Computing on Authenticated Data: New Privacy Definitions and Constructions

Nuttapong Attrapadung\(^1\), Benoit Libert\(^2\), Thomas Peters\(^3\)

1 - Research Institute for Secure Systems, AIST (Japan)
2 - Technicolor (France)
3 - Université catholique de Louvain, Crypto Group (Belgium)

Asiacrypt - 4th December 2012
Homomorphic Signature Schemes

- Ahn, Boneh, Camenisch, Hohenberger, shelat, Waters (TCC’12): Computing on Authenticated Data

\[ \text{Signed data} \quad \forall f \in H \quad \text{Signed valuation} \]

- Unified signature model: for all authorized malleability \( H \)
- Security model: \( H\)-unforgeability and context hiding
Homomorphic Signature Schemes

- Ahn, Boneh, Camenisch, Hohenberger, shelat, Waters (TCC’12): Computing onAuthenticated Data

\[ \text{Signed data} \quad \forall f \in H \quad \text{Signed valuation} \]

- Unified signature model: for all authorized malleability \( H \)
- Security model: \( H\)-unforgeability and context hiding
**P-Homomorphic signature schemes**

**Predicates**
- \( P : 2^M \times M \rightarrow \{0, 1\} \)
- If \( P(M, m') = 1 \), \( m' \) is derivable from \( M \)
  - e.g. \( P(\{\ldots m_i \ldots\}, m') = 1 \) only if \( f(\ldots m_i \ldots) = m' \)

**Derivability of Signatures**
- For \( m \in M : \text{Vrfy}(m, \sigma_m) = 1 \), when \( P(M, m') = 1 \)
  \[
  \sigma' \leftarrow \text{SignDerive}(pk, \{(m, \sigma_m)\}_{m \in M}, m')
  \]

**P-Unforgeability**
- For queries \( \{\sigma_m\}_{m \in M} \leftarrow \text{Sign}(sk, M) \)
  \[
  P(M, m') = 1 \quad \Rightarrow \quad (m', \sigma') \neq \text{forgery}
  \]
**P-Homomorphic signature schemes**

**Predicates**

- \( P : 2^\mathcal{M} \times \mathcal{M} \to \{0, 1\} \)
- If \( P(M, m') = 1 \), \( m' \) is derivable from \( M \)
  - e.g. \( P(\{\ldots m_i \ldots\}, m') = 1 \) only if \( f(\ldots m_i \ldots) = m' \)

**Derivability of Signatures**

- For \( m \in M : \text{Vrfy}(m, \sigma_m) = 1 \), when \( P(M, m') = 1 \)
  \[ \sigma' \leftarrow \text{SignDerive}(pk, \{(m, \sigma_m)\}_{m \in M}, m') \]

**P-Unforgeability**

- For queries \( \{\sigma_m\}_{m \in M} \leftarrow \text{Sign}(sk, M) \)
  \[ P(M, m') = 1 \implies (m', \sigma') \neq \text{forgery} \]
**P-Homomorphic signature schemes**

**Predicates**

- $P : 2^M \times M \rightarrow \{0, 1\}$
- If $P (M, m') = 1$, $m'$ is derivable from $M$
  - e.g. $P (\{\ldots m_i \ldots\}, m') = 1$ only if $f (\ldots m_i \ldots) = m'$

**Derivability of Signatures**

- For $m \in M : \text{Vrfy}(m, \sigma_m) = 1$, when $P (M, m') = 1$

\[
\sigma' \leftarrow \text{SignDerive} (pk, \{(m, \sigma_m)\}_{m \in M}, m')
\]

**P-Unforgeability**

- For queries $\{\sigma_m\}_{m \in M} \leftarrow \text{Sign}(sk, M)$

\[
P (M, m') = 1 \implies (m', \sigma') \neq \text{forgery}
\]
**P-Homomorphic signature schemes**

**Predicates**

- \( P : 2^\mathcal{M} \times \mathcal{M} \rightarrow \{0, 1\} \)
- If \( P(M, m') = 1 \), \( m' \) is derivable from \( M \)
  - e.g. \( P(\{\ldots m_i \ldots\}, m') = 1 \) only if \( f(\ldots m_i \ldots) = m' \)

**Derivability of Signatures**

- For \( m \in M : \text{Vrfy}(m, \sigma_m) = 1 \), when \( P(M, m') = 1 \)
  \[ \sigma' \leftarrow \text{SignDerive}(pk, \{(m, \sigma_m)\}_{m \in M}, m') \]

**P-Unforgeability**

- For queries \( \{\sigma_m\}_{m \in M} \leftarrow \text{Sign}(sk, M) \)
  \[ P(M, m') = 1 \implies (m', \sigma') \neq \text{forgery} \]
Homomorphic Signatures

- Johnson-Molnar-Song-Wagner (CT-RSA’02): Introduction;

- Boneh-Freeman-Katz-Waters (PKC’09): linearly homomorphic signatures over the integers, random-oracle model;

- Boneh-Freeman (PKC’11 & Eurocrypt’11): linearly homomorphic signatures over binary fields, random-oracle model;

- Catalano-Fiore-Warinschi (Eurocrypt’11 & PKC’12), Freeman (PKC’12): realization in the standard model;

- Attrapadung-Libert (PKC’11): in the standard model;

Homomorphic Signatures

- Johnson-Molnar-Song-Wagner (CT-RSA’02): Introduction;

- Boneh-Freeman-Katz-Waters (PKC’09): linearly homomorphic signatures over the integers, random-oracle model; SCH

- Boneh-Freeman (PKC’11 & Eurocrypt’11): linearly homomorphic signatures over binary fields, random-oracle model;

- Catalano-Fiore-Warinschi (Eurocrypt’11 & PKC’12), Freeman (PKC’12): realization in the standard model;

- Attrapadung-Libert (PKC’11): in the standard model; SCH

Homomorphic Signatures

- Johnson-Molnar-Song-Wagner (CT-RSA’02): Introduction;
- Boneh-Freeman-Katz-Waters (PKC’09): linearly homomorphic signatures over the integers, random-oracle model; SCH
- Boneh-Freeman (PKC’11 & Eurocrypt’11): linearly homomorphic signatures over binary fields, random-oracle model;
- Catalano-Fiore-Warinschi (Eurocrypt’11 & PKC’12), Freeman (PKC’12): realization in the standard model;
- Attrapadung-Libert (PKC’11): in the standard model; SCH
**Homomorphic Signatures**

- Johnson-Molnar-Song-Wagner (CT-RSA’02): Introduction;

- Boneh-Freeman-Katz-Waters (PKC’09): linearly homomorphic signatures over the integers, random-oracle model; SCH

- Boneh-Freeman (PKC’11 & Eurocrypt’11): linearly homomorphic signatures over binary fields, random-oracle model;

- Catalano-Fiore-Warinschi (Eurocrypt’11 & PKC’12), Freeman (PKC’12): realization in the standard model;

- Attrapadung-Libert (PKC’11): in the standard model; SCH

Homomorphic Signatures

- Johnson-Molnar-Song-Wagner (CT-RSA’02): Introduction;

- Boneh-Freeman-Katz-Waters (PKC’09): linearly homomorphic signatures over the integers, random-oracle model; SCH

- Boneh-Freeman (PKC’11 & Eurocrypt’11): linearly homomorphic signatures over binary fields, random-oracle model;

- Catalano-Fiore-Warinschi (Eurocrypt’11 & PKC’12), Freeman (PKC’12): realization in the standard model;

- Attrapadung-Libert (PKC’11): in the standard model; SCH

Strongly Context-Hiding

Motivation

Preventing confidential certified data from leaking information on others

- Medical files: Eye test $\rightarrow$ Genetic test has been done!
- Passport: Several authorized access $\rightarrow$ Reconstruct data-base!

Definition

$$\forall M \subset \mathcal{M}, \{\sigma_m\}_{m \in M} \leftarrow \text{Sign}(sk, M), m' \in \mathcal{M}, P(M, m') = 1 :$$

$$\{sk, \{\sigma_m\}_m, \text{Sign}(sk, m')\} \sim^S \{sk, \{\sigma_m\}_m, \text{SignDerive}(pk, (\{\sigma_m\}_m, M), m')\}$$

Constructions

- Subset predicates ($O(l)$-size public keys, for $l = \max_M |m|$)
- Quotable signatures in the standard model
**Strongly Context-Hiding**

**Motivation**

Preventing confidential certified data from leaking information on others

- Medical files: Eye test → Genetic test has been done!
- Passport: Several authorized access → Reconstruct data-base!

**Definition**

\[ \forall M \subseteq \mathcal{M}, \{\sigma_m\}_{m \in M} \leftarrow \text{Sign}(sk, M), \ m' \in \mathcal{M}, \ P(M, m') = 1 : \]

\[ \{sk, \{\sigma_m\}_m, \text{Sign}(sk, m')\} \sim^{S} \{sk, \{\sigma_m\}_m, \text{SignDerive}(pk, (\{\sigma_m\}_m, M), m')\} \]

**Constructions**

- Subset predicates (\(O(l)\)-size public keys, for \(l = \max_{\mathcal{M}} |m|\))
- Quotable signatures in the standard model
Strongly Context-Hiding

Motivation

Preventing confidential certified data from leaking information on others

- Medical files: Eye test → Genetic test has been done!
- Passport: Several authorized access → Reconstruct data-base!

Definition

\[ \forall M \subseteq \mathcal{M}, \{\sigma_m\}_{m \in M} \leftarrow \text{Sign}(sk, M), \ m' \in \mathcal{M}, \ P(M, m') = 1 : \]

\[ \{sk, \{\sigma_m\}_m, \text{Sign}(sk, m')\} \sim^S \{sk, \{\sigma_m\}_m, \text{SignDerive}(pk, ([\{\sigma_m\}_m, M], m')\} \]

Constructions

- Subset predicates \((O(l)\text{-size public keys}, \text{for } l = \max_{\mathcal{M}} |m|)\)
- Quotable signatures in the standard model
Strongly Context-Hiding

Motivation

Preventing confidential certified data from leaking information on others

- Medical files: Eye test → Genetic test has been done!
- Passport: Several authorized access → Reconstruct data-base!

Definition

∀ M ⊆ M, \{σ_m\}_{m \in M} \xleftarrow{} \text{Sign}(sk, M), m' \in M, P(M, m') = 1:

\{sk, \{σ_m\}_m, \text{Sign}(sk, m')\} \sim \{sk, \{σ_m\}_m, \text{SignDerive}(pk, (\{σ_m\}_m, M), m')\}

Constructions

- Subset predicates (O(l)-size public keys, for l = max_{M} |m|)
- Quotable signatures in the standard model
Strongly Context-Hiding

Motivation
Preventing confidential certified data from leaking information on others

- Medical files: Eye test $\rightarrow$ Genetic test has been done!
- Passport: Several authorized access $\rightarrow$ Reconstruct data-base!

Definition
\[
\forall M \subset \mathcal{M}, \{\sigma_m\}_{m \in M} \leftarrow \text{Sign}(sk, M), m' \in \mathcal{M}, P(M, m') = 1:
\]
\[
\{sk, \{\sigma_m\}_m, \text{Sign}(sk, m')\} \sim^S \{sk, \{\sigma_m\}_m, \text{SignDerive}(pk, (\{\sigma_m\}_m, M), m')\}
\]

Constructions

- Subset predicates ($O(l)$-size public keys, for $l = \max_M |m|$)
- Quotable signatures in the standard model
Our Contributions

New privacy definitions

- Adaptive context-hiding security
  (allows for adversarially-chosen signatures)
- Separations with existing privacy notions
- New unifying definition: complete context-hiding security

New constructions

- Linearly homomorphic signatures in the standard model
- Adaptively context-hiding construction
- Shorter weakly context-hiding signatures from the CDH assumption
- Subset predicate signatures in the standard model
  - Fully secure scheme with 1-bit false public key
  - New design principle using the randomizability of Groth-Sahai proofs
Our Contributions

New privacy definitions

- Adaptive context-hiding security
  (allows for adversarially-chosen signatures)
- Separations with existing privacy notions
- New *unifying* definition: *complete context-hiding* security

New constructions

- Linearly homomorphic signatures in the standard model
  - Adaptively context-hiding construction
  - Shorter weakly context-hiding signatures from the CDH assumption
- Subset predicate signatures in the standard model
  - Fully secure scheme with $O(1)$-size public keys
  - New design principle using the randomizability of Groth-Sahai proofs
Our Contributions

New privacy definitions
- Adaptive context-hiding security
  (allows for adversarially-chosen signatures)
- Separations with existing privacy notions
- New unifying definition: complete context-hiding security

New constructions
- Linearly homomorphic signatures in the standard model
  - Adaptively context-hiding construction
  - Shorter weakly context-hiding signatures from the CDH assumption
- Subset predicate signatures in the standard model
  - Fully secure scheme with $O(1)$-size public keys
  - New design principle using the randomizability of Groth-Sahai proofs
Our Contributions

New privacy definitions

- Adaptive context-hiding security (allows for adversarially-chosen signatures)
- Separations with existing privacy notions
- New unifying definition: complete context-hiding security

New constructions

- Linearly homomorphic signatures in the standard model
  - Adaptively context-hiding construction
  - Shorter weakly context-hiding signatures from the CDH assumption
- Subset predicate signatures in the standard model
  - Fully secure scheme with $O(1)$-size public keys
  - New design principle using the randomizability of Groth-Sahai proofs
Our Contributions

New privacy definitions

- Adaptive context-hiding security (allows for adversarially-chosen signatures)
- Separations with existing privacy notions
- New *unifying* definition: *complete context-hiding* security

New constructions

- Linearly homomorphic signatures in the standard model
  - Adaptively context-hiding construction
  - Shorter weakly context-hiding signatures from the CDH assumption
- Subset predicate signatures in the standard model
  - Fully secure scheme with $O(1)$-size public keys
  - New design principle using the randomizability of Groth-Sahai proofs
New Context-Hiding Definitions (1)

**Strongly Context-Hiding** (reminder)

\[ \forall M \subset \mathcal{M}, \{\sigma_m\}_{m \in M} \leftarrow \text{Sign}(sk, M), m' \in \mathcal{M} : P(M, m') = 1, \]

\[ \{sk, \{\sigma_m\}_m, \text{Sign}(sk, m')\} \sim^S \{sk, \{\sigma_m\}_m, \text{SignDerive}(pk, (\{\sigma_m\}_m, M), m')\} \]

**Randomizable Signature Case**

- From \((m, \sigma)\) can publicly compute \(\sigma' \leftarrow \text{Rand}(\sigma)\)
- If \(\text{Vrfy}(m, \sigma) = 1\) then \(\text{Vrfy}(m, \sigma') = 1\)

Rand could add subliminal information in \(\{\sigma_m\}_{m \in \mathcal{M}}\) before \(\text{SignDerive}\)
New Context-Hiding Definitions (1)

**Strongly Context-Hiding** (reminder)

\[ \forall M \subset \mathcal{M}, \{\sigma_m\}_{m \in M} \leftarrow \text{Sign}(sk, M), m' \in \mathcal{M} : P(M, m') = 1, \]

\[ \{sk, \{\sigma_m\}_m, \text{Sign}(sk, m')\} \sim^S \{sk, \{\sigma_m\}_m, \text{SignDerive}(pk, (\{\sigma_m\}_m, M), m')\} \]

**Randomizable Signature Case**

- From \((m, \sigma)\) can publicly compute \(\sigma' \leftarrow \text{Rand}(\sigma)\)
- If \(\text{Vrfy}(m, \sigma) = 1\) then \(\text{Vrfy}(m, \sigma') = 1\)

Rand could add subliminal information in \(\{\sigma_m\}_{m \in M}\) before \text{SignDerive}
New Context-Hiding Definitions (1)

Strongly Context-Hiding (reminder)

\[ \forall M \subset \mathcal{M}, \{\sigma_m\}_{m \in M} \leftarrow \text{Sign}(sk, M), m' \in \mathcal{M} : P(M, m') = 1, \]

\[ \{sk, \{\sigma_m\}_m, \text{Sign}(sk, m')\} \sim^S \{sk, \{\sigma_m\}_m, \text{SignDerive}(pk, (\{\sigma_m\}_m, M), m')\} \]

Randomizable Signature Case

- From \((m, \sigma)\) can publicly compute \(\sigma' \leftarrow \text{Rand}(\sigma)\)
- If \(\text{Vrfy}(m, \sigma) = 1\) then \(\text{Vrfy}(m, \sigma') = 1\)

Rand could add subliminal information in \(\{\sigma_m\}_{m \in \mathcal{M}}\) before \text{SignDerive}
New Context-Hiding Definitions (2)

Adaptive Context-Hiding Security

∀M ⊂ M, Vrfy(pk, M, \{σ_m\}_{m \in M}) = 1, m' ∈ M : P(M, m') = 1,

\{sk, \{σ_m\}_M, \text{Sign}(sk, m')\} \sim^S \{sk, \{σ_m\}_M, \text{SignDerive}(pk, (\{σ_m\}_M, M), m')\}

Complete Context-Hiding Security
New Context-Hiding Definitions (2)

Adaptive Context-Hiding Security

\[ \forall M \subset \mathcal{M}, \ Vrfy(pk, M, \{\sigma_m\}_{m \in M}) = 1, \ m' \in \mathcal{M} : P(M, m') = 1, \]
\[ \{sk, \{\sigma_m\}_m, \text{Sign}(sk, m')\} \sim^s \{sk, \{\sigma_m\}_m, \text{SignDerive}(pk, (\{\sigma_m\}_m, M), m')\} \]

Complete Context-Hiding Security
Linearly Homomorphic Signatures

Adaptively context-hiding security in the standard model:

- Signatures on $\vec{v} = (v_1, \ldots, v_n)$ of the form
  \[ \sigma = (\sigma_1, \sigma_2) = \left( \prod_{i=1}^{n} g_{i}^{v_i} \right)^{\alpha} \cdot (u^{\tau} \cdot v)^{r}, \ g^{r} \]

- Aggregation of
  - A one-time homomorphic signature of $\vec{v}$ as $\left( \prod_{i=1}^{n} g_{i}^{v_i} \right)^{sk}$
  - A Waters signature $\sigma = (\sigma_1, \sigma_2) = (h^{\alpha} \cdot (u^{\tau} \cdot v)^{r}, \ g^{r})$ on $\tau$

- Security proof requires groups of composite order $N = p_1 p_2 p_3$

- Adaptive context-hiding security under subgroup assumptions

- Variant in prime order groups is only weakly context-hiding
  
  ...but the shortest CDH-based signature in the standard model
Linearly Homomorphic Signatures

- **Keygen**(λ, n) : chooses groups \((G, G_T)\) of order \(N = p_1p_2p_3\) with a bilinear map \(e : G \times G \to G_T\), \(g, u, v, g_1, \ldots, g_n \stackrel{R}{\leftarrow} G_{p_1}, X_3 \stackrel{R}{\leftarrow} G_{p_3}\)

  Set

  \[ pk = (g, g^\alpha, u, v, g_1, \ldots, g_n, X_3), \quad sk = \alpha \in R \mathbb{Z}_N \]

- **Sign**(sk, τ, \(\vec{v} = (v_1, \ldots, v_n)\)) : choose \(r \in R \mathbb{Z}_N\), \(R_3, R_3' \stackrel{R}{\leftarrow} G_{p_3}\) and set

  \[ \sigma = (\sigma_1, \sigma_2) = (\prod_{i=1}^{n} g_i^{v_i})^\alpha \cdot (u^\tau \cdot v)^r \cdot R_3, \quad g^r \cdot R_3' \]

- **Verify**(pk, τ, \(\vec{v} = (v_1, \ldots, v_n), \sigma\)) : given, \(\sigma\) as \((\sigma_1, \sigma_2)\), return 1 iff

  \[ e(\sigma_1, g) = e\left(\prod_{i=1}^{n} g_i^{v_i}, g^\alpha\right) \cdot e(\sigma_2, u^\tau \cdot v) \]
Subset Predicates Signatures

- Binary predicate $P : \mathcal{M} \times \mathcal{M} \to \{0, 1\}$ defined such that

  \[ P(\text{Msg}, \text{Msg}') = 1 \iff \text{Msg'} \subseteq \text{Msg} \]

- Adversary should not mix elements of $\text{Msg}_1$ and $\text{Msg}_2$ in derived signatures

- Signatures on $\text{Msg} = \{m_1, \ldots, m_n\}$ obtained by
  1. Generating fresh pair $(sk', pk') \leftarrow \text{Keygen}(\lambda)$ and certifying $pk'$ with $\sigma_0 \leftarrow \text{Sign}(sk, pk')$
  2. Signing each $m \in \text{Msg}$ by computing $\sigma_m \leftarrow \text{Sign}(sk', m)$

Signature is $(pk', \sigma_0, \{\sigma_m\}_{m \in \text{Msg}})$ (Only weakly context-hiding)
Subset Predicates Signatures

- Binary predicate $P : \mathcal{M} \times \mathcal{M} \rightarrow \{0, 1\}$ defined such that

  $$P(\text{Msg, Msg'}) = 1 \iff \text{Msg' } \subseteq \text{Msg}$$

- Adversary should not mix elements of \text{Msg}_1 and \text{Msg}_2 in derived signatures

- Signatures on \text{Msg} = \{m_1, \ldots, m_n\} obtained by

  1. Generating fresh pair $(sk', pk') \leftarrow \text{Keygen}(\lambda)$ and certifying $pk'$ with
     $\sigma_0 \leftarrow \text{Sign}(sk, pk')$

  2. Signing each $m \in \text{Msg}$ by computing $\sigma_m \leftarrow \text{Sign}(sk', m)$

Signature is $(pk', \sigma_0, \{\sigma_m\}_{m \in \text{Msg}})$ (Only weakly context-hiding)
Subset Predicates Signatures

- Complete context-hiding security via randomizable proof systems (Groth-Sahai proofs)
- Signatures on a set $\text{Msg} = \{m_1, \ldots, m_n\}$ obtained by

1. Generating fresh pair $(sk', pk') \leftarrow \text{Keygen}(\lambda)$ and certifying $pk'$ with $\sigma_0 \leftarrow \text{Sign}(sk, pk')$
2. Signing each $m \in \text{Msg}$ by computing $\sigma_m \leftarrow \text{Sign}(sk', m)$
3. Commit to $(pk', \sigma_0), \{\sigma_m\}_{m \in \text{Msg}}$ and add NIWI randomizable proofs

Signature consists of all randomizable commitments and proofs

- Most efficient instantiation using Waters signatures and structure-preserving signatures (Abe et al., Crypto’10)
Conclusion

New privacy definitions

- Allowing for adversarially-randomized signatures
- A unified notion of complete context-hiding security

New constructions in the standard model

- Linearly homomorphic signatures:
  - Computational adaptive context-hiding security
  - Variant gives a new, more efficient CDH-based construction (25% shorter than Freeman’s)
  - Recently (PKC’13): a completely context-hiding scheme

- Subset predicates: construction with short public keys using a new approach (i.e., not based on attribute-based encryption)
Thank you!