RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: CRYP-F03

A Non-Interactive Shuffle Argument With Low Trust Assumptions

Antonis Aggelakis, Prastudy Fauzi, Georgios Korfiatis, Panos Louridas, Foteinos Mergoupis-Anagnou, Janno Siim, Michal Zajac

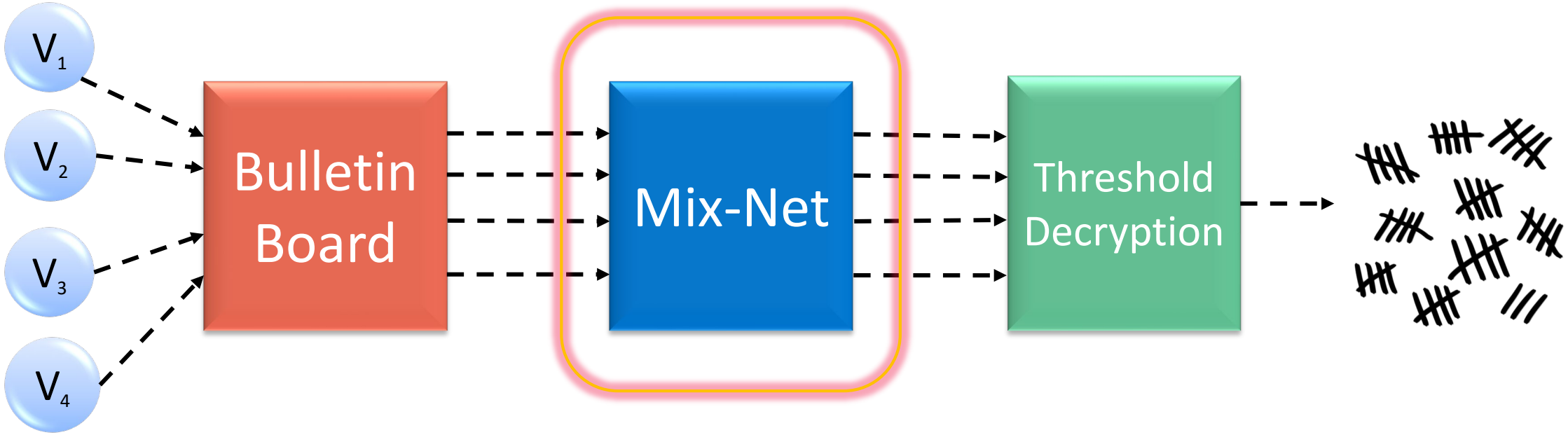
Janno Siim

Junior Research Fellow in Cryptography
University of Tartu

RSAConference2020

Motivation

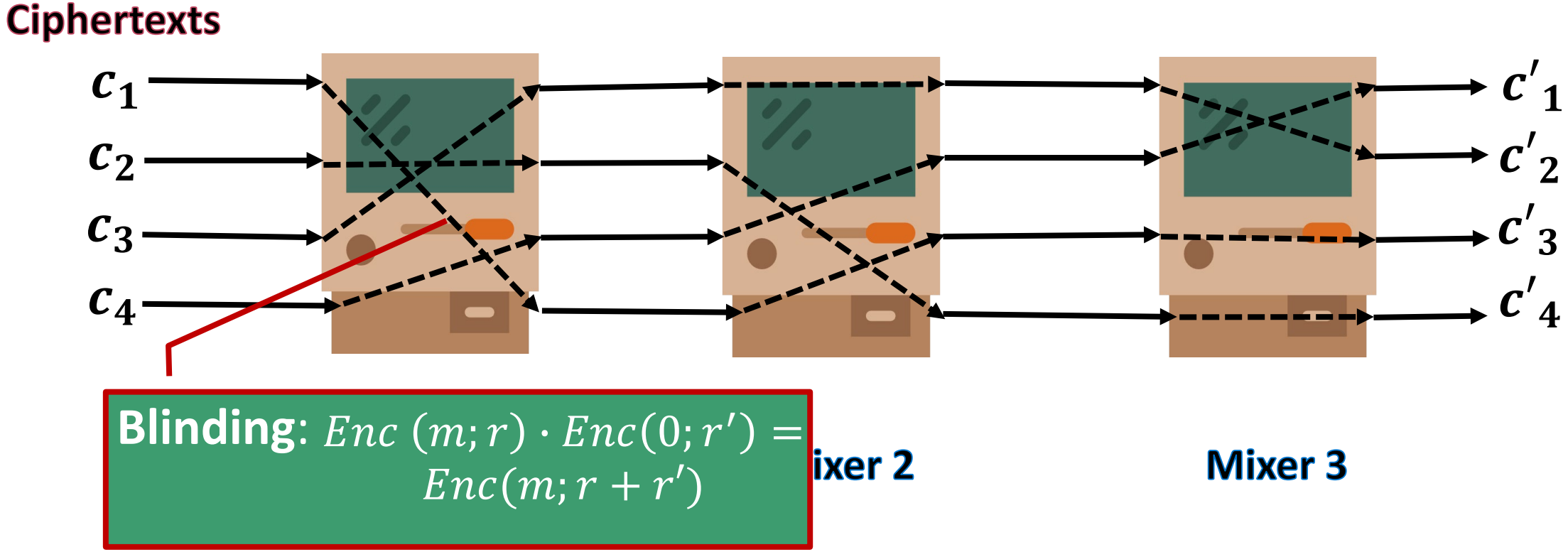
Internet Voting



Voters

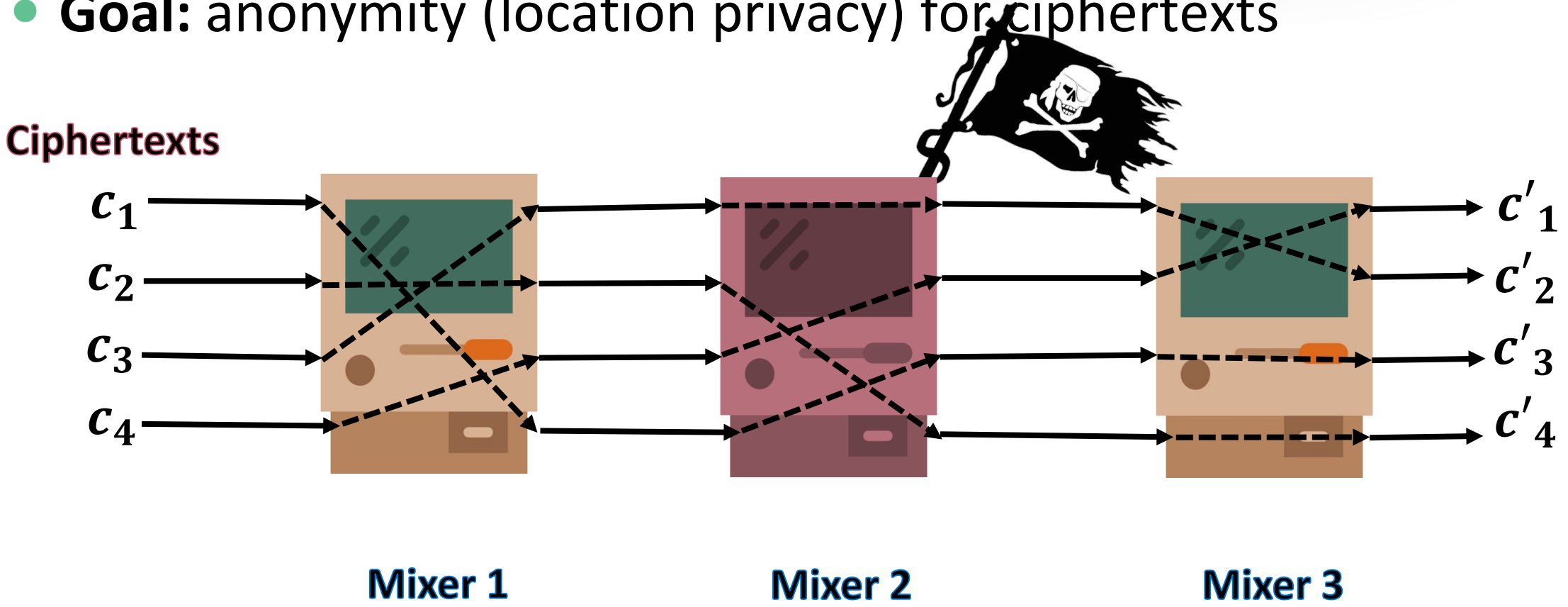
Mix-Net

- **Goal:** anonymity (location privacy) for ciphertexts



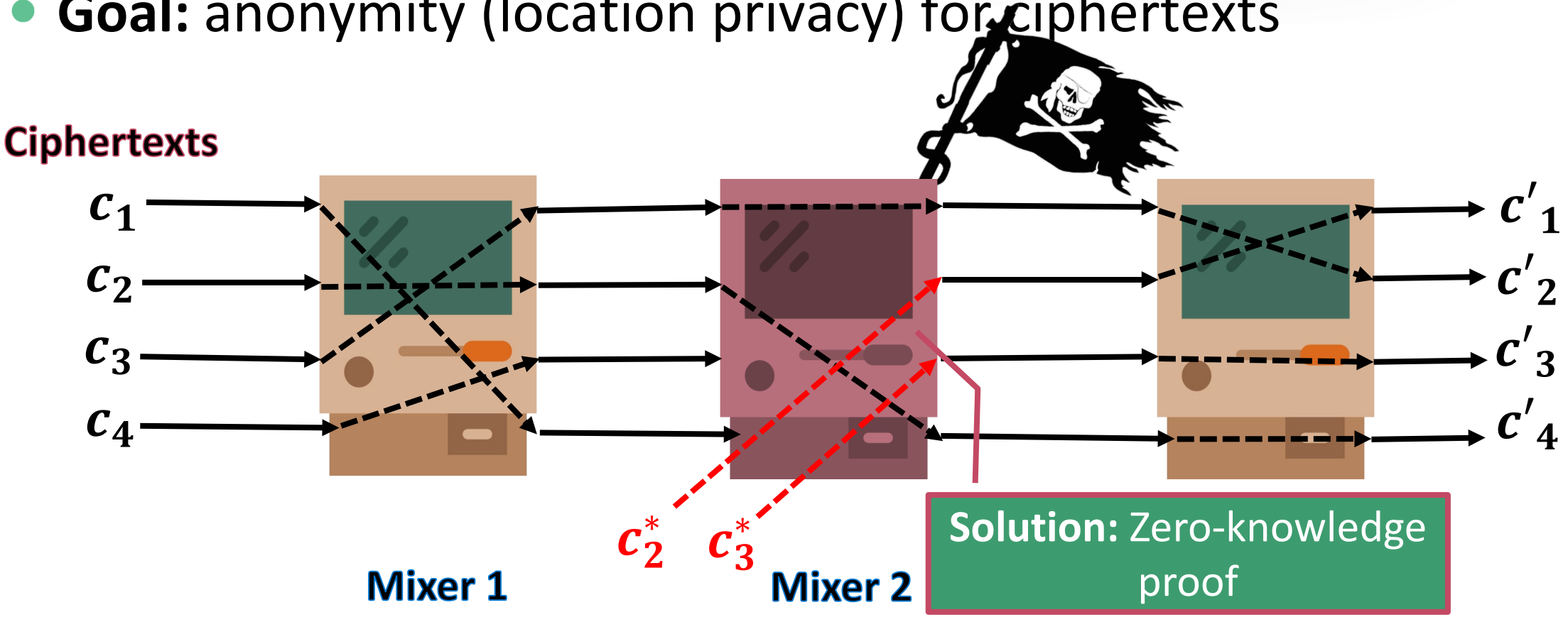
Mix-Net

- **Goal:** anonymity (location privacy) for ciphertexts



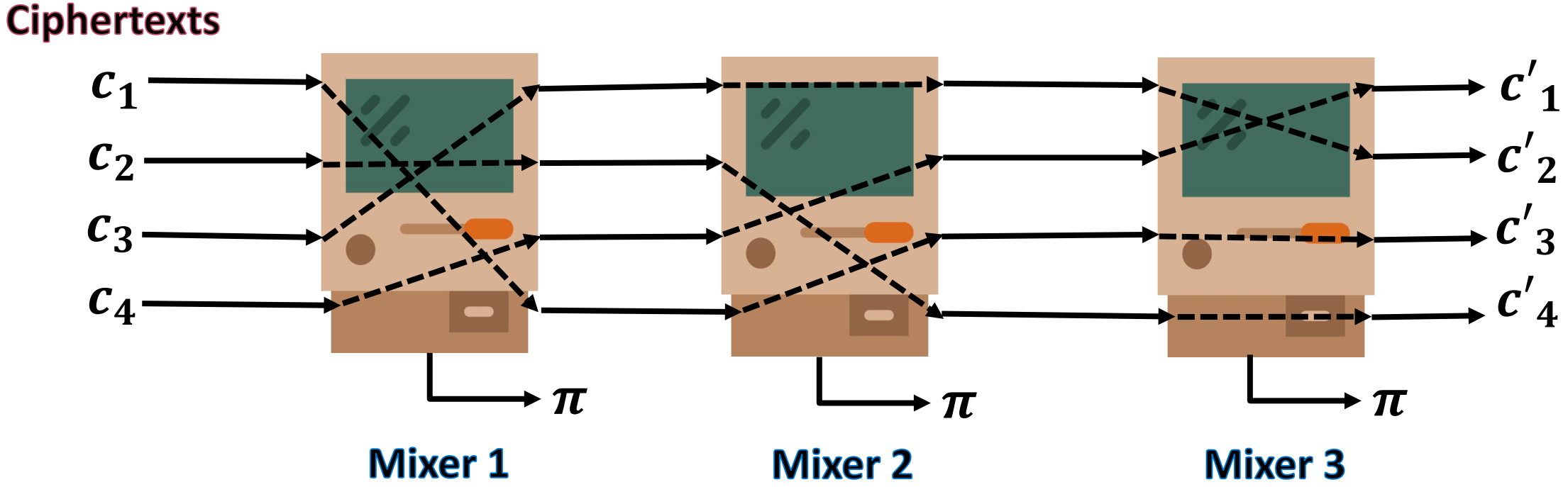
Mix-Net

- **Goal:** anonymity (location privacy) for ciphertexts



Mix-Net

- **Goal:** anonymity (location privacy) for ciphertexts



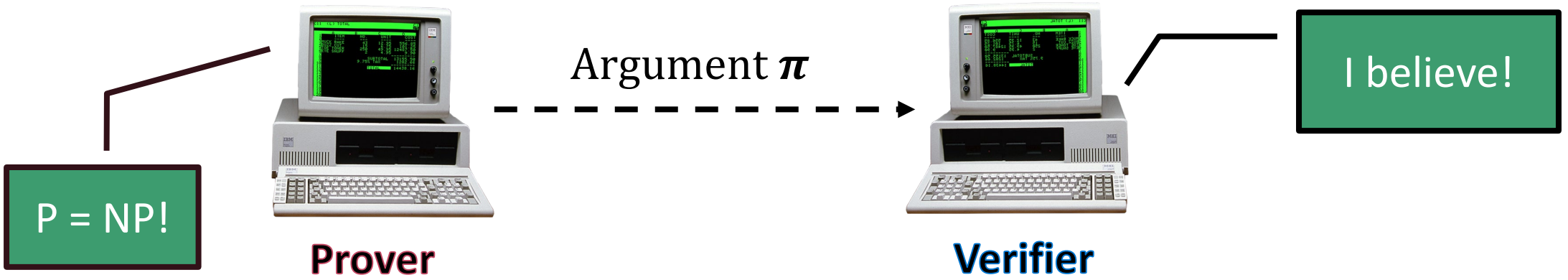
RSAConference2020

Zero-Knowledge Arguments

Zero-Knowledge Proof/Argument

Protocol between **Prover** and **Verifier** where

- **Prover** proves to **Verifier** validity of some statement (soundness)
- **Prover** does not leak **any** information besides validity (zero-knowledge)



More formally …

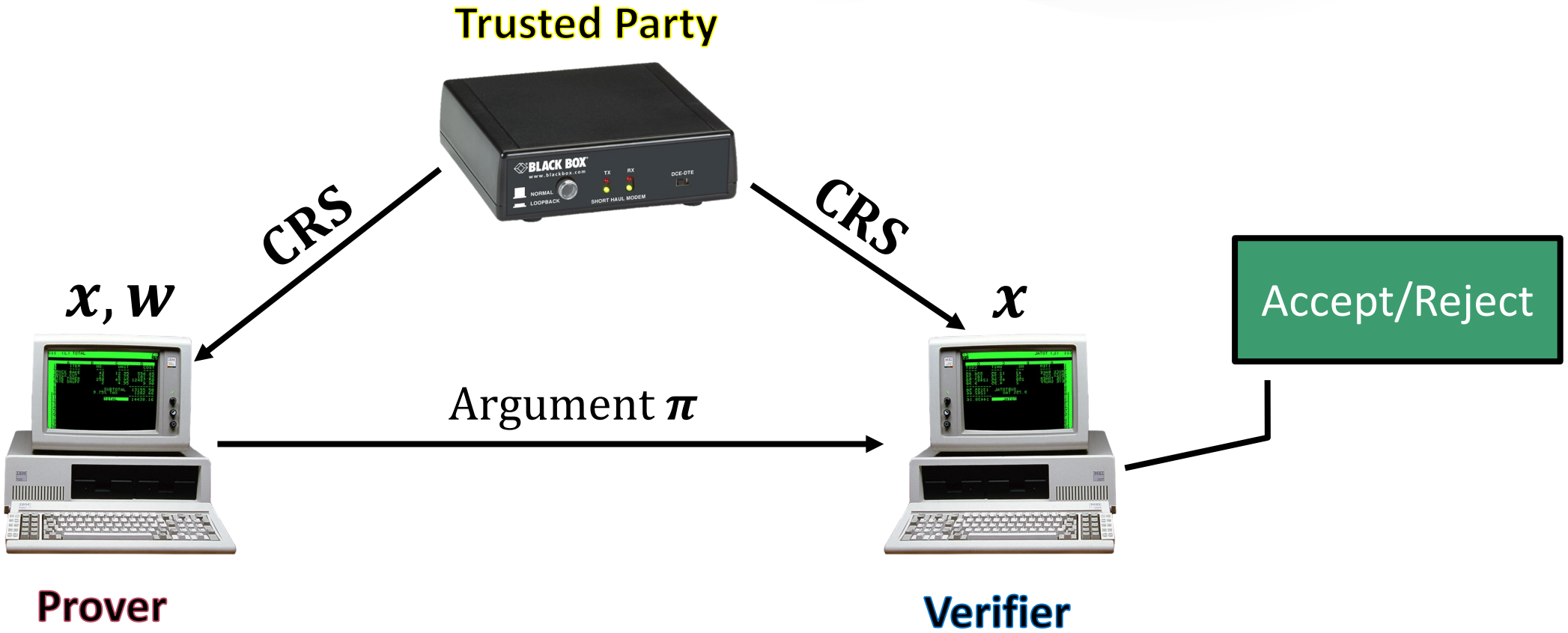
- Fix an **NP**-Language $\mathcal{L}$
- **Prover** claims $x \in \mathcal{L}$
- Honest **Prover** knows witness w for x
- Properties:
  - ***Completeness*** – honest **Prover's** argument is accepted
  - ***Soundness*** – computationally hard to find accepting proof for $x \notin \mathcal{L}$
  - ***Zero-Knowledge*** – proof can be simulated with a trapdoor

Shuffle Arguments

Best (non-interactive) shuffle arguments either require

- Random oracle model
  - Only a security heuristic 
- Common reference string (CRS) model
  - Trust in the setup phase 

CRS Model


Trusted Party
CRS
CRS
x, w
x
Accept/Reject
Argument π
Prover
Verifier

Idea

- Take the ‘best’ CRS model shuffle
- Reduce trust requirements as much as possible
- Recent techniques
  - Distributed CRS generation
  - Subversion zero-knowledge

RSAConference2020

Our Construction

FLSZ17 Shuffle Argument

Starting point: Shuffle argument by Fauzi et al. (Asiacrypt 2017)

- CRS model but no RO model
- Relatively efficient:
  - 100,000 ciphertexts proving + verification time < 2.5min
- Strong assumptions and generic group model

Our Contributions

- Simplifications in structure
- Weaker assumptions:
  - Generic group model -> algebraic group model
  - Less specialized assumptions
- Less trust:
  - Modifications to CRS such that distributed CRS generation is possible (security with N-1 malicious parties)
  - CRS verification algorithm for zero-knowledge (ZK even with N malicious parties)

Pairings

- Bilinear groups: $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ of size p with generators $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_T$
- Additive notation & bracket notation:
  - $a \cdot \mathcal{P}_1 \coloneqq [a]_1$
  - $a \cdot \mathcal{P}_2 \coloneqq [a]_2$
  - $a \cdot \mathcal{P}_T \coloneqq [a]_T$
- Bilinear map: $[a]_1 \bullet [b]_2 = [ab]_T$

Structure

Prove that commitment C opens to $(0, \dots, 0,1,0, \dots 0)$

Unit Vector Argument

ZK: unconditional
Knowledge soundness: power DL assumption in algebraic group model

Power DL: Given elements $[x, \dots, x^d]_1$ find x

Structure

Prove that commitments $C_1, \ldots C_n$ open to a permutation matrix

Unit Vector Argument

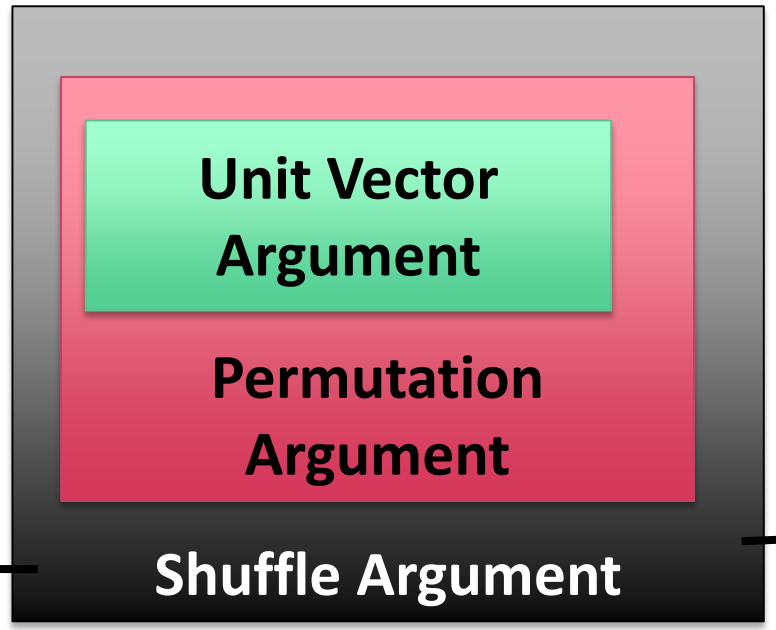
Permutation Argument

ZK: unconditional
Knowledge soundness: if unit vector argument is KS & commitment is binding

$$C_1 \xrightarrow{\text{opens}} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$C_2 \xrightarrow{\text{opens}}$$
$$C_3 \xrightarrow{\text{opens}}$$

Structure

- Commit to permutation matrix
- Give permutation argument
- Show that permutation was used for shuffling



ZK: unconditional
Soundness: if permutation argument is KS & (variation of) KerMDH assumption holds

KerMDH: Given matrix $[M]_1$ find non-zero $[x]_2$ s.t. $M^T x = 0$

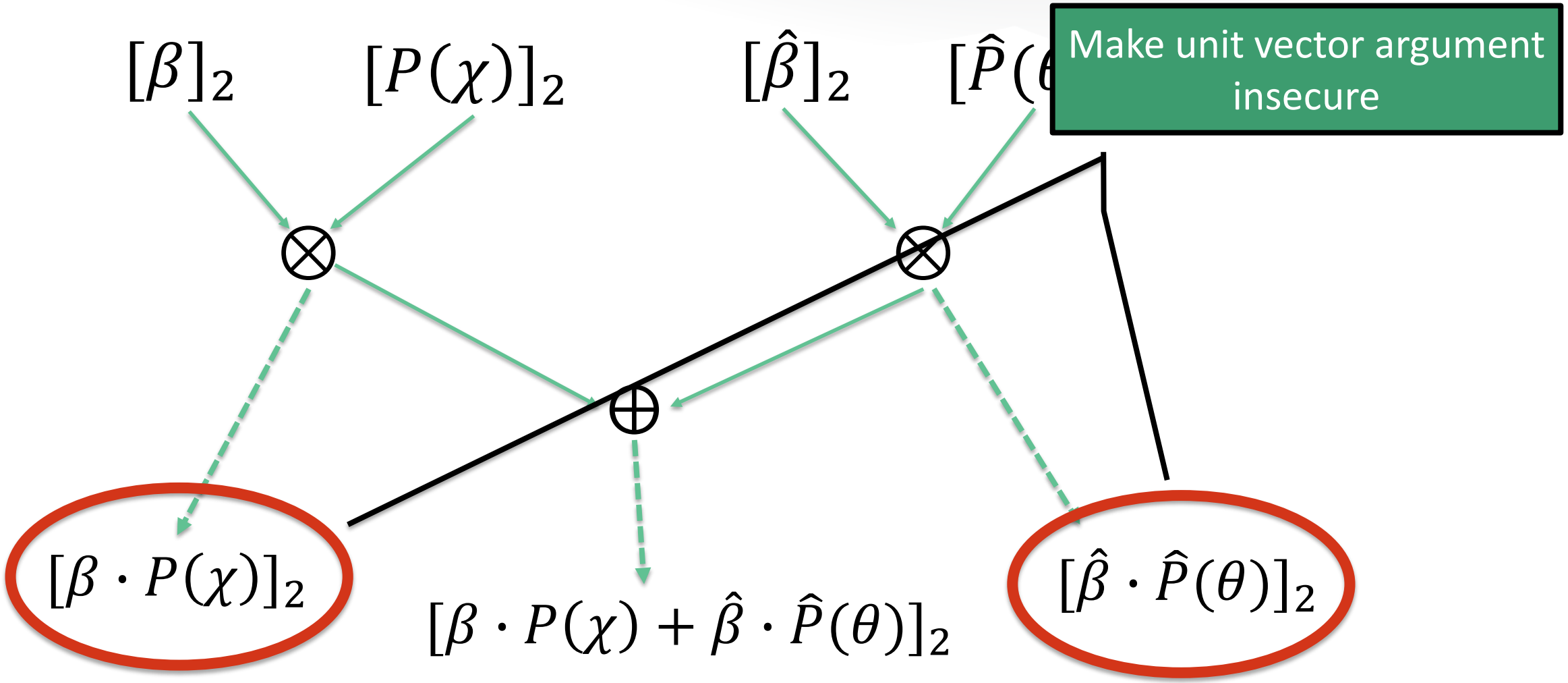
Distributed CRS Generation

- Ben-Sasson et al. (S&P 15) and Abdolmaleki et al. (Africacrypt 19) proposed specialized CRS generation protocols
- Very efficient
- Tolerates N-1 malicious parties
- But only for specific pairing-based arguments
- Not directly applicable for FLSZ17 shuffle 

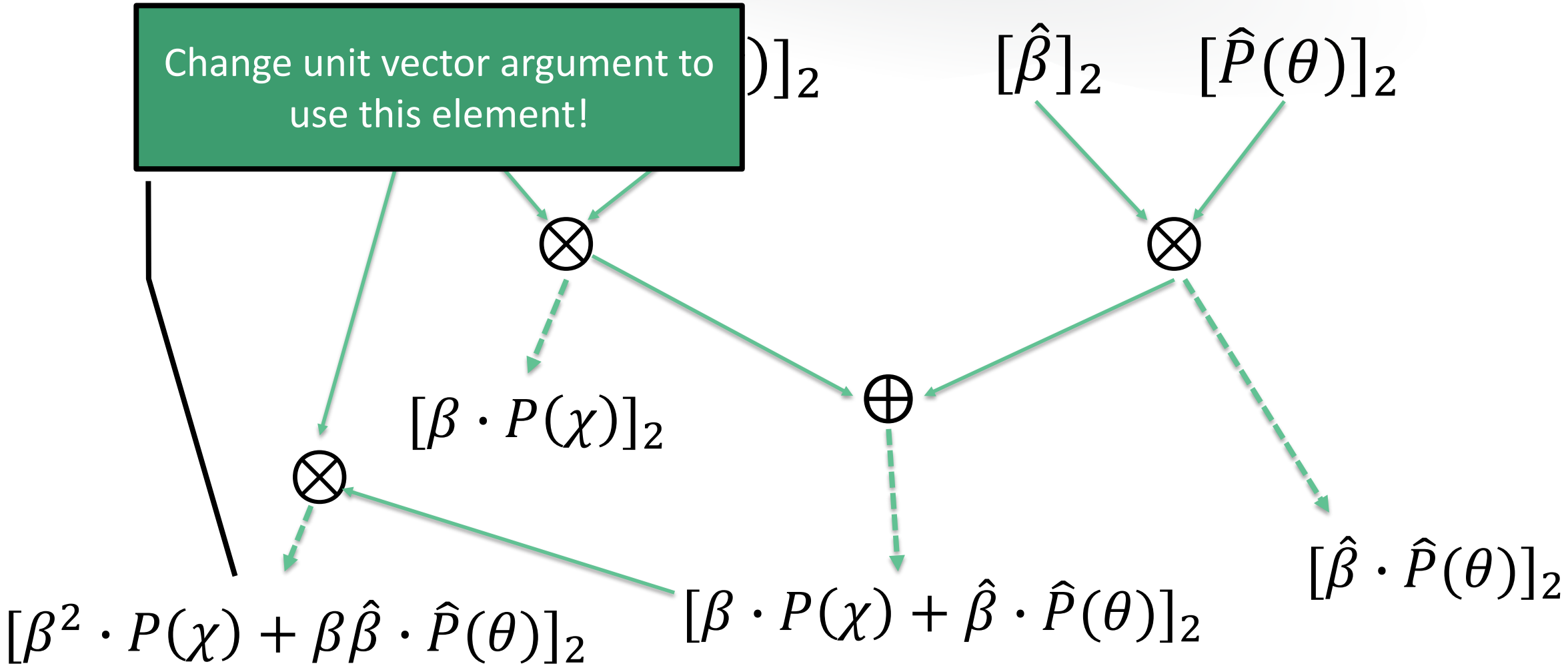
Modification to CRS

- Need to modify CRS of FLSZ17
- Lots of ad-hoc tricks
- Example:
  - $[\beta \cdot P(\chi) + \hat{\beta} \cdot \hat{P}(\theta)]_2$ where $\beta, \hat{\beta}, \theta \in \mathbb{Z}_p$ and $P(X)$ and $\hat{P}(Y)$ are polynomials
  - CRS generation requires that computation is done one multiplication and addition at the time

Example Continued



Example Continued



Subversion Zero-Knowledge

- Zero-knowledge even if CRS is malicious
- Idea from Bellare et al. (AC 2016) and Abdolmaleki et al. (AC 2017)
  - Prover verifies well-formedness of CRS
  - In security proof trapdoor is extracted with knowledge assumption

Example: well-formedness check

- Suppose $[\beta^2]_1$, $[P(\chi)]_2$, $[\beta\hat{\beta}]_1$, $[\hat{P}(\theta)]_2$ have been verified
- Then check that

$$[\beta^2]_1 \bullet [P(\chi)]_2 + [\beta\hat{\beta}]_1 \bullet [\hat{P}(\theta)]_2 = [1]_1 \bullet [\beta^2 \cdot P(\chi) + \beta\hat{\beta} \cdot \hat{P}(\theta)]_2$$

- Knowledge assumption: If adversary outputs $[\theta]_1$, $[\theta]_2$, then he knows θ

Prototype Implementation

- By GRNET team
- Zeus I-voting system
- https://github.com/grnet/lta_shuffle

Conclusion

- Improvement over state-of-the-art shuffle argument
- Reorganizing structure and weaker assumptions
- CRS generation protocol and verification algorithm:
  - Soundness holds if at least 1 party is honest
  - ZK holds even if all parties are malicious

RSAConference2020

Questions