Non-Interactive Zero-Knowledge Proofs: Shuffles

Alonso González Ulloa

Departamento de Cs. de la Computación
Universidad de Chile

April, 2015

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE CHILE

Joint work with Carla Ràfols and Alejandro Hevia

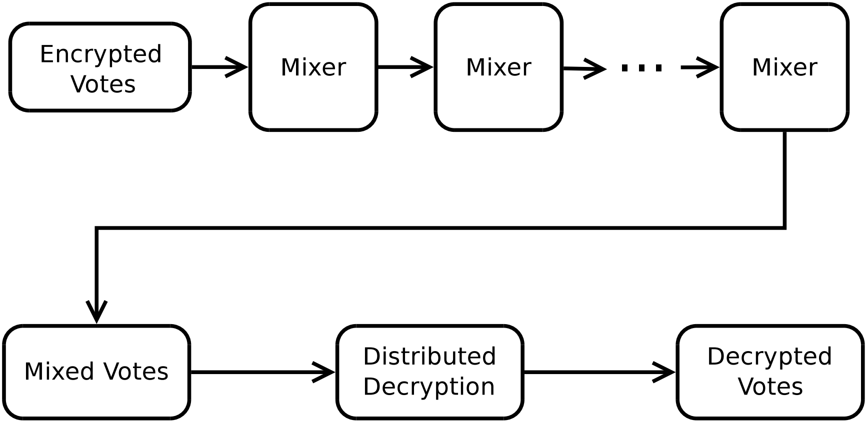
1 Introduction
- Mix-nets and Shuffles
- Non-Interactive Zero-Knowledge
- Bilinear Groups and Tools

2 State of the art
- Groth-Sahai Proofs
- NIZK for membership in Linear Subspaces of $\hat{\mathbb{G}}^n$

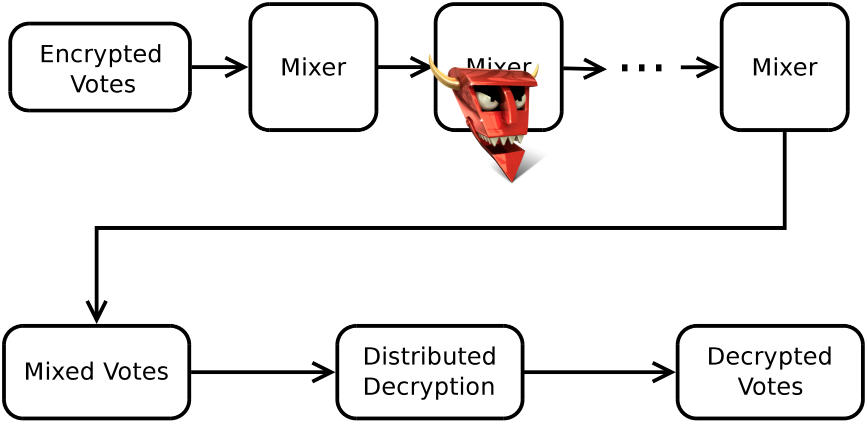
3 Prior Work
- NIZK for membership in Linear Subspaces of $\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n$
- Aggregation of quadratic equations

4 Efficient NIZK Shuffle Arguments

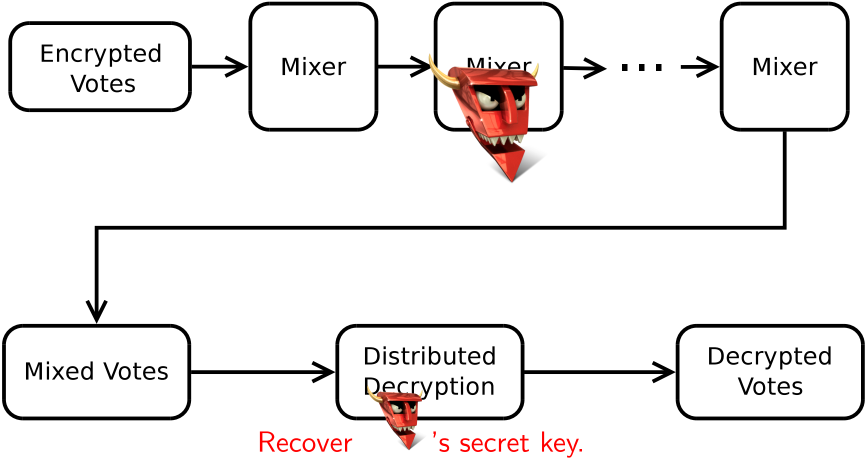
Mix-net based voting scheme



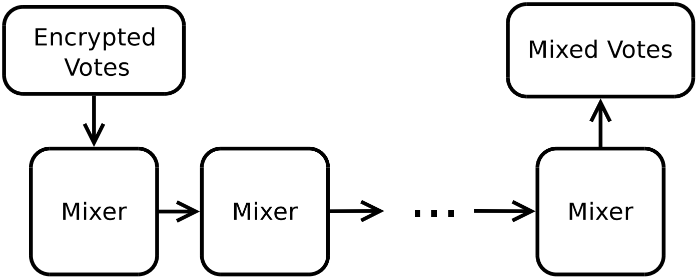
Mix-net based voting scheme



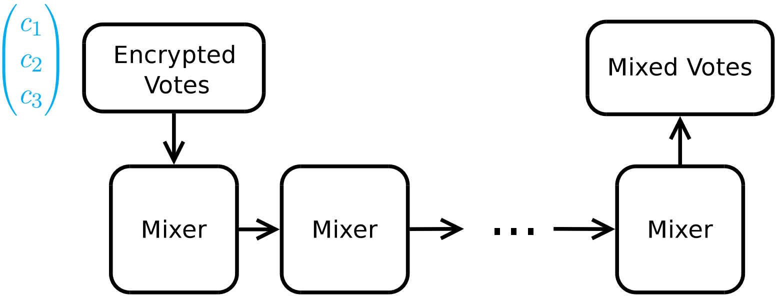
Mix-net based voting scheme



Mix-nets

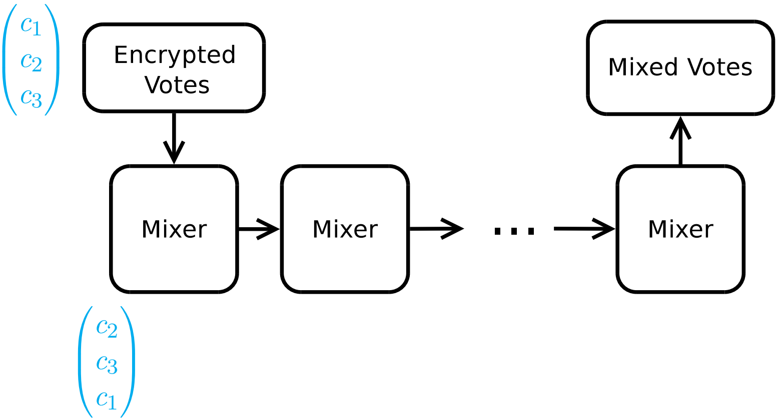


Mix-nets

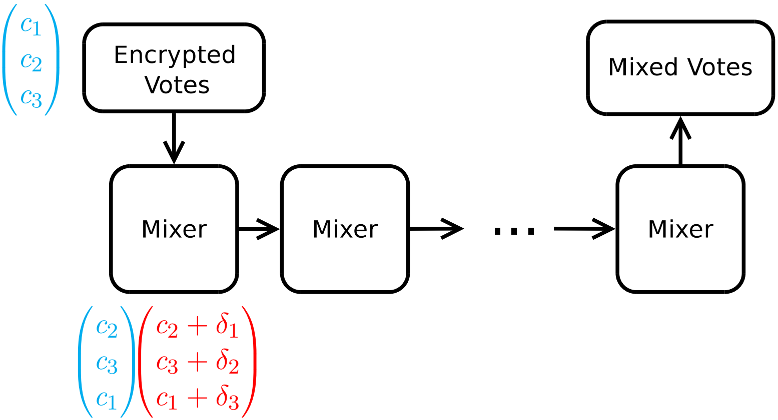


$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$
Encrypted Votes
Mixer
Mixer
...
Mixer
Mixed Votes

Mix-nets

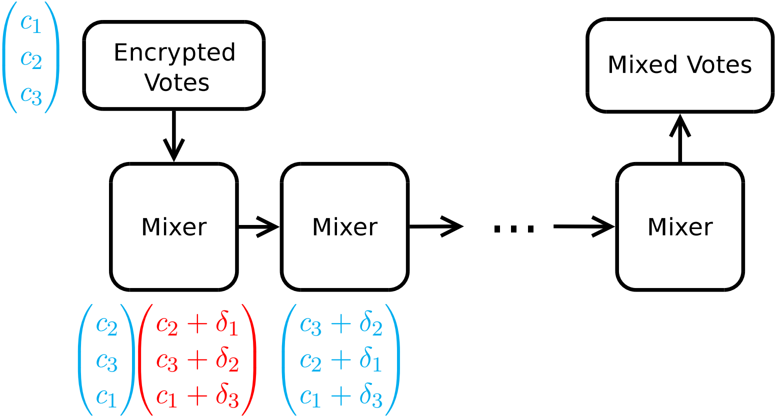

$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$
Encrypted Votes
Mixed Votes
Mixer
Mixer
...
Mixer
$\begin{pmatrix} c_2 \\ c_3 \\ c_1 \end{pmatrix}$

Mix-nets

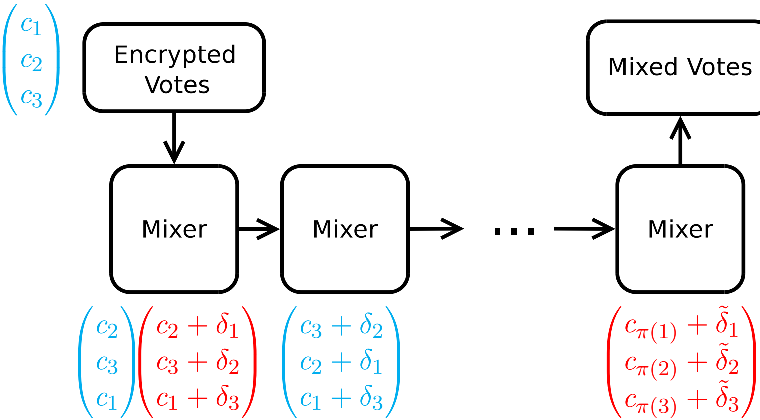


$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$
Encrypted Votes
Mixer
Mixer
...
Mixer
Mixed Votes
$\begin{pmatrix} c_2 \\ c_3 \\ c_1 \end{pmatrix}\begin{pmatrix} c_2 + \delta_1 \\ c_3 + \delta_2 \\ c_1 + \delta_3 \end{pmatrix}$

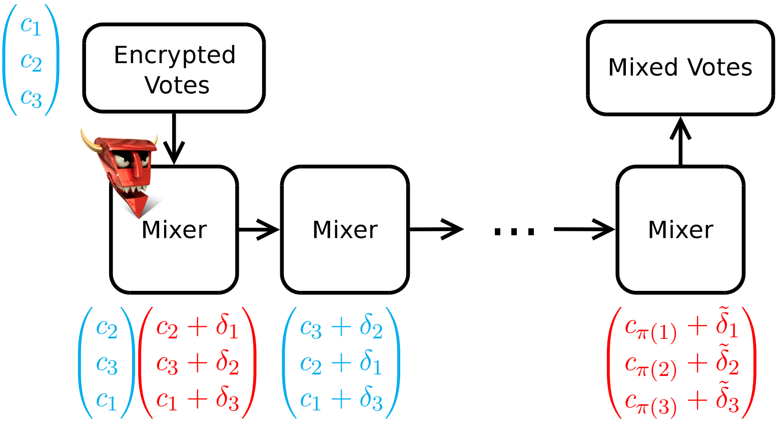
Mix-nets


c_1 c_2 c_3
Encrypted Votes
Mixer
Mixer
...
Mixer
Mixed Votes
c_2 c_3 c_1
$c_2 + \delta_1$ $c_3 + \delta_2$ $c_1 + \delta_3$
$c_3 + \delta_2$ $c_2 + \delta_1$ $c_1 + \delta_3$

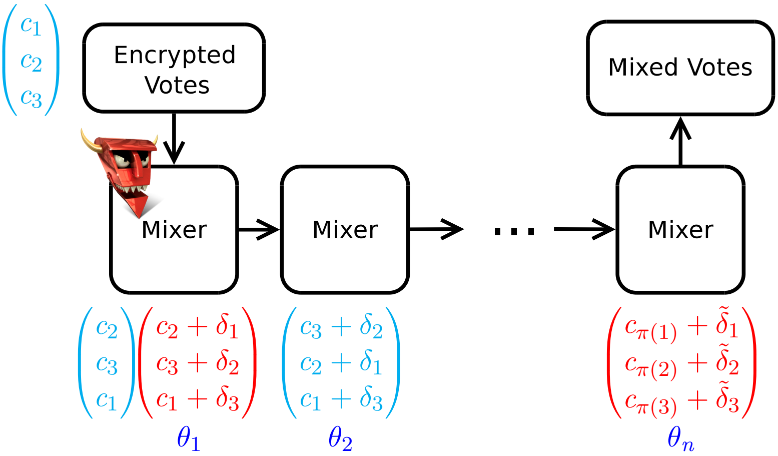
Mix-nets


Encrypted Votes
Mixer
Mixer
Mixer
Mixed Votes
(c_1, c_2, c_3)
(c_2, c_3, c_1)
$(c_2+\delta_1, c_3+\delta_2, c_1+\delta_3)$
$(c_3+\delta_2, c_2+\delta_1, c_1+\delta_3)$
$(c_{\pi(1)}+\tilde{\delta}_1, c_{\pi(2)}+\tilde{\delta}_2, c_{\pi(3)}+\tilde{\delta}_3)$

Mix-nets


$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$
Encrypted Votes
Mixed Votes
Mixer
Mixer
...
Mixer
$\begin{pmatrix} c_2 \\ c_3 \\ c_1 \end{pmatrix}$ $\begin{pmatrix} c_2 + \delta_1 \\ c_3 + \delta_2 \\ c_1 + \delta_3 \end{pmatrix}$
$\begin{pmatrix} c_3 + \delta_2 \\ c_2 + \delta_1 \\ c_1 + \delta_3 \end{pmatrix}$
$\begin{pmatrix} c_{\pi(1)} + \tilde{\delta}_1 \\ c_{\pi(2)} + \tilde{\delta}_2 \\ c_{\pi(3)} + \tilde{\delta}_3 \end{pmatrix}$

Mix-nets


$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$
Encrypted Votes
Mixed Votes
Mixer
Mixer
...
Mixer
$\begin{pmatrix} c_2 \\ c_3 \\ c_1 \end{pmatrix} \begin{pmatrix} c_2 + \delta_1 \\ c_3 + \delta_2 \\ c_1 + \delta_3 \end{pmatrix}$
θ_1
$\begin{pmatrix} c_3 + \delta_2 \\ c_2 + \delta_1 \\ c_1 + \delta_3 \end{pmatrix}$
θ_2
$\begin{pmatrix} c_{\pi(1)} + \tilde{\delta}_1 \\ c_{\pi(2)} + \tilde{\delta}_2 \\ c_{\pi(3)} + \tilde{\delta}_3 \end{pmatrix}$
θ_n

Zero-Knowledge Shuffle Argument

We want to prove that each $\mathbf{c}, \mathbf{d}$ belongs to

$$L_{\textsf{shuffle}} := \{(\mathbf{c}, \mathbf{d}) : \exists \pi \in S_n \text{ s.t. } \forall i \in [n]\ c_i - d_{\pi(i)} \text{ is an encryption of } 0\}.$$

Zero-Knowledge Shuffle Argument

We want to prove that each $\mathbf{c}, \mathbf{d}$ belongs to

$$L_{\text{shuffle}} := \{(\mathbf{c}, \mathbf{d}) : \exists \pi \in S_n \text{ s.t. } \forall i \in [n] \ c_i - d_{\pi(i)} \text{ is an encryption of } 0\}.$$

We are interested in a Non-Interactive Zero Knowledge Shuffle Argument:

Zero-Knowledge Shuffle Argument

We want to prove that each $\mathbf{c}, \mathbf{d}$ belongs to

$$L_{\text{shuffle}} := \{(\mathbf{c}, \mathbf{d}) : \exists \pi \in S_n \text{ s.t. } \forall i \in [n]\ c_i - d_{\pi(i)} \text{ is an encryption of } 0\}.$$

We are interested in a Non-Interactive Zero Knowledge Shuffle Argument:

- Efficiency.

Zero-Knowledge Shuffle Argument

We want to prove that each $\mathbf{c}, \mathbf{d}$ belongs to

$$L_{\mathsf{shuffle}} := \{(\mathbf{c}, \mathbf{d}) : \exists \pi \in S_n \text{ s.t. } \forall i \in [n]\ c_i - d_{\pi(i)} \text{ is an encryption of } 0\}.$$

We are interested in a Non-Interactive Zero Knowledge Shuffle Argument:

- Efficiency.
- Public verifiable.

Non-Interactive Zero-Knowledge Proofs for $L \in \text{NP}$

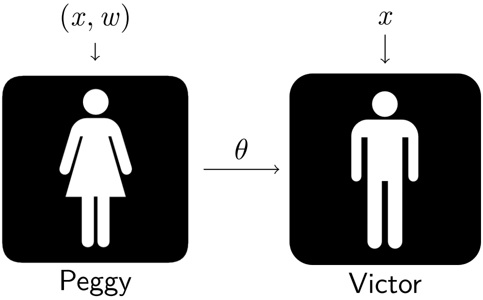
(x, w)
$\downarrow$

Peggy

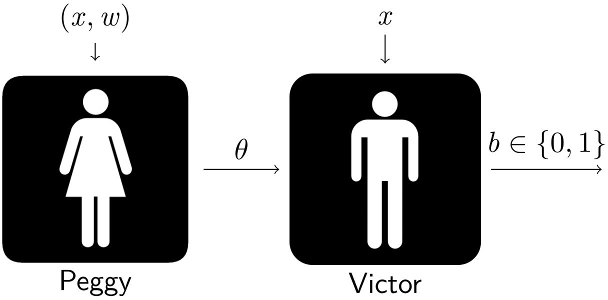
x
$\downarrow$

Victor

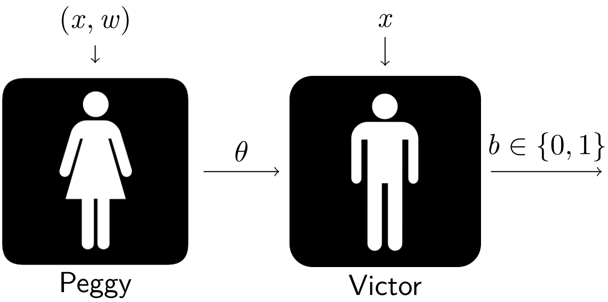
Non-Interactive Zero-Knowledge Proofs for $L \in \mathrm{NP}$



Non-Interactive Zero-Knowledge Proofs for $L \in \text{NP}$

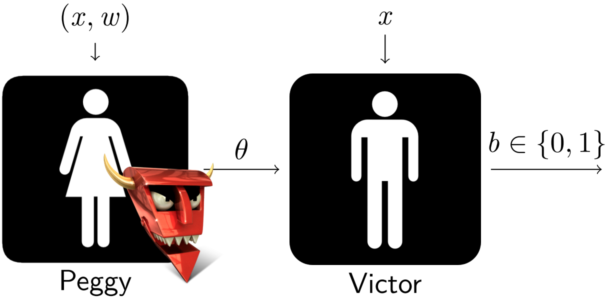


Non-Interactive Zero-Knowledge Proofs for $L \in \mathrm{NP}$



Completeness: If $x \in L$ Peggy convinces Victor.

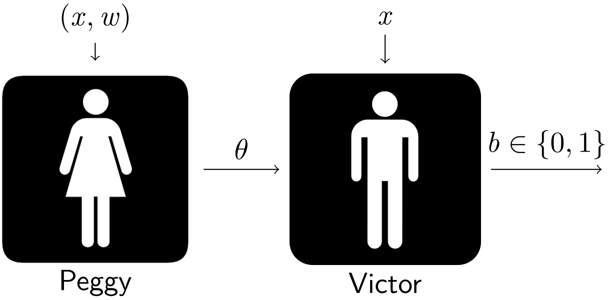
Non-Interactive Zero-Knowledge Proofs for $L \in \mathrm{NP}$



Completeness: If $x \in L$ Peggy convinces Victor.

Soundness: If $x \notin L$ no one can make Victor output 1 with non-negligible probability.

Non-Interactive Zero-Knowledge Proofs for $L \in \mathrm{NP}$

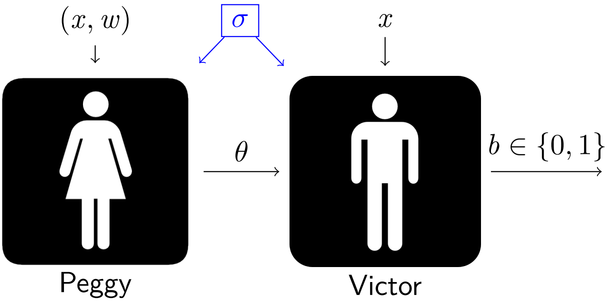


Completeness: If $x \in L$ Peggy convinces Victor.

Soundness: If $x \notin L$ no one can make Victor output 1 with non-negligible probability.

Zero-Knowledge: If $x \in L$, θ can be simulated without knowledge of w.

Non-Interactive Zero-Knowledge Proofs for $L \in \mathrm{NP}$



Completeness: If $x \in L$ Peggy convinces Victor.

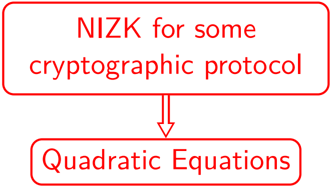
Soundness: If $x \notin L$ no one can make Victor output 1 with non-negligible probability.

Zero-Knowledge: If $x \in L$, θ can be simulated without knowledge of w.

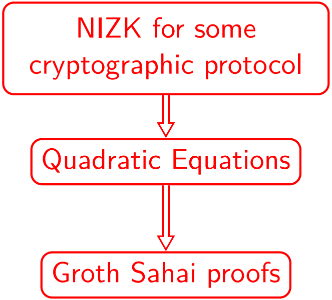
Our approach

NIZK for some
cryptographic protocol

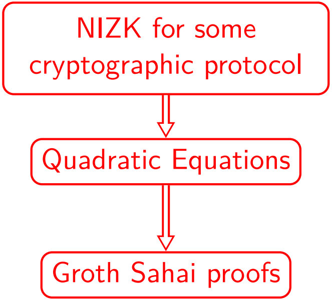
Our approach



Our approach

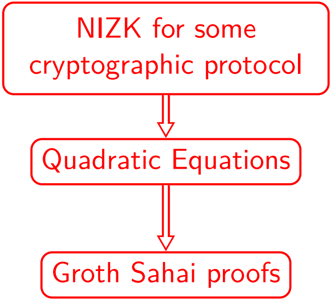


Our approach



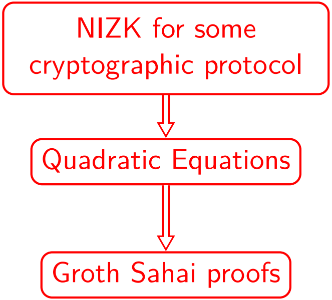
- GS proofs for n equations on m variables cost $O(n+m)$.

Our approach



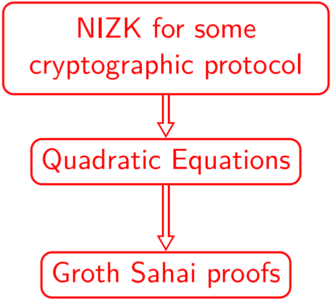
- GS proofs for n equations on m variables cost $O(n+m)$.
- NIZK for NP with $O(1)$ proof size.

Our approach



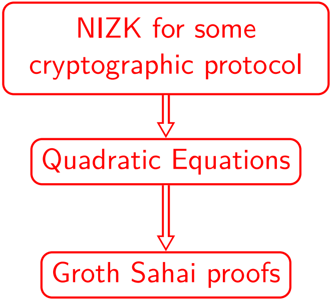
- GS proofs for n equations on m variables cost $O(n+m)$.
- NIZK for NP with $O(1)$ proof size.
- Unlike NIZK for NP, is based of mild assumptions (falsifiable assumptions).

Our approach



- GS proofs for n equations on m variables cost $O(n+m)$.
- NIZK for NP with $O(1)$ proof size.
- Unlike NIZK for NP, is based of mild assumptions (falsifiable assumptions).
- Recent results have further optimized proofs to $O(m)$ for some linear equations.

Our approach



- GS proofs for n equations on m variables cost $O(n + m)$.
- NIZK for NP with $O(1)$ proof size.
- Unlike NIZK for NP, is based of mild assumptions (falsifiable assumptions).
- Recent results have further optimized proofs to $O(m)$ for some linear equations.
- Previous work: Optimize GS proofs to $O(m)$ for other linear equations and quadratic equations.

Bilinear Groups

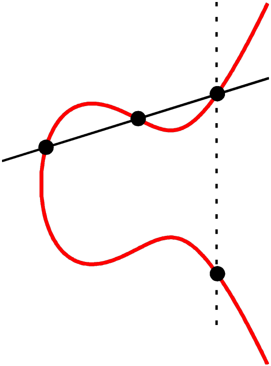
3 additive cyclic groups $\hat{\mathbb{G}}, \check{\mathbb{H}}$ and $\mathbb{T}$ with a bilinear map or pairing

$$e : \hat{\mathbb{G}} \times \check{\mathbb{H}} \to \mathbb{T}$$

Bilinear Groups

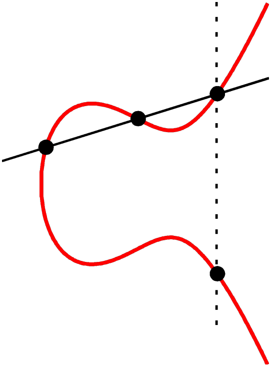
3 additive cyclic groups $\hat{\mathbb{G}}, \check{\mathbb{H}}$ and $\mathbb{T}$ with a bilinear map or pairing

$$e : \hat{\mathbb{G}} \times \check{\mathbb{H}} \to \mathbb{T}$$



3 additive cyclic groups $\hat{\mathbb{G}}, \check{\mathbb{H}}$ and $\mathbb{T}$ with a bilinear map or pairing

$$e : \hat{\mathbb{G}} \times \check{\mathbb{H}} \to \mathbb{T}$$



Type I: $\hat{\mathbb{G}} = \check{\mathbb{H}}$ a.k.a Symmetric.

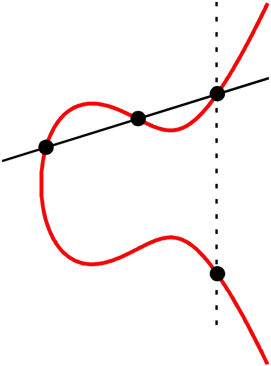
Type II: $\hat{\mathbb{G}} \neq \check{\mathbb{H}}$ with an efficiently computable homomorphism $\psi : \check{\mathbb{H}} \to \hat{\mathbb{G}}$ is known.

Type III: $\hat{\mathbb{G}} \neq \check{\mathbb{H}}$ but no efficiently computable homomorphism. Most desirable [Jou13, CM11, GPS06]

Bilinear Groups

3 additive cyclic groups $\hat{\mathbb{G}}, \check{\mathbb{H}}$ and $\mathbb{T}$ with a bilinear map or pairing

$$e : \hat{\mathbb{G}} \times \check{\mathbb{H}} \rightarrow \mathbb{T}$$



Type I: $\hat{\mathbb{G}} = \check{\mathbb{H}}$ a.k.a Symmetric.

Type II: $\hat{\mathbb{G}} \neq \check{\mathbb{H}}$ with an efficiently computable homomorphism $\psi : \check{\mathbb{H}} \rightarrow \hat{\mathbb{G}}$ is known.

Type III: $\hat{\mathbb{G}} \neq \check{\mathbb{H}}$ but no efficiently computable homomorphism. Most desirable [Jou13, CM11, GPS06]

Decisional Diffie-Hellman Assumption

Notation:

- $\langle g \rangle = \hat{\mathbb{G}}$, $\langle h \rangle = \check{\mathbb{H}}$ and $q = |\hat{\mathbb{G}}| = |\check{\mathbb{H}}|$.

Decisional Diffie-Hellman Assumption

Notation:

- $\langle g \rangle = \hat{\mathbb{G}}$, $\langle h \rangle = \check{\mathbb{H}}$ and $q = |\hat{\mathbb{G}}| = |\check{\mathbb{H}}|$.
- Given $a \in \mathbb{Z}_q$, $\hat{a}_g := ag$ and $\check{a}_h := ah$

Decisional Diffie-Hellman Assumption

Notation:

- $\langle g \rangle = \hat{\mathbb{G}}$, $\langle h \rangle = \check{\mathbb{H}}$ and $q = |\hat{\mathbb{G}}| = |\check{\mathbb{H}}|$.
- Given $a \in \mathbb{Z}_q$, $\hat{a}_g := ag$ and $\check{a}_h := ah$
- We omit sub-index so $\hat{1} = g$ and $\check{1} = h$.

Decisional Diffie-Hellman Assumption

Notation:

- $\langle g \rangle = \hat{\mathbb{G}}$, $\langle h \rangle = \check{\mathbb{H}}$ and $q = |\hat{\mathbb{G}}| = |\check{\mathbb{H}}|$.
- Given $a \in \mathbb{Z}_q$, $\hat{a}_g := ag$ and $\check{a}_h := ah$
- We omit sub-index so $\hat{1} = g$ and $\check{1} = h$.

Definition (DDH Assumption as Subset Membership Problem)

Every adversary $\mathcal{A}$ has at most negligible probability of wining in the next experiment:

Decisional Diffie-Hellman Assumption

Notation:

- $\langle g\rangle = \hat{\mathbb{G}}$, $\langle h\rangle = \check{\mathbb{H}}$ and $q = |\hat{\mathbb{G}}| = |\check{\mathbb{H}}|$.
- Given $a \in \mathbb{Z}_q$, $\hat{a}_g := ag$ and $\check{a}_h := ah$
- We omit sub-index so $\hat{1} = g$ and $\check{1} = h$.

Definition (DDH Assumption as Subset Membership Problem)

Every adversary $\mathcal{A}$ has at most negligible probability of wining in the next experiment:

- Pick $\hat{\mathbf{a}} \leftarrow \begin{pmatrix}\hat{\mathbb{G}}\\ \hat{1}\end{pmatrix}$ and $b \leftarrow \{0,1\}$.

Decisional Diffie-Hellman Assumption

Notation:

- $\langle g \rangle = \hat{\mathbb{G}}$, $\langle h \rangle = \check{\mathbb{H}}$ and $q = |\hat{\mathbb{G}}| = |\check{\mathbb{H}}|$.
- Given $a \in \mathbb{Z}_q$, $\hat{a}_g := ag$ and $\check{a}_h := ah$
- We omit sub-index so $\hat{1} = g$ and $\check{1} = h$.

Definition (DDH Assumption as Subset Membership Problem)

Every adversary $\mathcal{A}$ has at most negligible probability of wining in the next experiment:

- Pick $\hat{\mathbf{a}} \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $b \leftarrow \{0, 1\}$.
- If $b = 1$, pick $\hat{\mathbf{u}} \leftarrow \mathbf{Span}(\hat{\mathbf{a}})$ and compute $b' \leftarrow \mathcal{A}(\hat{\mathbf{a}}, \hat{\mathbf{u}})$.

Decisional Diffie-Hellman Assumption

Notation:

- $\langle g \rangle = \hat{\mathbb{G}}$, $\langle h \rangle = \check{\mathbb{H}}$ and $q = |\hat{\mathbb{G}}| = |\check{\mathbb{H}}|$.
- Given $a \in \mathbb{Z}_q$, $\hat{a}_g := ag$ and $\check{a}_h := ah$
- We omit sub-index so $\hat{1} = g$ and $\check{1} = h$.

Definition (DDH Assumption as Subset Membership Problem)

Every adversary $\mathcal{A}$ has at most negligible probability of wining in the next experiment:

- Pick $\hat{\mathbf{a}} \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $b \leftarrow \{0,1\}$.
- If $b = 1$, pick $\hat{\mathbf{u}} \leftarrow \mathbf{Span}(\hat{\mathbf{a}})$ and compute $b' \leftarrow \mathcal{A}(\hat{\mathbf{a}}, \hat{\mathbf{u}})$.
- If $b = 0$, pick $\hat{\mathbf{u}} \leftarrow \hat{\mathbb{G}}^2$ and compute $b' \leftarrow \mathcal{A}(\hat{\mathbf{a}}, \hat{\mathbf{u}})$.

Decisional Diffie-Hellman Assumption

Notation:

- $\langle g \rangle = \hat{\mathbb{G}}$, $\langle h \rangle = \check{\mathbb{H}}$ and $q = |\hat{\mathbb{G}}| = |\check{\mathbb{H}}|$.
- Given $a \in \mathbb{Z}_q$, $\hat{a}_g := ag$ and $\check{a}_h := ah$
- We omit sub-index so $\hat{1} = g$ and $\check{1} = h$.

Definition (DDH Assumption as Subset Membership Problem)

Every adversary $\mathcal{A}$ has at most negligible probability of wining in the next experiment:

- Pick $\hat{\mathbf{a}} \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $b \leftarrow \{0, 1\}$.
- If $b = 1$, pick $\hat{\mathbf{u}} \leftarrow \mathbf{Span}(\hat{\mathbf{a}})$ and compute $b' \leftarrow \mathcal{A}(\hat{\mathbf{a}}, \hat{\mathbf{u}})$.
- If $b = 0$, pick $\hat{\mathbf{u}} \leftarrow \hat{\mathbb{G}}^2$ and compute $b' \leftarrow \mathcal{A}(\hat{\mathbf{a}}, \hat{\mathbf{u}})$.
- $\mathcal{A}$ wins iff $b' = b$.

ElGamal in $\hat{\mathbb{G}}$

Let $\hat{\mathbf{u}} \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $r \leftarrow \mathbb{Z}_q$.

ElGamal in $\hat{\mathbb{G}}$

Let $\hat{\mathbf{u}} \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $r \leftarrow \mathbb{Z}_q$.

$$\hat{\mathbf{c}} := \begin{pmatrix} \hat{m} \\ \hat{0} \end{pmatrix} + r\hat{\mathbf{u}}$$ is an encryption of $\hat{m} \in \mathbb{Z}_q$

ElGamal in $\hat{\mathbb{G}}$

Let $\hat{\mathbf{u}} \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $r \leftarrow \mathbb{Z}_q$.

$$\hat{\mathbf{c}} := \begin{pmatrix} \hat{m} \\ \hat{0} \end{pmatrix} + r\hat{\mathbf{u}} \text{ is an encryption of } \hat{m} \in \mathbb{Z}_q$$

Security:

ElGamal in $\hat{\mathbb{G}}$

Let $\hat{\mathbf{u}} \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $r \leftarrow \mathbb{Z}_q$.

$$\hat{\mathbf{c}} := \begin{pmatrix} \hat{m} \\ \hat{0} \end{pmatrix} + \boxed{r\hat{\mathbf{u}}}$$ is an encryption of $\hat{m} \in \mathbb{Z}_q$

Security: $\approx$ random vector in $\hat{\mathbb{G}}^2$.

ElGamal in $\hat{\mathbb{G}}$

Let $\hat{\mathbf{u}} \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $r \leftarrow \mathbb{Z}_q$.

$$\hat{\mathbf{c}} := \boxed{\begin{pmatrix} \hat{m} \\ \hat{0} \end{pmatrix} + \boxed{r\hat{\mathbf{u}}}}$$ is an encryption of $\hat{m} \in \mathbb{Z}_q$

Security: $\approx$ random vector in $\hat{\mathbb{G}}^2$. $\approx$ random vector in $\hat{\mathbb{G}}^2$.

ElGamal in $\hat{\mathbb{G}}$

Let $\hat{\mathbf{u}} \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $r \leftarrow \mathbb{Z}_q$.

$$\hat{\mathbf{c}} := \begin{pmatrix} \hat{m} \\ \hat{0} \end{pmatrix} + r\hat{\mathbf{u}} \text{ is an encryption of } \hat{m} \in \mathbb{Z}_q$$

Security:

Decryption: The row vector $(1, -u_{2,1}) \in \mathbb{Z}_q^{1\times 2}$ allows to recover $\hat{m}$.

Commitment Schemes

A commitment to a value w is a safe-box for w.

Commitment Schemes

A commitment to a value w is a safe-box for w.

Hiding : The safe box "hides" w.

Commitment Schemes

A commitment to a value w is a safe-box for w.

Hiding : The safe box “hides” w.

Binding : The value inside the box can not be changed.

Commitments in $\mathbb{Z}_q$

Let $\hat{\mathbf{u}}_2 \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $\hat{\mathbf{u}}_1 \leftarrow \mathbf{Span}(\hat{\mathbf{u}}_2)$, and $r, s \leftarrow \mathbb{Z}_q$.

Commitments in $\mathbb{Z}_q$

Let $\hat{\mathbf{u}}_2 \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $\hat{\mathbf{u}}_1 \leftarrow \mathbf{Span}(\hat{\mathbf{u}}_2)$, and $r, s \leftarrow \mathbb{Z}_q$.

$$\hat{\mathbf{c}} := \quad w \begin{pmatrix} \hat{1} \\ \hat{0} \end{pmatrix} + \quad s\hat{\mathbf{u}}_1 + r\hat{\mathbf{u}}_2 \text{ is a commitment to } w \in \mathbb{Z}_q$$

Commitments in $\mathbb{Z}_q$

Let $\hat{\mathbf{u}}_2 \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $\hat{\mathbf{u}}_1 \leftarrow \mathbf{Span}(\hat{\mathbf{u}}_2)$, and $r, s \leftarrow \mathbb{Z}_q$.

$$\hat{\mathbf{c}} := \quad w \begin{pmatrix} \hat{1} \\ \hat{0} \end{pmatrix} + \quad s\hat{\mathbf{u}}_1 + r\hat{\mathbf{u}}_2 \text{ is a commitment to } w \in \mathbb{Z}_q$$

Hiding:

Commitments in $\mathbb{Z}_q$

Let $\hat{\mathbf{u}}_2 \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $\hat{\mathbf{u}}_1 \leftarrow \mathbf{Span}(\hat{\mathbf{u}}_2)$, and $r, s \leftarrow \mathbb{Z}_q$.

$\hat{\mathbf{c}} := \quad w \begin{pmatrix} \hat{1} \\ \hat{0} \end{pmatrix} + \boxed{s\hat{\mathbf{u}}_1 + r\hat{\mathbf{u}}_2}$ is a commitment to $w \in \mathbb{Z}_q$

Hiding: $\approx$ random vector in $\hat{\mathbb{G}}^2$.

Commitments in $\mathbb{Z}_q$

Let $\hat{\mathbf{u}}_2 \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $\hat{\mathbf{u}}_1 \leftarrow \mathbf{Span}(\hat{\mathbf{u}}_2)$, and $r, s \leftarrow \mathbb{Z}_q$.

$$\hat{\mathbf{c}} := \boxed{w \begin{pmatrix} \hat{1} \\ \hat{0} \end{pmatrix} + \boxed{s\hat{\mathbf{u}}_1 + r\hat{\mathbf{u}}_2}}$$ is a commitment to $w \in \mathbb{Z}_q$

Hiding: $\approx$ random vector in $\hat{\mathbb{G}}^2$. $\approx$ random vector in $\hat{\mathbb{G}}^2$.

Commitments in $\mathbb{Z}_q$

Let $\hat{\mathbf{u}}_2 \leftarrow \begin{pmatrix} \hat{\mathbb{G}} \\ \hat{1} \end{pmatrix}$ and $\hat{\mathbf{u}}_1 \leftarrow \mathbf{Span}(\hat{\mathbf{u}}_2)$, and $r, s \leftarrow \mathbb{Z}_q$.

$$\hat{\mathbf{c}} := \quad w \begin{pmatrix} \hat{1} \\ \hat{0} \end{pmatrix} + \quad s\hat{\mathbf{u}}_1 + r\hat{\mathbf{u}}_2 \text{ is a commitment to } w \in \mathbb{Z}_q$$

Hiding:

Binding: The row vector $(1, -u_{2,1}) \in \mathbb{Z}_q^{1\times 2}$ allows to recover $\hat{w}$.

1 Introduction
- Mix-nets and Shuffles
- Non-Interactive Zero-Knowledge
- Bilinear Groups and Tools

2 State of the art
- Groth-Sahai Proofs
- NIZK for membership in Linear Subspaces of $\hat{\mathbb{G}}^n$

3 Prior Work
- NIZK for membership in Linear Subspaces of $\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n$
- Aggregation of quadratic equations

4 Efficient NIZK Shuffle Arguments

Groth-Sahai Proofs [GS08]

Groth-Sahai (GS) Proofs are NIZK proofs for the satisfiability of equations of the form

$$\sum_{j\in[m_y]} \hat{\alpha}_j \check{y}_j + \sum_{i\in[m_x]} \hat{x}_i, \check{\beta}_i + \sum_{i\in[m_x]} \sum_{j\in[m_y]} \gamma_{i,j} \hat{x}_i \check{y}_j = t, \tag{PPE}$$

(MME)

(QE)

Groth-Sahai Proofs [GS08]

Groth-Sahai (GS) Proofs are NIZK proofs for the satisfiability of equations of the form

$$\sum_{j\in[m_y]} \hat{\alpha}_j \check{y}_j + \sum_{i\in[m_x]} \hat{x}_i, \check{\beta}_i + \sum_{i\in[m_x]} \sum_{j\in[m_y]} \gamma_{i,j} \hat{x}_i \check{y}_j = t, \qquad \text{(PPE)}$$

$$\sum_{j\in[m_y]} \hat{\alpha}_j y_j + \sum_{i\in[m_x]} \hat{x}_i, \beta_i + \sum_{i\in[m_x]} \sum_{j\in[m_y]} \gamma_{i,j} \hat{x}_i y_j = t, \qquad \text{(MME)}$$

(QE)

Groth-Sahai Proofs [GS08]

Groth-Sahai (GS) Proofs are NIZK proofs for the satisfiability of equations of the form

$$\sum_{j\in[m_y]} \hat{\alpha}_j \check{y}_j + \sum_{i\in[m_x]} \hat{x}_i, \check{\beta}_i + \sum_{i\in[m_x]} \sum_{j\in[m_y]} \gamma_{i,j} \hat{x}_i \check{y}_j = t, \qquad \text{(PPE)}$$

$$\sum_{j\in[m_y]} \hat{\alpha}_j y_j + \sum_{i\in[m_x]} \hat{x}_i, \beta_i + \sum_{i\in[m_x]} \sum_{j\in[m_y]} \gamma_{i,j} \hat{x}_i y_j = t, \qquad \text{(MME)}$$

$$\sum_{j\in[m_y]} \alpha_j y_j + \sum_{i\in[m_x]} x_i, \beta_i + \sum_{i\in[m_x]} \sum_{j\in[m_y]} \gamma_{i,j} x_i y_j = t \qquad \text{(QE)}$$

Example: Shuffles

How to prove that $(\hat{\mathbf{c}}, \hat{\mathbf{d}}) \in L_{\text{shuffle}}$?

Example: Shuffles

How to prove that $(\hat{\mathbf{c}}, \hat{\mathbf{d}}) \in L_{\text{shuffle}}$?
Show satisfiability of

$$
\begin{aligned}
p_{i,j}(p_{i,j} - 1) &= 0 \text{ for all } (i,j) \in [n]^2 && (1)\\
\sum_{j \in [n]} p_{i,j} &= 1 \text{ for all } i \in [n] && (2)\\
\sum_{i \in [n]} p_{i,j} &= 1 \text{ for all } i \in [n] && (3)\\
\sum_{j \in [n]} p_{i,j}\hat{\mathbf{c}}_j - \hat{\mathbf{d}}_i &= \delta_i \hat{\mathbf{u}} \text{ for all } i \in [n]. && (4)
\end{aligned}
$$

Example: Shuffles

How to prove that $(\hat{\mathbf{c}}, \hat{\mathbf{d}}) \in L_{\mathsf{shuffle}}$?
Show satisfiability of

$\mathbf{P}$ is a perm. matrix

$$
\begin{aligned}
p_{i,j}(p_{i,j} - 1) &= 0 \text{ for all } (i,j) \in [n]^2 && (1)\\
\sum_{j \in [n]} p_{i,j} &= 1 \text{ for all } i \in [n] && (2)\\
\sum_{i \in [n]} p_{i,j} &= 1 \text{ for all } i \in [n] && (3)\\
\sum_{j \in [n]} p_{i,j}\hat{\mathbf{c}}_j - \hat{\mathbf{d}}_i &= \delta_i \hat{\mathbf{u}} \text{ for all } i \in [n]. && (4)
\end{aligned}
$$

Example: Shuffles

How to prove that $(\hat{\mathbf{c}}, \hat{\mathbf{d}}) \in L_{\text{shuffle}}$?
Show satisfiability of

P is a perm. matrix

$$
\begin{aligned}
p_{i,j}(p_{i,j} - 1) &= 0 \text{ for all } (i,j) \in [n]^2 && (1)\\
\sum_{j \in [n]} p_{i,j} &= 1 \text{ for all } i \in [n] && (2)\\
\sum_{i \in [n]} p_{i,j} &= 1 \text{ for all } i \in [n] && (3)\\
\sum_{j \in [n]} p_{i,j}\hat{\mathbf{c}}_j - \hat{\mathbf{d}}_i &= \delta_i \hat{\mathbf{u}} \text{ for all } i \in [n]. && (4)
\end{aligned}
$$

Given a solution $\mathbf{P}, \boldsymbol{\delta}$ and CRS $\sigma := \{\hat{\mathbf{u}}_1, \hat{\mathbf{u}}_2\}$,

Example: Shuffles

How to prove that $(\hat{\mathbf{c}}, \hat{\mathbf{d}}) \in L_{\text{shuffle}}$?
Show satisfiability of

P is a perm. matrix

$$\begin{aligned}
p_{i,j}(p_{i,j}-1) &= 0 \text{ for all } (i,j) \in [n]^2 & (1)\\
\sum_{j\in[n]} p_{i,j} &= 1 \text{ for all } i \in [n] & (2)\\
\sum_{i\in[n]} p_{i,j} &= 1 \text{ for all } i \in [n] & (3)\\
\sum_{j\in[n]} p_{i,j}\hat{\mathbf{c}}_j - \hat{\mathbf{d}}_i &= \delta_i \hat{\mathbf{u}} \text{ for all } i \in [n]. & (4)
\end{aligned}$$

Given a solution $\mathbf{P}, \boldsymbol{\delta}$ and CRS $\sigma := \{\hat{\mathbf{u}}_1, \hat{\mathbf{u}}_2\}$, compute commitments $\check{\mathbf{p}}_{v,i,j} := p_{i,j}\check{\mathbf{e}}_1 + r_{i,j}\check{\mathbf{v}}_1 + s_{i,j}\check{\mathbf{v}}_2, \check{\boldsymbol{\delta}}_{v,i} := \delta_i\check{\mathbf{e}}_1 + r_i'\check{\mathbf{v}}_1 + s_i'\check{\mathbf{v}}_2$

Example: Shuffles

How to prove that $(\hat{\mathbf{c}}, \hat{\mathbf{d}}) \in L_{\text{shuffle}}$?
Show satisfiability of

P is a perm. matrix

$$\begin{aligned} p_{i,j}(p_{i,j}-1) &= 0 \text{ for all } (i,j) \in [n]^2 && (1)\\ \sum_{j\in[n]} p_{i,j} &= 1 \text{ for all } i \in [n] && (2)\\ \sum_{i\in[n]} p_{i,j} &= 1 \text{ for all } i \in [n] && (3)\\ \sum_{j\in[n]} p_{i,j}\hat{\mathbf{c}}_j - \hat{\mathbf{d}}_i &= \delta_i \hat{\mathbf{u}} \text{ for all } i \in [n]. && (4) \end{aligned}$$

Given a solution $\mathbf{P}, \boldsymbol{\delta}$ and CRS $\sigma := \{\hat{\mathbf{u}}_1, \hat{\mathbf{u}}_2\}$, compute commitments $\check{\mathbf{p}}_{v,i,j} := p_{i,j}\check{\mathbf{e}}_1 + r_{i,j}\check{\mathbf{v}}_1 + s_{i,j}\check{\mathbf{v}}_2, \check{\boldsymbol{\delta}}_{v,i} := \delta_i\check{\mathbf{e}}_1 + r'_i\check{\mathbf{v}}_1 + s'_i\check{\mathbf{v}}_2$ and compute proofs for each equations

Efficiency of the proofs

What is the cost of n of the previous proofs?

$$\text{Total proof size} \quad = \quad |\text{commitments}| + |\text{proofs}|$$

Efficiency of the proofs

What is the cost of n of the previous proofs?

$$\begin{aligned}\text{Total proof size} &= |\text{commitments}| + |\text{proofs}| \\ &= \underbrace{O(n^2)}_{\mathbf{P}} + \underbrace{O(n)}_{\boldsymbol{\delta}} + \underbrace{O(n^2)}_{(1)} + \underbrace{O(n)}_{(2),(3)\text{ and }(4)}\end{aligned}$$

Efficiency of the proofs

What is the cost of n of the previous proofs?

$$\begin{aligned}\text{Total proof size} &= |\text{commitments}| + |\text{proofs}| \\ &= \underbrace{O(n^2)}_{\mathbf{P}} + \underbrace{O(n)}_{\boldsymbol{\delta}} + \underbrace{O(n^2)}_{(1)} + \underbrace{O(n)}_{(2),(3)\text{ and }(4)}\end{aligned}$$

While the CRS size is $|ck| = O(1)$.

Proofs of Membership in Linear Sub-spaces of $\hat{\mathbb{G}}^n$

Observation 1

Ciphertexts $\hat{\mathbf{c}} := \hat{w}_1\mathbf{e}_1 + r_1\hat{\mathbf{u}}$ and $\hat{\mathbf{d}} := \hat{w}_2\mathbf{e}_1 + r_2\hat{\mathbf{u}}$ open to the same value iff there exists some $r \in \mathbb{Z}_q$ s.t. $\hat{\mathbf{c}} - \hat{\mathbf{d}} = r\hat{\mathbf{u}}$.

Proofs of Membership in Linear Sub-spaces of $\hat{\mathbb{G}}^n$

Observation 1

Ciphertexts $\hat{\mathbf{c}} := \hat{w}_1\mathbf{e}_1 + r_1\hat{\mathbf{u}}$ and $\hat{\mathbf{d}} := \hat{w}_2\mathbf{e}_1 + r_2\hat{\mathbf{u}}$ open to the same value iff there exists some $r \in \mathbb{Z}_q$ s.t. $\hat{\mathbf{c}} - \hat{\mathbf{d}} = r\hat{\mathbf{u}}$.

Observation 2

The vectors of commitments $\hat{\mathbf{c}} = (\hat{\mathbf{c}}_1 || \ldots || \hat{\mathbf{c}}_n)^\top \in \hat{\mathbb{G}}^{2n}$ and $\hat{\mathbf{d}} = (\hat{\mathbf{d}}_1 || \ldots || \hat{\mathbf{d}}_n)^\top \in \hat{\mathbb{G}}^{2n}$ open to the same value iff $\exists \mathbf{w} \in \mathbb{Z}_q^n$ s.t.

$$\hat{\mathbf{c}} - \hat{\mathbf{d}} = \begin{pmatrix} \hat{\mathbf{u}} & & \hat{\mathbf{0}} \\ & \ddots & \\ \hat{\mathbf{0}} & & \hat{\mathbf{u}} \end{pmatrix} \mathbf{w}.$$

Proofs of Membership in Linear Sub-spaces of $\hat{\mathbb{G}}^n$

Observation 1

Ciphertexts $\hat{\mathbf{c}} := \hat{w}_1\mathbf{e}_1 + r_1\hat{\mathbf{u}}$ and $\hat{\mathbf{d}} := \hat{w}_2\mathbf{e}_1 + r_2\hat{\mathbf{u}}$ open to the same value iff there exists some $r \in \mathbb{Z}_q$ s.t. $\hat{\mathbf{c}} - \hat{\mathbf{d}} = r\hat{\mathbf{u}}$.

Observation 2

The vectors of commitments $\hat{\mathbf{c}} = (\hat{\mathbf{c}}_1 || \ldots || \hat{\mathbf{c}}_n)^\top \in \hat{\mathbb{G}}^{2n}$ and $\hat{\mathbf{d}} = (\hat{\mathbf{d}}_1 || \ldots || \hat{\mathbf{d}}_n)^\top \in \hat{\mathbb{G}}^{2n}$ open to the same value iff $\exists \mathbf{w} \in \mathbb{Z}_q^n$ s.t.

$$\hat{\mathbf{c}} - \hat{\mathbf{d}} = \begin{pmatrix} \hat{\mathbf{u}} & & \hat{\mathbf{0}} \\ & \ddots & \\ \hat{\mathbf{0}} & & \hat{\mathbf{u}} \end{pmatrix} \mathbf{w}.$$

$$L_{\hat{\mathbf{M}}} := \{(\hat{\mathbf{c}}, \hat{\mathbf{d}}) : \exists \mathbf{w} \in \mathbb{Z}_q^t \text{ and } \hat{\mathbf{c}} - \hat{\mathbf{d}} = \hat{\mathbf{M}}\mathbf{w}\}, \text{ where } \hat{\mathbf{M}} = \begin{pmatrix} \hat{\mathbf{u}} & & \hat{\mathbf{0}} \\ & \ddots & \\ \hat{\mathbf{0}} & & \hat{\mathbf{u}} \end{pmatrix}$$

Quasi-Adaptive NIZK (QA-NIZK)

Recently (Libert et al EuroCrypt 2013, Jutla and Roy Crypto 2014, Abdalla et al. and Kiltz and Wee EuroCrypt 2015) it has been shown how to:

Linear Subspaces Constant size proofs of membership in the in linear subspaces of $\hat{\mathbb{G}}^n$

$$L_{\hat{\mathbf{M}}} = \{\hat{\mathbf{c}} : \exists \mathbf{w} \in \mathbb{Z}_q^t \text{ s.t. } \hat{\mathbf{c}} = \hat{\mathbf{M}}\mathbf{w}\}.$$

Quasi-Adaptive NIZK (QA-NIZK)

Recently (Libert et al EuroCrypt 2013, Jutla and Roy Crypto 2014, Abdalla et al. and Kiltz and Wee EuroCrypt 2015) it has been shown how to:

Linear Subspaces Constant size proofs of membership in the in linear subspaces of $\hat{\mathbb{G}}^n$

$$L_{\hat{\mathbf{M}}} = \{\hat{\mathbf{c}} : \exists \mathbf{w} \in \mathbb{Z}_q^t \text{ s.t. } \hat{\mathbf{c}} = \hat{\mathbf{M}}\mathbf{w}\}.$$

Aggregation of GS proofs Prove satisfiability of n one-sided linear equations using only one GS proof.

$$\sum_{i \in [m_x]} \hat{\alpha}_i, \hat{x}_i = t$$

Quasi-Adaptive NIZK (QA-NIZK)

Recently (Libert et al EuroCrypt 2013, Jutla and Roy Crypto 2014, Abdalla et al. and Kiltz and Wee EuroCrypt 2015) it has been shown how to:

Linear Subspaces Constant size proofs of membership in the in linear subspaces of $\hat{\mathbb{G}}^n$

$$L_{\hat{\mathbf{M}}} = \{\hat{\mathbf{c}} : \exists \mathbf{w} \in \mathbb{Z}_q^t \text{ s.t. } \hat{\mathbf{c}} = \hat{\mathbf{M}}\mathbf{w}\}.$$

Aggregation of GS proofs Prove satisfiability of n one-sided linear equations using only one GS proof.

$$\sum_{i \in [m_x]} \hat{\alpha}_i, \hat{x}_i = t$$

In both cases

$$|\text{proof}| = O(1)$$

Quasi-Adaptive NIZK (QA-NIZK)

Recently (Libert et al EuroCrypt 2013, Jutla and Roy Crypto 2014, Abdalla et al. and Kiltz and Wee EuroCrypt 2015) it has been shown how to:

Linear Subspaces Constant size proofs of membership in the in linear subspaces of $\hat{\mathbb{G}}^n$

$$L_{\hat{\mathbf{M}}} = \{\hat{\mathbf{c}} : \exists \mathbf{w} \in \mathbb{Z}_q^t \text{ s.t. } \hat{\mathbf{c}} = \hat{\mathbf{M}}\mathbf{w}\}.$$

Aggregation of GS proofs Prove satisfiability of n one-sided linear equations using only one GS proof.

$$\sum_{i \in [m_x]} \hat{\alpha}_i, \hat{x}_i = t$$

In both cases

$$|\text{proof}| = O(1)$$
$$|\text{CRS}| = O(n).$$

Kernel Assumptions

The security of the constructions for Linear Subspaces can be based on the next assumption.

Definition (Simultaneos Pairing Assumption)

Any adversary $\mathcal{A}$ has at most negligible probability of winning in the next game:

- Pick $\mathbf{a} \leftarrow \binom{\mathbb{Z}_q}{1}$.

Kernel Assumptions

The security of the constructions for Linear Subspaces can be based on the next assumption.

Definition (Simultaneos Pairing Assumption)

Any adversary $\mathcal{A}$ has at most negligible probability of winning in the next game:

- Pick $\mathbf{a} \leftarrow \binom{\mathbb{Z}_q}{1}$.
- Compute $\hat{\mathbf{x}} \leftarrow \mathcal{A}(\check{\mathbf{a}})$.

Kernel Assumptions

The security of the constructions for Linear Subspaces can be based on the next assumption.

Definition (Simultaneos Pairing Assumption)

Any adversary $\mathcal{A}$ has at most negligible probability of winning in the next game:

- Pick $\mathbf{a} \leftarrow \binom{\mathbb{Z}_q}{1}$.
- Compute $\hat{\mathbf{x}} \leftarrow \mathcal{A}(\check{\mathbf{a}})$.
- $\mathcal{A}$ wins iff $\mathbf{a}^\top \mathbf{x} = \mathbf{0}$ and $\mathbf{x} \neq \mathbf{0}$.

Membership in Linear Subspaces of $\hat{\mathbb{G}}^n$

Prove membership in $L_{\hat{\mathbf{M}}}$, where $\hat{\mathbf{M}} \in \hat{\mathbb{G}}^{n \times t}$.

Membership in Linear Subspaces of $\hat{\mathbb{G}}^n$

Prove membership in $L_{\hat{\mathbf{M}}}$, where $\hat{\mathbf{M}} \in \hat{\mathbb{G}}^{n\times t}$. Consider a MSK $\mathbf{\Delta} \leftarrow \mathbb{Z}_q^{2\times(n)}$,

$$\mathbf{\Delta} : \hat{\mathbb{G}}^n \to \hat{\mathbb{G}}^2.$$

Membership in Linear Subspaces of $\hat{\mathbb{G}}^n$

Prove membership in $L_{\hat{\mathbf{M}}}$, where $\hat{\mathbf{M}} \in \hat{\mathbb{G}}^{n\times t}$. Consider a MSK $\mathbf{\Delta} \leftarrow \mathbb{Z}_q^{2\times(n)}$,

$$\mathbf{\Delta} : \hat{\mathbb{G}}^n \to \hat{\mathbb{G}}^2.$$

QA-NIZK for $L_{\hat{\mathbf{M}}}$ from [LPJY14]

Membership in Linear Subspaces of $\hat{\mathbb{G}}^n$

Prove membership in $L_{\hat{\mathbf{M}}}$, where $\hat{\mathbf{M}} \in \hat{\mathbb{G}}^{n \times t}$. Consider a MSK $\mathbf{\Delta} \leftarrow \mathbb{Z}_q^{2 \times (n)}$,

$$\mathbf{\Delta} : \hat{\mathbb{G}}^n \to \hat{\mathbb{G}}^2.$$

QA-NIZK for $L_{\hat{\mathbf{M}}}$ from [LPJY14]

- The CRS contains $\hat{\mathbf{M}}_\Delta := \mathbf{\Delta}\hat{\mathbf{M}}$ and $\check{\mathbf{a}}_\Delta := \check{\mathbf{a}}^\top \mathbf{\Delta}$

Membership in Linear Subspaces of $\hat{\mathbb{G}}^n$

Prove membership in $L_{\hat{\mathbf{M}}}$, where $\hat{\mathbf{M}} \in \hat{\mathbb{G}}^{n\times t}$. Consider a MSK $\mathbf{\Delta} \leftarrow \mathbb{Z}_q^{2\times(n)}$,

$$\mathbf{\Delta} : \hat{\mathbb{G}}^n \to \hat{\mathbb{G}}^2.$$

QA-NIZK for $L_{\hat{\mathbf{M}}}$ from [LPJY14]

- The CRS contains $\hat{\mathbf{M}}_\Delta := \mathbf{\Delta}\hat{\mathbf{M}}$ and $\check{\mathbf{a}}_\Delta := \check{\mathbf{a}}^\top \mathbf{\Delta}$
- Proof for $\hat{\mathbf{x}} = \hat{\mathbf{M}}\mathbf{w}$ is $\hat{\boldsymbol{\rho}} := \hat{\mathbf{M}}_\Delta \mathbf{w}$.

Membership in Linear Subspaces of $\hat{\mathbb{G}}^n$

Prove membership in $L_{\hat{\mathbf{M}}}$, where $\hat{\mathbf{M}} \in \hat{\mathbb{G}}^{n\times t}$. Consider a MSK $\boldsymbol{\Delta} \leftarrow \mathbb{Z}_q^{2\times(n)}$,

$$\boldsymbol{\Delta} : \hat{\mathbb{G}}^n \to \hat{\mathbb{G}}^2.$$

QA-NIZK for $L_{\hat{\mathbf{M}}}$ from [LPJY14]

- The CRS contains $\hat{\mathbf{M}}_\Delta := \boldsymbol{\Delta}\hat{\mathbf{M}}$ and $\check{\mathbf{a}}_\Delta := \check{\mathbf{a}}^\top \boldsymbol{\Delta}$
- Proof for $\hat{\mathbf{x}} = \hat{\mathbf{M}}\mathbf{w}$ is $\hat{\boldsymbol{\rho}} := \hat{\mathbf{M}}_\Delta \mathbf{w}$.
- Victor checks $\check{\mathbf{a}}^\top \hat{\boldsymbol{\rho}} = \check{\mathbf{a}}_\Delta^\top \hat{\mathbf{x}}$

Returning to Shuffles

$$(\hat{\mathbf{c}}, \hat{\mathbf{d}}) \in L_{\text{shuffle}} \text{ iff } \begin{pmatrix} \hat{\mathbf{c}}_1 - \hat{\mathbf{d}}_{\pi(1)} \\ \vdots \\ \hat{\mathbf{c}}_n - \hat{\mathbf{d}}_{\pi(n)} \end{pmatrix} \in L_{\hat{\mathbf{M}}},$$

Returning to Shuffles

$(\hat{\mathbf{c}}, \hat{\mathbf{d}}) \in L_{\text{shuffle}}$ iff $\begin{pmatrix} \hat{\mathbf{c}}_1 - \hat{\mathbf{d}}_{\pi(1)} \\ \vdots \\ \hat{\mathbf{c}}_n - \hat{\mathbf{d}}_{\pi(n)} \end{pmatrix} \in L_{\hat{\mathbf{M}}}$, Consider a MSK $\boldsymbol{\Delta} \leftarrow \mathbb{Z}_q^{2\times(n)}$,

Returning to Shuffles

$(\hat{\mathbf{c}}, \hat{\mathbf{d}}) \in L_{\textsf{shuffle}}$ iff $\begin{pmatrix} \hat{\mathbf{c}}_1 - \hat{\mathbf{d}}_{\pi(1)} \\ \vdots \\ \hat{\mathbf{c}}_n - \hat{\mathbf{d}}_{\pi(n)} \end{pmatrix} \in L_{\hat{\mathbf{M}}}$, Consider a MSK $\boldsymbol{\Delta} \leftarrow \mathbb{Z}_q^{2\times(n)}$,

QA-NIZK for $L_{\textsf{shuffle}}$

Returning to Shuffles

$(\hat{\mathbf{c}}, \hat{\mathbf{d}}) \in L_{\text{shuffle}}$ iff $\begin{pmatrix} \hat{\mathbf{c}}_1 - \hat{\mathbf{d}}_{\pi(1)} \\ \vdots \\ \hat{\mathbf{c}}_n - \hat{\mathbf{d}}_{\pi(n)} \end{pmatrix} \in L_{\hat{\mathbf{M}}}$, Consider a MSK $\boldsymbol{\Delta} \leftarrow \mathbb{Z}_q^{2\times(n)}$,

QA-NIZK for L_{shuffle}

- The CRS contains $\hat{\mathbf{M}}_\Delta := \boldsymbol{\Delta}\hat{\mathbf{M}}$ and $\check{\mathbf{a}}_\Delta := \check{\mathbf{a}}^\top \boldsymbol{\Delta}$ and $\check{\mathbf{b}}_\Delta = (\check{\mathbf{a}}_{\Delta,\pi(1)}, \ldots, \check{\mathbf{a}}_{\Delta,\pi(n)})$.

Returning to Shuffles

$(\hat{\mathbf{c}}, \hat{\mathbf{d}}) \in L_{\text{shuffle}}$ iff $\begin{pmatrix} \hat{\mathbf{c}}_1 - \hat{\mathbf{d}}_{\pi(1)} \\ \vdots \\ \hat{\mathbf{c}}_n - \hat{\mathbf{d}}_{\pi(n)} \end{pmatrix} \in L_{\hat{\mathbf{M}}}$, Consider a MSK $\mathbf{\Delta} \leftarrow \mathbb{Z}_q^{2\times(n)}$,

QA-NIZK for L_{shuffle}

- The CRS contains $\hat{\mathbf{M}}_\Delta := \mathbf{\Delta}\hat{\mathbf{M}}$ and $\check{\mathbf{a}}_\Delta := \check{\mathbf{a}}^\top \mathbf{\Delta}$ and $\check{\mathbf{b}}_\Delta = (\check{\mathbf{a}}_{\Delta,\pi(1)}, \ldots, \check{\mathbf{a}}_{\Delta,\pi(n)})$.
- Proof for $(\hat{\mathbf{c}}, \hat{\mathbf{d}})$ s.t. $\hat{\mathbf{c}} - \hat{\mathbf{d}} = \hat{\mathbf{M}}\boldsymbol{\delta}$ is $\hat{\boldsymbol{\rho}} := \hat{\mathbf{M}}_\Delta \boldsymbol{\delta}$.

Returning to Shuffles

$(\hat{\mathbf{c}}, \hat{\mathbf{d}}) \in L_{\text{shuffle}}$ iff $\begin{pmatrix} \hat{\mathbf{c}}_1 - \hat{\mathbf{d}}_{\pi(1)} \\ \vdots \\ \hat{\mathbf{c}}_n - \hat{\mathbf{d}}_{\pi(n)} \end{pmatrix} \in L_{\hat{\mathbf{M}}}$, Consider a MSK $\boldsymbol{\Delta} \leftarrow \mathbb{Z}_q^{2\times(n)}$,

QA-NIZK for L_{shuffle}

- The CRS contains $\hat{\mathbf{M}}_\Delta := \boldsymbol{\Delta}\hat{\mathbf{M}}$ and $\check{\mathbf{a}}_\Delta := \check{\mathbf{a}}^\top \boldsymbol{\Delta}$ and $\check{\mathbf{b}}_\Delta = (\check{\mathbf{a}}_{\Delta,\pi(1)}, \ldots, \check{\mathbf{a}}_{\Delta,\pi(n)})$.
- Proof for $(\hat{\mathbf{c}}, \hat{\mathbf{d}})$ s.t. $\hat{\mathbf{c}} - \hat{\mathbf{d}} = \hat{\mathbf{M}}\boldsymbol{\delta}$ is $\hat{\boldsymbol{\rho}} := \hat{\mathbf{M}}_\Delta \boldsymbol{\delta}$.
- Victor checks $\check{\mathbf{a}}^\top \hat{\boldsymbol{\rho}} = \check{\mathbf{a}}_\Delta^\top \hat{\mathbf{c}} - \check{\mathbf{b}}_\Delta^\top \hat{\mathbf{d}}$.

Returning to Shuffles

- The permutation is fixed!

Returning to Shuffles

- The permutation is fixed! Include commitment to $\check{\mathbf{b}}_{\Delta}$

Returning to Shuffles

- The permutation is fixed! Include commitment to $\check{\mathbf{b}}_\Delta$
- How to prove that commitment $\check{\mathbf{f}}_1, \ldots, \check{\mathbf{f}}_n$ to $\check{\mathbf{b}}_\Delta$ was correctly computed?

Returning to Shuffles

- The permutation is fixed! Include commitment to $\check{\mathbf{b}}_\Delta$
- How to prove that commitment $\check{\mathbf{f}}_1, \ldots, \check{\mathbf{f}}_n$ to $\check{\mathbf{b}}_\Delta$ was correctly computed?
- Groth and Lu (AsiaCrypt 2007) basically assumed that $\check{\mathbf{f}}_1, \ldots, \check{\mathbf{f}}_n$ s.t. $\hat{\mathbf{f}}_i - \check{\mathbf{a}}_{\Delta,i}$ opens to 0 suffices.

Returning to Shuffles

- The permutation is fixed! Include commitment to $\check{\mathbf{b}}_\Delta$
- How to prove that commitment $\check{\mathbf{f}}_1, \ldots, \check{\mathbf{f}}_n$ to $\check{\mathbf{b}}_\Delta$ was correctly computed?
- Groth and Lu (AsiaCrypt 2007) basically assumed that $\check{\mathbf{f}}_1, \ldots, \check{\mathbf{f}}_n$ s.t. $\hat{\mathbf{f}}_i - \check{\mathbf{a}}_{\Delta,i}$ opens to 0 suffices.
- Groth and Lu's construction is the most efficient construction under mild assumptions with $O(n)$ communication.

Proving that a commitment opens to a permutation

- Prove that each $\check{\mathbf{f}}_i$ opens to an element from the list $\{\check{\mathbf{a}}_{\Delta,1}, \dots, \check{\mathbf{a}}_{\Delta,n}\}$.*

Proving that a commitment opens to a permutation

- Prove that each $\check{\mathbf{f}}_i$ opens to an element from the list $\{\check{\mathbf{a}}_{\Delta,1},\ldots,\check{\mathbf{a}}_{\Delta,n}\}$.*
- Prove that $\sum_i \check{\mathbf{f}}_i - \sum_i \check{\mathbf{a}}_{\Delta,i}$ opens to 0.

Proving that a commitment opens to a permutation

- Prove that each $\check{\mathbf{f}}_i$ opens to an element from the list $\{\check{\mathbf{a}}_{\Delta,1}, \ldots, \check{\mathbf{a}}_{\Delta,n}\}$.*
- Prove that $\sum_i \check{\mathbf{f}}_i - \sum_i \check{\mathbf{a}}_{\Delta,i}$ opens to 0.
- Note that $\sum_i \check{\mathbf{f}}_i = \sum_i \ell_i \check{\mathbf{a}}_{\Delta,i}$ for $\ell_i \in \mathbb{Z}_n$.

Proving that a commitment opens to a permutation

- Prove that each $\check{\mathbf{f}}_i$ opens to an element from the list $\{\check{\mathbf{a}}_{\Delta,1}, \ldots, \check{\mathbf{a}}_{\Delta,n}\}$.*
- Prove that $\sum_i \check{\mathbf{f}}_i - \sum_i \check{\mathbf{a}}_{\Delta,i}$ opens to 0.
- Note that $\sum_i \check{\mathbf{f}}_i = \sum_i \ell_i \check{\mathbf{a}}_{\Delta,i}$ for $\ell_i \in \mathbb{Z}_n$.
- If there is some $\ell_i \neq 1$ then $(\ell_1 - 1, \ldots, \ell_n - 1) \in \mathbf{Ker}(\check{\mathbf{a}}_\Delta^\top)$.

GS aggregation and QA-NIZK in asymmetric groups

We construct constant-size QA-NIZK proofs of membership in the language

$$L_{\hat{\mathbf{M}},\check{\mathbf{N}}} = \left\{ (\hat{\mathbf{x}}, \check{\mathbf{y}}) \in (\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n) : \exists \mathbf{w} \in \mathbb{Z}_q^t \text{ s.t. } \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} = \begin{pmatrix} \mathbf{M} \\ \mathbf{N} \end{pmatrix} \mathbf{w} \right\}.$$

GS aggregation and QA-NIZK in asymmetric groups

We construct constant-size QA-NIZK proofs of membership in the language

$$L_{\hat{\mathbf{M}},\check{\mathbf{N}}} = \left\{ (\hat{\mathbf{x}}, \check{\mathbf{y}}) \in (\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n) : \exists \mathbf{w} \in \mathbb{Z}_q^t \text{ s.t. } \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} = \begin{pmatrix} \mathbf{M} \\ \mathbf{N} \end{pmatrix} \mathbf{w} \right\}.$$

Which allows us to construct:

GS aggregation and QA-NIZK in asymmetric groups

We construct constant-size QA-NIZK proofs of membership in the language

$$L_{\hat{\mathbf{M}},\check{\mathbf{N}}} = \left\{ (\hat{\mathbf{x}}, \check{\mathbf{y}}) \in (\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n) : \exists \mathbf{w} \in \mathbb{Z}_q^t \text{ s.t. } \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} = \begin{pmatrix} \mathbf{M} \\ \mathbf{N} \end{pmatrix} \mathbf{w} \right\}.$$

Which allows us to construct:

- Constant-size proofs that two set set of commitments, even in different groups, opens to the same value.

GS aggregation and QA-NIZK in asymmetric groups

We construct constant-size QA-NIZK proofs of membership in the language

$$L_{\hat{\mathbf{M}},\check{\mathbf{N}}} = \left\{ (\hat{\mathbf{x}}, \check{\mathbf{y}}) \in (\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n) : \exists \mathbf{w} \in \mathbb{Z}_q^t \text{ s.t. } \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} = \begin{pmatrix} \mathbf{M} \\ \mathbf{N} \end{pmatrix} \mathbf{w} \right\}.$$

Which allows us to construct:

- Constant-size proofs that two set set of commitments, even in different groups, opens to the same value.
- Similar techniques allows to aggregate the proof of n two-sided linear equations into only two GS proofs.

Aggregation of Quadratic equations over $\mathbb{Z}_q$

We construct constant size QA-NIZK proofs of membership in the language

$$L_{\hat{\mathbf{U}}_1,\hat{\mathbf{U}}_2,\mathsf{bits}} = \{\hat{\mathbf{c}} \in \hat{\mathbb{G}}^n : \exists \mathbf{b} \in \{0,1\}^n, \mathbf{w} \in \mathbb{Z}_q^m \text{ s.t } \hat{\mathbf{c}} = \hat{\mathbf{U}}_1\mathbf{b} + \hat{\mathbf{U}}_2\mathbf{w}\}.$$

Aggregation of Quadratic equations over $\mathbb{Z}_q$

We construct constant size QA-NIZK proofs of membership in the language

$$L_{\hat{\mathbf{U}}_1,\hat{\mathbf{U}}_2,\text{bits}} = \{\hat{\mathbf{c}} \in \hat{\mathbb{G}}^n : \exists \mathbf{b} \in \{0,1\}^n, \mathbf{w} \in \mathbb{Z}_q^m \text{ s.t } \hat{\mathbf{c}} = \hat{\mathbf{U}}_1\mathbf{b} + \hat{\mathbf{U}}_2\mathbf{w}\}.$$

Equivalently, show satisfiability of

$$b_i(b_i - 1) = 0 \qquad\qquad \forall i \in [n]$$

Aggregation of Quadratic equations over $\mathbb{Z}_q$

We construct constant size QA-NIZK proofs of membership in the language

$$L_{\hat{\mathbf{U}}_1,\hat{\mathbf{U}}_2,\text{bits}} = \{\hat{\mathbf{c}} \in \hat{\mathbb{G}}^n : \exists \mathbf{b} \in \{0,1\}^n, \mathbf{w} \in \mathbb{Z}_q^m \text{ s.t } \hat{\mathbf{c}} = \hat{\mathbf{U}}_1\mathbf{b} + \hat{\mathbf{U}}_2\mathbf{w}\}.$$

Equivalently, show satisfiability of

$$b_i(b_i - 1) = 0 \qquad \forall i \in [n]$$

No such construction was known even in Symmetric Groups!

Higher degree equations

Show satisfiability of l equations of the form

$$\prod_{i \in [n]} (x - a_i) = 0$$

Higher degree equations

Show satisfiability of l equations of the form

$$\prod_{i \in [n]} (x - a_i) = 0$$

Which can be reformulated as

$$L_{\{a_1,\ldots,a_n\}} = \{\hat{\mathbf{c}} : \forall i \in [l] \ \hat{\mathbf{c}}_i \text{ opens to a value in } \{a_1, \ldots, a_n\}\}$$

Higher degree equations

Show satisfiability of l equations of the form

$$\prod_{i \in [n]} (x - a_i) = 0$$

Which can be reformulated as

$$L_{\{a_1,\ldots,a_n\}} = \{\hat{\mathbf{c}} : \forall i \in [l]\ \hat{\mathbf{c}}_i \text{ opens to a value in } \{a_1, \ldots, a_n\}\}$$

How to reduce to the satisfiability of quadratic equations?

Higher degree equations

Show satisfiability of l equations of the form

$$\prod_{i\in[n]}(x-a_i)=0$$

Which can be reformulated as

$$L_{\{a_1,\ldots,a_n\}}=\{\hat{\mathbf{c}}:\forall i\in[l]\ \hat{\mathbf{c}}_i \text{ opens to a value in } \{a_1,\ldots,a_n\}\}$$

How to reduce to the satisfiability of quadratic equations?

- $\prod_{i\in[n]}(x-a_i)=0 \iff (x-a_1)(x-a_2)=y_1,\ y_1(x-a_3)=y_2,\ldots$

Higher degree equations

Show satisfiability of l equations of the form

$$\prod_{i\in[n]}(x-a_i)=0$$

Which can be reformulated as

$$L_{\{a_1,\ldots,a_n\}}=\{\hat{\mathbf{c}}:\forall i\in[l]\ \hat{\mathbf{c}}_i \text{ opens to a value in } \{a_1,\ldots,a_n\}\}$$

How to reduce to the satisfiability of quadratic equations?

- $\prod_{i\in[n]}(x-a_i)=0 \iff (x-a_1)(x-a_2)=y_1,\ y_1(x-a_3)=y_2,\ldots$
- $O(n)$ proof for a single equation.

Higher degree equations

Show satisfiability of l equations of the form

$$\prod_{i \in [n]} (x - a_i) = 0$$

Which can be reformulated as

$$L_{\{a_1,\ldots,a_n\}} = \{\hat{\mathbf{c}} : \forall i \in [l]\ \hat{\mathbf{c}}_i \text{ opens to a value in } \{a_1, \ldots, a_n\}\}$$

How to reduce to the satisfiability of quadratic equations?

- $\prod_{i \in [n]}(x - a_i) = 0 \iff (x - a_1)(x - a_2) = y_1,\ y_1(x - a_3) = y_2, \ldots$
- $O(n)$ proof for a single equation.
- Proof for l equations can be aggregated into a single $O(n)$ proof.

Conclusion

- We reviewed NIZK Shuffle Arguments.

Conclusion

- We reviewed NIZK Shuffle Arguments.
- We reviewed NIZK proofs of membership in linear subspaces.

Conclusion

- We reviewed NIZK Shuffle Arguments.
- We reviewed NIZK proofs of membership in linear subspaces.
- We reviewed aggregation of quadratic equations.

Conclusion

- We reviewed NIZK Shuffle Arguments.
- We reviewed NIZK proofs of membership in linear subspaces.
- We reviewed aggregation of quadratic equations.
- We showed how to construct efficient NIZK Shuffle Arguments under mild assumptions.

1 Introduction
- Mix-nets and Shuffles
- Non-Interactive Zero-Knowledge
- Bilinear Groups and Tools

2 State of the art
- Groth-Sahai Proofs
- NIZK for membership in Linear Subspaces of $\hat{\mathbb{G}}^n$

3 Prior Work
- NIZK for membership in Linear Subspaces of $\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n$
- Aggregation of quadratic equations

4 Efficient NIZK Shuffle Arguments

1 Introduction
- Mix-nets and Shuffles
- Non-Interactive Zero-Knowledge
- Bilinear Groups and Tools

2 State of the art
- Groth-Sahai Proofs
- NIZK for membership in Linear Subspaces of $\hat{\mathbb{G}}^n$

3 Prior Work
- NIZK for membership in Linear Subspaces of $\hat{\mathbb{G}}^m \times \check{\mathbb{H}}^n$
- Aggregation of quadratic equations

4 Efficient NIZK Shuffle Arguments

Sanjit Chatterjee and Alfred Menezes.
On cryptographic protocols employing asymmetric pairings - the role of Ψ revisited.
Discrete Applied Mathematics, 159(13):1311–1322, 2011.

S.D. Galbraith, K.G. Paterson, and N.P. Smart.
Pairings for cryptographers.
Cryptology ePrint Archive, Report 2006/165, 2006.
http://eprint.iacr.org/2006/165.

Jens Groth and Amit Sahai.
Efficient non-interactive proof systems for bilinear groups.
In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432, Istanbul, Turkey, April 13–17, 2008. Springer, Berlin, Germany.

Antoine Joux.
Faster index calculus for the medium prime case application to 1175-bit and 1425-bit finite fields.

In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 177–193, Athens, Greece, May 26–30, 2013. Springer, Berlin, Germany.

Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung.
Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures.
In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 514–532, Copenhagen, Denmark, May 11–15, 2014. Springer, Berlin, Germany.