Fair Blind Signatures without Random Oracles

Georg Fuchsbauer Damien Vergnaud

École normale supérieure

AFRICACRYPT, 3.5.2010

Our Contributions

Model

- Strengthening of the security model
- Security against *active* adversaries

Our Contributions

Model

- Strengthening of the security model
- Security against *active* adversaries

Construction

- First construction w/o random oracles
- Satisfying strong model
- Using automorphic signatures and Groth-Sahai proofs

1. Fair Blind Signatures: The Model

2. Building Blocks

1. Overview of Construction

Blind Signatures: Algorithms

Blind signatures allow a user to obtain from a signer a signature on a message *hidden to the signer*
A user cannot obtain more signatures than those issued by the signer

(Setup, IKGen, Sign, User, Ver)

Blind Signatures: Algorithms

Blind signatures allow a user to obtain from a signer a signature on a message *hidden to the signer*
A user cannot obtain more signatures than those issued by the signer

$$(\texttt{Setup}, \texttt{IKGen}, \texttt{Sign}, \texttt{User}, \texttt{Ver})$$

$\texttt{Setup}$ outputs the public parameters pp

$\texttt{IKGen}$ outputs a key pair (ipk, isk) for the signer/issuer

$\texttt{Sign}, \texttt{User}$ are interactive algorithms

$$\text{accept/reject} \leftarrow \texttt{Sign}(pp, isk) \leftrightarrow \texttt{User}(pp, ipk, msg) \rightarrow \sigma/\emptyset$$

$\texttt{Ver}$ verifies a signature: $\texttt{Ver}(pp, ipk, msg, \sigma) \rightarrow \text{accept/reject}$

Blind Signatures: Security

Blindness

- $\mathcal{A}$ gets the issuer's key pair and outputs two messages
- Challenger simulates `User` with $\mathcal{A}$ on both messages *in random order* gives the adversary the resulting signatures
- $\mathcal{A}$ has to guess the order

Blind Signatures: Security

Blindness

- $\mathcal{A}$ gets the issuer's key pair and outputs two messages
- Challenger simulates `User` with $\mathcal{A}$ on both messages *in random order* gives the adversary the resulting signatures
- $\mathcal{A}$ has to guess the order

One-More Unforgeability

- $\mathcal{A}$ interacts q times with challenger which simulates `Sign`
- $\mathcal{A}$ wins if it outputs $q+1$ signatures on different messages

Fair Blind Signatures: Algorithms

Fair blind signatures allow an authority to *revoke anonymity*

- link issuing session to the resulting signature
- trace signature to user who requested it

$$(\texttt{Setup}, \texttt{IKGen}, \underline{\texttt{UKGen}}, \texttt{Sign}, \texttt{User}, \texttt{Ver}, \underline{\texttt{TrSig}}, \underline{\texttt{TrId}}, \underline{\texttt{ChkSig}}, \underline{\texttt{ChkId}})$$

Fair Blind Signatures: Algorithms

Fair blind signatures allow an authority to *revoke anonymity*

- link issuing session to the resulting signature
- trace signature to user who requested it

$$(\texttt{Setup}, \texttt{IKGen}, \underline{\texttt{UKGen}}, \texttt{Sign}, \texttt{User}, \texttt{Ver}, \underline{\texttt{TrSig}}, \underline{\texttt{TrId}}, \underline{\texttt{ChkSig}}, \underline{\texttt{ChkId}})$$

`Setup` besides pp outputs the *revocation key* rk for the authority

`UKGen` outputs a key pair (upk, usk) for the user

`TrSig` on input rk, transcript $trans$, outputs (id, π)

`ChkSig` on input $trans, \sigma, id, \pi$, output accept/reject

`TrId` on input rk, signature σ, outputs (upk, π)

`ChkId` on input σ, upk, π, output accept/reject

Fair Blind Signatures: Algorithms

Fair blind signatures allow an authority to *revoke anonymity*

- link issuing session to the resulting signature
- trace signature to user who requested it

(Setup, IKGen, UKGen, Sign, User, Ver, TrSig, TrId, ChkSig, ChkId)

Setup besides pp outputs the *revocation key* rk for the authority

UKGen outputs a key pair (upk, usk) for the user

TrSig on input rk, transcript $trans$, outputs (id, π)

ChkSig on input $trans, \sigma, id, \pi$, output accept/reject

TrId on input rk, signature σ, outputs (upk, π)

ChkId on input σ, upk, π, output accept/reject

Fair Blind Signatures: Security I

Blindness

Not even issuer with *tracing oracles* can link a msg/σ pair to issuing

Identity Traceability

No coalition of users & authority can produce signature which cannot be linked to a user identity

Fair Blind Signatures: Security I

Blindness

Not even issuer with *tracing oracles* can link a msg/σ pair to issuing

Identity Traceability

No coalition of users & authority can produce signature which cannot be linked to a user identity

Identity Non-Frameability

No coalition of issuer, users & authority can produce signature and proof that signature opens to honest user who did not ask for the signature

Fair Blind Signatures: Security I

Blindness

Not even issuer with *tracing oracles* can link a msg/σ pair to issuing

Identity Traceability

No coalition of users & authority can produce signature which cannot be linked to a user identity

Identity Non-Frameability

No coalition of issuer, users & authority can produce signature and proof that signature opens to honest user who did not ask for the signature

Fair Blind Signatures: Security II

Signature Traceability

No coalition of users & authority can produce a signature which is not traced by any issuing transcript

Signature Non-Frameability

No coalition of issuer, users & authority can produce a transcript which wrongfully opens to honest signature

Fair Blind Signatures: Security II

Signature Traceability

No coalition of users & authority can produce a signature which is not traced by any issuing transcript

Signature Non-Frameability

No coalition of issuer, users & authority can produce a transcript which wrongfully opens to honest signature

Differences to the Previous Model

[HT07] defined first formal model. We give stronger version

Blindness

Malicious issuer cannot *interact* with user.

HT07 $\mathcal{A}$ gets *isk*, outputs two users, a message, gets signature
$\Rightarrow$ honest-but-curious issuer

Ours $\mathcal{A}$ outpus U_1, m_1, U_2, m_2, challenger simulates `User` as U_b for m_b, then as U_{b-1} for m_{b-1}; gives signatures to $\mathcal{A}$

Differences to the Previous Model

[HT07] defined first formal model. We give stronger version

Blindness

Malicious issuer cannot *interact* with user.

HT07 $\mathcal{A}$ gets *isk*, outputs two users, a message, gets signature
$\Rightarrow$ honest-but-curious issuer

Ours $\mathcal{A}$ outpus U_1, m_1, U_2, m_2, challenger simulates `User` as U_b for m_b, then as U_{b-1} for m_{b-1}; gives signatures to $\mathcal{A}$

Identity non-frameability

HT07 $\mathcal{A}$ gets *rk*, outputs σ, opened by *challenger*; $\mathcal{A}$ wins if framed honest user $\Rightarrow$ honest-but-curious authority

Ours $\mathcal{A}$ outputs *msg*, σ, user, π;
wins if σ and π valid and user never asked for signature on *msg*

Differences to the Previous Model

[HT07] defined first formal model. We give stronger version

Identity non-frameability

HT07 $\mathcal{A}$ gets rk, outputs σ, opened by *challenger*; $\mathcal{A}$ wins if framed honest user $\Rightarrow$ honest-but-curious authority

Ours $\mathcal{A}$ outputs msg, σ, user, π;
wins if σ and π valid and user never asked for signature on msg

Signature non-frameability

Analogously to identity non-frameability
$\mathcal{A}$ must output a proof which the challenger verifies instead of producing it

1 Fair Blind Signatures: The Model

2 Building Blocks

1 Overview of Construction

Round-Optimal Blind Signatures

Round-Optimal: User sends one message, issuer sends one message

Fischlin's generic construction [Fis06]

In the common-reference string (CRS) model

- User sends (extractable) commitment to message to signer
- Signer sends signature on commitment
- Blind signature:
  - encryption of commitment to message
  - encryption of signature
  - non-interactive zero-knowledge proof (NIZK) that
    - encryptions contain valid signature/message pair
    - encrypted commitment opens to message

Round-Optimal Blind Signatures

Round-Optimal: User sends one message, issuer sends one message

Fischlin's generic construction [Fis06]

In the common-reference string (CRS) model

- User sends (extractable) commitment to message to signer
- Signer sends signature on commitment
- Blind signature:
  - encryption of commitment to message
  - encryption of signature
  - non-interactive zero-knowledge proof (NIZK) that
    - encryptions contain valid signature/message pair
    - encrypted commitment opens to message

[AO09] suggest to use Groth-Sahai witness-indistinguishable proofs instead of NIZK, but no compatible efficient signature scheme

Bilinear Groups and SXDH

- Bilinear group: $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G_1, G_2)$
  - $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ cyclic groups of prime order p
  - $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ bilinear, i.e. $\forall X \in \mathbb{G}_1, \forall Y \in \mathbb{G}_2, \forall a, b \in \mathbb{Z}$: $e(X^a, Y^b) = e(X, Y)^{ab}$
  - $\mathbb{G}_1 = \langle G_1 \rangle$, $\mathbb{G}_2 = \langle G_2 \rangle$, $\mathbb{G}_T = \langle e(G_1, G_2) \rangle$

Bilinear Groups and SXDH

- Bilinear group: $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G_1, G_2)$
  - $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ cyclic groups of prime order p
  - $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ bilinear, i.e. $\forall X \in \mathbb{G}_1, \forall Y \in \mathbb{G}_2, \forall a, b \in \mathbb{Z}$: $e(X^a, Y^b) = e(X, Y)^{ab}$
  - $\mathbb{G}_1 = \langle G_1 \rangle$, $\mathbb{G}_2 = \langle G_2 \rangle$, $\mathbb{G}_T = \langle e(G_1, G_2) \rangle$
- SXDH: for $i = 1, 2$:
  given $(G_i, G_i^a, G_i^b, G_i^c)$ it is hard to decide whether $c = ab$.

Bilinear Groups and SXDH

- Bilinear group: $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G_1, G_2)$
  - $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ cyclic groups of prime order p
  - $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ bilinear, i.e. $\forall X \in \mathbb{G}_1, \forall Y \in \mathbb{G}_2, \forall a, b \in \mathbb{Z}$: $e(X^a, Y^b) = e(X, Y)^{ab}$
  - $\mathbb{G}_1 = \langle G_1 \rangle$, $\mathbb{G}_2 = \langle G_2 \rangle$, $\mathbb{G}_T = \langle e(G_1, G_2) \rangle$
- SXDH: for $i = 1, 2$:
  given $(G_i, G_i^a, G_i^b, G_i^c)$ it is hard to decide whether $c = ab$.

Pairing-product equation over variables $X_1, \ldots, X_m \in \mathbb{G}_1$, $Y_1, \ldots, Y_n \in \mathbb{G}_2$

$$\prod_{i=1}^{n} e(A_i, Y_i) \prod_{i=1}^{m} e(X_i, B_i) \prod_{i=1}^{m} \prod_{j=1}^{n} e(X_i, Y_j)^{\gamma_{i,j}} = t_T \,, \qquad \text{(E)}$$

determined by $A_i \in \mathbb{G}_1, B_i \in \mathbb{G}_2$, $\gamma_{i,j} \in \mathbb{Z}_p$ and $t_T \in \mathbb{G}_T$

Bilinear Groups and SXDH

- Bilinear group: $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G_1, G_2)$
  - $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ cyclic groups of prime order p
  - $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ bilinear, i.e. $\forall X \in \mathbb{G}_1, \forall Y \in \mathbb{G}_2, \forall a, b \in \mathbb{Z}$: $e(X^a, Y^b) = e(X, Y)^{ab}$
  - $\mathbb{G}_1 = \langle G_1 \rangle$, $\mathbb{G}_2 = \langle G_2 \rangle$, $\mathbb{G}_T = \langle e(G_1, G_2) \rangle$
- SXDH: for $i = 1, 2$:
  given $(G_i, G_i^a, G_i^b, G_i^c)$ it is hard to decide whether $c = ab$.

Pairing-product equation over variables $X_1, \ldots, X_m \in \mathbb{G}_1$, $Y_1, \ldots, Y_n \in \mathbb{G}_2$

$$\prod_{i=1}^{n} e(A_i, Y_i) \prod_{i=1}^{m} e(X_i, B_i) \prod_{i=1}^{m} \prod_{j=1}^{n} e(X_i, Y_j)^{\gamma_{i,j}} = t_T \,, \qquad \text{(E)}$$

determined by $A_i \in \mathbb{G}_1, B_i \in \mathbb{G}_2$, $\gamma_{i,j} \in \mathbb{Z}_p$ and $t_T \in \mathbb{G}_T$

Groth, Sahai: NIWI proof of knowledge for *satisfiability* of PPE

Automorphic Signatures: Motivation

To instantiate generic construction, we need signature scheme s.t.

- messages are group elements
- signatures are group elements
- verification by PPE
- EUF-CMA

Automorphic Signatures: Motivation

To instantiate generic construction, we need signature scheme s.t.

- messages are group elements
- signatures are group elements
- verification by PPE
- EUF-CMA

Automorphic Signatures: Motivation

To instantiate generic construction, we need signature scheme s.t.

- messages are group elements
- signatures are group elements
- verification by PPE
- EUF-CMA

Automorphic Signatures: Motivation

To instantiate generic construction, we need signature scheme s.t.

- messages are group elements
- signatures are group elements
- verification by PPE
- EUF-CMA

Automorphic Signatures: Motivation

To instantiate generic construction, we need signature scheme s.t.

- messages are group elements
- signatures are group elements
- verification by PPE
- EUF-CMA

Automorphic Signatures: Motivation

To instantiate generic construction, we need signature scheme s.t.

- messages are group elements
- signatures are group elements
- verification by PPE
- EUF-CMA

F: Automorphic Signatures in Bilinear Groups, eprint 2009/320

- satisfy requirements
  additionally: verification keys lie in the message space

Automorphic Signatures: Instantiation

- Setup: given bilinear group, choose $G, K, F, T \leftarrow \mathbb{G}_1$, $H \leftarrow \mathbb{G}_2$
  Message space: $\mathcal{DH} := \{(G^m, H^m) \,|\, m \in \mathbb{Z}_p\}$,

Automorphic Signatures: Instantiation

- `Setup`: given bilinear group, choose $G, K, F, T \leftarrow \mathbb{G}_1$, $H \leftarrow \mathbb{G}_2$
  Message space: $\mathcal{DH} := \{(G^m, H^m) \mid m \in \mathbb{Z}_p\}$,
- `KeyGen`: secret key $x \leftarrow \mathbb{Z}_p$, public key $(X := G^x, Y := H^x)$

Automorphic Signatures: Instantiation

- Setup: given bilinear group, choose $G, K, F, T \leftarrow \mathbb{G}_1$, $H \leftarrow \mathbb{G}_2$
  Message space: $\mathcal{DH} := \{(G^m, H^m) \mid m \in \mathbb{Z}_p\}$,
- KeyGen: secret key $x \leftarrow \mathbb{Z}_p$, public key $(X := G^x, Y := H^x)$
- Sign$(x, (M, N))$: choose $c, r \leftarrow \mathbb{Z}_p$, return

$$A := (K \cdot T^r \cdot M)^{\frac{1}{x+c}} \qquad C := F^c \qquad D := H^c$$
$$R := G^r \qquad S := H^r$$

Automorphic Signatures: Instantiation

- `Setup`: given bilinear group, choose $G, K, F, T \leftarrow \mathbb{G}_1$, $H \leftarrow \mathbb{G}_2$
  Message space: $\mathcal{DH} := \{(G^m, H^m) \mid m \in \mathbb{Z}_p\}$,
- `KeyGen`: secret key $x \leftarrow \mathbb{Z}_p$, public key $(X := G^x, Y := H^x)$
- `Sign`$(x, (M, N))$: choose $c, r \leftarrow \mathbb{Z}_p$, return

$$A := (K \cdot T^r \cdot M)^{\frac{1}{x+c}} \qquad C := F^c \qquad D := H^c$$
$$R := G^r \qquad S := H^r$$

- `Ver`$((X, Y), (M, N), (A, C, D, R, S)$ for $(M, N) \in \mathcal{DH}$ return 1 if

$$e(A, Y \cdot D) = e(K \cdot M, H)\ e(T, S) \qquad e(C, H) = e(F, D)$$
$$e(R, H) = e(G, S)$$

Round-Optimal Blind Signatures: Instantiation

Automorphic signatures yield first efficient instantiation of

Round-Optimal Blind Signatures

Round-Optimal Blind Signatures: Instantiation

Automorphic signatures yield first efficient instantiation of

Round-Optimal Blind Signatures

- User: given $(M, N) \in \mathcal{DH}$, choose $\rho \leftarrow \mathbb{Z}_p$, send

$$U := T^{\rho} \cdot M, \quad \texttt{GSPoK}[(M, N, G^{\rho}, H^{\rho}) : U = T^{\rho} \cdot M]$$

Round-Optimal Blind Signatures: Instantiation

Automorphic signatures yield first efficient instantiation of

Round-Optimal Blind Signatures

- User: given $(M, N) \in \mathcal{DH}$, choose $\rho \leftarrow \mathbb{Z}_p$, send

$$U := T^{\rho} \cdot M, \quad \texttt{GSPoK}[(M, N, G^{\rho}, H^{\rho}) : U = T^{\rho} \cdot M]$$

- Signer: choose $c, r \leftarrow \mathbb{Z}_p$, send

$$A := (K \cdot T^{r} \cdot U)^{\frac{1}{x+c}} \qquad C := F^{c} \qquad D := H^{c}$$
$$R' := G^{r} \qquad S' := H^{r}$$

Round-Optimal Blind Signatures: Instantiation

Automorphic signatures yield first efficient instantiation of

Round-Optimal Blind Signatures

- User: given $(M, N) \in \mathcal{DH}$, choose $\rho \leftarrow \mathbb{Z}_p$, send

$$U := T^{\rho} \cdot M, \quad \texttt{GSPoK}[(M, N, G^{\rho}, H^{\rho}) : U = T^{\rho} \cdot M]$$

- Signer: choose $c, r \leftarrow \mathbb{Z}_p$, send

$$A := (K \cdot \underbrace{T^{r} \cdot U}_{=T^{r+\rho} \cdot M})^{\frac{1}{x+c}}$$

$$C := F^{c} \qquad D := H^{c}$$

$$R' := G^{r} \qquad S' := H^{r}$$

Round-Optimal Blind Signatures: Instantiation

Automorphic signatures yield first efficient instantiation of

Round-Optimal Blind Signatures

- User: given $(M, N) \in \mathcal{DH}$, choose $\rho \leftarrow \mathbb{Z}_p$, send

$$U := T^{\rho} \cdot M, \quad \texttt{GSPoK}[(M, N, G^{\rho}, H^{\rho}) : U = T^{\rho} \cdot M]$$

- Signer: choose $c, r \leftarrow \mathbb{Z}_p$, send

$$A := (K \cdot \underbrace{T^{r} \cdot U}_{= T^{r+\rho} \cdot M})^{\frac{1}{x+c}}$$

$$C := F^{c} \qquad D := H^{c}$$

$$R' := G^{r} \qquad S' := H^{r}$$

- User: set $R := R' \cdot G^{\rho} = G^{r+\rho}$,
  $S := S' \cdot H^{\rho} = H^{r+\rho}$,

$$\Sigma := \texttt{GSPoK}[(A, C, D, R, S) : \texttt{Verify}(vk, (M, N), (A, C, D, R, S)) = 1]$$

1. Fair Blind Signatures: The Model

2. Building Blocks

1. Overview of Construction

Modifications to Automorphic Blind Signatures

- Users have own pairs of verification/signing key

Modifications to Automorphic Blind Signatures

- Users have own pairs of verification/signing key
- Issuer (blindly) signs: message, user public key, identifier

Modifications to Automorphic Blind Signatures

- Users have own pairs of verification/signing key
- Issuer (blindly) signs: message, user public key, identifier
- Identifier is jointly computed and extractable from transcript

$\Rightarrow$ Traceability of signatures from transcripts

Modifications to Automorphic Blind Signatures

- Users have own pairs of verification/signing key
- Issuer (blindly) signs: message, user public key, identifier
- Identifier is jointly computed and extractable from transcript

$\Rightarrow$ Traceability of signatures from transcripts

- Blind signature contains committed user public key

$\Rightarrow$ Traceability of users from signatures

Modifications to Automorphic Blind Signatures

- Users have own pairs of verification/signing key
- Issuer (blindly) signs: message, user public key, identifier
- Identifier is jointly computed and extractable from transcript

$\Rightarrow$ Traceability of signatures from transcripts

- Blind signature contains committed user public key

$\Rightarrow$ Traceability of users from signatures

- User signs her message during issuing
  signs blind signature and proves knowledge of it

$\Rightarrow$ Non-frameable proofs of correct tracing

Modifications to Automorphic Blind Signatures

- Users have own pairs of verification/signing key
- Issuer (blindly) signs: message, user public key, identifier
- Identifier is jointly computed and extractable from transcript

$\Rightarrow$ Traceability of signatures from transcripts

- Blind signature contains committed user public key

$\Rightarrow$ Traceability of users from signatures

- User signs her message during issuing
  signs blind signature and proves knowledge of it

$\Rightarrow$ Non-frameable proofs of correct tracing

- Blind signature contains additional encryptions of tracing information

$\Rightarrow$ Anonymity against adversaries with tracing oracles

Thank you! ☺