Protocol for Data Aggregation

Using Smart Contracts and Homomorphic Encryption on Hyperledger Fabric

Author: Floor Joosen
f.e.joosen@student.tudelft.nl
Responsible Professor:
Dr. Kaitai Liang
kaitai.liang@tudelft.nl

1. Introduction

Data aggregation improves quality of services provided and quality of life

Situation

Present design uses centralised third-parties

Problem

Leaked sensitive data removed trust

Solution

Distributed design for data aggregation

2. Research Question

Create a private and secure protocol for data aggregation utilising Homomorphic Encryption specifically for use with smart contracts on the Hyperledger Fabric platform.

3. Methodology

Literature Study › Define or improve existing protocol › Implement protocol › Test and analyse

4. The Protocol

Data is obfuscated by nonces
Encryption data = Homomorphic
Encryption nonces = Post-Quantum
Operators are Participants

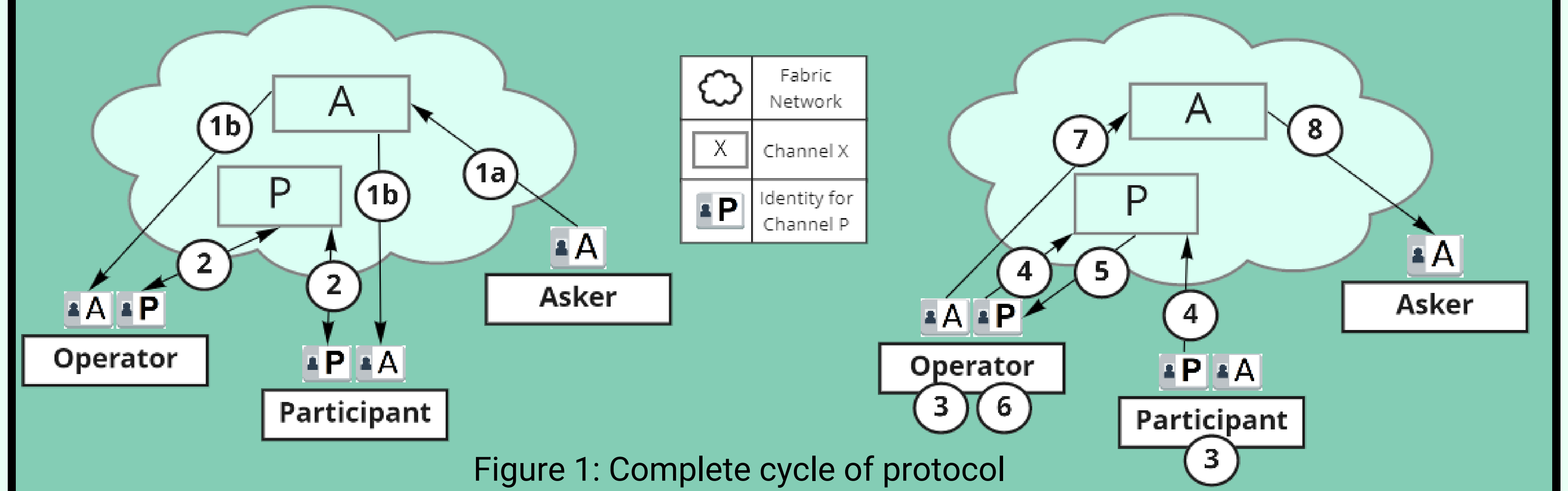

Figure 1: Complete cycle of protocol

1a. Asker starts process, sent: both public keys
1b. Participants get notified
2. Participants try to be Operators, sent: public key. They get notified when there are enough Operators
3. Participants: do I want to participate?
4. Yes, apply encrypted data and nonces
5. Time limit notifies Operator
6. Operators re-encrypt nonces
7. Operators report dat and nonces, and check reported data
8. Asker receives data and nonces

5. Security Improvements

Post-quantum encryption

Nonces are encrypted with post-quantum encryption

Prevents Collusion

Multiple Operators reduce the chance of collusion with Asker

Authorisation and privacy

Identity is checked but unknown to Asker

6. Performance Analysis

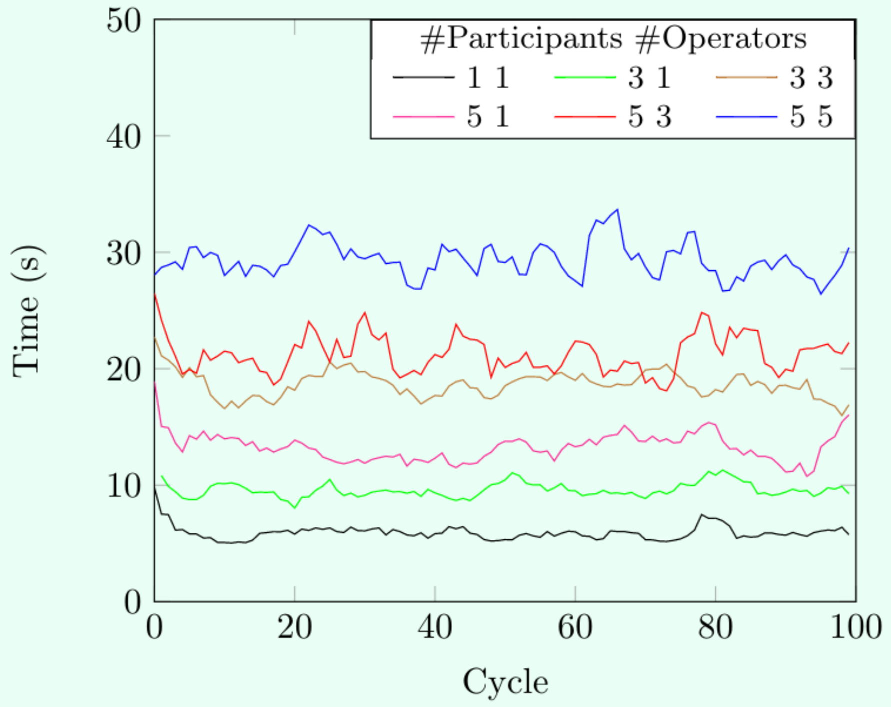

Figure 2: Performance of protocol under stress with different configurations

Table 1: Slowdown per factor

	Avg. Slowdown (s)
Per Operator	4.19
Per Participant	1.66
With Encryption	1.38

Performance is most dependent on
#Operators ▶ **#Participants** ▶ **Encryption**

7. Conclusion

- ➕ Generalised protocol for many use cases, on Hyperledger Fabric
- ➕ Increased security and privacy
- ➖ Not scalable in current implementation

8. Future Research

- Research effect on performance in a real world setting
- Research factors contributing to scalability, e.g. Composite keys
- Introduce roles or identities in implementation