Groth-Sahai proof system

Olivier Blazy

École normale supérieure

Jan. 21st 2011

Contents

Zero-Knowledge Proof Systems

- Introduced in 1985 by Goldwasser, Micali and Rackoff.

  $\rightsquigarrow$ Reveal nothing other than the validity of assertion being proven

- Used in many cryptographic protocols
  - **Anonymous credentials**
  - **Anonymous signatures**
  - **Online voting**
  - ...

Zero-Knowledge Proof Systems

- Introduced in 1985 by Goldwasser, Micali and Rackoff.

  $\rightsquigarrow$ Reveal nothing other than the validity of assertion being proven

- Used in many cryptographic protocols
  - **Anonymous credentials**
  - **Anonymous signatures**
  - **Online voting**
  - ...

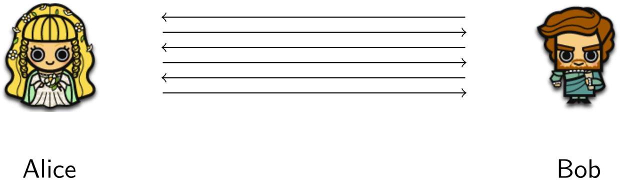
Zero-Knowledge Proof Systems

- Introduced in 1985 by Goldwasser, Micali and Rackoff.

  $\rightsquigarrow$ Reveal nothing other than the validity of assertion being proven

- Used in many cryptographic protocols
  - **Anonymous credentials**
  - **Anonymous signatures**
  - **Online voting**
  - ...

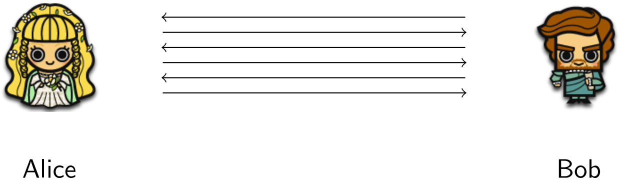
Zero-Knowledge Interactive Proof



- interactive method for one party to prove to another that a statement $\mathcal{S}$ is true, without revealing anything other than the veracity of $\mathcal{S}$.

1. **Completeness:** if $\mathcal{S}$ is true, the honest verifier will be convinced of this fact
2. **Soundness:** if $\mathcal{S}$ is false, no cheating prover can convince the honest verifier that it is true
3. **Zero-knowledge:** if $\mathcal{S}$ is true, no cheating verifier learns anything other than this fact.

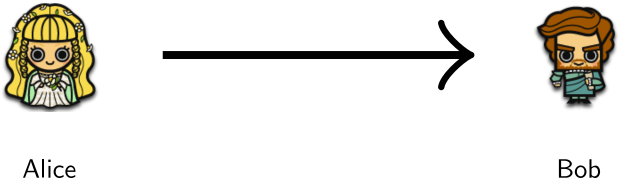
Zero-Knowledge Interactive Proof



- interactive method for one party to prove to another that a statement $\mathcal{S}$ is true, without revealing anything other than the veracity of $\mathcal{S}$.

1. **Completeness:** if $\mathcal{S}$ is true, the honest verifier will be convinced of this fact
2. **Soundness:** if $\mathcal{S}$ is false, no cheating prover can convince the honest verifier that it is true
3. **Zero-knowledge:** if $\mathcal{S}$ is true, no cheating verifier learns anything other than this fact.

Non-Interactive Zero-Knowledge Proof



- non-interactive method for one party to prove to another that a statement $\mathcal{S}$ is true, without revealing anything other than the veracity of $\mathcal{S}$.

1. **Completeness:** $\mathcal{S}$ is true $\rightsquigarrow$ verifier will be convinced of this fact
2. **Soundness:** $\mathcal{S}$ is false $\rightsquigarrow$ no cheating prover can convince the verifier that $\mathcal{S}$ is true
3. **Zero-knowledge:** $\mathcal{S}$ is true $\rightsquigarrow$ no cheating verifier learns anything other than this fact.

Non-Interactive Witness-Indistinguishable Proof

Alice Bob

- non-interactive method for one party to prove to another that a statement $\mathcal{S}$ is true, without revealing which witness was used.

1. **Completeness:** $\mathcal{S}$ is true $\rightsquigarrow$ verifier will be convinced of this fact
2. **Soundness:** $\mathcal{S}$ is false $\rightsquigarrow$ no cheating prover can convince the verifier that $\mathcal{S}$ is true
3. **Witness indistinguishability:** $\mathcal{S}$ is true $\rightsquigarrow$ no cheating verifier can distinguish between two provers that use different witnesses.

History of NIZK Proofs

Inefficient NIZK

- Blum-Feldman-Micali, 1988.
- ...
- De Santis-Di Crescenzo-Persiano, 2002.

Alternative: Fiat-Shamir heuristic, 1986: interactive ZK proof $\rightsquigarrow$ NIZK
But there are examples of insecure Fiat-Shamir transformation

- Groth-Ostrovsky-Sahai, 2006.
- Groth-Sahai, 2008.

History of NIZK Proofs

Inefficient NIZK

- Blum-Feldman-Micali, 1988.
- ...
- De Santis-Di Crescenzo-Persiano, 2002.

Alternative: Fiat-Shamir heuristic, 1986: interactive ZK proof $\rightsquigarrow$ NIZK
But there are examples of insecure Fiat-Shamir transformation

- Groth-Ostrovsky-Sahai, 2006.
- Groth-Sahai, 2008.

History of NIZK Proofs

Inefficient NIZK

- Blum-Feldman-Micali, 1988.
- ...
- De Santis-Di Crescenzo-Persiano, 2002.

Alternative: Fiat-Shamir heuristic, 1986: interactive ZK proof $\rightsquigarrow$ NIZK
But there are examples of insecure Fiat-Shamir transformation

- Groth-Ostrovsky-Sahai, 2006.
- Groth-Sahai, 2008.

History of NIZK Proofs

Inefficient NIZK

- Blum-Feldman-Micali, 1988.
- ...
- De Santis-Di Crescenzo-Persiano, 2002.

Alternative: Fiat-Shamir heuristic, 1986: interactive ZK proof $\rightsquigarrow$ NIZK
But there are examples of insecure Fiat-Shamir transformation

- **Groth-Ostrovsky-Sahai, 2006.**
- Groth-Sahai, 2008.

Applications of NIZK Proofs

- Fancy signature schemes
  - group signatures
  - ring signatures
  - traceable signatures
  - ...
- Efficient non-interactive proof of correctness of shuffle
- Non-interactive anonymous credentials
- CCA-2-secure encryption schemes
- Identification
- E-voting
- E-cash
- ...

Composite order bilinear structure: What ?

$(e, \mathbb{G}, \mathbb{G}_T, g, n)$ bilinear structure:

- $\mathbb{G}$, $\mathbb{G}_T$ multiplicative groups of order $n = pq$
  - $n =$ **RSA integer**
- $\langle g \rangle = \mathbb{G}$
- $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$
  - $\langle e(g, g) \rangle = \mathbb{G}_\mathbb{T}$
  - $e(g^a, g^b) = e(g, g)^{ab}$, $a, b \in \mathbb{Z}$
- deciding group membership, group operations, bilinear map } efficiently computable.

Composite order bilinear structure: Why ?

1. **Deciding Diffie-Hellman tuples:** given $(g, g^a, g^b, g^c) \in \mathbb{G}^4$

$$c = ab \iff e(g^a, g^b) = e(g, g^c)$$

2. **If $\mathbf{h} \in \mathbb{G}_\mathbf{q}$:**

$$\forall v \in \mathbb{G}, e(h, v)^q = 1$$

$$e(g^a h^b, g)^q = e(g, g)^{aq}$$

Applications: "Somewhat homomorphic" encryption, Traitor tracing, Signatures, Attribute-based encryption, Fully secure HIBE, ...

Composite order bilinear structure: Why ?

1. **Deciding Diffie-Hellman tuples:** given $(g, g^a, g^b, g^c) \in \mathbb{G}^4$

$$c = ab \iff e(g^a, g^b) = e(g, g^c)$$

2. **If $\mathbf{h} \in \mathbb{G}_\mathbf{q}$:**

$$\forall v \in \mathbb{G}, e(h, v)^q = 1$$

$$e(g^a h^b, g)^q = e(g, g)^{aq}$$

Applications: "Somewhat homomorphic" encryption, Traitor tracing, Signatures, Attribute-based encryption, Fully secure HIBE, ...

Composite order bilinear structure: Why ?

1. **Deciding Diffie-Hellman tuples:** given $(g, g^a, g^b, g^c) \in \mathbb{G}^4$

$$c = ab \iff e(g^a, g^b) = e(g, g^c)$$

2. **If h** $\in \mathbb{G}_{\mathbf{q}}$**:**

$$\forall v \in \mathbb{G}, e(h, v)^q = 1$$

$$e(g^a h^b, g)^q = e(g, g)^{aq}$$

Applications: "Somewhat homomorphic" encryption, Traitor tracing, Signatures, Attribute-based encryption, Fully secure HIBE, ...

Boneh-Goh-Nissim Encryption Scheme

Public key: $(e, \mathbb{G}, \mathbb{G}_T, n)$ bilinear structure with $n = pq$
$g \in \mathbb{G}, h \in \mathbb{G}_q$.

Secret key: p, q

Encryption: $c = g^m h^r$ $(r \stackrel{\$}{\leftarrow} \mathbb{Z}_n)$

Decryption: $c^q = (g^m h^r)^q = g^{mq} h^{qr} = (g^q)^m$ (+ DL)

IND-CPA-secure under the:

Subgroup Membership Assumption

Hard to distinguish $h \in \mathbb{G}_q$ from random h of order n

Boneh-Goh-Nissim Commitment Scheme

Public key: $(e, \mathbb{G}, \mathbb{G}_T, n = pq)$ bilinear structure
$g \in \mathbb{G}, h \in \mathbb{G}_q$.

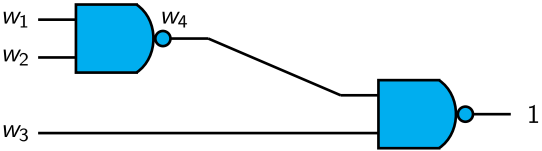
Commitment: $c = g^m h^r \ (r \stackrel{\$}{\leftarrow} \mathbb{Z}_n)$

- **Perfectly binding:** unique m mod p
- **Computationally hiding:** indistinguishable from h of order n
- **Somewhat homomorphic properties:** $(g^a h^r) \cdot (g^b h^s) = g^{a+b} h^{r+s}$

$$\begin{aligned} e(g^a h^r, g^b h^s) &= e(g^a, g^b) e(h^r, g^b) e(g^a, h^s) e(h^r, h^s) \\ &= e(g, g)^{ab} e(h, g^{as+rb} h^{rs}) \end{aligned}$$

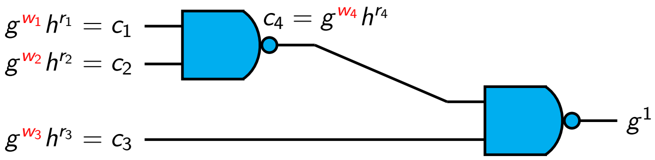
Groth-Ostrovsky-Sahai: NIZK Proof for Circuit SAT

- Groth, Ostrovsky and Sahai (2006)
  - Perfect completeness, perfect soundness, computational zero-knowledge for NP
  - Common reference string: $O(k)$ bits
  - Proof: $O(|C|k)$ bits
- Circuit-SAT is **NP-complete**



- **Idea:**
  - Commit w_i using BGN encryption
  - Prove the validity using homomorphic properties

NIZK Proof for Circuit SAT



- Prove $w_i \in \{0, 1\}$ for $i \in \{1, 2, 3, 4\}$
- Prove $w_4 = \neg(w_1 \wedge w_2)$
- Prove $1 = \neg(w_3 \wedge w_4)$

Proof for c Containing 0 or 1

- $w \bmod p \in \{0,1\} \iff w(w-1) = 0 \bmod p$
- For $c = g^{w} h^{r}$ we have

$$\begin{aligned} e(c, cg^{-1}) &= e(g^{w}h^{r}, g^{w-1}h^{r}) \\ &= e(g^{w}, g^{w-1})e(h^{r}, g^{w-1})e(g^{w}, h^{r})e(h^{r}, h^{r}) \\ &= e(g,g)^{w(w-1)}e(h, (\underbrace{g^{2w-1}h^{r}}_{\pi})^{r}) \end{aligned}$$

- $\pi = g^{2w-1}h^{r}$ = proof that c contains 0 or 1 $\bmod p$.
  (c detemines w uniquely $\bmod p$ since $\mathrm{ord}(h) = q$)
- Randomizable proof !

Proof for c Containing 0 or 1

- $w \bmod p \in \{0,1\} \iff w(w-1) = 0 \bmod p$
- For $c = g^{w}h^{r}$ we have

$$\begin{aligned} e(c, cg^{-1}) &= e(g^{w}h^{r}, g^{w-1}h^{r}) \\ &= e(g^{w}, g^{w-1})e(h^{r}, g^{w-1})e(g^{w}, h^{r})e(h^{r}, h^{r}) \\ &= e(g,g)^{w(w-1)}e(h, (\underbrace{g^{2w-1}h^{r}}_{\pi})^{r}) \end{aligned}$$

- $\pi = g^{2w-1}h^{r}$ = proof that c contains 0 or 1 $\bmod p$.
  (c detemines w uniquely $\bmod p$ since $\mathrm{ord}(h) = q$)
- **Randomizable proof !**

A Simple Observation

b_0	b_1	b_2	$b_0 + b_1 + 2b_2 - 2$
0	0	0	-2
0	0	1	0
0	1	0	-1
0	1	1	1
1	0	0	-1
1	0	0	-1
1	0	1	1
1	1	0	0
1	1	1	2

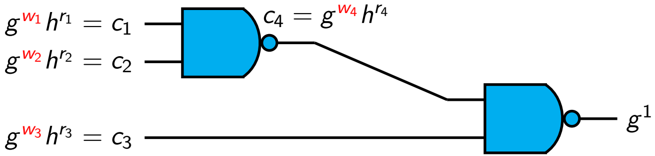
$$b_2 = \neg(b_0 \wedge b_1) \iff b_0 + b_1 + 2b_2 - 2 \in \{0, 1\}$$

A Simple Observation

b_0	b_1	b_2	$b_0 + b_1 + 2b_2 - 2$
0	0	0	-2
0	0	1	0
0	1	0	-1
0	1	1	1
1	0	0	-1
1	0	0	-1
1	0	1	1
1	1	0	0
1	1	1	2

$$b_2 = \neg(b_0 \wedge b_1) \iff b_0 + b_1 + 2b_2 - 2 \in \{0, 1\}$$

Proof for NAND-gate

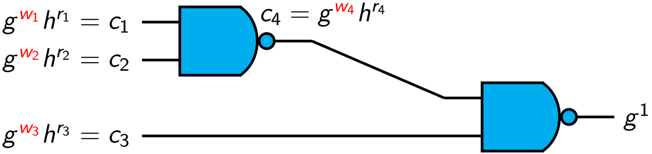


- Given c_1, c_2 and c_4 commitments for bits w_1, w_2, w_4
  $\rightsquigarrow$ Wish to prove $w_4 = \neg(w_1 \wedge w_2)$.
  i.e. $w_1 + w_2 + 2w_4 - 2 \in \{0, 1\}$
- We have

$$\begin{aligned} c_1 c_2 c_4^2 g^{-2} &= (g^{w_0} h^{r_0}) \cdot (g^{w_1} h^{r_1}) \cdot (g^{w_4} h^{r_4})^2 g^{-2} \\ &= g^{w_0 + w_1 + 2w_4 - 2} h^{r_0 + r_1 + 2r_4} \end{aligned}$$

- Prove that $c_1 c_2 c_4^2 g^{-2}$ contains 0 or 1

NIZK Proof for Circuit SAT



- Prove $w_i \in \{0,1\}$ for $i \in \{1,2,3,4\} \rightarrow 2k$ bits
  Prove $w_4 = \neg(w_1 \wedge w_2) \rightarrow k$ bits
  Prove $1 = \neg(w_3 \wedge w_4) \rightarrow k$ bits
- CRS size: $3k$ **bits**
  Proof size: $(2|W| + |C|)k$ **bits**

Groth-Ostrowsky-Sahai is ZK

Subgroup Membership Assumption

Hard to distinguish $h \in \mathbb{G}$ of order q from random h of order n

Simulation

- simulated CRS

h of order n by choosing $g = h^{\tau}$

- the simulation trapdoor is τ
- $\rightsquigarrow$ **perfectly hiding trapdoor commitments**

Groth-Ostrowsky-Sahai is ZK

Subgroup Membership Assumption

Hard to distinguish $h \in \mathbb{G}$ of order q from random h of order n

Simulation

- simulated CRS

h of order n by choosing $g = h^{\tau}$

- the simulation trapdoor is τ
- $\rightsquigarrow$ **perfectly hiding trapdoor commitments**

Groth-Ostrowsky-Sahai is ZK

Subgroup Membership Assumption

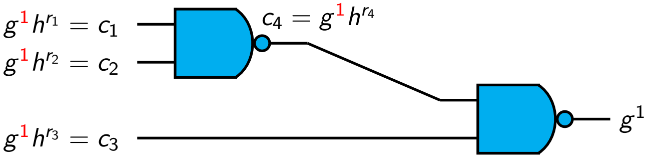
Hard to distinguish $h \in \mathbb{G}$ of order q from random h of order n

Simulation

- simulated CRS

h of order n by choosing $g = h^\tau$

- the simulation trapdoor is τ
- $\rightsquigarrow$ **perfectly hiding trapdoor commitments**



Groth-Ostrowsky-Sahai is ZK

Witness-indistinguishable 0/1-proof

- $c_1 = g^{1} h^{r_1}$
  - $\pi_1 = (g h^{r_1})^{r_1}$ is the proof that c_1 contains 1
- $c_1 = g^{1} h^{r_1} = g^{0} g h^{r_1} = g^{0} h^{\tau + r_1}$
  - $\pi_0 = (g^{-1} h^{\tau + r_1})^{\tau + r_1}$ is the proof that c_1 contains 0

  $\pi_0 = (g^{-1} h^{\tau + r_1})^{\tau + r_1} = (g^{-1} h^{\tau})^{\tau + r_1} (h^{r})^{r + \tau} = (h^{r+\tau})^{r} = (g^{1} h^{r})^{r} = \pi_1$

Witness-indistinguishable NAND-proof

- We have

$$\begin{aligned} c_1 c_2 c_4^2 g^{-2} &= (g^{1} h^{r_1}) \cdot (g^{1} h^{r_2}) \cdot (g^{1} h^{r_4})^2 g^{-2} \\ &= g^{2} h^{r_0 + r_1 + 2r_4} \\ &= g^{1} h^{\tau + r_1 + r_2 + 2r_4} \end{aligned}$$

Computational ZK → Subgroup membership assumption

Groth-Ostrovsky-Sahai: Summary

- Perfect completeness and soundness, computational **zero-knowledge** for **NP**
- **Idea:**
  - Commit **bits** using BGN encryption
  - Prove the validity using homomorphic properties

Plug the commitments $\vec{c}$ in the equations and provide additionnal group element $\vec{\pi}$ to check the validity

$$e(g^w, g^w g^{-1}) = 1 \rightsquigarrow e(c, cg^{-1}) = e(h, \pi)$$

- Common reference string: $O(k)$ bits
- Proof: $\mathbf{O}(|\mathbf{C}|\mathbf{k})$ bits

Groth-~~Ostrovsky~~-Sahai: Summary

- Perfect completeness and soundness, computational **zero-knowledge** for **NP**

- **Idea:**
  - Commit **bits** using BGN encryption
  - Prove the validity using homomorphic properties

> *Plug the commitments $\vec{c}$ in the equations and provide additionnal group element $\vec{\pi}$ to check the validity*

$$e(g^w, g^w g^{-1}) = 1 \rightsquigarrow e(c, cg^{-1}) = e(h, \pi)$$

- Common reference string: $O(k)$ bits
- Proof: $\mathbf{O}(|\mathbf{C}|\mathbf{k})$ bits

Groth-~~Ostrovsky~~-Sahai: Summary

witness-indistinguishability

- Perfect completeness and soundness, ~~computational **zero-knowledge**~~ for **NP**

- **Idea:**
  - Commit **bits** using BGN encryption
  - Prove the validity using homomorphic properties

Plug the commitments $\vec{c}$ in the equations and provide additionnal group element $\vec{\pi}$ to check the validity

$$e(g^w, g^w g^{-1}) = 1 \rightsquigarrow e(c, cg^{-1}) = e(h, \pi)$$

- Common reference string: $O(k)$ bits
- Proof: $\mathbf{O}(|\mathbf{C}|\mathbf{k})$ bits

Groth-~~Ostrovsky~~-Sahai: Summary

- Perfect completeness and soundness, ~~computational **zero-knowledge**~~ witness-indistinguishability for ~~**NP**~~ algebraic languages
- **Idea:**
  - Commit **bits** using BGN encryption
  - Prove the validity using homomorphic properties

Plug the commitments $\vec{c}$ in the equations and provide additionnal group element $\vec{\pi}$ to check the validity

$$e(g^w, g^w g^{-1}) = 1 \rightsquigarrow e(c, cg^{-1}) = e(h, \pi)$$

- Common reference string: $O(k)$ bits
- Proof: $\mathbf{O}(|\mathbf{C}|\mathbf{k})$ bits

Groth-~~Ostrovsky~~-Sahai: Summary

witness-indistinguishability

- Perfect completeness and soundness, ~~computational **zero-knowledge**~~ for ~~**NP**~~ algebraic languages
- **Idea:** group elements
  - Commit ~~**bits**~~ using BGN encryption
  - Prove the validity using homomorphic properties

Plug the commitments $\vec{c}$ in the equations and provide additionnal group element $\vec{\pi}$ to check the validity

$$e(g^w, g^w g^{-1}) = 1 \rightsquigarrow e(c, cg^{-1}) = e(h, \pi)$$

- Common reference string: $O(k)$ bits
- Proof: $\mathbf{O}(|\mathbf{C}|\mathbf{k})$ bits

Groth-~~Ostrovsky~~-Sahai: Summary

- Perfect completeness and soundness, ~~computational~~ ~~**zero-knowledge**~~ witness-indistinguishability for ~~**NP**~~ algebraic languages

- **Idea:**
  - Commit ~~**bits**~~ group elements using ~~BGN~~ encryption
  - Prove the validity using homomorphic properties

> *Plug the commitments $\vec{c}$ in the equations and provide additionnal group element $\vec{\pi}$ to check the validity*

$$e(g^w, g^w g^{-1}) = 1 \rightsquigarrow e(c, cg^{-1}) = e(h, \pi)$$

- Common reference string: $O(k)$ bits
- Proof: $\mathbf{O}(|\mathbf{C}|\mathbf{k})$ bits

Groth-~~Ostrovsky~~-Sahai: Summary

- Perfect completeness and soundness, ~~computational **zero-knowledge**~~ witness-indistinguishability for ~~**NP**~~ algebraic languages
- **Idea:**
  - Commit ~~**bits**~~ group elements using ~~BGN~~ encryption
  - Prove the validity using homomorphic properties

> *Plug the commitments $\vec{c}$ in the equations and provide additionnal group element $\vec{\pi}$ to check the validity*

$$e(g^w, g^w g^{-1}) = 1 \rightsquigarrow e(c, cg^{-1}) = e(h, \pi)$$

- Common reference string: $O(k)$ bits
- Proof: ~~$\mathbf{O(|C|k)}$~~ $O(|E|k)$ bits

Symmetric bilinear structure

$(e, \mathbb{G}, \mathbb{G}_T, g, p)$ bilinear structure:

- $\mathbb{G}$, $\mathbb{G}_T$ multiplicative groups of order p
  - $p =$ **prime integer**
- $\langle g \rangle = \mathbb{G}$
- $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
  - $\langle e(g, g) \rangle = \mathbb{G}_T$
  - $e(g^a, g^b) = e(g, g)^{ab}$, $a, b \in \mathbb{Z}$
- deciding group membership, group operations, bilinear map } efficiently computable.

Boneh-Boyen-Shacham Encryption Scheme

Public key: $(e, \mathbb{G}, \mathbb{G}_T, p)$
$g, u = g^x, v = g^y \in \mathbb{G}$

Secret key: x, y

Encryption: $(c_1, c_2, c_3) = (u^\alpha, v^\beta, mg^{\alpha+\beta})$ $(\alpha, \beta \stackrel{\$}{\leftarrow} \mathbb{Z}_p)$

Decryption: $c_3/(c_1^{1/x} c_2^{1/y}) = m$

IND-CPA-secure under the:

Decision Linear Assumption

given $(u, v, g, u^\alpha, v^\beta)$, Hard to distinguish $g^{\alpha+\beta}$ from random

Boneh-Boyen-Shacham Commitment Scheme

Public key: $(e, \mathbb{G}, \mathbb{G}_T, p)$
$g, u, v \in \mathbb{G}$

Commitment: $(c_1, c_2, c_3) = (u^\alpha, v^\beta, mg^{\alpha+\beta})$ $(\alpha, \beta \stackrel{\$}{\leftarrow} \mathbb{Z}_p)$

- **Perfectly binding:** unique $m \in \mathbb{G}$
- **Computationally hiding:** indistinguishable from random g
- **Addition:** $(c_1, c_2, c_3) \cdot (c'_1, c'_2, c'_3) = (u^{\alpha+\alpha'}, v^{\beta+\beta'}, mg^{\alpha+\alpha'+\beta+\beta'})$

Asymmetric bilinear structure

$(e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, p)$ bilinear structure:

- $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ multiplicative groups of order p
  - $p =$ **prime integer**
- $\langle g_i \rangle = \mathbb{G}_i$
- $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$
  - $\langle e(g_1, g_2) \rangle = \mathbb{G}_T$
  - $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$, $a, b \in \mathbb{Z}$
- deciding group membership, group operations, bilinear map } efficiently computable.

ElGamal Encryption Scheme

Public key: $(e, \mathbb{G}_1, \mathbb{G}_T, p)$
$g_1, h_1 = g_1^y \in \mathbb{G}_1$

Secret key: y

Encryption: $(c_1, c_2) = (g_1^\alpha, m h_1^\alpha)$ $(\alpha \xleftarrow{\$} \mathbb{Z}_p)$

Decryption: $c_2 / c_1^y = m$

IND-CPA-secure under the:

Decisional Diffie Hellman

given $(g_1, g_1^\alpha, g_1^\beta)$, Hard to distinguish $g_1^{\alpha\beta}$ from random

ElGamal Commitment Scheme

Public key: $(e, \mathbb{G}_1, \mathbb{G}_T, p)$
$g_1, h_1 \in \mathbb{G}_1$

Commitment: $(c_1, c_2) = (g_1^{\alpha}, m h_1^{\alpha})$ $(\alpha \stackrel{\$}{\leftarrow} \mathbb{Z}_p)$

- **Perfectly binding:** unique $m \in \mathbb{G}_1$
- **Computationally hiding:** indistinguishable from random g_1
- **Addition:** $(c_1, c_2) \cdot (c_1', c_2') = (g_1^{\alpha+\alpha'}, m h_1^{\alpha+\alpha'})$

Groth-Sahai Proof System

- **Pairing product equation (PPE):** for variables $\mathcal{X}_1, \ldots, \mathcal{X}_n \in \mathbb{G}$

$$(E) : \prod_{i=1}^{n} e(A_i, \mathcal{X}_i) \prod_{i=1}^{n} \prod_{j=1}^{n} e(\mathcal{X}_i, \mathcal{X}_j)^{\gamma_{i,j}} = t_T$$

determined by $A_i \in \mathbb{G}$, $\gamma_{i,j} \in \mathbb{Z}_p$ and $t_T \in \mathbb{G}_T$.

- Groth-Sahai $\rightsquigarrow$ WI proofs that elements in $\mathbb{G}$ that were committed to satisfy PPE

Assumption	DLIN	SXDH	SD
Variables	3	2	1
PPE	9	(2,2)	1
(Linear)	3	2	1
Verification	$12n + 27$	$5m + 3n + 16$	$n + 1$

O. B., G. Fuchsbauer, M. Izabachène, A. Jambert, H. Sibert, D. Vergnaud
Batch Groth-Sahai.
ACNS 2010

Groth-Sahai Proof System

- **Pairing product equation (PPE):** for variables $\mathcal{X}_1, \ldots, \mathcal{X}_n \in \mathbb{G}$

$$(E): \prod_{i=1}^{n} e(A_i, \mathcal{X}_i) \prod_{i=1}^{n} \prod_{j=1}^{n} e(\mathcal{X}_i, \mathcal{X}_j)^{\gamma_{i,j}} = t_T$$

determined by $A_i \in \mathbb{G}$, $\gamma_{i,j} \in \mathbb{Z}_p$ and $t_T \in \mathbb{G}_T$.

- Groth-Sahai $\rightsquigarrow$ WI proofs that elements in $\mathbb{G}$ that were committed to satisfy PPE

Assumption	DLIN	SXDH	SD
Variables	3	2	1
PPE	9	(2,2)	1
(Linear)	3	2	1
Verification	$12n + 27$	$5m + 3n + 16$	$n + 1$

O. B., G. Fuchsbauer, M. Izabachène, A. Jambert, H. Sibert, D. Vergnaud
Batch Groth-Sahai.
ACNS 2010

Groth-Sahai Proof System

Groth-Sahai Proof System

- **Pairing product equation (PPE):** for variables $\mathcal{X}_1, \ldots, \mathcal{X}_n \in \mathbb{G}$

$$(E) : \prod_{i=1}^{n} e(A_i, \mathcal{X}_i) \prod_{i=1}^{n} \prod_{j=1}^{n} e(\mathcal{X}_i, \mathcal{X}_j)^{\gamma_{i,j}} = t_T$$

determined by $A_i \in \mathbb{G}$, $\gamma_{i,j} \in \mathbb{Z}_p$ and $t_T \in \mathbb{G}_T$.

- Groth-Sahai $\rightsquigarrow$ WI proofs that elements in $\mathbb{G}$ that were committed to satisfy PPE

Assumption	DLIN	SXDH	SD
Variables	3	2	1
PPE	9	(2,2)	1
(Linear)	3	2	1
Verification	$3n + 6$	$m + 2n + 8$	$n + 1$

O. B., G. Fuchsbauer, M. Izabachène, A. Jambert, H. Sibert, D. Vergnaud
Batch Groth-Sahai.
ACNS 2010

Groth-Sahai Proof System: NIWI

$$(E) : \prod_{i=1}^{n} e(A_i, \mathcal{X}_i) \prod_{i=1}^{n} \prod_{j=1}^{n} e(\mathcal{X}_i, \mathcal{X}_j)^{\gamma_{i,j}} = t_T$$

Setup on input the bilinear group $\rightsquigarrow$ output a commitment key **ck**

Com on input **ck**, $X \in \mathbb{G}$, randomness $\rho \rightsquigarrow$ output commitment $\vec{c_X}$ to X

Prove on input **ck**, $(X_i, \rho_i)_{i=1,\dots,n}$ and $(E) \rightsquigarrow$ output a proof ϕ

Verify on input **ck**, $\vec{c_{X_i}}$, (E) and $\phi \rightsquigarrow$ output 0 or 1

Properties:

- correctness honestly generated proofs are accepted by **Verify**
- soundness **ExtSetup** outputs $(\mathbf{ck}, \mathbf{ek})$ s.t. given $\vec{c_{X_i}}$ and ϕ s.t. $\mathbf{Verify}(\mathbf{ck}, \vec{c_{X_i}}, E, \pi) = 1$ then $\mathbf{Extract}(\mathbf{ek}, \vec{c_{X_i}})$ returns $\vec{X_i'}$ that satisfies (E)
- witness-indistinguishability **WISetup** outputs $\mathbf{ck}^*$ indist. from **ck** s.t.
  - **Com** produces statistically hiding commitments
  - Given (X_i, ρ_i), (X_i', ρ_i') s.t. $\mathbf{Com}(\mathbf{ck}^*, \vec{X_i}, \rho_i) = \mathbf{Com}(\mathbf{ck}^*, \vec{X_i}, \rho_i)$ and $\vec{X_i}$ and $\vec{X_i}$ satisfy E then $\mathbf{Prove}(\mathbf{ck}^*, \vec{X_i}, \rho_i) \equiv \mathbf{Prove}(\mathbf{ck}^*, \vec{X_i}, \rho_i)$

Groth-Sahai Proof System: NIWI

$$(E) : \prod_{i=1}^{n} e(A_i, \mathcal{X}_i) \prod_{i=1}^{n} \prod_{j=1}^{n} e(\mathcal{X}_i, \mathcal{X}_j)^{\gamma_{i,j}} = t_T$$

Setup on input the bilinear group $\rightsquigarrow$ output a commitment key **ck**

Com on input **ck**, $X \in \mathbb{G}$, randomness $\rho \rightsquigarrow$ output commitment $\vec{c_X}$ to X

Prove on input **ck**, $(X_i, \rho_i)_{i=1,\ldots,n}$ and $(E) \rightsquigarrow$ output a proof ϕ

Verify on input **ck**, $\vec{c_{X_i}}$, (E) and $\phi \rightsquigarrow$ output 0 or 1

Properties:

- correctness honestly generated proofs are accepted by **Verify**
- soundness **ExtSetup** outputs $(\mathbf{ck}, \mathbf{ek})$ s.t. given $\vec{c_{X_i}}$ and ϕ s.t. $\mathbf{Verify}(\mathbf{ck}, \vec{c_{X_i}}, E, \pi) = 1$ then $\mathbf{Extract}(\mathbf{ek}, \vec{c_{X_i}})$ returns $\vec{X_i'}$ that satisfies (E)
- witness-indistinguishability **WISetup** outputs $\mathbf{ck}^*$ indist. from **ck** s.t.
  - **Com** produces statistically hiding commitments
  - Given (X_i, ρ_i), (X_i', ρ_i') s.t. $\mathbf{Com}(\mathbf{ck}^*, \vec{X_i}, \rho_i) = \mathbf{Com}(\mathbf{ck}^*, \vec{X_i}, \rho_i)$ and $\vec{X_i}$ and $\vec{X_i}$ satisfy E then $\mathbf{Prove}(\mathbf{ck}^*, \vec{X_i}, \rho_i) \equiv \mathbf{Prove}(\mathbf{ck}^*, \vec{X_i}, \rho_i)$

Groth-Sahai Proof System: NIWI

$$(E) : \prod_{i=1}^{n} e(A_i, \mathcal{X}_i) \prod_{i=1}^{n} \prod_{j=1}^{n} e(\mathcal{X}_i, \mathcal{X}_j)^{\gamma_{i,j}} = t_T$$

Setup on input the bilinear group $\rightsquigarrow$ output a commitment key **ck**

Com on input **ck**, $X \in \mathbb{G}$, randomness $\rho \rightsquigarrow$ output commitment $\vec{c_X}$ to X

Prove on input **ck**, $(X_i, \rho_i)_{i=1,\ldots,n}$ and $(E) \rightsquigarrow$ output a proof ϕ

Verify on input **ck**, $\vec{c_{X_i}}$, (E) and $\phi \rightsquigarrow$ output 0 or 1

Properties:

- correctness honestly generated proofs are accepted by **Verify**
- soundness **ExtSetup** outputs $(\mathbf{ck}, \mathbf{ek})$ s.t. given $\vec{c_{X_i}}$ and ϕ s.t. $\mathbf{Verify}(\mathbf{ck}, \vec{c_{X_i}}, E, \pi) = 1$ then $\mathbf{Extract}(\mathbf{ek}, \vec{c_{X_i}})$ returns $\vec{X_i'}$ that satisfies (E)
- witness-indistinguishability **WISetup** outputs $\mathbf{ck}^*$ indist. from **ck** s.t.
  - **Com** produces statistically hiding commitments
  - Given (X_i, ρ_i), (X_i', ρ_i') s.t. $\mathbf{Com}(\mathbf{ck}^*, \vec{X_i}, \rho_i) = \mathbf{Com}(\mathbf{ck}^*, \vec{X_i}, \rho_i)$ and $\vec{X_i}$ and $\vec{X_i}$ satisfy E then $\mathbf{Prove}(\mathbf{ck}^*, \vec{X_i}, \rho_i) \equiv \mathbf{Prove}(\mathbf{ck}^*, \vec{X_i}, \rho_i)$

Several subcases

$$(E) : \vec{A} \bullet \vec{\mathcal{X}} + \vec{\mathcal{X}} \bullet \Gamma \vec{\mathcal{X}} = t_T$$

- Pairing product equation $\rightsquigarrow \theta$: 9 elements
- $\Gamma = 0$, linear $\rightsquigarrow \theta$: 3 elements

Proof : $\vec{\phi} = S^\top i(\vec{A}) + S^\top(\Gamma + \Gamma^\top) i(\vec{\mathcal{X}}) + S^\top \Gamma S \vec{u} + \mathrm{rand}\ \vec{u}$.

Several subcases

$$(E) : \vec{A} \bullet \vec{\mathcal{X}} = t_T$$

- Pairing product equation $\rightsquigarrow \theta$: 9 elements
- $\Gamma = 0$, linear $\rightsquigarrow \theta$: 3 elements

Proof : $\vec{\phi} = S^\top i(\vec{A})$.

$$\pi = R^\top \vec{A}$$

Several subcases

$$(E) : \vec{a} \bullet \vec{Y} + \vec{x} \bullet \vec{B} + \vec{x} \bullet \Gamma \vec{Y} = \mathcal{T}$$

- Multi-scalar equation $\rightsquigarrow \theta$: 9 elements
- $x = 0$, linear $\rightsquigarrow \theta$: 3 elements in $\mathbb{Z}_p$
- $Y = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}$

Proof : $\vec{\phi} = R^\top i(\vec{B}) + R^\top \Gamma i(\vec{Y}) + S^\top i'(\vec{a}) + S^\top \Gamma^\top i(\vec{x}) + R^\top \Gamma S \vec{u} + \mathrm{rand}\ \vec{u}.$

Several subcases

$$(E) : \vec{a} \bullet \vec{Y} = \mathcal{T}$$

- Multi-scalar equation $\rightsquigarrow \theta$: 9 elements
- $x = 0$, linear $\rightsquigarrow \theta$: 3 elements in $\mathbb{Z}_p$
- $Y = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}$

Proof : $\vec{\phi} = S^\top i'(\vec{a})$.

Several subcases

$$(E) : \vec{x} \bullet \vec{B} = \mathcal{T}$$

- Multi-scalar equation $\rightsquigarrow \theta$: 9 elements
- $x = 0$, linear $\rightsquigarrow \theta$: 3 elements in $\mathbb{Z}_p$
- $Y = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}$

Proof : $\vec{\phi} = R^\top i(\vec{B})$.

$$\pi = R^\top \vec{B}$$

Several subcases

$$(E) : \vec{a} \bullet \vec{x} + \vec{x} \bullet \Gamma \vec{x} = t$$

- Quadratic equation $\rightsquigarrow \theta$: 6 elements
- $\Gamma = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{Z}_p$

Proof : $\vec{\phi} = R^\top i'(\vec{b}) + R^\top(\Gamma + \Gamma^\top) i'(\vec{x}) + R^\top \Gamma R \vec{u} + \mathrm{rand}\ \vec{u}$.

Several subcases

$$(E) : \vec{a} \bullet \vec{x} = t$$

- Quadratic equation $\leadsto \theta$: 6 elements
- $\Gamma = 0$, linear $\leadsto \theta$: 2 elements in $\mathbb{Z}_p$

Proof : $\vec{\phi} = R^\top i'(\vec{b})$.

$$\pi = R^\top \vec{b}$$

Groth-Sahai Proof System: DLin

$$(E) : e(\mathcal{X}, g^x) = 1_T$$

Setup $\mathbf{ck} = ((u_{1,1}, 1, g), (1, u_{2,2}, g), (u_{3,1}, u_{3,2}, u_{3,3})) \in (\mathbb{G}^3)^3$
$u_{1,1}, u_{2,2} \stackrel{\$}{\leftarrow} \mathbb{G}$ and $\lambda, \mu \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$
$\mathbf{u}_3 = \mathbf{u}_1^\lambda \odot \mathbf{u}_2^\mu = (u_{3,1} = u_{1,1}^\lambda, u_{3,2} = u_{2,2}^\mu, u_{3,3} = g^{\lambda+\mu})$

Com $\vec{c_Y} = (u_{1,1}^{s_1} \cdot u_{3,1}^{s_3}, u_{2,2}^{s_2} \cdot u_{3,2}^{s_3}, Y \cdot g^{s_1+s_2} \cdot u_{3,3}^{s_3})$.

Prove $\phi = (g^{s_1 x}, g^{s_2 x}, g^{s_3 x})^\top$

Verify $i(\vec{A}) \bullet \vec{c_Y} \stackrel{?}{=} \vec{u} \bullet \phi$

Groth-Sahai Proof System: DLin

$$(E) : e(\mathcal{X}, g^x) = 1_T$$

Setup $\mathbf{ck} = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$.

Com $\vec{c_Y} = (1, 1, Y) \odot \mathbf{u}_1^{s_1} \odot \mathbf{u}_2^{s_2} \odot \mathbf{u}_3^{s_3} = (u_{1,1}^{s_1} \cdot u_{3,1}^{s_3}, u_{2,2}^{s_2} \cdot u_{3,2}^{s_3}, Y \cdot g^{s_1+s_2} \cdot u_{3,3}^{s_3})$.

Prove $\phi = (g^{s_1 x}, g^{s_2 x}, g^{s_3 x})^\top$

Verify $i(\vec{A}) \bullet \vec{c_Y} \stackrel{?}{=} \vec{u} \bullet \phi$

Groth-Sahai Proof System: DLin

$$(E) : e(\mathcal{X}, g^x) = 1_T$$

Setup $\mathbf{ck} = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$.

Com $\vec{c_Y} = (u_{1,1}^{s_1} \cdot u_{3,1}^{s_3}, u_{2,2}^{s_2} \cdot u_{3,2}^{s_3}, Y \cdot g^{s_1+s_2} \cdot u_{3,3}^{s_3})$.

Prove $\phi = S^\top \vec{A} = (g^{s_1 x}, g^{s_2 x}, g^{s_3 x})^\top$

Verify $i(\vec{A}) \bullet \vec{c_Y} \stackrel{?}{=} \vec{u} \bullet \phi$

Groth-Sahai Proof System: DLin

$$(E) : e(\mathcal{X}, g^x) = 1_T$$

Setup $\mathbf{ck} = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$.

Com $\vec{c_Y} = (u_{1,1}^{s_1} \cdot u_{3,1}^{s_3}, u_{2,2}^{s_2} \cdot u_{3,2}^{s_3}, Y \cdot g^{s_1+s_2} \cdot u_{3,3}^{s_3})$.

Prove $\phi = (g^{s_1 x}, g^{s_2 x}, g^{s_3 x})^\top$

Verify $i(\vec{A}) \bullet \vec{c_Y} \stackrel{?}{=} \vec{u} \bullet \phi$

Groth-Sahai Proof System: DLin

$$(E) : e(\mathcal{X}, g^x) = 1_T$$

Setup $\mathbf{ck} = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$.

Com $\vec{c_Y} = (u_{1,1}^{s_1} \cdot u_{3,1}^{s_3}, u_{2,2}^{s_2} \cdot u_{3,2}^{s_3}, Y \cdot g^{s_1+s_2} \cdot u_{3,3}^{s_3})$.

Prove $\phi = (g^{s_1 x}, g^{s_2 x}, g^{s_3 x})^\top$

Verify $i(\vec{A}) \bullet \vec{c_Y} \stackrel{?}{=} \vec{u} \bullet \phi$

Properties:

- Pairing Product Equation
- Linear.

New Subcases with SXDH

$$(E) : \vec{A} \bullet \vec{Y} + \vec{\mathcal{X}} \bullet \vec{B} + \vec{\mathcal{X}} \bullet \Gamma \vec{Y} = t_T$$

- Pairing product equation $\rightsquigarrow \theta$: 2* 4 elements
- $\vec{\mathcal{X}} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}_1$
- $\vec{\mathcal{Y}} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}_2$

New Subcases with SXDH

$$(E) : \vec{A} \bullet \vec{Y} = t_T$$

- Pairing product equation $\rightsquigarrow \theta$: 2* 4 elements
- $\vec{\mathcal{X}} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}_1$
- $\vec{\mathcal{Y}} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}_2$

New Subcases with SXDH

$$(E) : \vec{\mathcal{X}} \bullet \vec{B} = t_T$$

- Pairing product equation $\rightsquigarrow \theta$: 2* 4 elements
- $\vec{\mathcal{X}} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}_1$
- $\vec{\mathcal{Y}} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}_2$

New Subcases with SXDH

$$(E) : \vec{A} \bullet \vec{y} + \vec{\mathcal{X}} \bullet \vec{b} + \vec{\mathcal{X}} \bullet \Gamma \vec{y} = \mathcal{T}_1$$

- Multi-scalar equation in $\mathbb{G}_1$ $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}_1$, 4 in $\mathbb{G}_2$
- $\vec{\mathcal{X}} = 0$, linear $\rightsquigarrow \theta$: 1 element in $\mathbb{G}_1$
- $\vec{y} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{Z}_p$

New Subcases with SXDH

$$(E) : \vec{A} \bullet \vec{y} = \mathcal{T}_1$$

- Multi-scalar equation in $\mathbb{G}_1$ $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}_1$, 4 in $\mathbb{G}_2$
- $\vec{\mathcal{X}} = 0$, linear $\rightsquigarrow \theta$: 1 element in $\mathbb{G}_1$
- $\vec{y} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{Z}_p$

New Subcases with SXDH

$$(E) : \vec{\mathcal{X}} \bullet \vec{b} = \mathcal{T}_1$$

- Multi-scalar equation in $\mathbb{G}_1$ $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}_1$, 4 in $\mathbb{G}_2$
- $\vec{\mathcal{X}} = 0$, linear $\rightsquigarrow \theta$: 1 element in $\mathbb{G}_1$
- $\vec{y} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{Z}_p$

New Subcases with SXDH

$$(E) : \vec{a} \bullet \vec{y} + \vec{x} \bullet \vec{b} + \vec{x} \bullet \Gamma \vec{y} = t$$

- Quadratic equation $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}_1$, 2 in $\mathbb{G}_2$
- $\vec{x} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{Z}_p$
- $\vec{y} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{Z}_p$

New Subcases with SXDH

$$(E) : \vec{a} \bullet \vec{y} = t$$

- Quadratic equation $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}_1$, 2 in $\mathbb{G}_2$
- $\vec{x} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{Z}_p$
- $\vec{y} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{Z}_p$

New Subcases with SXDH

$$(E) : \vec{x} \bullet \vec{b} = t$$

- Quadratic equation $\rightsquigarrow \theta$: 2 elements in $\mathbb{G}_1$, 2 in $\mathbb{G}_2$
- $\vec{x} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{Z}_p$
- $\vec{y} = 0$, linear $\rightsquigarrow \theta$: 2 elements in $\mathbb{Z}_p$

Groth-Sahai Proof System: NIZK

- such equations are not known to always have NIZK proofs
- auxiliary variables and equations have to be introduced.
- If $t_T = \prod_{j=1}^{n'} e(g_j, h_j)$ for known $g_1, \ldots, g_{n'}, h_1, \ldots, h_{n'} \in \mathbb{G}$, the simulator can prove that

$$\prod_{i=1}^{n} e(\mathcal{A}_i, \mathcal{X}_i) \cdot \prod_{i=1}^{n} \cdot \prod_{j=1}^{n} e(\mathcal{X}_i, \mathcal{X}_j)^{a_{ij}} = \prod_{j=1}^{n'} e(g_j, \mathcal{Y}_j)$$

  and that introduced variables $\mathcal{Y}_1, \ldots, \mathcal{Y}_{n'}$ satisfy the linear equations $\mathcal{Y}_j = h_j$.
- $\rightsquigarrow$ size of NIZK proofs not constant.

Conclusion

- Groth-Sahai framework for NIWI/NIZK proofs
- **Applications**
  - Non-frameable group signatures
  - Efficient (offline) e-cash system
  - Group signatures with VLR
  - Fair blind signatures
- **Ongoing work**
  - (Non-interactive) Receipt-Free E-voting
  - (Round-optimal) Blind Signatures (under classical assumption)