Batch Groth-Sahai

Olivier Blazy Georg Fuchsbauer Malika Izabachène
Amandine Jambert Hervé Sibert Damien Vergnaud

ENS - Paris - France

ACNS 2010

1 Introduction

1. Introduction
2. Groth Sahai Proof System
3. Batching Technique

1. Introduction
   - Non Interactive Zero Knowledge Proof
   - Non Interactive Witness Indistinguishable Proof
   - Bilinear Groups
   - Standard Assumptions
2. Groth Sahai Proof System
3. Batching Technique
4. Applications

Definition

A NIZK proof is a non-interactive protocol letting one party proving to another that a statement is true, without revealing anything other than the veracity of the statement.

Alice possesses a secret $s \in \mathcal{L}$ with a witness θ_s.

I know a secret $x \in \mathcal{L}$ $\longrightarrow$

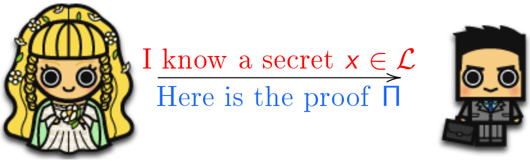
Here is the proof $\Pi(\theta_s)$

Bob is now convinced Alice possesses a secret $x \in \mathcal{L}$.

Definition

A NIWI proof is a non-interactive protocol where the verifier can't distinguish two instances of different secrets.

Alice possesses secret a secret $s \in \mathcal{L}$ with a witness $\theta_s \in T = \{\theta_1, \dots, \theta_n\}$. Bob knows T.



Bob can't decide which secret is known by Alice, despite his knowledge of T.

Bilinear Groups

- $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ finite cyclic groups of order p
- g_1 generates $\mathbb{G}_1$, g_2 generates $\mathbb{G}_2$
- $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$
- $e(g_1, g_2)$ generates $\mathbb{G}_T$
- $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$

SXDH/ DLIN assumptions

SXDH

Given $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$,
(u, u^x, u^y, u^z) and $(u, u^x, u^y, u^{x \cdot y})$ are computationally indistinguishable.(DDH is hard in both group)

DLIN

Given $(p, \mathbb{G}, \mathbb{G}_T, e, g)$,
(u, v, w, u^a, v^b, w^c) and $(u, v, w, u^a, v^b, w^{a+b})$ are computationally indistinguishable.

$\vec{a}, \vec{b} \in \mathbb{Z}_N^n$ and $\vec{\mathcal{A}}, \vec{\mathcal{B}} \in \mathbb{G}^n$.

$\langle \vec{a}, \vec{b} \rangle := \sum_{i=1}^n a_i \cdot b_i \quad \langle \vec{a}, \vec{\mathcal{B}} \rangle := \prod_{i=1}^n \mathcal{B}_i^{a_i} \quad \langle \vec{\mathcal{A}}, \vec{\mathcal{B}} \rangle := \prod_{i=1}^n e(\mathcal{A}_i, \mathcal{B}_i)$

(SXDH) $\bullet : \mathbb{G}_1^{n \times k} \times \mathbb{G}_2^{n \times k} \to \mathbb{G}_T^{k \times k}$

$\vec{\mathbf{c}} \bullet \vec{\mathbf{d}} := (\prod_{\ell=1}^n e(c_{\ell,i}, d_{\ell,j}))_{1 \leq i,j \leq k}$

(DLIN) $\overset{s}{\bullet} : \mathbb{G}^{n \times 3} \times \mathbb{G}^{n \times 3} \to \mathbb{G}_T^{3 \times 3}$

$\vec{\mathbf{c}} \overset{s}{\bullet} \vec{\mathbf{d}} := \left(\prod_{\ell=1}^n e(c_{\ell,i}, d_{\ell,j})^{1/2} e(c_{\ell,j}, d_{\ell,i})^{1/2}\right)_{1 \leq i,j \leq 3}$

Pairing-product equation:

$$\langle \vec{\mathcal{A}}, \vec{\mathcal{Y}} \rangle \cdot \langle \vec{\mathcal{X}}, \vec{\mathcal{B}} \rangle \cdot \langle \vec{\mathcal{X}}, \Gamma \vec{\mathcal{Y}} \rangle = t_T$$

Multi-scalar multiplication equation (in $\mathbb{G}_1$):

$$\langle \vec{x}, \vec{\mathcal{B}} \rangle \cdot \langle \vec{a}, \vec{\mathcal{Y}} \rangle \cdot \langle \vec{x}, \Gamma \vec{\mathcal{Y}} \rangle = T$$

Quadratic equation in $\mathbb{Z}_N$

$$\langle \vec{a}, \vec{y} \rangle + \langle \vec{x}, \vec{b} \rangle + \langle \vec{x}, \Gamma \vec{y} \rangle = t$$

(DLIN) Pairing Product Equation: $\langle \vec{\mathcal{A}}, \vec{\mathcal{Y}} \rangle \cdot \langle \vec{\mathcal{Y}}, \Gamma \vec{\mathcal{Y}} \rangle = t_T$

The verification relation of a proof $(\vec{\mathbf{d}}, \phi) \in \mathbb{G}^{n \times 3} \times \mathbb{G}^{3 \times 3}$ is the following:

$$\left[\iota(\vec{\mathcal{A}}) \overset{s}{\bullet} \vec{\mathbf{d}}\right] \odot \left[\vec{\mathbf{d}} \overset{s}{\bullet} \Gamma \vec{\mathbf{d}}\right] = \iota_T(t_T) \odot \left[\vec{\mathbf{u}} \overset{s}{\bullet} \vec{\phi}\right]$$

Small Exponents Test, BGR EC'98

$$\begin{cases} \prod_{i=1}^{k_1} e(f_{i,1}, h_{i,1})^{c_{i,1}} = A_1 \\ \dots \\ \prod_{i=1}^{k_n} e(f_{i,n}, h_{i,n})^{c_{i,n}} = A_n \end{cases}$$

Small Exponents Test, BGR EC'98

$$\left\{\begin{array}{l} \prod_{i=1}^{k_1} e(f_{i,1}, h_{i,1})^{c_{i,1}} = A_1 \\ \ldots \\ \prod_{i=1}^{k_n} e(f_{i,n}, h_{i,n})^{c_{i,n}} = A_n \end{array}\right.$$

- Pick small random exponents $\delta_1, \ldots, \delta_n$
- Check $\prod_{j=1}^{n} \prod_{i=1}^{k_j} e(f_{i,j}, h_{i,j})^{c_{i,j}\delta_j} = \prod_{j=1}^{m} A_j^{\delta_j}$

Small Exponents Test, BGR EC'98

$$\begin{cases} \prod_{i=1}^{k_1} e(f_{i,1}, h_{i,1})^{c_{i,1}} = A_1 \\ \dots \\ \prod_{i=1}^{k_n} e(f_{i,n}, h_{i,n})^{c_{i,n}} = A_n \end{cases}$$

- Pick small random exponents $\delta_1, \dots, \delta_n$
- Check $\prod_{j=1}^{n} \prod_{i=1}^{k_j} e(f_{i,j}, h_{i,j})^{c_{i,j}\delta_j} = \prod_{j=1}^{m} A_j^{\delta_j}$

Theorem (Ferrara, Green, Hohenberger and Pedersen, CT-RSA 09)

Given m pairing-based verification equations, the verifier with random exponents $\delta_1, \dots, \delta_m$ of ℓ bits accepts an invalid batch with probability at most $2^{-\ell}$.

1. **Move the exponent into the pairing:**
   $e(f_i, h_i)^{\delta_i} \rightarrow e(f_i^{\delta_i}, h_i)$

1. **Move the exponent into the pairing:**
   $e(f_i, h_i)^{\delta_i} \rightarrow e(f_i^{\delta_i}, h_i)$
2. **Move the product into the pairing:**
   $\prod_{j=1}^{m} e(f_j^{\delta_j}, h_i) \rightarrow e\left(\prod_{j=1}^{m} f_j^{\delta_j}, h_i\right)$

1. **Move the exponent into the pairing:**
   $e(f_i, h_i)^{\delta_i} \to e(f_i^{\delta_i}, h_i)$
2. **Move the product into the pairing:**
   $\prod_{j=1}^{m} e(f_j^{\delta_j}, h_i) \to e\left(\prod_{j=1}^{m} f_j^{\delta_j}, h_i\right)$
3. **Switch two products:**
   $\prod_{i=1}^{k} e\left(\prod_{j=1}^{m} f_j^{\delta_{i,j}}, h_i\right) \leftrightarrow \prod_{j=1}^{m} e\left(f_j, \prod_{i=1}^{k} h_i^{\delta_{i,j}}\right)$

$$
\begin{pmatrix}
\prod_{i=1}^{n} e(d_{i,1}, \prod d_{k,1}^{\gamma_{i,k}})^2 & \prod_{i=1}^{n} e(d_{i,1}, \prod d_{k,2}^{\gamma_{i,k}}) \cdot e(d_{i,2}, \prod d_{k,1}^{\gamma_{i,k}}) & \prod_{i=1}^{n} e(\mathcal{A}_i, d_{i,1}) e(d_{i,1}, \prod d_{k,3}^{\gamma_{i,k}}) \cdot e(d_{i,3}, \prod d_{k,1}^{\gamma_{i,k}}) \\
\prod_{i=1}^{n} e(d_{i,2}, \prod d_{k,1}^{\gamma_{i,k}}) \cdot e(d_{i,1}, \prod d_{k,2}^{\gamma_{i,k}}) & \prod_{i=1}^{n} e(d_{i,2}, \prod d_{k,2}^{\gamma_{i,k}})^2 & \prod_{i=1}^{n} e(\mathcal{A}_i, d_{i,2}) e(d_{i,2}, \prod d_{k,3}^{\gamma_{i,k}}) \cdot e(d_{i,3}, \prod d_{k,2}^{\gamma_{i,k}}) \\
\prod_{i=1}^{n} e(\mathcal{A}_i, d_{i,1}) \cdot e(d_{i,3}, \prod d_{k,1}^{\gamma_{i,k}}) \cdot e(d_{i,1}, \prod d_{k,3}^{\gamma_{i,k}}) & \prod_{i=1}^{n} e(\mathcal{A}_i, d_{i,2}) \cdot e(d_{i,3}, \prod d_{k,2}^{\gamma_{i,k}}) \cdot e(d_{i,2}, \prod d_{k,3}^{\gamma_{i,k}}) & \prod_{i=1}^{n} e(\mathcal{A}_i, d_{i,3})^2 \cdot e(d_{i,3}, \prod d_{k,3}^{\gamma_{i,k}})^2
\end{pmatrix}
$$

$$\prod_{i=1}^{n} e\Big(d_{i,1},\ \mathcal{A}_i^{r_{1,3}+r_{3,1}} \prod d_{k,1}^{\gamma_{i,k}{}^{2\cdot r_{1,1}}} d_{k,2}^{\gamma_{i,k}{}^{(r_{1,2}+r_{2,1})}} d_{k,3}^{\gamma_{i,k}{}^{(r_{1,3}+r_{3,1})}}\Big) \cdot$$

$$e\Big(d_{i,2},\ \mathcal{A}_i^{r_{2,3}+r_{3,2}} \prod d_{k,1}^{\gamma_{i,k}{}^{(r_{1,2}+r_{2,1})}} d_{k,2}^{\gamma_{i,k}{}^{2\cdot r_{2,2}}} d_{k,3}^{\gamma_{i,k}{}^{(r_{2,3}+r_{3,2})}}\Big) \cdot$$

$$e\Big(d_{i,3},\ \mathcal{A}_i^{2\cdot r_{3,3}} \prod d_{k,1}^{\gamma_{i,k}{}^{(r_{1,3}+r_{3,1})}} d_{k,2}^{\gamma_{i,k}{}^{(r_{2,3}+r_{3,2})}} d_{k,3}^{\gamma_{i,k}{}^{2\cdot r_{3,3}}}\Big)$$

	Naive	Batch
SXDH		
Pairing-product	$5m + 3n + 16$	$m + 2n + 8$
Multi-scalar in $\mathbb{G}_1$	$8m + 2n + 14$	$\min(2n + 9, 2m + n + 7)$
Multi-scalar in $\mathbb{G}_2$	$8n + 2m + 14$	$\min(2m + 9, 2n + m + 7)$
Quadratic	$8m + 8n + 12$	$2\min(m, n) + 8$
DLIN		
Pairing-product	$12n + 27$	$3n + 6$
Multi-scalar	$9n + 12m + 27$	$3n + 3m + 6$
Quadratic	$18n + 24$	$3n + 6$

1. Introduction
2. Groth Sahai Proof System
3. Batching Technique
4. Applications
   - Groth Group Signature
   - BCKL P-Signature

- pk $= (f, h, T) \in \mathbb{G}^2 \times \mathbb{G}_T$ (msk:$z \in \mathbb{G}$ such that $e(f, z) = T$)

- $\mathrm{pk} = (f, h, T) \in \mathbb{G}^2 \times \mathbb{G}_T$ (msk:$z \in \mathbb{G}$ such that $e(f, z) = T$)
- $C_i = (a, b)$ satisfying $e(a, vh)\, e(f, b) = T$, where $\mathrm{pk}_i = v = g^{x_i} \in \mathbb{G}, \mathrm{sk}_i = x_i$

- pk $= (f, h, T) \in \mathbb{G}^2 \times \mathbb{G}_T$ (msk:$z \in \mathbb{G}$ such that $e(f, z) = T$)
- $C_i = (a, b)$ satisfying $e(a, vh)\, e(f, b) = T$, where $\text{pk}_i = v = g^{x_i} \in \mathbb{G}, \text{sk}_i = x_i$
- To sign $m \in \mathbb{Z}_p$, computes $\sigma = g^{1/(x_i+m)}$; and forms GS commitments $\mathbf{d}_v$, $\mathbf{d}_b$ and $\mathbf{d}_\sigma$,

- pk $= (f, h, T) \in \mathbb{G}^2 \times \mathbb{G}_T$ (msk:$z \in \mathbb{G}$ such that $e(f, z) = T$)
- $C_i = (a, b)$ satisfying $e(a, vh)\, e(f, b) = T$, where $\mathrm{pk}_i = v = g^{x_i} \in \mathbb{G}, \mathrm{sk}_i = x_i$
- To sign $m \in \mathbb{Z}_p$, computes $\sigma = g^{1/(x_i+m)}$; and forms GS commitments $\mathbf{d}_v$, $\mathbf{d}_b$ and $\mathbf{d}_\sigma$,
- Make a proof that the associated plaintexts satisfy the following:

$$e(a, vh)\, e(f, b) = T \quad \text{and} \quad e(\sigma, g^m v) = e(g, g)$$

Batched result

	Naive Approach	With Batch
Independant Equation		
$e(a, vh)\, e(f, b) = T$	13	
$e(\sigma, g^m v) = e(g, g)$	20 + 35	
Combined		
Both	68	11
Several	$68n$	$4n + 7$

- $f, g \in \mathbb{G}_1, h \in \mathbb{G}_2$

- $f, g \in \mathbb{G}_1, h \in \mathbb{G}_2$
- $\mathsf{pk}_i = v, w \in \mathbb{G}_2$

- $f, g \in \mathbb{G}_1, h \in \mathbb{G}_2$
- $\mathsf{pk}_i = v, w \in \mathbb{G}_2$
- To sign $m \in \mathbb{Z}_p$, computes $\sigma = (C_1, C_2, C_3) \in \mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}_1$, such that $e(C_1, v h^m C_2) = e(g, h)$ and $e(f, C_2) = e(C_3, w)$

- $f, g \in \mathbb{G}_1, h \in \mathbb{G}_2$
- $\mathsf{pk}_i = v, w \in \mathbb{G}_2$
- To sign $m \in \mathbb{Z}_p$, computes $\sigma = (C_1, C_2, C_3) \in \mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}_1$, such that $e(C_1, vh^m C_2) = e(g, h)$ and $e(f, C_2) = e(C_3, w)$
- With the GS commitments $\mathbf{c_1}$,$\mathbf{c_2}$ and $\mathbf{c_3}$ for $C_1, M_1 = f^m, C_3$ in $\mathbb{G}_1$ and $\mathbf{d_1}, \mathbf{d_2}$ for $M_2 = h^m$ and C_2 in $\mathbb{G}_2$.

- $f, g \in \mathbb{G}_1, h \in \mathbb{G}_2$
- $\mathrm{pk}_i = v, w \in \mathbb{G}_2$
- To sign $m \in \mathbb{Z}_p$, computes $\sigma = (C_1, C_2, C_3) \in \mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}_1$, such that $e(C_1, v h^m C_2) = e(g, h)$ and $e(f, C_2) = e(C_3, w)$
- With the GS commitments $\mathbf{c_1}$,$\mathbf{c_2}$ and $\mathbf{c_3}$ for $C_1, M_1 = f^m, C_3$ in $\mathbb{G}_1$ and $\mathbf{d_1}, \mathbf{d_2}$ for $M_2 = h^m$ and C_2 in $\mathbb{G}_2$.
- Make a proof that they satisfy the following:

$$e(C_1, v M_2 C_2) = e(g, h), \quad e(f, C_2) = e(C_3, w)$$

$$\text{and} \quad e(f, M_2) = e(M_1, h)$$

Batched result

	Naive Approach	With Batch
SXDH		
One signature	68	15
Several	$68n$	$2n + 13$
DLIN		
One Signature	126	12
Several	$126n$	$3n + 9$

Thank you

Any Questions ?