Titokmegosztások és elosztott protokollok

Péter Sziklai[1], Péter Ligeti[2]

[1]ELTE, Faculty of Science, Dept. of Computer Science
[2]ELTE, Faculty of Informatics, Dept. of Computeralgebra

10-11 June, 2021
Teams, Hungary

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY

PROGRAM FINANCED FROM THE NRDI FUND

Part I: 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 gets a share
- The "good" guys can recover the secret
- Perfect SSS: the other guys can learn „nothing"

Parameters

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

National Research, Development and Innovation Office
Hungary
THE NRDI FUND

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 $\mathcal{A}$ exists a SSS? ($\forall$)
- 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

Generalized threshold schemes

Multilevel hierarchical threshold scheme

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

Multilevel hierarchical constructions

- Disjunctive: several solutions
- Conjunctive: some sporadic constructions only

National Research, Development and Innovation Office
Hungary
THE NRDI FUND

Generalized threshold schemes

Multilevel conjunctive hierarchical threshold scheme

- Construction: random or monotone allocation of elements (Tassa '04)
- Reconstruction: Birkhoff interpolation (Tassa '04)
- Reconstruction: bivariate Lagrange interpolation (Tassa, Dyn '09)
- Drawback: extremely large q

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

Generalized threshold schemes

2-level conjunctive hierarchical threshold scheme

- $\mathcal{P} = \mathcal{U} \bigcup \mathcal{L}$
- $\mathcal{A}^* = \binom{\mathcal{U} \cup \mathcal{L}}{k} \setminus \binom{\mathcal{L}}{k}$
- $(k, 1)-$scheme
- Construction: intersection properties in a projective plane (Fuji-Hara, Miao '08)
- Reconstruction: linear algebra (Brickell, Stinson '92)

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

Generalized threshold schemes

Result (LP, SzP, Takáts)

- 3-level construction: (4,2,1) scheme
- Based on finite geometry tools
- $|\mathcal{L}_1| = |\mathcal{L}_2| = q^{1/3}, |\mathcal{L}_3| = 1/3 \cdot q$
- Ideal scheme

Result (Gyarmati, LP, SzP, Takáts)

- 3-level construction: $(r, s, n+1)$ scheme
- Based on finite geometry tools
- $|\mathcal{L}_1| = |\mathcal{L}_2| = c \cdot q^{1/n}, |\mathcal{L}_3| = c \cdot q$
- Ideal scheme

HUNGARY
THE NKDI FUND

Generalized threshold schemes

Result (Gyarmati, LP, SzP, Takáts)

- 4-level construction: $(r, s, u, n+1)$ scheme
- Based on finite geometry tools
- $|\mathcal{L}_1| = |\mathcal{L}_2| = |\mathcal{L}_3| = c \cdot q^{1/n}, |\mathcal{L}_4| = c \cdot q$
- Ideal scheme

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

The geometric constructions, part 1

Definition: pencil arc (k-parc)

Let $\Psi_0, ..., \Psi_q$ be a pencil through some Π_{n-2} in $PG(n, q)$. A k-parc $\mathcal{K} \subseteq PG(n, q)$, $|\mathcal{K}| = k$, such that:

1. Each $\mathcal{K} \cap \Psi_i$ is a k_i-arc in Π_{n-1} for $0 \leq i \leq q$, where $k_i = |\mathcal{K} \cap \Psi_i|$;
2. $\mathcal{K} \cap \Psi_i \cap \Psi_j = \emptyset$ for $0 \leq i \neq j \leq q$;
3. Any $n + 1$ points of $\mathcal{K}$ not contained in any single Ψ_i are independent.

Note (Fuji-Hara, Miao): if there is a k-parc in $PG(t - 1, q)$ as above, with $k = k_0 + k_1 + ... + k_m$ points, $k_i \geq 1$ for $0 \leq i \leq m$ and $k_0 = \min\{k_i\}$, then there exists an ideal secret sharing scheme realizing compartmented access structure with upper bounds $t_1 = \cdots = t_m = t - 1$ on $|\mathcal{P}| = k - k_0$ participants.

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

The geometric constructions, part 1

Pencil arcs from planar arcs (Ligeti, SzP, Takáts) $PG(2,q^h) = AG(2,q^h) \cup (\ell_\infty)$

Identify $AG(2,q^h) \sim X \times Y$, where $X \sim \mathbb{F}_q^h$ and $Y \sim \mathbb{F}_q^h$ are the horizontal and the vertical axes. Let's call here the translates of the first factor (horizontal axis) the horizontal lines $\ell_0, ..., \ell_{q^h-1}$, which, together with ℓ_∞, form the pencil with center P. Let L_1 be a $(h-1)$-dim q-subspace of the horizontal axis, i.e. $X = L_0 \times L_1$ for some 1-dim q-vectorspace $L_0 \subset X$, wlog $L_0 = \mathbb{F}_q$. Let L_2 be a 1-dim q-subspace of the vertical axis Y, again wlog $L_2 = \mathbb{F}_q$. Finally, suppose wlog $\ell_0, ..., \ell_{q-1}$ are the pencil lines intersecting L_2.

Let $A_0 = L_1 \times L_2$. Any horizontal translate of it is either disjoint from A_0 or identical with it, hence they form a partition $\cup_{\lambda \in \mathbb{F}_q}(A_0 + \lambda) = \ell_0 \cup ... \cup \ell_{q-1}$. Note that here, for any point $Q \in \ell_0 \cup ... \cup \ell_{q-1}$, it has coordinates $Q = (a + \lambda, y)$, where $a \in L_1, \lambda \in L_0$ and $y \in L_2$.

Consider the affine plane $AG(2,q) \sim L_0 \times L_2$ and an arc S in it. Define

$$K := \{(a + \lambda, y) : a \in L_1, (\lambda, y) \in S\}.$$

The geometric constructions, part 1

Pencil arcs from planar arcs

$$K := \{(a + \lambda, y) : a \in L_1, (\lambda, y) \in S\}$$

Observe that K consists of $|S|$ "line segments", each contained in one of the pencil lines ℓ_i and of size $|L_1| = q^{h-1}$.
K is a pencil arc (of size $|S|q^{h-1}$)
There exist arcs of size $q+1$ in $AG(2,q)$ for q odd and arcs of size $q+2$ in $AG(2,q)$ for q even $\Longrightarrow$ (many) k-parcs with $k = q^h + q^{h-1}$ in planes of odd order q^h; and k-parcs with $k = q^h + 2q^{h-1}$ in planes of even order q^h.

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

The geometric constructions, part 2

Pencil arcs from caps (LP, SzP, Takáts) $PG(2,q^h) = AG(2,q^h) \cup (\ell_\infty)$

Let L_1 be a $(h-s)$-dim $\mathbb{F}_q$-subspace of the horizontal axis, i.e. $X = L_0 \times L_1$ for some s-dim $\mathbb{F}_q$-vectorspace $L_0 \subset X$. Let L_2 be a 1-dim $\mathbb{F}_q$-subspace of the vertical axis Y, wlog we may assume $L_2 = \mathbb{F}_q$. Suppose wlog that $\ell_0, ..., \ell_{q-1}$ are the pencil lines intersecting L_2.

Let $A_0 = L_1 \times L_2$. Any horizontal translate of it is either disjoint from A_0 or identical with it, hence they form a partition $\cup_{v \in L_0}(A_0 + v) = \ell_0 \cup ... \cup \ell_{q-1}$. Note that here, for any point $Q \in \ell_0 \cup ... \cup \ell_{q-1}$, it has coordinates $Q = (a + v, y)$, where $a \in L_1, v \in L_0$ and $y \in L_2$.

Consider the affine space $AG(s+1, q) \sim L_0 \times L_2$ and a **cap** S in it. (cap: a pointset with no collinear triple of points) Now define

$$K := \{(a + v, y) : a \in L_1, (v, y) \in S\}.$$

Observe that K consists of $|S|$ line segments', each contained in one of the pencil lines ℓ_i and of size $|L_1| = q^{h-s}$. Claim: K is a pencil arc (of size $|S|q^{h-s}$).

The geometric constructions, part 3

Definition: hierarchical arc (harc)

Let Ψ be a hyperplane of $PG(n,q)$, $\mathcal{K}_1$ be a set of k_1 points in $PG(n,q) \setminus \Psi$, and $\mathcal{K}_2$ be a set of k_2 points in Ψ. A *hierarchical arc* in $PG(n,q)$ is a set $\mathcal{K} = \mathcal{K}_1 \cup \mathcal{K}_2$ of $k_1 + k_2$ points in $PG(n,q)$, also called a (k_1, k_2)-*harc*, satisfying the following conditions:
(1) $\mathcal{K}_1$ is a k_1-arc in $PG(n,q)$;
(2) $\mathcal{K}_2$ is a k_2-arc in $PG(n-1,q)$;
(3) Any $n+1$ points of $\mathcal{K}$ not contained in the hyperplane Ψ are independent.
Fuji-Hara and Miao showed that if there is a (k_1, k_2)-harc in $PG(t-1,q)$ with $k_1 \geq 2$ and $k_2 \geq 0$ then there exists an ideal conjunctive $(1,t)$-hierarchical scheme with $|\mathcal{P}| = k_1 + k_2 - 1$.

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

The geometric constructions, part 3

A conjunctive hierarchical $(1, 2, n+1)$-scheme ($n \geq 3$): new constructions for harcs in $PG(n, q)$ (LP, SzP, Takáts)

A geometric scheme composed of 3 levels $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$. A valid subset should contain at least $n+1$ elements from $\mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$, such that at least 2 elements are from $\mathcal{L}_1 \cup \mathcal{L}_2$ and at least 1 element from $\mathcal{L}_1$.
In $PG(n, q) = AG(n, q) \cup H_\infty$ we will choose our sets as follows. Let

- $|\mathcal{L}_1| = k_1 = c_1 q^{1/n}$ be a subset of an arc (e.g. a so-called normal rational curve) in $AG(n, q)$;
- $|\mathcal{L}_2| = k_2 = c_2 q^{1/n}$ be a subset of an arc, e.g. a normal rational curve in H_∞) and
- $|\mathcal{L}_3| = k_3 = c_3 q^{1/n}$ be a subset of an arc, e.g. a normal rational curve in H, which is a $(n-2)$-dimensional subspace of H_∞;
- furthermore, a set $\mathcal{D} \subset AG(n, q)$ of size $c_4 q$ is determined, such that the *dealer*, i.e. a point D will be chosen from $\mathcal{D}$.

Generalized threshold schemes

Results

- Novel construction: finite geometry tools (LP, SzP, Takáts DCC)
- For special parameters: $(1, n), (1, 2, n)$
- Advantages: ideal, smaller field size ($O(n^3)$ improvement)
- Drawbacks: restrictions on the number/value of thresholds

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

Generalized threshold schemes

Results

- Goal: generalize the constructions
- Done: arbitrary levels, arbitrary thresholds, ideal, improved field size

TODO

- Optimization (size of levels & field)
- Additional constructions
- Disjunctive schemes
- Constructions based on polynomials

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

Results

Conference talks

- M. Gyarmati, P. Ligeti, P. Sziklai, M. Takáts: Multilevel secret sharing by finite geometry, *21st Central European Conference on Cryptology (CECC 2021)*

Papers

- P. Ligeti, P. Sziklai, M. Takáts: Generalized threshold secret sharing and finite geometry, *Designs, Codes and Crypt.* DOI 10.1007/s10623-021-00900-9
- M. Gyarmati, P. Ligeti: On the information ratio of graphs without high-degree neighbours, *Discrete Applied Mathematics*, under review
- M. Gyarmati, P. Ligeti, P. Sziklai, M. Takáts: Conjunctive hierarchical secret sharing by finite geometry, under construction

AND INNOVATION OFFICE
HUNGARY
THE NRDI FUND

Part II: Secure Distributed Applications

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

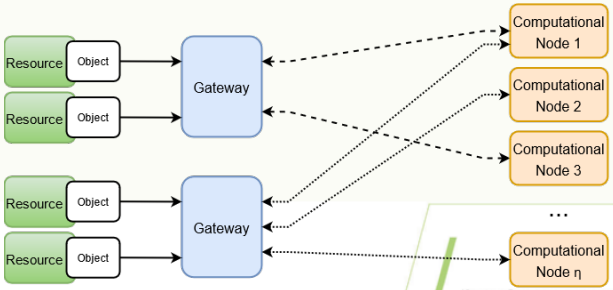
Examples

- Buzzwords: IoT + cloud
- Data validation in IoT
- ABE in cloud
- **Distributed resource discovery (location-based, IoT/ABE support)**

Motivation

Resource discovery in IoT

- Gather and discover real-time generated data by IoT (re)sources
- Gather: gateways
- Discover: clients



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

Motivation

Problems

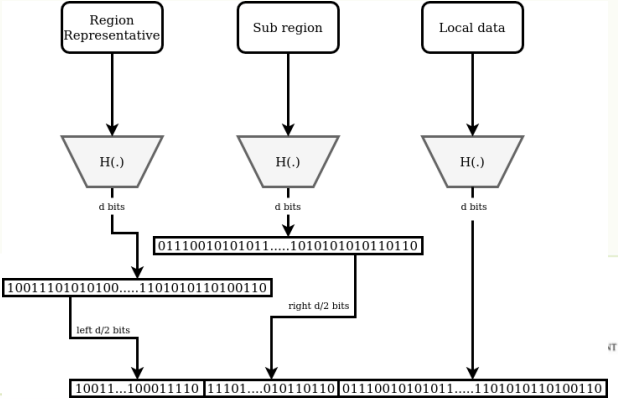
- Diversity of IoT perception layer
- Avoid TTPs – distributed communication + computation
- Location-awareness
- Security requirements
  - Fine-grained access control
  - Privacy
  - Availability

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

Solutions – distributed*

Ideas

- Computation: additive secret sharing
- Discoverability: region-based ID generation + DHT

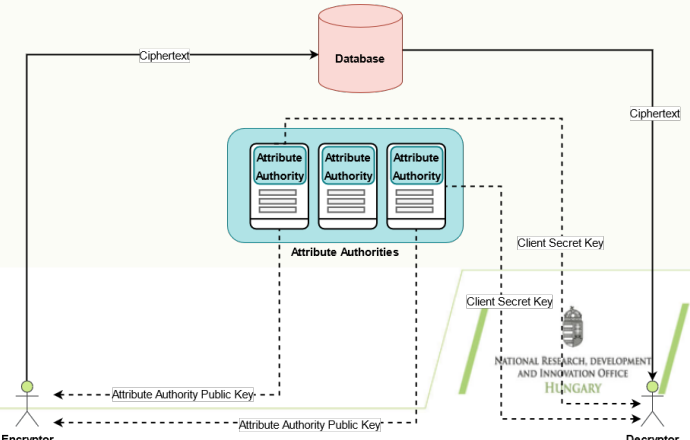


PROGRAM FINANCED FROM THE NRDI FUND

Solution – security*

Ideas

- Attribute-based access control
- Multi-authority scheme



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

Solution

Results (Kamel, Reich, Yan, LP '21 Sensors)

- Precise security requirements + proofs
- Preliminary implementation results (on few Raspberry PI 3)

Next steps

- Validation on large scale test-network
- Extend the security model
- Formal protocol verification

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

Results

Conference talks

- Y. Yan, P. Ligeti: Improving Security and Privacy in Attribute-based Encryption with Anonymous Credential, *4th International Conference on Recent Innovations in Computing (ICRIC-2021)*
- M. Yaseen, M.B.M. Kamel, P. Ligeti: Security Analysis and Deployment Measurement of Transport Layer Security Protocol, *(ICRIC-2021)*

Papers

- M. Kamel, Y. Yan, P. Ligeti, C. Reich: Attred: Attribute based Resource Discovery for IoT, *Sensors* under review
- 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*, under review
- M. Kamel, P. Ligeti, C. Reich: Lamred: Location-Aware and Privacy Preserving Multi-Layer Resource Discovery for IoT, *Acta Cybernetica* to appear

Q&A

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY

PROGRAM FINANCED FROM THE NRDI FUND