Robustness Modelling and Verification of a Mix Net Protocol

Stathis Stathakidis, Steve Schneider and James Heather

Department of Computing, University of Surrey, UK

SSR 2014, RHUL, 16 December 2014

Outline

- Mix Nets
- Standards
- Ximix: a Mix Net Implementation
- Formal Modelling and Verification
- Conclusion

Mix Nets

- Cryptographic protocol
- Unlinks the correspondence between its input and output messages
- Untraceable electronic mail (Chaum, 1981)
- Electronic voting, cash payments, anonymous Web browsing (Tor), RFID tags etc.

Mix Nets

Inputs: vector of encrypted messages (ciphertexts)

Outputs: vector of permuted plaintexts

Mix Nets

Inputs: vector of encrypted messages (ciphertexts)

Outputs: vector of permuted plaintexts

Mix Nets

Inputs: vector of encrypted messages (ciphertexts)

Outputs: vector of permuted plaintexts

Mix Nets

- Use a number of mix servers to distribute trust
- Sequential execution
- Associated with a Web Bulletin Board (WBB) for posting the messages
- All communications via the WBB

Re-encryption Mix Nets

- Technique for introducing new randomness to a ciphertext
- A ciphertext is the composite of the message and a random value
- Only the external appearance is modified - the underlying message remains unaltered
- Important that messages are re-encrypted and shuffled before decryption

Re-encryption Mix Nets

- El Gamal cryptosystem (mostly)
- The Mix Net's public key is jointly generated
- The secret key is distributed to the mix servers

Re-encryption Mix Nets

- A threshold number of mix servers should combine to decrypt the final ciphertexts

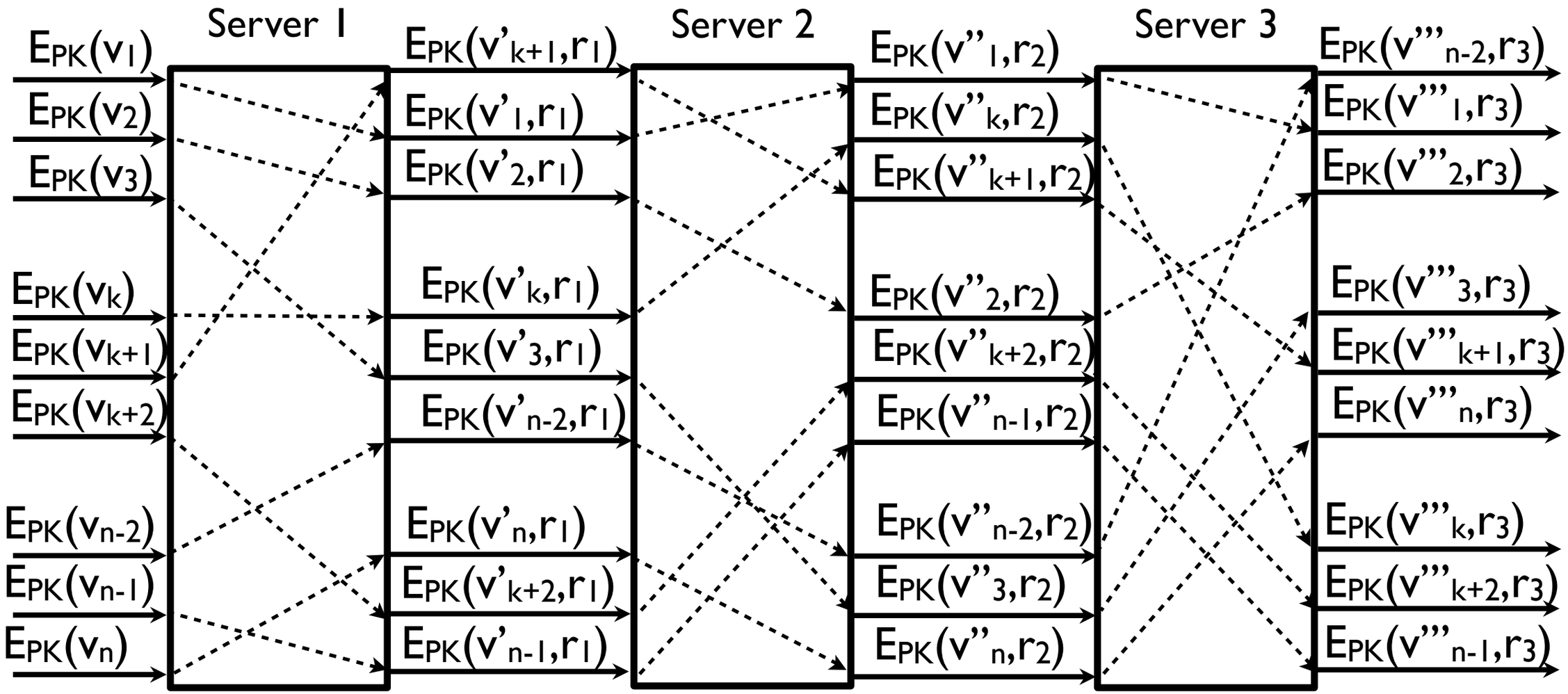
- Normally, a threshold is greater than two thirds (e.g. 3 out of 5)

- When decrypting, the output cannot be mapped back to an input (untraceability) provided at least one mix server is honest

- Operations should be publicly verifiable (zero-knowledge proofs)

Re-encryption Mix Nets

Mixing (anonymisation) phase

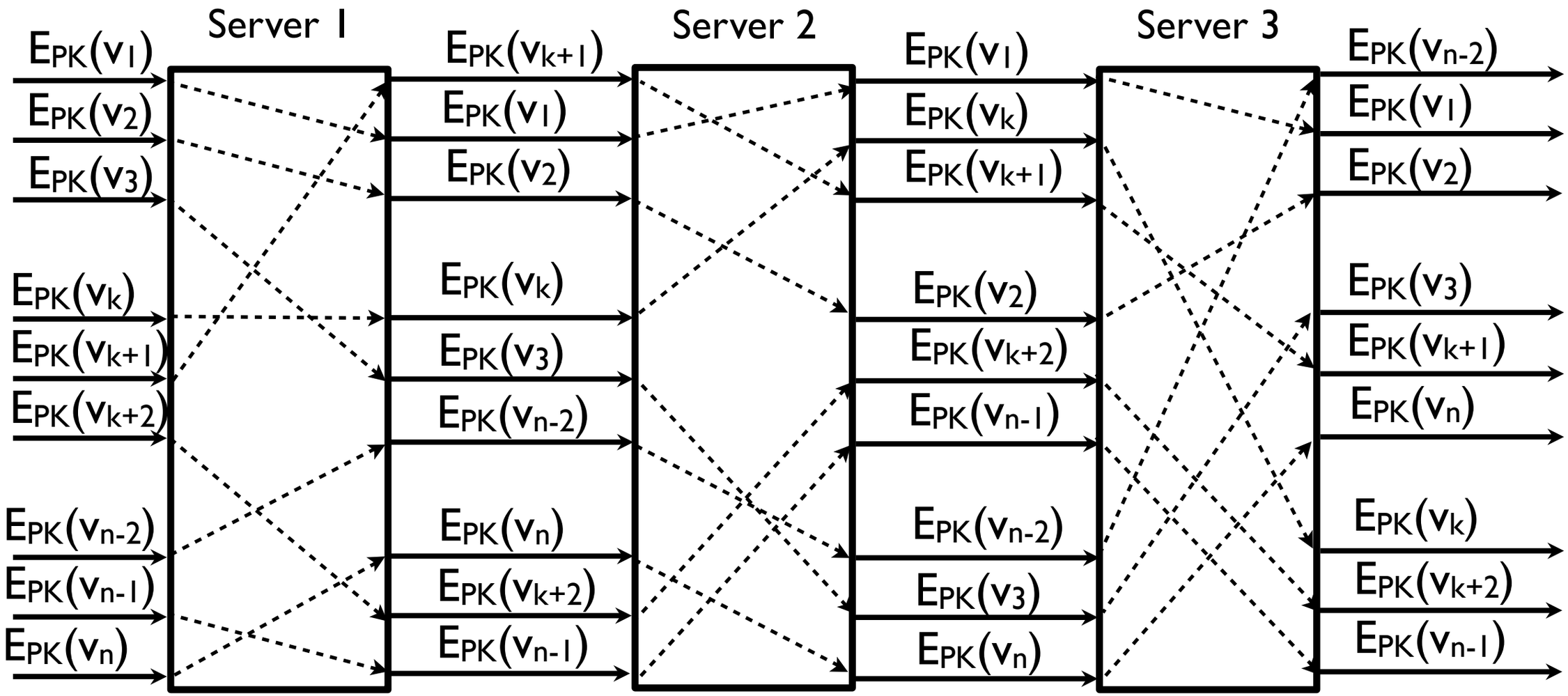


Shuffling and re-encryption with new randomness

Mix Net is private provided fewer than a threshold number of servers are dishonest

Re-encryption Mix Nets

Mixing (anonymisation) phase

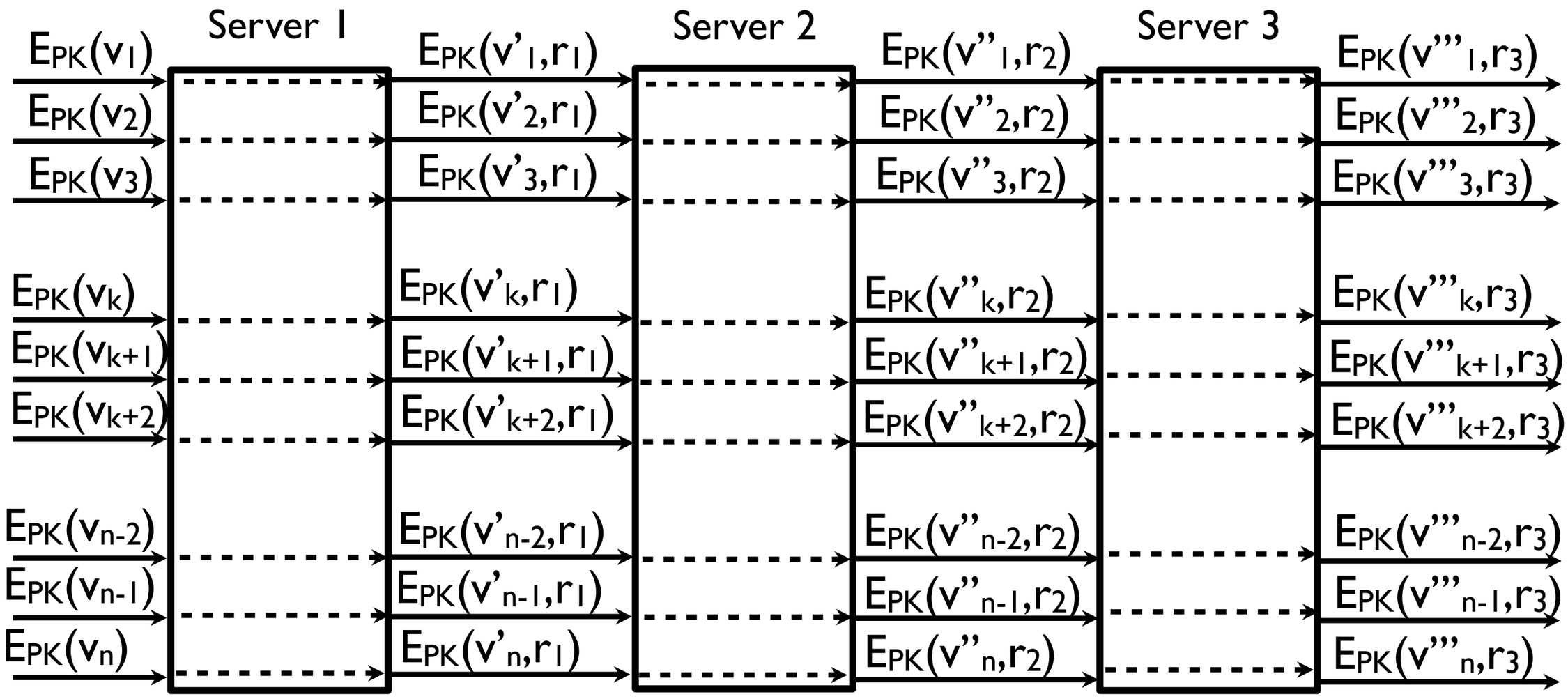


Shuffling without adding new randomness

Mix Net is not private

Re-encryption Mix Nets

Mixing (anonymisation) phase

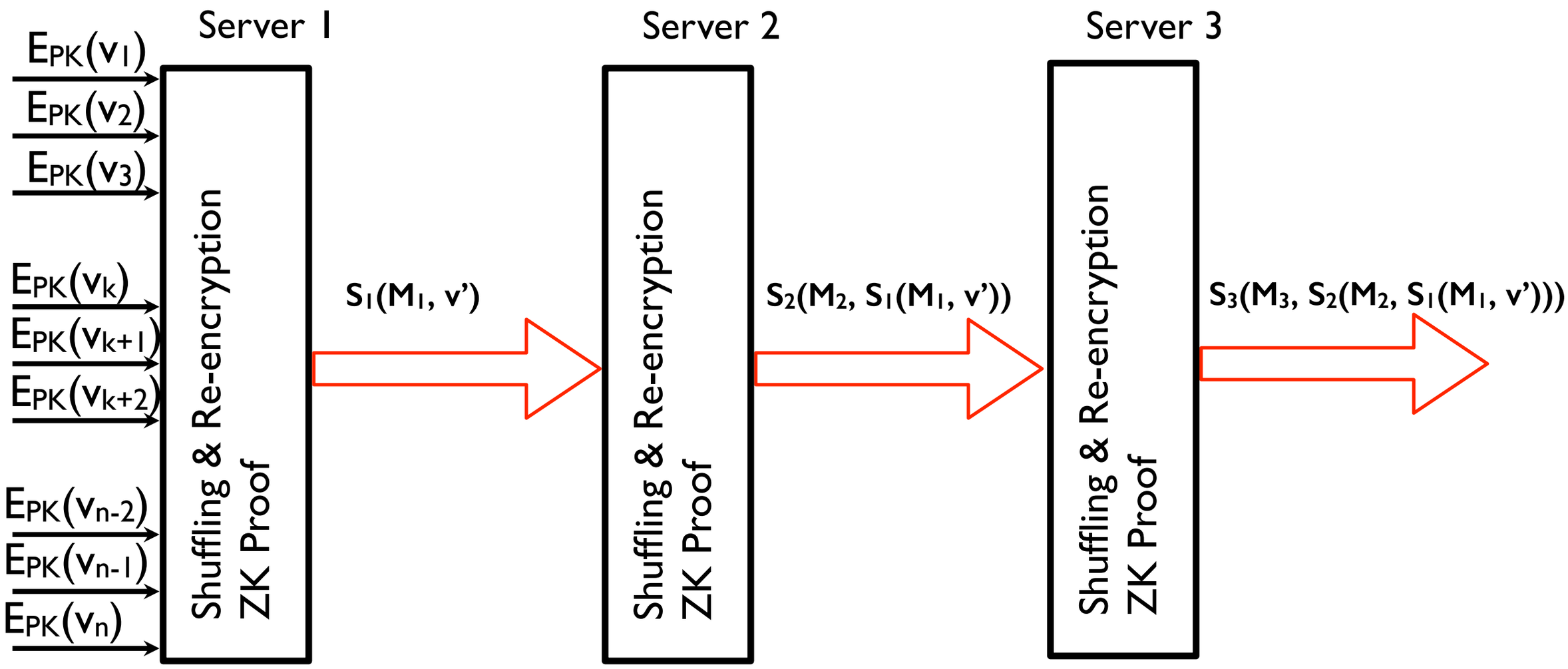


Re-encryption without shuffling

Mix Net is not private - mapping between submitted and plaintext values

Re-encryption Mix Nets

Mixing (anonymisation) phase



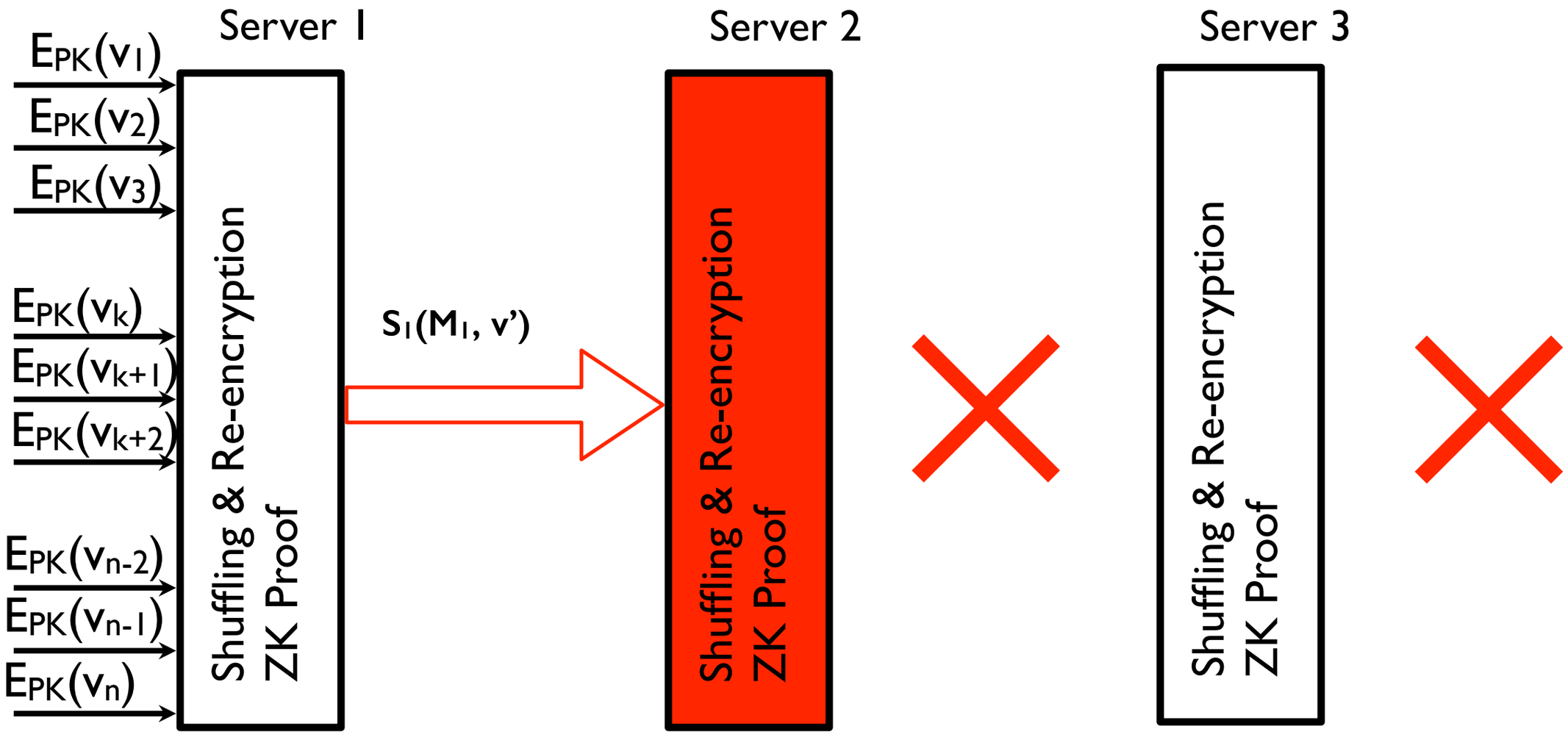
Unlinks the correspondence between its inputs and outputs

Privacy is maintained

Re-encryption Mix Nets

(most literature assumes all mix servers participate)

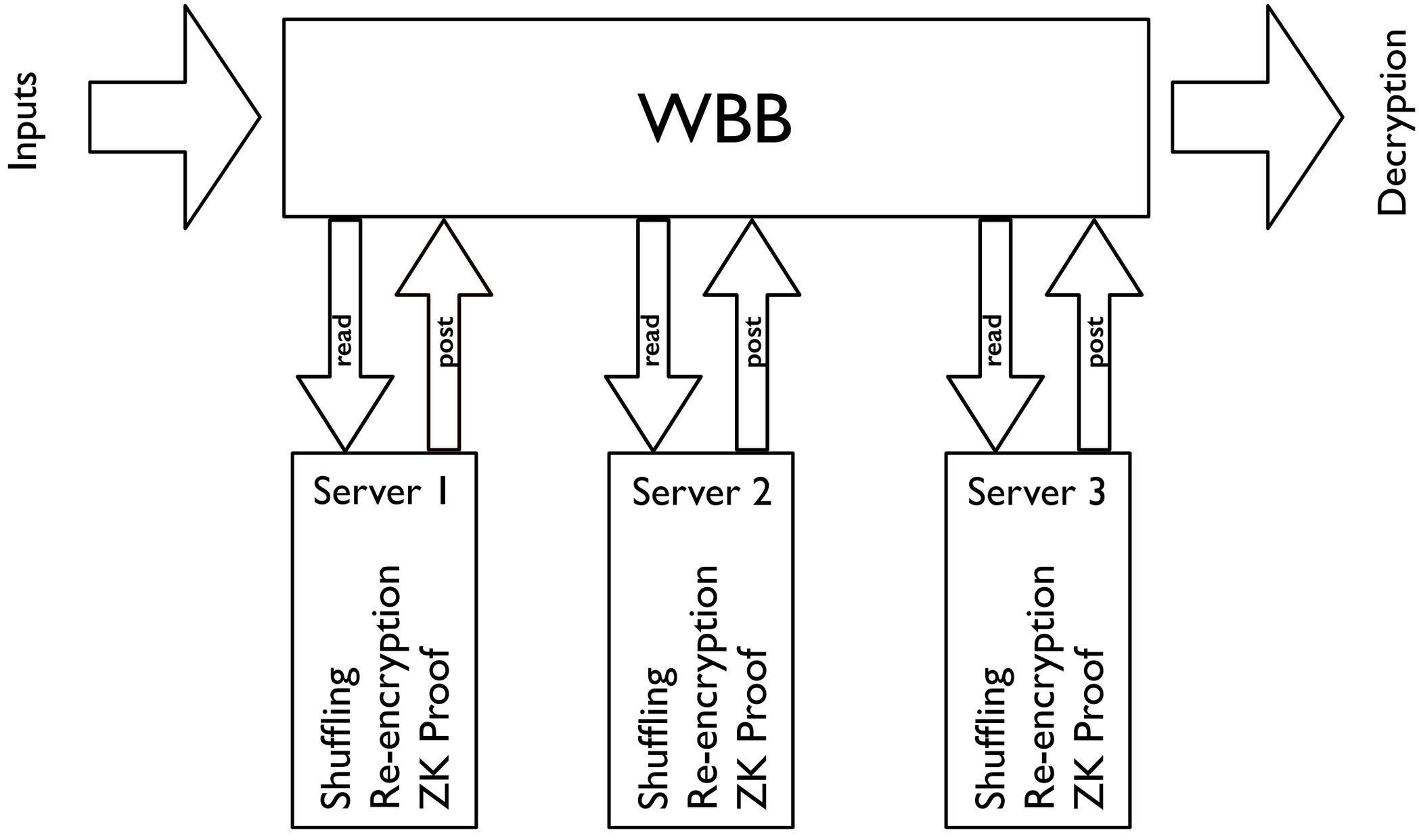
Mixing (anonymisation) phase



Server 2 refuses to participate

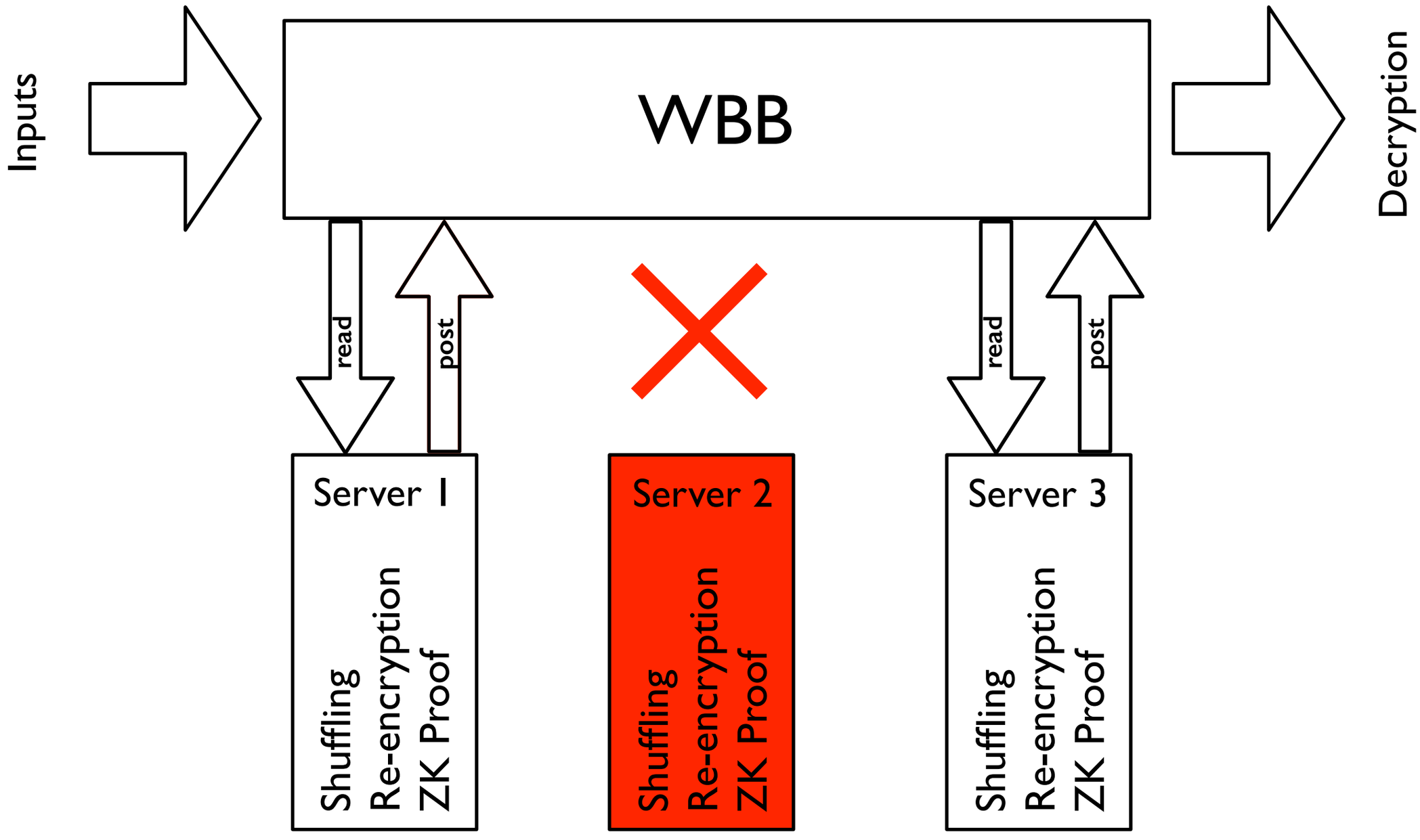
Mix Net is not robust - no output

Mix Nets - WBB



WBB is the communication medium (broadcast channel)

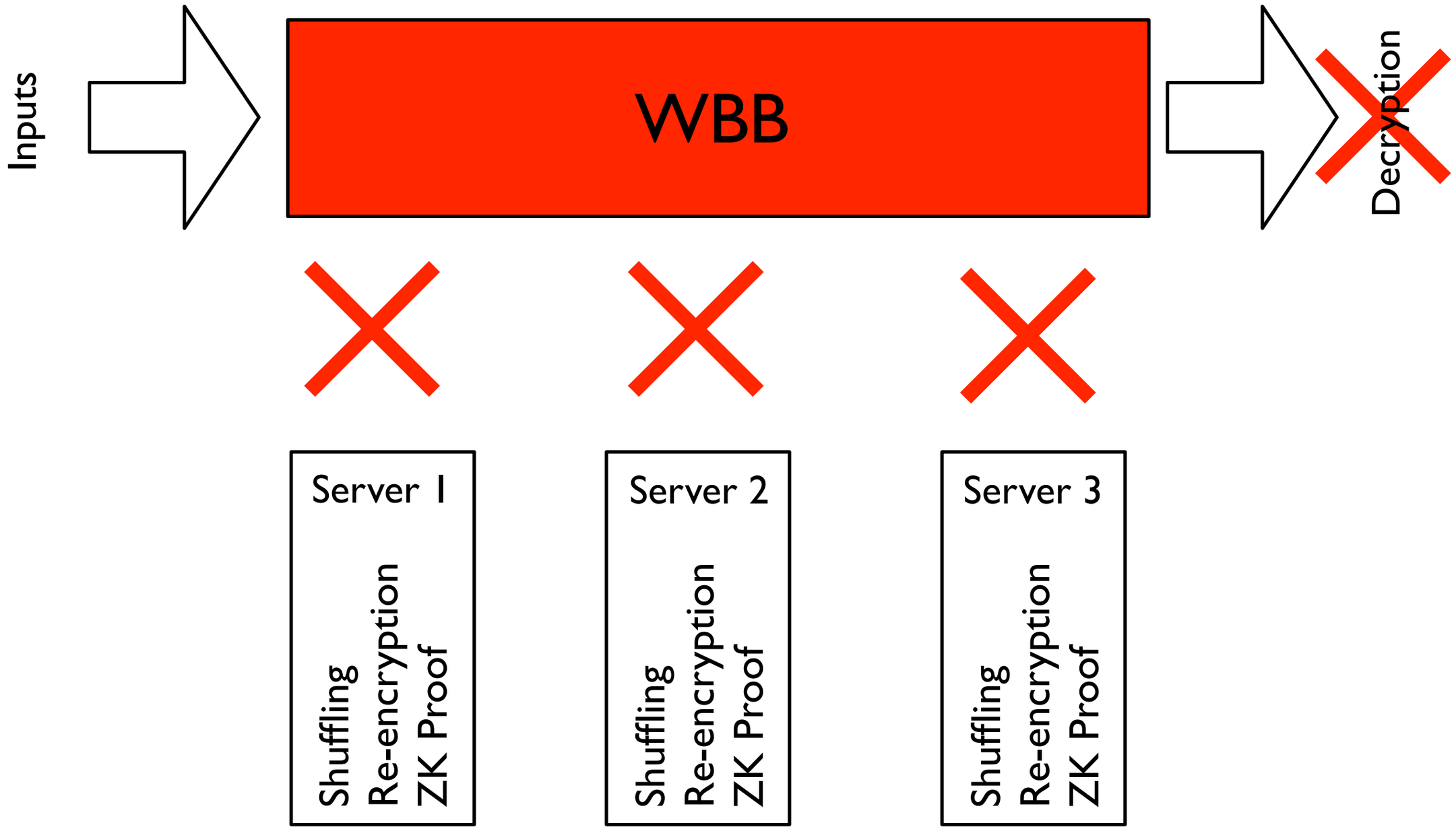
Mix Nets - WBB



Server 2 refuses to participate

Mix Net is still robust

Mix Nets - WBB



WBB is a single point of trust / failure

Mix Net is not robust

Issues for Standardisation

- Many different designs in the literature
- Not clear which security requirements are met
- Implementations are based on developers' interpretation of research proposals
- Omissions and deviations lead to security breaches

Issues for Standardisation

- Reference for future implementations
- Specific techniques will also become standardised
- Do not leave it up to the constructor to decide

Ximix - Introduction

- Elliptic Curve El Gamal re-encryption Mix Net
- Victoria State elections, Australia, November 2014
- Source code in Java
- Based on Randomised Partial Checking (RPC) auditing technique
- Combination of research papers

Ximix - Introduction

This work:

- Beta version (mid January 2014)
- Identified omissions and deviations from original proposals
- Formal modelling and verification against liveness
- Proposed sound solutions to problems

Ximix - Components

- Mix Servers
- Command Service (CS)
- Transient Boards (TB)
- Visible Board (VB)

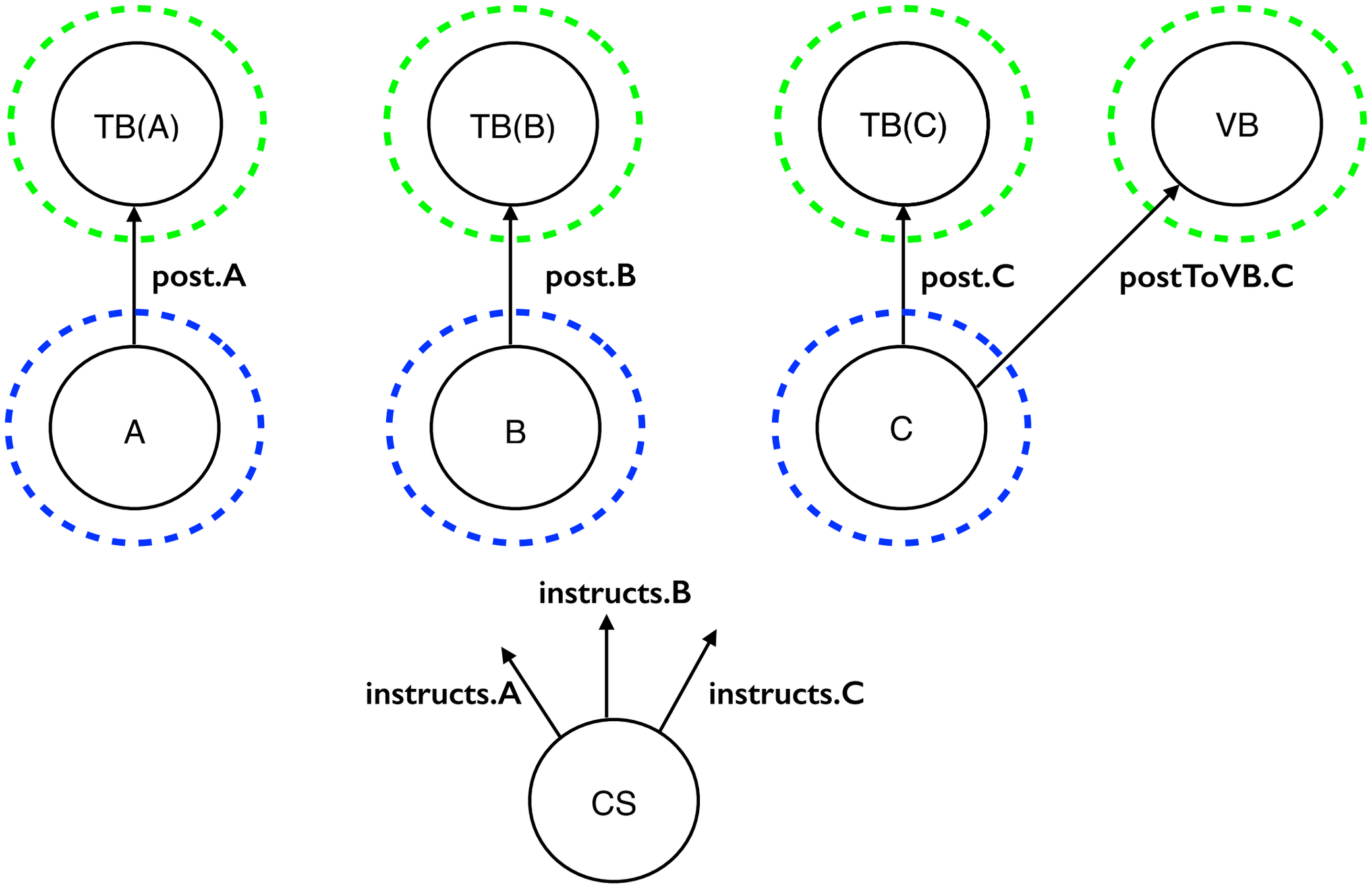
Ximix - Command Service

- Instructs mix servers to operate and create TBs to store data
- Selects the shuffle plan (order of execution)
- Assembles partially decrypted messages
- Great deal of power - controls the data flow
- Single point of trust / failure
- Ximix's robustness relies heavily on CS

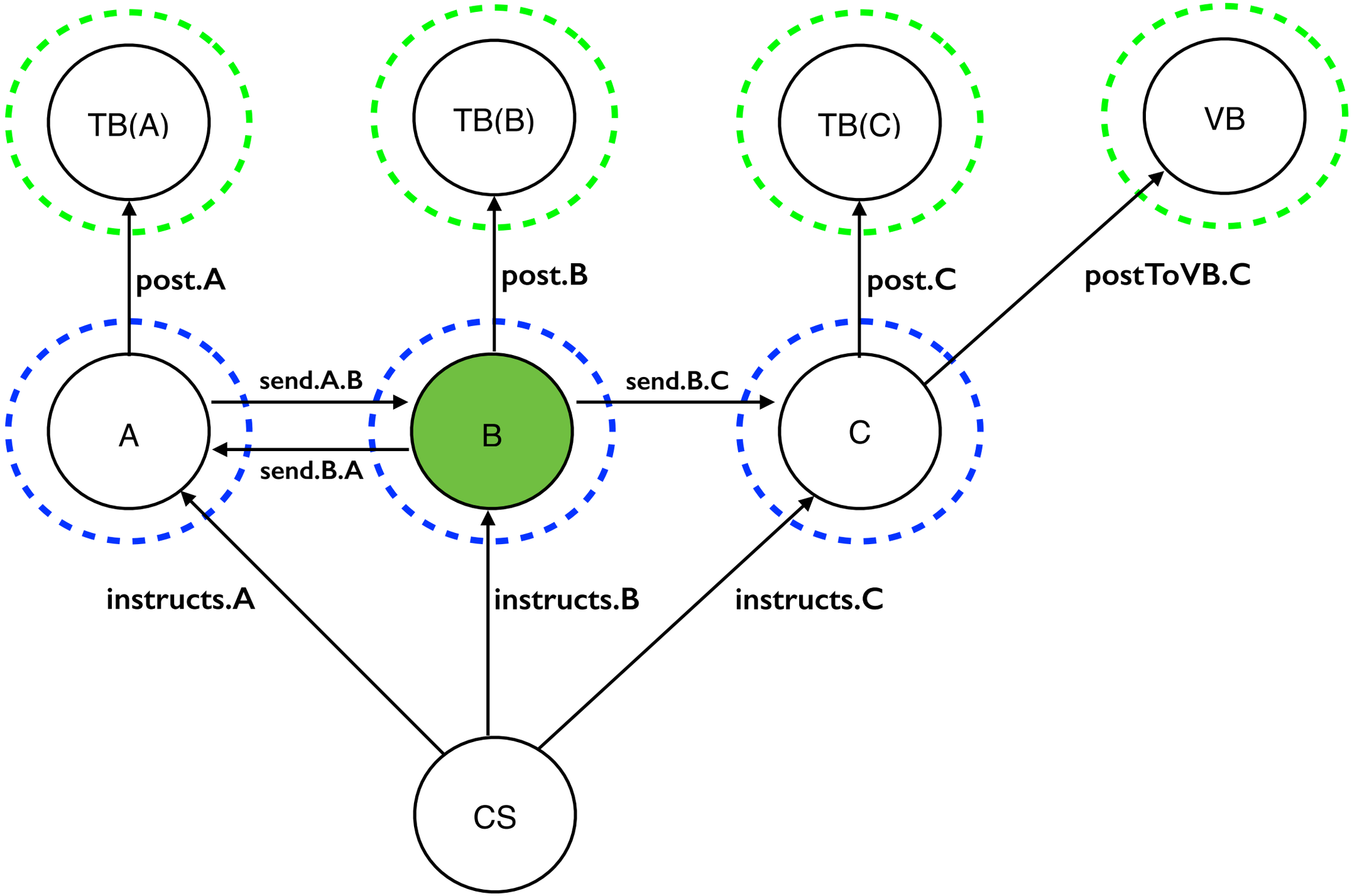
Ximix - Transient Board

- Internal to each mix server
- Allows read and post requests from the owner mix server
- Hosts intermediate results and commitments to secret permutations
- Blind on what posted to the other TBs

Ximix - Components



Ximix - Data Flow



Ximix - Found Deviations from RPC

- CS - mix servers do not check the integrity of the instructions
- Use of TBs
- Interactive zero-knowledge proofs
- Only the data produced by the last mix server is posted on the VB

Ximix - Problems

- Follow instructions without asset their correctness - give out more than half input/output correspondence - violate secrecy

- Failure to prove correctness of the operation to a third party - violate public verifiability

- The CS does not post the commitments/challenges - violate public verifiability

- The mix servers post their intermediate results only locally

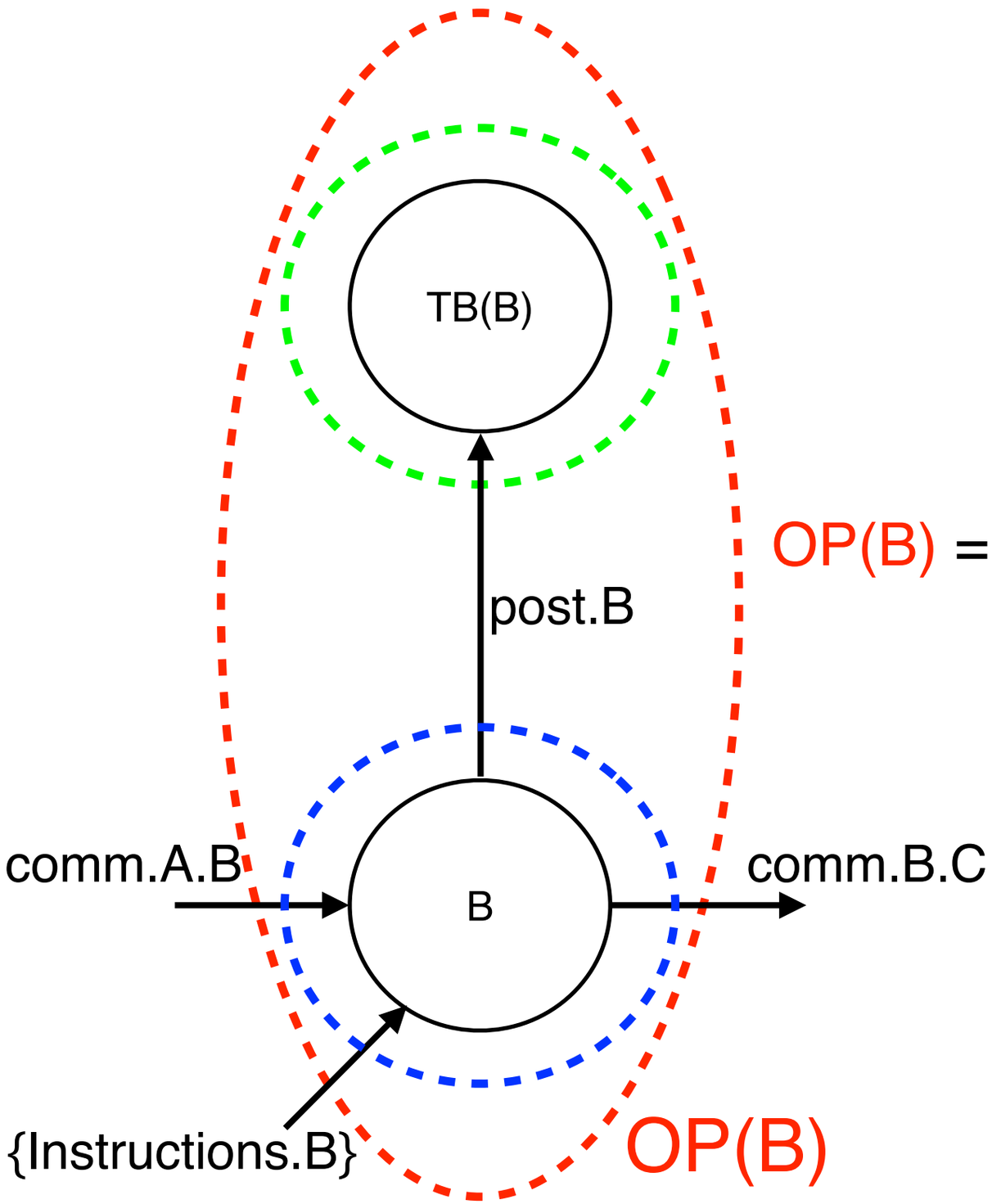
Ximix - Formal Analysis

- Faithful model of Ximix (beta version)
- Strong intruder based on the Dolev-Yao model
- Found attacks
- Solutions to make Ximix robust

Ximix - Formal Analysis - Approach

- Use of the process algebra CSP and the model checker FDR
- Cryptographic primitives are treated as symbolic operations
- Each component is modelled as an individual process
- Synchronous communications

Ximix - Formal Analysis - Approach

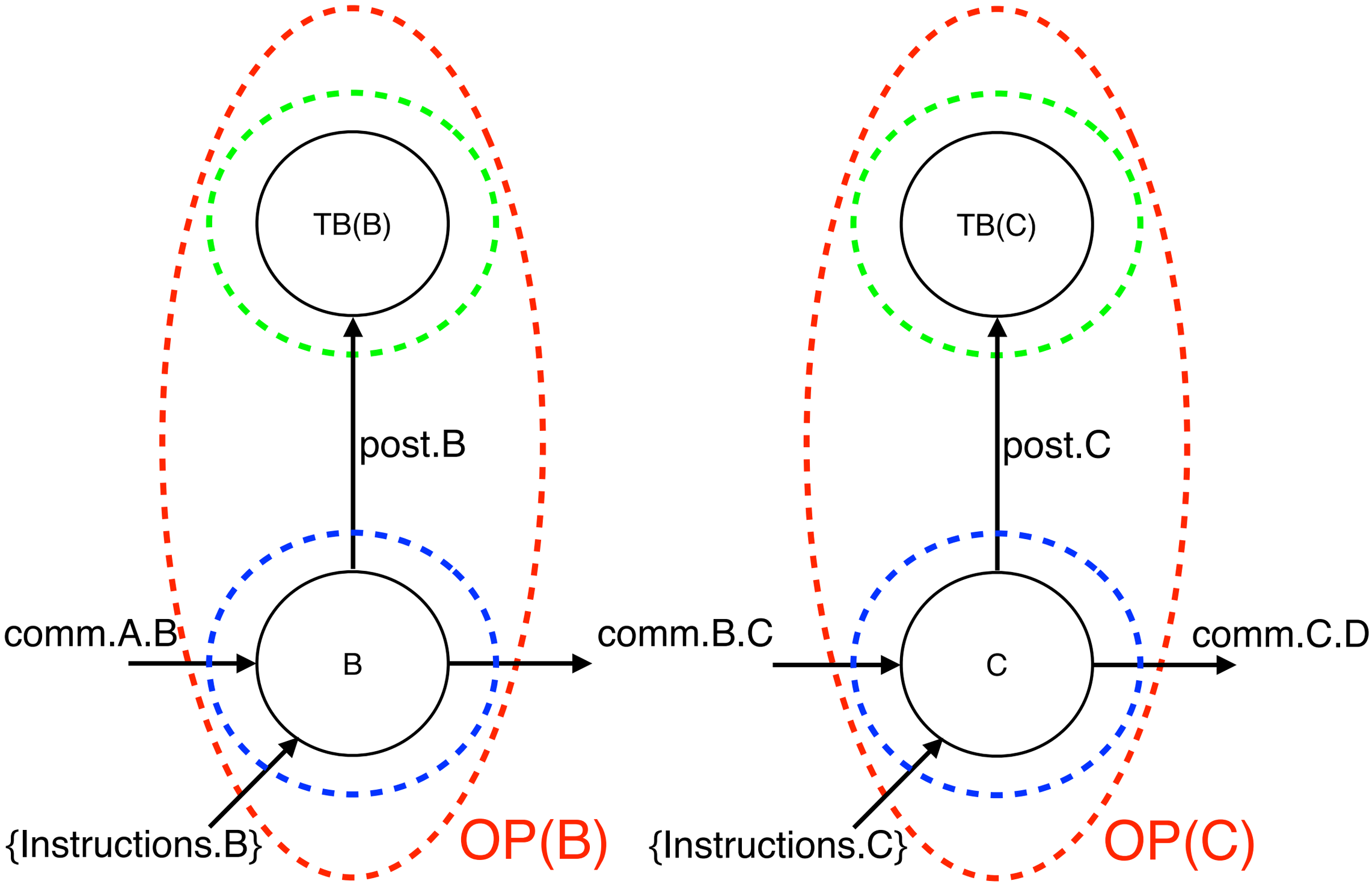


SERVER(B)

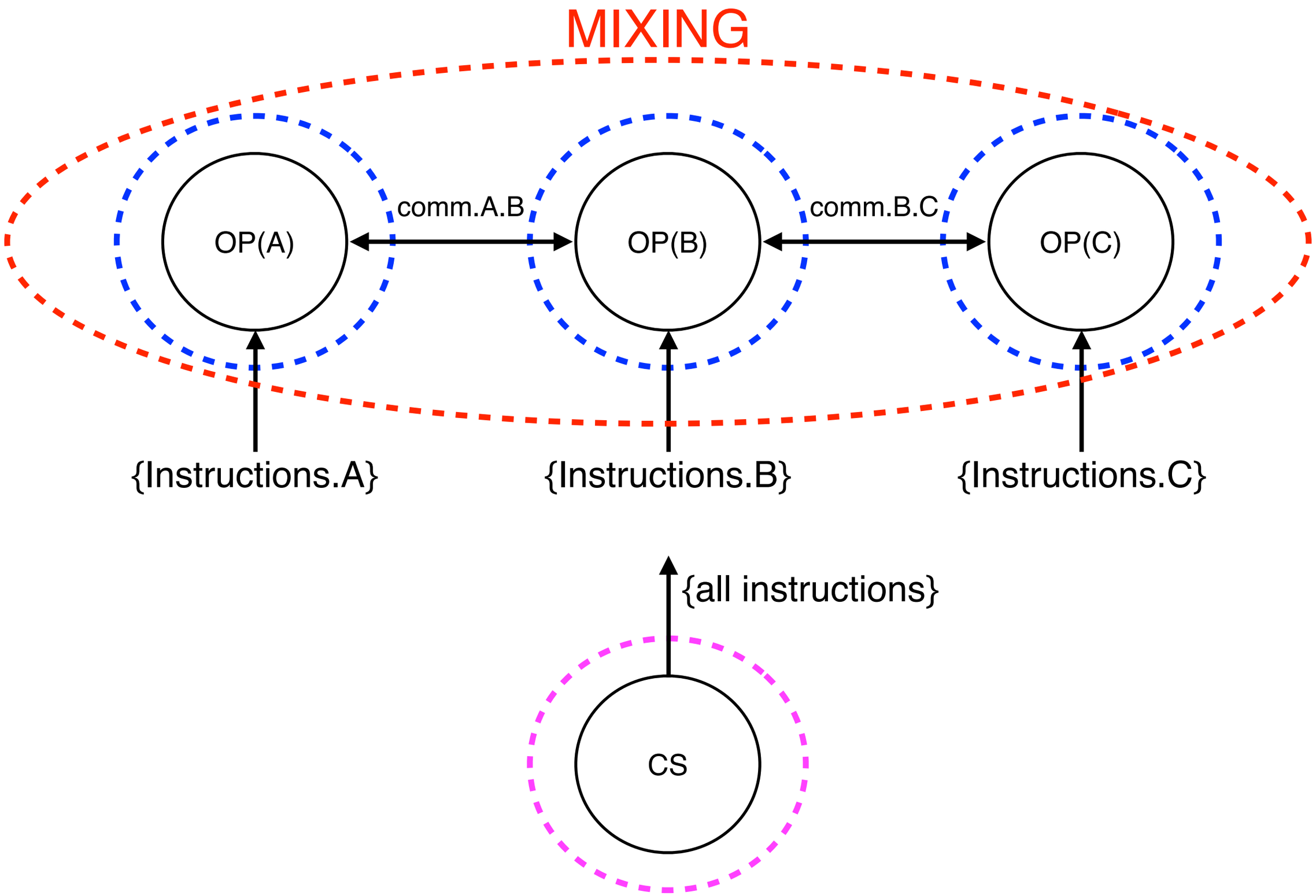
TB(B)

OP(B) = SERVER(B) [|{| post.B |}|] TB(B)

Ximix - Formal Analysis - Approach



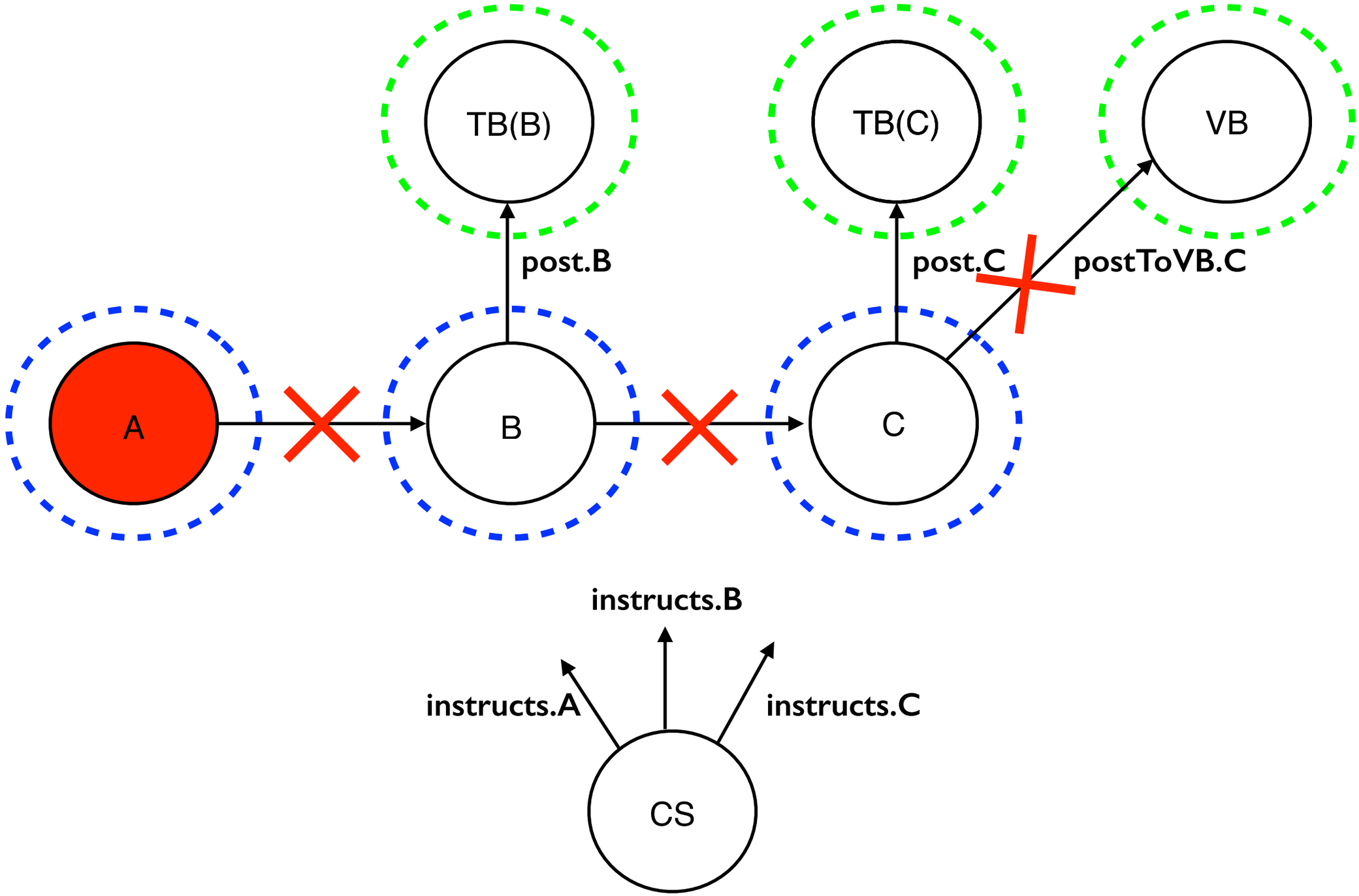
Ximix - Formal Analysis - Approach



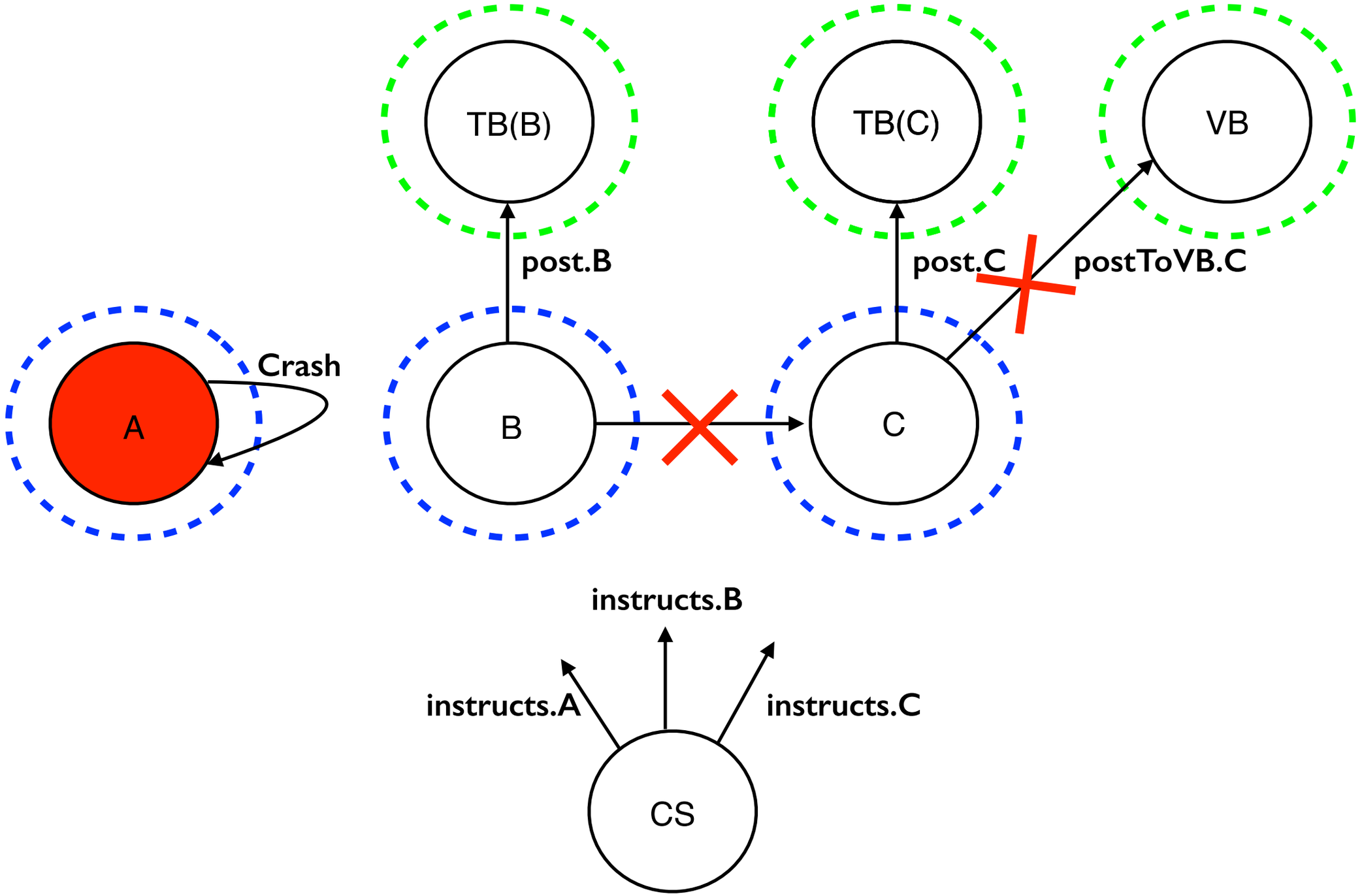
Ximix - Formal Analysis - Threat Model

- Roscoe and Goldsmith's perfect Spy
- Corrupt a minority of mix servers
- Learns, infers and says messages
- Active attacks
  - refuse to send messages
  - send different messages to different mix servers
  - perform DoS by perpetually posting onto the VB
  - post any message onto the VB

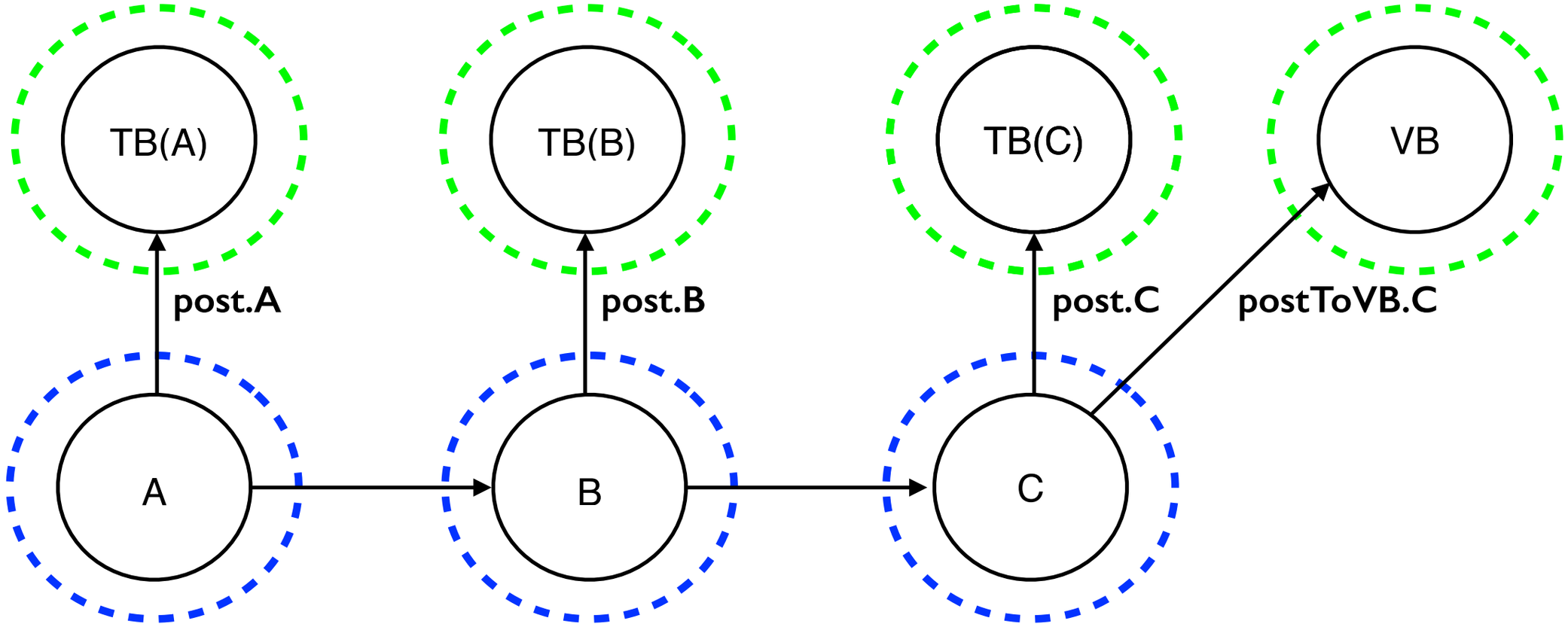
Ximix - Formal Analysis - Threat Model

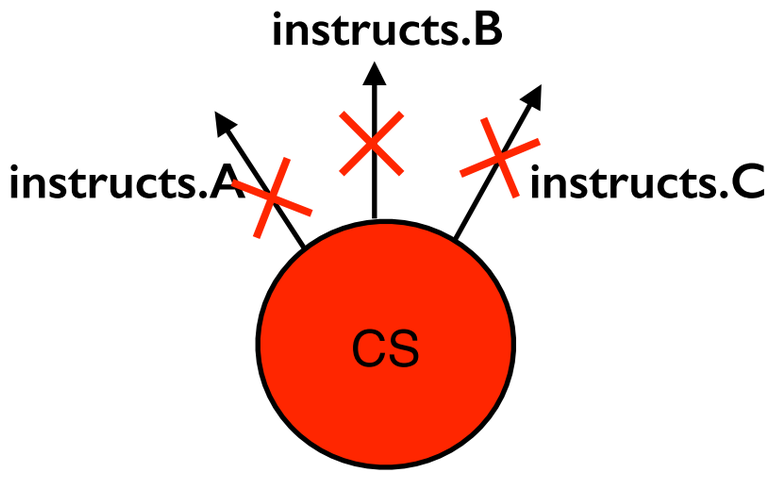


Ximix - Formal Analysis - Threat Model



Ximix - Formal Analysis - Threat Model





Ximix - Formal Analysis - Robust Ximix

- Distribute the trust by removing the CS
- Direct communications between the mix servers
- Give the power to mix servers to decide about other's honesty
- Use of timeout before or after receiving a message
- Any interested party can combine the partial decryptions

Conclusion

- Formal modelling and verification of beta version of Ximix
- Addressed key issues raised in this work
- The analysis demonstrated that the beta version was not robust in the presence of an intruder
- Proposed sound solutions
- Modified Ximix guarantees completion and produces a valid output

Conclusion

- The production version of Ximix was successfully used in large scale elections, Victoria State, Australia in November 2014
- Explained the impact on the lack of standardisation in Mix Nets and in what extent they can be standardised

Thank you!

Questions?