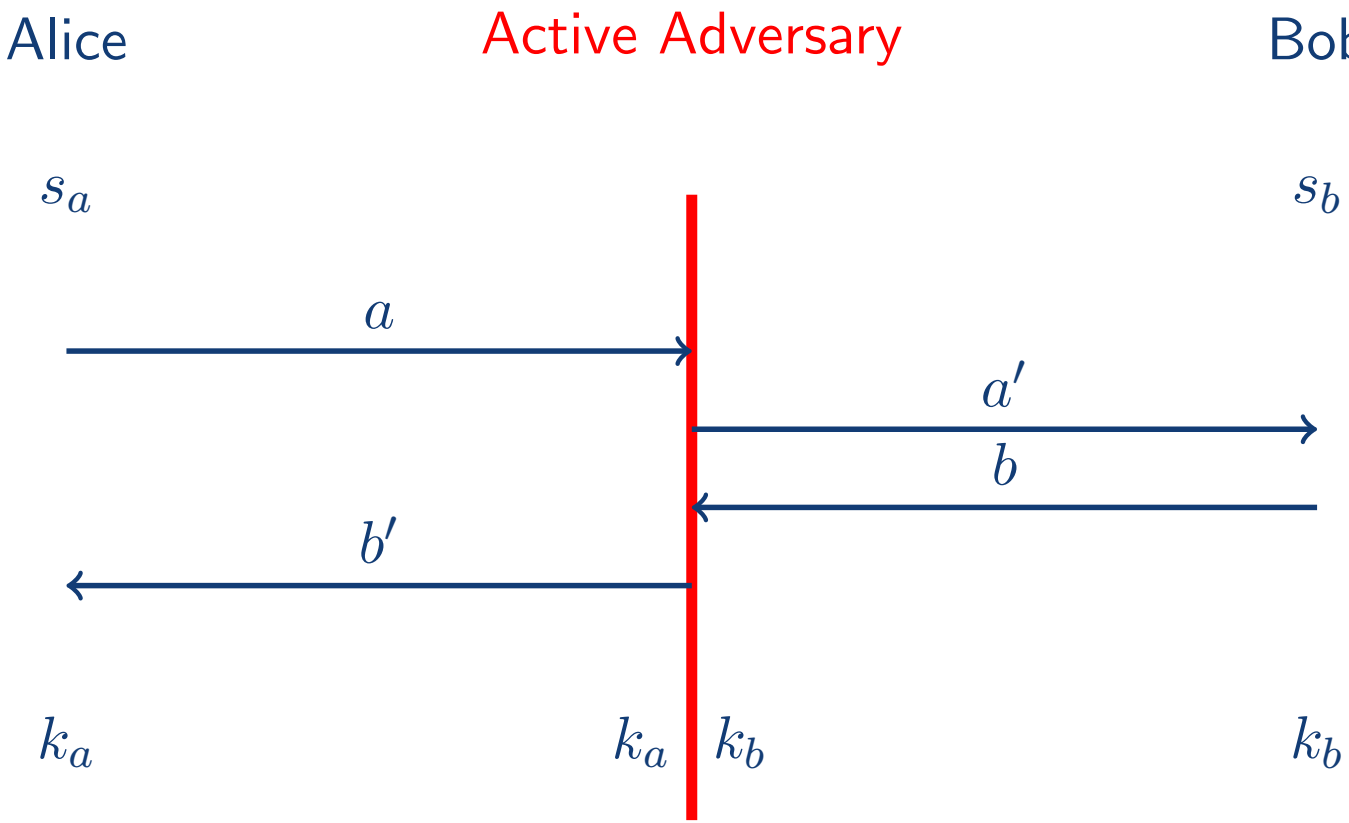


Post-Quantum Key Exchange

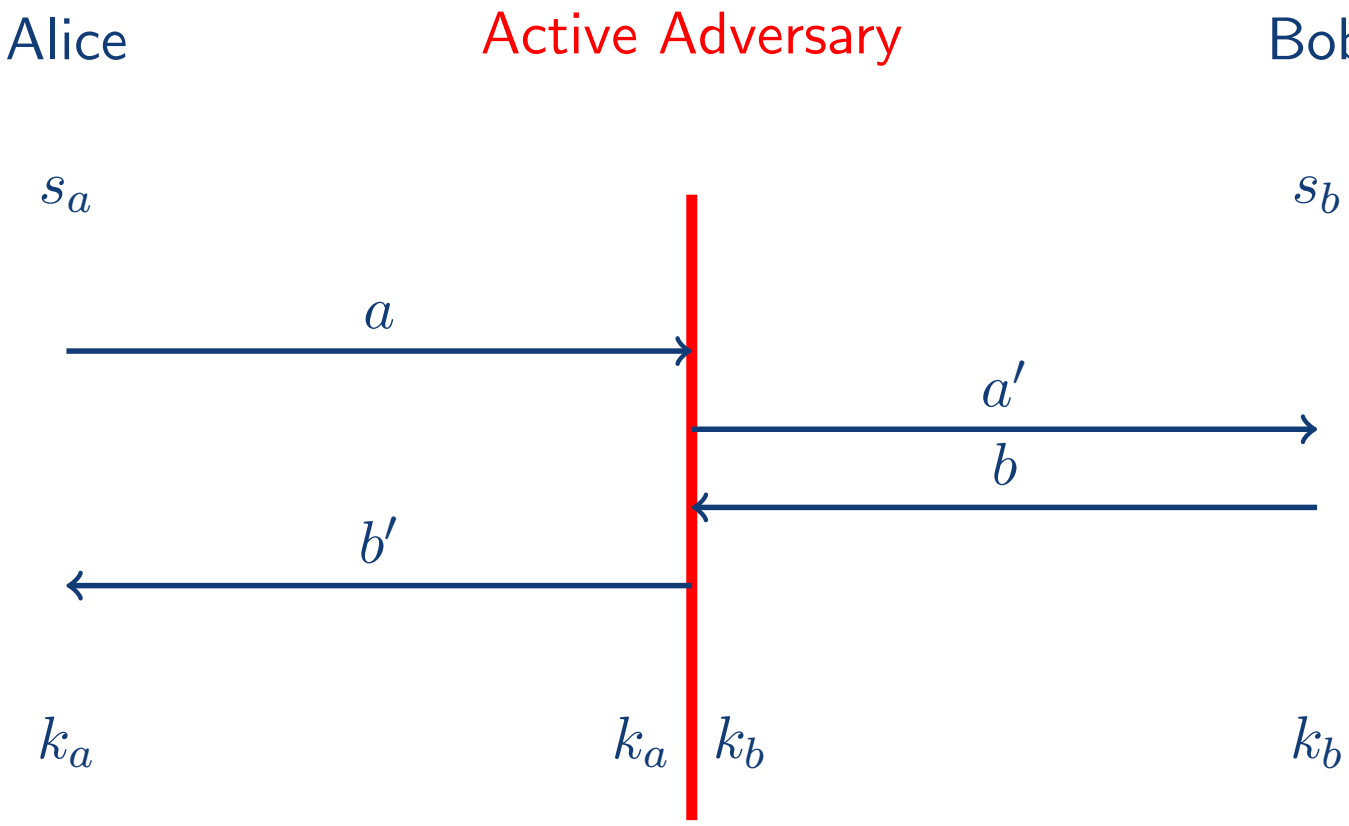
Alice | Active Adversary | Bob

s_a s_b

Post-Quantum Key Exchange

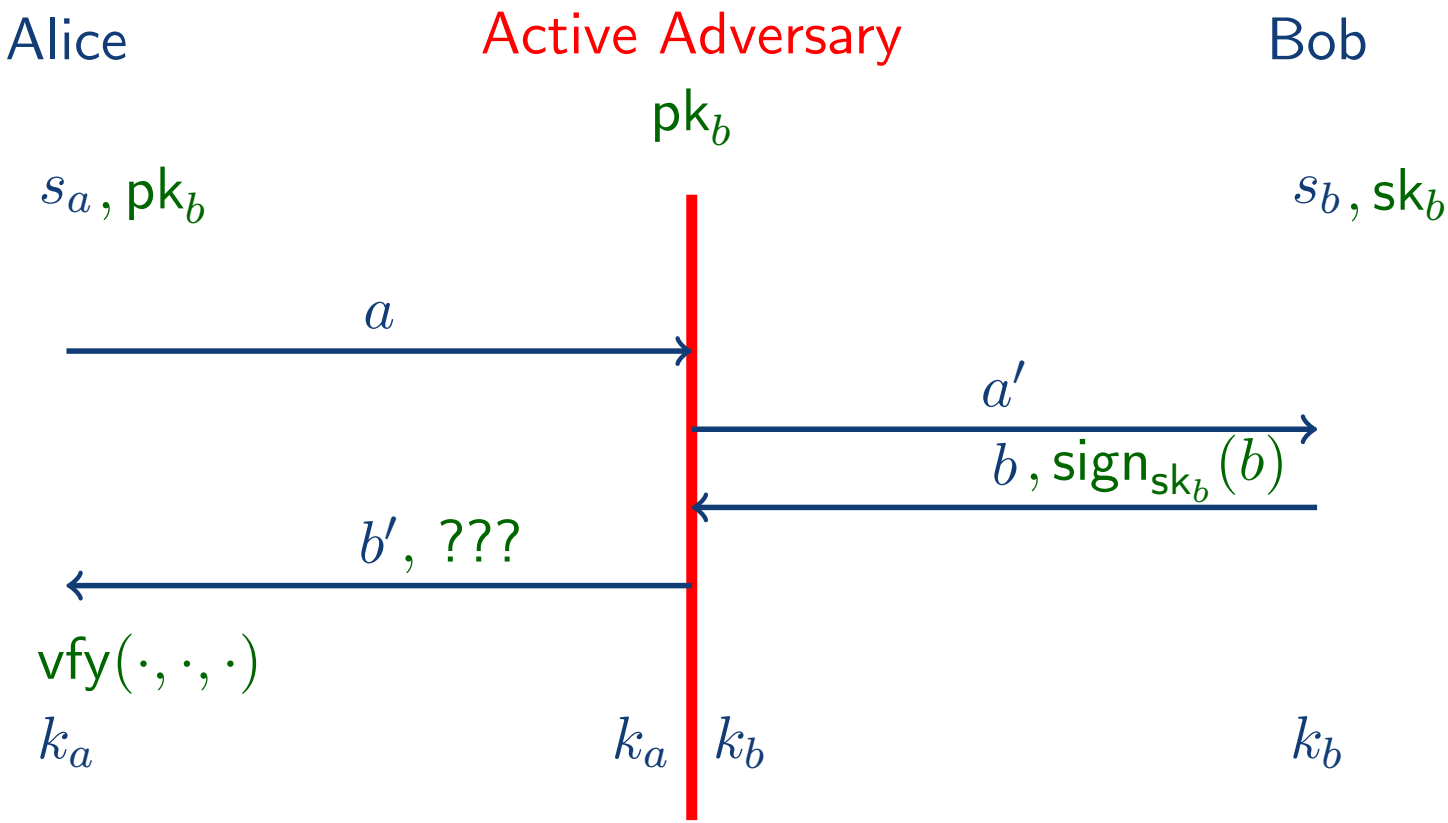


Post-Quantum Key Exchange



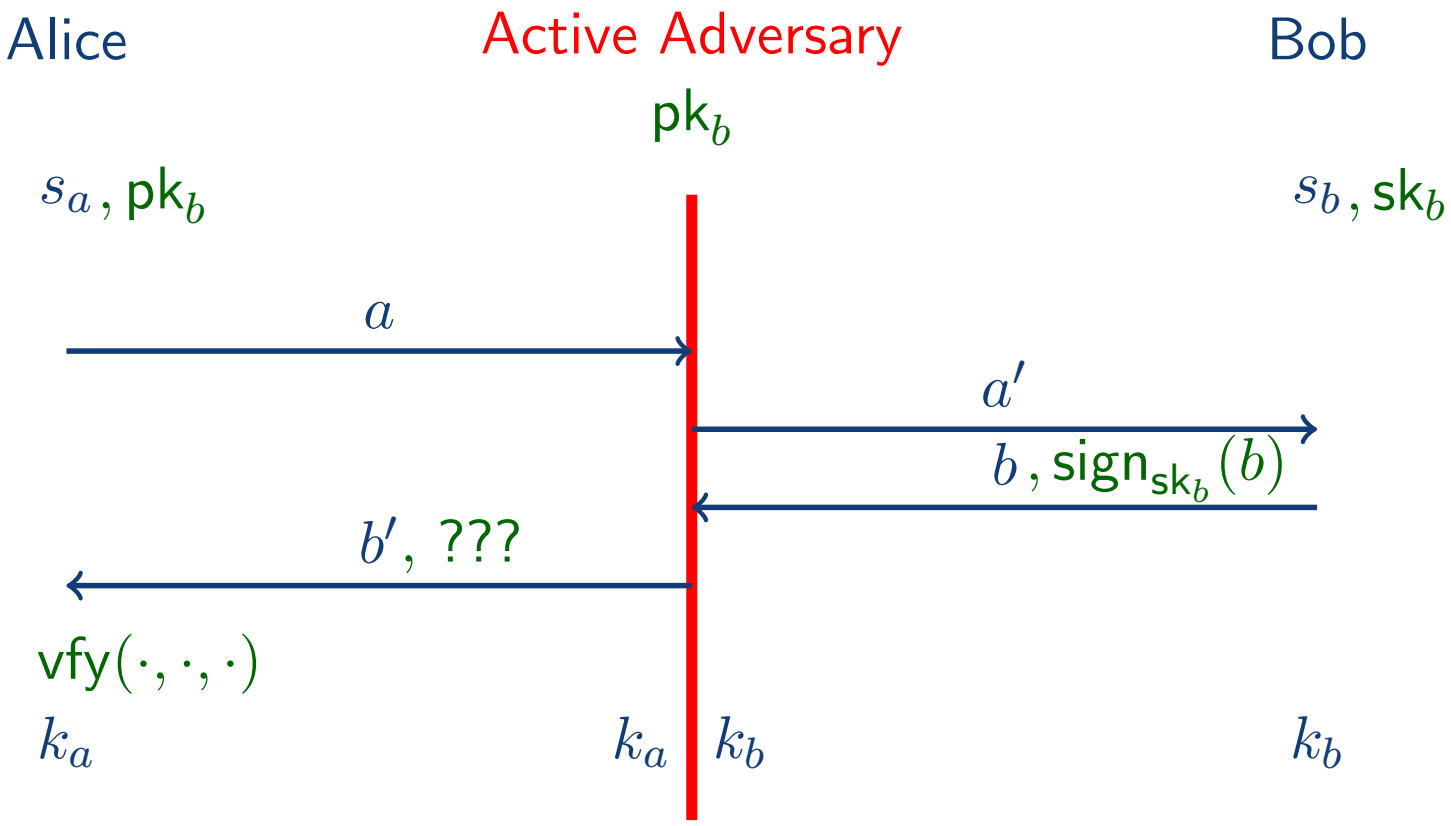
How to kill MitM?

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

Public Key Infrastructure (PKI)

Alice

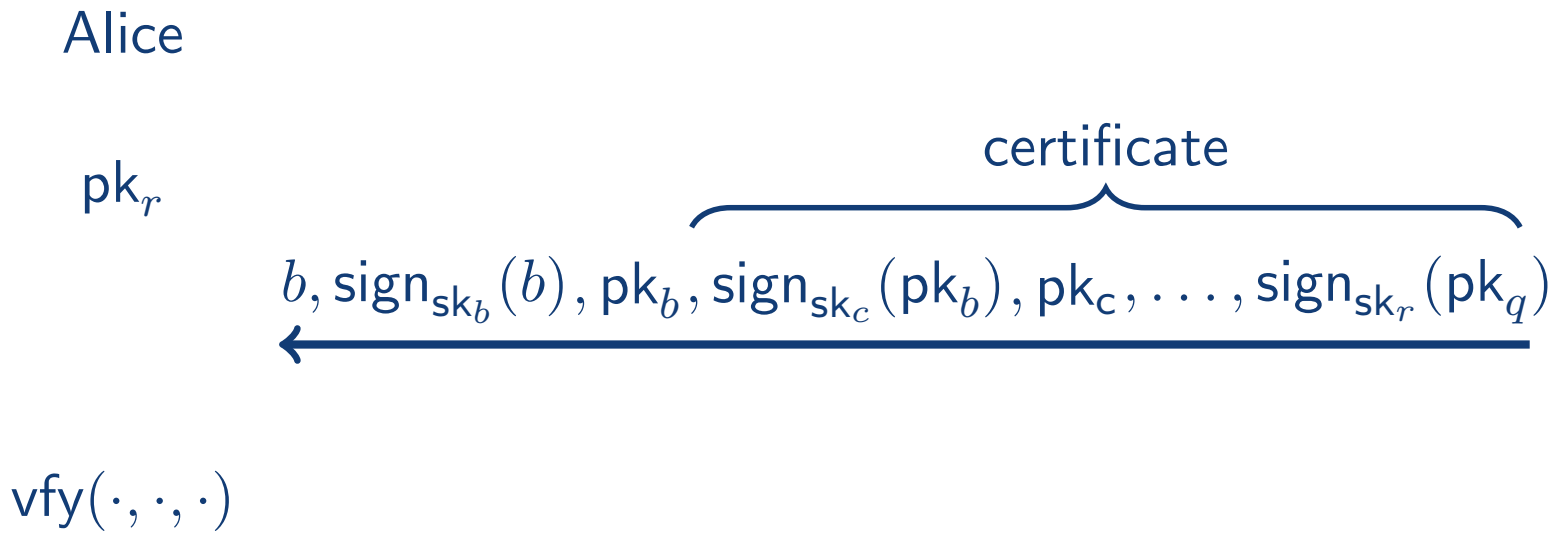
Public Key Infrastructure (PKI)

Alice

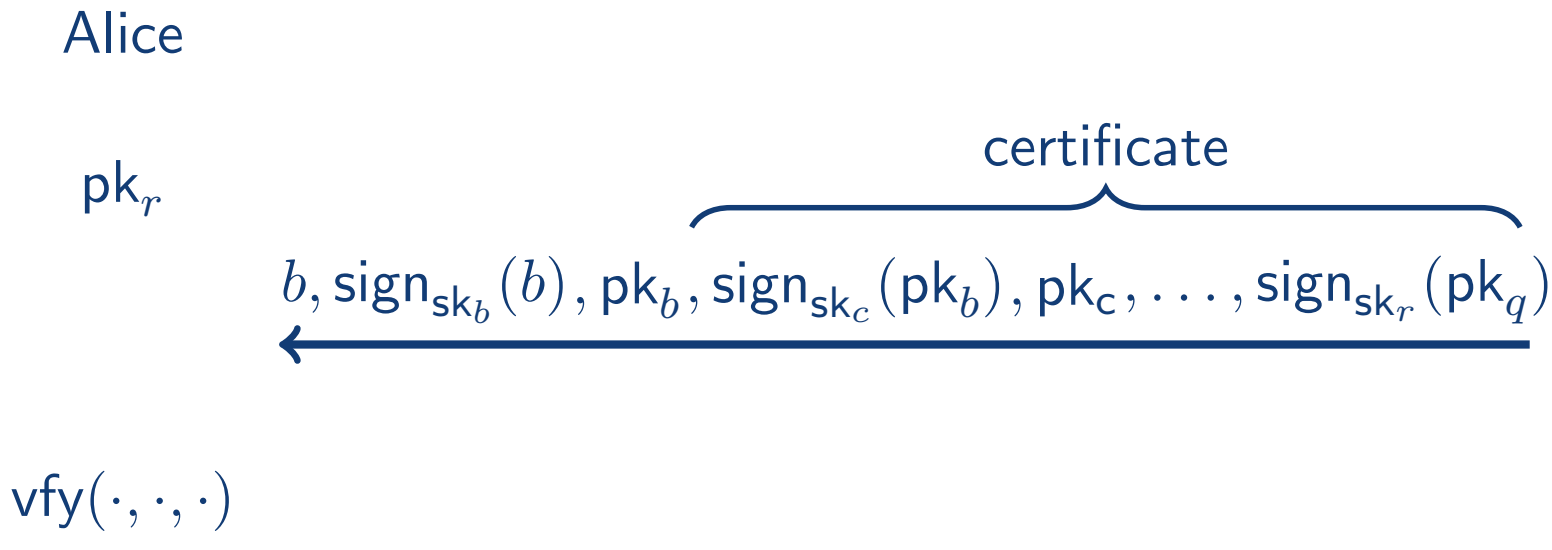
Public Key Infrastructure (PKI)

Alice

Public Key Infrastructure (PKI)



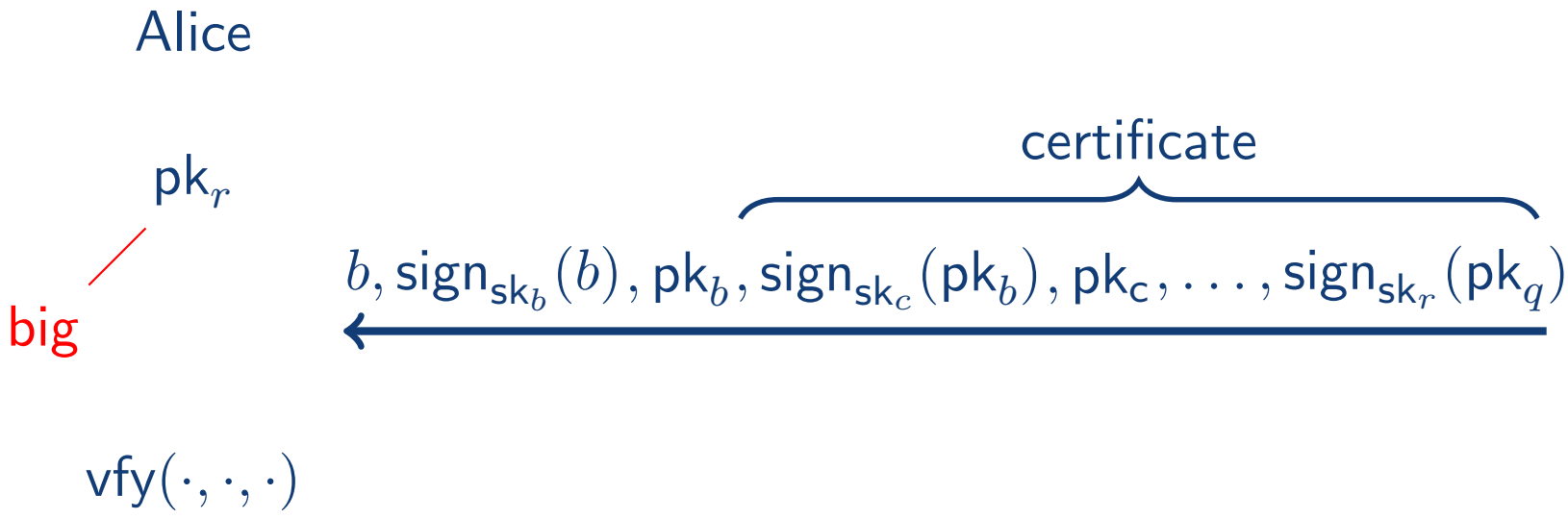
Public Key Infrastructure (PKI)



desirable properties

acceptable drawbacks

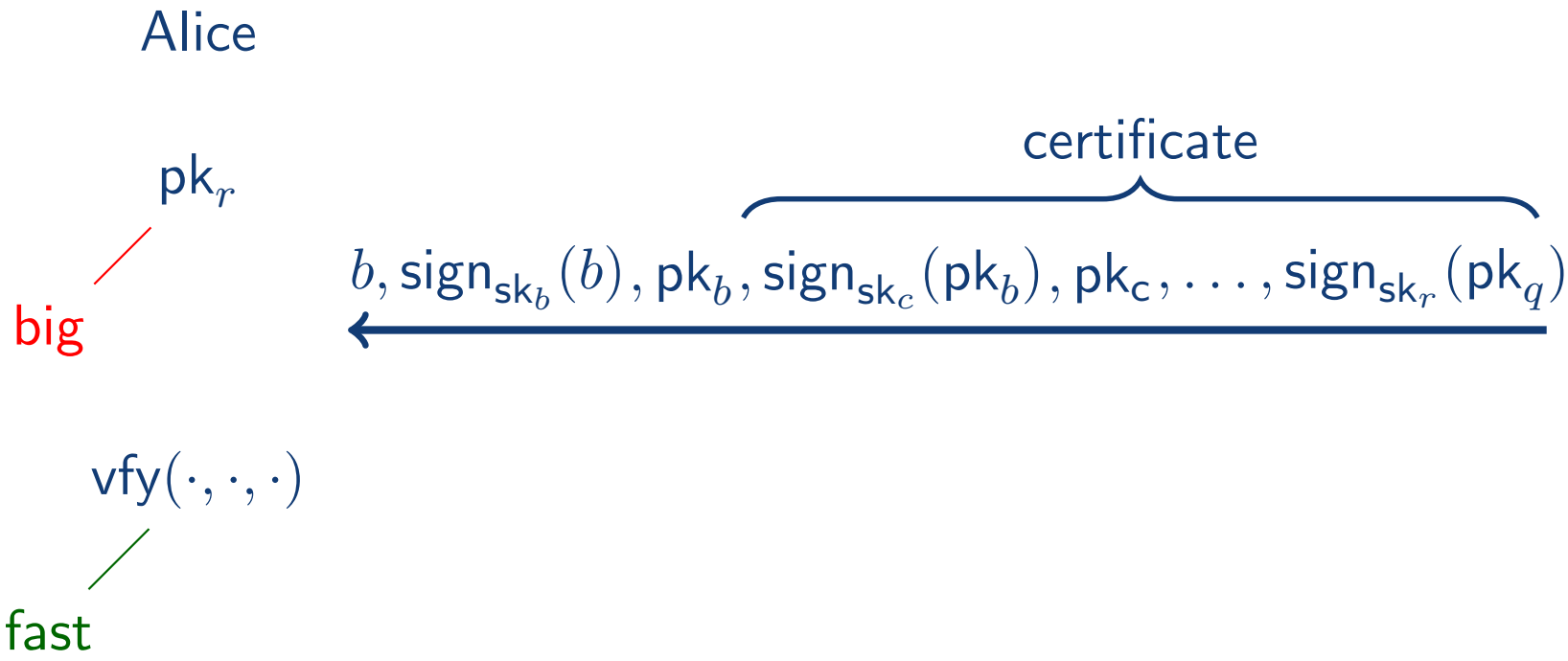
Public Key Infrastructure (PKI)



desirable properties

acceptable drawbacks

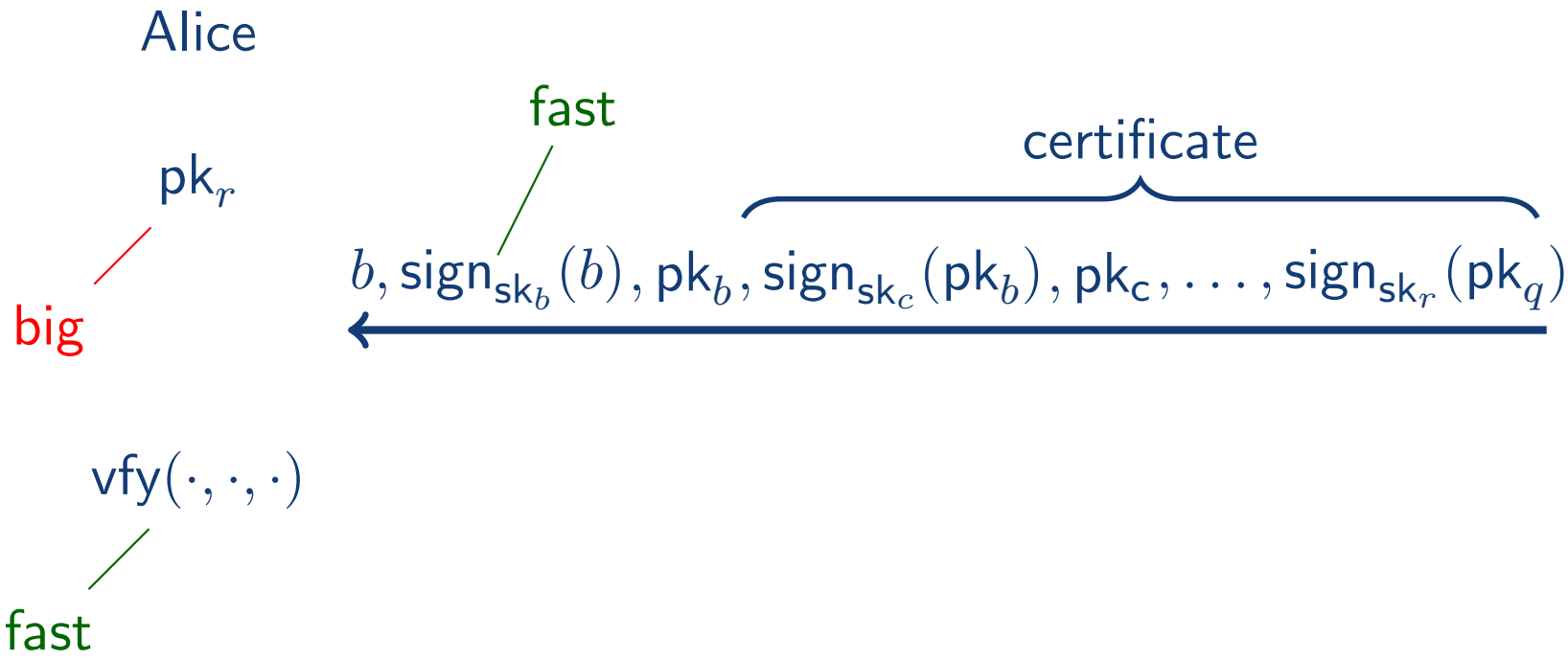
Public Key Infrastructure (PKI)



desirable properties

acceptable drawbacks

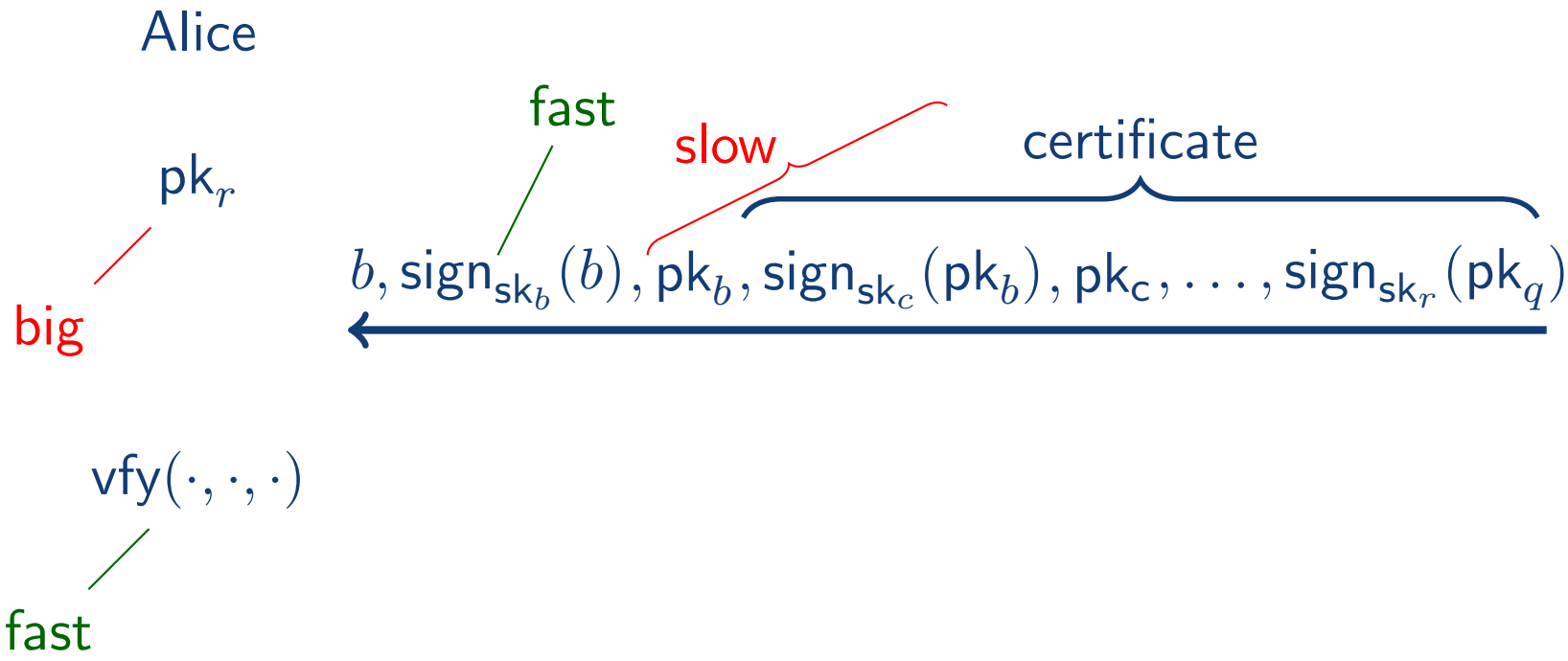
Public Key Infrastructure (PKI)



desirable properties

acceptable drawbacks

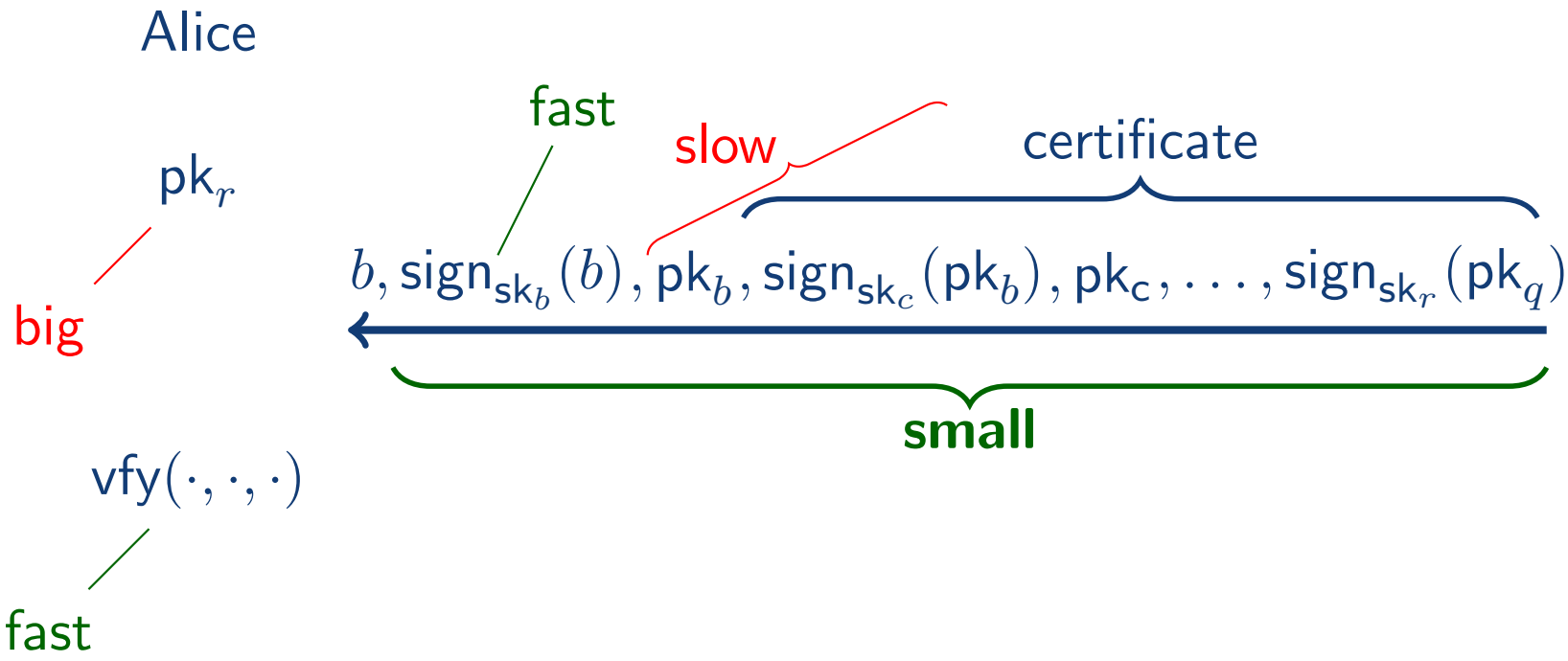
Public Key Infrastructure (PKI)



desirable properties

acceptable drawbacks

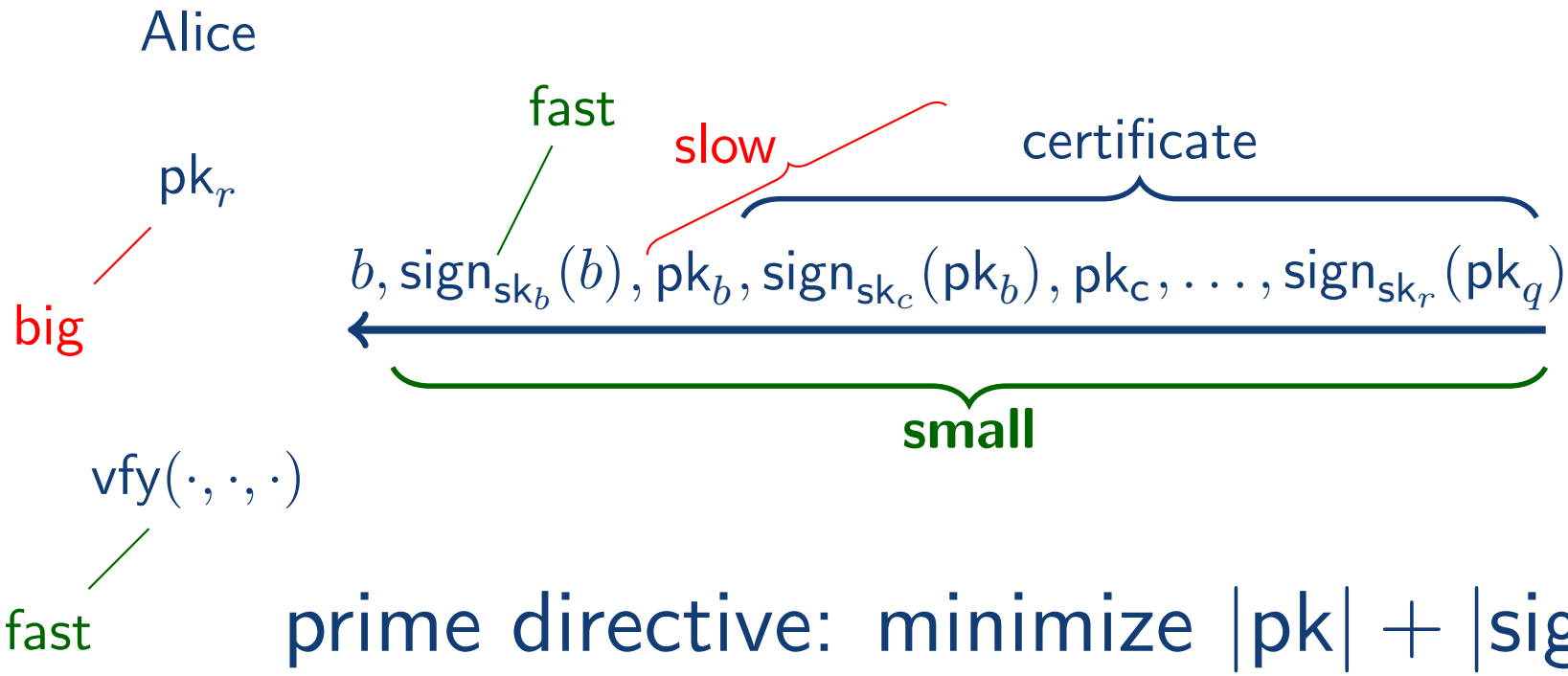
Public Key Infrastructure (PKI)



desirable properties

acceptable drawbacks

Public Key Infrastructure (PKI)

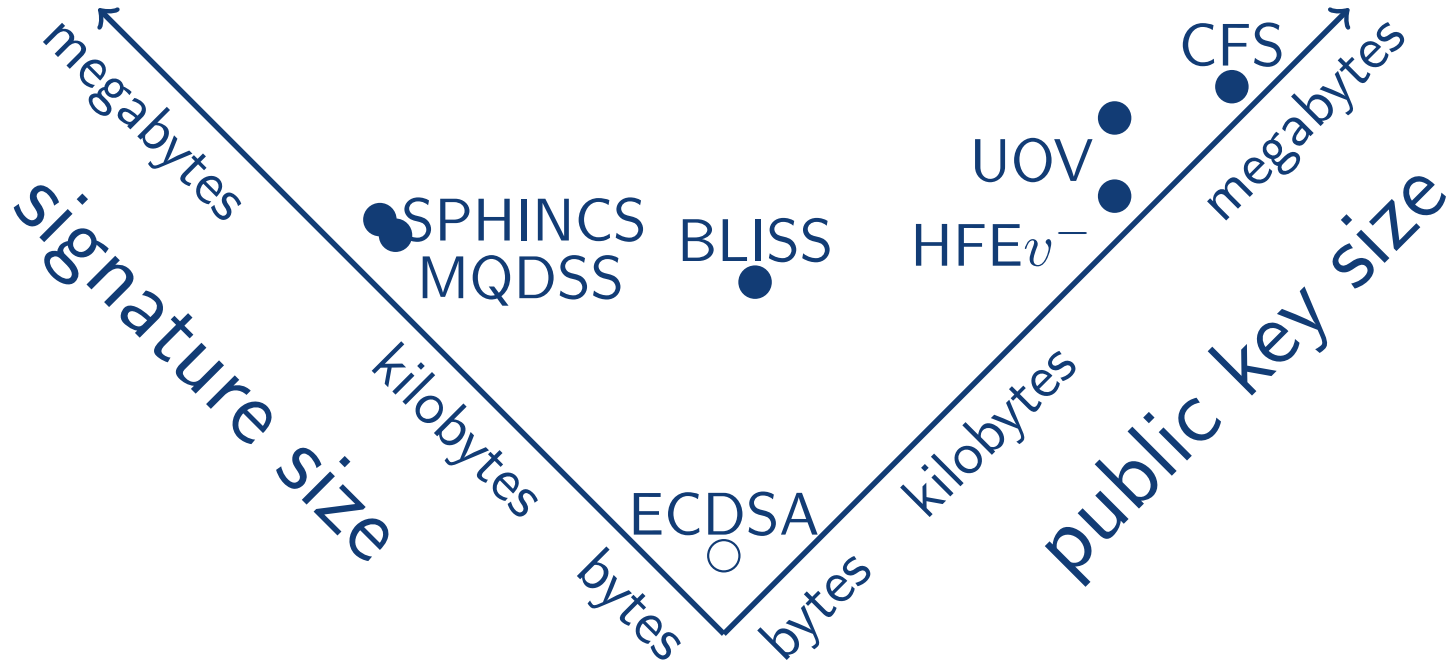


prime directive: minimize $|\mathsf{pk}| + |\mathsf{sig}|$

desirable properties

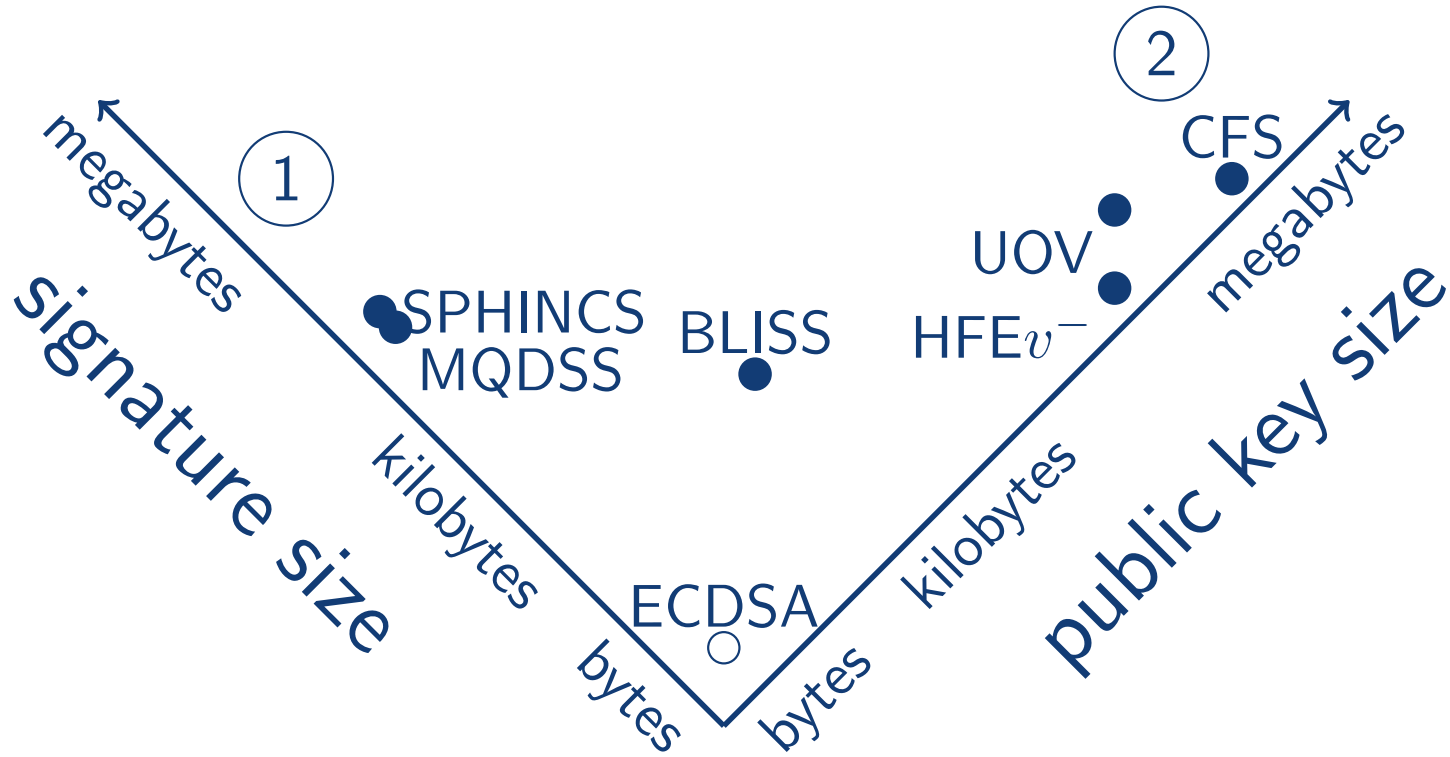
acceptable drawbacks

Post-Quantum Signature Schemes



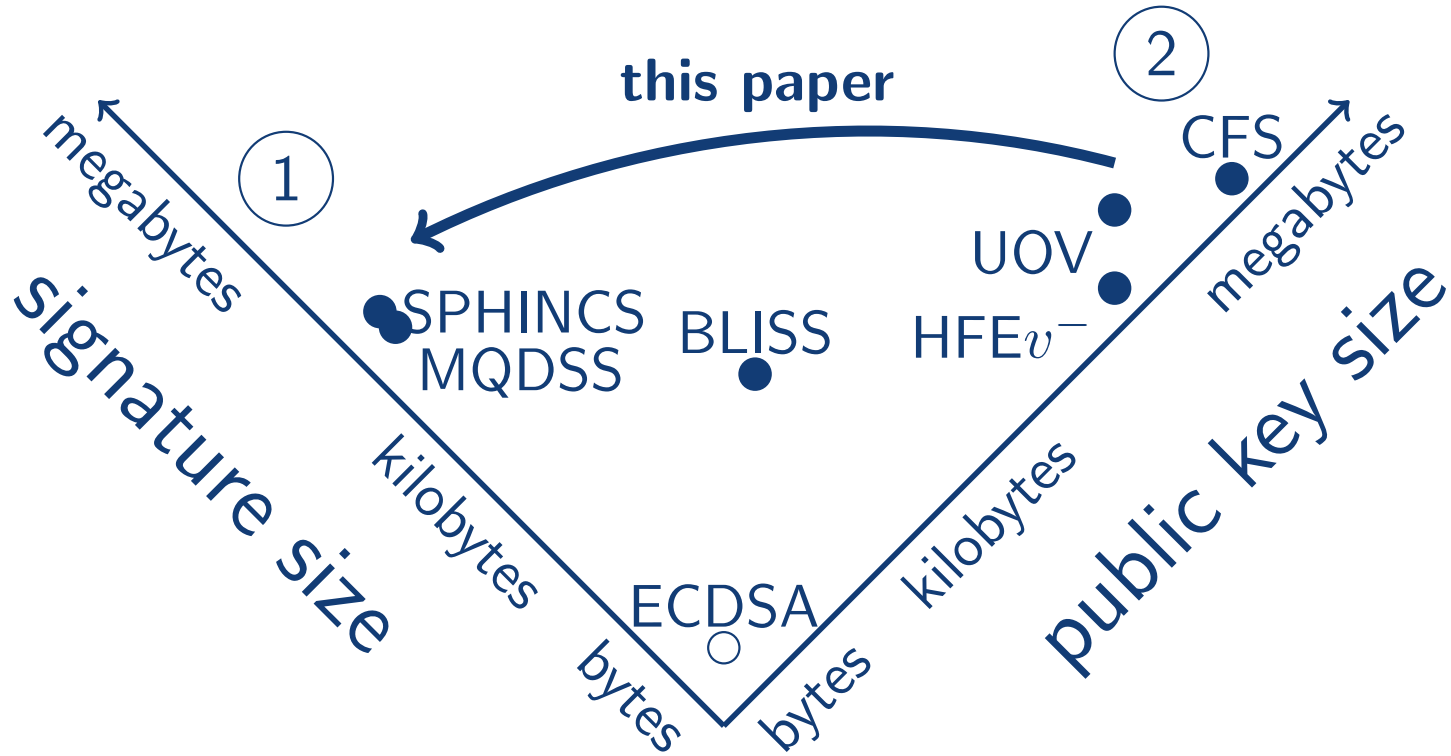
strategy: *transform MQ-signature schemes to shrink* $|\mathsf{pk}| + |\mathsf{s}|$

Post-Quantum Signature Schemes



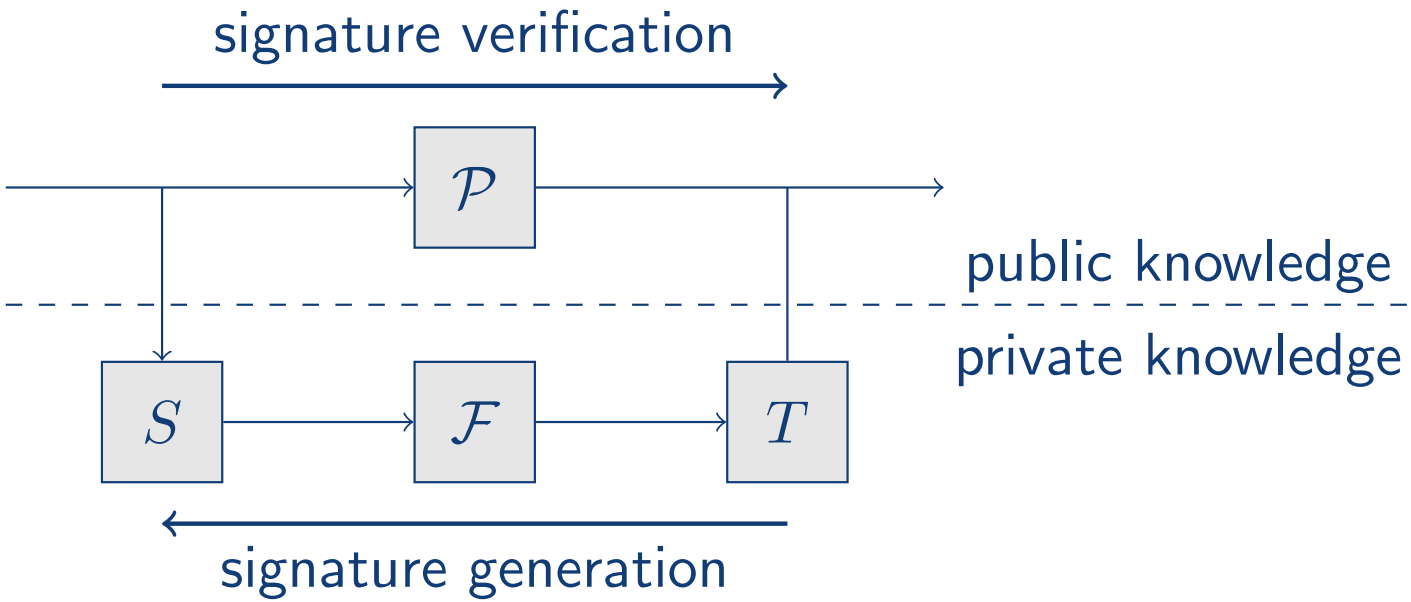
strategy: *transform MQ-signature schemes to shrink* $|\mathsf{pk}| + |\mathsf{s}|$

Post-Quantum Signature Schemes



strategy: *transform MQ-signature schemes to shrink* $|\mathsf{pk}| + |\mathsf{s}|$

MQ Signature Schemes



$\mathcal{P}, \mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ $\qquad$ $\mathbf{s} \in \mathbb{F}_q^n$

$T, S \in \mathsf{GL}(\mathbb{F}_q)$ $\qquad$ $\mathsf{vfy} : \mathcal{P}(\mathbf{s}) \stackrel{?}{=} \mathsf{H}(d)$

Transformation

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

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

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

Transformation

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

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

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

Transformation

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

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

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 $\mathcal{R}(\mathbf{x}), \mathcal{P}(\mathbf{x})$

Transformation

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

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

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 $\mathbf{t}\mathcal{P}(\mathbf{x}) = \mathcal{R}(\mathbf{x})$

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

Transformation

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

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

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 ϑ randomly chosen points

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

Transformation

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

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

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 ϑ randomly chosen points

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

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

Transformation

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

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

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 $\mathbf{t}\mathcal{P}(\mathbf{x}) = \mathcal{R}(\mathbf{x})$

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

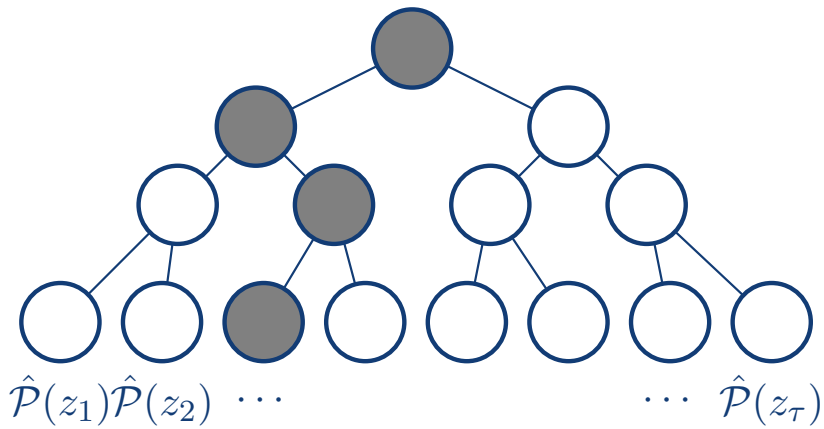
2c. verify $\mathbf{t}\hat{\mathcal{P}}(z_i) = \hat{\mathcal{R}}(z_i)$ in only ϑ randomly chosen points

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

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

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

Merkle Tree


$\hat{\mathcal{P}}(z_1)\hat{\mathcal{P}}(z_2)$ $\cdots$
$\cdots$ $\hat{\mathcal{P}}(z_\tau)$

Provable Security

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

Provable Security

$$
\begin{aligned}
\mathsf{InSec}_{\mathsf{NEW}}^{\mathsf{EUF-CMA}}(t,Q) \leq\ & \mathsf{InSec}_{\mathsf{ORIGINAL}}^{\mathsf{EUF-CMA}}(t+O(Q),Q) && \Big\} \text{ original scheme} \\
+\quad & (2\tau-1)\tfrac{Q+1}{2^{\kappa}} && \Big\} \text{ Merkle tree} \\
+\quad & \left(\tfrac{n(n+1)}{2\tau}\right)^{\vartheta}(Q+1) && \Big\} \text{ MAC polynomials} \\
+\quad & q^{-\alpha}(Q+1) && \Big\} \text{ lucky s}
\end{aligned}
$$

Provable Security

... in the QROM

$$\mathsf{InSec}^{\mathsf{EUF-CMA}}_{\mathsf{NEW}}(t,\hat{Q}) \leq \mathsf{InSec}^{\mathsf{EUF-CMA}}_{\mathsf{ORIGINAL}}(t+O(\hat{Q}),\hat{Q}) \quad \} \text{ original scheme}$$

$$+\Theta\left((2\tau-1)\frac{(\hat{Q}+1)^2}{2^\kappa}\right) \quad \} \text{ Merkle tree}$$

$$+\Theta\left(\left(\frac{n(n+1)}{2\tau}\right)^\vartheta(\hat{Q}+1)^2\right) \quad \} \text{ MAC polynomials}$$

$$+\Theta\left(q^{-\alpha}(\hat{Q}+1)^2\right) \quad \} \text{ lucky s}$$

Example Parameters

scheme	parameters	sec. lvl.	$\lvert\mathsf{pk}\rvert$	$\lvert s\rvert$
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
- $\mathbf{s}_1, \ldots, \mathbf{s}_\sigma$ such that $\mathcal{P}(\mathbf{s}_i) = \mathsf{H}(d\|i)$

Improvement

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

Improvement

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

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

Security Proof Fails

$$\mathsf{InSec}^{\mathsf{EUF-CMA}}_{\mathsf{NEW}}(t,\hat{Q}) \leq \mathsf{InSec}^{\mathsf{EUF-CMA}}_{\mathsf{ORIGINAL}}(t+O(\hat{Q}),\hat{Q})$$ } original scheme

$$+\Theta\left((2\tau-1)\frac{(\hat{Q}+1)^2}{2^\kappa}\right)$$ } Merkle tree

$$+\Theta\left(\left(\frac{n(n+1)}{2\tau}\right)^\vartheta(\hat{Q}+1)^2\right)$$ } MAC polynomials

~~$+\Theta\left(q^{-\sigma\alpha}(\hat{Q}+1)^2\right)$~~ } lucky s

Security Proof Fails

$$\mathsf{InSec}^{\mathsf{EUF-CMA}}_{\mathsf{NEW}}(t,\hat{Q}) \leq \mathsf{InSec}^{\mathsf{EUF-CMA}}_{\mathsf{ORIGINAL}}(t+O(\hat{Q}),\hat{Q})$$ } original scheme

$$+\Theta\left((2\tau-1)\frac{(\hat{Q}+1)^2}{2^\kappa}\right)$$ } Merkle tree

$$+\Theta\left(\left(\frac{n(n+1)}{2\tau}\right)^\vartheta(\hat{Q}+1)^2\right)$$ } MAC polynomials

~~$+\Theta\left(q^{-\sigma\alpha}(\hat{Q}+1)^2\right)$~~ } lucky s

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

Security Proof Fails

$$\mathsf{InSec}^{\mathsf{EUF-CMA}}_{\mathsf{NEW}}(t,\hat{Q}) \leq \mathsf{InSec}^{\mathsf{EUF-CMA}}_{\mathsf{ORIGINAL}}(t+O(\hat{Q}),\hat{Q})$$ } original scheme

$$+\Theta\left((2\tau-1)\frac{(\hat{Q}+1)^2}{2^\kappa}\right)$$ } Merkle tree

$$+\Theta\left(\left(\frac{n(n+1)}{2\tau}\right)^\vartheta(\hat{Q}+1)^2\right)$$ } MAC polynomials

~~$+\Theta\left(q^{-\sigma\alpha}(\hat{Q}+1)^2\right)$~~ } lucky s

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

... but $\mathbf{s}_i$ are not!

Security Proof Fails

$$\mathsf{InSec}^{\mathsf{EUF-CMA}}_{\mathsf{NEW}}(t,\hat{Q}) \not\leq \mathsf{InSec}^{\mathsf{EUF-CMA}}_{\mathsf{ORIGINAL}}(t+O(\hat{Q}),\hat{Q}) \quad \} \text{ original scheme}$$

$$+\Theta\left((2\tau-1)\frac{(\hat{Q}+1)^2}{2^\kappa}\right) \quad \} \text{ Merkle tree}$$

$$+\Theta\left(\left(\frac{n(n+1)}{2\tau}\right)^\vartheta(\hat{Q}+1)^2\right) \quad \} \text{ MAC polynomials}$$

$$+\Theta\left(q^{-\sigma\alpha}(\hat{Q}+1)^2\right) \quad \} \text{ lucky } \mathbf{s}$$

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

... but $\mathbf{s}_i$ are not!

Low-Dim Errors

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

Low-Dim Errors

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

Low-Dim Errors

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

AMQ Problem

Definition

AMQ Problem. (Approximate Multivariate Quadratic)
Given: $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m; \mathbf{y}_1, \ldots, \mathbf{y}_\sigma \in \mathbb{F}_q^m$
Find: $\mathbf{x}_1, \ldots, \mathbf{x}_\sigma \in \mathbb{F}_q^n$
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: $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m; \mathbf{y}_1, \ldots, \mathbf{y}_\sigma \in \mathbb{F}_q^m$
Find: $\mathbf{x}_1, \ldots, \mathbf{x}_\sigma \in \mathbb{F}_q^n$
Such that: $\dim \langle \{\mathcal{P}(\mathbf{x}_i) - \mathbf{y}_i\}_i \rangle \leq r$

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

Example Parameters

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