Verifiable Mixing

Philipp Locher

Bern University of Applied Sciences

E-Voting PhD Days 2013

November 2013

Outline

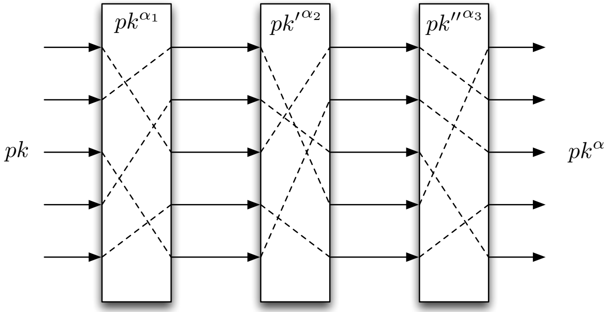
1. Introduction
2. Mix-Nets – an Overview
3. Preliminaries
4. Wikström/Terelius's Mix-Net Revisited
5. Conclusion

UniVote: Verifiable Electronic Voting over the Internet

- Internet voting system for student board elections at Swiss universities
- Project started in 2012
- First elections in spring 2013
- https://www.univote.ch

UniVote is end-to-end (E2E) verifiable and offers anonymized vote casting [Neff01, HS11].

Mixing of public keys:

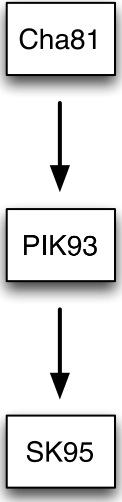


Introduction

Before the final decryption and tally phase, the ballots are mixed.

- Late registration (students cannot be forced to register before voting phase)
- Anonymous channel cannot always be expected
- No performance issue (only a few thousand ballots)

Mix-Nets – an Overview



Cha81:

- Anonymous Channel

  $E_1(r_1||E_2(r_2||\ldots E_k(r_k||B_i||E_{B_i}(m))))$

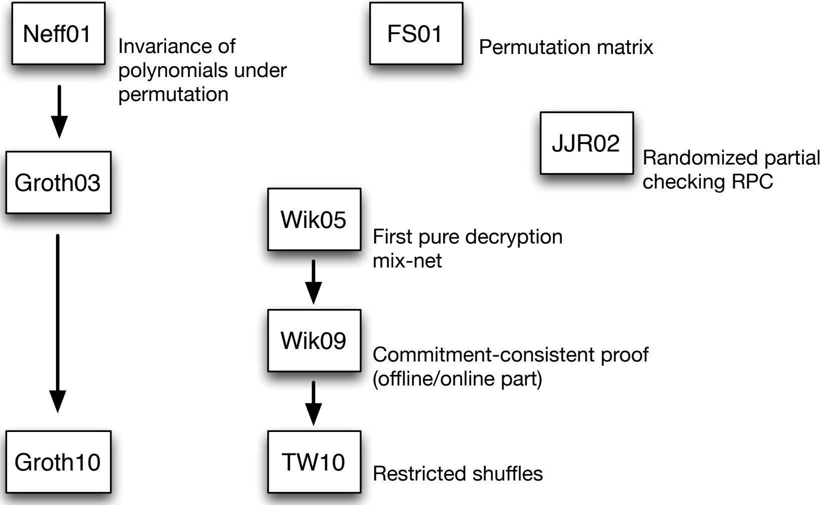
PIK93:

- No ciphertext length expansion
- ElGamal, partially decryption/re-encryption

SK95:

- First universal verifiable mix-net

Mix-Nets – an Overview



Mix-Nets – an Overview

Why Wikström/Terelius's Mix-Net?

- Not covered by patents
- Kind of modularity
- As efficient as other efficient mix-nets

Outline

ElGamal Encryption

$$Enc(m, r) = (g^r, y^r m)$$

- Private key x and public key $pk = (g, y)$, g is a generator of G_q and $y = g^x$
- $m \in G_q$ and $r \in_R \mathbb{Z}_q$
- Multiplicative homomorphic: $Enc(m_1, r_1) \cdot Enc(m_2, r_2) = Enc(m_1 m_2, r_1 + r_2)$
- Re-encryption: $ReEnc(c, r') = c \cdot Enc(1, r')$

Pedersen Commitment

$$Com(m, r) = g^r \cdot h^m$$

- g, h independently chosen generators of G_q
- $m \in \mathbb{Z}_q$ and $r \in_R \mathbb{Z}_q$
- Perfectly hiding and computationally binding
- Additive homomorphic:
  $Com(m_1, r_1) \cdot Com(m_2, r_2) = Com(m_1 + m_2, r_1 + r_2)$

Generalized Pedersen Commitment

$$Com(\bar{m}, r) = g^r \cdot h_1^{m_1} \cdots h_N^{m_N} = g^r \prod_{i=1}^{N} h_i^{m_i}$$

- $g, h_1, \ldots, h_N$ independently chosen generators of G_q
- $\bar{m} = (m_1, \ldots, m_N) \in \mathbb{Z}_q^N$ and $r \in_R \mathbb{Z}_q$
- Perfectly hiding and computationally binding
- Additive homomorphic:
  $Com(\bar{m}_1, r_1) \cdot Com(\bar{m}_2, r_2) = Com(\bar{m}_1 + \bar{m}_2, r_1 + r_2)$

Matrix Commitment

$$Com(M, \bar{r}) = (Com((m_{i,1})_{i=1}^{N}, r_1), \cdots, Com((m_{i,N})_{i=1}^{N}, r_N))$$

- $M = (m_{i,j}) \in \mathbb{Z}_q^{N \times N}$ is a $N \times N$ - matrix
- Perfectly hiding and computationally binding
- $Com(M, \bar{r})^{\bar{e}} = Com(M\bar{e}, \langle \bar{r}, \bar{e} \rangle)$

Zero-Knowledge Proof of Knowledge

Zero-Knowledge Proof of Knowledge
Example: Schnorr Protocol

Prover $\mathcal{P}$ proves to verifier $\mathcal{V}$ knowledge of x such that $y = g^x$

$\mathcal{P}$		$\mathcal{V}$
$r \in_R \mathbb{Z}_q$		
$t = g^r$		
	$\xrightarrow{t}$	
		$c \in_R \mathbb{Z}_q$
	$\xleftarrow{c}$	
$s = r + cx$		
	$\xrightarrow{s}$	
		$g^s \stackrel{?}{=} ty^c$

Maurer's Generic Preimage Proof 1/2

- Consider two groups $(G, \star)$ and $(H, \otimes)$ of finite order.
- If a function $\phi : G \rightarrow H$ is a homomorphism such that

$$\phi(a \star b) = \phi(a) \otimes \phi(b)$$

than $\mathcal{P}$ can prove knowledge of x such that $y = \phi(x)$ using the following protocol:

Maurer's Generic Preimage Proof 2/2

$\mathcal{P}$		$\mathcal{V}$
$r \in_R G$		
$t = \phi(r)$		
	$\xrightarrow{\quad t \quad}$	
		$c \in_R \mathcal{C}$
	$\xleftarrow{\quad c \quad}$	
$s = r \star c^x$		
	$\xrightarrow{\quad s \quad}$	
		$\phi(s) \stackrel{?}{=} t \otimes y^c$

Proof of Knowledge of Several Values (Composition)

- Consider N group homomorphisms

$$G_i \to H_i : x \mapsto \phi_i(x).$$

- The composition

$$G_1 \times \cdots \times G_N \to H_1 \times \cdots \times H_N : \\ (x_1, \ldots, x_N) \mapsto \phi(x_1, \ldots, x_N) = (\phi_i(x_i), \ldots, \phi_N(x_N))$$

is also a group homomorphism and so prover $\mathcal{P}$ can prove in one stroke knowledge of $x_1, \ldots, x_N$ such that $y_i = \phi_i(x_i)$.

Proof of Equality of Embedded Values (Common Preimage)

- Consider N group homomorphisms with the same domain G

$$G \to H_i : x \mapsto \phi_i(x).$$

- The prover $\mathcal{P}$ can prove knowledge of x such that $y_i = \phi_i(x)$ using the function

$$G \to H_1 \times \cdots \times H_N : \\ x \mapsto \phi(x) = (\phi_i(x), \ldots, \phi_N(x)).$$

Outline

Wikström/Terelius's Mix-Net Revisited

[**Wik09**] A Commitment-Consistent Proof of a Shuffle

- Offline part: Commit to a permutation matrix and proof that it is indeed a permutation matrix.
- Online part: Shuffle the input batch and give a commitment-consistent proof of a shuffle.

[**TW10**] Proofs of Restricted Shuffles

- Restricting the set of permutations.
- A new proof of a shuffle based on a permutation matrix.

An $N \times N$ - matrix M is a permutation matrix if there is exactly one non-zero element in each row and column and if this non-zero element is equal to one.

Example:

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_3 \\ x_1 \\ x_2 \end{pmatrix}$$

If M_π is a permutation matrix for the permutation π then

$$M_\pi \cdot \bar{x} = \bar{x}' = (x_{\pi(1)}, \ldots, x_{\pi(N)})$$

Theorem (Permutation Matrix) [TW10]
Let $M = (m_{i,j})$ be an $N \times N$ - matrix over $\mathbb{Z}_q$ and $\bar{x} = (x_1, \ldots, x_N)$ be a list of variables. Then M is a permutation matrix if and only if

$$\prod_{i=1}^{N} \langle \bar{m}_i, \bar{x} \rangle = \prod_{i=1}^{N} x_i \quad \text{and} \quad M\bar{1} = \bar{1}$$

m_i denotes the i-th row vector of M and $\langle \bar{m}_i, \bar{x} \rangle = \sum_{j=1}^{N} m_{i,j}\, x_j$ the inner product of $\bar{m}_i$ and $\bar{x}$

Wikström/Terelius's Mix-Net Revisited

Recall the property of a matrix commitment:

$$Com(M, \bar{s})^{\bar{e}} = Com(M\bar{e}, \langle \bar{s}, \bar{e} \rangle)$$

If M is a permutation matrix then $M\bar{e} = \bar{e}' = (e_{\pi(1)}, \ldots, e_{\pi(N)})$ and $Com(M, \bar{s})^{\bar{e}}$ is a publicly computed commitment to the permuted $\bar{e}$ - vector based on the commitment to M.

Proof of Knowledge of Permutation Matrix (offline) 1/2

Common Input: Matrix commitment c_π
Private Input: Permutation matrix M_π and $\bar{s}$ such that $c_\pi = Com(M_\pi, \bar{s})$.

1. $\mathcal{V}$ chooses $\bar{e} \in \mathbb{Z}_q^N$ randomly and hands $\bar{e}$ to $\mathcal{P}$
2. $\mathcal{P}$ computes $v = \langle \bar{1}, \bar{s} \rangle$, $w = \langle \bar{e}, \bar{s} \rangle$ and $\bar{e}' = M_\pi \bar{e}$.
3. $\mathcal{V}$ outputs the result of

$$\Sigma\text{-proof}\left[\begin{matrix} v, w \in \mathbb{Z}_q \\ \bar{e}' \in \mathbb{Z}_q^N \end{matrix} \middle| Com(\bar{1}, v) = {c_\pi}^{\bar{1}} \wedge Com(\bar{e}', w) = {c_\pi}^{\bar{e}} \wedge \prod_{i=1}^{N} e'_i = \prod_{i=1}^{N} e_i \right]$$

Proof of Knowledge of Permutation Matrix (offline) 2/2

The Σ-proof of the proof of knowledge of permutation matrix can be transformed into a generic preimage proof:

$$\mathbb{Z}_q^{2N+3} \to G_q^{N+3} : (v, w, \bar{r}, d, \bar{e}') \mapsto \phi_{offline}(v, w, \bar{r}, d, \bar{e}') = \left(Com(0, v), Com(\bar{e}', w), g^{r_1} c_0^{e'_1}, \ldots, g^{r_N} c_{N-1}^{e'_N}, Com(0, d)\right)$$

With additional private input: Randomness $\bar{r} \in \mathbb{Z}_q^N$ and $d = d_N$ and $d_i = r_i + e'_i d_{i-1}$ for $i = 2, \ldots, N$ with $d_1 = r_1$. $c_i = g^{r_i} c_{i-1}^{e'_i}$ and $c_0 = h$.

Commitment-Consistent Proof of a Shuffle (online) 1/2

Common Input: Permutation matrix commitment c_π and ciphertexts (ElGamal) $u_1, \ldots, u_N, u'_1, \ldots, u'_N \in (G_q \times G_q)$.
Private Input: Permutation π and randomness $\bar{r} \in \mathbb{Z}_q^N$ such that $u'_i = ReEnc(u_{\pi(i)}, r_{\pi(i)})$.

1. $\mathcal{V}$ chooses $\bar{e} \in \mathbb{Z}_q^N$ randomly and hands $\bar{e}$ to $\mathcal{P}$
2. $\mathcal{P}$ computes $w = \langle \bar{e}, \bar{s} \rangle$, $r = \langle \bar{e}, \bar{r} \rangle$ and $\bar{e}' = M_\pi \bar{e}$.
3. $\mathcal{V}$ outputs the result of

$$\Sigma\text{-proof}\left[\begin{array}{c} r, w \in \mathbb{Z}_q \\ \bar{e}' \in \mathbb{Z}_q^N \end{array} \middle| \; Com(\bar{e}', w) = {c_\pi}^{\bar{e}} \wedge \prod_{i=1}^{N} (u'_i)^{e'_i} = ReEnc(\prod_{i=1}^{N} (u_i)^{e_i}, r)\right]$$

Commitment-Consistent Proof of a Shuffle (online) 3/3

The Σ-proof of the proof of knowledge of permutation matrix can be transformed into a generic preimage proof:

$$\mathbb{Z}_q^{N+2} \to G_q^3 : (r, w, \bar{e}') \mapsto \phi_{online}(r, w, \bar{e}') = \left(Com(\bar{e}', w), \prod_{i=1}^{N} (u_i')^{e_i'} Enc(1, -r) \right)$$

Conclusion and Questions