Who was that masked voter? The tally won't tell!

[1] Peter Y.A. Ryan,
[1] Peter B. Roenne,
[1] Dimiter Ostrev,
[2] Philip B. Stark,
[1] Najmeh Soroush,
[1] Fatima -E. El Orche

[1] University of Luxembourg
[2] University of California, Berkeley

E-Vote-ID 2021
October 2021

SnT
securityandtrust.lu

uni.lu
UNIVERSITÉ DU LUXEMBOURG

Risk-Limiting Tallies & Risk-Limiting Audits:

	Plaintext ballots	Subset of ballots
Ballot 1	Anahita	Anahita
Ballot 2	Mithra	Mithra
Ballot 3	Mithra	Ahriman
Ballot 4	Ahura Mazda	Ahura Mazda
Ballot 5	Anahita	Anahita
Ballot 6	Anahita	Anahita
Ballot 7	Ahura Mazda	
Ballot 8	Ahura Mazda	
Ballot 9	Mithra	Mithra
Ballot 10	Anahita	Anahita

Plausible deniability to handle certain corner cases:

- unanimous votes
- signature attacks
- absence of any votes for certain candidates

[1] SOBA: RLA techniques
[2] VAULT: RLA techniques using HE scheme

[3] Risk-limiting tallies :

Propose an RLT technique: Unmask randomly selected ballots one at a time until the confidence level is met.

- The actual margin
- Luck of the draw

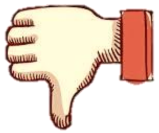
[1] Benaloh, J., Jones, D.W., Lazarus, E., Lindeman, M., Stark, P.B.: SOBA: Secrecy preserving observable ballot-level audit. EVT/WOTE 11 (2011)

[2] Benaloh, J., Stark, P.B., Teague, V.: VAULT: Verifiable audits using limited transparency. E-Vote-ID 2019 p. 69 (2019)

[3] Jamroga, W., Roenne, P.B., Ryan, P.Y., Stark, P.B.: Risk-limiting tallies. In: International Joint Conference on Electronic Voting. pp. 183{199. Springer (2019)

Risk-Limiting Tallies & Risk-Limiting Audits:

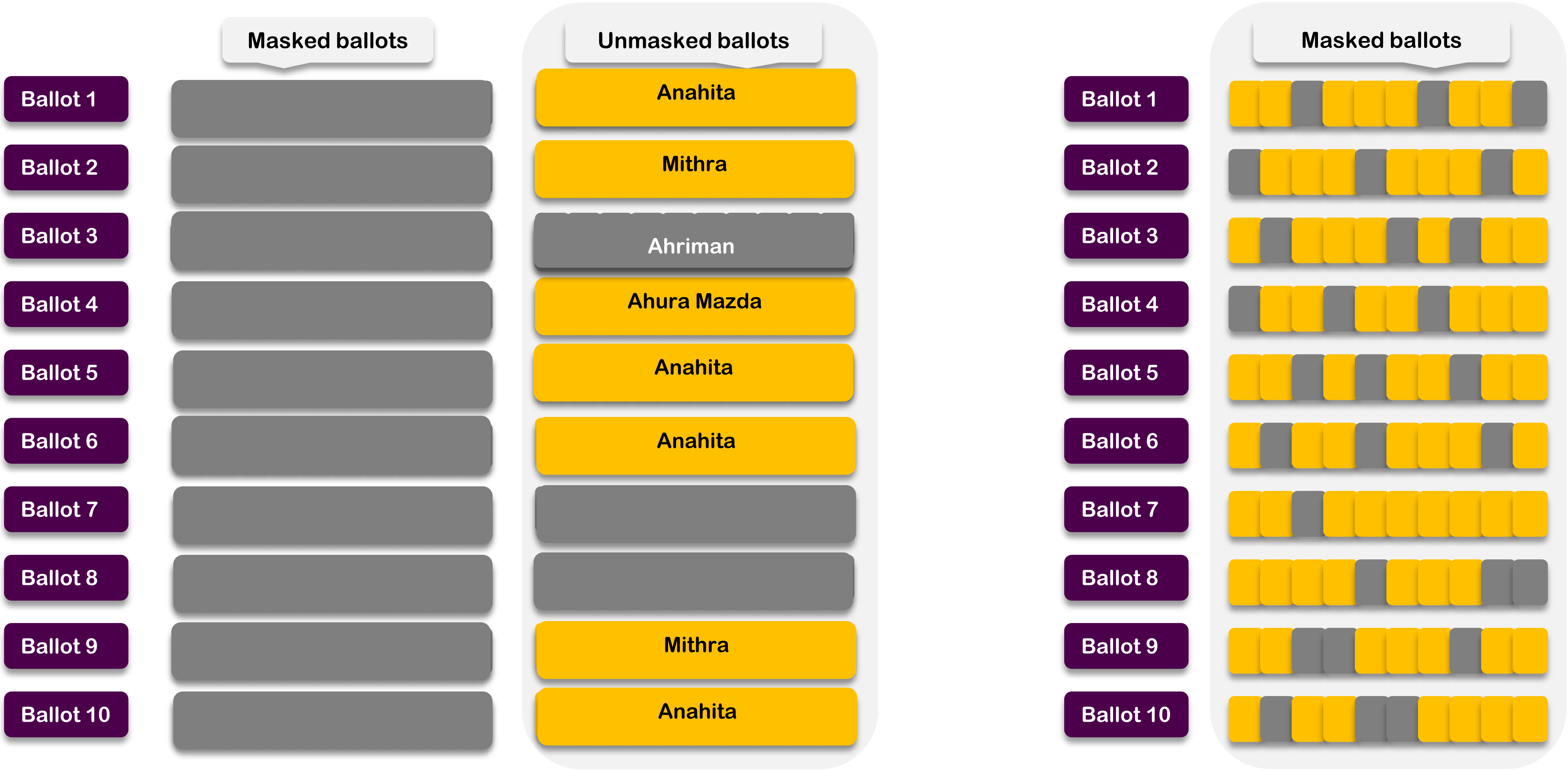
	Plaintext ballots	Subset of ballots
Ballot 1	Anahita	Anahita
Ballot 2	Mithra	Mithra
Ballot 3	Mithra	
Ballot 4	Ahura Mazda	Ahura Mazda
Ballot 5	Anahita	Anahita
Ballot 6	Anahita	Anahita
Ballot 7	Ahura Mazda	
Ballot 8	Ahura Mazda	
Ballot 9	Mithra	Mithra
Ballot 10	Anahita	Anahita



Handling elections with complex ballots

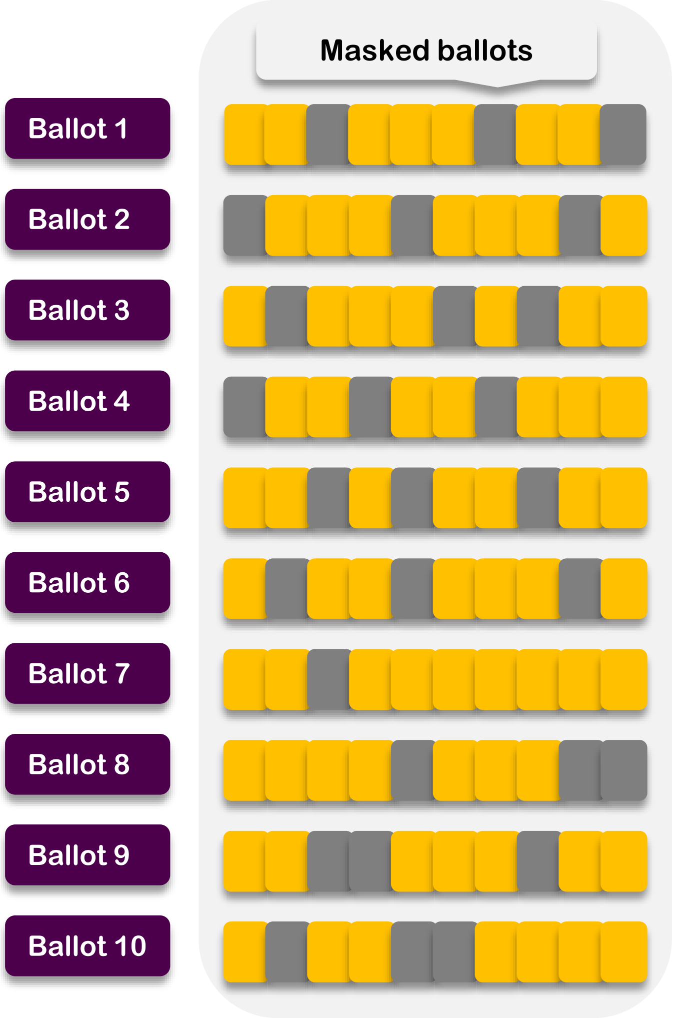
RLT is arguably undemocratic.

Masked Risk Limiting Tallies : Reveal m out of k positions



Masked Risk Limiting Tallies : Reveal m out of k positions

Decrease the chance of a signature ballot to be visible
Can be seen as more democratic than RLT
Improve the receipt-freeness compared to RLT



Towards Masked RLT

1- Analyze (simultaneous) signature attacks, Using methods from coding theory

2- Propose various measures of verifiability and coercion-resistance and investigate how several masking strategies perform against these measures

3- Define new quantitative measures for the level of vote-buying-resistance

4- Define new quantitative measures for the level of coercion-resistance without plausible deniability

How many simultaneous signature attacks can a coercer launch?

$Hamming\ distance$: $d_H(x, y) = \{\mathrm{i}: x_i \neq \mathrm{y}_i\}$

$\boldsymbol{y} = (\mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{1})$

$\boldsymbol{x} = (\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0})$

$\boldsymbol{a} = (\mathbf{1}, *, *, *, \mathbf{1})$

$\boldsymbol{b} = (*, *, \mathbf{0}, *, \mathbf{1})$

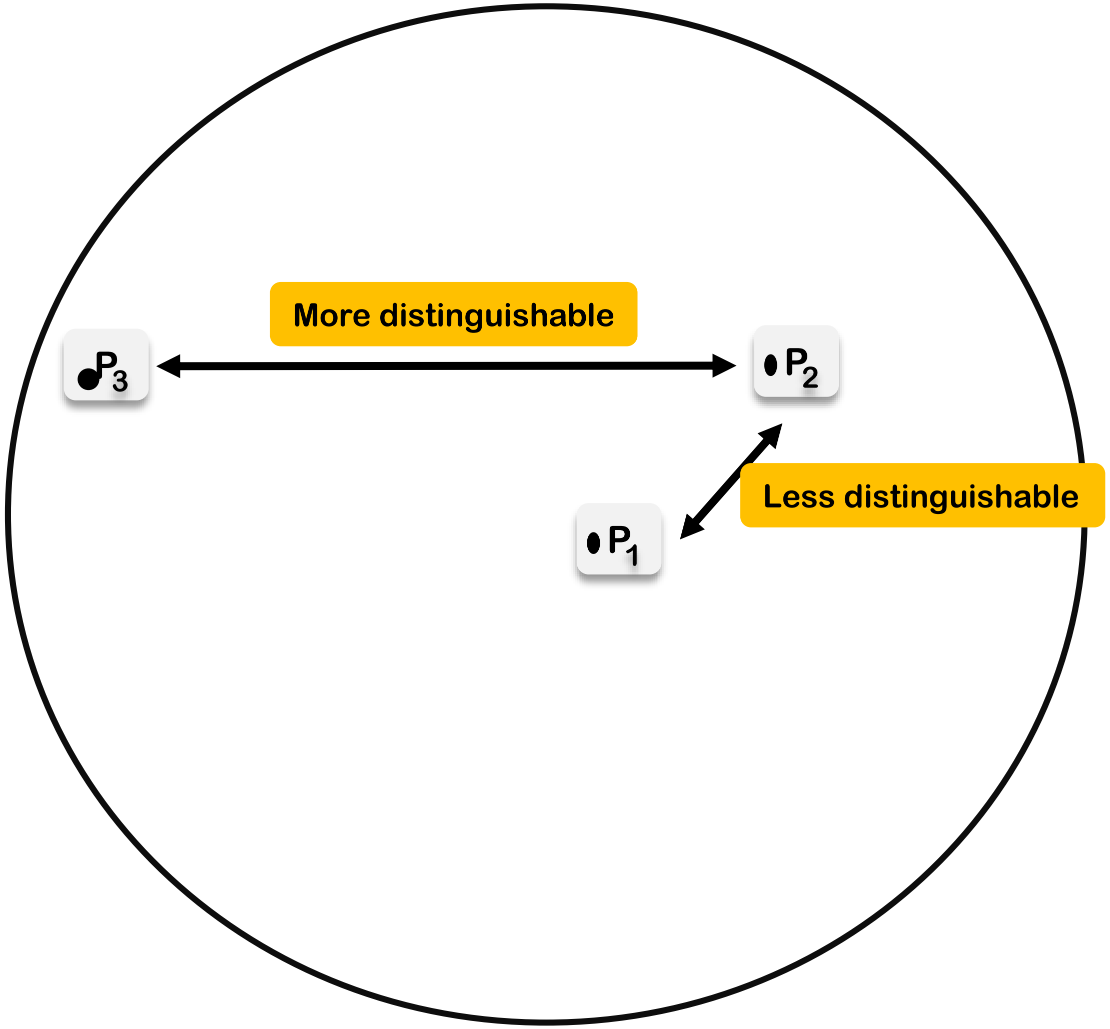
$d_H(x, y) = 2 < d_H(\mathrm{z}, x) = 4$

$\boldsymbol{z} = (\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0})$

$\boldsymbol{c} = (\mathbf{1}, *, *, *, \mathbf{0})$

$\boldsymbol{k} = \mathbf{5}, \boldsymbol{\varphi} = \{\mathbf{0}, \mathbf{1}\}$

How many simultaneous signature attacks can a coercer launch?



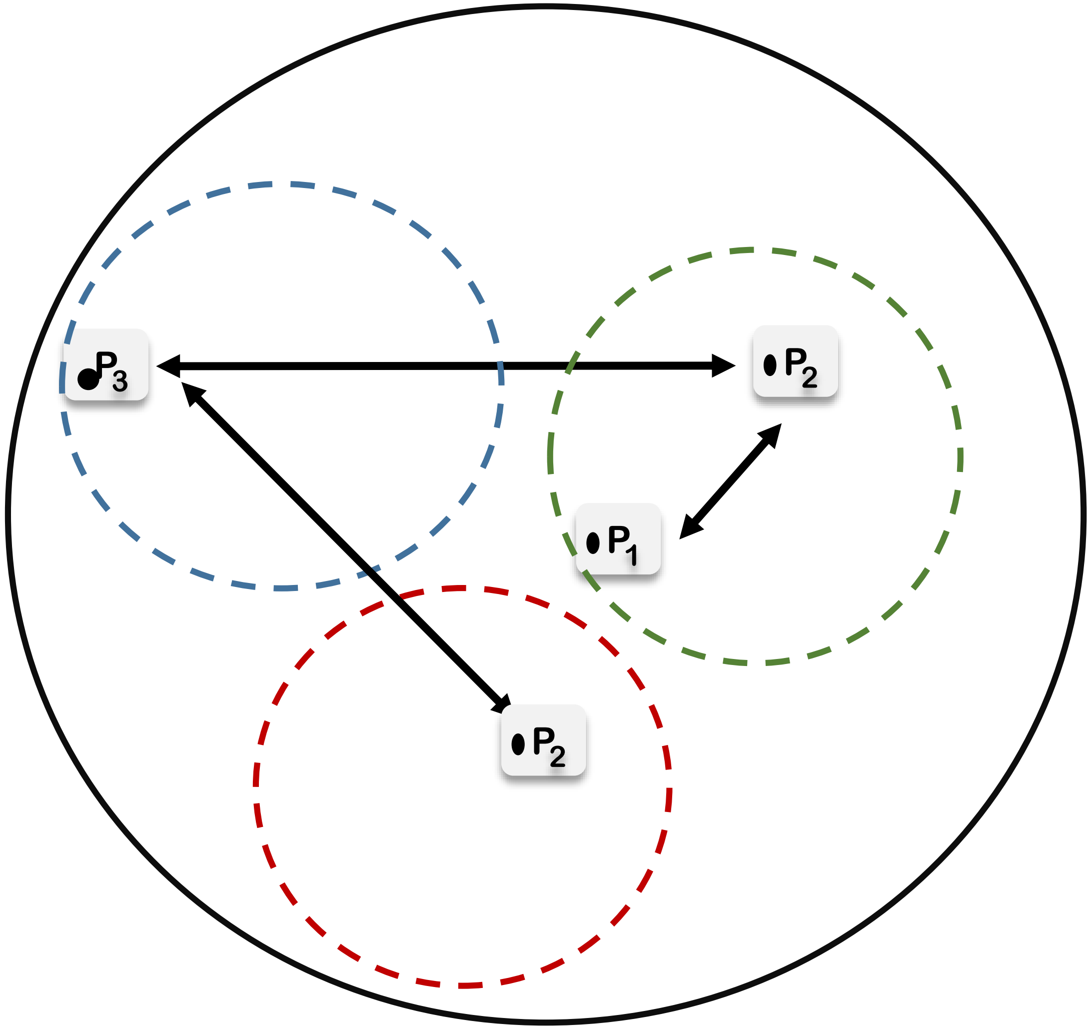
$$\mathit{Hamming\ distance}\colon\ d_H(x,y) = \{\mathrm{i}\colon x_i \neq \mathrm{y}_i\}$$

$$q_{S,x_S}(s,\alpha) = p_S(s)\delta_{x_S,\alpha}$$

$$d_{p_S}(x,y) = \frac{1}{2}\|q_{S,x_S} - q_{S,y_S}\|_1$$

There is a class of distributions p_S such that d_{p_S} does not even depend on all details of the set of positions where x, y differ, but only on the Hamming distance between x and y,

How many simultaneous signature attacks can a coercer launch?



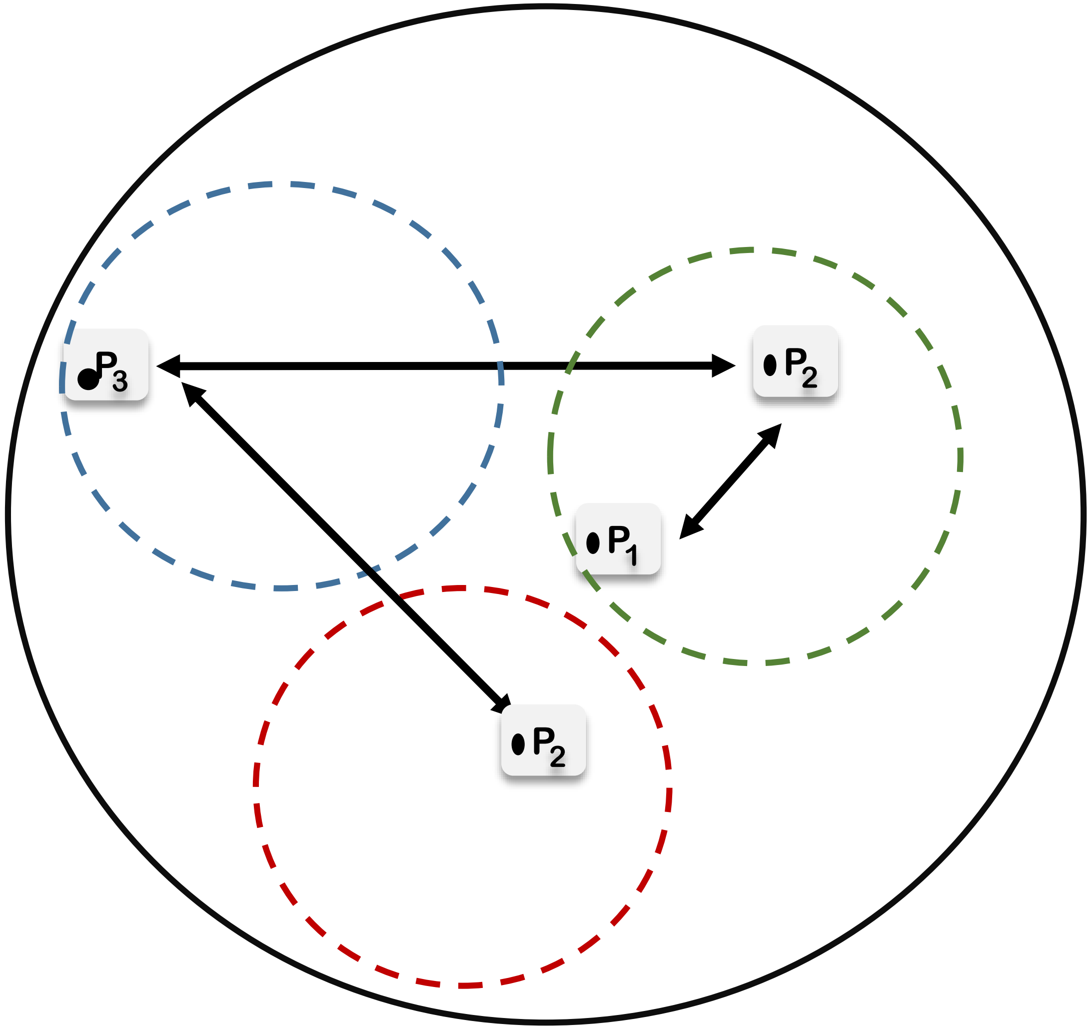
Theorem

For every finite set $\mathcal{V}$*, for every* $k \in \mathbb{N}$*, for every probability distribution* p_S *on subsets of* $\{1, \dots, k\}$ *satisfying* $\exists (r(0), \dots, r(k)) \forall s, p_S(s) = \frac{r(|s|)}{\binom{k}{|s|}}$*, for every* $q \in [0, 1 - p_S(\emptyset)]$*, let* $r_{max}(\mathcal{V}, k, p_S, q)$ *denote the size of the largest collection* $\{x_1, \dots x_r\}$ *with the property* $\forall i \neq j, d_{p_S}(x_i, x_j) \geq q$*. Then:*

$$\frac{|\mathcal{V}|^k}{\sum_{j=0}^{g_{p_S}(q)-1} \binom{k}{j} (|\mathcal{V}| - 1)^j} \leq r_{max}(\mathcal{V}, k, p_S, q) \leq$$

$$\leq \frac{|\mathcal{V}|^k}{\sum_{j=0}^{\lfloor (g_{p_S}(q)-1)/2 \rfloor} \binom{k}{j} (|\mathcal{V}| - 1)^j}$$

How to quantify the effect of a particular masking strategy on individual verifiability?



Quantify the effect of a particular masking strategy, (probability distribution p_S), on individual verifiability:

$$IV(p_S) = \inf_{x \neq y \in \mathcal{V}^k} d_{p_S}(x, y)$$

1. This quantity takes values between 0 and 1
2. $IV(p_S) = 1$: The masking strategy leaves the individual verifiability of the underlying voting protocol invariant
3. $IV(p_S) = 0$: The masking strategy destroys any individual verifiability that was present in the underlying voting protocol.

Measured and Compared various definitions for different masked tally method and investigate how several sampling/masking strategies perform against these measures

Full ballot disclosure

RLT

1– δ –Privacy
2– δ – Coercion Resistance
3- No Deniability
4- Receipt- Freeness

Masked RLT

Result Only

δ –Privacy: Game based definition:

$\mathcal{O}$: An observer		$\mathcal{V}_{obs}$: under observation
$(v_0, v_1) \leftarrow \mathcal{O}$	$\mathcal{O} \xrightarrow{(v_0, v_1)} \mathcal{V}_{obs}$	$b \leftarrow \{0,1\}$
		$\mathcal{V}_{obs} \xrightarrow{Cast[v_b]} BB$
$\mathcal{O}(BB) \rightarrow b^*$		

An election has δ-privacy if:

$$Advantage(\mathcal{O}) = |\Pr[\mathcal{O} \mapsto 0 | b = 0] - \Pr[\mathcal{O} \mapsto 0 | b = 1]| \leq \delta$$

δ –Privacy in Masked RLT: (m out of k)

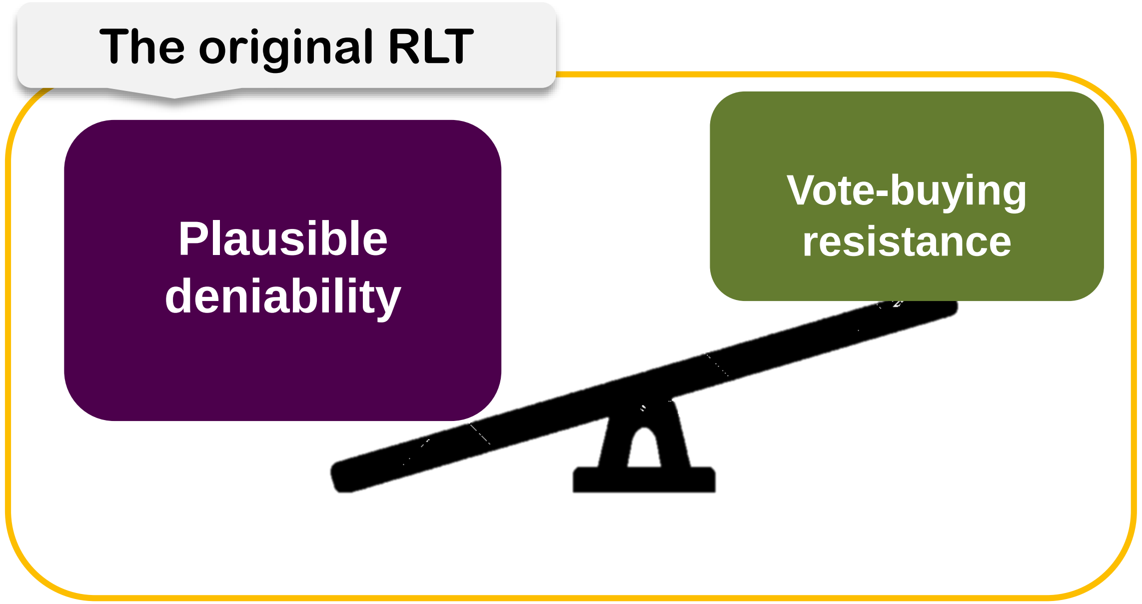
v_0^O: the most unlikely ballot

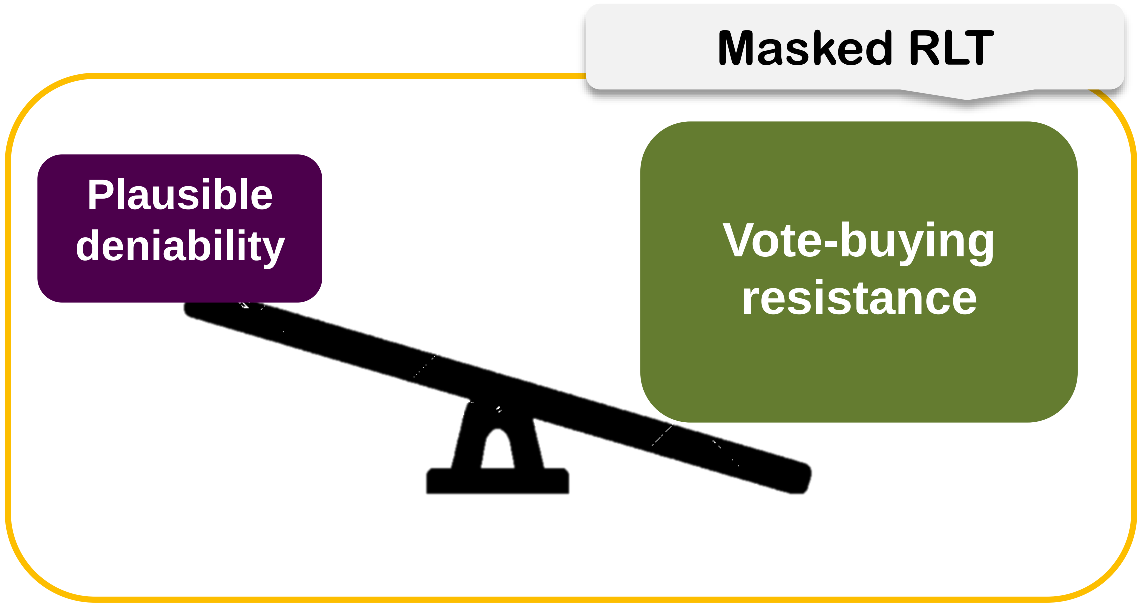
v_1^O: the most likely ballot

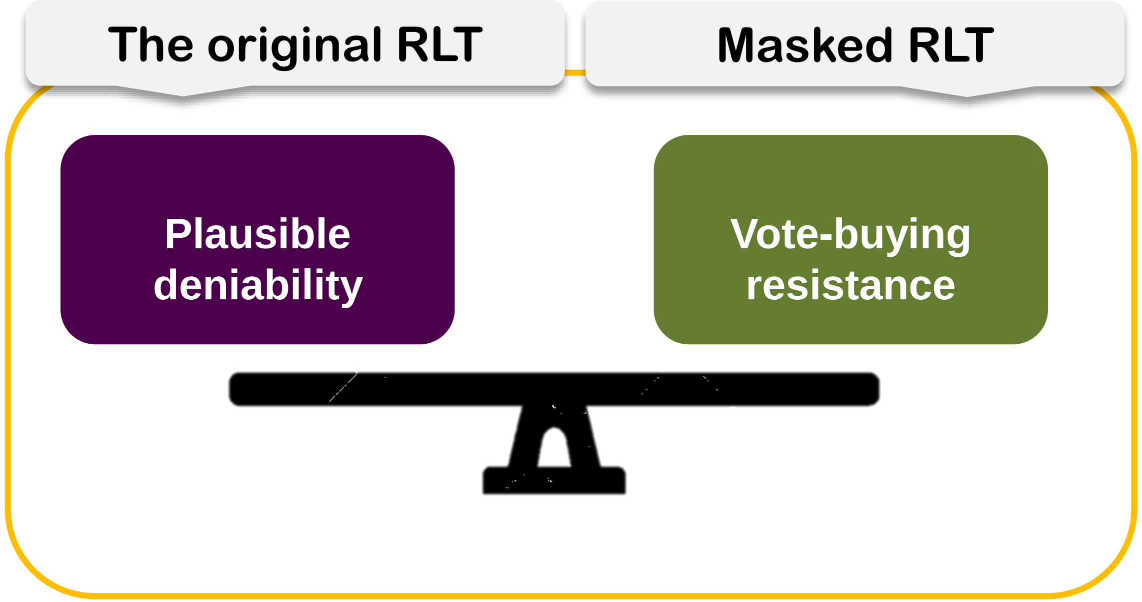
$$N_{v^*-collision} = |\{v : Masked^{(m,k)}(v) = Masked^{(m,k)}(v^*)\}|$$

$$p_{v_0-collision} = 1/\binom{k}{m} \cdot \sum_{1 \leq i_1 < i_2 < \ldots < i_m \leq k} p_{i_1} \cdots p_{i_m}$$

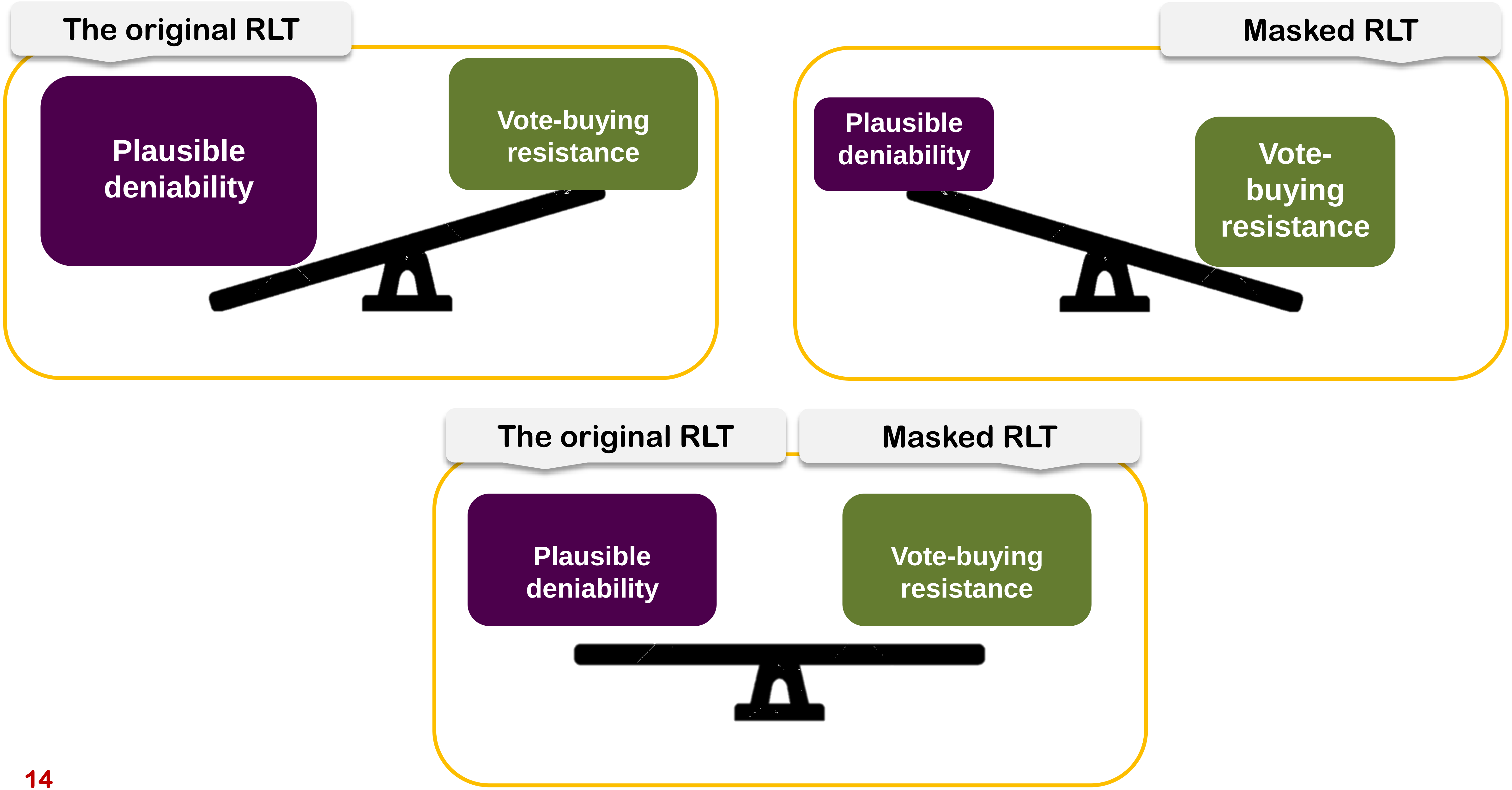
Plausible deniability & Vote-buying resistance







Plausible deniability & Vote-buying resistance



An Example:

$x = (x_1, x_2, x_3)\ , x_i\ \in \{0,1\}$

$Pr[x_1 = 1] = Pr[x_2 = 1] = \frac{1}{2}\ , Pr[x_3 = 1] = 0$

$coercer : \ x^* = (0\ , 0\ , 1)$

$voter \ : \ x = (1\ , 0\ , 0)$

1. cast a vote $(1, 0, 0)$ without the 0 probability signature part ; no deniability
   - $m = 1$ this happens with $p = (2/3)^{n_h+1}$
   - $m = 2$ with $p = (11/12)^{n_h}$
   - both are small if we have many voters
2. casting a vote $(1, 0, 1)$ with the signature part.
   - $m = 1$ with probability $1/3(2/3)^{n_h}$
   - $m = 2$ with probability $1/3 + 1/3(11/12)^{n_h}$

Thus for $m = 1$ strategy 2) is always better, but for $m = 2$ strategy 1) is better when we have more than 13 voters. In some cases the voter strategy thus depends on m, which might not be know beforehand

Conclusion

	δ –Privacy	Receipt- Freeness	δ – Coercion Resistance	No Deniability
Masked RLT	✓	✓	✓	?

Future Work

Define the level of plausibility for new RLT which can guarantee that the voter always has a certain level of coercion-resistance

From Game Theory Perspective!

Finding Optimal Strategy When the voter has a relaxed goal allowing to cast a signature part or not!

What is the optimal strategy a voter can choose to satisfy the two followings:

- Achieve a high level plausible deniability
- Casting a ballot close to of her own choice

Thanks for listening!