Efficient Non-interactive Proof Systems for Bilinear Groups

Jens Groth

University College London

Amit Sahai

University of California Los Angeles

Non-interactive proof

Zero-knowledge: Bob learns nothing about witness

Witness w

$(x,w) \in R_L$

Statement $\in L$

Proof

Why?

Witness-indistinguishable: Bob does not learn *which* witness Alice has in mind

Yes dear, $x \in L$

A brief history of non-interactive zero-knowledge proofs

- Blum-Feldman-Micali 88
- Damgård 92
- Feige-Lapidot-Shamir 99
- Kilian-Petrank 98
- De Santis-Di Crescenzo-Persiano 02

Efficiency problems with non-interactive zero-knowledge proofs

- Non-interactive proofs for general NP-complete language such as Circuit SAT. Any practical statement such as ”the ciphertext c contains a signature on m” must go through a size-increasing NP-reduction.

- Inefficient non-interactive proofs for Circuit SAT. Use the so-called ”hidden random bits” method.

Our goal

- We want non-interactive proofs for statements arising in practice such as ”the ciphertext c contains a signature on m”. No NP-reduction!

- We want high efficiency. Practical non-interactive proofs!

A brief history of non-interactive zero-knowledge proofs continued

	Circuit SAT	Practical statements
Inefficient	Kilian-Petrank 98	Groth 06
Efficient	Groth-Ostrovsky-Sahai 06	This work

Bilinear group

Prime order or composite order

$G_1 = G_2$ or $G_1 \neq G_2$

- G_1, G_2, G_T finite cyclic groups of order n
- P_1 generates G_1, P_2 generates G_2
- e: $G_1 \times G_2 \rightarrow G_T$
  - $e(P_1,P_2)$ generates G_T
  - $e(aP_1,bP_2) = e(P_1,P_2)^{ab}$
- Deciding membership, group operations, bilinear map efficiently computable

Many possible assumptions: Subgroup Decision, Symmetric External Diffie-Hellman, Decison Linear, ...

Constructions in bilinear groups

$a, b \in Z_n$, $A, C \in G_1$, $B, D \in G_2$

→

$t = a+xb$

$T_1 = xY+xA+tC$

$T_2 = B+D+Z$

$t_T = e(T_1,B+bT_2)$

Non-interactive cryptographic proofs for correctness of constructions

Yes, here is a proof.

Are the constructions correct? I do not know your secret x, Y, Z.

→

$t = a+xb$

$T_1 = xY+xA+tC$

$T_2 = B+D+Z$

$t_T = e(T_1,B+bT_2)$

→ Proof

Cryptographic constructions

- Constructions can be built from
  - public exponents and public group elements
  - secret exponents and secret group elements
- Using any of the bilinear group operations
  - Addition and multiplication of exponents
  - Point addition or scalar multiplication in G_1 or G_2
  - Bilinear map e
  - Multiplication in G_T
- Our result: Non-interactive cryptographic proofs for correctness of a set of bilinear group constructions

Examples of statements we can prove

- Here is a ciphertext c and a signature s. They have been constructed such that s is a signature on the secret plaintext.
- Here are three commitments A,B and C to secret exponents a,b and c. They have been constructed such that c=ab mod n.

Quadratic equations in a bilinear group

- Variables $X_i \in G_1, Y_i \in G_2, x_i, y_i \in Z_n$
- Pairing product equations

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

- Multi-scalar multiplication equations in G_1 (or G_2)

$$T_1 = \sum_{i=1}^{n'} y_i A_i + \sum_{i=1}^{m} b_i X_i + \sum_{i=1}^{m} \sum_{j=1}^{n'} \gamma_{ij} y_j X_i$$

- Quadratic equations in $\mathbf{Z}_n$

$$t = \sum_{i=1}^{n'} a_i y_i + \sum_{i=1}^{m'} x_i b_i + \sum_{i=1}^{m'} \sum_{j=1}^{n'} \gamma_{ij} x_i y_j$$

Our contribution

- Statement S = (eq_1,...,eq_N) bilinear group equations
- Efficient non-interactive witness-indistinguishable (NIWI) proofs for satisfiability of all equations in S
- Efficient non-interactive zero-knowledge (NIZK) proofs for satisfiability of all equations in S (all t_T=1)
- Many choices of bilinear groups and cryptographic assumptions Subgroup Decision, Symmetric External Diffie-Hellman, Decision Linear, etc.
- Common reference string O(1) group elements

Size of NIWI proofs

Each equation constant cost.
Cost independent of number of public constants and secret variables.
NIWI proofs can have sub-linear size compared with statement!

Cost of each variable/equation	Subgro Decision	al DH	Linear
Variable in G_1, G_2 or $\mathbf{Z}_n$	1		3
Pairing product	1	8	9
Multiscalar mult.	1	6	9
Quadratic in $\mathbf{Z}_n$	1	4	6

Size of NIZK proofs

Cost of each variable/equation	Subgroup Decision	Symmetric External DH	Decision Linear
Variable in $\mathbf{Z}_n$	1	2	3
Variable in G_1, G_2	1 (+3)	2 (+10)	3 (+15)
Pairing product equation (t_T=1)	1	8	9
Multiscalar mult.	2	10	12
Quadratic in $\mathbf{Z}_n$	1	4	6

Applications of efficient NIWI and NIZK proofs

- Constant size group signatures
  Boyen-Waters 07 (independently of our work)
  Groth 07
- Sub-linear size ring signatures
  Chandran-Groth-Sahai 07
- Non-interactive NIZK proof for correctness of shuffle
  Groth-Lu 07
- Non-interactive anonymous credentials
  Belienky-Chase-Kohlweiss-Lysyanskaya 08
- …

Where does the generality come from?

- View bilinear groups as special cases of modules with a bilinear map
- Commutative ring R
- R-modules A_1, A_2, A_T
- Bilinear map f: $A_1 \times A_2 \rightarrow A_T$

Pairing product equations

- Pairing product equations

$$t_T = \prod_{i=1}^{n} e(A_i ; Y_i) \cdot \prod_{i=1}^{m} e(X_i ; B_i) \cdot \prod_{i=1}^{m}\prod_{j=1}^{n} e(X_i ; Y_j)^{\gamma_{ij}}$$

- Use R = $\mathbf{Z}_n$, $A_1 = G_1$, $A_2 = G_2$, $A_T = G_T$, f(X,Y)=e(X,Y) and write $A_T = G_T$with additive notation to get

$$t_T = \sum_{i=1}^{n} f(A_i ; Y_i) + \sum_{i=1}^{m} f(X_i ; B_i) + \sum_{i=1}^{m}\sum_{j=1}^{n} \gamma_{ij} f(X_i ; Y_j)$$

Multi-scalar multiplication in G_1

- Multi-scalar multiplication equations in G_1

$$T_1 = \sum_{i=1}^{n'} y_i A_i + \sum_{i=1}^{m} b_i X_i + \sum_{i=1}^{m} \sum_{j=1}^{n'} \gamma_{ij} y_j X_i$$

- Use $R = \mathbf{Z}_n$, $A_1 = G_1$, $A_2 = \mathbf{Z}_n$, $A_T = G_1$, $f(X,y)=yX$

$$T_1 = \sum_{i=1}^{n'} f(A_i; y_i) + \sum_{i=1}^{m} f(X_i; b_i) + \sum_{i=1}^{m} \sum_{j=1}^{n'} \gamma_{ij} f(X_i; y_j)$$

Quadratic equation in Z_n

- Quadratic equations in $\mathbf{Z}_n$

$$t = \sum_{i=1}^{n'} a_i y_i + \sum_{i=1}^{m'} x_i b_i + \sum_{i=1}^{m'} \sum_{j=1}^{n'} \gamma_{ij} x_i y_j$$

- Use R = $\mathbf{Z}_n$, $A_1 = \mathbf{Z}_n$, $A_2 = \mathbf{Z}_n$, $A_T = \mathbf{Z}_n$, f(x,y)=xy

$$t = \sum_{i=1}^{n'} f(a_i, y_i) + \sum_{i=1}^{m'} f(x_i, b_i) + \sum_{i=1}^{m'} \sum_{j=1}^{n'} \gamma_{ij} f(x_i, y_j)$$

Generality continued

- All four types of bilinear group equations can be seen as example of quadratic equations over modules with bilinear map
- The assumptions Subgroup Decision, Symmetric External Diffie-Hellman, Decision Linear, etc., can be interpreted as assumption in (different) modules with bilinear map as well

Sketch of NIWI proofs

$$t = \sum_{i=1}^{n'} f(a_i; y_i) + \sum_{i=1}^{m'} f(x_i; b_i) + \sum_{i=1}^{m'} \sum_{j=1}^{n'} \gamma_{ij} f(x_i; y_j)$$

- Commit to secret elements in A_1 and A_2
- Commitment scheme is homomorphic with respect to addition in A_1, A_2, A_T and with respect to bilinear map f
- Can therefore use homomorphic properties to get commitment $c = \text{commit}_{A_T}(t; r)$
- Reveal commitment randomizer r to verify that equation is satisfied
- To get witness-indistinguishability first rerandomize commitment c before opening with r´

Final remarks

- Summary: Efficient non-interactive cryptographic proofs for use in bilinear groups
- Open problem: Construct cryptographically useful modules with bilinear map that are not based on bilinear groups
- Acknowledgment: Thanks to Brent Waters
- Questions?