Key-Homomorphic Signatures
and Applications to Simulation Sound Extractable NIZK

David Derler, Graz University of Technology
March 22, 2017—Paderborn University

Based on joint work with Daniel Slamanig
Example 1

- Given two signatures $\sigma_1$ and $\sigma_2$ on $m$
- Valid under $pk_1$ and $pk_2$
  $\Rightarrow$ Publicly compute $\sigma'$ valid under $pk' = pk_1 \circ pk_2$

Example 2

- Given a signature $\sigma$ on $m$ valid under $pk$
- Adapt $\sigma$ to $\sigma'$ valid under $pk'$
- Well defined relationship between $pk$ and $pk'$

Extremely simple, yet very powerful!

- Never explicitly studied before
Implicit usage in signatures schemes:

- Security under related (re-randomized) keys \([BCM11,BPT12]\)
- DSS under randomizable keys \([FKM^{+}16]\)
- DSS from canonical identification schemes \([FF13,KMP16]\)

Other directions:

- Key-homomorphic encryption \([\text{AHI}11, \text{Rot}11, \text{BGG}^{+}14, \text{DMS}16]\)
- (Constrained) key-homomorphic PRFs \([\text{BLMR}13, \text{BP}14, \text{BFP}^{+}15]\)
- Key-homomorphic projective hashes \([\text{BJL}16, \text{BJL}17]\)
Results in [DS16]

- publicly key-hom. DSS
- adaptable DSS
- perfectly adaptable DSS
- Multisignatures [IN83]
- tight key-prefixed MU-EUF-CMA [GMS02, MS04]
- Ring Signatures [RST01]
- (weak) SSE NIZK [Gro06]
- Universal Designated Verifier DSS [SBWPO3]
- key-succinct multikey hom. DSS

Diagram:
- sk → pk hom. DSS
- adaptability:
  - publicly key-hom. DSS
  - adaptable DSS
  - perfectly adaptable DSS
- Relationships:
  - RSR canonical ID schemes [KMP16]
  - + RO
  - + NIWI
  - + NIWI
- Other components:
  - key-succinct multikey hom. DSS
  - Multisignatures [IN83]
  - tight key-prefixed MU-EUF-CMA [GMS02, MS04]
  - Ring Signatures [RST01]
  - (weak) SSE NIZK [Gro06]
  - Universal Designated Verifier DSS [SBWPO3]
Outline

Covered in this talk

- publicly key-hom. DSS
- adaptable DSS
- perfectly adaptable DSS
- key-succinct multikey hom. DSS

→ Multisignatures [IN83]
→ tight key-prefixed MU-EUF-CMA [GMS02, MS04]
→ RSR canonical ID schemes [KMP16]
→ + RO
→ adaptable DSS

→ + NIWI
→ + NIWI
→ + NIWI

→ Ring Signatures [RST01]
→ (weak) SSE NIZK [Gro06]
→ Universal Designated Verifier DSS [SBWPO3]

→ [CLO6]
→ SoKs [CLO6]
Variants of key-homomorphisms

- Publicly key-hom. DSS
- Adaptable DSS
- Perfectly adaptable DSS

- Multisignatures [IN83]
- Tight key-prefixed MU-EUF-CMA [GMS02, MS04]
- Ring Signatures [RST01]
- (Weak) SSE NIZK [Gro06]
- Universal Designated Verifier DSS [SBWPO3]
- Key-succinct multikey hom. DSS
Secret keys and public keys live in groups $G$ and $H$

- Group homomorphism $\mu : H \rightarrow G$

\[ \forall \ sk, sk' \in H : \mu(sk + sk') = \mu(sk) + \mu(sk') \]

+ For all $(sk, pk) \leftarrow \text{KeyGen}(1^\kappa)$ it must hold that 

\[ pk = \mu(sk) \]

Keys may also be vectors:

- Straightforward extension
- Not made explicit for compactness
Class of functions $\Phi^+$

- Representing linear shifts
- Functions identified by “shift amount” $\Delta$

Conventional signature scheme

- Secret-key-to-public-key homomorphism
- Additional PPT algorithm

$$(pk', \sigma') \leftarrow \text{Adapt}(pk, m, \sigma, \Delta)$$

⇒ Shift signature from $pk$ to $pk' = pk \cdot \mu(\Delta)$

Question: possible to have $\text{Adapt}'$ taking $\mu(\Delta)$ instead of $\Delta$?

- No: efficient $\text{Adapt}'$ would imply an UUF-NMA adversary
Identical distribution of fresh and adapted signatures

• “Initial” signature on $m$ under $sk$ not revealed

\[
\text{Adapt}(pk, m, \text{Sign}(sk, m), \Delta) \quad \text{and} \quad (pk \cdot \mu(\Delta), \text{Sign}(sk + \Delta, m))
\]
Perfect Adaptation of Signatures

Identical distribution of fresh and adapted signatures

- Even when seeing the initial signatures $\sigma \leftarrow \text{Sign}(sk, m)$

$$(\sigma, \text{Adapt}(pk, m, \sigma, \Delta))$$

$$(\sigma, pk \cdot \mu(\Delta), \text{Sign}(sk + \Delta, m))$$
Publicly Key-Homomorphic Signatures

Conventional signature scheme with

- Secret-key-to-public-key homomorphism
- Additional algorithm Combine

\[(\hat{pk}, \hat{\sigma}) \leftarrow \text{Combine}((pk_i)_{i=1}^n, m, (\sigma_i)_{i=1}^n)\]

- Combine multiple signatures on \(m\) under distinct keys
- Combined key \(\hat{pk} = \prod_{i=1}^n pk_i\)
Examples of Key-Homomorphic Schemes

Publicly key-homomorphic schemes

- BLS signatures [BLS04]
- CL signature variant [CHP12]
- Waters’ signatures with shared params [Wat05, BFG13]

Adaptable schemes

- Schnorr signatures [Sch91]
- Katz-Wang signatures [KWO3, GJKW07]

Perfectly adaptable schemes

- BLS signatures [BLS04]
- CL signature variant [CHP12]
- Waters’ signatures with shared params [Wat05, BFG13]
- Pointcheval-Sanders signatures [PS16]
Outline

Application to SSE NIZK

publicly key-hom. DSS

adaptable DSS

perfectly adaptable DSS

RSR canonical ID schemes [KMP16]

sk → pk hom. DSS

Multisignatures [IN83]

tight key-prefixed MU-EUF-CMA [GMS02, MS04]

Ring Signatures [RST01]

(weak) SSE NIZK [Gro06]

Universal Designated Verifier DSS [SBWPO3]

key-succinct multikey hom. DSS
Non-Interactive Proof Systems

NP-language $L$ w.r.t. relation $R$

- $x \in L \iff \exists w : (x, w) \in R$

Non-interactive proof system

$(x, w) \in R$

$\pi \leftarrow \text{Proof}(x, w)$

$\checkmark/\times \leftarrow \text{Verify}(x, \pi)$
Non-Interactive Proof Systems - Properties

Completeness

• Honestly computed proof for \((x, w) \in R\) will always verify

Soundness

• Infeasible to produce valid proof for \(x \notin L\)

Extractability

• Stronger variant of soundness
• Extract witness from valid proof (using trapdoor)
Witness Indistinguishability (WI)

- Distinguish proofs for same x w.r.t. different $w, w'$

Zero-Knowledge (ZK)

- Stronger variant of witness indistinguishability
- Simulate proofs without knowing $w$ (using trapdoor)
Simulation Sound Extractability (SSE)

Very strong notion

- Combination of zero-knowledge and extractability
- Adversary sees simulated proofs for arbitrary \( x \)
- Still infeasible to forge proof for new \( x \notin L \)

\[ \Rightarrow \] Can extract witness for any proof with “new” \( x \)

Requires non-malleability

- **weak SSE**: non-malleability w.r.t. proven statement
- **SSE**: non-malleability w.r.t. proof and proven statement
Construction Idea - weak SSE

Extend proof with adaptable signature

- Sign proof under a random key $pk'$
- Include signature on proven statement under $pk'$

Extend Language $L$ to $L'$

- Include $pk$ in CRS

$$x \in L \iff \exists w : (x, w) \in R$$

$$(x, pk, pk') \in L' \iff \exists w : (x, w) \in R \lor \exists \Delta : pk = pk' \cdot \mu(\Delta)$$

$\Rightarrow$ Shift amount allows to extract valid signature under $pk$

Can construct an SSE NIZK proof system for $L$

- From extractable WI proof system for $L'$
  + Adaptable signature scheme
Observations

- Either need witness for 1st or 2nd literal in OR clause

\[(x, w) \in R \lor \exists \Delta : pk = pk' \cdot \mu(\Delta)\]

- Prover has to use \(w\) s.t. \((x, w) \in R\)

\[\Rightarrow \text{Otherwise needs signature under } pk\]

Zero-Knowledge

- Set up CRS so that \(sk\) for \(pk\) is known
- Create signature \(\sigma\) on proof under \(sk\)
- Shift \(\sigma\) to \(\sigma'\) under random key \(pk'\)
- Create proof using “shift amount” \(\Delta\)

\[\Rightarrow \text{Cannot be detected under WI}\]
Weak Simulation Sound Extractability

- Simulate as before
  - Use $pk$ from EUF-CMA challenger
  - Obtain signatures via $\text{Sign}$ oracle
- Use extractor from underlying proof system
- EUF-CMA implies extraction of $w$ s.t. $(x, w) \in R$

Simulation Sound Extractability

- Additionally use strong one-time DSS
Recall Waters’ variant in SXDH setting

- Public parameters \( U = (u_0, \ldots, u_n) \sim \mathbb{G}_1^n \)
- Waters’ hash \( H(m) := u_0 \prod_{i \in [n]} u_i^{m_i} \) where \( m \in \{0, 1\}^m \)
- Public key: \( sk \sim g^x \in \mathbb{G}_1, pk \sim \hat{g}^x \in \mathbb{G}_2, \) with \( x \sim \mathbb{Z}_p \)
- Signature: \( \sigma \sim (g^x \cdot H(m)^r, g^r, \hat{g}^r) \), with \( r \sim \mathbb{Z}_p \)
- Verification via pairing

Perfect adaptability

- Signature \( \sigma = (\sigma_1, \sigma_2, \sigma_3) \)
- Shift amount \( \Delta = (\Delta_1, \Delta_2) \in \mathbb{G}_1 \times \mathbb{G}_2 \)
- With \( e(\Delta_1, \hat{g}) = e(g, \Delta_2) \)
- Shift \( \left( pk', \sigma' \right) \sim (\hat{g}^x \cdot \Delta_2, (\sigma_1 \cdot \Delta_1 \cdot H(m)^{r'}, \sigma_2 \cdot g^{r'}, \sigma_3 \cdot \hat{g}^{r'}) \)

Combination with Groth-Sahai proofs

- Only requires to prove knowledge of single element in \( \mathbb{G}_1 \)!
Conclusions

Generic compilers for various signature variants

- Applicable to large classes of schemes
- Strong security guarantees from very mild requirements
- Extremely simple
- Favorable regarding efficiency w.r.t. previous schemes
- Deeper understanding of construction paradigms

Directly yields novel instantiations

- Comparing favorably to existing work
- Standard model & assumptions: Waters’ sigs + GS proofs
Conclusions

Results in [DS16]

- publicly key-hom. DSS
- adaptable DSS
- perfectly adaptable DSS

- Multisignatures [IN83]
- tight key-prefixed MU-EUF-CMA [GMS02, MS04]
- Ring Signatures [RST01]
- (weak) SSE NIZK [Gro06]
- Universal Designated Verifier DSS [SBWPO3]

- key-succinct multikey hom. DSS

\[ \text{sk} \mapsto \text{pk hom. DSS} \]

- RSR canonical ID schemes [KMP16]

- + RO
- + NIWI
- + NIWI
Thank you.

Preprint available as IACR ePrint Archive Report 2016/792

✉️ david.derler@iaik.tugraz.at   🔄 @dderler