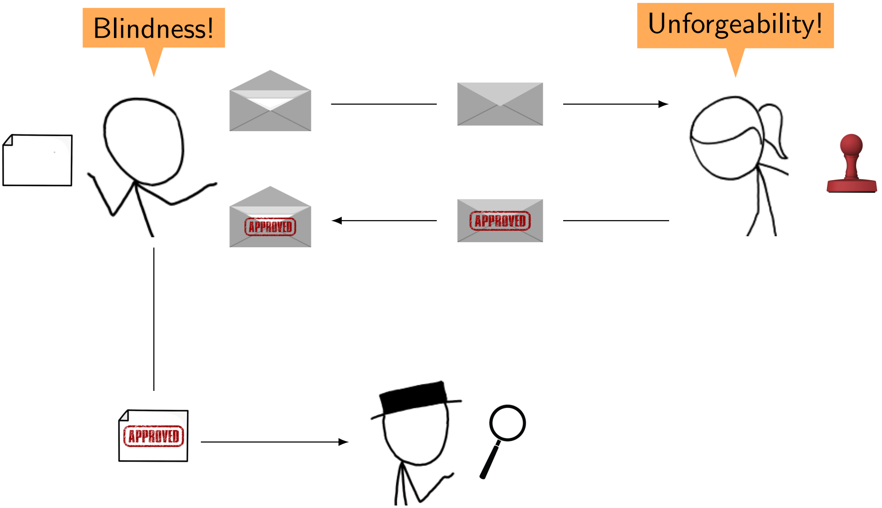
Practical Round-Optimal Blind Signatures in the Standard Model from Weaker Assumptions

G. Fuchsbauer[*], C. Hanser[†] C. Kamath[‡], and D. Slamanig[†]

[*]École Normale Supérieure, Paris
[†]IAIK, Graz University of Technology, Austria
[‡]Institute of Science and Technology Austria

September 2, 2016

Blind Signatures



xkcd.com

Overview

- Desiderata:
  1. Round-optimality (hence efficiency and composability)
  2. No heuristic assumptions
  3. No set-up assumptions

- Hard to construct: [FS10]
- Possibility: [GG14,GRS+11]

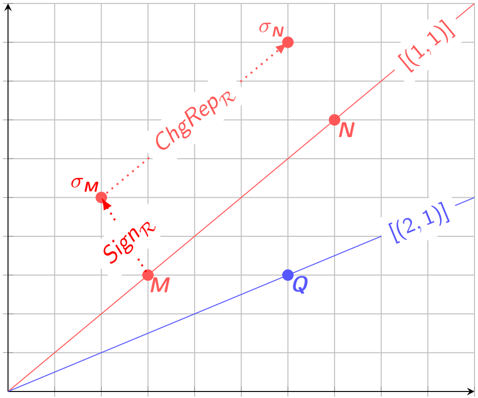
- First practical scheme: [FHS15]
  - SPS-EQ + commitments
  - ~~CDH~~, EUF-CMA $\implies$ Unforgeability
  - ~~Interactive~~ variant of DDH $\implies$ Blindness

- *Our contribution:* weaker assumptions!

Preliminaries

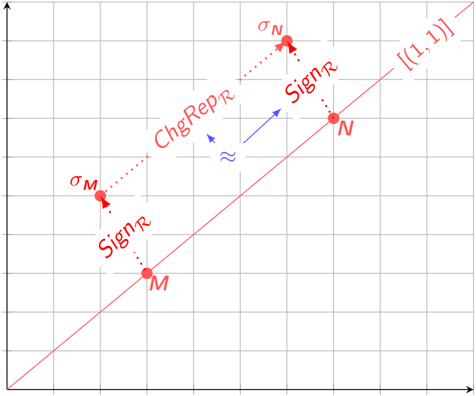
- Asymmetric pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$
  - **Bilinearity**: $e(aP, b\hat{P}) = e(P, \hat{P})^{ab}$
  - **Non-degeneracy**: $e(P, \hat{P}) \neq 1_{\mathbb{G}_T}$
  - **Efficiency**: $e(\cdot, \cdot)$ efficiently computable
- Structure-Preserving Signatures [AFG+10]
  - Signing vector of group elements
  - Signatures and PKs consist *only* of group elements
  - Verification via
    1. pairing-product equations
    2. group membership tests

SPS on Equivalence Classes



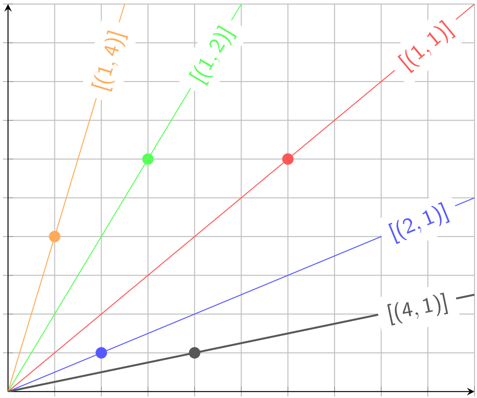
- Equivalence relation $\sim_{\mathcal{R}}$ on $\mathbb{G}^{\ell}$: $\boldsymbol{M} \sim_{\mathcal{R}} \boldsymbol{N} \Leftrightarrow \exists \mu \in \mathbb{Z}_p^* : \boldsymbol{N} = \mu \cdot \boldsymbol{M}$
- SPS-EQ := SPS + "change representative" functionality

SPS-EQ: Security



- Class-hiding: $ChgRep_{\mathcal{R}}(\boldsymbol{M}, \sigma, \mu, \mathtt{pk}) \approx Sign_{\mathcal{R}}(\mu\boldsymbol{M}, \mathtt{sk})$
  - Malicious keys: $ChgRep_{\mathcal{R}}(\boldsymbol{M}, \sigma, \mu, \mathtt{pk})$ uniform in space of signatures on $\mu\boldsymbol{M}$

SPS-EQ: Security

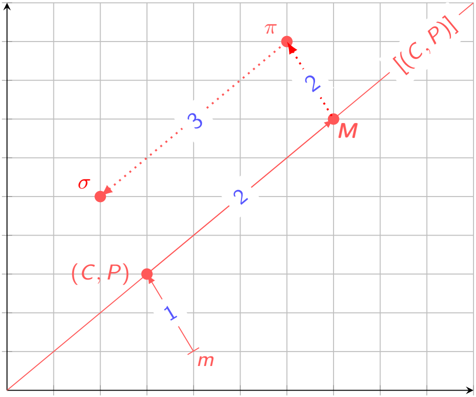


- Class-hiding: $\mathit{ChgRep}_{\mathcal{R}}(\boldsymbol{M}, \sigma, \mu, \mathtt{pk}) \approx \mathit{Sign}_{\mathcal{R}}(\mu \boldsymbol{M}, \mathtt{sk})$
  - Malicious keys: $\mathit{ChgRep}_{\mathcal{R}}(\boldsymbol{M}, \sigma, \mu, \mathtt{pk})$ uniform in space of signatures on $\mu \boldsymbol{M}$
- Unforgeability: EUF-CMA w.r.t $\sim_{\mathcal{R}}$

Blind Signatures from SPS-EQ

FHS Blind Signature

- Bob:
  1. Commits to m using Pedersen commitment $C = mP + rQ$
  2. Obtains signature π from Alice on random $\boldsymbol{M} \sim [(C, P)]_{\mathcal{R}}$
  3. Derives σ on (C, P) using $ChgRep_{\mathcal{R}}$
  4. Outputs $\tau = (\sigma$, opening of $C)$ to Charlie



$\mathrm{pk} = (\mathrm{pk}_{\mathcal{R}}, (Q, \hat{Q}) = q \cdot (P, \hat{P}))$

Pedersen Commitment

$m \in \mathbb{Z}_p^*$
$r, s \in \mathbb{Z}_p^*$

$\boldsymbol{M} = s \cdot (mP + rQ, P) \longrightarrow$

$\longleftarrow \pi \leftarrow \mathit{Sign}_{\mathcal{R}}(\boldsymbol{M}, \mathrm{sk})$

$\mathrm{sk} = (\mathrm{sk}_{\mathcal{R}}, q)$

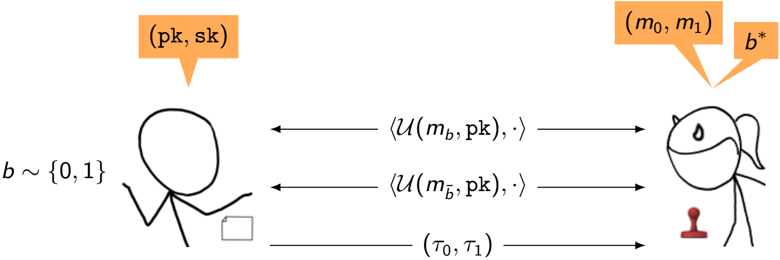
$\sigma \leftarrow \mathit{ChgRep}_{\mathcal{R}}(\boldsymbol{M}, \pi, 1/s, \mathrm{pk}_{\mathcal{R}})$
$\tau \leftarrow (\sigma, R = rP, T = rQ)$

Opening

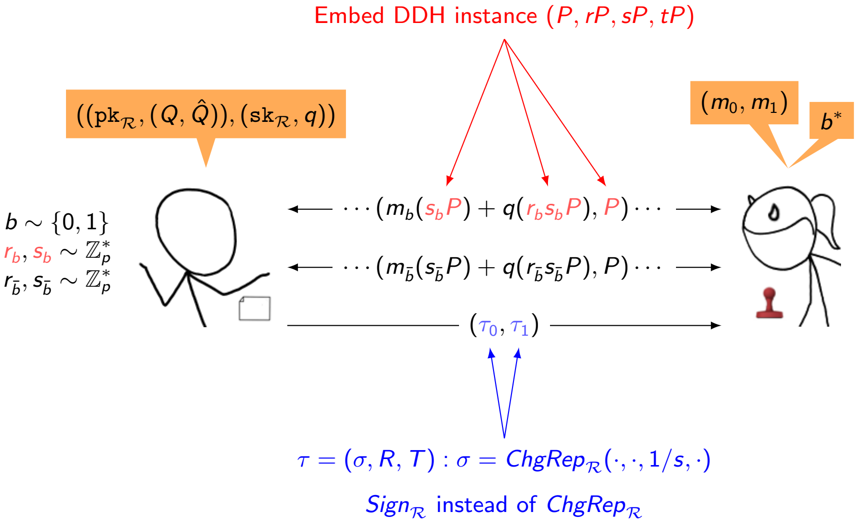
$(m, \tau) \longrightarrow$

$\mathit{Verify}_{\mathcal{R}}((mP + T, P), \sigma, \mathrm{pk}_{\mathcal{R}}) \stackrel{?}{=} 1$
$e(R, \hat{Q}) \stackrel{?}{=} e(T, \hat{P})$

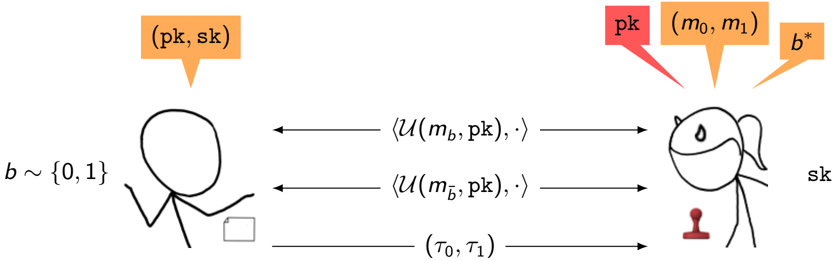
Blindness: Honest-Key Model



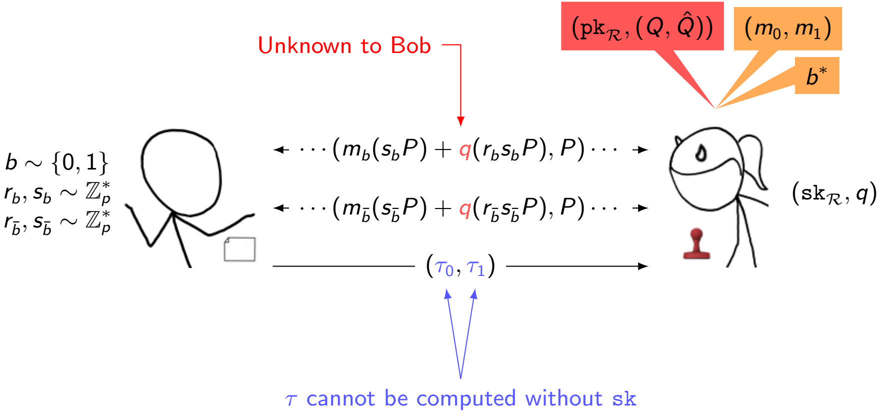
Blindness: Honest-Key Model...



Blindness: Malicious-Key Model



Blindness: Malicious-Key Model...



- Solution:
  1. Interactive variant of DDH needed
  2. Rewind Alice to generate signatures ($ChgRep_{\mathcal{R}}$ uniform)

Our construction

- Idea: *Bob* chooses parameters for commitment
  - Must be *perfectly binding*

- Bob:
  1. *Chooses "one-time" keys (P, Q) for El-Gamal encryption*
  2. Commits to m using $C = mP + rQ$
  3. Obtains signature π from Alice on $\boldsymbol{M} \sim [(C, rP, Q, P)]_{\mathcal{R}}$
  4. Derives σ on (C, rP, Q, P) using $ChgRep_{\mathcal{R}}$
  5. Outputs $\tau = (\sigma$, opening of $C)$ to Charlie

sR allows verification!
$e(M_1 - mM_4) \stackrel{?}{=} e(M_2, \hat{Q})$

$\mathrm{pk} = \mathrm{pk}_{\mathcal{R}}$

$m \in \mathbb{Z}_p^*$
$r, s \in \mathbb{Z}_p^*, R = rP$
$q \in \mathbb{Z}_p^*, Q := qP$

$\boldsymbol{M} = s \cdot (mP + rQ, R, Q, P)$ →

← $\pi \leftarrow \mathit{Sign}_{\mathcal{R}}(\boldsymbol{M}, \mathrm{sk})$

$\mathrm{sk} = \mathrm{sk}_{\mathcal{R}}$

$\sigma \leftarrow \mathit{ChgRep}_{\mathcal{R}}(\boldsymbol{M}, \pi, 1/s, \mathrm{pk}_{\mathcal{R}})$
$\tau \leftarrow (\sigma, R, Q, Z = rQ, \hat{Q} = q\hat{P})$

Solution: split q

(m, τ) →

$\mathit{Verify}_{\mathcal{R}}((mP + Z, R, Q, P), \sigma, \mathrm{pk}_{\mathcal{R}}) \stackrel{?}{=} 1$
$e(Q, \hat{P}) \stackrel{?}{=} e(P, \hat{Q}),\ e(Z, \hat{P}) \stackrel{?}{=} e(R, \hat{Q})$

$\mathrm{pk} = \mathrm{pk}_{\mathcal{R}}$

$m \in \mathbb{Z}_p^*$

$r, s \in \mathbb{Z}_p^*, R = rP$

$u, v \in \mathbb{Z}_p^*, Q := uvP$

$\boldsymbol{M} = s \cdot (mP + rQ, R, Q, P)$ →

← $\pi \leftarrow \mathit{Sign}_{\mathcal{R}}(\boldsymbol{M}, \mathrm{sk})$

$\mathrm{sk} = \mathrm{sk}_{\mathcal{R}}$

$\sigma \leftarrow \mathit{ChgRep}_{\mathcal{R}}(\boldsymbol{M}, \pi, 1/s, \mathrm{pk}_{\mathcal{R}})$

$\tau \leftarrow (\sigma, R, Q, Y = rQ, U = uP, X = ruP, \hat{U} = u\hat{P}, \hat{V} = v\hat{P})$

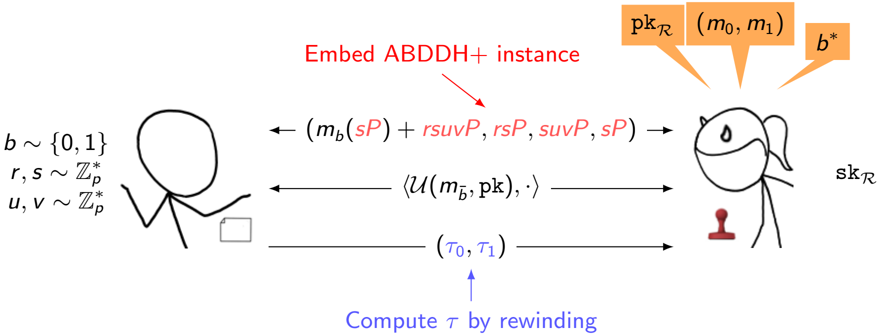
(m, τ) →

$\mathit{Verify}_{\mathcal{R}}((mP + Y, R, Q, P), \sigma, \mathrm{pk}_{\mathcal{R}}) \stackrel{?}{=} 1$

$e(Q, \hat{P}) \stackrel{?}{=} e(U, \hat{V}),\ e(U, \hat{P}) \stackrel{?}{=} e(P, \hat{U})$

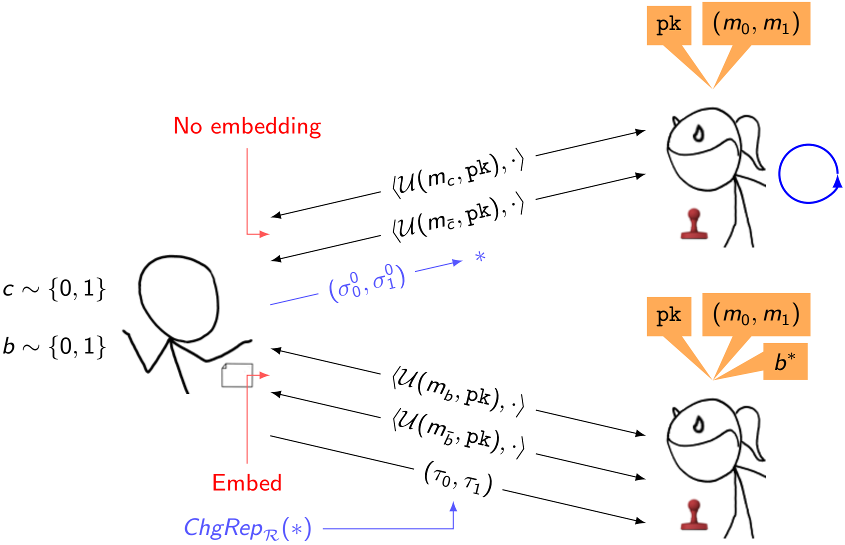
$e(X, \hat{P}) \stackrel{?}{=} e(R, \hat{U}),\ e(Y, \hat{P}) \stackrel{?}{=} e(X, \hat{V})$

Blindness: Malicious-Key Model



- ABDDH+ assumption: hard to distinguish $ruvP$ from random given: rP, uP, uvP, $u\hat{P}$, $v\hat{P}$
  - ABDDH+ $\Longrightarrow$ DDH
  - Hard in generic group model

Blindness: Malicious-Key Model...



- Multiple rewinds required: fails for single rewind!

Comparison

	[GG14]	[FHS15]	This work
Assumption	DLIN	Interactive DDH	ABDDH+
Public-key	$43\mathbb{G}$	$1\mathbb{G}_1 + 3\mathbb{G}_2$	$4\mathbb{G}_2$
Communication	$> 41\mathbb{G}$	$4\mathbb{G}_1 + 1\mathbb{G}_2$	$6\mathbb{G}_1 + 1\mathbb{G}_2$
Signatures	$183\mathbb{G}$	$4\mathbb{G}_1 + 1\mathbb{G}_2$	$7\mathbb{G}_1 + 3\mathbb{G}_2$
Computation	$9e$	$7e$	$14e$

References

AFG+10 M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, M. Ohkubo *Structure-Preserving Signatures and Commitments to Group Elements*.

FHS15 G. Fuchsbauer, C. Hanser and D. Slamanig. *Practical Round-Optimal Blind Signatures in the Standard Model*. CRYPTO 2015

FS10 M. Fischlin and D. Schröder. *On the Impossibility of Three-Move Blind Signature Schemes*. EUROCRYPT 2010

GG14 S. Garg and D. Gupta. *Efficient Round Optimal Blind Signatures*. EUROCRYPT 2014

GRS+11 S. Garg, V. Rao, A. Sahai, D. Schröder and D. Unruh. *Round Optimal Blind Signatures*. CRYPTO 2011