On Pairing-Free Blind Signature Schemes in the Algebraic Group Model

Julia Kastner
ETH Zürich

Julian Loss
CISPA

Jiayu Xu
Algorand

PKC 2022

Three-Move Blind Signature Schemes

Three-Move Blind Signature Schemes

sk

Three-Move Blind Signature Schemes

sk

pk, m

Three-Move Blind Signature Schemes

sk

pk, m

$R \xleftarrow{\$} \mathsf{Sign}_1(\mathsf{sk})$

Three-Move Blind Signature Schemes

sk

pk, m

$R \xleftarrow{\$} \mathsf{Sign}_1(\mathsf{sk})$

R

Three-Move Blind Signature Schemes

sk

pk, m

$R \xleftarrow{\$} \mathsf{Sign}_1(\mathsf{sk})$

R

$c \xleftarrow{\$} \mathsf{User}_1(\mathsf{pk}, R, m)$

Three-Move Blind Signature Schemes

sk

pk, m

$R \xleftarrow{\$} \mathsf{Sign}_1(\mathsf{sk})$

R

$c \xleftarrow{\$} \mathsf{User}_1(\mathsf{pk}, R, m)$

c

Three-Move Blind Signature Schemes

sk

pk, m

$R \xleftarrow{\$} \mathrm{Sign}_1(\mathrm{sk})$

R

$c \xleftarrow{\$} \mathrm{User}_1(\mathrm{pk}, R, m)$

c

$s \xleftarrow{\$} \mathrm{Sign}_2(\mathrm{sk}, R, c)$

Three-Move Blind Signature Schemes

sk

pk, m

$R \xleftarrow{\$} \mathsf{Sign}_1(\mathsf{sk})$

R

$c \xleftarrow{\$} \mathsf{User}_1(\mathsf{pk}, R, m)$

c

$s \xleftarrow{\$} \mathsf{Sign}_2(\mathsf{sk}, R, c)$

s

Three-Move Blind Signature Schemes

sk

pk, m

$R \xleftarrow{\$} \mathsf{Sign}_1(\mathsf{sk})$

R

$c \xleftarrow{\$} \mathsf{User}_1(\mathsf{pk}, R, m)$

c

$s \xleftarrow{\$} \mathsf{Sign}_2(\mathsf{sk}, R, c)$

s

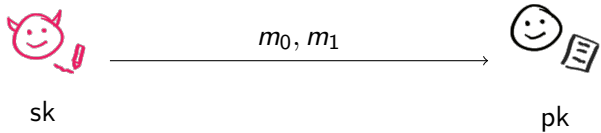
$\sigma \xleftarrow{\$} \mathsf{User}_2(\mathsf{pk}, R, s, m)$

Security Notions - Blindness

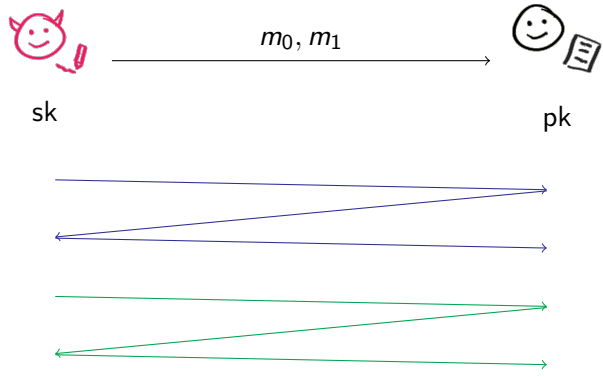
sk

pk

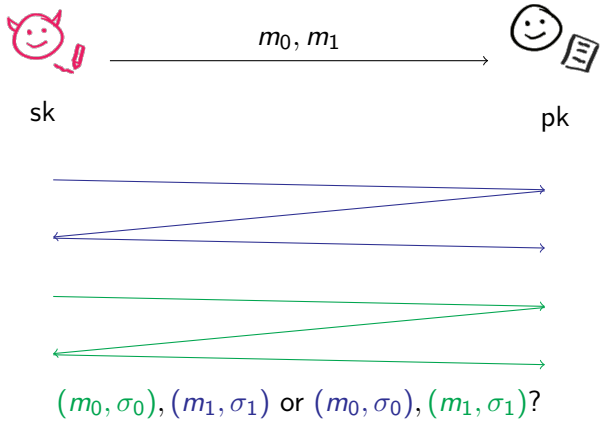
Security Notions - Blindness



Security Notions - Blindness

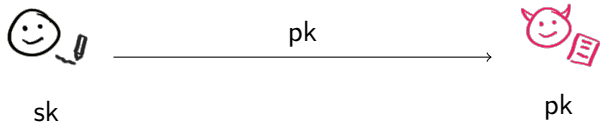


Security Notions - Blindness

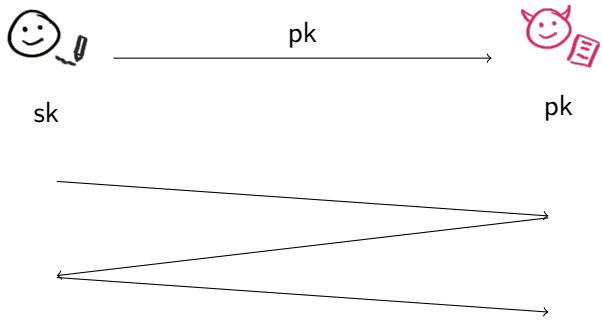


Security Notions - One-more-unforgeability

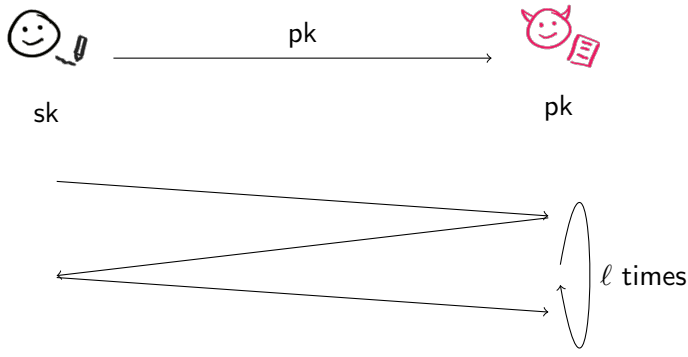
Security Notions - One-more-unforgeability



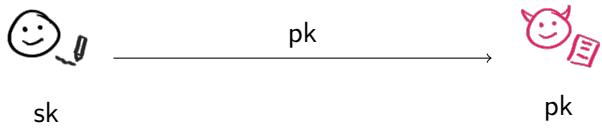
Security Notions - One-more-unforgeability

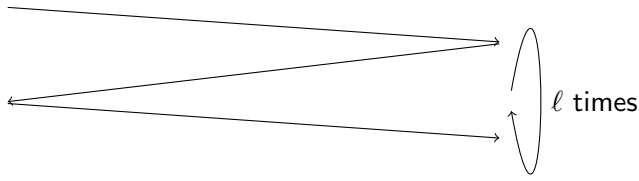


Security Notions - One-more-unforgeability



Security Notions - One-more-unforgeability



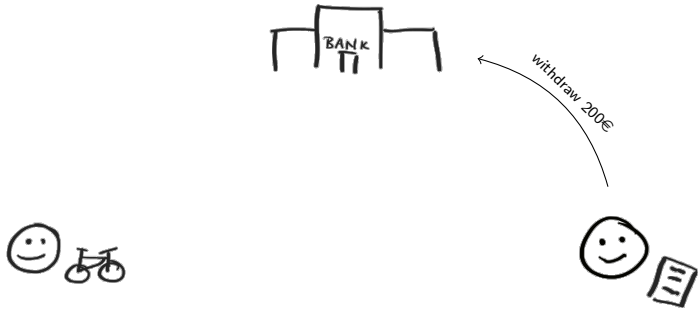


$\Downarrow$

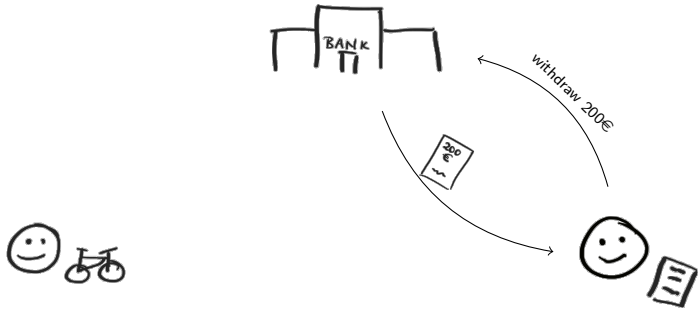
$(m_1, \sigma_1), \ldots, (m_{\ell+1}, \sigma_{\ell+1})$

Motivation - eCash [Cha82]

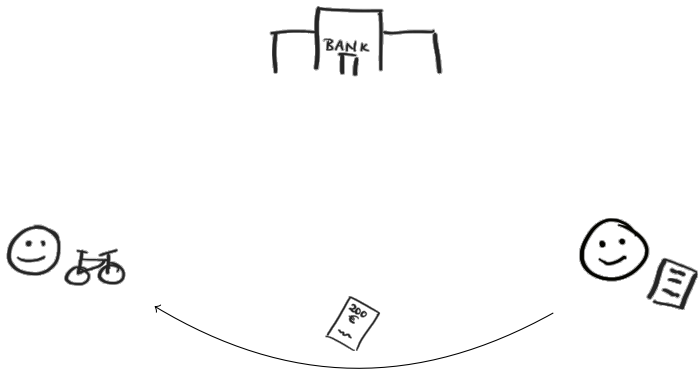
Motivation - eCash [Cha82]



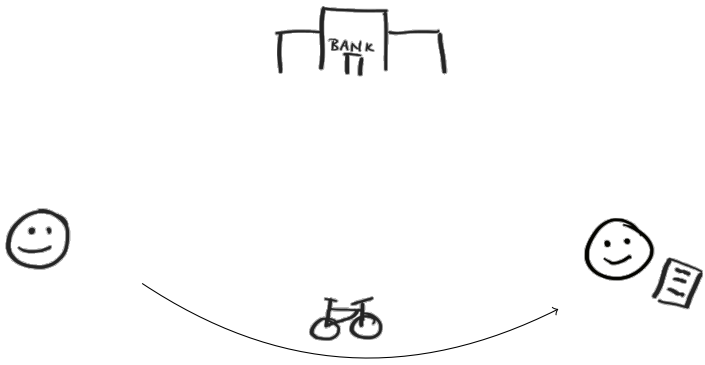
Motivation - eCash [Cha82]



Motivation - eCash [Cha82]

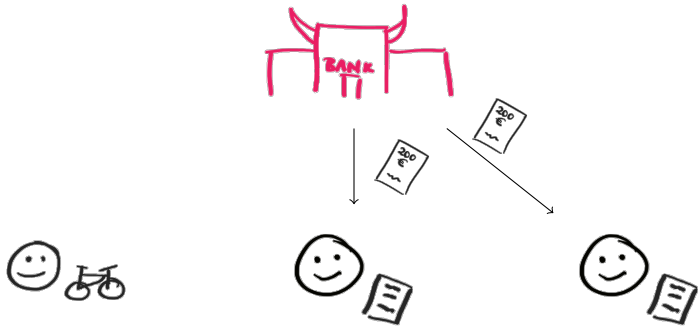


Motivation - eCash [Cha82]

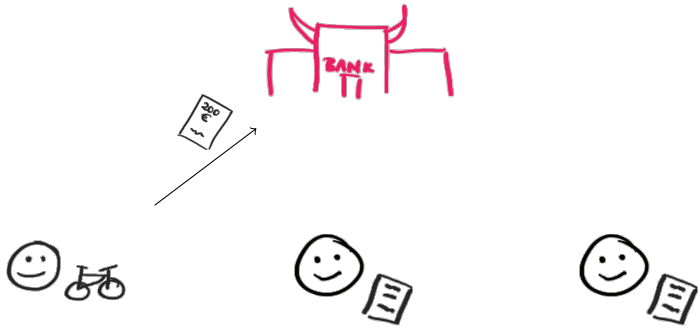


Motivation - eCash[Cha82]

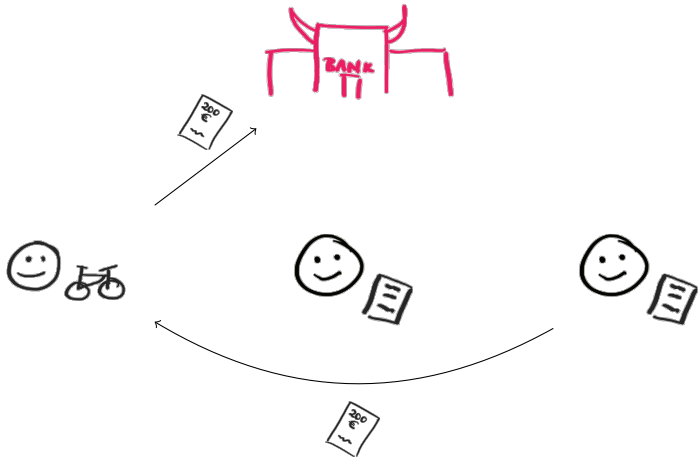
Motivation - eCash[Cha82]



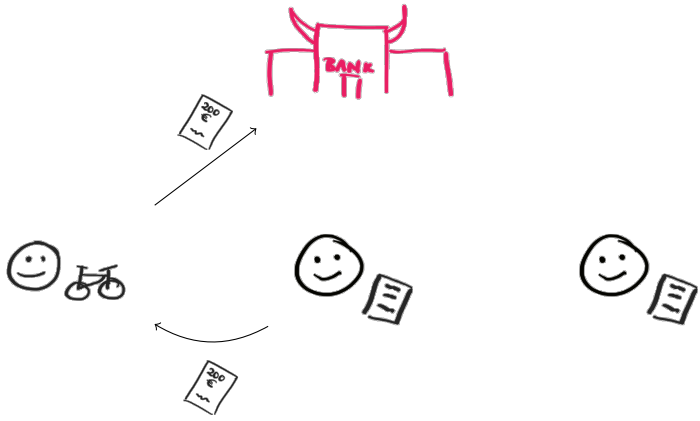
Motivation - eCash[Cha82]



Motivation - eCash[Cha82]

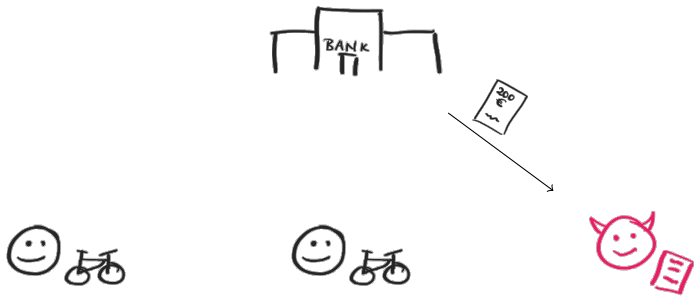


Motivation - eCash[Cha82]

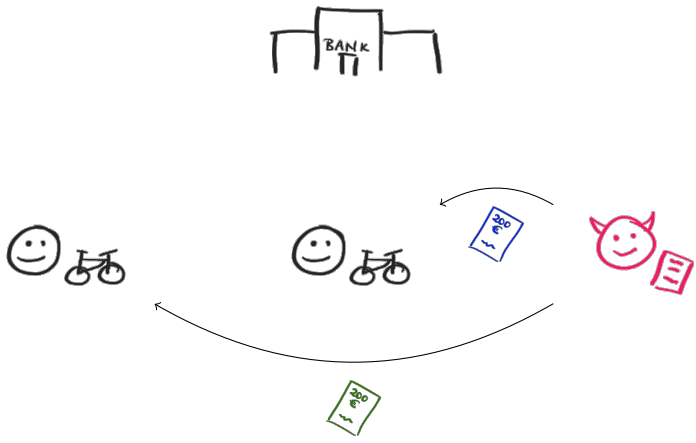


Motivation - eCash [Cha82]

Motivation - eCash [Cha82]



Motivation - eCash [Cha82]



Partial Blindness [AF96]

Additional information info

- Date/Time
- Expiration Date
- Value 50€, 100€, 200€, ...

State of the Art

- Blind Schnorr:

State of the Art

- Blind Schnorr:
  - used in blockchain protocols

State of the Art

- Blind Schnorr:
  - used in blockchain protocols
  - ROS-attack [Sch01]

State of the Art

- Blind Schnorr:
  - used in blockchain protocols
  - ROS-attack [Sch01]
  - Standard (group) model impossibility [BL13]

State of the Art

- Blind Schnorr:
  - used in blockchain protocols
  - ROS-attack [Sch01]
  - Standard (group) model impossibility [BL13]
  - concurrent security in AGM + ROM + ROS-assumption + OMDL [FPS20]

State of the Art

- Blind Schnorr:
  - used in blockchain protocols
  - ROS-attack [Sch01]
  - Standard (group) model impossibility [BL13]
  - concurrent security in AGM + ROM + ROS-assumption + OMDL [FPS20]
  - poly-time attack on ROS [Ben+21]

State of the Art

- Blind Schnorr:
  - used in blockchain protocols
  - ROS-attack [Sch01]
  - Standard (group) model impossibility [BL13]
  - concurrent security in AGM + ROM + ROS-assumption + OMDL [FPS20]
  - poly-time attack on ROS [Ben+21]
- Abe's Scheme [Abe01]

State of the Art

- Blind Schnorr:
  - used in blockchain protocols
  - ROS-attack [Sch01]
  - Standard (group) model impossibility [BL13]
  - concurrent security in AGM + ROM + ROS-assumption + OMDL [FPS20]
  - poly-time attack on ROS [Ben+21]
- Abe's Scheme [Abe01]
  - immune to ROS-attack

State of the Art

- Blind Schnorr:
  - used in blockchain protocols
  - ROS-attack [Sch01]
  - Standard (group) model impossibility [BL13]
  - concurrent security in AGM + ROM + ROS-assumption + OMDL [FPS20]
  - poly-time attack on ROS [Ben+21]
- Abe's Scheme [Abe01]
  - immune to ROS-attack
  - original forking based proof flawed

State of the Art

- Blind Schnorr:
  - used in blockchain protocols
  - ROS-attack [Sch01]
  - Standard (group) model impossibility [BL13]
  - concurrent security in AGM + ROM + ROS-assumption + OMDL [FPS20]
  - poly-time attack on ROS [Ben+21]
- Abe's Scheme [Abe01]
  - immune to ROS-attack
  - original forking based proof flawed
  - GGM-proof [OA03]

Our Contributions

- DLog + AGM + ROM: Abe's scheme **concurrently** secure

Our Contributions

- DLog + AGM + ROM: Abe's scheme **concurrently** secure
- OMDL + AGM + ROM: Schnorr's scheme *sequentially* secure

Our Contributions

- DLog + AGM + ROM: Abe's scheme **concurrently** secure
- OMDL + AGM + ROM: Schnorr's scheme *sequentially* secure
- for algebraic OMDL reduction: need at least as many OMDL queries as closed signing sessions

Our Contributions

- DLog + AGM + ROM: Abe's scheme **concurrently** secure
- OMDL + AGM + ROM: Schnorr's scheme *sequentially* secure
- for algebraic OMDL reduction: need at least as many OMDL queries as closed signing sessions

The Algebraic Group Model [FKL18]

$$(y, \quad) \xleftarrow{\$} A(x_1, \ldots, x_n)$$

The Algebraic Group Model [FKL18]

$$(y, \overrightarrow{z}) \xleftarrow{\$} A(x_1, \ldots, x_n)$$

$$y = \prod_{j=1}^{n} x_j^{z_j}$$

Blind Schnorr Signatures

$\mathsf{sk} = x$

m

Blind Schnorr Signatures

$\mathsf{sk} = x$

$\mathsf{pk} = \mathsf{y} = \mathsf{g}^x, m$

Blind Schnorr Signatures

$\mathsf{sk} = x$

$r \xleftarrow{\$} \mathbb{Z}_q$

$\mathsf{pk} = \mathsf{y} = \mathsf{g}^x, m$

Blind Schnorr Signatures

$\mathsf{sk} = x$

$\mathsf{pk} = \mathsf{y} = \mathsf{g}^x, m$

$r \xleftarrow{\$} \mathbb{Z}_q$

$R = g^r$

Blind Schnorr Signatures

$\mathsf{sk} = x$

$\mathsf{pk} = \mathsf{y} = \mathsf{g}^x, m$

$r \xleftarrow{\$} \mathbb{Z}_q$

$R = g^r$

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$

$c := H(R\mathsf{g}^\alpha \mathsf{y}^\beta, m) + \beta$

Blind Schnorr Signatures

$\mathsf{sk} = x$

$\mathsf{pk} = \mathsf{y} = \mathsf{g}^x, m$

$r \xleftarrow{\$} \mathbb{Z}_q$

$R = g^r$

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$

c

$c := H(R\mathsf{g}^\alpha \mathsf{y}^\beta, m) + \beta$

Blind Schnorr Signatures

$\mathsf{sk} = x$

$\mathsf{pk} = \mathsf{y} = \mathsf{g}^x, m$

$r \xleftarrow{\$} \mathbb{Z}_q$

$R = g^r$

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$

c

$c := H(R\mathsf{g}^{\alpha}\mathsf{y}^{\beta}, m) + \beta$

$s := c \cdot x + r$

Blind Schnorr Signatures

$\mathsf{sk} = x$

$\mathsf{pk} = \mathsf{y} = \mathsf{g}^x, m$

$r \xleftarrow{\$} \mathbb{Z}_q$

$R = g^r$

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$

c

$c := H(R\mathsf{g}^{\alpha}\mathsf{y}^{\beta}, m) + \beta$

$s := c \cdot x + r$

s

Blind Schnorr Signatures

$\mathsf{sk} = x$

$\mathsf{pk} = \mathsf{y} = \mathsf{g}^x, m$

$r \xleftarrow{\$} \mathbb{Z}_q$

$R = \mathsf{g}^r$

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$

$c \coloneqq H(R\mathsf{g}^\alpha \mathsf{y}^\beta, m) + \beta$

c

$s \coloneqq c \cdot x + r$

s

$\mathsf{g}^s \stackrel{?}{=} R \cdot \mathsf{y}^c$

$c' = c - \beta, s' \coloneqq s + \alpha$

$(m, \sigma = (c', s'))$

Reduction

$\mathsf{sk} = x$

$\mathsf{pk} = \mathsf{y} = \mathsf{g}^x, m$

$r \xleftarrow{\$} \mathbb{Z}_q$

$R = \mathsf{g}^r$

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$

$c := H(R\mathsf{g}^\alpha \mathsf{y}^\beta, m) + \beta$

c

$s := c \cdot x + r$

s

$\mathsf{g}^s \stackrel{?}{=} R \cdot \mathsf{y}^c$

$c' := c - \beta, s' := s + \alpha$

$(m, \sigma = (c', s'))$

Reduction

$\mathsf{Y} = \mathsf{chal}$

$\mathsf{pk} = \mathsf{Y}, m$

$r \xleftarrow{\$} \mathbb{Z}_q$

$R = g^r$

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$

$c := H(R g^{\alpha} y^{\beta}, m) + \beta$

c

$s := c \cdot x + r$

s

$g^s \stackrel{?}{=} R \cdot y^c$

$c' := c - \beta, s' := s + \alpha$

$(m, \sigma = (c', s'))$

Reduction

$\mathsf{Y} = \mathsf{chal}$

$\mathsf{pk} = \mathsf{Y}, m$

$\mathsf{R} = \mathsf{chal}$

R

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$

c

$c := H(R\mathsf{g}^{\alpha}\mathsf{y}^{\beta}, m) + \beta$

$s := c \cdot x + r$

s

$\mathsf{g}^{s} \stackrel{?}{=} R \cdot \mathsf{y}^{c}$

$c' := c - \beta, s' := s + \alpha$

$(m, \sigma = (c', s'))$

Reduction

$\mathsf{Y} = \mathsf{chal}$

$\mathsf{pk} = \mathsf{Y}, m$

$\mathsf{R} = \mathsf{chal}$

R

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$

c

$c := H(R\mathsf{g}^{\alpha}\mathsf{y}^{\beta}, m) + \beta$

$s := \mathsf{dlog}(R \cdot Y^c)$

s

$\mathsf{g}^s \stackrel{?}{=} R \cdot \mathsf{y}^c$

$c' := c - \beta, s' := s + \alpha$

$(m, \sigma = (c', s'))$

Reduction

$\mathsf{Y} = \mathsf{chal}$

$\mathsf{pk} = \mathsf{Y}, m$

$\mathsf{R} = \mathsf{chal}$

R

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$

c

$c := H(R\mathsf{g}^{\alpha}\mathsf{y}^{\beta}, m) + \beta$

$s := \mathsf{dlog}(R \cdot Y^c)$

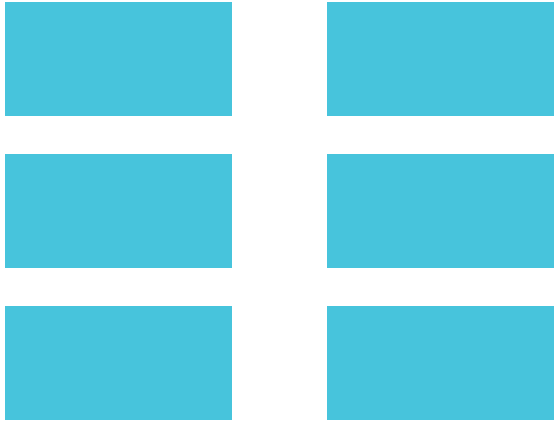
s

$\mathsf{g}^s \stackrel{?}{=} R \cdot \mathsf{y}^c$

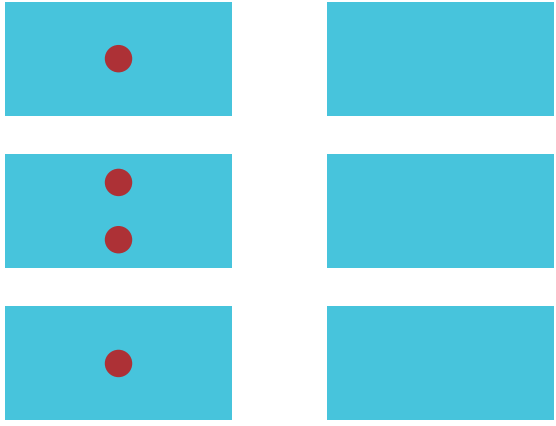
$c' := c - \beta, s' := s + \alpha$

$(m, \sigma = (c', s'))$

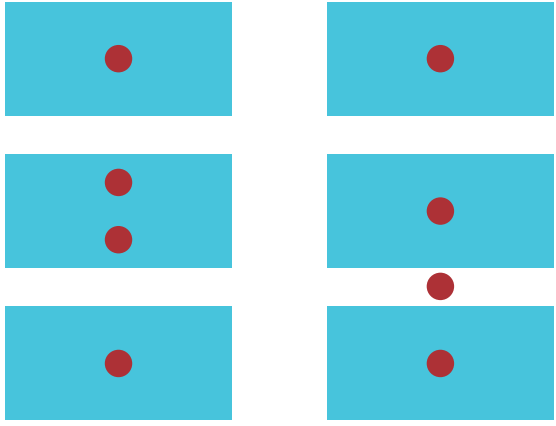
Sequential security of Blind Schnorr Signatures



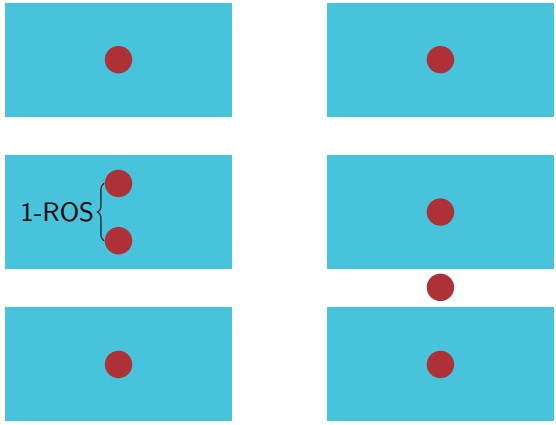
Sequential security of Blind Schnorr Signatures



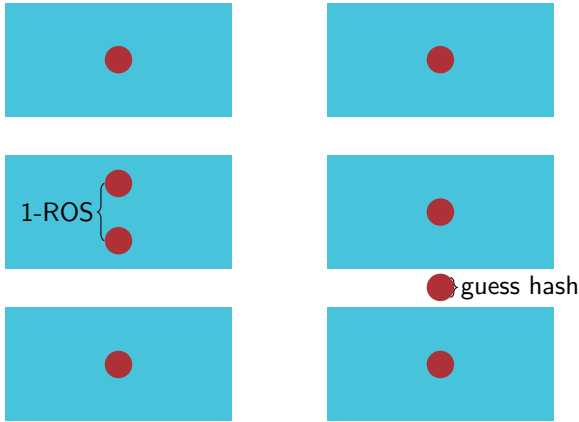
Sequential security of Blind Schnorr Signatures



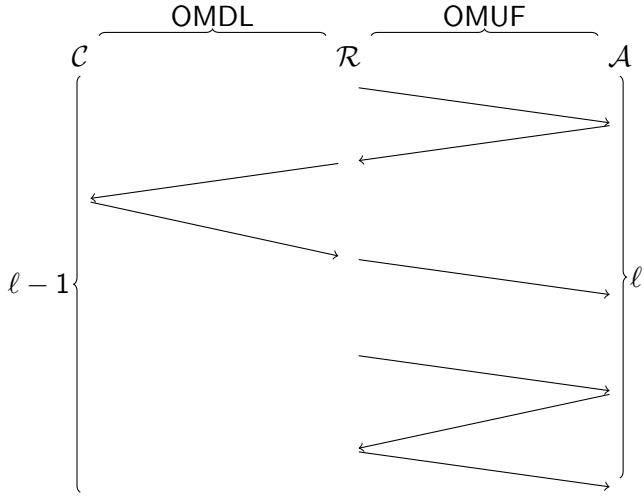
Sequential security of Blind Schnorr Signatures



Sequential security of Blind Schnorr Signatures



Optimality of the result



Abe's blind signature scheme [Abe01]

Abe's blind signature scheme [Abe01]

x | h, z

Abe's blind signature scheme [Abe01]

x | h, z

$y = g^x$ | h, z

Abe's blind signature scheme [Abe01]

x h, z

$y = g^x$ h, z

R= a $, z_1, b_1, b_2$

Abe's blind signature scheme [Abe01]

x | h, z

$y = g^x$ | h, z

R= a | z_1, b_1, b_2

R

Abe's blind signature scheme [Abe01]

x h, z

$\mathsf{y} = \mathsf{g}^x$ h, z

$\mathsf{R}=$ $a, \mathsf{z}_1, b_1, b_2$

R

$\varepsilon \xleftarrow{\$} H_3(\zeta, \zeta_1, \alpha, \beta_1, \beta_2, \eta, \mathsf{m})$

$\mathsf{e} = \varepsilon +$ $+$

Abe's blind signature scheme [Abe01]

x | h, z

$y = g^x$ | h, z

$R = a, z_1, b_1, b_2$

R

$\varepsilon \xleftarrow{\$} H_3(\zeta, \zeta_1, \alpha, \beta_1, \beta_2, \eta, m)$

$e = \varepsilon +$ | $+$

e

Abe's blind signature scheme [Abe01]

x | h, z

$y = g^x$ | h, z

R= a, z_1, b_1, b_2

R

$\varepsilon \xleftarrow{\$} H_3(\zeta, \zeta_1, \alpha, \beta_1, \beta_2, \eta, m)$

$e = \varepsilon +$ ▢ $+$ ▢

e

$e = c + d$

r, s_1, s_2

Abe's blind signature scheme [Abe01]

x | h, z

$y = g^x$ | h, z

R= a, z_1, b_1, b_2

R

$\varepsilon \xleftarrow{\$} H_3(\zeta, \zeta_1, \alpha, \beta_1, \beta_2, \eta, m)$

$e = \varepsilon +$ | |

e

$e = c +$ | d

r, s_1, s_2

c, r, d, s_1, s_2

Abe's blind signature scheme [Abe01]

x h, z

$y = g^x$ h, z

R= a, z_1, b_1, b_2

R

$\varepsilon \xleftarrow{\$} H_3(\zeta, \zeta_1, \alpha, \beta_1, \beta_2, \eta, m)$

$e = \varepsilon +$ ▢ $+$ ▢

e

$e = c + d$

r, s_1, s_2

c, r, d, s_1, s_2

$\varepsilon = \omega + \delta$

$\rho, \zeta, \zeta_1, \sigma_1, \sigma_2, \mu$

Abe's blind signature scheme [Abe01]

Y $h = g^w, z = g^{w_0}$

Y h, z

R= a, z_1, b_1, b_2

R

$\varepsilon \xleftarrow{\$} H_3(\zeta, \zeta_1, \alpha, \beta_1, \beta_2, \eta, m)$

$e = \varepsilon +$ $+$

e

$e = c + d$

r, s_1, s_2

c, r, d, s_1, s_2

$\varepsilon = \omega +$ δ

$\rho, \zeta, \zeta_1, \sigma_1, \sigma_2, \mu$

Abe's blind signature scheme [Abe01]

x Y z

x Y z

R= a, z_1, b_1, b_2

R

$\varepsilon \xleftarrow{\$} H_3(\zeta, \zeta_1, \alpha, \beta_1, \beta_2, \eta, \mathrm{m})$

$\mathrm{e} = \varepsilon +$ $+$

e

$\mathrm{e} = c + d$

r, s_1, s_2

c, r, d, s_1, s_2

$\varepsilon = \omega + \delta$

$\rho, \zeta, \zeta_1, \sigma_1, \sigma_2, \mu$

Abe's blind signature scheme [Abe01]

x h Y

x h Y

R= a, z_1, b_1, b_2

R

$\varepsilon \xleftarrow{\$} H_3(\zeta, \zeta_1, \alpha, \beta_1, \beta_2, \eta, \mathrm{m})$

$\mathrm{e} = \varepsilon +$ $+$

e

$\mathrm{e} = c + d$

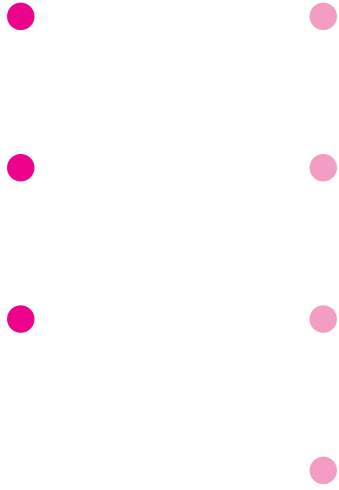
r, s_1, s_2

c, r, d, s_1, s_2

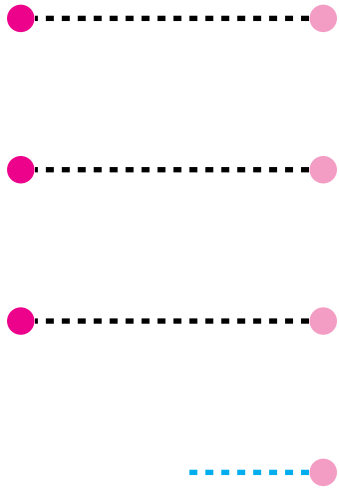
$\varepsilon = \omega + \delta$

$\rho, \zeta, \zeta_1, \sigma_1, \sigma_2, \mu$

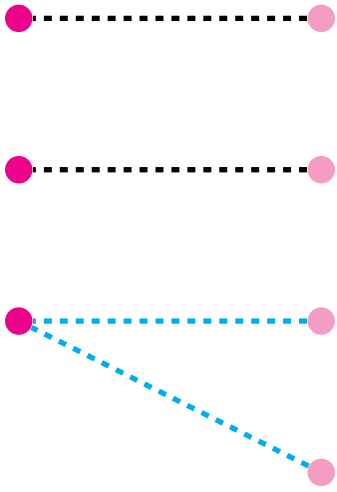
Linking Components



Linking Components

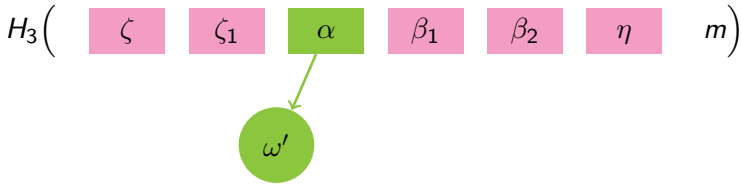


Linking Components

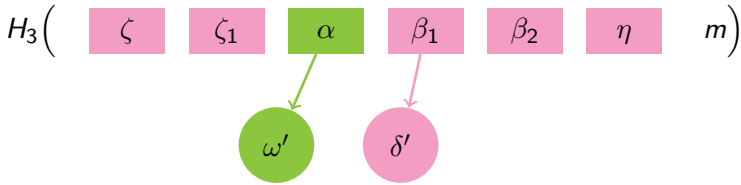


Preliminary Components

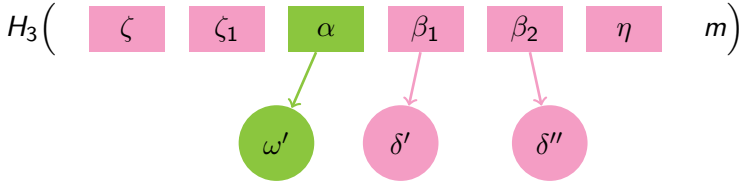
Preliminary Components



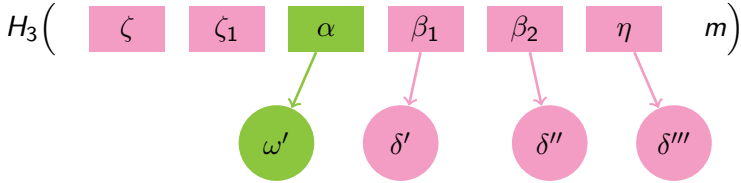
Preliminary Components



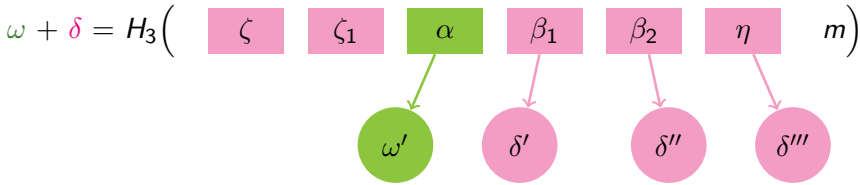
Preliminary Components



Preliminary Components



Preliminary Components



How can the preliminary components be the same?

- guess hash value

How can the preliminary components be the same?

- guess hash value
- solve some discrete log

How can the preliminary components be the same?

- guess hash value
- solve some discrete log
- behave honestly
  - match linking components
  - solve 1-ROS

Recap

- DLog + AGM + ROM: Abe's scheme **concurrently** secure
- OMDL + AGM + ROM: Schnorr's scheme *sequentially* secure
- for algebraic OMDL reduction: need at least as many OMDL queries as closed signing sessions

Open questions

- Security of Abe's scheme in ROM only
- Schnorr's scheme with low concurrency in AGM + ROM

References I


Masayuki Abe. "A Secure Three-Move Blind Signature Scheme for Polynomially Many Signatures". In: *EUROCRYPT 2001*. 2001.


Masayuki Abe and Eiichiro Fujisaki. "How to Date Blind Signatures". In: *ASIACRYPT'96*. 1996.


Fabrice Benhamouda et al. "On the (in)security of ROS". In: *EUROCRYPT 2021, Part I*. 2021.


Foteini Baldimtsi and Anna Lysyanskaya. "On the Security of One-Witness Blind Signature Schemes". In: *ASIACRYPT 2013, Part II*. 2013.


David Chaum. "Blind Signatures for Untraceable Payments". In: *CRYPTO'82*. 1982.


Georg Fuchsbauer, Eike Kiltz, and Julian Loss. "The Algebraic Group Model and its Applications". In: *CRYPTO 2018, Part II*. 2018.


Georg Fuchsbauer, Antoine Plouviez, and Yannick Seurin. "Blind Schnorr Signatures and Signed ElGamal Encryption in the Algebraic Group Model". In: *EUROCRYPT 2020, Part II*. 2020.

References II

Miyako Ohkubo and Masayuki Abe. *Security of Some Three-move Blind Signature Schemes Reconsidered*. The 2003 Symposium on Cryptography and Information Security. 2003.

Claus-Peter Schnorr. "Security of Blind Discrete Log Signatures against Interactive Attacks". In: *ICICS 01*. 2001.