Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups

Masayuki Abe, NTT

Jens Groth, University College London

Kristiyan Haralambiev, NYU

Miyako Ohkubo, NICT

Mathematical structures in cryptography

- Cyclic prime order group $\mathbb{G}$
- Useful mathematical structure
  - ElGamal encryption
  - Pedersen commitments
  - Schnorr proofs
  - …

Pairing-based cryptography

- Groups $\mathbb{G}$, $\mathbb{H}$, $\mathbb{T}$ with bilinear map e: $\mathbb{G}\times\mathbb{H}\rightarrow\mathbb{T}$
- Additional mathematical structure
  - Identity-based encryption
  - Short digital signatures
  - Non-interactive zero-knowledge proofs
  - …

Bilinear group

- Gen(1^k) returns $(p,\mathbb{G},\mathbb{H},\mathbb{T},G,H,e)$
  - Groups $\mathbb{G}$, $\mathbb{H}$, $\mathbb{T}$ of prime order p
  - $\mathbb{G} = \langle G \rangle$, $\mathbb{H} = \langle H \rangle$
  - Bilinear map $e: \mathbb{G}\times\mathbb{H}\rightarrow\mathbb{T}$
    - $e(G^a,H^b) = e(G,H)^{ab}$
    - $\mathbb{T} = \langle e(G,H) \rangle$
  - Can efficiently compute group operations, evaluate bilinear map and decide membership

Asymmetric group

No efficiently computable homomorphisms between $\mathbb{G}$ and $\mathbb{H}$

Structure-preserving signatures with generic signer

- The public verification key, the messages and the signatures consist of group elements in $\mathbb{G}$ and $\mathbb{H}$
- The verifier evaluates pairing product equations
  - Accept signature if

$$e(M,V_1)e(S_1,V_2) = 1$$
$$e(S_2,V_2)e(M,V_2) = e(G,V_3)$$

- The signer only uses generic group operations
  - Signature of the form $(S_1,S_2,\ldots)$ where

$$S_1 = M^{\alpha}G^{\beta},\ S_2 = \ldots$$

Structure-preserving signatures

- Composes well with other pairing-based schemes
  - Easy to encrypt structure-preserving signatures
  - Easy use with non-interactive zero-knowledge proofs
  - …
- Applications
  - Group signatures
  - Blind signatures
  - …

Results

- Lower bound
  - A structure-preserving signature consists of at least 3 group elements
- Construction
  - A structure-preserving signature scheme matching the lower bound

Lower bound

- Theorem
  - A structure-preserving signature made by a generic signer consists of at least 3 group elements
- Proof uses the *structure-preservation* and the fact that the signer only does *generic group* operations
  - Not information-theoretic bound
    - Shorter non-structure-preserving signatures exist
  - Uses generic group model on signer instead of adversary

Proof overview

- Without loss of generality lower bound for $M \in \mathbb{G}$
- Theorems
  - Impossible to have unilateral structure-preserving signatures (all elements in $\mathbb{G}$ or all elements in $\mathbb{H}$)
  - Impossible to have a single verification equation (for example $e(S_2,V_2)e(M,V_2) = 1$)
  - Impossible to have signatures of the form $(S,T) \in \mathbb{G} \times \mathbb{H}$

Unilateral signatures are impossible

A similar argument shows there are no unilateral signatures $(S_1,S_2,\ldots,S_k) \in \mathbb{G}^k$

- Case I
  - There is no single element signature $S \in \mathbb{G}$ for $M \in \mathbb{G}$
- Proof
  - If $S \in \mathbb{G}$ the verification equations are wlog of the form

$$e(M,V)e(S,W) = Z$$

  - Given two signatures S_1, S_2 on random M_1, M_2 we have for all the verification equations

$$e(M_1^2 M_2^{-1},V)e(S_1^2 S_2^{-1},W) = Z$$

  - This means $S_1^2 S_2^{-1}$ is a signature on $M_1^2 M_2^{-1}$

Unilateral signatures are impossible

A similar argument shows there are no unilateral signatures $(T_1, T_2, \ldots, T_k) \in \mathbb{H}^k$

- Case II
  - There is no single element signature $T \in \mathbb{H}$ for $M \in \mathbb{G}$
- Proof
  - A generic signer wlog computes $T = H^t$ where t is chosen independently of M
  - Since T is independent of M either the signature scheme is not correct or the signature is valid for any choice of M and therefore easily forgeable

A single verification equation is impossible

- Theorem
  - There is no structure-preserving signature for message $M \in \mathbb{G}$ with a single verification equation
- Proof
  - Let the public key be $(U_1, U_2, \ldots, V_1, V_2, \ldots)$
  - The most general verification equation is of the form
    $$\prod e(S_i, T_j)^{a_{ij}} \prod e(S_i, V_j)^{b_{ij}} \prod e(M, T_j)^{c_j} \prod e(M, V_j)^{d_j} \prod e(U_i, T_j)^{e_{ij}} = Z$$
  - Using linear algebra we can show the scheme is vulnerable to a random message attack

No signature with 2 group elements

- Theorem
  - There are no 2 group element structure-preserving signatures for $M \in \mathbb{G}$
- Proof strategy
  - Since signatures cannot be unilateral we just need to rule out signatures of the form $(S,T) \in \mathbb{G} \times \mathbb{H}$
  - Generic signer generates them as $S = M^{\alpha} G^{\beta}$ and $T = H^{\tau}$
  - Proof shows the correctness of the signature scheme implies all the verification equations collapse to a single verification equation, which we know is impossible

No signature with 2 group elements

- Proof sketch
  - Consider wlog a verification equation of the form

$$e(S,T)^a e(M,T)^b e(U,T) e(S,V) e(M,W) = Z$$

  - Taking discrete logarithms and using the bilinearity of e

$$ast + bmt + ut + sv + mw = z$$

  - Using that the generic signer generates $S = M^{\alpha}G^{\beta}$ and $T = H^{\tau}$ we have $s = \alpha m+\beta$ and $t = \tau$ giving us

$$(a\alpha + b\tau + \alpha v + w)m + a\beta\tau + u\tau + \beta v = z$$

  - A generic signer does not know m, so the correctness of the signature scheme implies

$$a\alpha + b\tau + \alpha v + w = 0 \qquad a\beta\tau + u\tau + \beta v = z$$

No signature with 2 group elements

- Proof sketch cont'd
  - Each verification equation corresponds to a pair of equalities of the form

$$a\alpha + b\tau + \alpha v + w = 0 \qquad a\beta\tau + u\tau + \beta v = z$$

  - Using linear algebra we can show that all these pairs of equalities are linearly related
  - So they are equivalent to a single verification equation
  - By our previous theorem a single verification equation is vulnerable to a random message attack
  - Therefore 2 group element structure-preserving signatures can be broken by a random message attack

Optimal structure-preserving signatures

- Signature scheme
  - Messages $(M_1,M_2,\ldots,N_1,N_2,\ldots) \in \mathbb{G}^{k_M} \times \mathbb{H}^{k_N}$
  - Public key $(U_1,U_2,\ldots,V,W_1,W_2,\ldots,Z) \in \mathbb{G}^{k_M} \times \mathbb{H}^{k_N+2}$
  - Signing key $(u_1,u_2,\ldots,v,w_1,w_2,\ldots,z) \in (\mathbb{Z}_p^*)^{k_M+k_N+2}$
  - Signatures $(R,S,T) \in \mathbb{G}^2 \times \mathbb{H}$

$$R = G^r \qquad S = G^{z-rv} \prod M_i^{-w_i} \qquad T = H\left(\prod N_i^{-u_i}\right)^{\frac{1}{r}}$$

  - Verification

$$e(R,V)e(S,H)\prod e(M_i,W_i) = 1$$
$$e(R,T)\prod e(U_i,N_i) = e(G,H)$$

Optimal structure-preserving signatures

- Optimal
  - Signature size is 3 group elements
  - Verification uses 2 pairing product equations
- Security
  - Strongly existentially unforgeable under adaptive chosen message attack
  - Proven secure in the generic group model

Further results

- One-time signatures (unilateral messages)
  - Unilateral, 2 group elements, single verification equation
- Non-interactive assumptions (q-style)
  - 4 group elements for unilateral messages
  - 6 group elements for bilateral messages
- Rerandomizable signatures
  - 3 group elements for unilateral messages

Summary

- Lower bound
  - Structure-preserving signatures created by generic signers consist of at least 3 group elements
- Optimal construction
  - Structure-preserving signature scheme with 3 group element signatures that is sEUF-CMA in the generic group model