Secure Distributed Protocols

Ligeti Péter

ELTE IK Komputeralgebra tsz.
Digitális szolgáltatások

2022. május 26-27.

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE HUNGARY

PROGRAM FINANCED FROM THE NRDI FUND

Motivation

Theory: secret sharing

- Goal: distribution of sensitive data
- Challenge: security + efficiency
- Tool: interesting combinatorial constructions

Practice: distributed communication systems

- Goal: secure distributed*
- Challenge: decentralization + constraints
- Tool: network + crypto protocols

National Research, Development and Innovation Office Hungary
Financed from the NRDI Fund

Secret sharing

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY
PROGRAM FINANCED FROM THE NRDI FUND

Motivation

Secret sharing scheme

- Some secret data is distributed into shares
- Each participant get a share
- The "good" guys can recover the secret
- Perfect SS: the other guys learn „nothing"

Algorithmic point of view

- Distribution: $s \to (s_1, \ldots, s_n)$ by the dealer
- Reconstruction $(s_{i_1}, \ldots, s_{i_k}) \to s$ by $\{i_1, \ldots, i_k\} \subseteq \mathcal{P}$

National Research, Development and Innovation Office Hungary
Financed from the NRDI Fund

Research problem

Multilevel conjunctive hierarchical threshold schemes

- $\mathcal{P} = \bigcup_{i=1}^{m} \mathcal{L}_i$
- Different thresholds for different levels: $t_1 < \cdots < t_m$
- $|A \cap \bigcup_{i=1}^{j} \mathcal{L}_j| \geq t_j$
- $\mathcal{A} = \{A \subseteq \mathcal{P} : \forall j (|A \cap \bigcup_{i=1}^{j} \mathcal{L}_j| \geq t_j)\}$

Existing solutions

- Mostly for 2 levels only
- Construction: random or monotone allocation of elements (Tassa '04)
- Reconstruction: Birkhoff interpolation (Tassa '04)
- Reconstruction: bivariate Lagrange interpolation (Tassa, Dyn '09)
- Drawback: restrictions for the field size/characteristics

Solution

Results (Sziklai, Takáts, LP '21)

- Novel construction for 3 levels: finite geometry tools
- Construction: intersection properties in a projective space
- Reconstruction: linear algebra
- Advantages: ideal, smaller field size ($O(n^3)$ improvement)
- Sziklai, Takáts, LP: *Generalized threshold secret sharing and finite geometry*, Designs, Codes and Cryptography, **89** pp. 2067–2078 (2021)

National Research, Development and Innovation Office Hungary
PROGRAM FINANCED FROM THE NRDI FUND

Distributed communication systems

National Research, Development and Innovation Office
Hungary
PROGRAM FINANCED FROM THE NRDI FUND

Motivation

Problems

- Centralized vs. distributed protocols
- Security drawbacks: DOS, TTP, ...
- Device constraints: computation, communication, location, ...
- Crypto drawbacks: efficient tools only

Examples

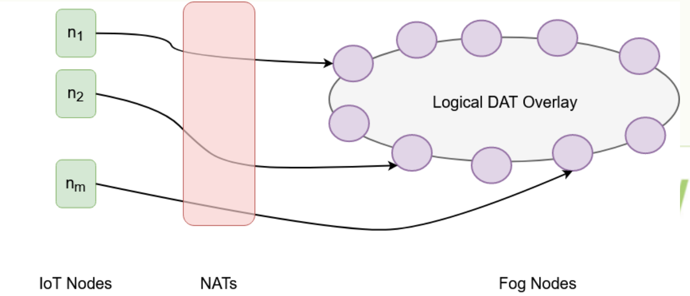
- Data validation in IIoT
- Attribute based access control
- Distributed address distribution
- Location-awareness, lightweight devices

M
D

Research problem

Distributed Address Table (DAT)

- Decentralized end-to-end communication in IoT
- Address distribution without TTP
- NAT traversal problem
- Efficiency/security trade-off

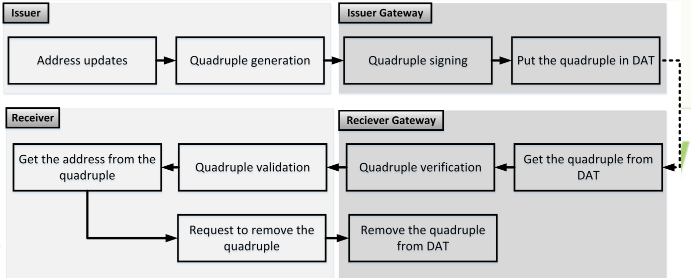


PROGRAM FINANCED FROM THE NRDI FUND

Solution

Building blocks

- Communication
  - structured P2P overlay
  - DHT + F2F
- Crypto
  - hash functions
  - symmetric/public key methods



PROGRAM FINANCED FROM THE NRDI FUND

Solution

Results (Kamel, Nagy, Reich, LP '22)

- ID generation + address distribution algorithms
- Simple + realistic assumptions
- Precise security requirements + proofs
- Preliminary implementation results (PeerSim + RPI3)
- Kamel, Nagy, Reich, LP: *Distributed Address Table (DAT): A Decentralized Model for End-to-End Communication in IoT*, Peer-to-Peer Networking and Applications, **15** pp. 178–193 (2022)

National Research, Development and Innovation Office Hungary
PROGRAM FINANCED FROM THE NRDI FUND

Q&A

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY

PROGRAM FINANCED FROM THE NRDI FUND