Armored Twins:
Flexible Privacy Protection for Digital Twins through Conditional Proxy Re-Encryption and Multi-Party Computation

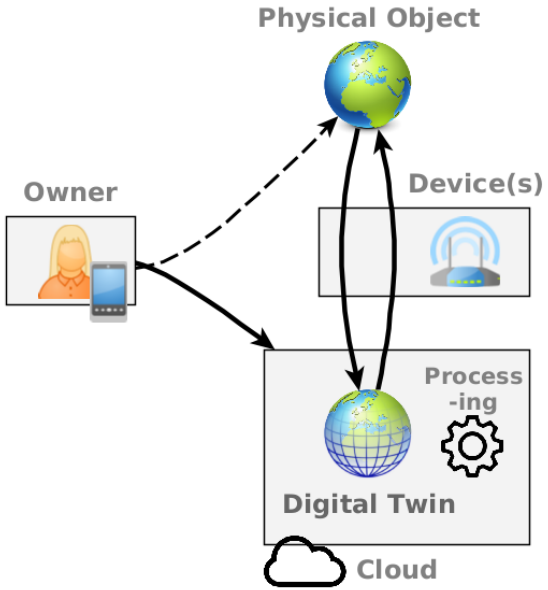
Felix Hörandner
Graz University of Technology
Graz, Austria

Bernd Prünster
Graz University of Technology
Graz, Austria

July 06, 2021

Setting: Digital Twins

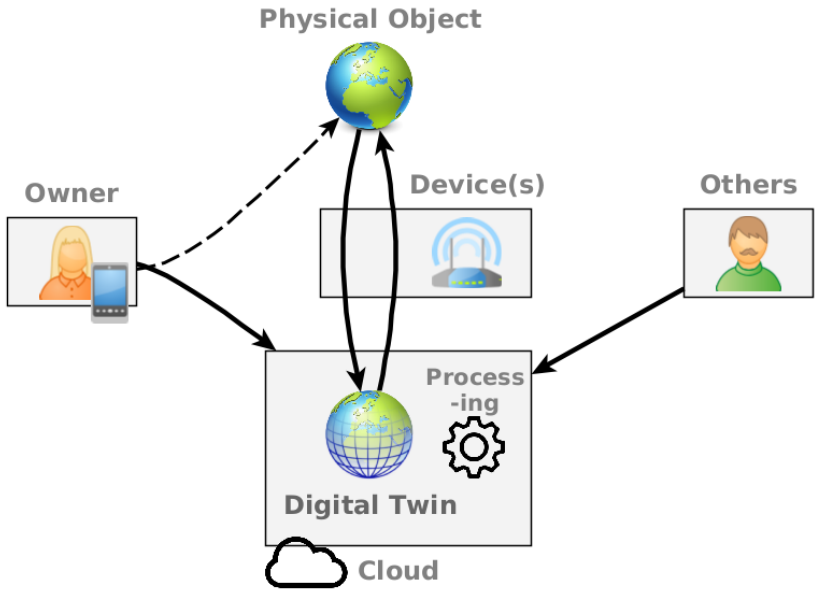
- **Internet of Things (IoT)**
  - Billions of smart devices
  - Connect with each other and Internet services
  - Broad concept with many instantiations
- **Digital Twins:** Structure for IoT systems [FFDB20]
  - Two-way synchronization
  - Convenient monitoring
  - Interaction via digital twin
  - Accumulate data for powerful computation
- **Use Cases**
  - Manufacturing: Products, Equipment, Design
  - Aircrafts: Maintenance
  - Health: Tailored treatments



[FFDB20] Fuller, A., Fan, Z., Day, C., and Barlow, C. “Digital Twin: Enabling Technologies, Challenges and Open Research”. IEEE Access 2020

Challenges

- **Sensitive data** on different subjects
  - Health or personal data
- Multiple stakeholders with **different trust**
  - Who owns data? Who can simulate?
  - Semi-trusted cloud
- **Changing relationships vs. Inflexibility**
  - New receivers?
  - New use cases?
  - Device broken?
- **Protection vs. Computation**
  - Encryption hinders computation



Ambition & Contribution

Challenges:

- **Sensitive data** on different subjects
  - Health or personal data
- Multiple stakeholders with **different trust**
  - Who owns data? Who can simulate?
  - Semi-trusted cloud
- **Changing relationships vs. Inflexibility**
  - New receivers?
  - New use cases?
  - Device broken?
- **Protection vs. Computation**
  - Encryption hinders computation

Our Contribution: Armored Twins

Protected & flexible digital twin system

- **Protect digital twin data**
- Give **owner control**
- **Dynamic maintenance** of sharing permissions
- **Recovery/replacement** of devices
- **Retain functionality** of digital twins (processing)
- Choose Trade-Off: **Privacy vs Computation Costs**

Approach

Approach: Apply advanced crypto to digital twin system

[ZFZ10]

Key-Policy Conditional Proxy Re-Encryption

- End-to-end confidential data sharing
- Fine-Granular: Based on attributes and policies
- Flexibility
- Enables processing on subsets

[BNTW12]

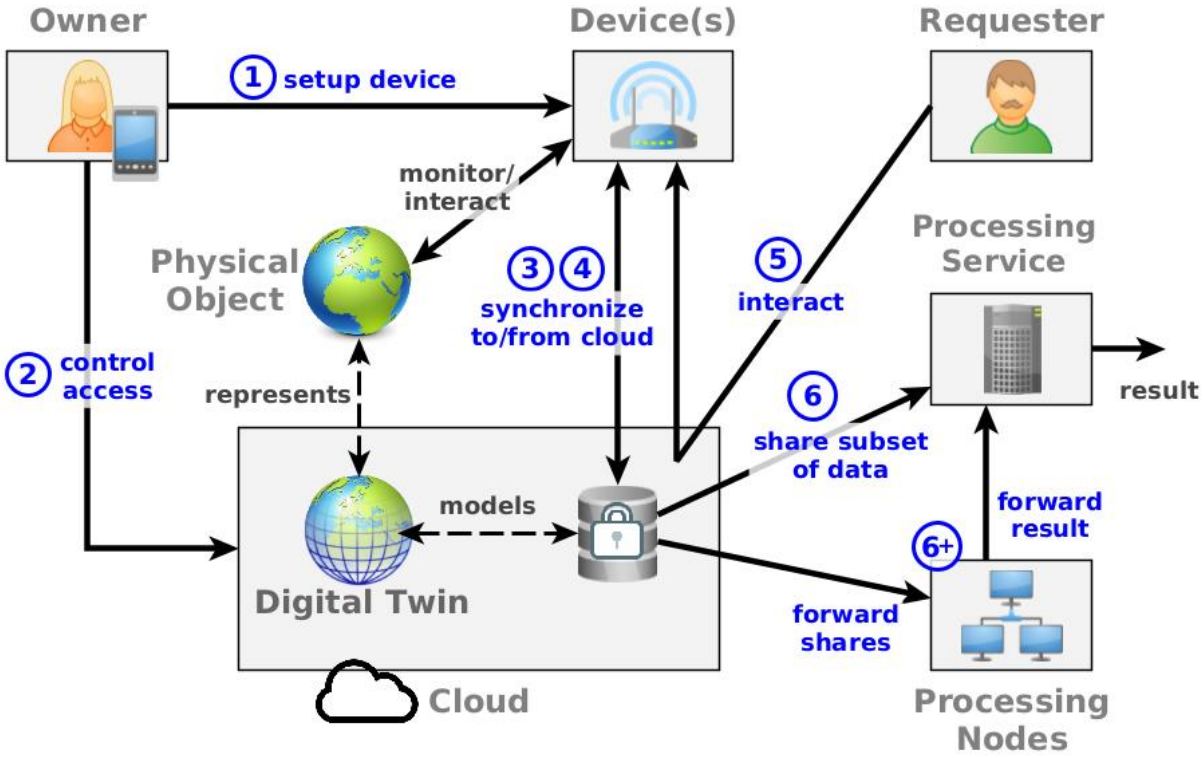
Multi-Party Computation

- Processing without revealing data

[ZFZ10] Zhao, J., Feng, D., and Zhang, Z. Attribute-Based Conditional Proxy Re-Encryption with Chosen-Ciphertext Security. GLOBECOM 2010

[BNTW12] Bogdanov, D., Niitsoo, M., Toft, T., and Willemson, J. High-performance secure multi-party computation for data mining applications. International Journal of Information Security 2012

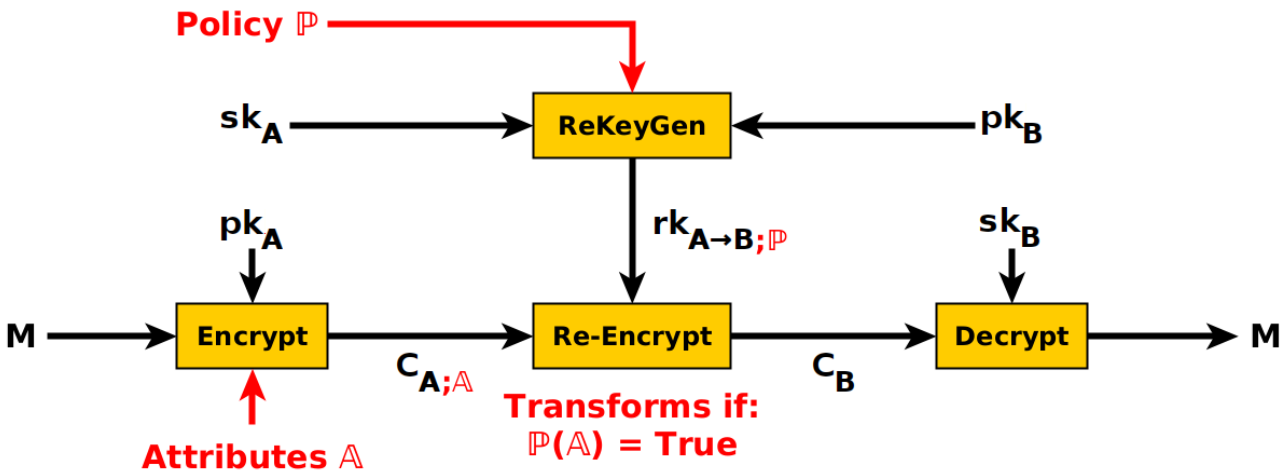
System Model



Operations &

Trust Relationships

Background: Proxy Re-Encryption (PRE) [AFGH06]



- **End-to-end confidential**
- User: **no need to fully trust proxy**
- **Control**: through re-encryption key
- No duplicate data

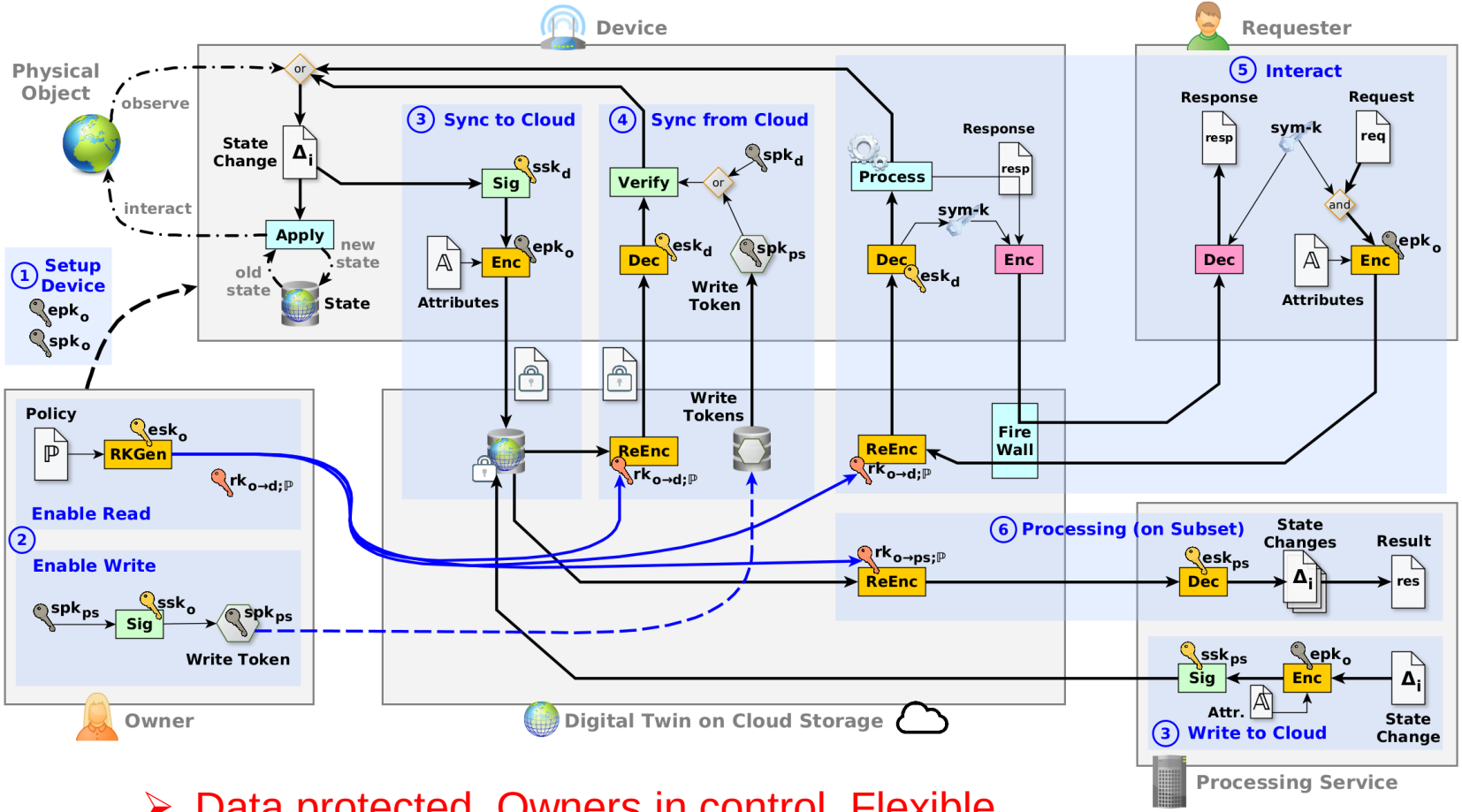
Key-Policy Conditional PRE

- Ciphertext for attribute set
- Re-Encryption key for policy
- Re-Encryption only successful if attributes satisfy policy [ZFZ10]

[AFGH06] Ateniese G., Fu K., Green M., Hohenberger S.: ACM Trans. Inf. Syst. Secur. 2006 Improved proxy re-encryption schemes with applications to secure distributed storage.

[ZFZ10] Zhao, J., Feng, D., and Zhang, Z. Attribute-Based Conditional Proxy Re-Encryption with Chosen-Ciphertext Security. GLOBECOM 2010

Armored Twins: Protected Digital Twins



➢ Data protected, Owners in control, Flexible

Maintenance and Recovery

- Handle **changes** in actors and trust relationships
- **KP-CPRE** decouples device from access decisions

- **User-managed access**
  - **Controlled by owner**, via private keys
  - **Read Access**:
    - Generate/remove re-encryption keys
    - Extend/limit policy
  - **Write Access**: Issue/remove write tokens
  - **Example**: Change access of processing service

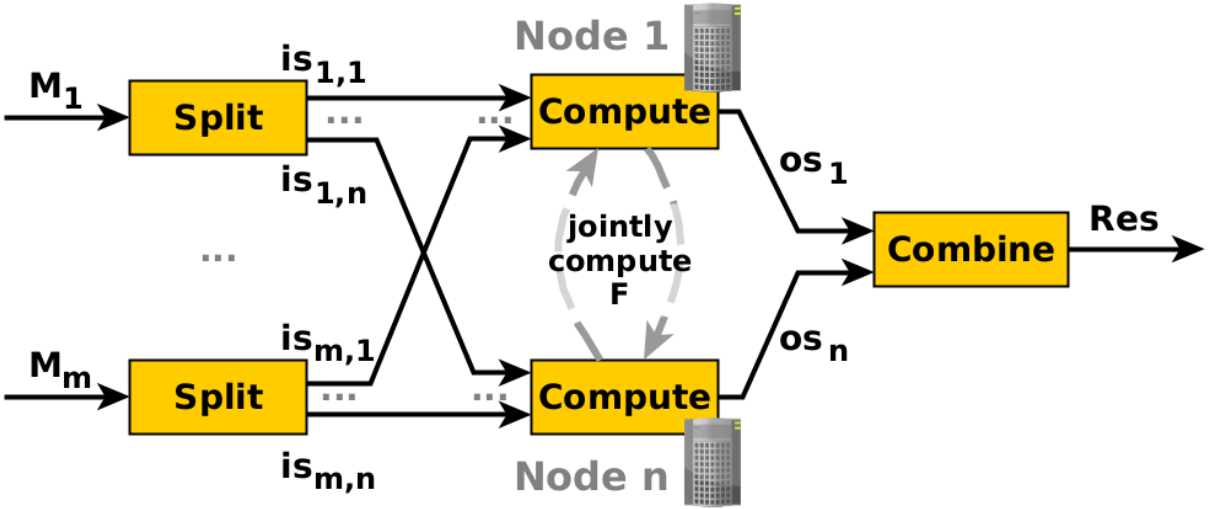
- **Recovery from device-loss**
  - Replace old device
  - Re-encryption to grant access
  - Seamlessly route requests to new device

Processing vs. Highly-Sensitive Data

- **Sharing subsets**
  - Sufficient for many use cases
  - Users can decide for themselves
  - But processing services still learn something

- **For highly-sensitive data**
  - Don’t want to expose even parts
  - Valuable results
  - Alternative: Integrating Secure Multi-Party Computation

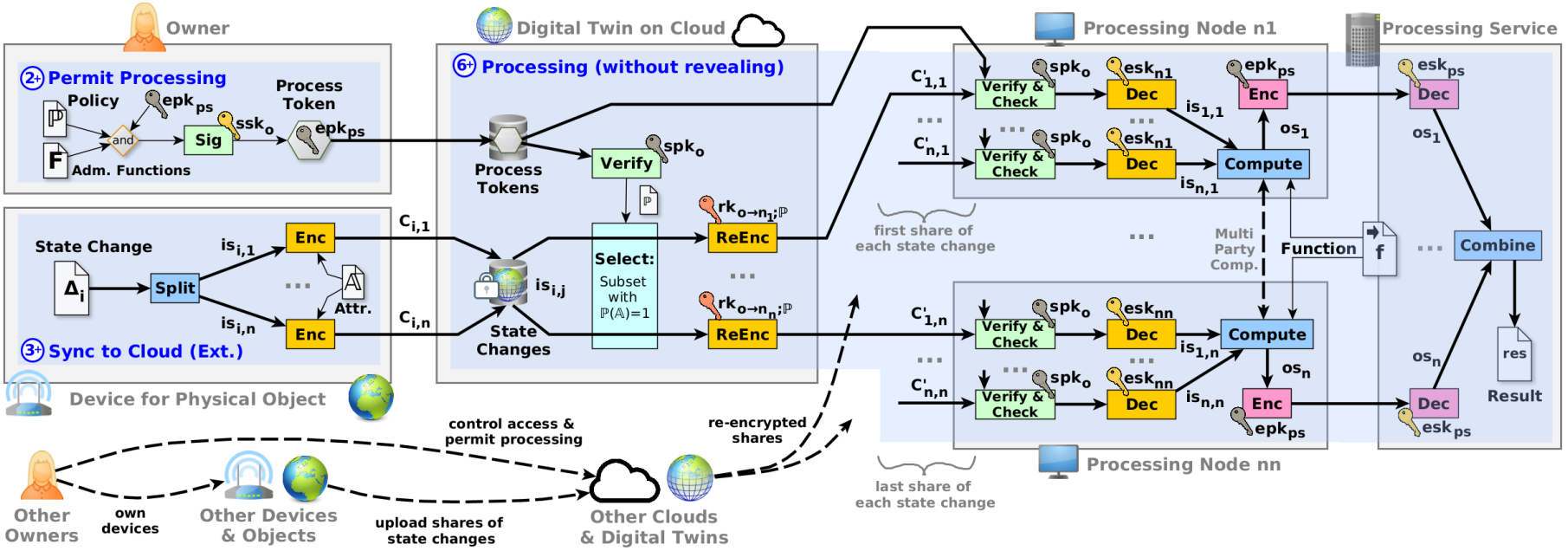
Background: Secure Multi-Party Computation (MPC)



- **Secret sharing-based MPC** [BNTW12]
- Nodes jointly compute function F
- Nodes do not learn plain inputs or output
- As long as insufficiently many nodes are corrupted

[BNTW12] Bogdanov, D., Niitsoo, M., Toft, T., and Willemson, J. High-performance secure multi-party computation for data mining applications. International Journal of Information Security 2012

Extension: Processing with Multi-Party Computation



- Privacy-Preserving Processing
  - Does not reveal input/result to nodes
  - Only processing service learns result

Performance Evaluation

- **Well known:** AES, ECDSA, and ECIES
- **Focus on:**

[ZFZ10]

Key-Policy Conditional Proxy Re-Encryption

- Generic numbers

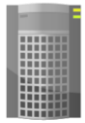
[BNTW12]

Multi-Party Computation

- For concrete use case

Implementation and Evaluation: KP-CPRE

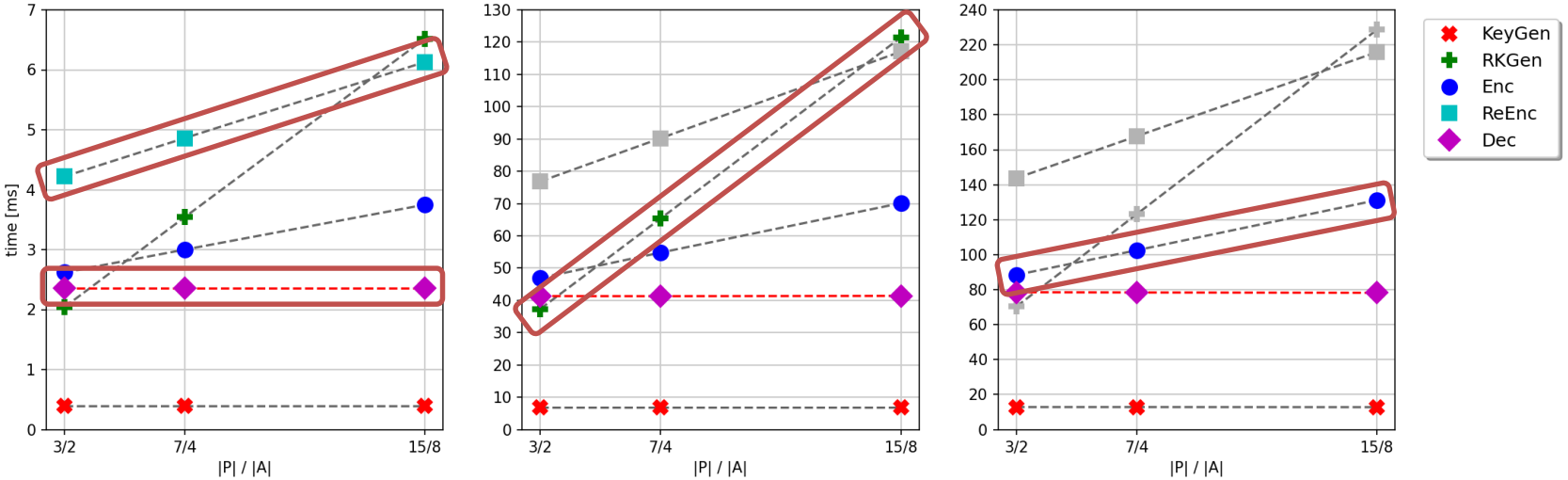
KP-CPRE [ZFZ10], RELIC toolkit, 128bit security, sharing AES keys, single-threaded



PC / Server:
AMD Ryzen 5600X

Mobile phone:
OnePlus 6T

IoT device:
Raspberry PI 4B



➢ Practical performance

[ZFZ10] Zhao, J., Feng, D., and Zhang, Z. Attribute-Based Conditional Proxy Re-Encryption with Chosen-Ciphertext Security. GLOBECOM 2010

Implementation and Evaluation: Contact Tracing

- **Concrete use case**
  to evaluate MPC performance
- **Contact tracing**
  - Sensitive location information
  - Compare path of 1 infected person to n other people
  - For each person: How many times too close?
- **Parameters**
  - Variable number of users
  - Each with one phone (device)
  - Recording path of 50 points (100 items/device)
  - Each in different epochs (no re-use of keys)
  - Split for 3 nodes (300 shares/device)
- **Implementation**: SCALE-MAMBA
  - 3 nodes with 30ms round-trip time

2+ Control Access: per user, on phone (OnePlus 6T)		
PRE.RKGen	53.99	× #devices/user × #nodes
SIG.Sign	1.44	× 1
UseCase-Σ =	**163.39**	*(per user)*
3+ Sync. to Cloud: per device, on phone (OnePlus 6T)		
MPC.Split	0.02	× #items/device
AES.Enc	<0.01	× #shares/device
PRE.Enc	51.13	× #epochs × #nodes
UseCase-Σ =	**7672.41**	*(per user, over epochs)*
6+ Processing: cumulated, on PC (AMD Ryzen 5600X)		
PRE.ReEnc	4.52	× #devs. × #epochs × #nodes
SIG.Verify	0.19	× #users
PRE.Dec	2.35	× #devices × #epochs
AES.Dec	<0.01	× #shares
MPC.Compute	6530.58	× #users +12433.61
PKE.Enc	0.18	× 1
PKE.Dec	0.12	× #nodes
MPC.Combine	0.08	× 1
UseCase-Σ =	**8242.24**	*(per user) + 12433.61 (const.)*

(SIG.Verify … PKE.Enc: on each node)

Summary: Key Messages

Our Contribution: Digital twin system

- Protect sensitive digital twin data
- Give owner control
- Support multiple stakeholders with different trust
- Flexibility: Provide dynamic maintenance of sharing permissions and recovery
- Retain functionality of digital twins (processing, interaction)
- Trade-off: Privacy vs. Computational Complexity

Approach:

1. Key-Policy Conditional Proxy Re-Encryption
   - Protect digital twin data
   - Gives flexibility
   - Enable processing on subsets
2. Multi-Party Computation
   - Processing without revealing data

Evaluation

- Practical performance

Thank you! Any Questions?