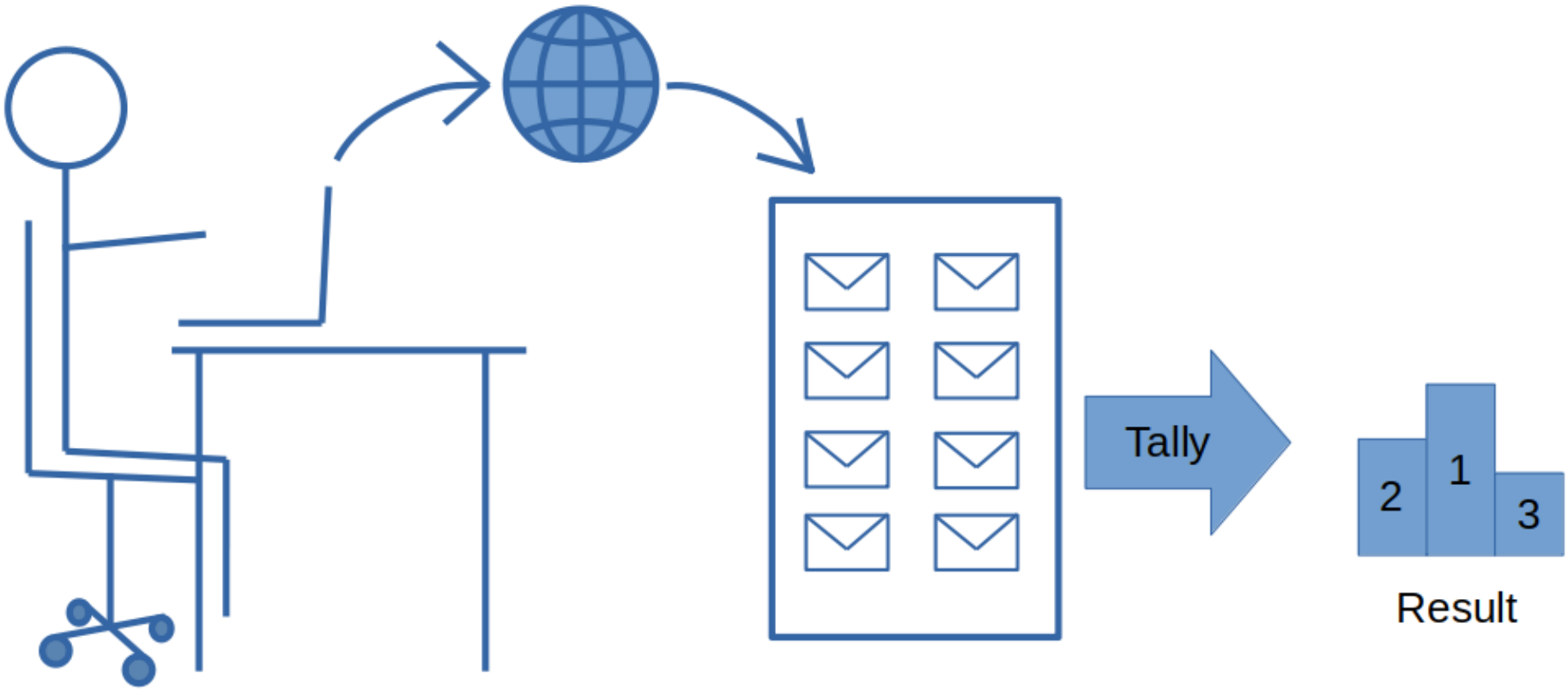
A toolbox for verifiable tally-hiding e-voting systems

Véronique Cortier Pierrick Gaudry **Quentin Yang**

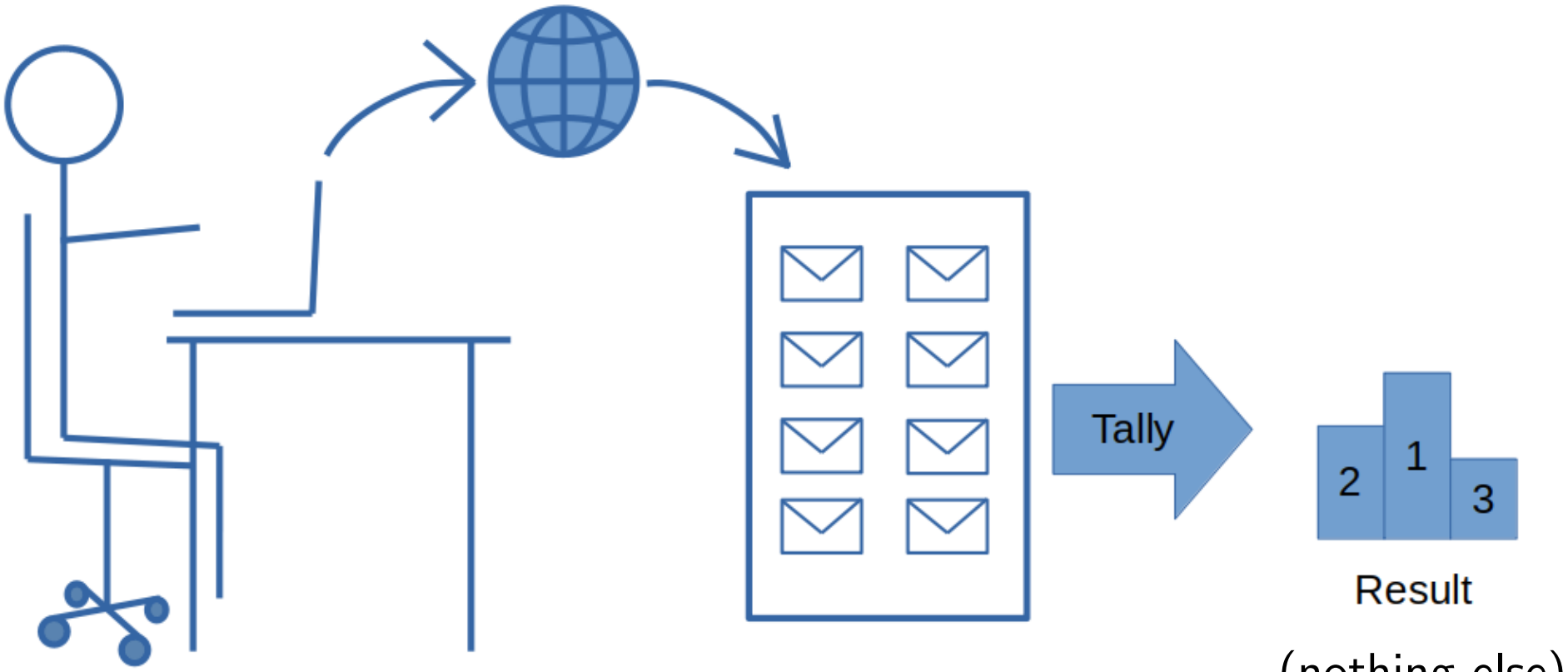
Université de Lorraine, CNRS, Inria Nancy - Grand-Est

ESORICS, September 2022

What is electronic voting?



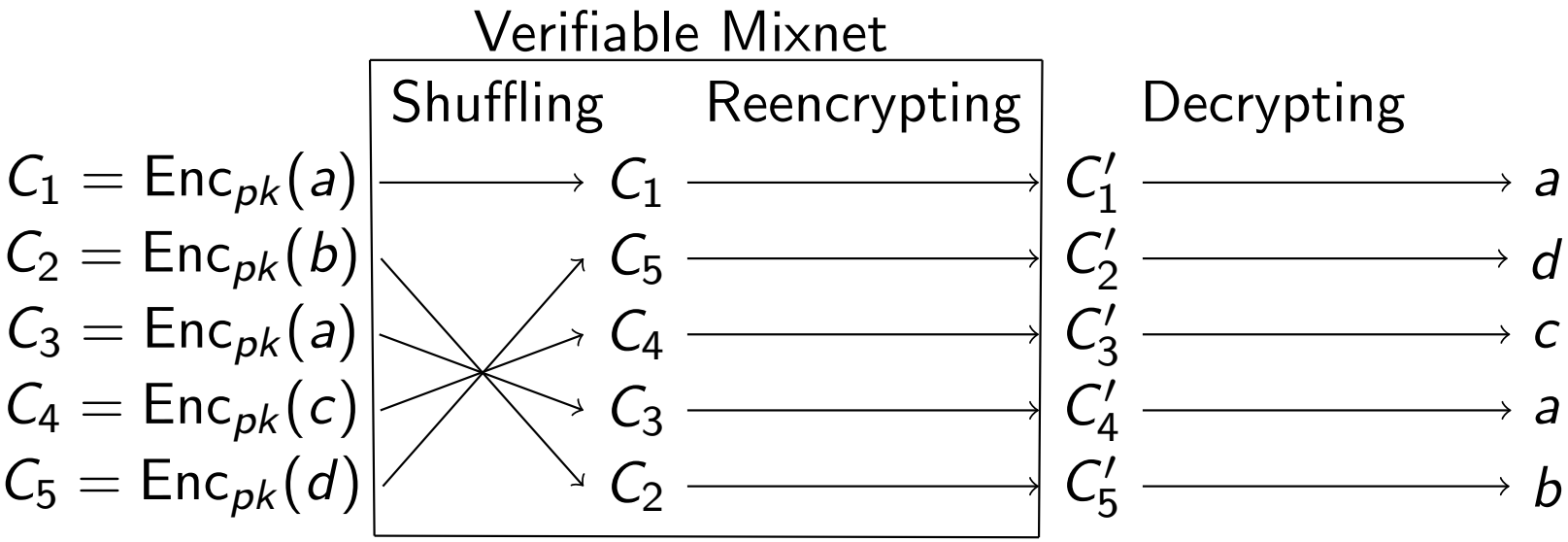
What is electronic voting?



(nothing else)

Why tally hiding?

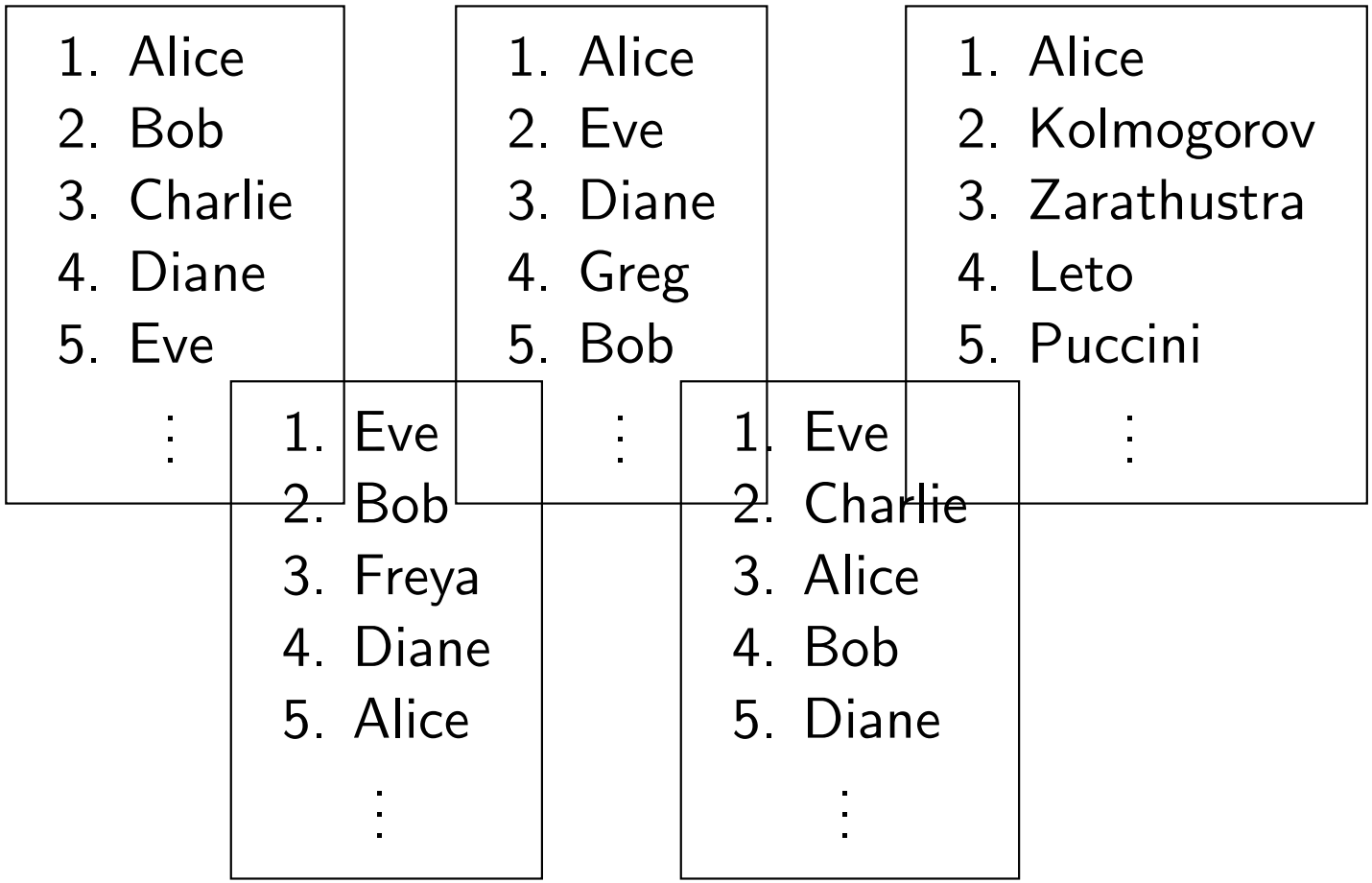
One key step is tallying, which is often done with shuffling.



Shuffling reveals the list of voting options chosen.

Why tally hiding?

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

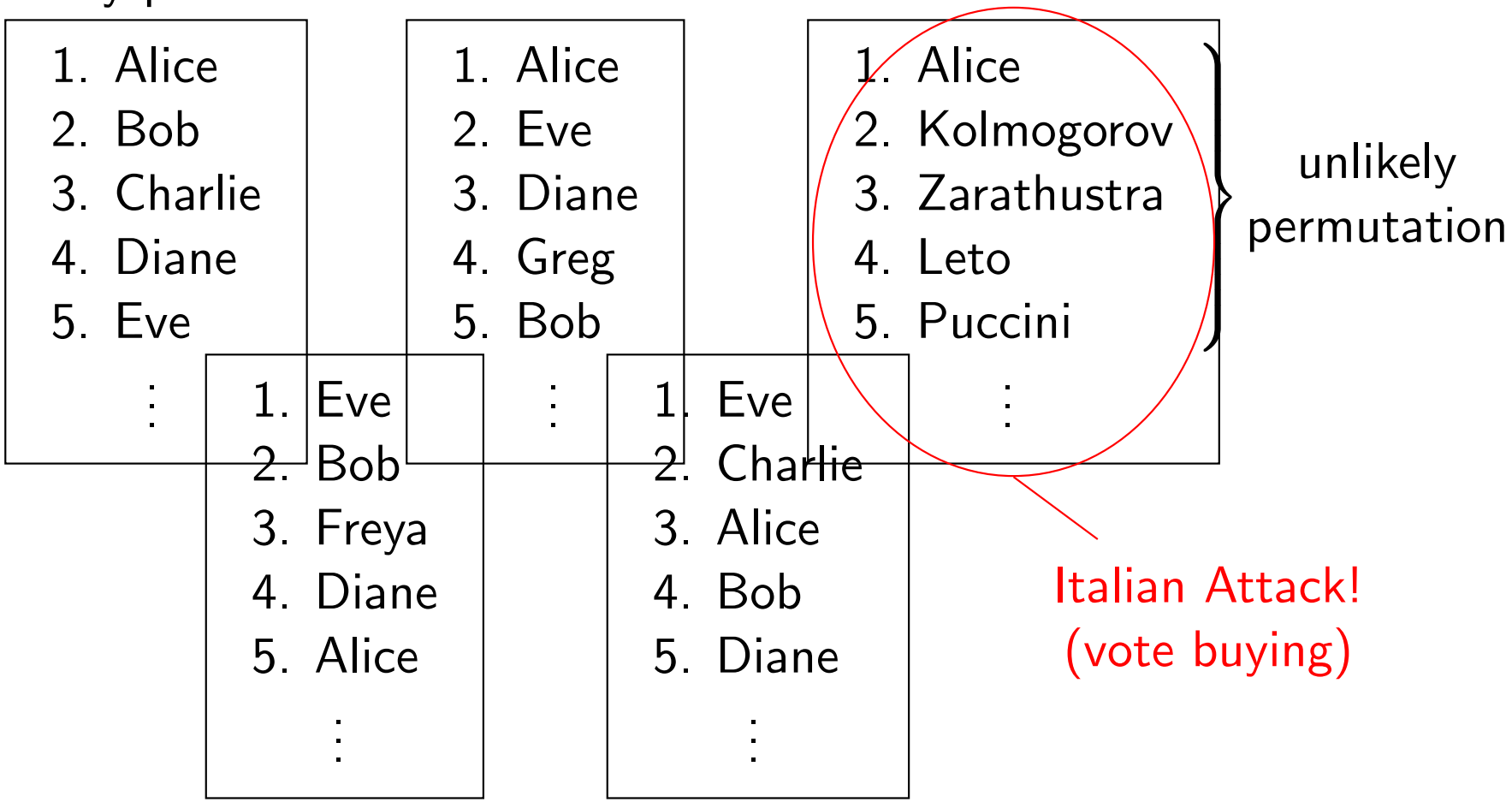


Why tally hiding?

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

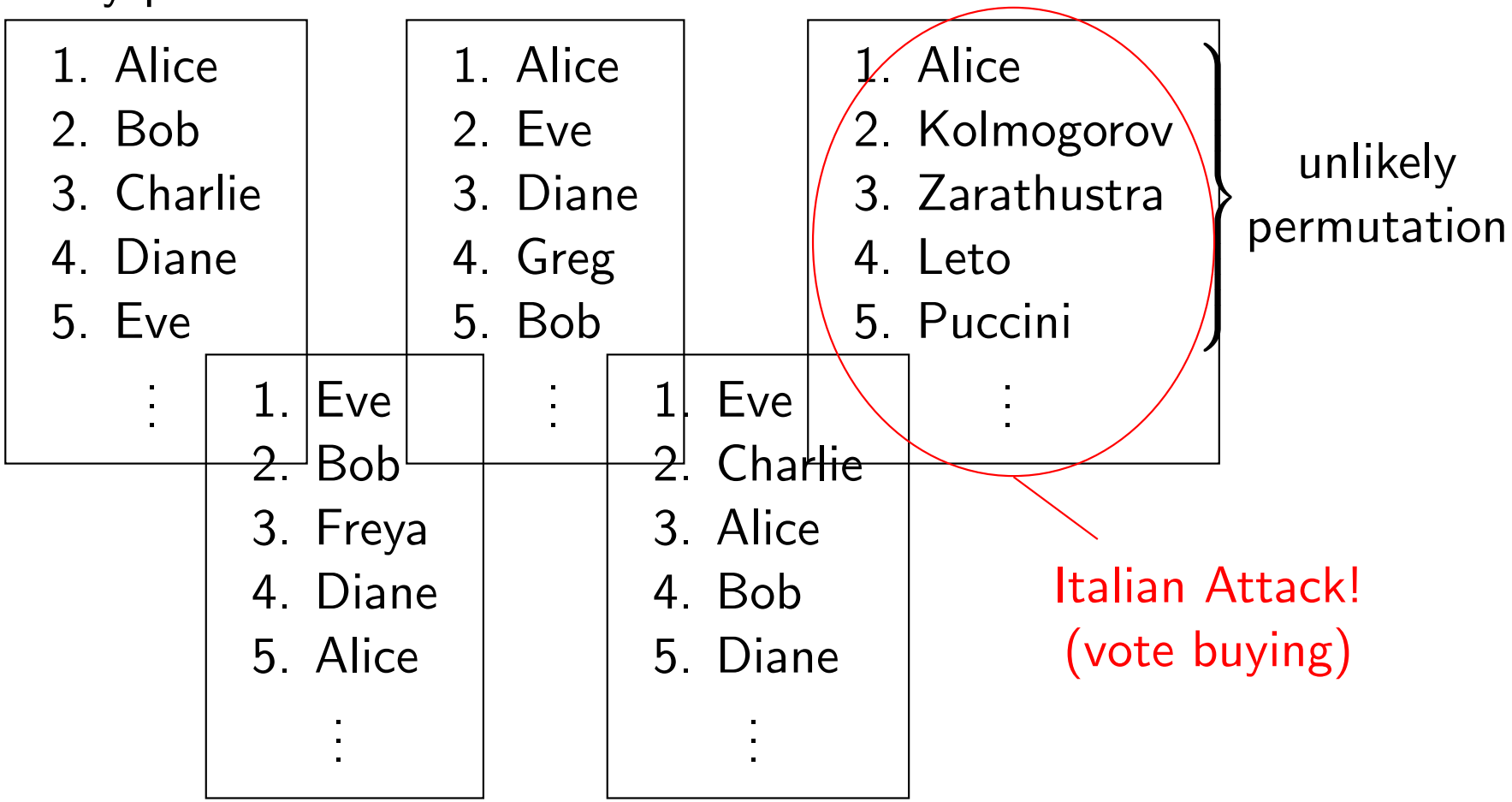
Why tally hiding?

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



Why tally hiding?

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



Tally hiding: Alice wins.

Why tally hiding?

Articolo pubblicato il 15 Marzo 2014

VOTO

QUEL SEGRETO CHE LA MAFIA CONOSCE

La nostra libertà di voto oggi costa appena 50€

Se in Italia, e soprattutto in terra di mafia, i cittadini fossero effettivamente liberi di votare per chi vogliono, la qualità degli eletti sarebbe certamente migliore.

Da tempo denunciamo questa vergognosa realtà ma nessuno prende provvedimenti; evidentemente il controllo del voto torna utile a molti. Abbiamo anche scritto al Presidente Napolitano nel marzo del 2012 ma non abbiamo ricevuto risposta. Ascolta lo SPOT AUDIO _il VOTO quel segreto che la mafia conosce_(1) della campasgna

L'Art. 48 della Costituzione fra l'altro stabilisce che: Il voto è personale ed eguale, libero e

Petition to stop vote buying in Italia (Libero Futuro)

Le Monde

Consulter le journal

Se connecter S'abonner

ACTUALITÉS PRÉSIDENTIELLE 2022 ÉCONOMIE VIDÉOS DÉBATS CULTURE M LE MAG SERVICES

INTERNATIONAL • LETTRES DE

Partage

« Beaucoup d'électeurs sont prêts à vendre leur voix » : l'achat de votes, un fléau bulgare

A la veille des élections législatives en Bulgarie du 4 avril, une étude confirme une pratique endémique et partagée par tous les partis du pays : payer les électeurs pour s'assurer leur voix.

Par Jean-Baptiste Chastand (Vienne, correspondant régional)

Publié le 02 avril 2021 à 00h14 - Mis à jour le 02 avril 2021 à 12h18 · Lecture 4 min.

Article about vote buying in Bulgaria (Le Monde)

Tally hiding in the literature

Single choice voting: Voters select one candidate or list.

- $s-$best. Küsters, Liedtke, Mueller, Rausch and Vogt, EuroS&P'20 (Ordinos).
- Hare-Niemeyer. Hertel *et al.*, E-VoteID'20.

Tally hiding in the literature

Ranked Voting: Voters rank candidates.

- Condorcet. Haines, Pattinson and Tiwari, VSTTE'19.

- Condorcet. Hertel *et al.*, E-VoteID'20.

Tally hiding in the literature

Ranked Voting: Voters rank candidates.

- Condorcet. Haines, Pattinson and Tiwari, VSTTE'19.
- Condorcet. Hertel *et al.*, E-VoteID'20.
- Borda. Hertel *et al.*, E-VoteID'20.

Tally hiding in the literature

Ranked Voting: Voters rank candidates.

- Condorcet. Haines, Pattinson and Tiwari, VSTTE'19.
- Condorcet. Hertel *et al.*, E-VoteID'20.
- Borda. Hertel *et al.*, E-VoteID'20.
- Single Transferable Vote. Benaloh, Moran, Naish, Ramchen and Teague, IEEE TIFS'10.
- Instant Run-off Voting. Culnane, Pereira, Ramchen and Teague, FC'19.
- Instant Run-off Voting. Hertel *et al.*, E-VoteID'20.

Tally hiding in the literature

Ranked Voting: Voters rank candidates.

- Condorcet. Haines, Pattinson and Tiwari, VSTTE'19.
- Condorcet. Hertel *et al.*, E-VoteID'20.
- Borda. Hertel *et al.*, E-VoteID'20.
- Single Transferable Vote. Benaloh, Moran, Naish, Ramchen and Teague, IEEE TIFS'10.
- Instant Run-off Voting. Culnane, Pereira, Ramchen and Teague, FC'19.
- Instant Run-off Voting. Hertel *et al.*, E-VoteID'20.

Majority Judgment: Voters grade each candidate.

- Canard, Pointcheval, Santos, Traoré (ESORICS'18).

Tally hiding in the literature

Ranked Voting: Voters rank candidates.

- ~~Condorcet. Haines, Pattinson and Tiwari, VSTTE'19.~~

  Privacy breach when two candidates are ranked equal.
- Condorcet. Hertel *et al.*, E-VoteID'20.

  Does **not** allow equal ranking.
- Borda. Hertel *et al.*, E-VoteID'20.
- Single Transferable Vote. Benaloh, Moran, Naish, Ramchen and Teague, IEEE TIFS'10. (Not fully tally-hiding.)
- Instant Run-off Voting. Culnane, Pereira, Ramchen and Teague, FC'19. (Not fully tally-hiding.)
- ~~Instant Run-off Voting. Hertel *et al.*, E-VoteID'20.~~

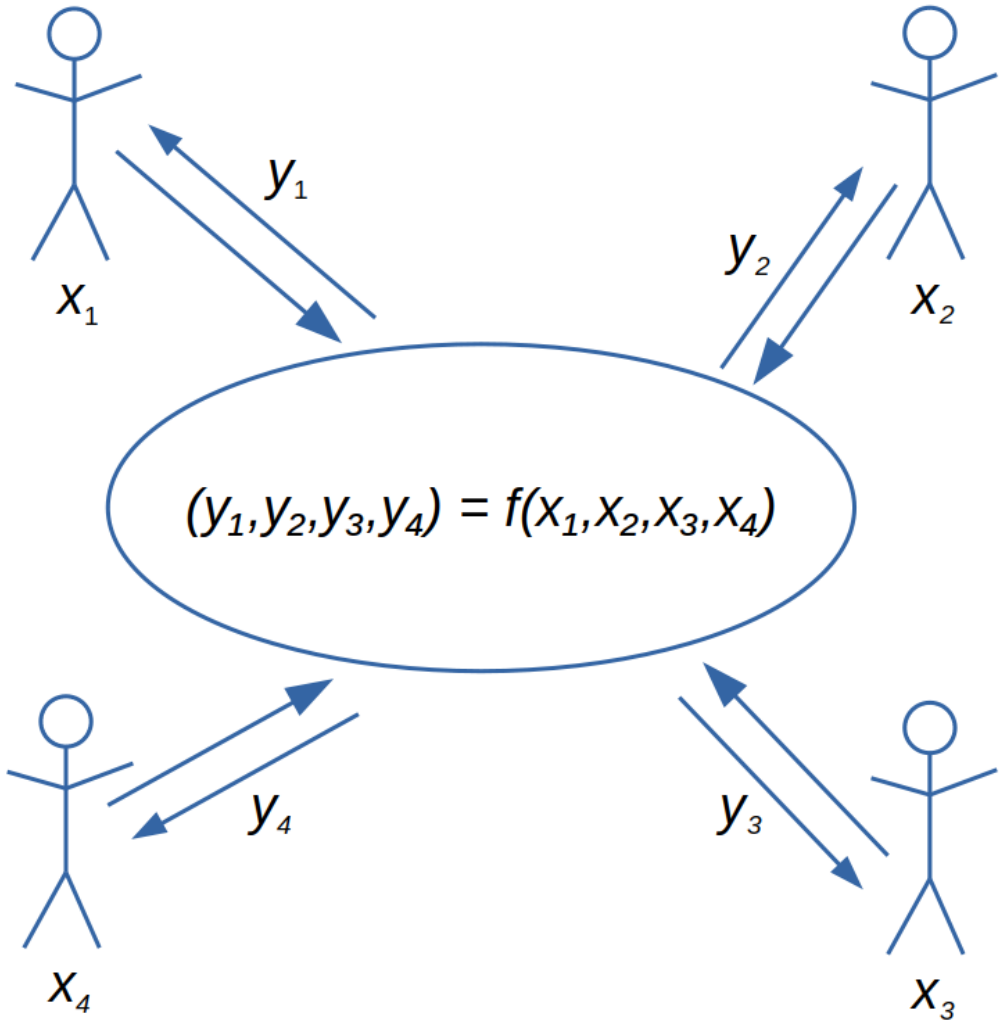
  Super-exponential complexity.

Majority Judgment: Voters grade each candidate.

- ~~Canard, Pointcheval, Santos, Traoré (ESORICS'18).~~

  Fails to tally in some not-so-rare cases.

Multi-party computation



Multi-party computation

Encryption	Paillier	ElGamal
Property	additively homomorphic	homomorphic

Multi-party computation

Encryption	Paillier	ElGamal
Property	additively homomorphic	homomorphic
Based on	Decisional Composite Residuosity Assumption	Decisional Diffie-Hellman
Key size	3072 bits	256 bits

Multi-party computation

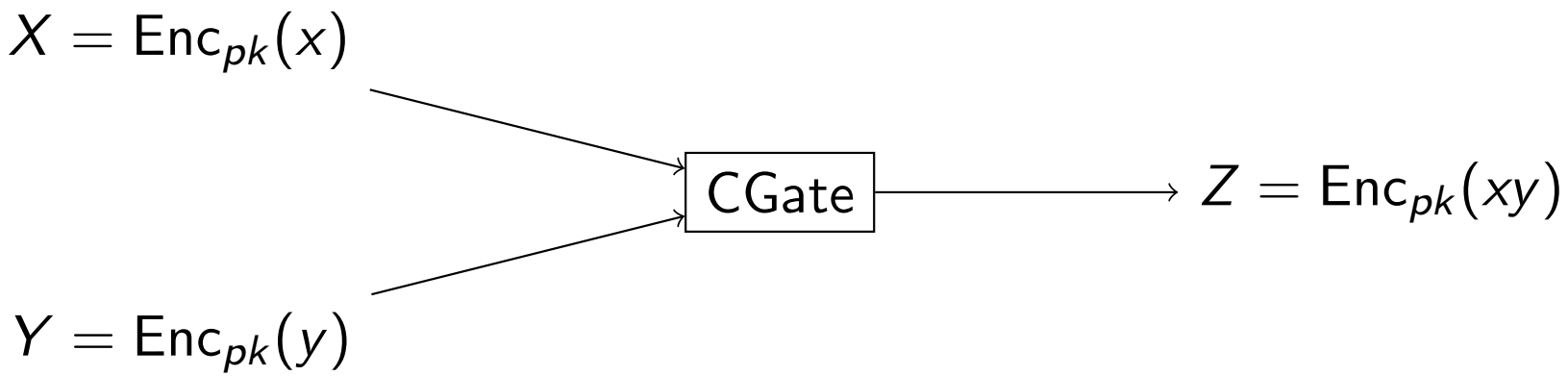
Encryption	Paillier	ElGamal
Property	additively homomorphic	homomorphic
Based on	Decisional Composite Residuosity Assumption	Decisional Diffie-Hellman
Key size	3072 bits	256 bits
Operation	3072−bits exponentiation modulo a 6144−bits integer	256−bits exponentiation

Multi-party computation

Encryption	Paillier	ElGamal
Property	additively homomorphic	homomorphic
Based on	Decisional Composite Residuosity Assumption	Decisional Diffie-Hellman
Key size	3072 bits	256 bits
Operation	3072−bits exponentiation modulo a 6144−bits integer	256−bits exponentiation
Libraries	??	Libsodium, OpenSSL, Crypto++, $\cdots$

Multi-party computation

We use the CGate primitive to build our MPC protocols:

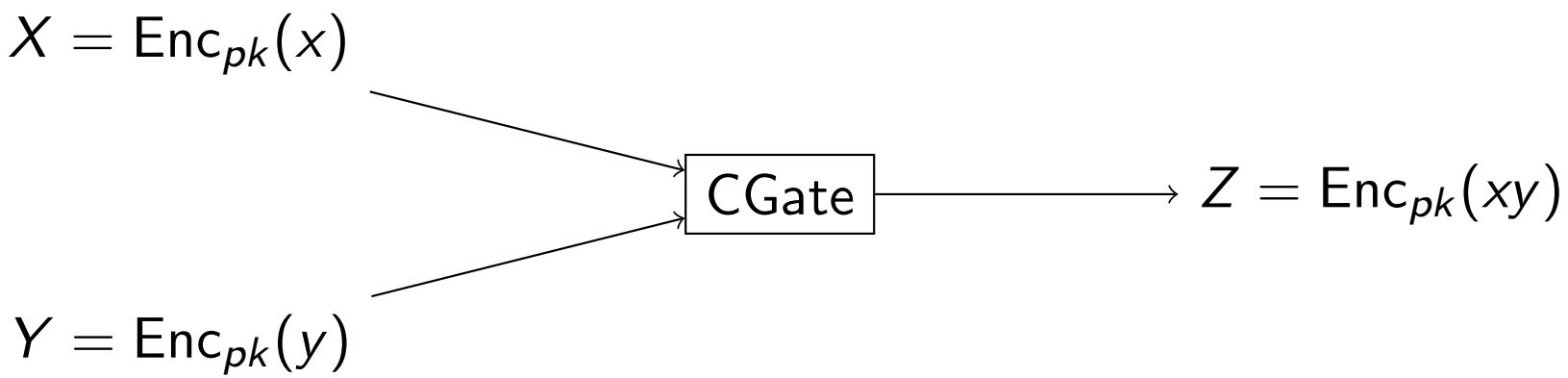


It allows logical operations on encrypted bits.

(Primitive adapted from Shoenmakers and Tuyls, Asiacrypt'04.)

Multi-party computation

We use the CGate primitive to build our MPC protocols:



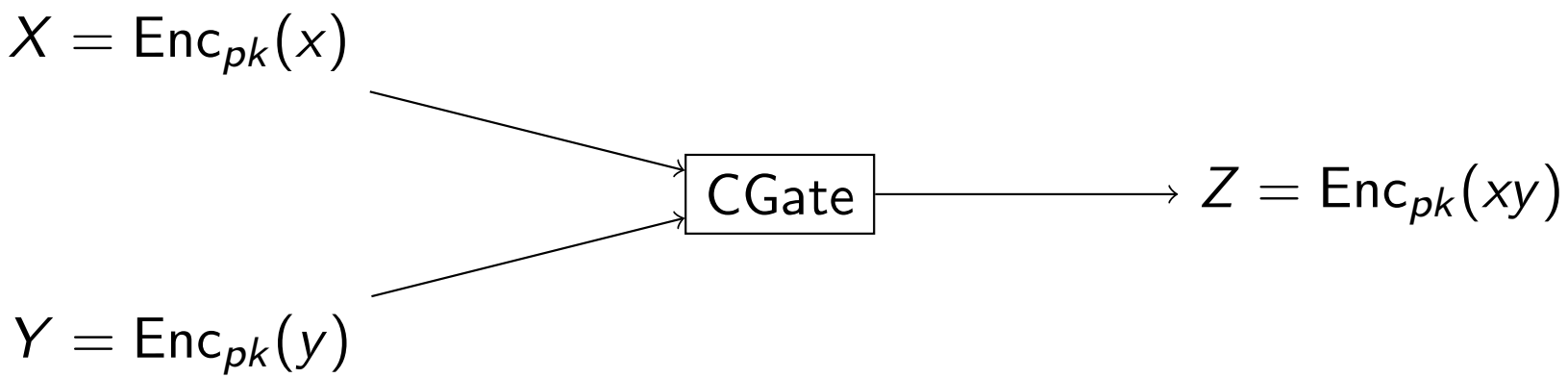
It allows logical operations on encrypted bits.

(Primitive adapted from Shoenmakers and Tuyls, Asiacrypt'04.)

Not gate: $\mathrm{Not}(B) = \mathrm{Enc}(1)/B \equiv \mathrm{Enc}(1-b)$

Multi-party computation

We use the CGate primitive to build our MPC protocols:

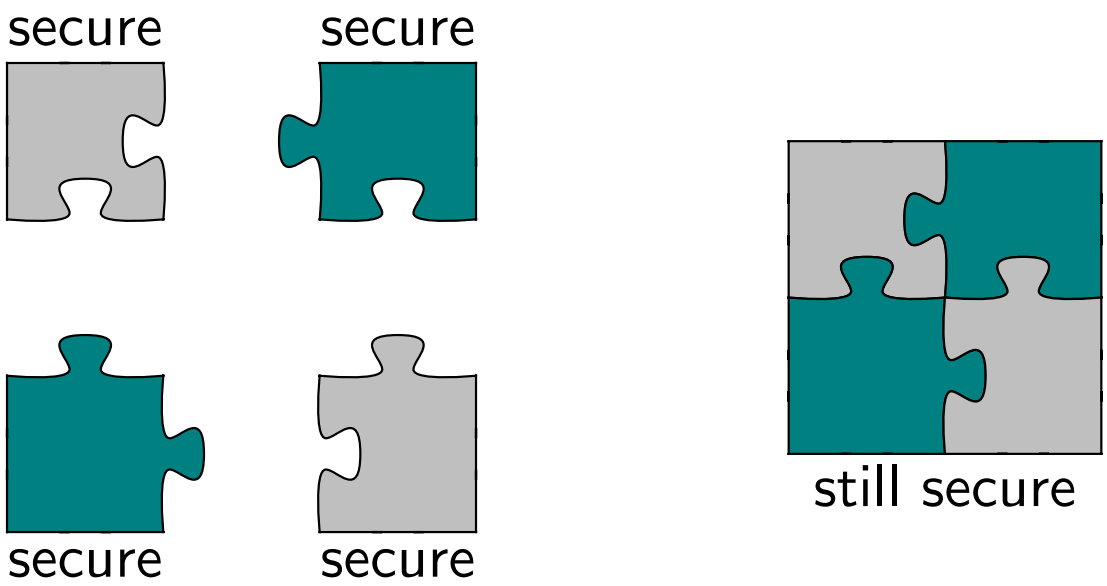


It allows logical operations on **encrypted bits**.

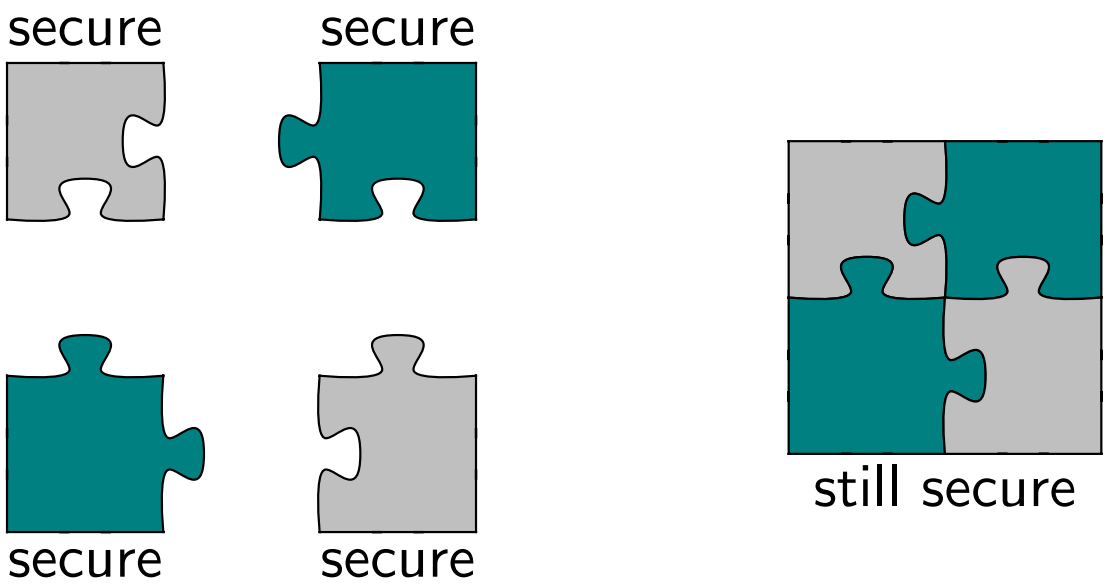
(Primitive adapted from Shoenmakers and Tuyls, Asiacrypt'04.)

Not gate: $\mathrm{Not}(B) = \mathrm{Enc}(1)/B \equiv \mathrm{Enc}(1-b)$

Universally composable security



Universally composable security



We use the security framework of Canetti, Cohen and Lindell, Crypto'15.

Our Contribution

A generic toolbox for complete tally hiding in ElGamal.

Operation	Comment
Basic	$+, -, x$
Fixed-point division	$/$
Comparisons	$\leq, <, =$

Our Contribution

A generic toolbox for complete tally hiding in ElGamal.

Operation	Comment
Basic	$+, -, x$
Fixed-point division	$/$
Comparisons	$\leq, <, =$
Conditionals	(for branch-freeness)
$\vdots$	$\vdots$

Our Contribution

A generic toolbox for complete tally hiding in ElGamal.

Operation	Comment
Basic	$+, -, x$
Fixed-point division	$/$
Comparisons	$\leq, <, =$
Conditionals	(for branch-freeness)
$\vdots$	$\vdots$

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

All of those come with several optimizations and trade-offs.

Our Contribution

A generic toolbox for complete tally hiding in ElGamal.

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 in ElGamal.

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 in ElGamal.

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 in ElGamal.

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 in ElGamal.

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**

Another counting function? We can do it!

Thank you!

Security proofs:

- Privacy
- Verifiability
- UC-security

Complete algorithmic description:

- Optimizations and trade-offs
- Original ballot encodings

Full version available on eprint:
eprint.iacr.org/2021/491

New algorithms:

- Majority Judgment
- Homomorphic Condorcet

Implementation:

- Condorcet-Schulze
- It is fast!