University of Fribourg

Bern University of Applied Sciences

Efficient Coercion-Resistant Remote E-Voting

Oliver Spycher

Darmstadt, December 16th, 2010

Outline

Outline

A Good Voting Scheme

- Accuracy (Casted as intended, tallied as casted)
- Uniqueness and Eligibility
- Verifiability (Individual, Universal, Eligibility)

- Privacy (No link vote - voter)
- Fairness (No premature results)

- Receipt-Freeness (Not enough)
- Coercion-Resistance (Coercion and bribery are infeasible)

A Good Voting Scheme

- Accuracy (Casted as intended, tallied as casted)
- Uniqueness and Eligibility
- Verifiability (Individual, Universal, Eligibility)

- Privacy (No link vote - voter)
- Fairness (No premature results)

- Receipt-Freeness (Not enough)
- Coercion-Resistance (Coercion and bribery are infeasible)

Primitives (1)

IND – CPA Secure El Gamal

Notation / Properties

- $E_e(m, \alpha)$ encryption of message m under randomness α and public key e
- Infeasible to compute m given $E_e(m, \alpha)$
- Easy to compute m as $\mathrm{Dec}_d(\mathrm{E}_e(m, \alpha))$, d private key
- Infeasible to decide $m_1 = m_2$ given $\mathrm{E}_e(m_1, \alpha_1)$, $\mathrm{E}_e(m_2, \alpha_2)$
- Homomorphic Property: $\mathrm{E}_e(m_1) \cdot \mathrm{E}_e(m_2) = \mathrm{E}_e(m_1 \cdot m_2)$

Group Threshold Computation

- Secrets shared among n_A parties
- Computations performed by $t_A > \frac{n_A}{2}$ trusted parties

Primitives (2)

Mix - Nets

- Input: encryptions $(C_1, ..., C_N)$
- Output: mixed re-encryptions $(\hat{C}_{\pi(1)}, ..., \hat{C}_{\pi(N)})$, where $\hat{C}_{\pi(i)} = C_i \cdot \mathrm{E}_e(1, \alpha_i)$ and π, α_i unknown

Non-Interactive Zero-Knowledge Proofs

- All computations that involve exponentiation are justified.
- Example: "*I know* α: $\hat{C} = C \cdot \mathrm{E}_e(1, \alpha)$", i.e. $\mathrm{Dec}_d(\hat{C}) = \mathrm{Dec}_d(C)$

Outline

Setup JCJ

1. Registrars jointly compute public credential S as $\mathrm{E}_e(\sigma, \alpha_S)$
2. Pass shared secret credential σ and designated proof to V

Voter Roll

#	**Voter**	**S**
1	Wolf	$\mathrm{E}_e(\sigma_1)$
2	Dwarf	$\mathrm{E}_e(\sigma_2)$
3	Gretel	$\mathrm{E}_e(\sigma_3)$
4	King	$\mathrm{E}_e(\sigma_4)$
5	Snow White	$\mathrm{E}_e(\sigma_5)$
n	Witch	$\mathrm{E}_e(\sigma_n)$

Cast Votes

V posts to voting board through anonymous channel

1. (**A**) Encryption of secret credential σ: $\mathrm{E}_e(\sigma, \alpha_A)$
2. (**B**) Encryption of vote $c \in \mathcal{C}$: $\mathrm{E}_e(c, \alpha_B)$
3. (**P**) Proofs: $c \in \mathcal{C}$, knowledge of α_B

Voting Board

#	**A**	**B**	**P**
1	$\mathrm{E}_e(\sigma_1)$	$\mathrm{E}_e(c_1)$	...
2	$\mathrm{E}_e(\sigma_2)$	$\mathrm{E}_e(c_2)$	...
3	$\mathrm{E}_e(\sigma_3)$	$\mathrm{E}_e(c_3)$	...
4	$\mathrm{E}_e(\sigma_4)$	$\mathrm{E}_e(c_4)$	...
5	$\mathrm{E}_e(\sigma_5)$	$\mathrm{E}_e(c_5)$	...
N	$\mathrm{E}_e(\sigma_n)$	$\mathrm{E}_e(c_N)$	...

Undermining Coercion

Coercion

- Receipt Based
- Forced Abstention
- Randomization
- Simulation

JCJ Medicine

1. (V claims $\bar{\sigma} \neq \sigma$ to be his secret credential)
2. (V follows coercer's instructions)
3. V secretly casts his real vote using σ

Tallying

To Do:

1. Remove Duplicates

Voting Board

#	**A**	**B**
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Tallying

Voter Roll

#	**V**	**S**
1	Wo	$\mathrm{E}_e(\sigma_1)$
2	Dw	$\mathrm{E}_e(\sigma_2)$
3	Gr	$\mathrm{E}_e(\sigma_3)$
4	Ki	$\mathrm{E}_e(\sigma_4)$
5	SW	$\mathrm{E}_e(\sigma_5)$
n	Wi	$\mathrm{E}_e(\sigma_n)$

To Do:

1. Remove Duplicates
2. Authorize Votes

Voting Board

#	**A**	**B**
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Tallying

Voter Roll

#	**V**	**S**
1	Wo	$\mathrm{E}_e(\sigma_1)$
2	Dw	$\mathrm{E}_e(\sigma_2)$
3	Gr	$\mathrm{E}_e(\sigma_3)$
4	Ki	$\mathrm{E}_e(\sigma_4)$
5	SW	$\mathrm{E}_e(\sigma_5)$
n	Wi	$\mathrm{E}_e(\sigma_n)$

To Do:

1. Remove Duplicates
2. Authorize Votes

$\longrightarrow$ PET

Voting Board

#	**A**	**B**
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

PET - Plaintext Equivalence Test

Given $\mathrm{E}_e(p_1)$, $\mathrm{E}_e(p_2)$, decide whether $p_1 = p_2$, without revealing plaintexts.

Algorithm

1. Compute $\mathrm{E}_e(\frac{p_1}{p_2}) = \frac{\mathrm{E}_e(p_1)}{\mathrm{E}_e(p_2)}$
2. Compute $\mathrm{E}_e((\frac{p_1}{p_2})^z) = \mathrm{E}_e^z(\frac{p_1}{p_2})$, $z \in_R \mathbb{Z}_q$, fresh unknown
3. Compute $(\frac{p_1}{p_2})^z = \mathrm{Dec}_d(\mathrm{E}_e((\frac{p_1}{p_2})^z))$
4. Return *true* if $(\frac{p_1}{p_2})^z = 1$, *false* otherwise.

Remove Duplicates Using PET

$\mathrm{PET}(A_N, A_7) = \mathit{false}$ $\longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_N, A_6) = \mathit{false}$ $\longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_N, A_5) = \mathit{false}$ $\longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_N, A_4) = \mathit{false}$ $\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

$\longrightarrow$

Remove Duplicates Using PET

$\mathrm{PET}(A_N, A_3) = \mathit{false} \longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

$\longrightarrow$

Remove Duplicates Using PET

$\mathrm{PET}(A_N, A_2) = \mathit{false} \longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_N, A_1) = \mathit{false}$ $\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

$\longrightarrow$

Remove Duplicates Using PET

$\mathrm{PET}(A_7, A_6) = \mathit{false}$ $\longrightarrow$ $\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_7, A_5) = \mathit{false}$ $\longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_7, A_4) = \mathit{false}$ $\longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_7, A_3) = \mathit{false} \longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_7, A_2) = \mathit{false} \longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_7, A_1) = \mathit{false} \longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_6, A_5) = \mathit{false}$ $\longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_6, A_4) = \mathit{false} \longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_6, A_3) = \mathit{false} \longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_6, A_2) = \mathit{false} \longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_6, A_1) = \mathit{false} \longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
$\longrightarrow$ 6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_5, A_4) = \mathit{false}$ $\longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_5, A_3) = \mathit{true}$ $\longrightarrow$ $\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
~~3~~	$\mathrm{E}_e(\bar{\sigma}_3)$	~~$\mathrm{E}_e(c_3)$~~
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_5, A_2) = \mathit{false}$ $\longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
~~3~~	$\mathrm{E}_e(\bar{\sigma}_3)$	~~$\mathrm{E}_e(c_3)$~~
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_5, A_1) = \mathit{false}$ ⟶

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$
~~3~~	$\mathrm{E}_e(\bar{\sigma}_3)$	~~$\mathrm{E}_e(c_3)$~~
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
⟶ 5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_4, A_2) = \mathit{true}$ $\longrightarrow$ $\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
~~2~~	$\mathrm{E}_e(\bar{\sigma}_2)$	~~$\mathrm{E}_e(c_2)$~~
~~3~~	$\mathrm{E}_e(\bar{\sigma}_3)$	~~$\mathrm{E}_e(c_3)$~~
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$\mathrm{PET}(A_4, A_1) = \mathit{false}$ $\longrightarrow$

$\longrightarrow$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
~~2~~	$\mathrm{E}_e(\bar{\sigma}_2)$	~~$\mathrm{E}_e(c_2)$~~
~~3~~	$\mathrm{E}_e(\bar{\sigma}_3)$	~~$\mathrm{E}_e(c_3)$~~
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
~~2~~	$\mathrm{E}_e(\bar{\sigma}_2)$	~~$\mathrm{E}_e(c_2)$~~
~~3~~	$\mathrm{E}_e(\bar{\sigma}_3)$	~~$\mathrm{E}_e(c_3)$~~
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Remove Duplicates Using PET

$O(N^2)$

Voting Board

#	A	B
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
~~2~~	$\mathrm{E}_e(\bar{\sigma}_2)$	~~$\mathrm{E}_e(c_2)$~~
~~3~~	$\mathrm{E}_e(\bar{\sigma}_3)$	~~$\mathrm{E}_e(c_3)$~~
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Authorize Votes

Voter Roll

i	V_i	S_i
1	Wo	$E_e(\sigma_1)$
2	Dw	$E_e(\sigma_2)$
3	Gr	$E_e(\sigma_3)$
4	Ki	$E_e(\sigma_4)$
5	SW	$E_e(\sigma_5)$
n	Wi	$E_e(\sigma_n)$

To Do:

1. Remove Duplicates
2. Authorize Votes

Now PET?

Voting Board

i	A_i	B_i
1	$E_e(\bar{\sigma}_1)$	$E_e(c_1)$
~~2~~	$E_e(\bar{\sigma}_2)$	~~$E_e(c_2)$~~
~~3~~	$E_e(\bar{\sigma}_3)$	~~$E_e(c_3)$~~
4	$E_e(\bar{\sigma}_4)$	$E_e(c_4)$
5	$E_e(\bar{\sigma}_5)$	$E_e(c_5)$
6	$E_e(\bar{\sigma}_6)$	$E_e(c_6)$
7	$E_e(\bar{\sigma}_7)$	$E_e(c_7)$
N	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

Authorize Votes

Voter Roll

i	V_i	S_i
1	Wo	$E_e(\sigma_1)$
2	Dw	$E_e(\sigma_2)$
3	Gr	$E_e(\sigma_3)$
4	Ki	$E_e(\sigma_4)$
5	SW	$E_e(\sigma_5)$
n	Wi	$E_e(\sigma_n)$

To Do:

1. Remove Duplicates
2. Authorize Votes

Now PET?

→ Mix first.

Voting Board

i	A_i	B_i
1	$E_e(\bar{\sigma}_1)$	$E_e(c_1)$
~~2~~	$E_e(\bar{\sigma}_2)$	~~$E_e(c_2)$~~
~~3~~	$E_e(\bar{\sigma}_3)$	~~$E_e(c_3)$~~
4	$E_e(\bar{\sigma}_4)$	$E_e(c_4)$
5	$E_e(\bar{\sigma}_5)$	$E_e(c_5)$
6	$E_e(\bar{\sigma}_6)$	$E_e(c_6)$
7	$E_e(\bar{\sigma}_7)$	$E_e(c_7)$
N	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\longleftarrow$ $\mathrm{PET}(\hat{A}_1, \hat{S}_1) = \mathit{false}$ $\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
1	$\hat{E}_e(\bar{\sigma}_1)$	$\hat{E}_e(c_1)$
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\leftarrow$

$\text{PET}(\hat{A}_1, \hat{S}_2) = \mathit{false}$ $\rightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
1	$\hat{E}_e(\bar{\sigma}_1)$	$\hat{E}_e(c_1)$
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\leftarrow$

$\text{PET}(\hat{A}_1, \hat{S}_3) = \mathit{false}$ $\rightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
1	$\hat{E}_e(\bar{\sigma}_1)$	$\hat{E}_e(c_1)$
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\leftarrow$

$\text{PET}(\hat{A}_1, \hat{S}_4) = \mathit{false}$ $\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
1	$\hat{E}_e(\bar{\sigma}_1)$	$\hat{E}_e(c_1)$
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\leftarrow$

$\text{PET}(\hat{A}_1, \hat{S}_5) = \mathit{false}$ $\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
1	$\hat{E}_e(\bar{\sigma}_1)$	$\hat{E}_e(c_1)$
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\leftarrow$

$\text{PET}(\hat{A}_1, \hat{S}_n) = \mathit{false}$ $\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
1	$\hat{E}_e(\bar{\sigma}_1)$	$\hat{E}_e(c_1)$
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\leftarrow$

$\text{PET}(\hat{A}_1, \hat{S}_1) = \textit{false}$

$\rightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
~~2~~	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\longleftarrow$ $\mathrm{PET}(\hat{A}_1, \hat{S}_2) = \mathit{true}$ $\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
~~2~~	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\leftarrow$

$\mathrm{PET}(\hat{A}_3, \hat{S}_1) = \mathit{false}$ $\rightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
~~2~~	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\longleftarrow$ $\mathrm{PET}(\hat{A}_3, \hat{S}_3) = \mathit{false}$ $\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
~~2~~	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\leftarrow$

$\text{PET}(\hat{A}_3, \hat{S}_4) = \textit{true}$ $\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
~~2~~	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
~~4~~	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\leftarrow$

$\mathrm{PET}(\hat{A}_4, \hat{S}_1) = \mathit{false}$ $\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
~~2~~	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\longleftarrow$

$\text{PET}(\hat{A}_4, \hat{S}_3) = \mathit{false}$ $\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
~~2~~	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
~~4~~	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\leftarrow$

$\mathrm{PET}(\hat{A}_4, \hat{S}_5) = \mathit{false}$ $\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
~~2~~	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
~~4~~	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
~~n~~	$\hat{E}_e(\sigma_n)$

$\leftarrow$

$\mathrm{PET}(\hat{A}_4, \hat{S}_n) = \mathit{true}$ $\rightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
~~2~~	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
~~4~~	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
~~n~~	$\hat{E}_e(\sigma_n)$

$\leftarrow$

$\mathrm{PET}(\hat{A}_5, \hat{S}_1) = \mathit{false}$ $\rightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
~~2~~	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
~~4~~	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
~~n~~	$\hat{E}_e(\sigma_n)$

$\longleftarrow$

$\mathrm{PET}(\hat{A}_5, \hat{S}_3) = \mathit{false}$ $\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
~~2~~	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
~~4~~	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
~~n~~	$\hat{E}_e(\sigma_n)$

$\longleftarrow$ $\mathrm{PET}(\hat{A}_5, \hat{S}_5) = \mathit{false}$ $\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
~~5~~	$\hat{E}_e(\bar{\sigma}_5)$	~~$\hat{E}_e(c_5)$~~
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

$\mathbf{i}$	$\hat{\mathbf{S}}_\mathbf{i}$
~~1~~	$\hat{\mathrm{E}}_e(\sigma_1)$
~~2~~	$\hat{\mathrm{E}}_e(\sigma_2)$
3	$\hat{\mathrm{E}}_e(\sigma_3)$
~~4~~	$\hat{\mathrm{E}}_e(\sigma_4)$
5	$\hat{\mathrm{E}}_e(\sigma_5)$
~~n~~	$\hat{\mathrm{E}}_e(\sigma_n)$

$\leftarrow$

$\mathrm{PET}(\hat{A}_N, \hat{S}_1) = \mathit{true}$ $\rightarrow$

(Voting Board)

$\mathbf{j}$	$\hat{\mathbf{A}}_\mathbf{j}$	$\hat{\mathbf{B}}_\mathbf{j}$
~~1~~	$\hat{\mathrm{E}}_e(\bar{\sigma}_1)$	~~$\hat{\mathrm{E}}_e(c_1)$~~
2	$\hat{\mathrm{E}}_e(\bar{\sigma}_2)$	$\hat{\mathrm{E}}_e(c_2)$
3	$\hat{\mathrm{E}}_e(\bar{\sigma}_3)$	$\hat{\mathrm{E}}_e(c_3)$
4	$\hat{\mathrm{E}}_e(\bar{\sigma}_4)$	$\hat{\mathrm{E}}_e(c_4)$
~~5~~	$\hat{\mathrm{E}}_e(\bar{\sigma}_5)$	~~$\hat{\mathrm{E}}_e(c_5)$~~
N	$\hat{\mathrm{E}}_e(\bar{\sigma}_N)$	$\hat{\mathrm{E}}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
~~1~~	$\hat{E}_e(\sigma_1)$
~~2~~	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
~~4~~	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
~~n~~	$\hat{E}_e(\sigma_n)$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
~~5~~	$\hat{E}_e(\bar{\sigma}_5)$	~~$\hat{E}_e(c_5)$~~
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (2)

Imagine these values mixed.

(Voter Roll)

i	$\hat{S}_i$
~~1~~	$\hat{E}_e(\sigma_1)$
~~2~~	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
~~4~~	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
~~n~~	$\hat{E}_e(\sigma_n)$

$O(n \cdot N)$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
~~5~~	$\hat{E}_e(\bar{\sigma}_5)$	~~$\hat{E}_e(c_5)$~~
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Outline

Solutions

Smith / Weber

Employs different PET mechanism

Not coercion resistant, as it turned out

Solutions

Smith / Weber

Employs different PET mechanism

Not coercion resistant, as it turned out

Araujo et al.

Based on group-signatures

No verifiability of eligibility

Requires channel from authorities to voters prior to every vote

Solutions

Smith / Weber

Employs different PET mechanism

Not coercion resistant, as it turned out

Araujo et al.

Based on group-signatures

No verifiability of eligibility

Requires channel from authorities to voters prior to every vote

SKHS

Strongly based on JCJ, same assumptions

Combines approach by Smith / Weber with original PET

PET - The Smith / Weber Flavour

Given $\mathrm{E}_e(p_1)$, $\mathrm{E}_e(p_2)$, decide whether $p_1 = p_2$, without revealing plaintexts.

Algorithm

1. Compute $\mathrm{E}_e^z(p_1)$, $\mathrm{E}_e^z(p_2)$, $z \in_R \mathbb{Z}_q$ unknown
2. Compute $p_1^z = \mathrm{Dec}_d(\mathrm{E}_e^z(p_1))$, $p_2^z = \mathrm{Dec}_d(\mathrm{E}_e^z(p_2))$
3. Return *true* if $p_1^z = p_2^z$, *false* otherwise.

Remove Duplicates

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\bar{\sigma}_i{}^z$

Voting Board

i	A_i	B_i
1	$E_e(\bar{\sigma}_1)$	$E_e(c_1)$
2	$E_e(\bar{\sigma}_2)$	$E_e(c_2)$
3	$E_e(\bar{\sigma}_3)$	$E_e(c_3)$
4	$E_e(\bar{\sigma}_4)$	$E_e(c_4)$
5	$E_e(\bar{\sigma}_5)$	$E_e(c_5)$
6	$E_e(\bar{\sigma}_6)$	$E_e(c_6)$
7	$E_e(\bar{\sigma}_7)$	$E_e(c_7)$
N	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

Remove Duplicates

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\bar{\sigma}_i{}^z$
$\bar{\sigma}_N{}^z$

$\leftarrow$

Voting Board

i	A_i	B_i
1	$E_e(\bar{\sigma}_1)$	$E_e(c_1)$
2	$E_e(\bar{\sigma}_2)$	$E_e(c_2)$
3	$E_e(\bar{\sigma}_3)$	$E_e(c_3)$
4	$E_e(\bar{\sigma}_4)$	$E_e(c_4)$
5	$E_e(\bar{\sigma}_5)$	$E_e(c_5)$
6	$E_e(\bar{\sigma}_6)$	$E_e(c_6)$
7	$E_e(\bar{\sigma}_7)$	$E_e(c_7)$
N	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$\bar{\sigma}_N{}^z \longrightarrow$

Remove Duplicates

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\bar{\sigma}_i{}^z$
$\bar{\sigma}_N{}^z$
$\bar{\sigma}_7{}^z$

$\leftarrow$

Voting Board

$\bar{\sigma}_7{}^z \longrightarrow$

i	A_i	B_i
1	$E_e(\bar{\sigma}_1)$	$E_e(c_1)$
2	$E_e(\bar{\sigma}_2)$	$E_e(c_2)$
3	$E_e(\bar{\sigma}_3)$	$E_e(c_3)$
4	$E_e(\bar{\sigma}_4)$	$E_e(c_4)$
5	$E_e(\bar{\sigma}_5)$	$E_e(c_5)$
6	$E_e(\bar{\sigma}_6)$	$E_e(c_6)$
7	$E_e(\bar{\sigma}_7)$	$E_e(c_7)$
N	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

Remove Duplicates

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\bar{\sigma}_i{}^z$
$\bar{\sigma}_N{}^z$
$\bar{\sigma}_7{}^z$
$\bar{\sigma}_6{}^z$

$\leftarrow$

$\bar{\sigma}_6{}^z \longrightarrow$

Voting Board

i	A_i	B_i
1	$E_e(\bar{\sigma}_1)$	$E_e(c_1)$
2	$E_e(\bar{\sigma}_2)$	$E_e(c_2)$
3	$E_e(\bar{\sigma}_3)$	$E_e(c_3)$
4	$E_e(\bar{\sigma}_4)$	$E_e(c_4)$
5	$E_e(\bar{\sigma}_5)$	$E_e(c_5)$
6	$E_e(\bar{\sigma}_6)$	$E_e(c_6)$
7	$E_e(\bar{\sigma}_7)$	$E_e(c_7)$
N	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

Remove Duplicates

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\bar{\sigma}_i{}^z$
$\bar{\sigma}_N{}^z$
$\bar{\sigma}_7{}^z$
$\bar{\sigma}_6{}^z$
$\bar{\sigma}_5{}^z$

$\leftarrow$

$\bar{\sigma}_5{}^z \longrightarrow$

Voting Board

i	A_i	B_i
1	$E_e(\bar{\sigma}_1)$	$E_e(c_1)$
2	$E_e(\bar{\sigma}_2)$	$E_e(c_2)$
3	$E_e(\bar{\sigma}_3)$	$E_e(c_3)$
4	$E_e(\bar{\sigma}_4)$	$E_e(c_4)$
5	$E_e(\bar{\sigma}_5)$	$E_e(c_5)$
6	$E_e(\bar{\sigma}_6)$	$E_e(c_6)$
7	$E_e(\bar{\sigma}_7)$	$E_e(c_7)$
N	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

Remove Duplicates

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\bar{\sigma}_i{}^z$
$\bar{\sigma}_N{}^z$
$\bar{\sigma}_7{}^z$
$\bar{\sigma}_6{}^z$
$\bar{\sigma}_5{}^z$
$\bar{\sigma}_4{}^z$

$\leftarrow$

$\bar{\sigma}_4{}^z \longrightarrow$

Voting Board

i	A_i	B_i
1	$E_e(\bar{\sigma}_1)$	$E_e(c_1)$
2	$E_e(\bar{\sigma}_2)$	$E_e(c_2)$
3	$E_e(\bar{\sigma}_3)$	$E_e(c_3)$
4	$E_e(\bar{\sigma}_4)$	$E_e(c_4)$
5	$E_e(\bar{\sigma}_5)$	$E_e(c_5)$
6	$E_e(\bar{\sigma}_6)$	$E_e(c_6)$
7	$E_e(\bar{\sigma}_7)$	$E_e(c_7)$
N	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

Remove Duplicates

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\bar{\sigma}_i{}^z$
$\bar{\sigma}_N{}^z$
$\bar{\sigma}_7{}^z$
$\bar{\sigma}_6{}^z$
$\bar{\sigma}_5{}^z$
$\bar{\sigma}_4{}^z$

$\leftarrow$

$\bar{\sigma}_3{}^z \longrightarrow$

Voting Board

i	A_i	B_i
1	$E_e(\bar{\sigma}_1)$	$E_e(c_1)$
2	$E_e(\bar{\sigma}_2)$	$E_e(c_2)$
~~3~~	$E_e(\bar{\sigma}_3)$	~~$E_e(c_3)$~~
4	$E_e(\bar{\sigma}_4)$	$E_e(c_4)$
5	$E_e(\bar{\sigma}_5)$	$E_e(c_5)$
6	$E_e(\bar{\sigma}_6)$	$E_e(c_6)$
7	$E_e(\bar{\sigma}_7)$	$E_e(c_7)$
N	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

Remove Duplicates

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\bar{\sigma}_i{}^z$
$\bar{\sigma}_N{}^z$
$\bar{\sigma}_7{}^z$
$\bar{\sigma}_6{}^z$
$\bar{\sigma}_5{}^z$
$\bar{\sigma}_4{}^z$

$\leftarrow$

$\bar{\sigma}_2{}^z \longrightarrow$

Voting Board

i	A_i	B_i
1	$E_e(\bar{\sigma}_1)$	$E_e(c_1)$
~~2~~	$E_e(\bar{\sigma}_2)$	~~$E_e(c_2)$~~
~~3~~	$E_e(\bar{\sigma}_3)$	~~$E_e(c_3)$~~
4	$E_e(\bar{\sigma}_4)$	$E_e(c_4)$
5	$E_e(\bar{\sigma}_5)$	$E_e(c_5)$
6	$E_e(\bar{\sigma}_6)$	$E_e(c_6)$
7	$E_e(\bar{\sigma}_7)$	$E_e(c_7)$
N	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

Remove Duplicates

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\bar{\sigma}_i{}^z$
$\bar{\sigma}_N{}^z$
$\bar{\sigma}_7{}^z$
$\bar{\sigma}_6{}^z$
$\bar{\sigma}_5{}^z$
$\bar{\sigma}_4{}^z$
$\bar{\sigma}_1{}^z$

$\leftarrow$

$\bar{\sigma}_1{}^z \longrightarrow$

Voting Board

i	A_i	B_i
1	$E_e(\bar{\sigma}_1)$	$E_e(c_1)$
~~2~~	$E_e(\bar{\sigma}_2)$	~~$E_e(c_2)$~~
~~3~~	$E_e(\bar{\sigma}_3)$	~~$E_e(c_3)$~~
4	$E_e(\bar{\sigma}_4)$	$E_e(c_4)$
5	$E_e(\bar{\sigma}_5)$	$E_e(c_5)$
6	$E_e(\bar{\sigma}_6)$	$E_e(c_6)$
7	$E_e(\bar{\sigma}_7)$	$E_e(c_7)$
N	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

Authorize Votes (1)

Voter Roll

i	V_i	S_i
1	Wo	$\mathrm{E}_e(\sigma_1)$
2	Dw	$\mathrm{E}_e(\sigma_2)$
3	Gr	$\mathrm{E}_e(\sigma_3)$
4	Ki	$\mathrm{E}_e(\sigma_4)$
5	SW	$\mathrm{E}_e(\sigma_5)$
n	Wi	$\mathrm{E}_e(\sigma_n)$

To Do:

1. Remove Duplicates
2. Authorize Votes

Now S/W PET?

Voting Board

i	A_i	B_i
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
~~2~~	$\mathrm{E}_e(\bar{\sigma}_2)$	~~$\mathrm{E}_e(c_2)$~~
~~3~~	$\mathrm{E}_e(\bar{\sigma}_3)$	~~$\mathrm{E}_e(c_3)$~~
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Authorize Votes (1)

Voter Roll

i	V_i	S_i
1	Wo	$\mathrm{E}_e(\sigma_1)$
2	Dw	$\mathrm{E}_e(\sigma_2)$
3	Gr	$\mathrm{E}_e(\sigma_3)$
4	Ki	$\mathrm{E}_e(\sigma_4)$
5	SW	$\mathrm{E}_e(\sigma_5)$
n	Wi	$\mathrm{E}_e(\sigma_n)$

To Do:

1. Remove Duplicates
2. Authorize Votes

Now S/W PET?

$\longrightarrow$ Mix.

Voting Board

i	A_i	B_i
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$
~~2~~	$\mathrm{E}_e(\bar{\sigma}_2)$	~~$\mathrm{E}_e(c_2)$~~
~~3~~	$\mathrm{E}_e(\bar{\sigma}_3)$	~~$\mathrm{E}_e(c_3)$~~
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$

Authorize Votes (2)

Imagine the voter roll mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

Lookup

$\sigma_i{}^z$

Authorize Votes (2)

Imagine the voter roll mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\longleftarrow \sigma_1{}^z$

Lookup

$\longrightarrow$

$\sigma_i{}^z$
$\sigma_1{}^z$

Authorize Votes (2)

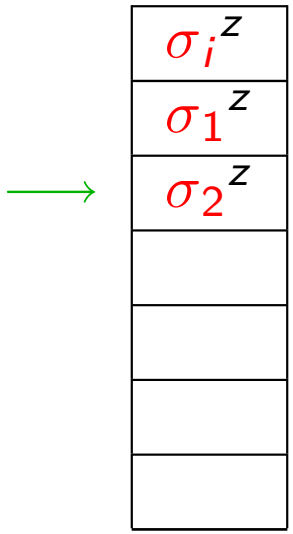
Imagine the voter roll mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\longleftarrow {\sigma_2}^z$

Lookup



Authorize Votes (2)

Imagine the voter roll mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\longleftarrow \sigma_3{}^z$

$\longrightarrow$

Lookup

$\sigma_i{}^z$
$\sigma_1{}^z$
$\sigma_2{}^z$
$\sigma_3{}^z$

Authorize Votes (2)

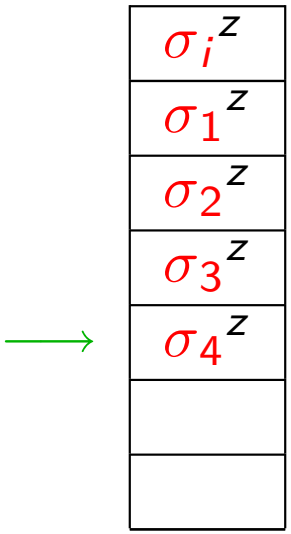
Imagine the voter roll mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\longleftarrow \sigma_4{}^z$

Lookup



Authorize Votes (2)

Imagine the voter roll mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\longleftarrow {\sigma_5}^z$

Lookup

${\sigma_i}^z$
${\sigma_1}^z$
${\sigma_2}^z$
${\sigma_3}^z$
${\sigma_4}^z$
${\sigma_5}^z$

$\longrightarrow$

Authorize Votes (2)

Imagine the voter roll mixed.

(Voter Roll)

i	$\hat{S}_i$
1	$\hat{E}_e(\sigma_1)$
2	$\hat{E}_e(\sigma_2)$
3	$\hat{E}_e(\sigma_3)$
4	$\hat{E}_e(\sigma_4)$
5	$\hat{E}_e(\sigma_5)$
n	$\hat{E}_e(\sigma_n)$

$\longleftarrow \sigma_n{}^z$

Lookup

$\sigma_i{}^z$
$\sigma_1{}^z$
$\sigma_2{}^z$
$\sigma_3{}^z$
$\sigma_4{}^z$
$\sigma_5{}^z$
$\sigma_n{}^z$

$\longrightarrow$

Authorize Votes (3)

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\sigma_i{}^z$
$\sigma_1{}^z$
$\sigma_2{}^z$
$\sigma_3{}^z$
$\sigma_4{}^z$
$\sigma_5{}^z$
$\sigma_n{}^z$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
1	$\hat{E}_e(\bar{\sigma}_1)$	$\hat{E}_e(c_1)$
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (3)

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\sigma_i{}^z$
$\sigma_1{}^z$
$\sigma_2{}^z$
$\sigma_3{}^z$
$\sigma_4{}^z$
$\sigma_5{}^z$
$\sigma_n{}^z$

$\longleftarrow$

$\longrightarrow$ (Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (3)

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\sigma_i{}^z$
$\sigma_1{}^z$
$\sigma_2{}^z$
$\sigma_3{}^z$
$\sigma_4{}^z$
$\sigma_5{}^z$
$\sigma_n{}^z$

$\longleftarrow$ $\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (3)

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\sigma_i{}^z$
$\sigma_1{}^z$
$\sigma_2{}^z$
$\sigma_3{}^z$
$\sigma_4{}^z$
$\sigma_5{}^z$
$\sigma_n{}^z$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (3)

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\sigma_i{}^z$
$\sigma_1{}^z$
$\sigma_2{}^z$
$\sigma_3{}^z$
$\sigma_4{}^z$
$\sigma_5{}^z$
$\sigma_n{}^z$

$\leftarrow$

$\rightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
5	$\hat{E}_e(\bar{\sigma}_5)$	$\hat{E}_e(c_5)$
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (3)

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\sigma_i{}^z$
$\sigma_1{}^z$
$\sigma_2{}^z$
$\sigma_3{}^z$
$\sigma_4{}^z$
$\sigma_5{}^z$
$\sigma_n{}^z$

$\longleftarrow$

$\longrightarrow$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
~~5~~	$\hat{E}_e(\bar{\sigma}_5)$	~~$\hat{E}_e(c_5)$~~
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Authorize Votes (3)

Use a lookup table to perform PET over multiple encryptions.

Lookup

$\sigma_i{}^z$
$\sigma_1{}^z$
$\sigma_2{}^z$
$\sigma_3{}^z$
$\sigma_4{}^z$
$\sigma_5{}^z$
$\sigma_n{}^z$

(Voting Board)

j	$\hat{A}_j$	$\hat{B}_j$
~~1~~	$\hat{E}_e(\bar{\sigma}_1)$	~~$\hat{E}_e(c_1)$~~
2	$\hat{E}_e(\bar{\sigma}_2)$	$\hat{E}_e(c_2)$
3	$\hat{E}_e(\bar{\sigma}_3)$	$\hat{E}_e(c_3)$
4	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$
~~5~~	$\hat{E}_e(\bar{\sigma}_5)$	~~$\hat{E}_e(c_5)$~~
N	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

Where does Smith/Weber fail?

SKHS - Basics

Vote Casting

Associate vote (A, B) with voter roll entry S_i

Tallying

Remove duplicates as per Smith/Weber

Authorize votes by performing PET over A and only S_i

Cast Votes - Naive

1. (**A**) Encryption of secret credential σ: $\mathrm{E}_e(\sigma, \alpha_B)$
2. (**I**) Index of V's entry in voter roll

Voting Board

#	**A**	**B**	**P**	**I**
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$	...	5
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$	...	2
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$	...	$> n$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$	...	2
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$	...	$> n$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$	...	n
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$	...	5
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$	...	1

Cast Votes

1. (**A**) Encryption of secret credential σ: $\mathrm{E}_e(\sigma, \alpha_B)$
2. (**I**) Encrypted index of V's entry in voter roll

Voting Board

#	**A**	**B**	**P**	**I**
1	$\mathrm{E}_e(\bar{\sigma}_1)$	$\mathrm{E}_e(c_1)$	...	$\mathrm{E}_e(5)$
2	$\mathrm{E}_e(\bar{\sigma}_2)$	$\mathrm{E}_e(c_2)$	...	$\mathrm{E}_e(2)$
3	$\mathrm{E}_e(\bar{\sigma}_3)$	$\mathrm{E}_e(c_3)$	...	$\mathrm{E}_e(> n)$
4	$\mathrm{E}_e(\bar{\sigma}_4)$	$\mathrm{E}_e(c_4)$	...	$\mathrm{E}_e(2)$
5	$\mathrm{E}_e(\bar{\sigma}_5)$	$\mathrm{E}_e(c_5)$	...	$\mathrm{E}_e(> n)$
6	$\mathrm{E}_e(\bar{\sigma}_6)$	$\mathrm{E}_e(c_6)$	...	$\mathrm{E}_e(n)$
7	$\mathrm{E}_e(\bar{\sigma}_7)$	$\mathrm{E}_e(c_7)$	...	$\mathrm{E}_e(5)$
N	$\mathrm{E}_e(\bar{\sigma}_N)$	$\mathrm{E}_e(c_N)$	...	$\mathrm{E}_e(1)$

Tallying - Naive (1)

1. Remove duplicates as per Smith/Weber
2. Mix voting board
3. Decrypt voting board indices **I**
4.
5.

Tallying - Naive (2)

Voter Roll with Associated Votes

i	Voter	S	$\hat{\mathbf{A}}_1$	$\hat{\mathbf{B}}_1$	$\hat{\mathbf{A}}_2$	$\hat{\mathbf{B}}_2$	$\hat{\mathbf{A}}_3$
1	Wolf	$\mathrm{E}_e(\sigma_1)$	$\hat{\mathrm{E}}_e(\bar{\sigma}_N)$	$\hat{\mathrm{E}}_e(c_N)$			
2	Dwarf	$\hat{\mathrm{E}}_e(\sigma_2)$	$\hat{\mathrm{E}}_e(\bar{\sigma}_4)$	$\hat{\mathrm{E}}_e(c_4)$			
3	Gretel	$\hat{\mathrm{E}}_e(\sigma_3)$					
4	King	$\hat{\mathrm{E}}_e(\sigma_4)$					
5	Snow White	$\hat{\mathrm{E}}_e(\sigma_5)$	$\hat{\mathrm{E}}_e(\bar{\sigma}_7)$	$\hat{\mathrm{E}}_e(c_7)$	$\hat{\mathrm{E}}_e(\bar{\sigma}_1)$	$\hat{\mathrm{E}}_e(c_1)$	
n	Witch	$\hat{\mathrm{E}}_e(\sigma_n)$	$\hat{\mathrm{E}}_e(\bar{\sigma}_6)$	$\hat{\mathrm{E}}_e(c_6)$			

Tallying - Naive (3)

1. Remove duplicates as per Smith/Weber
2. Mix voting board
3. Decrypt voting board indices I
4. Mix tuples $(\mathbf{S}, \hat{\mathbf{A}}, \hat{\mathbf{B}}) \rightarrow (\hat{\mathbf{S}}, \hat{\hat{\mathbf{A}}}, \hat{\hat{\mathbf{B}}})$
5. Perform PET over tuples $(\hat{\mathbf{S}}, \hat{\hat{\mathbf{A}}})$ to authorize votes

Is this as secure as JCJ?

Tallying (1)

1. Authorities simulate a random number X_i of votes associated with V_i
2. Remove duplicates as per Smith/Weber
3. Mix voting board
4. Decrypt voting board indices $\mathbf{I}$
5. Mix tuples $(\mathbf{S}, \hat{\mathbf{A}}, \hat{\mathbf{B}}) \rightarrow (\hat{\mathbf{S}}, \hat{\hat{\mathbf{A}}}, \hat{\hat{\mathbf{B}}})$
6. Perform PET over tuples $(\hat{\mathbf{S}}, \hat{\hat{\mathbf{A}}})$ to authorize votes

Tallying (2)

1. Trusted authority simulates a random number X_i of votes associated with V_i
2. Remove duplicates as per Smith/Weber
3. Mix voting board
4. Decrypt voting board indices $\mathbf{I}$
5. Mix tuples $(\mathbf{S}, \hat{\mathbf{A}}, \hat{\mathbf{B}}) \rightarrow (\hat{\mathbf{S}}, \hat{\hat{\mathbf{A}}}, \hat{\hat{\mathbf{B}}})$
6. Perform PET over tuples $(\hat{\mathbf{S}}, \hat{\hat{\mathbf{A}}})$ to authorize votes

$\longrightarrow \mathbb{O}(N + n)$

Thank You

Questions / Remarks

Find
"*A New Approach Towards Coercion-Resistant Remote E-Voting in Linear Time*" by Spycher, Koenig, Haenni, and Schläpfer in

www.e-voting.bfh.ch