Blind signatures, undeniable signatures

Why homomorphic properties can be interesting

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Blind signatures

Chaum, 1983

Alice can request signatures from Sam the signer and Sam should not know what he signs.

Blind signatures

Chaum, 1983

Alice can request signatures from Sam the signer and Sam should not know what he signs.

Typical application: eCash.
Sam is a bank, eCash is in the form of signed tokens.
Alice withdraws a token (expense charged to her account) by asking for a signature on a random serial number chosen by her.

Problem: This allows the bank to trace Alice's payment.

Blind signatures

Chaum, 1983

Alice can request signatures from Sam the signer and Sam should not know what he signs.

Typical application: eCash.
Sam is a bank, eCash is in the form of signed tokens.
Alice withdraws a token (expense charged to her account) by asking for a signature on a random serial number chosen by her.

Problem: This allows the bank to trace Alice's payment.

Solution: Use a homomorphic signature.

Blind signatures

Chaum, 1983

Alice can request signatures from Sam the signer and Sam should not know what he signs.

Typical application: eCash.
Sam is a bank, eCash is in the form of signed tokens.
Alice withdraws a token (expense charged to her account) by asking for a signature on a random serial number chosen by her.

Problem: This allows the bank to trace Alice's payment.

Solution: Use a homomorphic signature.

Details for RSA:
Sam has keypair $((n, d), (n, e))$. Signature on m is $m^d \bmod n$.

1. Alice picks blinding factor $0 < r < n$ with $\gcd(r, n) = 1$.
2. Asks for signature on $m' \equiv r^e \cdot m \bmod n$.

Blind signatures

Chaum, 1983

Alice can request signatures from Sam the signer and Sam should not know what he signs.

Typical application: eCash.
Sam is a bank, eCash is in the form of signed tokens.
Alice withdraws a token (expense charged to her account) by asking for a signature on a random serial number chosen by her.

Problem: This allows the bank to trace Alice's payment.

Solution: Use a homomorphic signature.

Details for RSA:
Sam has keypair $((n, d), (n, e))$. Signature on m is $m^d \bmod n$.

1. Alice picks blinding factor $0 < r < n$ with $\gcd(r, n) = 1$.
2. Asks for signature on $m' \equiv r^e \cdot m \bmod n$.
3. Upon receiving $s' \equiv (m')^d \equiv r \cdot m^d \bmod n$, computes $s \equiv s'/r \bmod n$, a valid signature on m.

Undeniable signature

Chaum and vn Antwerpen, 1989, Chaum 1990

Alice gives Bob a signed message, but Bob needs to interact with Alice to verify it.
Benefit for Alice: she can limit who gets to verify;
she can also prove that she did not produce a purported signature.

Make this acceptable to Bob by adding legal framework
(assume she signed if she refuses to cooperate).

Undeniable signature

Chaum and vn Antwerpen, 1989, Chaum 1990

Alice gives Bob a signed message, but Bob needs to interact with Alice to verify it.
Benefit for Alice: she can limit who gets to verify;
she can also prove that she did not produce a purported signature.

Make this acceptable to Bob by adding legal framework
(assume she signed if she refuses to cooperate).

Details for DLP-based scheme in group $G = \langle g \rangle$, $H : \{0,1\}^* \rightarrow G$.
Alice has keypair $(a, h_A = g^a)$. Signature on m is $s = (H(m))^a$.

Verification:

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.

Undeniable signature

Chaum and vn Antwerpen, 1989, Chaum 1990

Alice gives Bob a signed message, but Bob needs to interact with Alice to verify it.
Benefit for Alice: she can limit who gets to verify;
she can also prove that she did not produce a purported signature.

Make this acceptable to Bob by adding legal framework
(assume she signed if she refuses to cooperate).

Details for DLP-based scheme in group $G = \langle g \rangle$, $H : \{0,1\}^* \to G$.
Alice has keypair $(a, h_A = g^a)$. Signature on m is $s = (H(m))^a$.

Verification:

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.
3. Alice sends back $v = c^{a^{-1}}$, where a^{-1} is computed modulo $|G|$.

Undeniable signature

Chaum and vn Antwerpen, 1989, Chaum 1990

Alice gives Bob a signed message, but Bob needs to interact with Alice to verify it.
Benefit for Alice: she can limit who gets to verify;
she can also prove that she did not produce a purported signature.

Make this acceptable to Bob by adding legal framework
(assume she signed if she refuses to cooperate).

Details for DLP-based scheme in group $G = \langle g \rangle$, $H : \{0,1\}^* \to G$.
Alice has keypair $(a, h_A = g^a)$. Signature on m is $s = (H(m))^a$.

Verification:

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.
3. Alice sends back $v = c^{a^{-1}}$, where a^{-1} is computed modulo $|G|$.
4. Bob accepts the signature if $(H(m))^e g^f = v$.

Undeniable signature

Chaum and vn Antwerpen, 1989, Chaum 1990

Alice gives Bob a signed message, but Bob needs to interact with Alice to verify it.
Benefit for Alice: she can limit who gets to verify;
she can also prove that she did not produce a purported signature.

Make this acceptable to Bob by adding legal framework (assume she signed if she refuses to cooperate).

Details for DLP-based scheme in group $G = \langle g \rangle$, $H : \{0,1\}^* \rightarrow G$.
Alice has keypair $(a, h_A = g^a)$. Signature on m is $s = (H(m))^a$.

Verification:

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.
3. Alice sends back $v = c^{a^{-1}}$, where a^{-1} is computed modulo $|G|$.
4. Bob accepts the signature if $(H(m))^e g^f = v$.

A valid transcript is accepted because

$$v = c^{a^{-1}} = (s^e h_A^f)^{a^{-1}}$$

Undeniable signature

Chaum and vn Antwerpen, 1989, Chaum 1990

Alice gives Bob a signed message, but Bob needs to interact with Alice to verify it.
Benefit for Alice: she can limit who gets to verify;
she can also prove that she did not produce a purported signature.

Make this acceptable to Bob by adding legal framework
(assume she signed if she refuses to cooperate).

Details for DLP-based scheme in group $G = \langle g \rangle$, $H : \{0,1\}^* \to G$.
Alice has keypair $(a, h_A = g^a)$. Signature on m is $s = (H(m))^a$.

Verification:

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.
3. Alice sends back $v = c^{a^{-1}}$, where a^{-1} is computed modulo $|G|$.
4. Bob accepts the signature if $(H(m))^e g^f = v$.

A valid transcript is accepted because

$$v = c^{a^{-1}} = (s^e h_A^f)^{a^{-1}} = ((H(m))^{ae} g^{af})^{a^{-1}} = (H(m))^e g^f.$$

Undeniable signature

Chaum and vn Antwerpen, 1989, Chaum 1990

Alice gives Bob a signed message, but Bob needs to interact with Alice to verify it.
Benefit for Alice: she can limit who gets to verify;
she can also prove that she did not produce a purported signature.

Make this acceptable to Bob by adding legal framework
(assume she signed if she refuses to cooperate).

Details for DLP-based scheme in group $G = \langle g \rangle$, $H : \{0,1\}^* \to G$.
Alice has keypair $(a, h_A = g^a)$. Signature on m is $s = (H(m))^a$.

Verification:

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.
3. Alice sends back $v = c^{a^{-1}}$, where a^{-1} is computed modulo $|G|$.
4. Bob accepts the signature if $(H(m))^e g^f = v$.

A valid transcript is accepted because

$$v = c^{a^{-1}} = (s^e h_A^f)^{a^{-1}} = ((H(m))^{ae} g^{af})^{a^{-1}} = (H(m))^e g^f.$$

Bob does not learn any information on a: he can compute v anyways.

Undeniable signature – example

Chaum and vn Antwerpen, 1989, Chaum 1990

Details for DLP-based scheme in group $G = \langle g \rangle$, $H : \{0,1\}^* \to G$.
Alice has keypair $(a, h_A = g^a)$. Signature on m is $s = (H(m))^a$.

Verification:

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.
3. Alice sends back $v = c^{a^{-1}}$.
4. Bob accepts the signature if $(H(m))^e g^f = v$.

Use $g = 2 \in \mathbb{F}_{23}$, $|G| = 11$.
$a = 9$, thus $h_A = 2^9 \equiv 6 \bmod 23, 9^{-1} \equiv 5 \bmod 11$.
Assume $H(m) = 15$.

Undeniable signature – example

Chaum and vn Antwerpen, 1989, Chaum 1990

Details for DLP-based scheme in group $G = \langle g \rangle$, $H : \{0,1\}^* \to G$.
Alice has keypair $(a, h_A = g^a)$. Signature on m is $s = (H(m))^a$.

Verification:

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.
3. Alice sends back $v = c^{a^{-1}}$.
4. Bob accepts the signature if $(H(m))^e g^f = v$.

Use $g = 2 \in \mathbb{F}_{23}$, $|G| = 11$.
$a = 9$, thus $h_A = 2^9 \equiv 6 \bmod 23, 9^{-1} \equiv 5 \bmod 11$.
Assume $H(m) = 15$. Then $s = 15^9 \equiv 14 \bmod 23$.

1. Bob picks $e = 2, f = 3$.
2. Computes and sends challenge $c = s^e h_A^f = 14^2 \cdot 6^3 \equiv 16 \bmod 23$.

Undeniable signature – example

Chaum and vn Antwerpen, 1989, Chaum 1990

Details for DLP-based scheme in group $G = \langle g \rangle$, $H : \{0,1\}^* \to G$.
Alice has keypair $(a, h_A = g^a)$. Signature on m is $s = (H(m))^a$.

Verification:

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.
3. Alice sends back $v = c^{a^{-1}}$.
4. Bob accepts the signature if $(H(m))^e g^f = v$.

Use $g = 2 \in \mathbb{F}_{23}$, $|G| = 11$.
$a = 9$, thus $h_A = 2^9 \equiv 6 \bmod 23, 9^{-1} \equiv 5 \bmod 11$.
Assume $H(m) = 15$. Then $s = 15^9 \equiv 14 \bmod 23$.

1. Bob picks $e = 2, f = 3$.
2. Computes and sends challenge $c = s^e h_A^f = 14^2 \cdot 6^3 \equiv 16 \bmod 23$.
3. Alice sends back $v = c^{a^{-1}} = 16^5 \equiv 6 \bmod 23$.
4. Bob accepts the signature if $(H(m))^e g^f = 15^2 \cdot 2^3 \equiv 6 \bmod 23$ matches $v = 6$.

Undeniable signature – example

Chaum and vn Antwerpen, 1989, Chaum 1990

Details for DLP-based scheme in group $G = \langle g \rangle$, $H : \{0,1\}^* \to G$.
Alice has keypair $(a, h_A = g^a)$. Signature on m is $s = (H(m))^a$.

Verification:

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.
3. Alice sends back $v = c^{a^{-1}}$.
4. Bob accepts the signature if $(H(m))^e g^f = v$.

Use $g = 2 \in \mathbb{F}_{23}$, $|G| = 11$.
$a = 9$, thus $h_A = 2^9 \equiv 6 \bmod 23, 9^{-1} \equiv 5 \bmod 11$.
Assume $H(m) = 15$. Then $s = 15^9 \equiv 14 \bmod 23$.

1. Bob picks $e = 2, f = 3$.
2. Computes and sends challenge $c = s^e h_A^f = 14^2 \cdot 6^3 \equiv 16 \bmod 23$.
3. Alice sends back $v = c^{a^{-1}} = 16^5 \equiv 6 \bmod 23$.
4. Bob accepts the signature if $(H(m))^e g^f = 15^2 \cdot 2^3 \equiv 6 \bmod 23$ matches $v = 6$. Worked.

Undeniable signature – disavowal

Chaum and vn Antwerpen, 1989, Chaum 1990

If Alice did not produce s, i.e., $s \neq (H(m))^a$, then verification fails

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.
3. Alice sends back $v = c^{a^{-1}}$.
4. Bob accepts the signature if $(H(m))^e g^f = v$.

To check whether Alice answers consistently using the correct a^{-1} Bob does a second round, with new random choices r, t.

Bob then has (for an honest Alice):
$v_1 = c_1^{a^{-1}} = (s^e h_A^f)^{a^{-1}} = s^{e \cdot a^{-1}} g^f$
$v_2 = c_2^{a^{-1}} = (s^r h_A^t)^{a^{-1}} = s^{r \cdot a^{-1}} g^t$

Undeniable signature – disavowal

Chaum and vn Antwerpen, 1989, Chaum 1990

If Alice did not produce s, i.e., $s \neq (H(m))^a$, then verification fails

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.
3. Alice sends back $v = c^{a^{-1}}$.
4. Bob accepts the signature if $(H(m))^e g^f = v$.

To check whether Alice answers consistently using the correct a^{-1} Bob does a second round, with new random choices r, t.

Bob then has (for an honest Alice):
$v_1 = c_1^{a^{-1}} = (s^e h_A^f)^{a^{-1}} = s^{e \cdot a^{-1}} g^f$
$v_2 = c_2^{a^{-1}} = (s^r h_A^t)^{a^{-1}} = s^{r \cdot a^{-1}} g^t$

Thus

$(v_1 g^{-f})^r$

Undeniable signature – disavowal

Chaum and vn Antwerpen, 1989, Chaum 1990

If Alice did not produce s, i.e., $s \neq (H(m))^a$, then verification fails

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.
3. Alice sends back $v = c^{a^{-1}}$.
4. Bob accepts the signature if $(H(m))^e g^f = v$.

To check whether Alice answers consistently using the correct a^{-1} Bob does a second round, with new random choices r, t.

Bob then has (for an honest Alice):
$v_1 = c_1^{a^{-1}} = (s^e h_A^f)^{a^{-1}} = s^{e \cdot a^{-1}} g^f$
$v_2 = c_2^{a^{-1}} = (s^r h_A^t)^{a^{-1}} = s^{r \cdot a^{-1}} g^t$

Thus

$$(v_1 g^{-f})^r = (s^{e \cdot a^{-1}} g^f g^{-f})^r = (s^{e \cdot a^{-1}})^r$$

Undeniable signature – disavowal

Chaum and vn Antwerpen, 1989, Chaum 1990

If Alice did not produce s, i.e., $s \neq (H(m))^a$, then verification fails

1. Bob picks $e, f \in [1, |G| - 1]$.
2. Computes and sends challenge $c = s^e h_A^f$ to Alice.
3. Alice sends back $v = c^{a^{-1}}$.
4. Bob accepts the signature if $(H(m))^e g^f = v$.

To check whether Alice answers consistently using the correct a^{-1} Bob does a second round, with new random choices r, t.

Bob then has (for an honest Alice):
$v_1 = c_1^{a^{-1}} = (s^e h_A^f)^{a^{-1}} = s^{e \cdot a^{-1}} g^f$
$v_2 = c_2^{a^{-1}} = (s^r h_A^t)^{a^{-1}} = s^{r \cdot a^{-1}} g^t$

Thus

$$(v_1 g^{-f})^r = (s^{e \cdot a^{-1}} g^f g^{-f})^r = (s^{e \cdot a^{-1}})^r = (s^{r \cdot a^{-1}})^e = (s^{r \cdot a^{-1}} g^t g^{-t})^e = (v_2 g^{-t})^e$$

So accept disavowal (Alice did not sign) if $(v_1 g^{-f})^r = (v_2 g^{-t})^e$.