Chair of Distributed Systems & Operating Systems
Department of Computer Science // TUM School of Computation, Information and Technology
Technical University of Munich

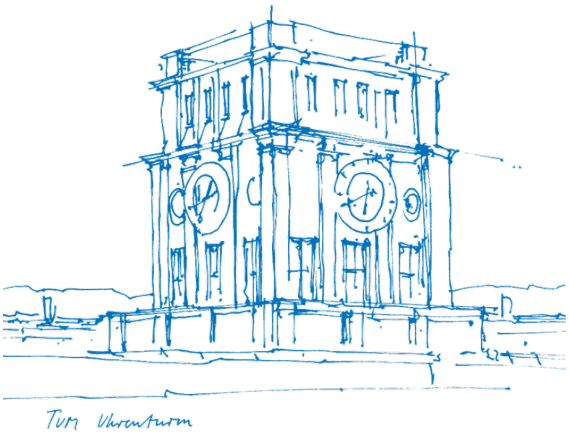
Kernel Functions of a Trusted NIC Architecture

Guided Research

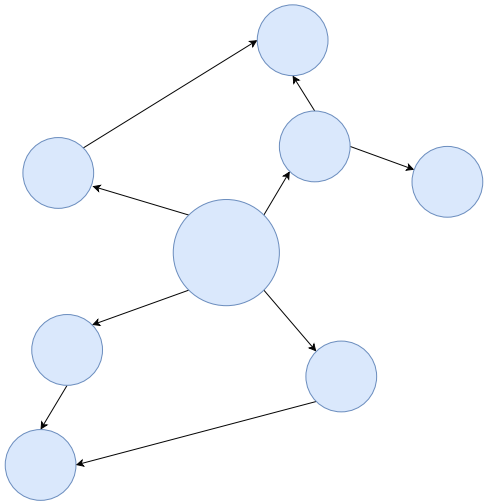
Robert Schambach

Chair of Distributed Systems & Operating Systems
Department of Computer Science // TUM School of Computation, Information and Technology
Technical University of Munich

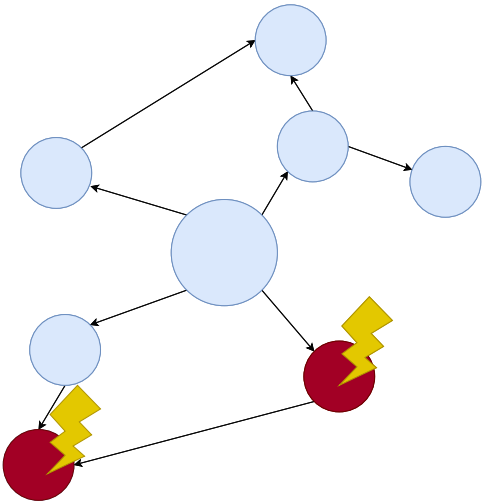
June 5th, 2023



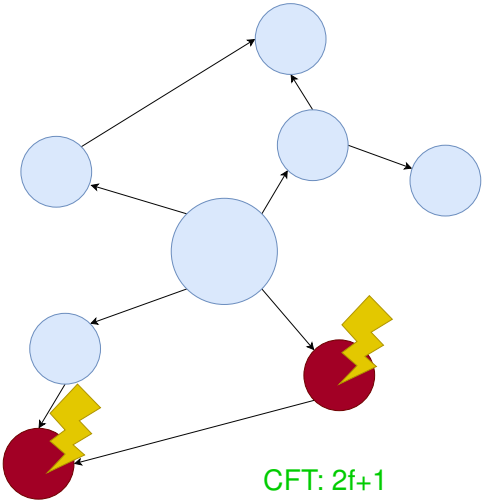
Problem Statement



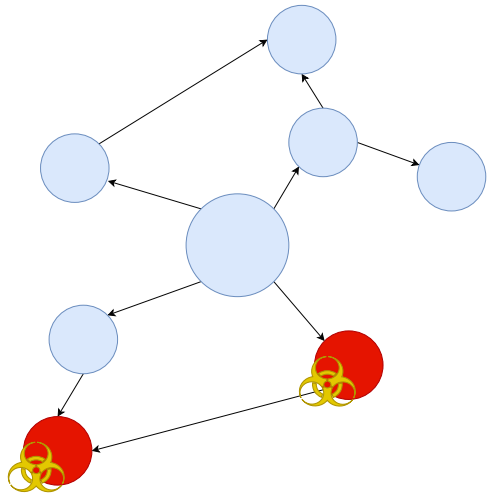
Problem Statement



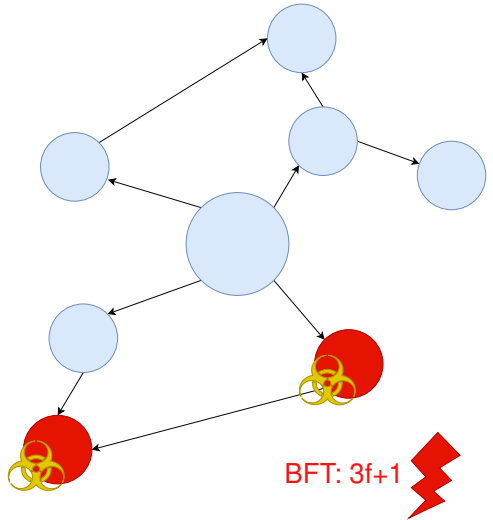
Problem Statement



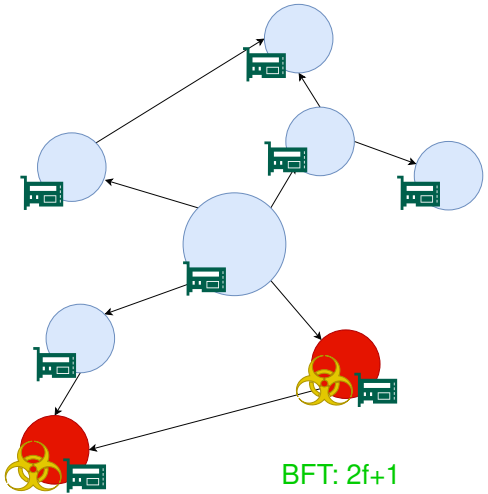
Problem Statement



Problem Statement

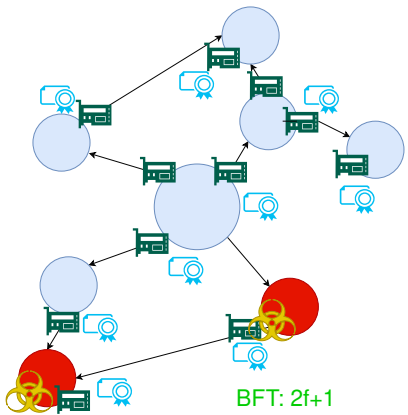


Problem Statement



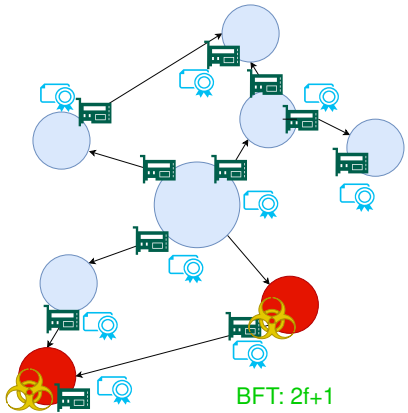
Our Proposal

- ensure BFT via **Kernel Functions** in s-NIC on NW path



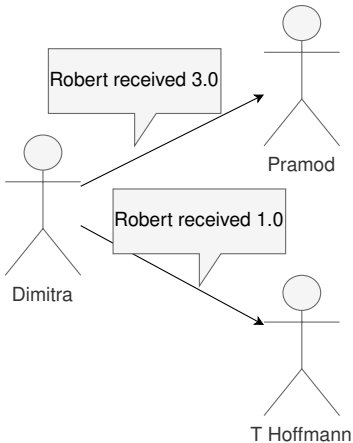
Our Proposal

- ensure BFT via **Kernel Functions** in s-NIC on NW path
- prevent **equivocation** and enable **transferable authenticity**



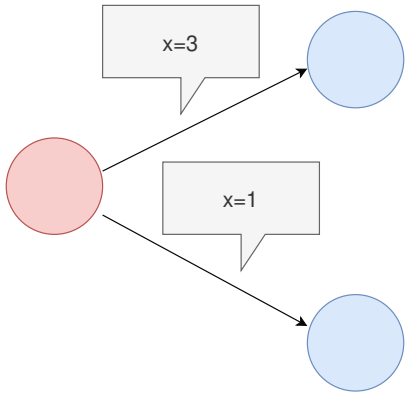
Challenges: Equivocation

- making conflicting statements



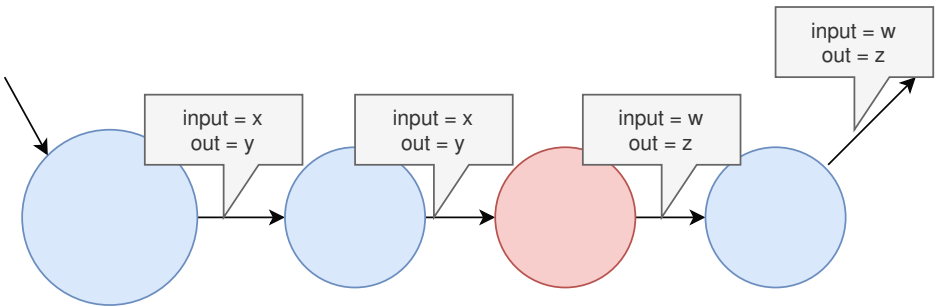
Challenges: Equivocation

- making conflicting statements



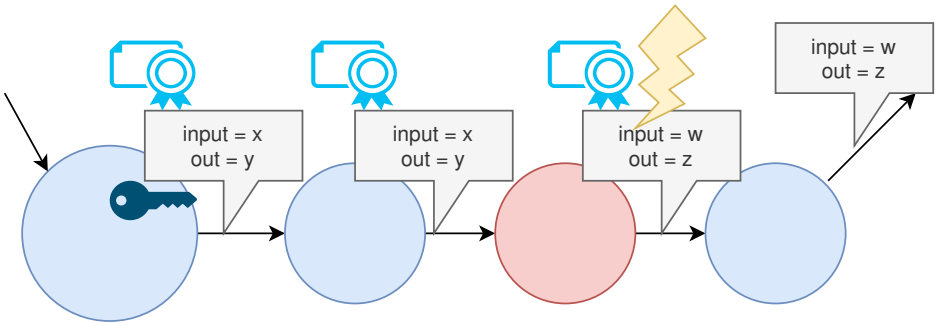
Challenges: Transferable Authenticity

- allow for transitive authentication via PKI



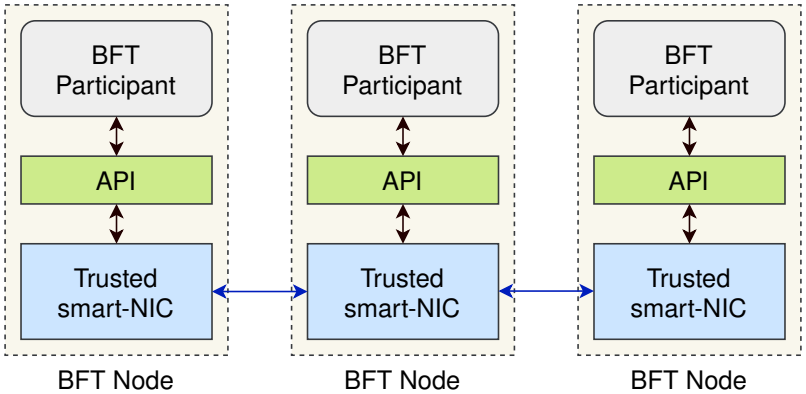
Challenges: Transferable Authenticity

- allow for transitive authentication via PKI



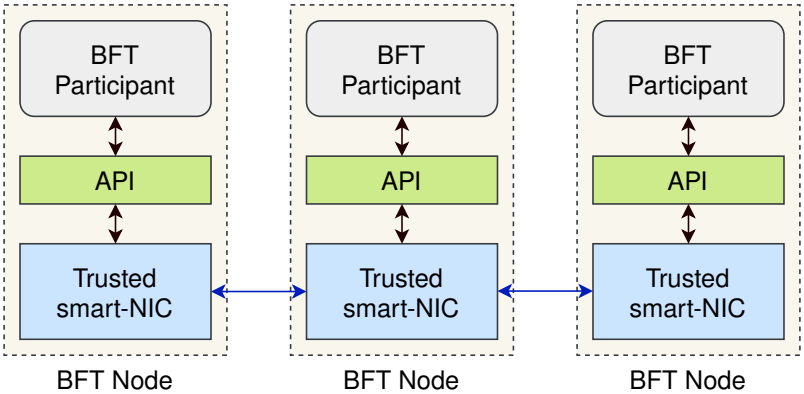
System Overview

- Host and trusted smart-NIC are **separate**



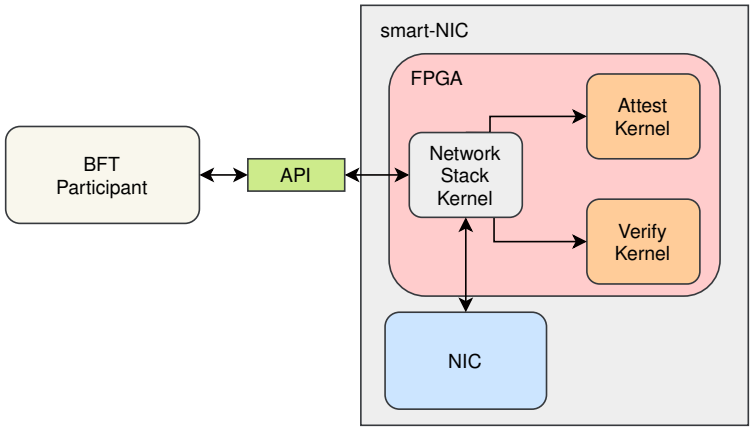
System Overview

- Host and trusted smart-NIC are **separate**
- smart-NIC is on the **network path**



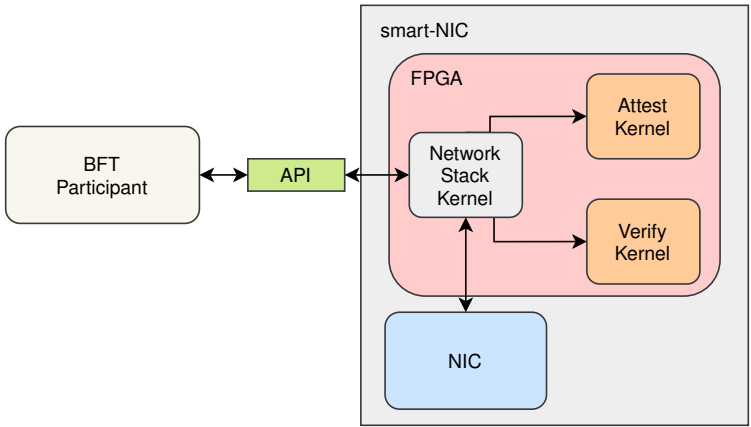
System Layout

- kernel functions: **Attest** and **Verify** Kernels



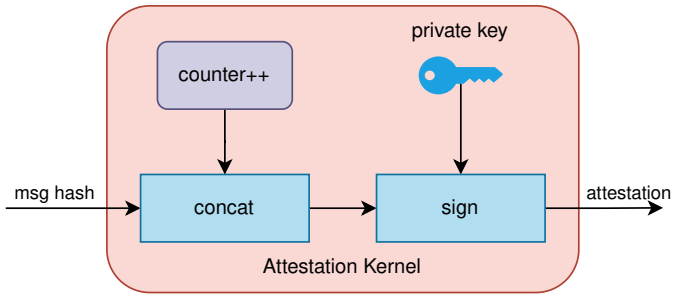
System Layout

- kernel functions: **Attest** and **Verify** Kernels
- Network Stack Kernel: **combines** components



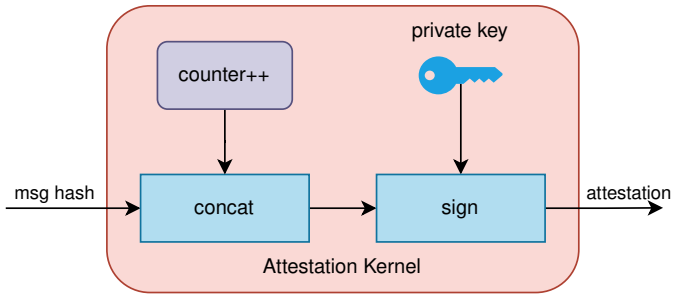
Kernel Function: Attest

- input: **message hash** (SHA-256 32B hash)



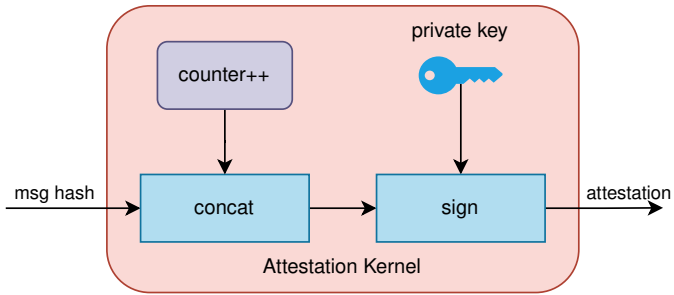
Kernel Function: Attest

- input: **message hash** (SHA-256 32B hash)
- output: **attestation** (PKI signature)



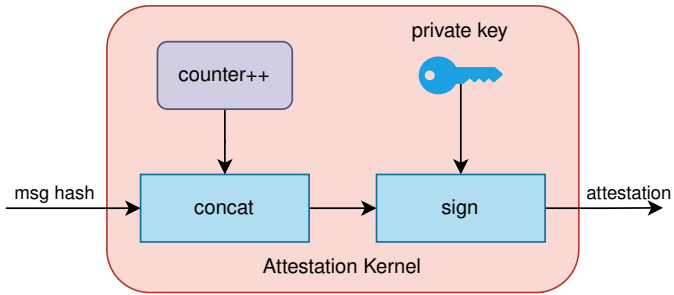
Kernel Function: Attest

- input: **message hash** (SHA-256 32B hash)
- output: **attestation** (PKI signature)
- counter: prevents **equivocation**



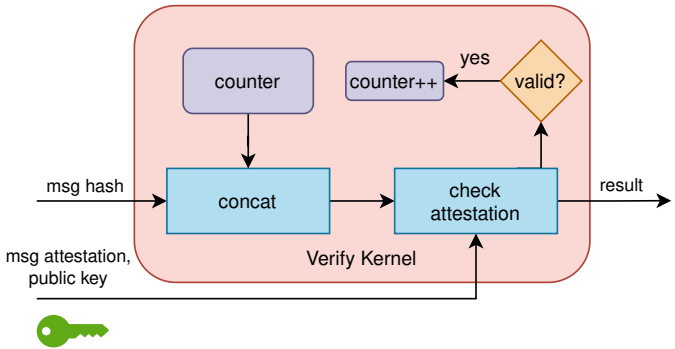
Kernel Function: Attest

- input: **message hash** (SHA-256 32B hash)
- output: **attestation** (PKI signature)
- counter: prevents **equivocation**
- PKI: enables **transferable authentication**



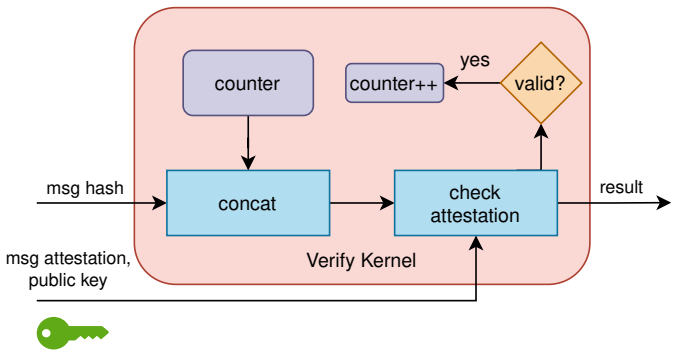
Kernel Function: Verify

- analog to attest



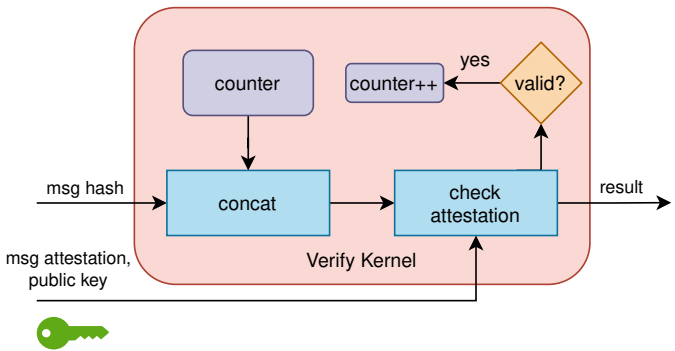
Kernel Function: Verify

- analog to attest
- receives candidate **message hash** and **attestation**



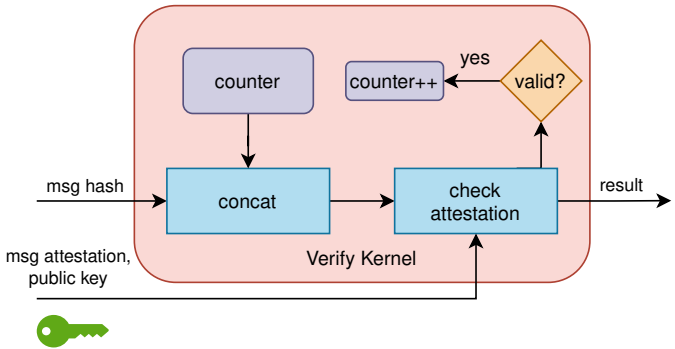
Kernel Function: Verify

- analog to attest
- receives candidate **message hash** and **attestation**
- pre-provided with **public key**



Kernel Function: Verify

- analog to attest
- receives candidate **message hash** and **attestation**
- pre-provided with **public key**
- own **counter** to track count of valid messages



Challenge: Equivocation

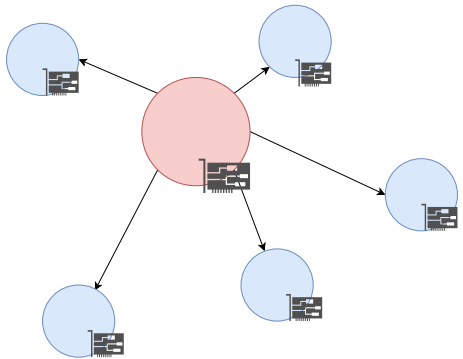
- recall: making **conflicting** statements

Challenge: Equivocation

- recall: making **conflicting** statements
- use **counter**: implementation protocol specific

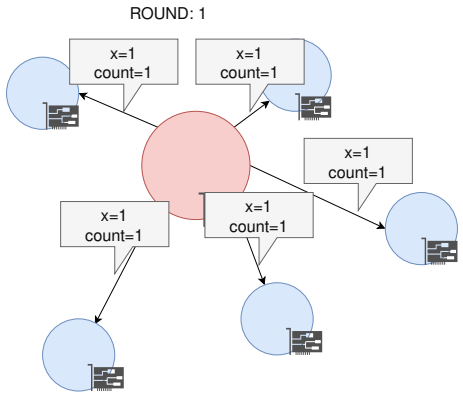
Challenge: Equivocation

- recall: making **conflicting** statements
- use **counter**: implementation protocol specific
- e.g. reliable broadcast



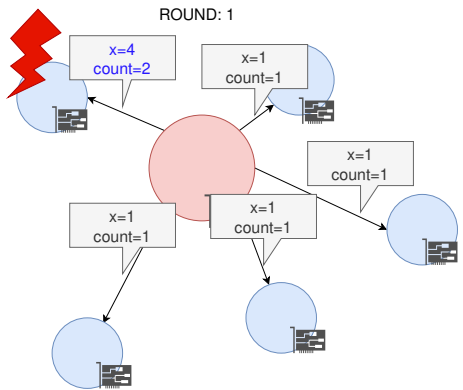
Challenge: Equivocation

- recall: making **conflicting** statements
- use **counter**: implementation protocol specific
- e.g. reliable broadcast



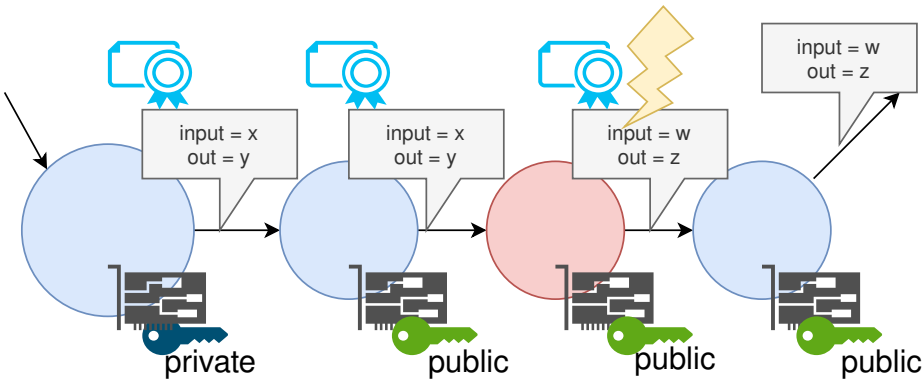
Challenge: Equivocation

- recall: making **conflicting** statements
- use **counter**: implementation protocol specific
- e.g. reliable broadcast



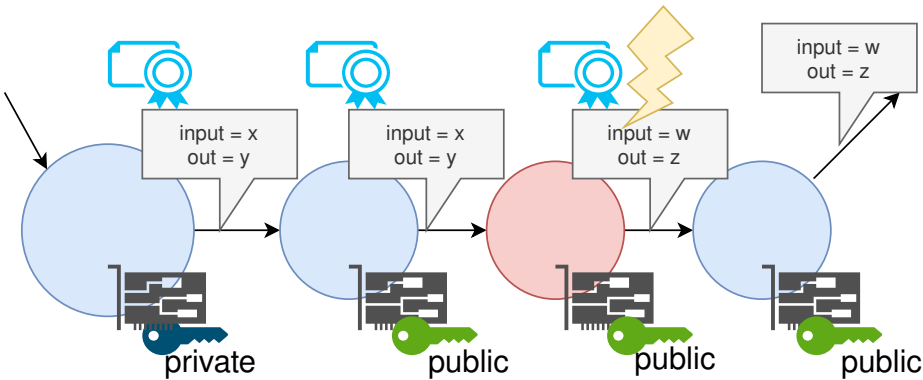
Challenge: Transferable Authentication

- recall: verify **authenticity** of non-point-2-point messages



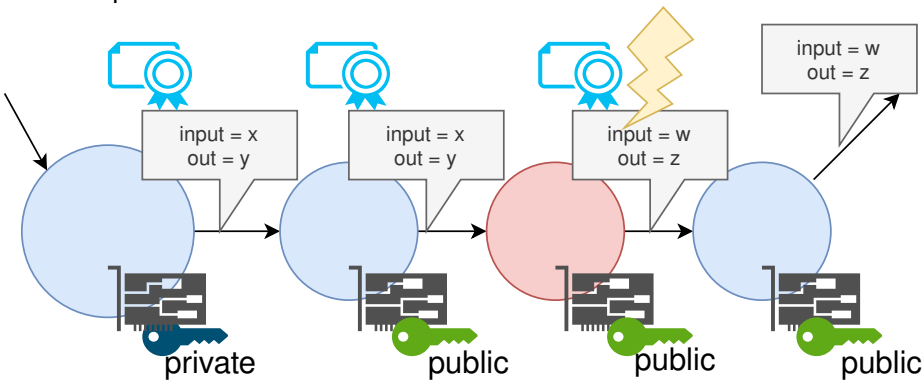
Challenge: Transferable Authentication

- recall: verify **authenticity** of non-point-2-point messages
- use **PKI** in smart-NICs: sign and verify messages



Challenge: Transferable Authentication

- recall: verify **authenticity** of non-point-2-point messages
- use **PKI** in smart-NICs: sign and verify messages
- e.g.: chain replication



Evaluation
Attestation

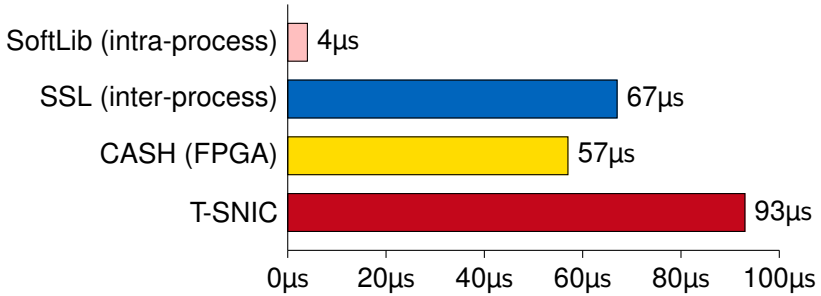


Figure 1 Subsystem Attest Benchmark Comparison

Evaluation
Verification

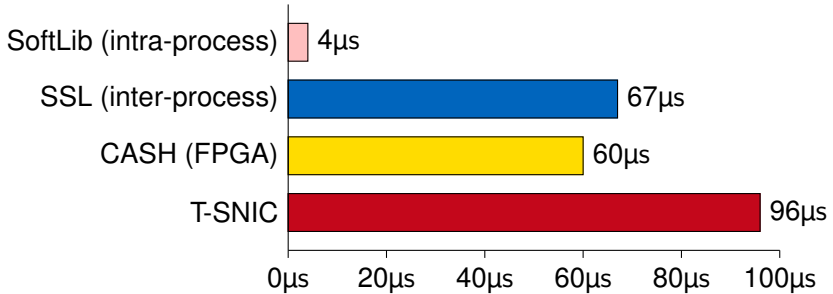


Figure 2 Subsystem Verify Benchmark Comparison

Conclusion

- **trusted hardware** reduces replicas from $3f + 1$ to $2f + 1$ for BFT

Conclusion

- **trusted hardware** reduces replicas from $3f + 1$ to $2f + 1$ for BFT
- **smart-NIC**:

Conclusion

- **trusted hardware** reduces replicas from $3f + 1$ to $2f + 1$ for BFT
- **smart-NIC**:
  - on NW path

Conclusion

- **trusted hardware** reduces replicas from $3f + 1$ to $2f + 1$ for BFT
- **smart-NIC**:
  - on NW path
  - transparent usage

Conclusion

- **trusted hardware** reduces replicas from $3f + 1$ to $2f + 1$ for BFT
- **smart-NIC**:
  - on NW path
  - transparent usage
  - suitable for heterogeneous DC architectures

Conclusion

- **trusted hardware** reduces replicas from $3f + 1$ to $2f + 1$ for BFT
- **smart-NIC**:
  - on NW path
  - transparent usage
  - suitable for heterogeneous DC architectures
- **Kernel Functions** in smart-NIC:

Conclusion

- **trusted hardware** reduces replicas from $3f + 1$ to $2f + 1$ for BFT
- **smart-NIC**:
  - on NW path
  - transparent usage
  - suitable for heterogeneous DC architectures
- **Kernel Functions** in smart-NIC:
  - prevent **equivocation**

Conclusion

- **trusted hardware** reduces replicas from $3f + 1$ to $2f + 1$ for BFT
- **smart-NIC**:
  - on NW path
  - transparent usage
  - suitable for heterogeneous DC architectures
- **Kernel Functions** in smart-NIC:
  - prevent **equivocation**
  - enable transferable authentication

Conclusion

- **trusted hardware** reduces replicas from $3f + 1$ to $2f + 1$ for BFT
- **smart-NIC**:
  - on NW path
  - transparent usage
  - suitable for heterogeneous DC architectures
- **Kernel Functions** in smart-NIC:
  - prevent **equivocation**
  - enable transferable authentication
  - acceptable performance

Conclusion

- **trusted hardware** reduces replicas from $3f + 1$ to $2f + 1$ for BFT
- **smart-NIC**:
  - on NW path
  - transparent usage
  - suitable for heterogeneous DC architectures
- **Kernel Functions** in smart-NIC:
  - prevent **equivocation**
  - enable transferable authentication
  - acceptable performance