

University of Fribourg
Bern University of Applied Sciences

Efficient Coercion-Resistant Remote E-Voting

Oliver Spycher

Münchenwiler, November 17th, 2010

Outline

Introduction

JCJ - A Highly Coercion Resistant Protocol

Coercion Resistance in Linear Time

Smith / Weber

SKHS

Outline

Introduction

JCJ - A Highly Coercion Resistant Protocol

Coercion Resistance in Linear Time

Smith / Weber

SKHS

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 $E_e(m, \alpha)$ and e
- ▶ Easy to compute m as $\text{Dec}_d(E_e(m, \alpha))$, d private key
- ▶ Infeasible to decide $m_1 = m_2$ given $E_e(m_1, \alpha_1)$, $E_e(m_2, \alpha_2)$, e
- ▶ Homomorphic Property: $E_e(m_1) \cdot E_e(m_2) = E_e(m_1 \cdot m_2)$

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, \dots, C_N)
- ▶ Output: mixed re-encryptions $(\hat{C}_{\pi(1)}, \dots, \hat{C}_{\pi(N)})$, where $\hat{C}_{\pi(i)} = C_i \cdot E_e(1, \alpha_i)$ and π, α_i unknown

Non-Interactive Zero-Knowledge Proofs

- ▶ All computations that involve exponentiation are justified.
- ▶ Example: “I know α : $\hat{C} = C \cdot E_e(1, \alpha)$ ”, i.e.
 $Dec_d(\hat{C}) = Dec_d(C)$

Outline

Introduction

JCJ - A Highly Coercion Resistant Protocol

Coercion Resistance in Linear Time

Smith / Weber

SKHS

Setup JCJ

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

Voter Roll

#	Voter	S
1	Wolf	$E_e(\sigma_1)$
2	Dwarf	$E_e(\sigma_2)$
3	Gretel	$E_e(\sigma_3)$
4	King	$E_e(\sigma_4)$
5	Snow White	$E_e(\sigma_5)$
n	Witch	$E_e(\sigma_n)$

Cast Votes

V posts to voting board through anonymous channel

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

Voting Board

#	A	B	P
1	$E_e(\sigma_1)$	$E_e(c_1)$...
2	$E_e(\sigma_2)$	$E_e(c_2)$...
3	$E_e(\sigma_3)$	$E_e(c_3)$...
4	$E_e(\sigma_4)$	$E_e(c_4)$...
5	$E_e(\sigma_5)$	$E_e(c_5)$...
N	$E_e(\sigma_n)$	$E_e(c_N)$...

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	$E_e(\bar{\sigma}_1)$	$E_e(c_1)$
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

Tallying

Voter Roll

#	V	S
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

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

Tallying

Voter Roll

#	V	S
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

→ **PET**

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

PET - Plaintext Equivalence Test

Given $E_e(p_1)$, $E_e(p_2)$, decide whether $p_1 = p_2$, without revealing plaintexts.

Algorithm

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

Remove Duplicates Using PET

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$$\text{PET}(A_N, A_7) = \textit{false} \begin{array}{l} \longrightarrow \\ \longrightarrow \end{array}$$

Remove Duplicates Using PET

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$PET(A_N, A_6) = false$ →



Remove Duplicates Using PET

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$PET(A_N, A_5) = false \rightarrow$



Remove Duplicates Using PET

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$PET(A_N, A_4) = false \rightarrow$



Remove Duplicates Using PET

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$PET(A_N, A_3) = false \rightarrow$



Remove Duplicates Using PET

$PET(A_N, A_2) = false \rightarrow$

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

\rightarrow

Remove Duplicates Using PET

$PET(A_N, A_1) = false \rightarrow$

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

\rightarrow

Remove Duplicates Using PET

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$PET(A_7, A_6) = false$ \rightarrow



Remove Duplicates Using PET

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$PET(A_7, A_5) = false \rightarrow$



Remove Duplicates Using PET

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$PET(A_7, A_4) = false$ →



Remove Duplicates Using PET

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$PET(A_7, A_3) = false \rightarrow$



Remove Duplicates Using PET

$PET(A_7, A_2) = false \rightarrow$

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

\rightarrow

Remove Duplicates Using PET

$\text{PET}(A_7, A_1) = \text{false}$ \rightarrow

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

\rightarrow

Remove Duplicates Using PET

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$PET(A_6, A_5) = false$ \rightarrow



Remove Duplicates Using PET

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$PET(A_6, A_4) = false$ →



Remove Duplicates Using PET

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$PET(A_6, A_3) = false \rightarrow$



Remove Duplicates Using PET

$PET(A_6, A_2) = false \rightarrow$

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

\rightarrow

Remove Duplicates Using PET



$PET(A_6, A_1) = false \rightarrow$

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

\rightarrow

Remove Duplicates Using PET

$\text{PET}(A_5, A_4) = \text{false}$  

Voting Board

#	A	B
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 Using PET

$PET(A_5, A_3) = true$ →

→

Voting Board

#	A	B
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 Using PET

$PET(A_5, A_2) = false \rightarrow$

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

\rightarrow

Remove Duplicates Using PET

$PET(A_5, A_1) = false \rightarrow$

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

\rightarrow

Remove Duplicates Using PET

$PET(A_4, A_2) = true \rightarrow$

\rightarrow

Voting Board

#	A	B
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 Using PET

$PET(A_4, A_1) = false$ →

→

Voting Board

#	A	B
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 Using PET

Voting Board

#	A	B
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 Using PET

Voting Board

#	A	B
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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$O(N^2)$

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	$\hat{E}_e(\sigma_n)$

\leftarrow $\text{PET}(\hat{A}_1, \hat{S}_1) = \text{false}$ \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	$\hat{E}_e(\sigma_n)$

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



(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	$\hat{E}_e(\sigma_n)$

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

(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	$\hat{E}_e(\sigma_n)$

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

(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	$\hat{E}_e(\sigma_n)$

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

(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	$\hat{E}_e(\sigma_n)$

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

(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	$\hat{E}_e(\sigma_n)$



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

(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	$\hat{E}_e(\sigma_n)$



$$\text{PET}(\hat{A}_1, \hat{S}_2) = \text{true}$$



(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	$\hat{E}_e(\sigma_n)$



$$\text{PET}(\hat{A}_3, \hat{S}_1) = \textit{false} \quad \longrightarrow$$

(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	$\hat{E}_e(\sigma_n)$

← $\text{PET}(\hat{A}_3, \hat{S}_3) = \text{false}$ →

(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	$\hat{E}_e(\sigma_n)$

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

(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	$\hat{E}_e(\sigma_n)$



(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	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

$$\text{PET}(\hat{A}_4, \hat{S}_1) = \textit{false} \quad \rightarrow$$



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	$\hat{E}_e(\sigma_n)$



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

(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	$\hat{E}_e(\sigma_n)$



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

(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	$\hat{E}_e(\sigma_5)$
$\#$	$\hat{E}_e(\sigma_n)$



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

(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	$\hat{E}_e(\sigma_5)$
$\#$	$\hat{E}_e(\sigma_n)$



(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	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

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

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	$\hat{E}_e(\sigma_5)$
$\#$	$\hat{E}_e(\sigma_n)$



$$\text{PET}(\hat{A}_5, \hat{S}_3) = \text{false} \rightarrow$$

(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	$\hat{E}_e(\sigma_5)$
$\#$	$\hat{E}_e(\sigma_n)$



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



(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	$\hat{E}_e(\sigma_5)$
$\#$	$\hat{E}_e(\sigma_n)$



(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	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$

$$\text{PET}(\hat{A}_N, \hat{S}_1) = \text{true} \longrightarrow$$

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	$\hat{E}_e(\sigma_5)$
$\#$	$\hat{E}_e(\sigma_n)$

(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	$\hat{E}_e(\sigma_5)$
$\#$	$\hat{E}_e(\sigma_n)$

$O(n \cdot N)$

(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

Introduction

JCJ - A Highly Coercion Resistant Protocol

Coercion Resistance in Linear Time

Smith / Weber

SKHS

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 $E_e(p_1)$, $E_e(p_2)$, decide whether $p_1 = p_2$, without revealing plaintexts.

Algorithm

1. Compute $E_e^z(p_1)$, $E_e^z(p_2)$, $z \in_R \mathbb{Z}_q$ unknown
2. Compute $p_1^z = \text{Dec}_d(E_e^z(p_1))$, $p_2^z = \text{Dec}_d(E_e^z(p_2))$
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

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



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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

$\bar{\sigma}_N^z$ →

Remove Duplicates

Use a lookup table to perform PET over multiple encryptions.

Lookup

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



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	$E_e(\bar{\sigma}_N)$	$E_e(c_N)$

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



Remove Duplicates

Use a lookup table to perform PET over multiple encryptions.

Lookup

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



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

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



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

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



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

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

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



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

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



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

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

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



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

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	$E_e(\sigma_1)$
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 S/W 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 (1)

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	W_i	$E_e(\sigma_n)$

To Do:

1. Remove Duplicates
2. Authorize Votes

Now S/W PET?

→ Mix.

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 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

σ_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	$\hat{E}_e(\sigma_n)$

$\leftarrow \sigma_1^z$

Lookup

σ_i^z
σ_1^z

\rightarrow

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	$\hat{E}_e(\sigma_n)$

← σ_2^z

Lookup

σ_i^z
σ_1^z
σ_2^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	$\hat{E}_e(\sigma_n)$

← σ_3^z

Lookup

σ_i^z
σ_1^z
σ_2^z
σ_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	$\hat{E}_e(\sigma_n)$

← σ_4^z

Lookup

σ_i^z
σ_1^z
σ_2^z
σ_3^z
σ_4^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	$\hat{E}_e(\sigma_n)$

← σ_5^z

Lookup

σ_i^z
σ_1^z
σ_2^z
σ_3^z
σ_4^z
σ_5^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	$\hat{E}_e(\sigma_n)$

← σ_n^z

Lookup

σ_i^z
σ_1^z
σ_2^z
σ_3^z
σ_4^z
σ_5^z
σ_n^z

→

Authorize Votes (3)

Use a lookup table to perform PET over multiple encryptions.

Lookup

σ_i^z
σ_1^z
σ_2^z
σ_3^z
σ_4^z
σ_5^z
σ_n^z

(Voting Board)

j	$\hat{\mathbf{A}}_j$	$\hat{\mathbf{B}}_j$
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

σ_i^z
σ_1^z
σ_2^z
σ_3^z
σ_4^z
σ_5^z
σ_n^z



(Voting Board)

j	$\hat{\mathbf{A}}_j$	$\hat{\mathbf{B}}_j$
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

σ_i^z
σ_1^z
σ_2^z
σ_3^z
σ_4^z
σ_5^z
σ_n^z



(Voting Board)

j	$\hat{\mathbf{A}}_j$	$\hat{\mathbf{B}}_j$
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

σ_i^z
σ_1^z
σ_2^z
σ_3^z
σ_4^z
σ_5^z
σ_n^z



(Voting Board)

j	$\hat{\mathbf{A}}_j$	$\hat{\mathbf{B}}_j$
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

σ_i^z
σ_1^z
σ_2^z
σ_3^z
σ_4^z
σ_5^z
σ_n^z



(Voting Board)

j	$\hat{\mathbf{A}}_j$	$\hat{\mathbf{B}}_j$
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

σ_i^z
σ_1^z
σ_2^z
σ_3^z
σ_4^z
σ_5^z
σ_n^z



(Voting Board)

j	$\hat{\mathbf{A}}_j$	$\hat{\mathbf{B}}_j$
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

σ_i^z
σ_1^z
σ_2^z
σ_3^z
σ_4^z
σ_5^z
σ_n^z



(Voting Board)

j	$\hat{\mathbf{A}}_j$	$\hat{\mathbf{B}}_j$
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?

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 : $E_e(\sigma, \alpha_B)$
2. **(I)** Index of V 's entry in voter roll

Voting Board

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

Cast Votes

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

Voting Board

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

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	$E_e(\sigma_1)$	$\hat{E}_e(\bar{\sigma}_N)$	$\hat{E}_e(c_N)$			
2	Dwarf	$\hat{E}_e(\sigma_2)$	$\hat{E}_e(\bar{\sigma}_4)$	$\hat{E}_e(c_4)$			
3	Gretel	$\hat{E}_e(\sigma_3)$					
4	King	$\hat{E}_e(\sigma_4)$					
5	Snow White	$\hat{E}_e(\sigma_5)$	$\hat{E}_e(\bar{\sigma}_7)$	$\hat{E}_e(c_7)$	$\hat{E}_e(\bar{\sigma}_1)$	$\hat{E}_e(c_1)$	
n	Witch	$\hat{E}_e(\sigma_n)$	$\hat{E}_e(\bar{\sigma}_6)$	$\hat{E}_e(c_6)$			

Tallying - Naive (3)

1. Remove duplicates as per Smith/Weber
2. Mix voting board
3. Decrypt voting board indices \mathbf{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
- $\rightarrow \mathbb{O}(N + n)$