Titokmegosztások és elosztott protokollok

Ligeti Péter

ELTE IK Komputeralgebra tsz.
Digitális szolgáltatások

2022. január 13-14.
Teams

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY

PROGRAM FINANCED FROM THE NRDI FUND

Titokmegosztások

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"

Parameters

- Dealer has secret s
- Participants $\mathcal{P} = \{1, \ldots, n\}$
- Qualified sets $\mathcal{A} \subseteq 2^{\mathcal{P}}$

Motivation

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 $\{i_1, \ldots, i_k\} \subseteq \mathcal{P}$

Security point of view

Given $\mathcal{P}, \mathcal{A}$ choose s and compute shares s_i such that

- $\{i_1, \ldots, i_k\} \in \mathcal{A} \Rightarrow s$ can be computed from $s_{i_1}, \ldots, s_{i_k}$
- $\{j_1, \ldots, j_l\} \notin \mathcal{A} \Rightarrow$ all possible s can be computed with the same probability from $s_{j_1}, \ldots, s_{j_l}$ (i.e. independence)

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

Motivation

Problems

- For which $\mathcal{A}$ exsists a SS? ($\forall$)
- Are these methods efficient? (Efficient???)

Efficient schemes

- Storage: low information ratio + ideal schemes
- Computational (Reconstruction)

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

Graph based schemes

- $\mathcal{A}$ is monotone: if $A \in \mathcal{A}$ and $A \subset B$, then $B \in \mathcal{A}$.
- $(P, \mathcal{A}_0)$ is a hypergraph.

Graph based SS

- The minimal qualified subsets has two elements.
- Graph representation of $\mathcal{A}$ is a graph $G = (V, E)$ such that:
  - $V = P$.
  - $uv \in E$ iff $\{u, v\}$ is qualified.
  - $A \subset V$ independent if A is non-qualified.
- If G is the graph representation of $\mathcal{A}$, then $\sigma(G) := \sigma(\mathcal{A})$.

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

Graph based schemes

Examples

- Small graphs ($|V| \leq 6$)
- Trees: $\sigma(T) = 2 - 1/c(G)$ (Csirmaz, Tardos '13)
- Large girth graphs: $\sigma(T) = 2 - 1/d$ (Csirmaz, LP '09)

Problems

- Connection between the tree + girth results
- Reduce the assumptions for girth
- $\sigma(G)$ for larger family of graphs

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

Graphs without high-degree neighbours

Results (Gyarmati, LP '21 DAM)

- simple graph reduction
- $\forall G = (V, E) : u, v \in V : d(u), d(v) \geq 3 \Rightarrow \{u, v\} \notin E$
- $\sigma(G) = 2 - \frac{1}{\max_{v \in V^*} d(v) - t(v)}$

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

Elosztott protokollok

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

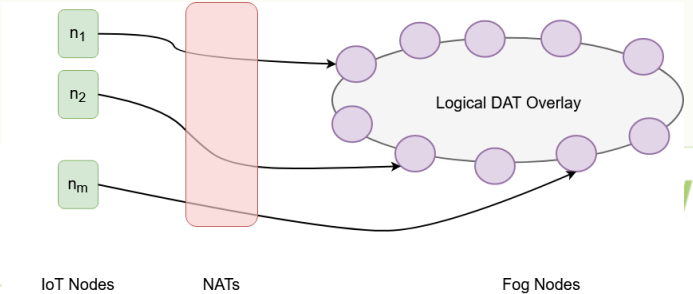
Examples

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

Motivation

Distributed Address Table (DAT)

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

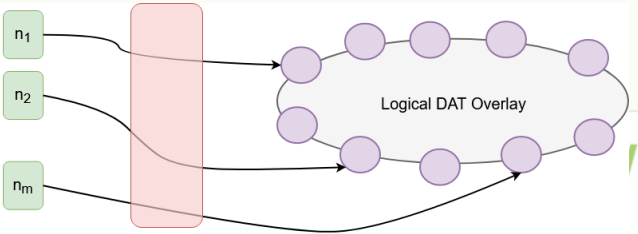


PROGRAM
FINANCED FROM
THE NRDI FUND

Solution

Building blocks

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

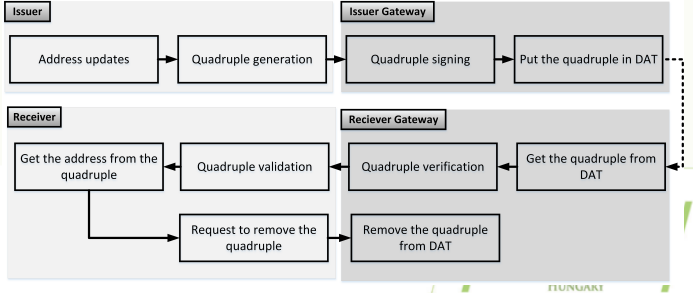


PROGRAM
FINANCED FROM
THE NRDI FUND

Solution

Ideas

- Sophisticated ID generation
- IoT nodes + gateways
- Data packets: $DATQ \leftarrow (header|ts|IN|c)$

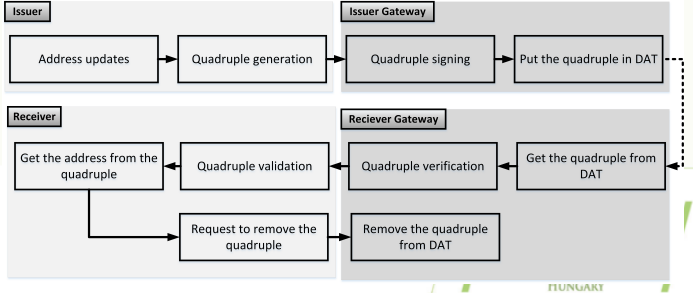


PROGRAM FINANCED FROM THE NRDI FUND

Solution

Security requirements

- Weak anonymity
- Address privacy
- Soundness



PROGRAM FINANCED FROM THE NRDI FUND

Solution

Results (Kamel, Nagy, Reich, LP '21 P2P Net & App)

- ID generation + address distribution algorithms
- Simple + realistic assumptions
- Precise security requirements + proofs
- Preliminary implementation results (PeerSim + RPI3)

Next steps

- Validation on large scale test-network

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

Results

Conference talks

- M. Kamel, P. Ligeti, C. Reich: LADA: Locality Aware Distributed Addressing for Edge/Fog Computing Infrastructures, *IEEE Conf. on International Conference on Electrical, Computer and Energy Technologies (ICECET '21)*

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

Results

Papers

- M. Gyarmati, P. Ligeti: On the information ratio of graphs without high-degree neighbours, *Discrete Applied Mathematics* (Q2)
- M. Kamel, P. Ligeti, C. Reich: Lamred: Location-Aware and Privacy Preserving Multi-Layer Resource Discovery for IoT, *Acta Cybernetica* (Q4)
- M. Kamel, P. Ligeti, Á. Nagy, C. Reich: Distributed Address Table (DAT): A Decentralized Model for End-to-End Communication in IoT, *Peer-to-Peer Networking and Applications* (Q2)

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