KU LEUVEN

A Practical Multivariate Blind Signature Scheme

April 2017

Albrecht Petzoldt, **Alan Szepieniec**,
Mohamed Saied Emam Mohamed

1. Blind Signatures
2. MQ Signatures
   - Rainbow
   - MQDSS
3. Multivariate Blind Signature Scheme
   - Scheme
   - Numbers

Blind Signature

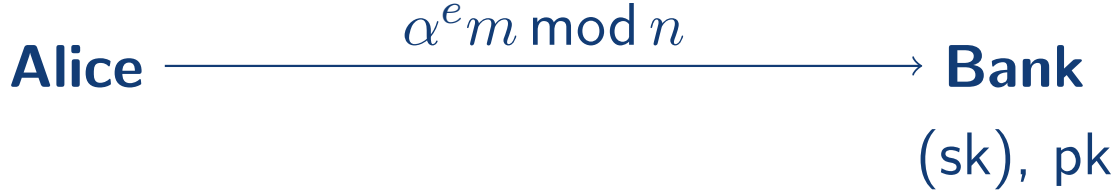
Alice

Bank

(sk), pk

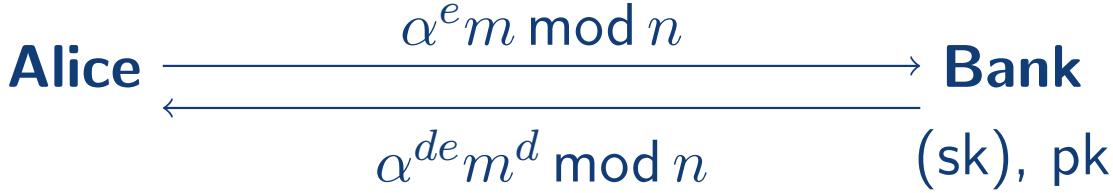
Merchant

Blind Signature



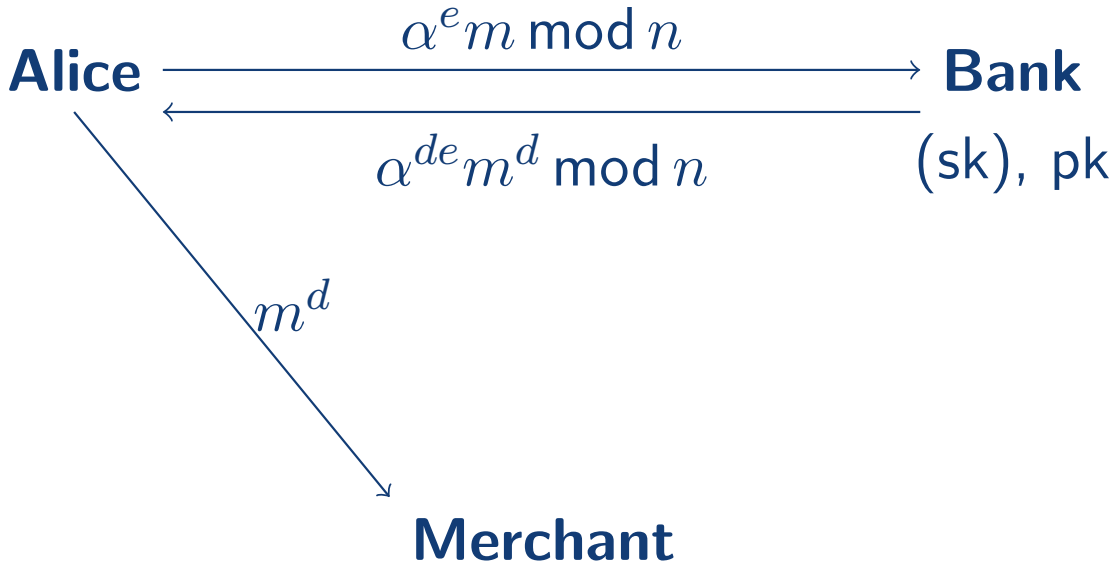
Merchant

Blind Signature

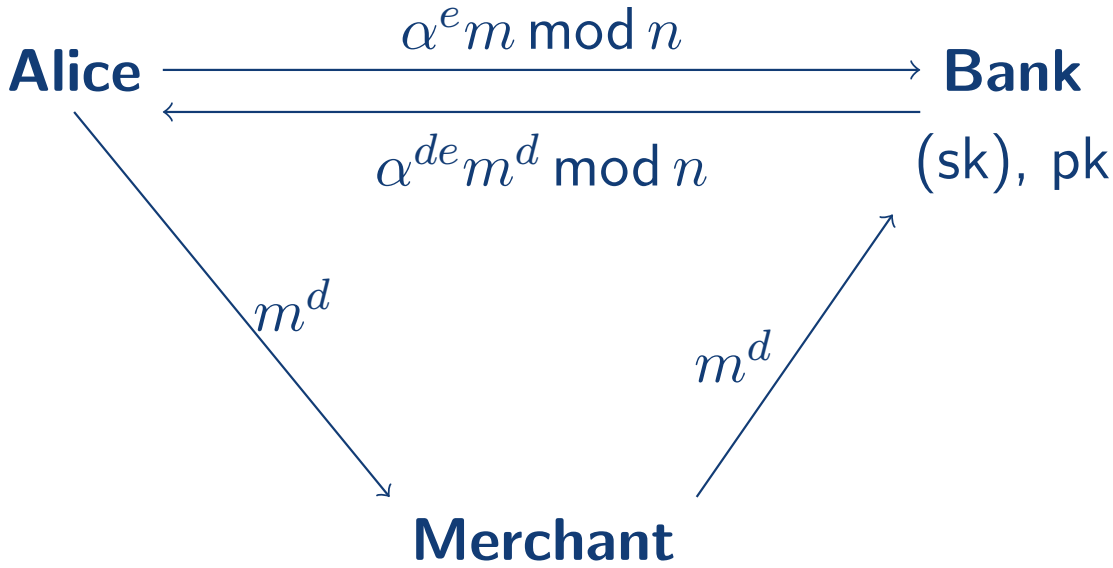


Merchant

Blind Signature

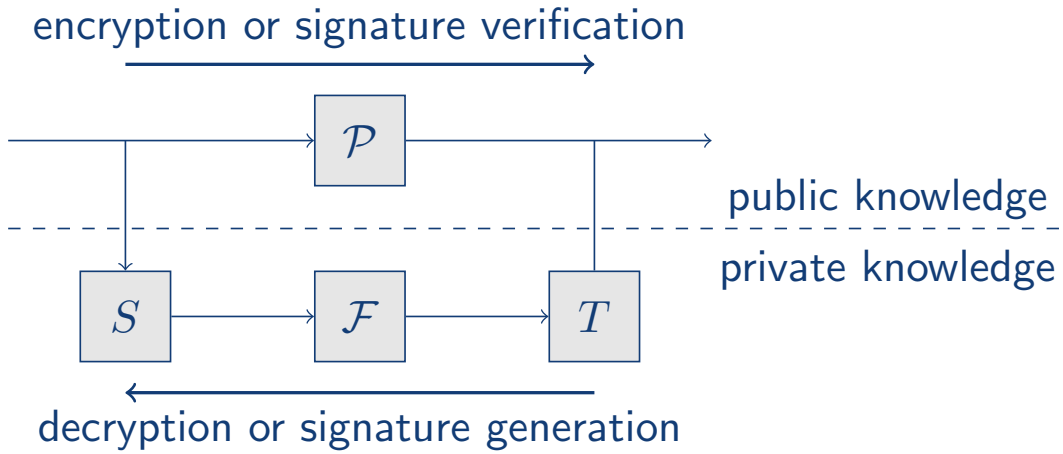


Blind Signature



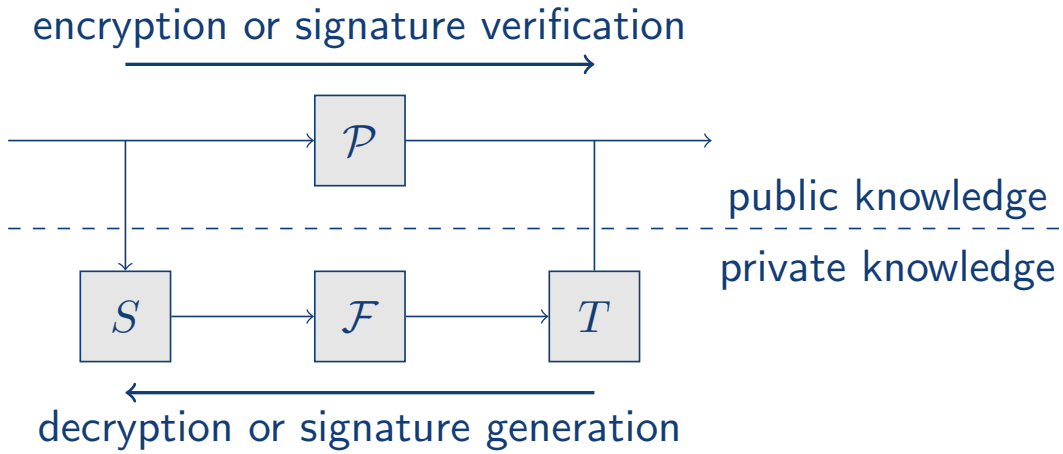
MQ Signature Scheme

- EIP-based
  - HFEv-, UOV, **Rainbow**
  - $\mathcal{P} = T \circ \mathcal{F} \circ S$
  - verify $\mathbf{s}$: $\mathcal{P}(\mathbf{s}) \stackrel{?}{=} \mathcal{H}(m)$



MQ Signature Scheme

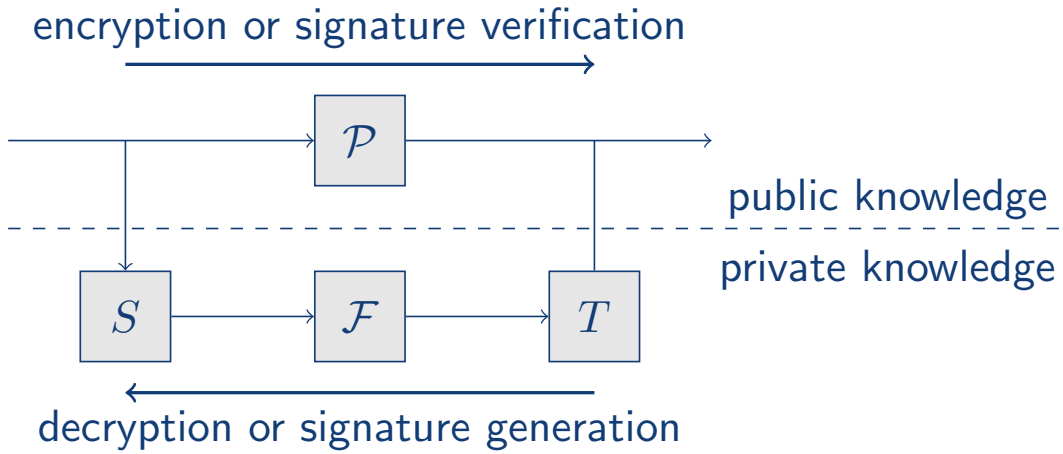
- EIP-based
  - HFEv-, UOV, **Rainbow**
  - $\mathcal{P} = T \circ \mathcal{F} \circ S$
  - verify $\mathbf{s}$: $\mathcal{P}(\mathbf{s}) \stackrel{?}{=} \mathcal{H}(m)$



- ZKPoK-based
  - SSH (crypto'11), **MQDSS** (asiacrypt'16)
  - verify NIZKPoK$\{(\mathbf{x}) : \mathcal{P}(\mathbf{x}) = \mathbf{y}\}$

MQ Signature Scheme

- EIP-based
  - HFEv-, UOV, **Rainbow**
  - $\mathcal{P} = T \circ \mathcal{F} \circ S$
  - verify $\mathbf{s}$: $\mathcal{P}(\mathbf{s}) \stackrel{?}{=} \mathcal{H}(m)$



- ZKPoK-based
  - SSH (crypto'11), **MQDSS** (asiacrypt'16)
  - verify NIZKPoK$\{(\mathbf{x}) : \mathcal{P}(\mathbf{x}) = \mathbf{y}\}$

- Blind Signature: EIP + ZKPoK

UOV

- Unbalanced Oil and Vinegar: precursor to Rainbow
- v *vinegar* variables and o *oil* variables ($v \approx 2o$)
- vinegar mixes with anything; oil never mixes with oil

UOV

- Unbalanced Oil and Vinegar: precursor to Rainbow
- v *vinegar* variables and o *oil* variables ($v \approx 2o$)
- vinegar mixes with anything; oil never mixes with oil
- $\mathcal{F}, \mathcal{P} : \mathbb{F}_q^{v+o} \to \mathbb{F}_q^o$ with $\mathcal{P} = \mathcal{F} \circ S$
- $f_i(\mathbf{x}) = f_i(\mathbf{x}_v; \mathbf{x}_o) = (\mathbf{x}_v^\mathsf{T}, \mathbf{x}_o^\mathsf{T}) \begin{pmatrix} \blacksquare & \blacksquare \\ \blacksquare & \end{pmatrix} \begin{pmatrix} \mathbf{x}_v \\ \mathbf{x}_o \end{pmatrix}, \quad i = 1, \ldots, o$

UOV

- Unbalanced Oil and Vinegar: precursor to Rainbow
- v *vinegar* variables and o *oil* variables ($v \approx 2o$)
- vinegar mixes with anything; oil never mixes with oil
- $\mathcal{F}, \mathcal{P} : \mathbb{F}_q^{v+o} \to \mathbb{F}_q^o$ with $\mathcal{P} = \mathcal{F} \circ S$
- $f_i(\mathbf{x}) = f_i(\mathbf{x}_v; \mathbf{x}_o) = (\mathbf{x}_v^\mathsf{T}, \mathbf{x}_o^\mathsf{T}) \begin{pmatrix} \blacksquare & \blacksquare \\ \blacksquare & \end{pmatrix} \begin{pmatrix} \mathbf{x}_v \\ \mathbf{x}_o \end{pmatrix}, \quad i = 1, \ldots, o$
- signature generation:
  - choose $\mathbf{x}_v \xleftarrow{\$} \mathbb{F}_q^v$
  - solve linear system to obtain $\mathbf{x}_o$ (#eqns = #vars = o)
  - invert linear transformation S

Rainbow

- two layers of UOV

Rainbow

- two layers of UOV
- partition $\mathbf{x}^{\mathsf{T}} = (\mathbf{x}_v^{\mathsf{T}}, \mathbf{x}_{o_1}^{\mathsf{T}}, \mathbf{x}_{o_2}^{\mathsf{T}})$

Rainbow

- two layers of UOV
- partition $\mathbf{x}^\mathsf{T} = (\mathbf{x}_v^\mathsf{T}, \mathbf{x}_{o_1}^\mathsf{T}, \mathbf{x}_{o_2}^\mathsf{T})$
- $\mathcal{P}, \mathcal{F} : \mathbb{F}_q^{v+o_1+o_2} \to \mathbb{F}_q^{o_1+o_2}$ with $\mathcal{P} = T \circ \mathcal{F} \circ S$
- $f_i(\mathbf{x}) = (\mathbf{x}_v^\mathsf{T}, \mathbf{x}_{o_1}^\mathsf{T}, \mathbf{x}_{o_2}^\mathsf{T})$  $\begin{pmatrix} \mathbf{x}_v \\ \mathbf{x}_{o_1} \\ \mathbf{x}_{o_2} \end{pmatrix}$, $\quad i = 1, \ldots, o_1$
- $f_i(\mathbf{x}) = (\mathbf{x}_v^\mathsf{T}, \mathbf{x}_{o_1}^\mathsf{T}, \mathbf{x}_{o_2}^\mathsf{T})$  $\begin{pmatrix} \mathbf{x}_v \\ \mathbf{x}_{o_1} \\ \mathbf{x}_{o_2} \end{pmatrix}$, $\quad i = o_1 + 1, \ldots, o_1 + o_2$

Rainbow

- two layers of UOV
- partition $\mathbf{x}^\mathsf{T} = (\mathbf{x}_v^\mathsf{T}, \mathbf{x}_{o_1}^\mathsf{T}, \mathbf{x}_{o_2}^\mathsf{T})$
- $\mathcal{P}, \mathcal{F} : \mathbb{F}_q^{v+o_1+o_2} \to \mathbb{F}_q^{o_1+o_2}$ with $\mathcal{P} = T \circ \mathcal{F} \circ S$
- $f_i(\mathbf{x}) = (\mathbf{x}_v^\mathsf{T}, \mathbf{x}_{o_1}^\mathsf{T}, \mathbf{x}_{o_2}^\mathsf{T})$  $\begin{pmatrix} \mathbf{x}_v \\ \mathbf{x}_{o_1} \\ \mathbf{x}_{o_2} \end{pmatrix}$, $\quad i = 1, \ldots, o_1$
- $f_i(\mathbf{x}) = (\mathbf{x}_v^\mathsf{T}, \mathbf{x}_{o_1}^\mathsf{T}, \mathbf{x}_{o_2}^\mathsf{T})$  $\begin{pmatrix} \mathbf{x}_v \\ \mathbf{x}_{o_1} \\ \mathbf{x}_{o_2} \end{pmatrix}$, $\quad i = o_1 + 1, \ldots, o_1 + o_2$
- signature generation:
  - invert linear transformation T
  - choose $\mathbf{x}_v \xleftarrow{\$} \mathbb{F}_q^v$
  - solve o_1 linear equations to obtain $\mathbf{x}_{o_1}$
  - treat $(\mathbf{x}_v; \mathbf{x}_{o_1})$ as vinegar variables
  - solve o_2 linear equations to obtain $\mathbf{x}_{o_2}$
  - invert linear transformation S

SSH Protocol

- ZKPoK$\{(\mathbf{s}) : \mathcal{P}(\mathbf{s}) = \mathbf{v}\}$
- uses *polar form*: $\mathcal{G}(\mathbf{x}, \mathbf{y}) = \mathcal{P}(\mathbf{x} + \mathbf{y}) - \mathcal{P}(\mathbf{x}) - \mathcal{P}(\mathbf{y}) + \mathcal{P}(\mathbf{0})$

Prover: $\mathcal{P}, \mathbf{s}, \mathbf{v}$		Verifier: $\mathcal{P}, \mathbf{v}$
$\mathbf{r}_0, \mathbf{t}_0 \xleftarrow{\$} \mathbb{F}_q^n; \mathbf{e}_0 \xleftarrow{\$} \mathbb{F}_q^m; \mathbf{r}_1 \leftarrow \mathbf{s} - \mathbf{r}_0$		
$c_0 = Com(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0)$		
$c_1 = Com(\mathbf{r}_1, \mathcal{G}(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0)$		
	$\xrightarrow{c_0, c_1}$	
	$\xleftarrow{\alpha}$	$\alpha \xleftarrow{\$} \mathbb{F}_q$
$\mathbf{t}_1 \leftarrow \alpha\mathbf{r}_0 - \mathbf{t}_0$		
$\mathbf{e}_1 \leftarrow \alpha\mathcal{P}(\mathbf{r}_0) - \mathbf{e}_0$		
	$\xrightarrow{\mathbf{t}_1, \mathbf{e}_1}$	
	$\xleftarrow{ch}$	$ch \xleftarrow{\$} \{0, 1\}$
	$\xrightarrow{\mathbf{r}_{ch}}$	
		$ch = 0 \rightarrow c_0 \stackrel{?}{=} Com(\cdot)$
		$ch = 1 \rightarrow c_1 \stackrel{?}{=} Com(\cdot)$

MQDSS

- turns SSH protocol into signature scheme
- non-interactive using Fiat-Shamir (sort of)
- optimization for speed and size
- 2.43 ms for signature generation (256 bits security)

Blind Signature Scheme: General Idea

dedicated signature scheme

$+$ basic algebraic properties

$+$ zero-knowledge proof

---

blind signature scheme

Blind Signature Scheme: General Idea

dedicated signature scheme

$+$ basic algebraic properties

$+$ zero-knowledge proof

---

blind signature scheme

Multivariate Blind Signature

Alice

Bank

$(\mathsf{sk} = (T, \mathcal{F}, S))$

$\mathsf{pk} = (\mathcal{P}, \mathcal{R})$

Merchant

$$\mathsf{NIZKPoK}\{(\mathbf{z}, \mathbf{z}^*) \ : \ \mathcal{P}(\mathbf{z}^*) + \mathcal{R}(\mathbf{z}) = \mathcal{H}(m)\}$$

Multivariate Blind Signature

$\mathbf{z} \xleftarrow{\$} \mathbb{F}_q^n$

$\mathbf{w}^* = \mathcal{H}(m) - \mathcal{R}(\mathbf{z})$

Alice

Bank

$(\mathsf{sk} = (T, \mathcal{F}, S))$

$\mathsf{pk} = (\mathcal{P}, \mathcal{R})$

Merchant

$$\mathsf{NIZKPoK}\{(\mathbf{z}, \mathbf{z}^*) \ : \ \mathcal{P}(\mathbf{z}^*) + \mathcal{R}(\mathbf{z}) = \mathcal{H}(m)\}$$

Multivariate Blind Signature

$\mathbf{z} \xleftarrow{\$} \mathbb{F}_q^n$

$\mathbf{w}^* = \mathcal{H}(m) - \mathcal{R}(\mathbf{z})$

Alice $\xrightarrow{\quad \mathbf{w}^* \quad}$ **Bank**

$\mathbf{z}^*$ st. $\mathcal{P}(\mathbf{z}^*) = \mathbf{w}^*$ $\xleftarrow{\quad}$

$(\mathsf{sk} = (\mathcal{T}, \mathcal{F}, \mathcal{S}))$

$\mathsf{pk} = (\mathcal{P}, \mathcal{R})$

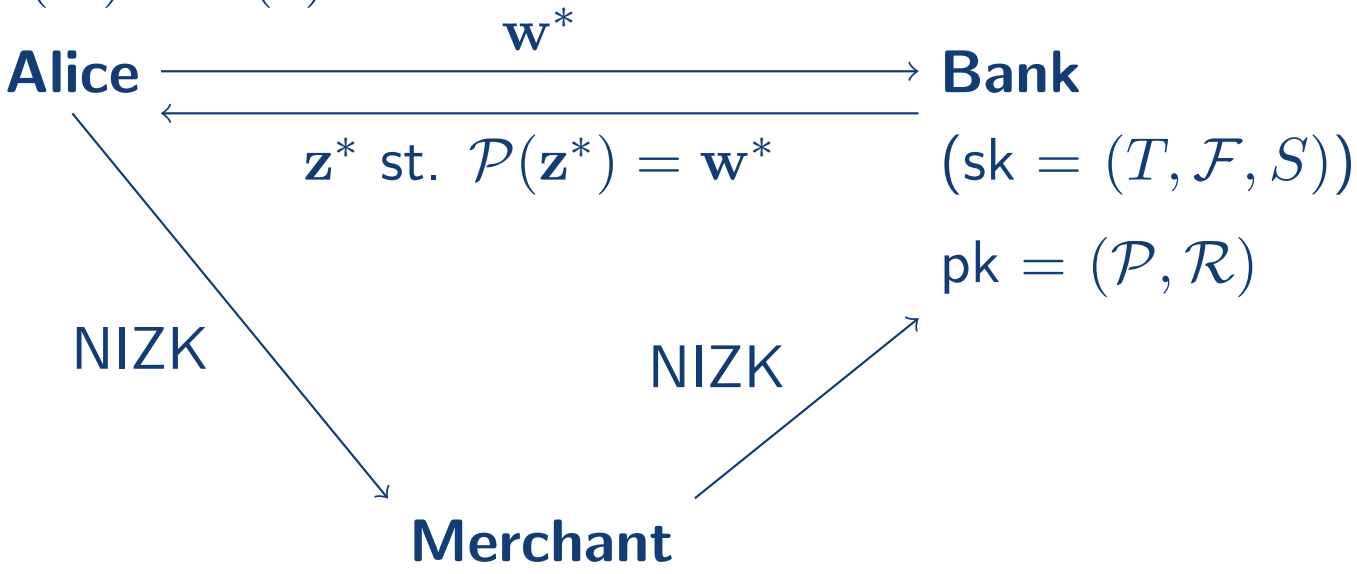
Merchant

$$\mathsf{NIZKPoK}\{(\mathbf{z}, \mathbf{z}^*) \ : \ \mathcal{P}(\mathbf{z}^*) + \mathcal{R}(\mathbf{z}) = \mathcal{H}(m)\}$$

Multivariate Blind Signature

$\mathbf{z} \xleftarrow{\$} \mathbb{F}_q^n$

$\mathbf{w}^* = \mathcal{H}(m) - \mathcal{R}(\mathbf{z})$



NIZKPoK$\{(\mathbf{z}, \mathbf{z}^*) \ : \ \mathcal{P}(\mathbf{z}^*) + \mathcal{R}(\mathbf{z}) = \mathcal{H}(m)\}$

Security Quirks

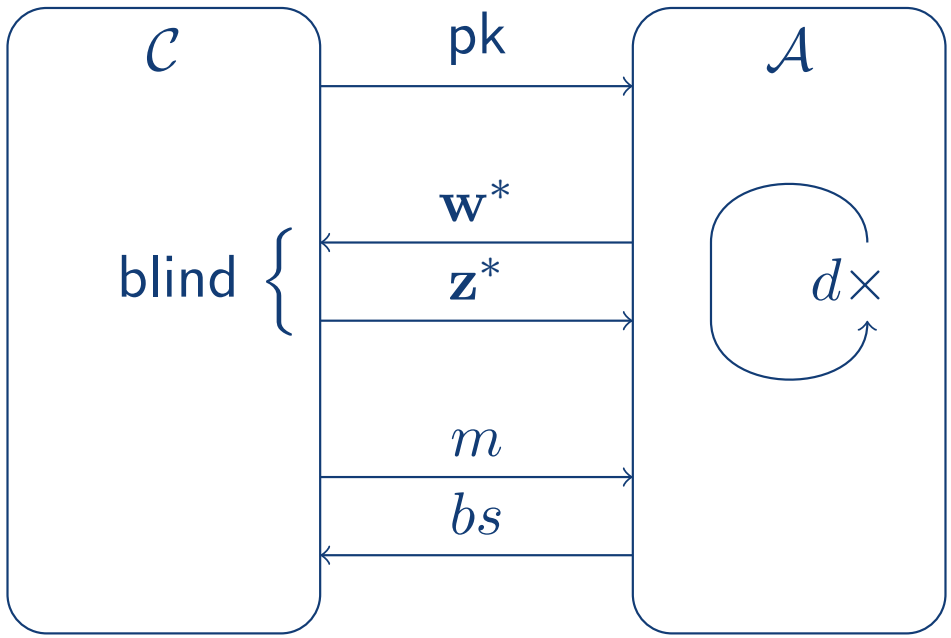
- need *perfectly hiding* commitments for blindness

Security Quirks

- need *perfectly hiding* commitments for blindness
- *classical* random oracle model

Security Quirks

- need *perfectly hiding* commitments for blindness
- *classical* random oracle model
- *universal* one-more unforgeability
  - generalization of UUF-CMA to one-more-unforgeability



parameters, comparison

security level (bit)	parameters $(\mathbb{F}, (v_1, o_1, o_2))$	# rounds	public key size (kB)	private key size (kB)	blind sig. size (kB)
80	(GF(31),(16,18,17))	84	29.4	20.1	11.5
100	(GF(31),(20,22,21))	105	54.6	36.6	17.6
128	(GF(31),(25,27,27))	135	106.8	70.2	28.5
192	(GF(31),(37,35,35))	202	342.8	219.0	63.2
256	(GF(31),(50,53,53))	269	802.4	507.1	111.9

Table: Proposed parameters for our blind signature scheme (GF(31)).

Security lvl. (bit)	Scheme	comm.	Pub. key size (kB)	Sig. size (kB)	Post-quantum?
76	RSA-1229	2	1.2	1.2	×
	Lattice-1024	4	10.2	66.9	✓
	Our scheme	2	29.4	11.5	✓
102	RSA-3313	2	3.3	3.3	×
	Lattice-2048	4	23.6	89.4	✓
	Our scheme	2	54.6	17.6	✓

Table: Comparison of blind signature schemes — RSA / Rückert / ours

Sage implementation

sec. lvl.	Key Gen.	Sign (`Signer`)	Sig. Gen. (`User`)	Sig. Verification
80	4,007	7	2,018	1,424
100	9,392	13	3,649	2,656
128	25,517	19	7,760	5,505
192	87,073	41	23,692	16,040
256	613,968	103	86,540	59,669

Table: Operational speed (milliseconds)