A toolbox for verifiable tally-hiding e-voting systems

eprint.iacr.org/2021/491

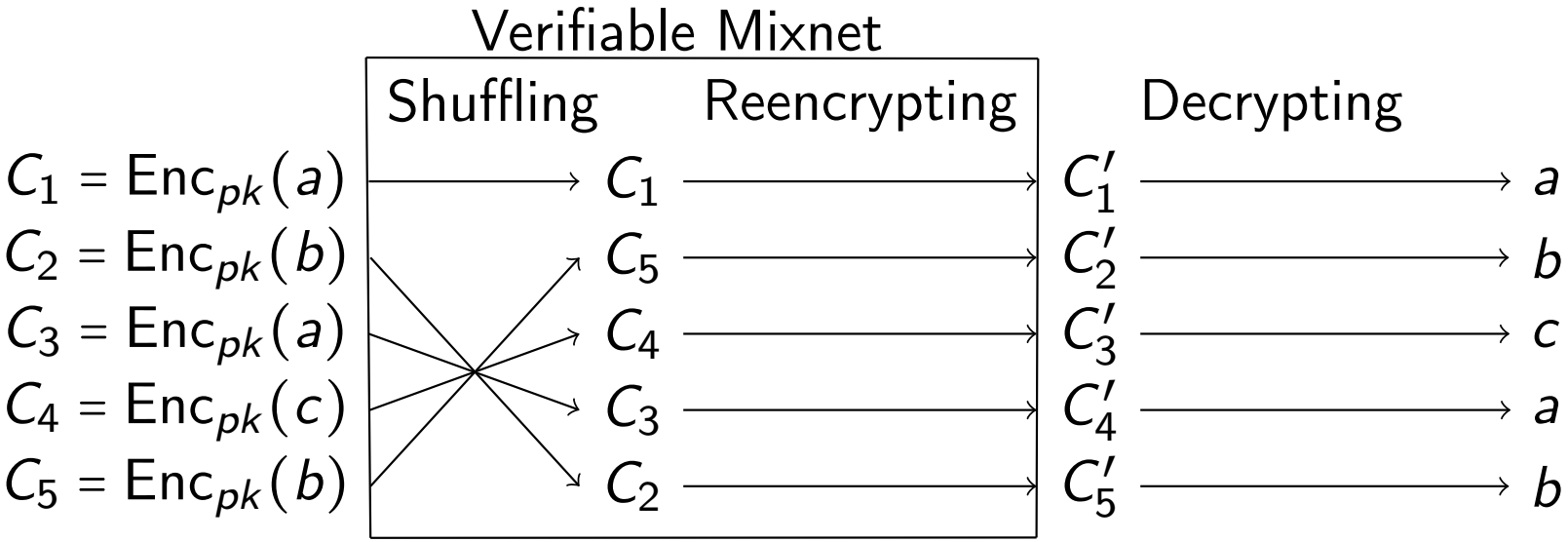
Véronique Cortier Pierrick Gaudry **Quentin Yang**

LORIA - CNRS, Inria Nancy - Grand-Est, Université de Lorraine

CSF 5 min talks, June 2021

Why tally hiding?

One key step is tallying, which is often done with shuffling.



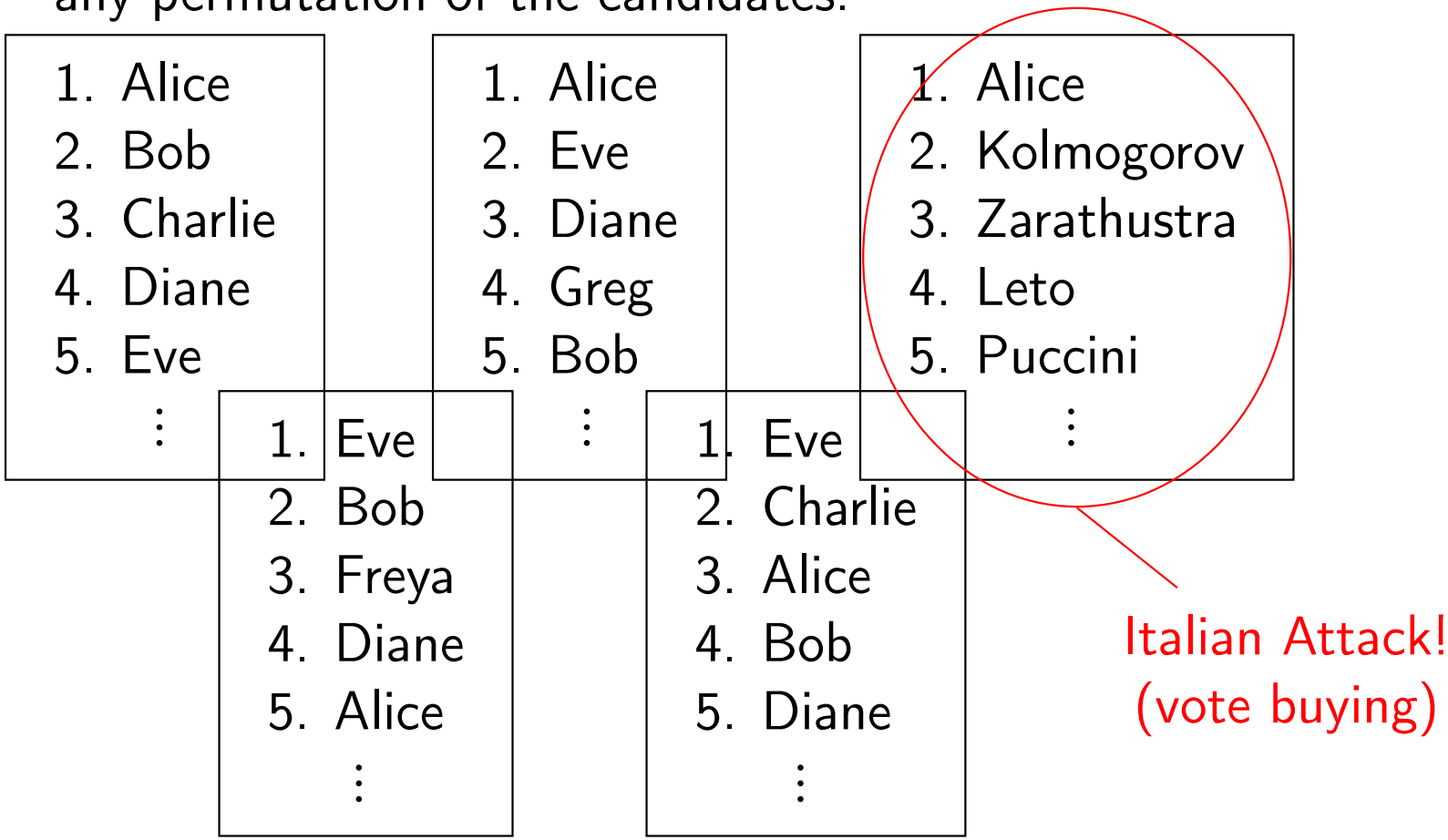
Shuffling reveals the list of voting options chosen.

Why tally hiding?

Some voting systems (Condorcet, STV) let you chose any permutation of the candidates.

Why tally hiding?

Some voting systems (Condorcet, STV) let you chose any permutation of the candidates.



Tally hiding in the litterature

Ordinos: Voters select one candidate, the candidate(s) with the most votes are elected. Kuesters, Liedtke, Mueller, Rausch, Vogt (2020). (Very specific counting function.)

Ranked Voting: Voters rank candidates.

- Condorcet. Haines, Pattinson, Tiwari (2019).

- Single Transferable Vote. Benaloh, Moran, Naish, Ramchen, Teague (2010). (Not fully tally-hiding.)

Majority Judgment: Voters grade each candidate, the one with the best median sequence is elected. Canard, Pointcheval, Santos, Traoré (2018).

Tally hiding in the litterature

Ordinos: Voters select one candidate, the candidate(s) with the most votes are elected. Kuesters, Liedtke, Mueller, Rausch, Vogt (2020). (Very specific counting function.)

Ranked Voting: Voters rank candidates.

- ~~Condorcet. Haines, Pattinson, Tiwari (2019).~~

  Privacy breach when two candidates are ranked equal.

- Single Transferable Vote. Benaloh, Moran, Naish, Ramchen, Teague (2010). (Not fully tally-hiding.)

~~**Majority Judgment:** Voters grade each candidate, the one with the best median sequence is elected. Canard, Pointcheval, Santos, Traoré (2018).~~

Fails to tally in some cases (22% fail rate for 100 voters).

Our Contribution

A generic toolbox for complete tally hiding.

Single vote	- Fix shortcoming in case of equality - **Adaptation to D'Hondt method**
Majority Judgment	- -
Condorcet	- - - -
STV	- -

Our Contribution

A generic toolbox for complete tally hiding.

Single vote	- Fix shortcoming in case of equality - **Adaptation to D'Hondt method**
Majority Judgment	- Fix the fact that it fails in not-so-rare cases - Complete leakage-free algorithm, **based on ElGamal**
Condorcet	- - - -
STV	- -

Our Contribution

A generic toolbox for complete tally hiding.

Single vote	- Fix shortcoming in case of equality - **Adaptation to D'Hondt method**
Majority Judgment	- Fix the fact that it fails in not-so-rare cases - Complete leakage-free algorithm, **based on ElGamal**
Condorcet	- Fix privacy issue when candidates are ranked equal - Several efficiency/leakage compromises - **Original ballot encoding** and ZKP by the voters - Complete leakage-free algorithm
STV	- -

Our Contribution

A generic toolbox for complete tally hiding.

Single vote	- Fix shortcoming in case of equality - **Adaptation to D'Hondt method**
Majority Judgment	- Fix the fact that it fails in not-so-rare cases - Complete leakage-free algorithm, **based on ElGamal**
Condorcet	- Fix privacy issue when candidates are ranked equal - Several efficiency/leakage compromises - **Original ballot encoding** and ZKP by the voters - Complete leakage-free algorithm
STV	- Ideal STV has exponential worst-case complexity - Complete leakage-free algorithm, with **fast arithmetic**

Our Contribution

A generic toolbox for complete tally hiding.

Single vote	- Fix shortcoming in case of equality - **Adaptation to D'Hondt method**
Majority Judgment	- Fix the fact that it fails in not-so-rare cases - Complete leakage-free algorithm, **based on ElGamal**
Condorcet	- Fix privacy issue when candidates are ranked equal - Several efficiency/leakage compromises - **Original ballot encoding** and ZKP by the voters - Complete leakage-free algorithm
STV	- Ideal STV has exponential worst-case complexity - Complete leakage-free algorithm, with **fast arithmetic**

Support complex operations: Sorting, Finding the s greatest values...

Another counting function? We can do it!

Thank you!

Check it out on eprint: eprint.iacr.org/2021/491

Figure: Different trade-offs for the Condorcet counting function

Version	Leakage	Voters # exp.	Authorities # exp.	Authorities # comm.	Size of the transcript
[19]	adj. matrix **privacy breach** [i]	$10k^2$	$18ank^2$	2	$10ank^2$
ballots as list of integers (partial MPC)	adj. matrix	$8k \log k$	$30nak^2 \log k$	$2 \log k$	$27nak^2 \log k$
ballots as list of integers (full MPC)	$\varnothing$	$8k \log k$	$10nak^2(3 \log k + 5m)$ $+120mak^3$	$m(m+4k)$	$9nak^2(3 \log k + 5m)$ $+108mak^3$
ballots as matrices	adj. matrix	$\frac{51}{2}k^2$	$\frac{51}{2}nk^2$	0	$\frac{29}{2}nk^2$
ballots as matrices (naive, for comparison)	adj. matrix	$20k^3$	$20nk^3$	0	$20nk^3$

[i] [19] leaks, for each ballot, the number of candidates ranked at equality. In particular, who voted blank is known to everyone.

Figure 5. Leading terms of the cost of MPC implementations of Condorcet winners. n: number of voters, $m = \lceil \log(n+1) \rceil$, k: number of candidates, a: number of authorities.