The self-blindable U-Prove scheme from FC'14 is forgeable

Eric Verheul, **Sietse Ringers** and Jaap-Henk Hoepman

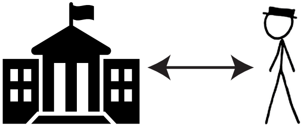
sringers@cs.ru.nl

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen

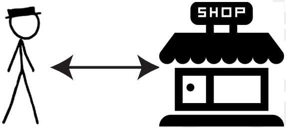
February 23, 2016
Financial Crypto, Barbados

Credential schemes

IssueCredential



ShowCredential



Features:

- No communication with issuer during transactions
- Provably unforgeable

Attribute-based credential schemes

$\Longrightarrow$

Credential

- Attributes $(x_1, \ldots, x_n)$
- Signature on attributes

Features:

- Selective disclosure
- **Unlinkability**

Attribute-based credential schemes

$\Longrightarrow$

Credential

- Attributes $(x_1, \ldots, x_n)$
- Signature on attributes

Features:

- Selective disclosure
- **Unlinkability**

Attribute-based credential schemes

$\Longrightarrow$

Credential

- Attributes $(x_1, \ldots, x_n)$
- Signature on attributes

Features:

- Selective disclosure
- **Unlinkability**

Existing ABCs

Idemix Camenisch, Lysyanskaya	RSA-like groups	unlinkable	unforgeable
U-Prove Brands	elliptic curves	not unlinkable	?
FC'14 scheme Hanzlik, Klukzniak	**elliptic curves**	**unlinkable**	**forgeable**

Existing ABCs

Idemix Camenisch, Lysyanskaya	RSA-like groups	unlinkable	unforgeable
U-Prove Brands	elliptic curves	not unlinkable	?
FC'14 scheme Hanzlik, Klukzniak	**elliptic curves**	**unlinkable**	**forgeable**

Hanzlik and Kluczniak's scheme

Setup:

- Type 2 bilinear pairing $e\colon G_1 \times G_2 \to G_T$
  - G_1, G_2 elliptic curves of prime order
- Issuer public key: $(e, g_0, \ldots, g_n, p, p', p_0, p_1)$
  - with $g_0, \ldots, g_n \in G_1, \quad p, p' \in G_2, \quad p_0 = (p')^z, p_1 = p^f$
- Issuer private key: (f, z)

A credential over attributes $(x_1, \ldots, x_n)$:

$$(\underbrace{h, h_2, h_3, h_4,}_{\in G_1} \underbrace{\alpha, b_1, b_2}_{\text{numbers}})$$

- $h = (g_0 g_1^{x_1} \cdots g_n^{x_n})^\alpha$
- $h_2 = h^f$
- $h_3 = h^{b_1} h_2^{b_2}$
- $h_4 = h_3^z$

Hanzlik and Kluczniak's scheme

Setup:

- Type 2 bilinear pairing $e\colon G_1 \times G_2 \to G_T$
  - G_1, G_2 elliptic curves of prime order
- Issuer public key: $(e, g_0, \ldots, g_n, p, p', p_0, p_1)$
  - with $g_0, \ldots, g_n \in G_1, \quad p, p' \in G_2, \quad p_0 = (p')^z, p_1 = p^f$
- Issuer private key: (f, z)

A credential over attributes $(x_1, \ldots, x_n)$:

$$(\underbrace{h, h_2, h_3, h_4}_{\in G_1},\ \underbrace{\alpha, b_1, b_2}_{\text{numbers}})$$

- $h = (g_0 g_1^{x_1} \cdots g_n^{x_n})^\alpha$
- $h_2 = h^f$
- $h_3 = h^{b_1} h_2^{b_2}$
- $h_4 = h_3^z$

Showing a credential

Credential: $(x_1, \ldots, x_n), (h, h_2, h_3, h_4, \ \alpha, b_1, b_2)$

- $h = (g_0 g_1^{x_1} \cdots g_n^{x_n})^\alpha$
- $h_2 = h^f$
- $h_3 = h^{b_1} {h_2}^{b_2}$
- $h_4 = h_3^z$

Showing a credential, disclosing x_1:

- Blind the credential as above
- Zero-knowledge proof over $x_2, \ldots, x_n, \alpha k, b_1 \ell, b_2 \ell$

Showing a credential

Credential: $(x_1, \ldots, x_n), (h^{k}, h_2^{k}, h_3^{k\ell}, h_4^{k\ell},\ \alpha k, b_1\ell, b_2\ell)$

- $h^{k} = (g_0 g_1^{x_1} \cdots g_n^{x_n})^{\alpha k}$
- $h_2^{k} = h^{kf}$
- $h_3^{k\ell} = (h^{k})^{b_1\ell}(h_2^{k})^{b_2\ell}$
- $h_4^{k\ell} = h_3^{k\ell z}$

Showing a credential, disclosing x_1:

- Blind the credential as above
- Zero-knowledge proof over $x_2, \ldots, x_n, \alpha k, b_1\ell, b_2\ell$

Showing a credential

Credential: $(x_1, \dots, x_n), (h^{k}, h_2^{k}, h_3^{k\ell}, h_4^{k\ell},\ \alpha k, b_1\ell, b_2\ell)$

- $h^{k} = (g_0 g_1^{x_1} \cdots g_n^{x_n})^{\alpha k}$
- $h_2^{k} = h^{kf}$
- $h_3^{k\ell} = (h^{k})^{b_1\ell}(h_2^{k})^{b_2\ell}$
- $h_4^{k\ell} = h_3^{k\ell z}$

Showing a credential, disclosing x_1:

- Blind the credential as above
- Zero-knowledge proof over $x_2, \dots, x_n, \alpha k, b_1\ell, b_2\ell$

The attack: 2 colliding users

Set $\widetilde{g}_i = g_i^f$

- $h_j = (g_0 g_1^{x_{1,j}} \cdots g_n^{x_{n,j}})^\alpha, \quad h_{2,j} = h^f$
- $h_{3,j} = h_j^{b_{1,j}} h_{2,j}^{b_{2,j}}$

The attack: 2 colliding users

Set $\widetilde{g}_i = g_i^f$

- $h_j = g_0 g_1^{x_{1,j}} \cdots g_n^{x_{n,j}}, \quad h_{2,j} = h^f$
- $h_{3,j} = h_j^{b_{1,j}} h_{2,j}^{b_{2,j}}$

The attack: 2 colliding users

Set $\widetilde{g}_i = g_i^f$

- $h_j = g_0 g_1^{x_{1,j}}, \quad h_{2,j} = h^f$
- $h_{3,j} = h_j^{b_{1,j}} h_{2,j}^{b_{2,j}}$

The attack: 2 colliding users

Set $\widetilde{g}_i = g_i^f$

- $h_j = g_0 g_1^{x_{1,j}}, \quad h_{2,j} = h^f$
- $h_{3,j} = h_j^{b_{1,j}} h_{2,j}^{b_{2,j}}$

$$= g_0^{b_{1,j}} \widetilde{g}_0^{b_{2,j}} g_1^{b_{1,j} x_{1,j}} \widetilde{g}_1^{b_{2,j} x_{1,j}}$$

The attack: 2 colliding users

Set $\widetilde{g}_i = g_i^f$

- $h_j = g_0 g_1^{x_{1,j}}, \quad h_{2,j} = h^f$
- $h_{3,j} = h_j^{b_{1,j}} h_{2,j}^{b_{2,j}}$

$$= g_0^{b_{1,j}} \widetilde{g}_0^{b_{2,j}} g_1^{b_{1,j} x_{1,j}} \widetilde{g}_1^{b_{2,j} x_{1,j}}$$

$$= g_0^{c_{0,j}} \widetilde{g}_0^{d_{0,j}} g_1^{c_{1,j}} \widetilde{g}_1^{d_{1,j}}$$

The attack: 2 colliding users

Set $\widetilde{g}_i = g_i^f$

- $h_j = g_0 g_1^{x_{1,j}}, \quad h_{2,j} = h^f$
- $h_{3,j} = h_j^{b_{1,j}} h_{2,j}^{b_{2,j}}$

$$= g_0^{b_{1,j}} \widetilde{g}_0^{b_{2,j}} g_1^{b_{1,j} x_{1,j}} \widetilde{g}_1^{b_{2,j} x_{1,j}}$$

$$= g_0^{c_{0,j}} \widetilde{g}_0^{d_{0,j}} g_1^{c_{1,j}} \widetilde{g}_1^{d_{1,j}}$$

User 1 and 2 calculate:

$$\frac{h_{3,1}^{1/d_{1,1}}}{h_{3,2}^{1/d_{1,2}}} = g_0^u \widetilde{g}_0^{\,v} g_1^w$$

The attack: 2 colliding users

Set $\widetilde{g}_i = g_i^f$

- $h_j = g_0 g_1^{x_{1,j}}, \quad h_{2,j} = h^f$
- $h_{3,j} = h_j^{b_{1,j}} h_{2,j}^{b_{2,j}}$

$$= g_0^{b_{1,j}} \widetilde{g}_0^{b_{2,j}} g_1^{b_{1,j} x_{1,j}} \widetilde{g}_1^{b_{2,j} x_{1,j}}$$

$$= g_0^{c_{0,j}} \widetilde{g}_0^{d_{0,j}} g_1^{c_{1,j}} \widetilde{g}_1^{d_{1,j}}$$

User 1 and 2 calculate:

$$\frac{h_{3,1}^{1/d_{1,1}}}{h_{3,2}^{1/d_{1,2}}} = g_0^u \widetilde{g}_0^{\,v} g_1^w$$

$\widetilde{g}_1$ is gone!

The attack: 2 colliding users

Set $\widetilde{g}_i = g_i^f$

- $h_j = g_0 g_1^{x_{1,j}}, \quad h_{2,j} = h^f$
- $h_{3,j} = h_j^{b_{1,j}} h_{2,j}^{b_{2,j}}$

$$= g_0^{b_{1,j}} \widetilde{g}_0^{b_{2,j}} g_1^{b_{1,j} x_{1,j}} \widetilde{g}_1^{b_{2,j} x_{1,j}}$$

$$= g_0^{c_{0,j}} \widetilde{g}_0^{d_{0,j}} g_1^{c_{1,j}} \widetilde{g}_1^{d_{1,j}}$$

User 1 and 2 calculate:

$$\frac{h_{3,1}^{1/d_{1,1}}}{h_{3,2}^{1/d_{1,2}}} = g_0^u \widetilde{g}_0^{\,v} g_1^w$$

$\widetilde{g}_1$ is gone!

- $\widetilde{g}_1$ shared across all credentials
- Group order known $\Rightarrow$ can invert exponents

The attack: many colliding users

$$h_3 = g_0^{c_0} \widetilde{g}_0^{d_0} g_1^{c_1} \widetilde{g}_1^{d_1}, \qquad h_4 = h_3^z$$

- 2 users can remove $\widetilde{g}_1$ from h_3 and $\widetilde{g}_1^z$ from h_4
- 8 users can:
  - compute $\widetilde{g}_0$ and $\widetilde{g}_0^z$, g_0^z, $\widetilde{g}_1$, $\widetilde{g}_1^z$, g_1^z
  - compute signatures on base points g_i
  - create credentials containing arbitrary attributes.
- n attributes $\Rightarrow 2^{2n+1}$ users $\Rightarrow 2n+2$ users

The attack: many colliding users

$$h_3 = g_0^{c_0} \widetilde{g}_0^{d_0} g_1^{c_1} \widetilde{g}_1^{d_1}, \qquad h_4 = h_3^z$$

- 2 users can remove $\widetilde{g}_1$ from h_3 **and** $\widetilde{g}_1^z$ from h_4
- 8 users can:
  - compute $\widetilde{g}_0$ **and** $\widetilde{g}_0^z$, g_0^z, $\widetilde{g}_1$, $\widetilde{g}_1^z$, g_1^z
  - compute signatures on base points g_i
  - create credentials containing arbitrary attributes.
- n attributes $\Rightarrow 2^{2n+1}$ users $\Rightarrow 2n+2$ users

The attack: many colliding users

$$h_3 = g_0^{c_0} \widetilde{g}_0^{d_0} g_1^{c_1} \widetilde{g}_1^{d_1}, \qquad h_4 = h_3^z$$

- 2 users can remove $\widetilde{g}_1$ from h_3 **and** $\widetilde{g}_1^z$ from h_4
- 8 users can:
  - compute $\widetilde{g}_0$ **and** $\widetilde{g}_0^z$, g_0^z, $\widetilde{g}_1$, $\widetilde{g}_1^z$, g_1^z
  - compute signatures on base points g_i
  - create credentials containing arbitrary attributes.
- n attributes $\Rightarrow 2^{2n+1}$ users $\Rightarrow 2n+2$ users

The attack: many colliding users

$$h_3 = g_0^{c_0} \tilde{g}_0^{d_0} g_1^{c_1} \tilde{g}_1^{d_1}, \qquad h_4 = h_3^z$$

- 2 users can remove $\tilde{g}_1$ from h_3 **and** $\tilde{g}_1^z$ from h_4
- 8 users can:
  - compute $\tilde{g}_0$ **and** $\tilde{g}_0^z$, g_0^z, $\tilde{g}_1$, $\tilde{g}_1^z$, g_1^z
  - compute signatures on base points g_i
  - create credentials containing arbitrary attributes.
- n attributes $\Rightarrow 2^{2n+1}$ users $\Rightarrow 2n+2$ users

The attack: many colliding users

$$h_3 = g_0^{c_0}\tilde{g}_0^{d_0}g_1^{c_1}\tilde{g}_1^{d_1}, \qquad h_4 = h_3^z$$

- 2 users can remove $\tilde{g}_1$ from h_3 **and** $\tilde{g}_1^z$ from h_4
- 8 users can:
  - compute $\tilde{g}_0$ **and** $\tilde{g}_0^z$, g_0^z, $\tilde{g}_1$, $\tilde{g}_1^z$, g_1^z
  - compute signatures on base points g_i
  - create credentials containing arbitrary attributes.
- n attributes $\Rightarrow 2^{2n+1}$ users $\Rightarrow 2n + 2$ users

The attack: many colliding users

$$h_3 = g_0^{c_0} \widetilde{g}_0^{d_0} g_1^{c_1} \widetilde{g}_1^{d_1}, \qquad h_4 = h_3^z$$

- 2 users can remove $\widetilde{g}_1$ from h_3 **and** $\widetilde{g}_1^z$ from h_4
- 8 users can:
  - compute $\widetilde{g}_0$ **and** $\widetilde{g}_0^z$, g_0^z, $\widetilde{g}_1$, $\widetilde{g}_1^z$, g_1^z
  - compute signatures on base points g_i
  - create credentials containing arbitrary attributes.
- n attributes $\Rightarrow 2^{2n+1}$ users $\Rightarrow 2n+2$ users

Analysis

Ingredients of attack:

- Fixed base points $g_0, \ldots, g_n$
- Invertibility of exponents

Questions?

Analysis

Ingredients of attack:

- Fixed base points $g_0, \ldots, g_n$
- Invertibility of exponents

Questions?