An efficient self-blindable attribute-based credential scheme

Sietse Ringers, Eric Verheul, and Jaap-Henk Hoepman

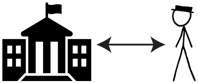
sringers@cs.ru.nl

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

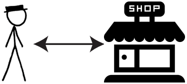
April 3, 2017
Financial Crypto, Malta

Attribute-based credential schemes

IssueCredential



ShowCredential



Credential

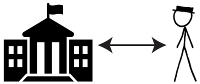
- Attributes $(k_1, \ldots, k_n)$
- Signature on attributes

$\Longleftrightarrow$

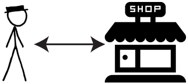
- Selective disclosure
- Efficient
- Unforgeable
- Unlinkable

Attribute-based credential schemes

IssueCredential



ShowCredential



Credential

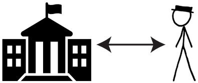
- Attributes $(k_1, \ldots, k_n)$
- Signature on attributes

$\Longleftrightarrow$

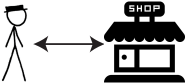
- Selective disclosure
- Efficient
- Unforgeable
- Unlinkable

Attribute-based credential schemes

IssueCredential



ShowCredential



Credential

- Attributes $(k_1, \ldots, k_n)$
- Signature on attributes

$\Longleftrightarrow$

- Selective disclosure
- Efficient
- Unforgeable
- Unlinkable

Credentials: attributes and signatures

- Bilinear pairing $e\colon G_1 \times G_2 \to G_T$ of prime order p
  - i.e. $e(P^a, Q) = e(P, Q^a) = e(P, Q)^a$ for all $P \in G_1,\ Q \in G_2$
- Issuer secret key: $a, a_1, \ldots, a_n, z \in_R \mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$

Issuer public key

$$Q, \quad A = Q^a, \quad A_i = Q^{a_i}, \quad Z = Q^z \in G_2$$

Attributes $(k_1, \ldots, k_n)$, signature $(\kappa, K, S, S_1, \ldots, S_n, T)$

- $\kappa \in_R \mathbb{Z}_p, \quad K \in_R G_1$
- $S = K^a, \quad S_i = K^{a_i} \in G_1$
- $T = C^z \in G_1$ where $C = KS^\kappa S_1^{k_1} \cdots S_n^{k_n}$

Credentials: attributes and signatures

- Bilinear pairing $e\colon G_1 \times G_2 \to G_T$ of prime order p
  - i.e. $e(P^a, Q) = e(P, Q^a) = e(P, Q)^a$ for all $P \in G_1,\ Q \in G_2$
- Issuer secret key: $a, a_1, \ldots, a_n, z \in_R \mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$

Issuer public key

$Q, \quad A = Q^a, \quad A_i = Q^{a_i}, \quad Z = Q^z \in G_2$

Attributes $(k_1, \ldots, k_n)$, signature $(\kappa, K, S, S_1, \ldots, S_n, T)$

- $\kappa \in_R \mathbb{Z}_p, \quad K \in_R G_1$
- $S = K^a, \quad S_i = K^{a_i} \in G_1$
- $T = C^z \in G_1$ where $C = KS^\kappa S_1^{k_1} \cdots S_n^{k_n}$

Credentials: attributes and signatures

- Bilinear pairing $e\colon G_1 \times G_2 \to G_T$ of prime order p
  - i.e. $e(P^a, Q) = e(P, Q^a) = e(P, Q)^a$ for all $P \in G_1,\ Q \in G_2$
- Issuer secret key: $a, a_1, \ldots, a_n, z \in_R \mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$

Issuer public key

$$Q, \quad A = Q^a, \quad A_i = Q^{a_i}, \quad Z = Q^z \in G_2$$

Attributes $(k_1, \ldots, k_n)$, signature $(\kappa, K, S, S_1, \ldots, S_n, T)$

- $\kappa \in_R \mathbb{Z}_p, \quad K \in_R G_1$
- $S = K^a, \quad S_i = K^{a_i} \in G_1$
- $T = C^z \in G_1$ where $C = KS^\kappa S_1^{k_1} \cdots S_n^{k_n}$

Credentials: attributes and signatures

- Bilinear pairing $e\colon G_1 \times G_2 \to G_T$ of prime order p
  - i.e. $e(P^a, Q) = e(P, Q^a) = e(P, Q)^a$ for all $P \in G_1,\ Q \in G_2$
- Issuer secret key: $a, a_1, \ldots, a_n, z \in_R \mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$

Issuer public key

$Q, \quad A = Q^a, \quad A_i = Q^{a_i}, \quad Z = Q^z \in G_2$

Attributes $(k_1, \ldots, k_n)$, signature $(\kappa, K, S, S_1, \ldots, S_n, T)$

- $\kappa \in_R \mathbb{Z}_p, \quad K \in_R G_1$
- $S = K^a, \quad S_i = K^{a_i} \in G_1$
- $T = C^z \in G_1$ where $C = KS^\kappa S_1^{k_1} \cdots S_n^{k_n}$

Credentials: attributes and signatures

- Bilinear pairing $e\colon G_1 \times G_2 \to G_T$ of prime order p
  - i.e. $e(P^a, Q) = e(P, Q^a) = e(P, Q)^a$ for all $P \in G_1,\ Q \in G_2$
- Issuer secret key: $a, a_1, \ldots, a_n, z \in_R \mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$

Issuer public key

$$Q, \quad A = Q^a, \quad A_i = Q^{a_i}, \quad Z = Q^z \in G_2$$

Attributes $(k_1, \ldots, k_n)$, signature $(\kappa, K, S, S_1, \ldots, S_n, T)$

- $\kappa \in_R \mathbb{Z}_p, \quad K \in_R G_1$
- $S = K^a, \quad S_i = K^{a_i} \in G_1$
- $T = C^z \in G_1$ where $C = KS^\kappa S_1^{k_1} \cdots S_n^{k_n}$

Credentials: attributes and signatures

- Bilinear pairing $e\colon G_1 \times G_2 \to G_T$ of prime order p
  - i.e. $e(P^a, Q) = e(P, Q^a) = e(P, Q)^a$ for all $P \in G_1,\ Q \in G_2$
- Issuer secret key: $a, a_1, \ldots, a_n, z \in_R \mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$

Issuer public key

$$Q, \quad A = Q^a, \quad A_i = Q^{a_i}, \quad Z = Q^z \in G_2$$

Attributes $(k_1, \ldots, k_n)$, signature $(\kappa, K, S, S_1, \ldots, S_n, T)$

- $\kappa \in_R \mathbb{Z}_p, \quad K \in_R G_1$
- $S = K^a, \quad S_i = K^{a_i} \in G_1$
- $T = C^z \in G_1$ where $C = KS^\kappa S_1^{k_1} \cdots S_n^{k_n}$

Credentials: attributes and signatures

- Bilinear pairing $e\colon G_1 \times G_2 \to G_T$ of prime order p
  - i.e. $e(P^a, Q) = e(P, Q^a) = e(P, Q)^a$ for all $P \in G_1,\ Q \in G_2$
- Issuer secret key: $a, a_1, \ldots, a_n, z \in_R \mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$

Issuer public key

$$Q, \quad A = Q^a, \quad A_i = Q^{a_i}, \quad Z = Q^z \in G_2$$

Attributes $(k_1, \ldots, k_n)$, signature $(\kappa, K, S, S_1, \ldots, S_n, T)$

- $\kappa \in_R \mathbb{Z}_p, \quad K \in_R G_1$
- $S = K^a, \quad S_i = K^{a_i} \in G_1$
- $T = C^z \in G_1$ where $C = KS^\kappa S_1^{k_1} \cdots S_n^{k_n}$

Credentials: attributes and signatures

Issuer public key

$Q, \quad A = Q^a, \quad A_i = Q^{a_i}, \quad Z = Q^z \in G_2$

Attributes $(k_1, \ldots, k_n)$, signature $(\kappa, K, S, S_1, \ldots, S_n, T)$

- $\kappa \in_R \mathbb{Z}_p, \quad K \in_R G_1$
- $S = K^a, \quad S_i = K^{a_i} \in G_1$
- $T = C^z \in G_1$ where $C = KS^\kappa S_1^{k_1} \cdots S_n^{k_n}$

Verification

- $e(K^a, Q) = e(S, Q) \stackrel{?}{=} e(K, A) = e(K, Q^a)$
- $e(S_i, Q) \stackrel{?}{=} e(K, A_i)$
- $e(T, Q) \stackrel{?}{=} e(KS^\kappa S_1^{k_1} \cdots S_n^{k_n}, Z)$

Credentials: attributes and signatures

Issuer public key

$$Q, \quad A = Q^a, \quad A_i = Q^{a_i}, \quad Z = Q^z \in G_2$$

Attributes $(k_1, \dots, k_n)$, signature $(\kappa, K, S, S_1, \dots, S_n, T)$

- $\kappa \in_R \mathbb{Z}_p, \quad K \in_R G_1$
- $S = K^a, \quad S_i = K^{a_i} \in G_1$
- $T = C^z \in G_1$ where $C = KS^\kappa S_1^{k_1} \cdots S_n^{k_n}$

Verification

- $e(K^a, Q) = e(S, Q) \stackrel{?}{=} e(K, A) = e(K, Q^a)$
- $e(S_i, Q) \stackrel{?}{=} e(K, A_i)$
- $e(T, Q) \stackrel{?}{=} e(KS^\kappa S_1^{k_1} \cdots S_n^{k_n}, Z)$

Credentials: attributes and signatures

Issuer public key

$$Q, \quad A = Q^a, \quad A_i = Q^{a_i}, \quad Z = Q^z \in G_2$$

Attributes $(k_1, \ldots, k_n)$, signature $(\kappa, K, S, S_1, \ldots, S_n, T)$

- $\kappa \in_R \mathbb{Z}_p, \quad K \in_R G_1$
- $S = K^a, \quad S_i = K^{a_i} \in G_1$
- $T = C^z \in G_1$ where $C = KS^\kappa S_1^{k_1} \cdots S_n^{k_n}$

Verification

- $e(K^a, Q) = e(S, Q) \stackrel{?}{=} e(K, A) = e(K, Q^a)$
- $e(S_i, Q) \stackrel{?}{=} e(K, A_i)$
- $e(T, Q) \stackrel{?}{=} e(KS^\kappa S_1^{k_1} \cdots S_n^{k_n}, Z)$

Credentials: attributes and signatures

Issuer public key

$Q, \quad A = Q^a, \quad A_i = Q^{a_i}, \quad Z = Q^z \in G_2$

Attributes $(k_1, \ldots, k_n)$, signature $(\kappa, K, S, S_1, \ldots, S_n, T)$

- $\kappa \in_R \mathbb{Z}_p, \quad K \in_R G_1$
- $S = K^a, \quad S_i = K^{a_i} \in G_1$
- $T = C^z \in G_1$ where $C = KS^\kappa S_1^{k_1} \cdots S_n^{k_n}$

Verification

- $e(K^a, Q) = e(S, Q) \stackrel{?}{=} e(K, A) = e(K, Q^a)$
- $e(S_i, Q) \stackrel{?}{=} e(K, A_i)$
- $e(T, Q) \stackrel{?}{=} e(KS^\kappa S_1^{k_1} \cdots S_n^{k_n}, Z)$

Showing a blinded credential $n = 3$

Credential (k_1, k_2, k_3), $(\kappa, K, S, S_1, S_2, S_3, T)$

- $S = K^a, \quad S_i = K^{a_i}, \quad C = KS^\kappa S_1^{k_1} S_2^{k_2} S_3^{k_3}, \quad T = C^z$

1: Blind the credential

Choose $\alpha, \beta \in_R \mathbb{Z}_p^*$

- Set $\bar{K} = K^\alpha, \quad \bar{S} = S^\alpha, \quad \bar{S}_i = S_i^\alpha$
- Set $\tilde{C} = (C^\alpha)^\beta, \quad \tilde{T} = (T^\alpha)^\beta$

Blinded credential

- $\bar{S} = \bar{K}^a$
- $\bar{S}_i = \bar{K}^{a_i}$
- $\tilde{T} = \tilde{C}^z$

2: show credential, disclosing k_2, k_3

- Send $(\bar{K}, \bar{S}, \bar{S}_1, \bar{S}_1, \bar{S}_2, \bar{S}_3)$, $(\tilde{C}, \tilde{T})$
- Both sides set $D = \bar{K} \bar{S}_2^{k_2} \bar{S}_3^{k_3}$
- Prove knowledge of β, κ, k_1 s.t.

$$\tilde{C}^{1/\beta} = D \bar{S}^\kappa \bar{S}_1^{k_1} = \bar{K} \bar{S}^\kappa \bar{S}_1^{k_1} \bar{S}_2^{k_2} \bar{S}_3^{k_3}$$

Showing a blinded credential $n = 3$

Credential (k_1, k_2, k_3), $(\kappa, K, S, S_1, S_2, S_3, T)$

- $S = K^a$, $S_i = K^{a_i}$, $C = KS^\kappa S_1^{k_1} S_2^{k_2} S_3^{k_3}$, $T = C^z$

1: Blind the credential

Choose $\alpha, \beta \in_R \mathbb{Z}_p^*$

- Set $\bar{K} = K^\alpha$, $\bar{S} = S^\alpha$, $\bar{S}_i = S_i^\alpha$
- Set $\tilde{C} = (C^\alpha)^\beta$, $\tilde{T} = (T^\alpha)^\beta$

Blinded credential

- $\bar{S} = \bar{K}^a$
- $\bar{S}_i = \bar{K}^{a_i}$
- $\tilde{T} = \tilde{C}^z$

2: show credential, disclosing k_2, k_3

- Send $(\bar{K}, \bar{S}, \bar{S}_1, \bar{S}_1, \bar{S}_2, \bar{S}_3)$, $(\tilde{C}, \tilde{T})$
- Both sides set $D = \bar{K}\bar{S}_2^{k_2}\bar{S}_3^{k_3}$
- Prove knowledge of β, κ, k_1 s.t.

$$\tilde{C}^{1/\beta} = D\bar{S}^\kappa \bar{S}_1^{k_1} = \bar{K}\bar{S}^\kappa \bar{S}_1^{k_1} \bar{S}_2^{k_2} \bar{S}_3^{k_3}$$

Showing a blinded credential $n = 3$

Credential (k_1, k_2, k_3), $(\kappa, K, S, S_1, S_2, S_3, T)$

- $S = K^a, \quad S_i = K^{a_i}, \quad C = KS^\kappa S_1^{k_1} S_2^{k_2} S_3^{k_3}, \quad T = C^z$

1: Blind the credential

Choose $\alpha, \beta \in_R \mathbb{Z}_p^*$

- Set $\bar{K} = K^\alpha, \quad \bar{S} = S^\alpha, \quad \bar{S}_i = S_i^\alpha$
- Set $\tilde{C} = (C^\alpha)^\beta, \quad \tilde{T} = (T^\alpha)^\beta$

Blinded credential

- $\bar{S} = \bar{K}^a$
- $\bar{S}_i = \bar{K}^{a_i}$
- $\tilde{T} = \tilde{C}^z$

2: show credential, disclosing k_2, k_3

- Send $(\bar{K}, \bar{S}, \bar{S}_1, \bar{S}_1, \bar{S}_2, \bar{S}_3)$, $(\tilde{C}, \tilde{T})$
- Both sides set $D = \bar{K} \bar{S}_2^{k_2} \bar{S}_3^{k_3}$
- Prove knowledge of β, κ, k_1 s.t.

$$\tilde{C}^{1/\beta} = D \bar{S}^\kappa \bar{S}_1^{k_1} = \bar{K} \bar{S}^\kappa \bar{S}_1^{k_1} \bar{S}_2^{k_2} \bar{S}_3^{k_3}$$

Showing a blinded credential $n = 3$

Credential (k_1, k_2, k_3), $(\kappa, K, S, S_1, S_2, S_3, T)$

- $S = K^a, \quad S_i = K^{a_i}, \quad C = KS^\kappa S_1^{k_1} S_2^{k_2} S_3^{k_3}, \quad T = C^z$

1: Blind the credential

Choose $\alpha, \beta \in_R \mathbb{Z}_p^*$

- Set $\bar{K} = K^\alpha, \quad \bar{S} = S^\alpha, \quad \bar{S}_i = S_i^\alpha$
- Set $\tilde{C} = (C^\alpha)^\beta, \quad \tilde{T} = (T^\alpha)^\beta$

Blinded credential

- $\bar{S} = \bar{K}^a$
- $\bar{S}_i = \bar{K}^{a_i}$
- $\tilde{T} = \tilde{C}^z$

2: show credential, disclosing k_2, k_3

- Send $(\bar{K}, \bar{S}, \bar{S}_1, \bar{S}_1, \bar{S}_2, \bar{S}_3)$, $(\tilde{C}, \tilde{T})$
- Both sides set $D = \bar{K}\bar{S}_2^{k_2}\bar{S}_3^{k_3}$
- Prove knowledge of β, κ, k_1 s.t.

$$\tilde{C}^{1/\beta} = D\bar{S}^\kappa \bar{S}_1^{k_1} = \bar{K}\bar{S}^\kappa \bar{S}_1^{k_1} \bar{S}_2^{k_2} \bar{S}_3^{k_3}$$

Showing a blinded credential $n = 3$

Credential $(k_1, k_2, k_3),\ (\kappa, K, S, S_1, S_2, S_3, T)$

- $S = K^a, \quad S_i = K^{a_i}, \quad C = KS^\kappa S_1^{k_1} S_2^{k_2} S_3^{k_3}, \quad T = C^z$

1: Blind the credential

Choose $\alpha, \beta \in_R \mathbb{Z}_p^*$

- Set $\bar{K} = K^\alpha, \quad \bar{S} = S^\alpha, \quad \bar{S}_i = S_i^\alpha$
- Set $\tilde{C} = (C^\alpha)^\beta, \quad \tilde{T} = (T^\alpha)^\beta$

Blinded credential

- $\bar{S} = \bar{K}^a$
- $\bar{S}_i = \bar{K}^{a_i}$
- $\tilde{T} = \tilde{C}^z$

2: show credential, disclosing k_2, k_3

- Send $(\bar{K}, \bar{S}, \bar{S}_1, \bar{S}_1, \bar{S}_2, \bar{S}_3),\ (\tilde{C}, \tilde{T})$
- Both sides set $D = \bar{K}\bar{S}_2^{k_2}\bar{S}_3^{k_3}$
- Prove knowledge of β, κ, k_1 s.t.

$$\tilde{C}^{1/\beta} = D\bar{S}^\kappa \bar{S}_1^{k_1} = \bar{K}\bar{S}^\kappa \bar{S}_1^{k_1}\bar{S}_2^{k_2}\bar{S}_3^{k_3}$$

Showing a blinded credential $n = 3$

Credential (k_1, k_2, k_3), $(\kappa, K, S, S_1, S_2, S_3, T)$

- $S = K^a, \quad S_i = K^{a_i}, \quad C = KS^\kappa S_1^{k_1} S_2^{k_2} S_3^{k_3}, \quad T = C^z$

1: Blind the credential

Choose $\alpha, \beta \in_R \mathbb{Z}_p^*$

- Set $\bar{K} = K^\alpha, \quad \bar{S} = S^\alpha, \quad \bar{S}_i = S_i^\alpha$
- Set $\tilde{C} = (C^\alpha)^\beta, \quad \tilde{T} = (T^\alpha)^\beta$

Blinded credential

- $\bar{S} = \bar{K}^a$
- $\bar{S}_i = \bar{K}^{a_i}$
- $\tilde{T} = \tilde{C}^z$

2: show credential, disclosing k_2, k_3

- Send $(\bar{K}, \bar{S}, \bar{S}_1, \bar{S}_1, \bar{S}_2, \bar{S}_3)$, $(\tilde{C}, \tilde{T})$
- Both sides set $D = \bar{K}\bar{S}_2^{k_2}\bar{S}_3^{k_3}$
- Prove knowledge of β, κ, k_1 s.t.

$$\tilde{C}^{1/\beta} = D\bar{S}^\kappa \bar{S}_1^{k_1} = \bar{K}\bar{S}^\kappa \bar{S}_1^{k_1} \bar{S}_2^{k_2} \bar{S}_3^{k_3}$$

Security

Theorem (Unlinkability)

The ShowCredential protocol is a zero-knowledge proof of knowledge for possession of a credential containing the disclosed attributes.

Theorem

Credentials are forgeable $\iff \exists$ *algorithm that can output tuples*

$$(\kappa, K, S, T) \quad \text{with} \quad S = K^a, \; T = (KS^\kappa)^z$$

with differing κ*'s, without knowing* a, z*, in polynomial-time.*

Theorem (Unforgeability)

Taking the LRSW assumption, our credential scheme is unforgeable.

Lysyanksaya, Rivest, Sahai, Wolf '99

Security

Theorem (Unlinkability)

The ShowCredential protocol is a zero-knowledge proof of knowledge for possession of a credential containing the disclosed attributes.

Theorem

Credentials are forgeable $\iff \exists$ *algorithm that can output tuples*

$$(\kappa, K, S, T) \quad \text{with} \quad S = K^a,\ T = (KS^\kappa)^z$$

with differing κ*'s, without knowing* a, z*, in polynomial-time.*

Theorem (Unforgeability)

Taking the LRSW assumption, our credential scheme is unforgeable.

Lysyanksaya, Rivest, Sahai, Wolf '99

Security

Theorem (Unlinkability)

The ShowCredential protocol is a zero-knowledge proof of knowledge for possession of a credential containing the disclosed attributes.

Theorem

Credentials are forgeable $\iff \exists$ *algorithm that can output tuples*

$$(\kappa, K, S, T) \quad \text{with} \quad S = K^a,\ T = (KS^\kappa)^z$$

with differing κ*'s, without knowing* a, z*, in polynomial-time.*

Theorem (Unforgeability)

Taking the LRSW assumption, our credential scheme is unforgeable.

Lysyanksaya, Rivest, Sahai, Wolf '99

Security

Theorem

Credentials are forgeable $\Longleftrightarrow \exists$ *algorithm that can output tuples*

$$(\kappa, K, S, T) \quad \text{with} \quad S = K^a,\ T = (KS^\kappa)^z$$

with differing κ*'s, without knowing* a, z*, in polynomial-time.*

Theorem (Unforgeability)

Taking the LRSW assumption, our credential scheme is unforgeable.

Lysyanksaya, Rivest, Sahai, Wolf '99

Known Exponent Assumption

Given G_1 and $P, P^a \in G_1$, the only way to output R, R^a is to take $r \in \mathbb{Z}_p$ and output $(P^r, (P^a)^r) \Rightarrow$ implies LRSW assumption.

Performance

Comparison of our scheme (254 bits) with Idemix (IRMA project, `www.irmacard.org`, 1024 bits $\rightsquigarrow$ 144 bits)

# attributes		prover		verifier	
total	discl.	This work	Idemix	This work	Idemix
6	1	2.9	11.7	5.7	11.2
9	1	3.4	14.3	8.0	14.0
12	1	4.2	17.1	10.2	16.9
6	5	2.1	7.6	5.9	9.2
9	8	2.4	7.4	7.9	10.7
12	11	2.8	7.5	9.9	12.0