Bifurcated Signatures:
Folding the Accountability vs. Anonymity Dilemma into a Single Private Signing Scheme

Benoît Libert
ENSL, CNRS, France

Khoa Nguyen
UOW, Australia

Thomas Peters
UCLouvain, Belgium

Moti Yung
Google, USA

Zagreb (remote) - the 21st of October

$\longrightarrow$ Initiate research on

Bifurcated Cryptography

On the one branch	On the other branch
End-to-End Encryption	Key Escrow
Unconditional Anonymity	Identity Escrow
Everlasting Privacy	Accountability
Perfectly hiding...	Perfectly binding...
$\vdots$	$\vdots$

Goal: reconcile both branches in a single scheme

$\longrightarrow$ Initiate research on

Bifurcated Cryptography

On the one branch		On the other branch
End-to-End Encryption		Key Escrow
Unconditional Anonymity		Identity Escrow
Everlasting Privacy		Accountability
Perfectly hiding...		Perfectly binding...
$\vdots$		$\vdots$

Goal: reconcile both branches in a single scheme

$\longrightarrow$ Initiate research on

Bifurcated Cryptography

On the one branch		On the other branch
End-to-End Encryption		Key Escrow
Unconditional Anonymity		Identity Escrow
Everlasting Privacy		Accountability
Perfectly hiding...		Perfectly binding...
$\vdots$		$\vdots$

Goal: reconcile both branches in a single scheme

$\longrightarrow$ In the case of

Anonymous Signatures

On the one branch

Ring Signatures
(Unconditional Anonymity)

. . . even if linkable, k-times

On the other branch

Group signatures
(Traceability)

. . . even with restricted opening

One exception: Accountable tracing signatures

$\longrightarrow$ Still, signing keys (secretly) fix the branch!

$\longrightarrow$ In the case of

Anonymous Signatures

On the one branch

Ring Signatures
(Unconditional Anonymity)

. . . even if linkable, k-times

On the other branch

Group signatures
(Traceability)

. . . even with restricted opening

One exception: Accountable tracing signatures

$\longrightarrow$ Still, signing keys (secretly) fix the branch!

Why should we choose the branch at the key generation time?

Can we avoid authoritarily freezing the targeted security notions?

Can we have the best of both branches in a flexible and rallying feature?

$\longrightarrow$ We introduce the primitive of

Bifurcated Anonymous Signatures

Predicate-based branching

Pointwise traceability, known at the signing time $\rightarrow$ educated choice

Branch-Hiding

Whether a signature is traceable or not is hidden $\rightarrow$ free choice

Branch-Soundness

Malicious signers/authority cannot flip the branch $\rightarrow$ secure choice

$\longrightarrow$ We introduce the primitive of

Bifurcated Anonymous Signatures

Predicate-based branching

Pointwise traceability, known at the signing time $\rightarrow$ educated choice

Branch-Hiding

Whether a signature is traceable or not is hidden $\rightarrow$ free choice

Branch-Soundness

Malicious signers/authority cannot flip the branch $\rightarrow$ secure choice

$\longrightarrow$ We introduce the primitive of

Bifurcated Anonymous Signatures

Predicate-based branching

Pointwise traceability, known at the signing time $\rightarrow$ educated choice

Branch-Hiding

Whether a signature is traceable or not is hidden $\rightarrow$ free choice

Branch-Soundness

Malicious signers/authority cannot flip the branch $\rightarrow$ secure choice

$\longrightarrow$ We introduce the primitive of

Bifurcated Anonymous Signatures

Predicate-based branching

Pointwise traceability, known at the signing time $\rightarrow$ educated choice

Branch-Hiding

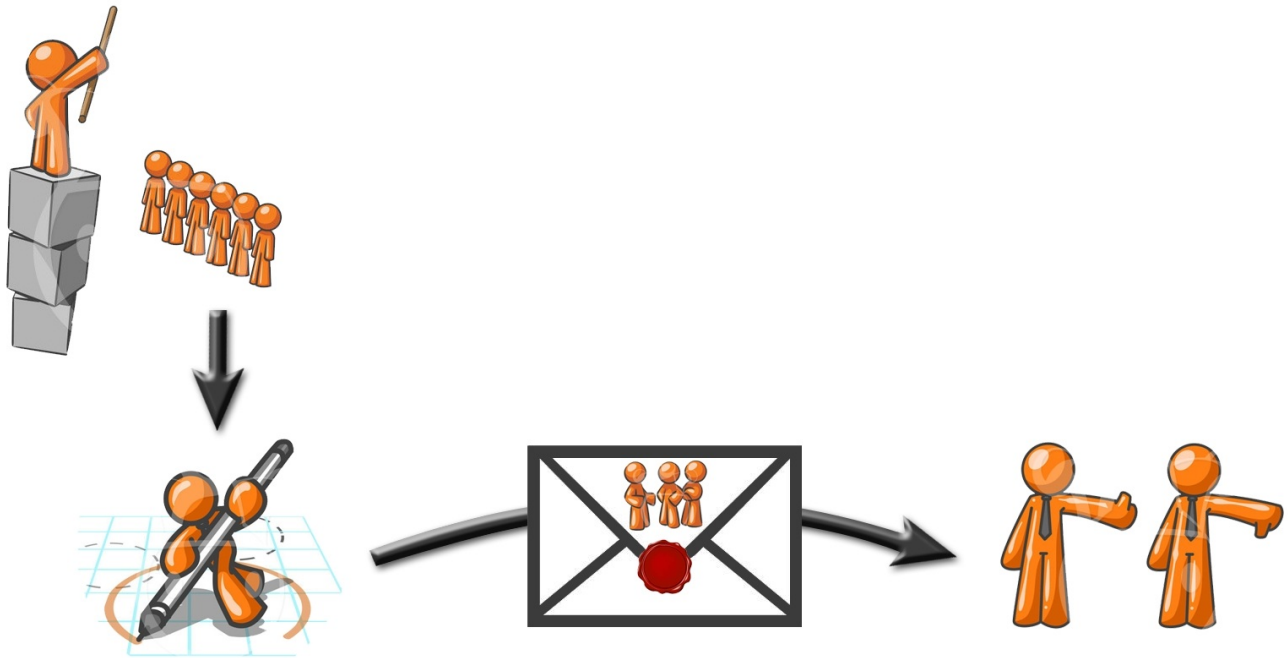
Whether a signature is traceable or not is hidden $\rightarrow$ free choice

Branch-Soundness

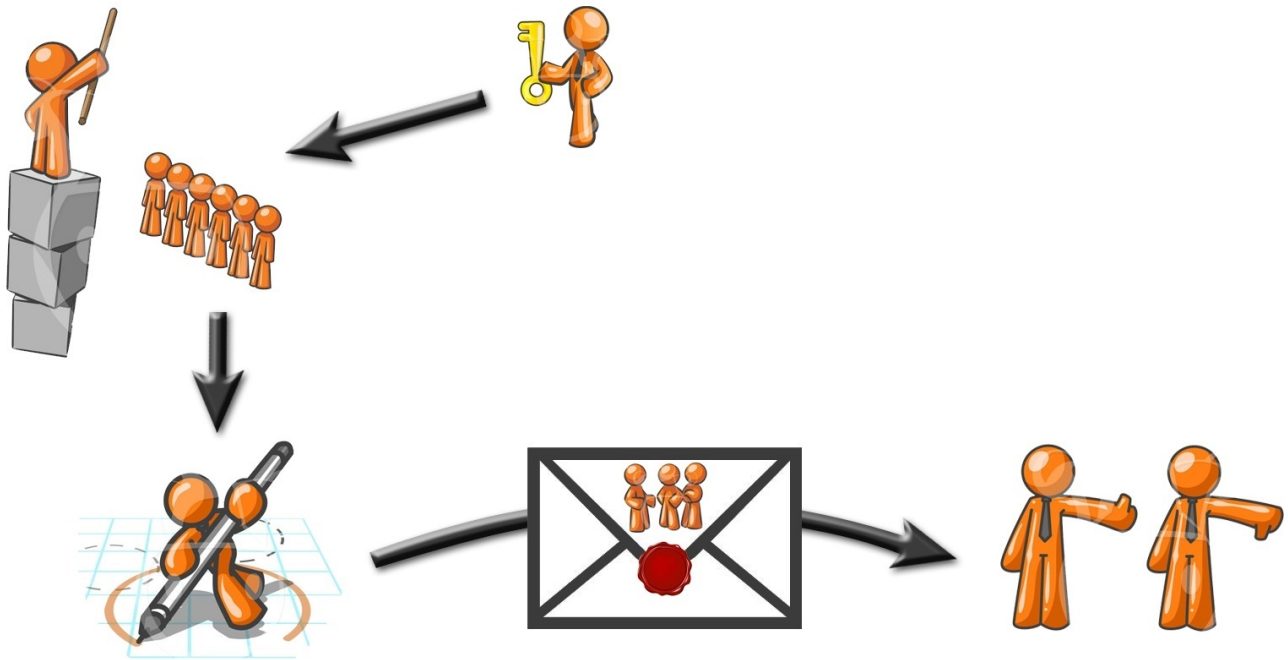
Malicious signers/authority cannot flip the branch $\rightarrow$ secure choice

bifurcated: "two branches in one"

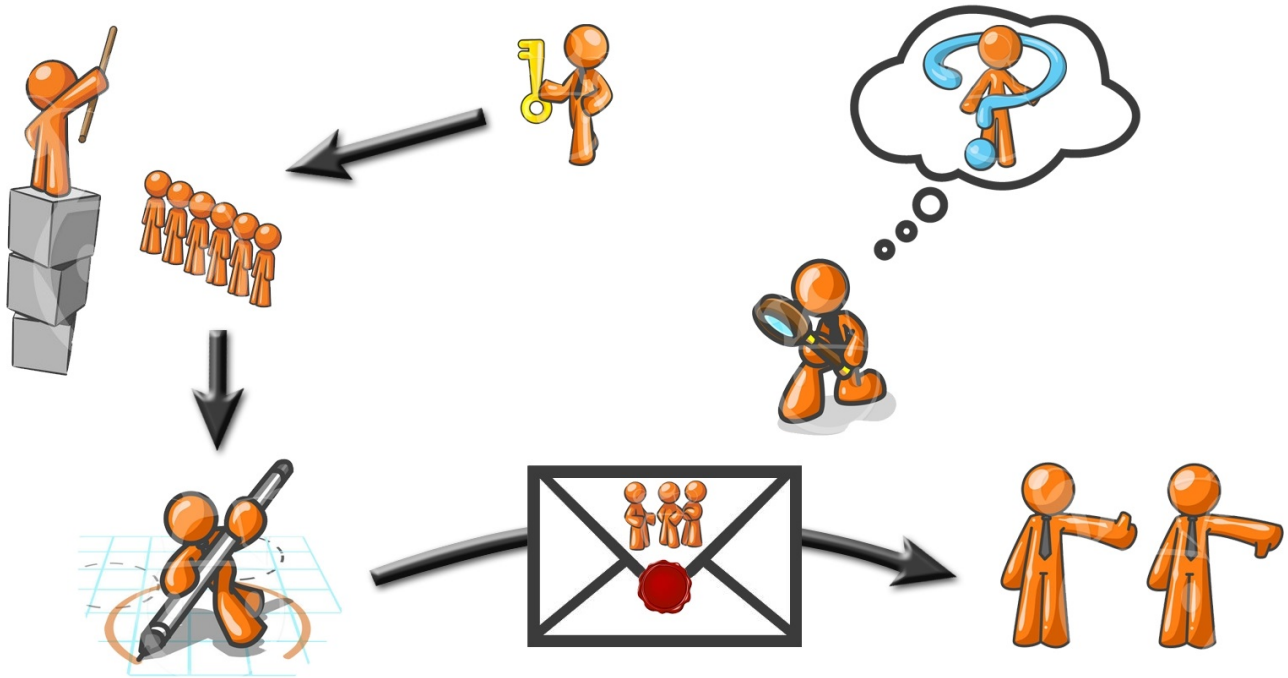
Bifurcated Anonymous Signatures (BiAS)



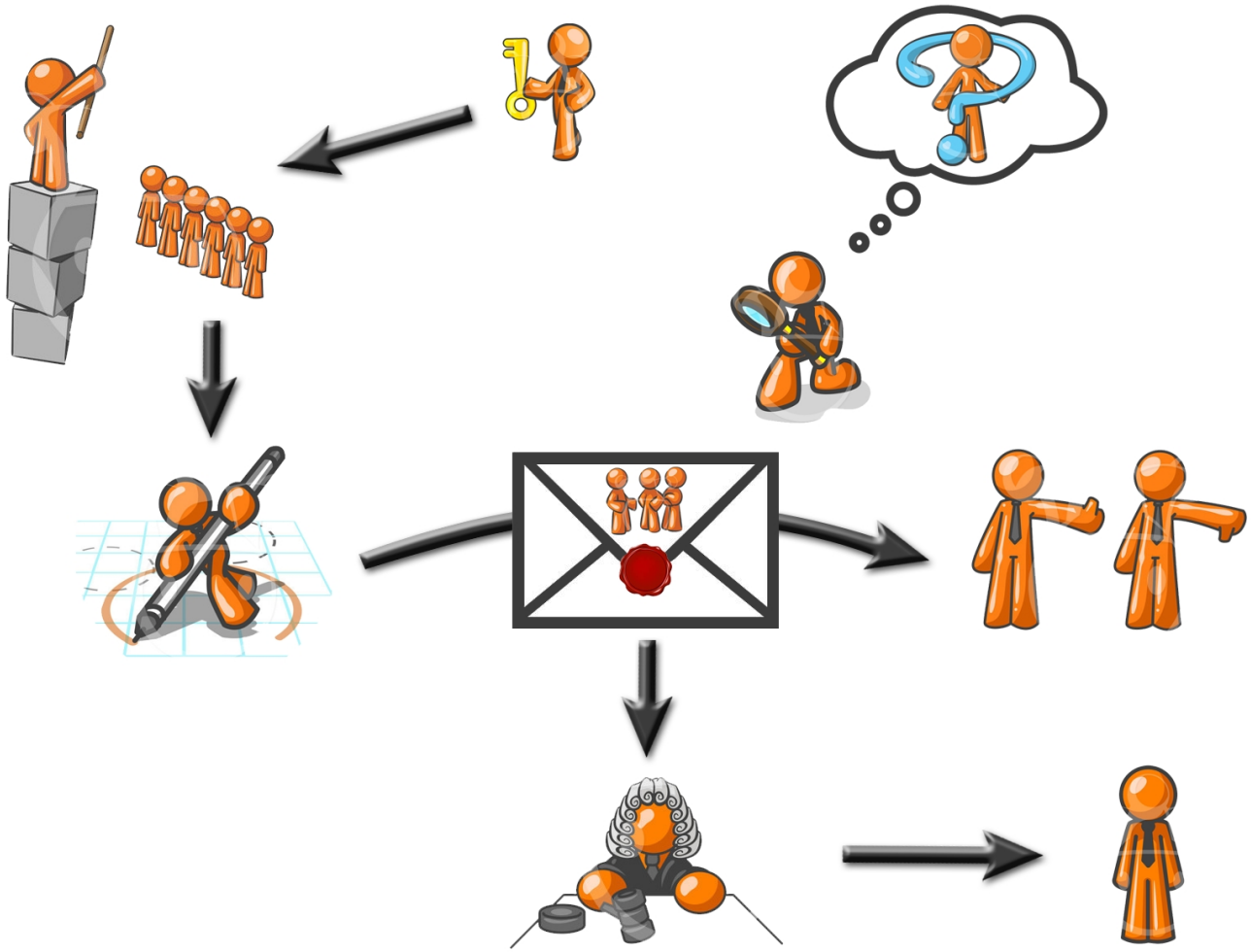
Bifurcated Anonymous Signatures (BiAS)



Bifurcated Anonymous Signatures (BiAS)



Bifurcated Anonymous Signatures (BiAS)



(Short) State of The Art

- Chaum-van Heyst (Eurocrypt'91): birth of Group Signatures
  Registered group members can sign messages while remaining anonymous

- Ateniese-Camenisch-Joye-Tsudik (Crypto'00): coalition-resistance
  . . . but analyzed *w.r.t.* a list of security requirements

- Bellare-Micciancio-Warinschi (Eurocrypt'03):
  Security model; construction based on trapdoor permutations

- Bellare-Shi-Zhang (CT-RSA'05), Kiayias-Yung (IJSN 2006):
  Model extensions to dynamic groups

- Rivest-Shamir-Tauman (Asiacrypt'01): birth of Ring Signatures
  How to leak a secret, wistleblowing app., unconditional anonymity

- Bender-Katz-Morselli (JoC'07):
  Stronger Definitions, constructions without random oracles

(Short) State of The Art

- Chaum-van Heyst (Eurocrypt'91): birth of Group Signatures
  Registered group members can sign messages while remaining anonymous
- Ateniese-Camenisch-Joye-Tsudik (Crypto'00): coalition-resistance
  . . . but analyzed *w.r.t.* a list of security requirements
- Bellare-Micciancio-Warinschi (Eurocrypt'03):
  Security model; construction based on trapdoor permutations
- Bellare-Shi-Zhang (CT-RSA'05), Kiayias-Yung (IJSN 2006):
  Model extensions to dynamic groups
- Rivest-Shamir-Tauman (Asiacrypt'01): birth of Ring Signatures
  How to leak a secret, wistleblowing app., unconditional anonymity
- Bender-Katz-Morselli (JoC'07):
  Stronger Definitions, constructions without random oracles

(Short) State of The Art

- Chaum-van Heyst (Eurocrypt'91): birth of Group Signatures
  Registered group members can sign messages while remaining anonymous
- Ateniese-Camenisch-Joye-Tsudik (Crypto'00): coalition-resistance
  . . . but analyzed *w.r.t.* a list of security requirements
- Bellare-Micciancio-Warinschi (Eurocrypt'03):
  Security model; construction based on trapdoor permutations
- Bellare-Shi-Zhang (CT-RSA'05), Kiayias-Yung (IJSN 2006):
  Model extensions to dynamic groups
- Rivest-Shamir-Tauman (Asiacrypt'01): birth of Ring Signatures
  How to leak a secret, wistleblowing app., unconditional anonymity
- Bender-Katz-Morselli (JoC'07):
  Stronger Definitions, constructions without random oracles

(Short) Related Work

- Restricted openings in Group Signatures:
  Message-dependent opening, Traceable signatures
- Restricted anonymity in Ring Signatures:
  Linkable/Traceable ring signatures, k-times anonymity
- Distinct (properties of) opening authorities, computational anonymity:
  Convertible linkable signatures, Accountable ring signatures, interactive
- Controlling who can sign what:
  Attribute-based/Policy-based/Functional signatures, Dynamic groups
- Ring and group signatures co-exist:
  Accountable tracing signatures, unotified users, setup frozen

(Short) Related Work

- Restricted openings in Group Signatures:
  Message-dependent opening, Traceable signatures
- Restricted anonymity in Ring Signatures:
  Linkable/Traceable ring signatures, k-times anonymity
- Distinct (properties of) opening authorities, computational anonymity:
  Convertible linkable signatures, Accountable ring signatures, interactive
- Controlling who can sign what:
  Attribute-based/Policy-based/Functional signatures, Dynamic groups
- Ring and group signatures co-exist:
  Accountable tracing signatures, unotified users, setup frozen

(Short) Related Work

- Restricted openings in Group Signatures:
  Message-dependent opening, Traceable signatures
- Restricted anonymity in Ring Signatures:
  Linkable/Traceable ring signatures, k-times anonymity
- Distinct (properties of) opening authorities, computational anonymity:
  Convertible linkable signatures, Accountable ring signatures, interactive
- Controlling who can sign what:
  Attribute-based/Policy-based/Functional signatures, Dynamic groups
- Ring and group signatures co-exist:
  Accountable tracing signatures, unotified users, setup frozen

Our Contributions

Bifurcated Anonymous Signatures

- Formal primitive: predicate family, branch-hiding, branch-soundness
- Unconditional anonymity if the predicate $P(M, \mathrm{id}, w)$ evaluates to 1
- Extractable mode (indistinguishable): traceability, unframeability

Generic Constructions

- General predicate as bounded-depth Boolean circuit
- Signature-size independent of the circuit size
- LWE instantiation (FHE, poly-) + Paring-based instantiation (NC^1)

Our Contributions

Bifurcated Anonymous Signatures

- Formal primitive: predicate family, branch-hiding, branch-soundness
- Unconditional anonymity if the predicate $P(M, \mathsf{id}, w)$ evaluates to 1
- Extractable mode (indistinguishable): traceability, unframeability

Generic Constructions

- General predicate as bounded-depth Boolean circuit
- Signature-size independent of the circuit size
- LWE instantiation (FHE, poly-) + Paring-based instantiation (NC^1)

Our Contributions

Bifurcated Anonymous Signatures

- Formal primitive: predicate family, branch-hiding, branch-soundness
- Unconditional anonymity if the predicate $P(M, \mathrm{id}, w)$ evaluates to 1
- Extractable mode (indistinguishable): traceability, unframeability

Generic Constructions

- General predicate as bounded-depth Boolean circuit
- Signature-size independent of the circuit size
- LWE instantiation (FHE, poly-) + Paring-based instantiation (NC^1)

BiAS

High-level Description

- **Setup:** $\mathcal{S}_{\mathsf{GM}}$, $\mathcal{S}_{\mathsf{OA}}$, predicate family $\mathcal{P} = \{P_i : \mathcal{M} \times \mathcal{ID} \times \mathcal{W} \to \{0,1\}\}_i$
- **Join:** $[\mathsf{GM}(\mathcal{S}_{\mathsf{GM}}) \rightleftharpoons \mathcal{U}] \to (\mathsf{id}, \mathsf{cert}, \mathsf{sec})$, **Sign:** $(\mathsf{id}, \mathsf{cert}, \mathsf{sec}, M, w, P) \to \sigma$
- **Open:** $(\mathcal{S}_{\mathsf{OA}}, M, \sigma, P) \to \mathsf{id} \in \mathcal{ID} \cup \{\perp\}$, **Verify:** $(M, \sigma, P) \to 0/1$

Potential Applications

- Money-laundering/Tax-evasion protection in financial transactions:
  $M = \mathsf{Enc}(\text{“who-to-who”})$, $w = \text{“amount”}$, $P_i = \text{“}w \in [a_i, b_i] \vee \mathsf{Dec}(M)\text{:local”}$
- Renting/Buying e-book: $P_i = \text{“only harmless content?”}$
- Free investigative journalism: $P_i = \text{“id in country}_i \text{ w/o freedom of speech?”}$

BiAS

High-level Description

- **Setup:** $\mathcal{S}_{\mathsf{GM}}$, $\mathcal{S}_{\mathsf{OA}}$, predicate family $\mathcal{P} = \{P_i : \mathcal{M} \times \mathcal{ID} \times \mathcal{W} \to \{0,1\}\}_i$
- **Join:** $[\mathsf{GM}(\mathcal{S}_{\mathsf{GM}}) \rightleftharpoons \mathcal{U}] \to (\mathsf{id}, \mathsf{cert}, \mathsf{sec})$, **Sign:** $(\mathsf{id}, \mathsf{cert}, \mathsf{sec}, M, w, P) \to \sigma$
- **Open:** $(\mathcal{S}_{\mathsf{OA}}, M, \sigma, P) \to \mathsf{id} \in \mathcal{ID} \cup \{\perp\}$, **Verify:** $(M, \sigma, P) \to 0/1$

Potential Applications

- Money-laundering/Tax-evasion protection in financial transactions:
  $M = \mathsf{Enc}(\text{“who-to-who”})$, $w = \text{“amount”}$, $P_i = \text{“}w \in [a_i, b_i] \vee \mathsf{Dec}(M)\text{:local”}$
- Renting/Buying e-book: $P_i = \text{“only harmless content?”}$
- Free investigative journalism: $P_i = \text{“id in country}_i \text{ w/o freedom of speech?”}$

Security notions

Privacy: complementary anonymity flavors

- **Non-traceable case:** $P(M, \mathrm{id}_0, w_0) = 1 = P(M, \mathrm{id}_1, w_1)$
  $\Longrightarrow \sigma \leftarrow \mathrm{Sign}(\mathrm{id}_b, \mathrm{cert}_b, \mathrm{sec}_b, M, w_b, P)$ statistically hides b
- **Traceable case:** includes $P(M, \mathrm{id}_0, w_0) \neq P(M, \mathrm{id}_1, w_1)$, branch-hiding
  $\Longrightarrow$ CCA-like definition with opening queries, computational

Security: two-step notions

- **Extractable mode:** SimSetup creates τ, $\mathrm{Extract}_\tau$ retrieves (id, w) w.o.p.
- Branch-soundness: (comp.) indistinguishable modes given $\mathcal{S}_{\mathrm{GM}}$ and $\mathcal{S}_{\mathrm{OA}}$
- Given extracted (id, w) define **traceability** and **unframeability**

Security notions

Privacy: complementary anonymity flavors

- **Non-traceable case:** $P(M, \mathrm{id}_0, w_0) = 1 = P(M, \mathrm{id}_1, w_1)$
  $\Longrightarrow$ $\sigma \leftarrow \mathrm{Sign}(\mathrm{id}_b, \mathrm{cert}_b, \mathrm{sec}_b, M, w_b, P)$ statistically hides b
- **Traceable case:** includes $P(M, \mathrm{id}_0, w_0) \neq P(M, \mathrm{id}_1, w_1)$, branch-hiding
  $\Longrightarrow$ CCA-like definition with opening queries, computational

Security: two-step notions

- **Extractable mode:** SimSetup creates τ, $\mathrm{Extract}_\tau$ retrieves (id, w) w.o.p.
- Branch-soundness: (comp.) indistinguishable modes given $\mathcal{S}_{\mathrm{GM}}$ and $\mathcal{S}_{\mathrm{OA}}$
- Given extracted (id, w) define **traceability** and **unframeability**

Security notions

Privacy: complementary anonymity flavors

- **Non-traceable case:** $P(M, \mathrm{id}_0, w_0) = 1 = P(M, \mathrm{id}_1, w_1)$
  $\Longrightarrow$ $\sigma \leftarrow \mathrm{Sign}(\mathrm{id}_b, \mathrm{cert}_b, \mathrm{sec}_b, M, w_b, P)$ statistically hides b
- **Traceable case:** includes $P(M, \mathrm{id}_0, w_0) \neq P(M, \mathrm{id}_1, w_1)$, branch-hiding
  $\Longrightarrow$ CCA-like definition with opening queries, computational

Security: two-step notions

- **Extractable mode:** SimSetup creates τ, $\mathrm{Extract}_\tau$ retrieves (id, w) w.o.p.
- Branch-soundness: (comp.) indistinguishable modes given $\mathcal{S}_{\mathsf{GM}}$ and $\mathcal{S}_{\mathsf{OA}}$
- Given extracted (id, w) define **traceability** and **unframeability**

Security notions

Privacy: complementary anonymity flavors

- **Non-traceable case:** $P(M, \mathrm{id}_0, w_0) = 1 = P(M, \mathrm{id}_1, w_1)$
  $\Longrightarrow$ $\sigma \leftarrow \mathrm{Sign}(\mathrm{id}_b, \mathrm{cert}_b, \mathrm{sec}_b, M, w_b, P)$ statistically hides b
- **Traceable case:** includes $P(M, \mathrm{id}_0, w_0) \neq P(M, \mathrm{id}_1, w_1)$, branch-hiding
  $\Longrightarrow$ CCA-like definition with opening queries, computational

Security: two-step notions

- **Extractable mode:** SimSetup creates τ, $\mathrm{Extract}_\tau$ retrieves (id, w) w.o.p.
- Branch-soundness: (comp.) indistinguishable modes given $\mathcal{S}_{\mathsf{GM}}$ and $\mathcal{S}_{\mathsf{OA}}$
- Given extracted (id, w) define **traceability** and **unframeability**

Generic Construction

To join the group, pick a signing key pair $(\mathsf{sk}_{\mathsf{id}}, \mathsf{pk}_{\mathsf{id}})$, set $\mathsf{sec} = \mathsf{sk}_{\mathsf{id}}$ and get

$$\mathsf{cert} \leftarrow \mathsf{GM.Sign}(\mathcal{S}_{\mathsf{GM}}, (\mathsf{id}, \mathsf{pk}_{\mathsf{id}}))$$

Signing a message $M \in \{0,1\}^{\ell}$:

- Compute the message-dependent circuit $C_M(\cdot,\cdot) = P(M,\cdot,\cdot)$
- Pick one-time key pair $(\mathsf{VK}, \mathsf{SK})$ of a SUF-CMA signature scheme
- Commit to (id, w) by computing an R-lossy ciphertext
$$\mathsf{ct}_{(\mathsf{id},w)} \leftarrow \mathsf{RL.Enc}(\mathsf{pk}_{RL}, \mathsf{VK}, (\mathsf{id}, w))$$
- Let $c_{\mathsf{ev}} = C_M(\mathsf{id}, w)$ and compute a lossy ciphertext of
$$\mathsf{ct}_{\mathsf{id}} \leftarrow \mathsf{L.Enc}(\mathsf{pk}_e, (1 - c_{\mathsf{ev}}) \cdot \mathsf{id})$$
- Also compute a Homomorphic Equivocal Commitment of
$$\mathsf{com}_{(\mathsf{id},w)} = \mathsf{HE.Com}((\mathsf{id}, w); r)$$
and the opening $\mathsf{open}(\mathsf{id}, w) = \mathsf{HE.Open}(C_M, (\mathsf{id}, w), r)$
- Compute a signature $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_{\mathsf{id}}, (M, P, \mathsf{ct}_{(\mathsf{id},w)}))$
- Make a dual-mode statistical NIZK argument π of "everything"

Generic Construction

To join the group, pick a signing key pair $(\mathsf{sk}_{\mathsf{id}}, \mathsf{pk}_{\mathsf{id}})$, set $\mathsf{sec} = \mathsf{sk}_{\mathsf{id}}$ and get

$$\mathsf{cert} \leftarrow \mathsf{GM.Sign}(\mathcal{S}_{\mathsf{GM}}, (\mathsf{id}, \mathsf{pk}_{\mathsf{id}}))$$

Signing a message $M \in \{0,1\}^{\ell}$:

- Compute the message-dependent circuit $C_M(\cdot,\cdot) = P(M,\cdot,\cdot)$
- Pick one-time key pair $(\mathsf{VK}, \mathsf{SK})$ of a SUF-CMA signature scheme
- Commit to (id, w) by computing an R-lossy ciphertext

$$\mathsf{ct}_{(\mathsf{id},w)} \leftarrow \mathsf{RL.Enc}(\mathsf{pk}_{RL}, \mathsf{VK}, (\mathsf{id}, w))$$

- Let $c_{\mathsf{ev}} = C_M(\mathsf{id}, w)$ and compute a lossy ciphertext of

$$\mathsf{ct}_{\mathsf{id}} \leftarrow \mathsf{L.Enc}(\mathsf{pk}_e, (1 - c_{\mathsf{ev}}) \cdot \mathsf{id})$$

- Also compute a Homomorphic Equivocal Commitment of

$$\mathsf{com}_{(\mathsf{id},w)} = \mathsf{HE.Com}((\mathsf{id}, w); r)$$

and the opening $\mathsf{open}(\mathsf{id}, w) = \mathsf{HE.Open}(C_M, (\mathsf{id}, w), r)$

- Compute a signature $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_{\mathsf{id}}, (M, P, \mathsf{ct}_{(\mathsf{id},w)}))$
- Make a dual-mode statistical NIZK argument π of "everything"

Generic Construction

To join the group, pick a signing key pair $(\mathsf{sk}_{\mathsf{id}}, \mathsf{pk}_{\mathsf{id}})$, set $\mathsf{sec} = \mathsf{sk}_{\mathsf{id}}$ and get

$$\mathsf{cert} \leftarrow \mathsf{GM.Sign}(\mathcal{S}_{\mathsf{GM}}, (\mathsf{id}, \mathsf{pk}_{\mathsf{id}}))$$

Signing a message $M \in \{0,1\}^{\ell}$:

- Compute the message-dependent circuit $C_M(\cdot,\cdot) = P(M,\cdot,\cdot)$
- Pick one-time key pair $(\mathsf{VK}, \mathsf{SK})$ of a SUF-CMA signature scheme
- Commit to (id, w) by computing an R-lossy ciphertext
$$\mathsf{ct}_{(\mathsf{id},w)} \leftarrow \mathsf{RL.Enc}(\mathsf{pk}_{RL}, \mathsf{VK}, (\mathsf{id}, w))$$
- Let $c_{\mathsf{ev}} = C_M(\mathsf{id}, w)$ and compute a lossy ciphertext of
$$\mathsf{ct}_{\mathsf{id}} \leftarrow \mathsf{L.Enc}(\mathsf{pk}_e, (1 - c_{\mathsf{ev}}) \cdot \mathsf{id})$$
- Also compute a Homomorphic Equivocal Commitment of
$$\mathsf{com}_{(\mathsf{id},w)} = \mathsf{HE.Com}((\mathsf{id}, w); r)$$
and the opening $\mathsf{open}(\mathsf{id}, w) = \mathsf{HE.Open}(C_M, (\mathsf{id}, w), r)$
- Compute a signature $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_{\mathsf{id}}, (M, P, \mathsf{ct}_{(\mathsf{id},w)}))$
- Make a dual-mode statistical NIZK argument π of "everything"

Generic Construction

To join the group, pick a signing key pair $(\mathsf{sk}_{\mathsf{id}}, \mathsf{pk}_{\mathsf{id}})$, set $\mathsf{sec} = \mathsf{sk}_{\mathsf{id}}$ and get

$$\mathsf{cert} \leftarrow \mathsf{GM.Sign}(\mathcal{S}_{\mathsf{GM}}, (\mathsf{id}, \mathsf{pk}_{\mathsf{id}}))$$

Signing a message $M \in \{0,1\}^{\ell}$:

- Compute the message-dependent circuit $C_M(\cdot,\cdot) = P(M,\cdot,\cdot)$
- Pick one-time key pair $(\mathsf{VK}, \mathsf{SK})$ of a SUF-CMA signature scheme
- Commit to (id, w) by computing an R-lossy ciphertext

$$\mathsf{ct}_{(\mathsf{id},w)} \leftarrow \mathsf{RL.Enc}(\mathsf{pk}_{RL}, \mathsf{VK}, (\mathsf{id}, w))$$

- Let $c_{\mathsf{ev}} = C_M(\mathsf{id}, w)$ and compute a lossy ciphertext of

$$\mathsf{ct}_{\mathsf{id}} \leftarrow \mathsf{L.Enc}(\mathsf{pk}_e, (1 - c_{\mathsf{ev}}) \cdot \mathsf{id})$$

- Also compute a Homomorphic Equivocal Commitment of

$$\mathsf{com}_{(\mathsf{id},w)} = \mathsf{HE.Com}((\mathsf{id}, w); r)$$

and the opening $\mathsf{open}(\mathsf{id}, w) = \mathsf{HE.Open}(C_M, (\mathsf{id}, w), r)$

- Compute a signature $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_{\mathsf{id}}, (M, P, \mathsf{ct}_{(\mathsf{id},w)}))$
- Make a dual-mode statistical NIZK argument π of "everything"

Generic Construction

To join the group, pick a signing key pair $(\mathsf{sk}_{\mathsf{id}}, \mathsf{pk}_{\mathsf{id}})$, set $\mathsf{sec} = \mathsf{sk}_{\mathsf{id}}$ and get

$$\mathsf{cert} \leftarrow \mathsf{GM.Sign}(\mathcal{S}_{\mathsf{GM}}, (\mathsf{id}, \mathsf{pk}_{\mathsf{id}}))$$

Signing a message $M \in \{0,1\}^{\ell}$:

- Compute the message-dependent circuit $C_M(\cdot,\cdot) = P(M,\cdot,\cdot)$
- Pick one-time key pair $(\mathsf{VK}, \mathsf{SK})$ of a SUF-CMA signature scheme
- Commit to (id, w) by computing an R-lossy ciphertext
$$\mathsf{ct}_{(\mathsf{id},w)} \leftarrow \mathsf{RL.Enc}(\mathsf{pk}_{RL}, \mathsf{VK}, (\mathsf{id}, w))$$
- Let $c_{\mathsf{ev}} = C_M(\mathsf{id}, w)$ and compute a lossy ciphertext of
$$\mathsf{ct}_{\mathsf{id}} \leftarrow \mathsf{L.Enc}(\mathsf{pk}_e, (1 - c_{\mathsf{ev}}) \cdot \mathsf{id})$$
- Also compute a Homomorphic Equivocal Commitment of
$$\mathsf{com}_{(\mathsf{id},w)} = \mathsf{HE.Com}((\mathsf{id}, w); r)$$
and the opening $\mathsf{open}(\mathsf{id}, w) = \mathsf{HE.Open}(C_M, (\mathsf{id}, w), r)$
- Compute a signature $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_{\mathsf{id}}, (M, P, \mathsf{ct}_{(\mathsf{id},w)}))$
- Make a dual-mode statistical NIZK argument π of "everything"

Generic Construction

To join the group, pick a signing key pair $(\mathsf{sk}_{\mathsf{id}}, \mathsf{pk}_{\mathsf{id}})$, set $\mathsf{sec} = \mathsf{sk}_{\mathsf{id}}$ and get

$$\mathsf{cert} \leftarrow \mathsf{GM.Sign}(\mathcal{S}_{\mathsf{GM}}, (\mathsf{id}, \mathsf{pk}_{\mathsf{id}}))$$

Signing a message $M \in \{0,1\}^{\ell}$:

- Compute the message-dependent circuit $C_M(\cdot,\cdot) = P(M,\cdot,\cdot)$
- Pick one-time key pair $(\mathsf{VK}, \mathsf{SK})$ of a SUF-CMA signature scheme
- Commit to (id, w) by computing an R-lossy ciphertext
$$\mathsf{ct}_{(\mathsf{id},w)} \leftarrow \mathsf{RL.Enc}(\mathsf{pk}_{RL}, \mathsf{VK}, (\mathsf{id}, w))$$
- Let $c_{\mathsf{ev}} = C_M(\mathsf{id}, w)$ and compute a lossy ciphertext of
$$\mathsf{ct}_{\mathsf{id}} \leftarrow \mathsf{L.Enc}(\mathsf{pk}_e, (1 - c_{\mathsf{ev}}) \cdot \mathsf{id})$$
- Also compute a Homomorphic Equivocal Commitment of
$$\mathsf{com}_{(\mathsf{id},w)} = \mathsf{HE.Com}((\mathsf{id}, w); r)$$
and the opening $\mathsf{open}(\mathsf{id}, w) = \mathsf{HE.Open}(C_M, (\mathsf{id}, w), r)$
- Compute a signature $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_{\mathsf{id}}, (M, P, \mathsf{ct}_{(\mathsf{id},w)}))$
- Make a dual-mode statistical NIZK argument π of "everything"

Generic Construction

To join the group, pick a signing key pair $(\mathsf{sk}_{\mathsf{id}}, \mathsf{pk}_{\mathsf{id}})$, set $\mathsf{sec} = \mathsf{sk}_{\mathsf{id}}$ and get

$$\mathsf{cert} \leftarrow \mathsf{GM.Sign}(\mathcal{S}_{\mathsf{GM}}, (\mathsf{id}, \mathsf{pk}_{\mathsf{id}}))$$

Signing a message $M \in \{0,1\}^{\ell}$:

- Compute the message-dependent circuit $C_M(\cdot,\cdot) = P(M,\cdot,\cdot)$
- Pick one-time key pair $(\mathsf{VK}, \mathsf{SK})$ of a SUF-CMA signature scheme
- Commit to (id, w) by computing an R-lossy ciphertext
$$\mathsf{ct}_{(\mathsf{id},w)} \leftarrow \mathsf{RL.Enc}(\mathsf{pk}_{RL}, \mathsf{VK}, (\mathsf{id}, w))$$
- Let $c_{\mathsf{ev}} = C_M(\mathsf{id}, w)$ and compute a lossy ciphertext of
$$\mathsf{ct}_{\mathsf{id}} \leftarrow \mathsf{L.Enc}(\mathsf{pk}_e, (1 - c_{\mathsf{ev}}) \cdot \mathsf{id})$$
- Also compute a Homomorphic Equivocal Commitment of
$$\mathsf{com}_{(\mathsf{id},w)} = \mathsf{HE.Com}((\mathsf{id}, w); r)$$
and the opening $\mathsf{open}(\mathsf{id}, w) = \mathsf{HE.Open}(C_M, (\mathsf{id}, w), r)$
- Compute a signature $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_{\mathsf{id}}, (M, P, \mathsf{ct}_{(\mathsf{id},w)}))$
- Make a dual-mode statistical NIZK argument π of "everything"

Generic Construction

To join the group, pick a signing key pair $(\mathsf{sk}_{\mathsf{id}}, \mathsf{pk}_{\mathsf{id}})$, set $\mathsf{sec} = \mathsf{sk}_{\mathsf{id}}$ and get

$$\mathsf{cert} \leftarrow \mathsf{GM.Sign}(\mathcal{S}_{\mathsf{GM}}, (\mathsf{id}, \mathsf{pk}_{\mathsf{id}}))$$

Signing a message $M \in \{0,1\}^{\ell}$:

- Compute the message-dependent circuit $C_M(\cdot,\cdot) = P(M,\cdot,\cdot)$
- Pick one-time key pair $(\mathsf{VK}, \mathsf{SK})$ of a SUF-CMA signature scheme
- Commit to (id, w) by computing an R-lossy ciphertext
$$\mathsf{ct}_{(\mathsf{id},w)} \leftarrow \mathsf{RL.Enc}(\mathsf{pk}_{RL}, \mathsf{VK}, (\mathsf{id}, w))$$
- Let $c_{\mathsf{ev}} = C_M(\mathsf{id}, w)$ and compute a lossy ciphertext of
$$\mathsf{ct}_{\mathsf{id}} \leftarrow \mathsf{L.Enc}(\mathsf{pk}_e, (1 - c_{\mathsf{ev}}) \cdot \mathsf{id})$$
- Also compute a Homomorphic Equivocal Commitment of
$$\mathsf{com}_{(\mathsf{id},w)} = \mathsf{HE.Com}((\mathsf{id}, w); r)$$
and the opening $\mathsf{open}(\mathsf{id}, w) = \mathsf{HE.Open}(C_M, (\mathsf{id}, w), r)$
- Compute a signature $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_{\mathsf{id}}, (M, P, \mathsf{ct}_{(\mathsf{id},w)}))$
- Make a dual-mode statistical NIZK argument π of "everything"

Conclusion

New Bifurcated Cryptographic Primitive

- Anonymous signatures: unconditional anonymity vs. accountability
- Generic construction *in the standard model*, bounded-depth circuit
- Instantiations: LWE + Pairing-based $(23 \cdot |w| + 44 \cdot |\mathsf{id}| + 171$ in $\mathbb{G})$

Open Problems

- **Bifurcated encryption:** conditional escrow frozen in the predicate
- **Practical BiAS:** specific predicates (ROM, simple assumptions)
- **Model Extensions:** malicious keys (subverted anonymity), revocation

Thank you!

Conclusion

New Bifurcated Cryptographic Primitive

- Anonymous signatures: unconditional anonymity vs. accountability
- Generic construction *in the standard model*, bounded-depth circuit
- Instantiations: LWE + Pairing-based $(23 \cdot |w| + 44 \cdot |\mathsf{id}| + 171$ in $\mathbb{G})$

Open Problems

- **Bifurcated encryption:** conditional escrow frozen in the predicate
- **Practical BiAS:** specific predicates (ROM, simple assumptions)
- **Model Extensions:** malicious keys (subverted anonymity), revocation

Thank you!

Conclusion

New Bifurcated Cryptographic Primitive

- Anonymous signatures: unconditional anonymity vs. accountability
- Generic construction *in the standard model*, bounded-depth circuit
- Instantiations: LWE + Pairing-based $(23 \cdot |w| + 44 \cdot |\mathsf{id}| + 171$ in $\mathbb{G})$

Open Problems

- **Bifurcated encryption:** conditional escrow frozen in the predicate
- **Practical BiAS:** specific predicates (ROM, simple assumptions)
- **Model Extensions:** malicious keys (subverted anonymity), revocation

Thank you!