CRT-based Secret Sharing Schemes

Design and Security

Constantin Cătălin Drăgan Ferucio Laurenţiu Ţiplea

Department of Computer Science
Alexandru Ioan Cuza University of Iaşi
Iaşi, Romania
E-mail: {constantin.dragan,fltiplea}@info.uaic.ro

Outline

Secret Sharing Schemes

- 1979, Blakley and Shamir
- Secret sharing scheme:
  - secret space and dealer
  - participants and share spaces
  - access structure
- Security concepts:
  - perfectness
  - idealness
  - perfect zero-knowledge

Secret Sharing Schemes

Applications in cryptography and distributed computing:

- Byzantine agreement
- Secure multi-party computation
- Threshold and visual cryptography
- Access control
- Attribute-based encryption
- Generalized oblivious transfer
- etc.

Secret Sharing Schemes

- Construction techniques
  - Polynomial interpolation (univariate or bivariate interpolation)
  - Chinese Remainder Theorem (standard CRT, CRT in polynomial rings, interpolation and CRT in polynomial rings)
  - Graphs, matroids, lattices
  - Geometric constructions
- Classes of access structures:
  - Threshold
  - Unanimous consent
  - Weighted
  - Multilevel (conjunctive, disjunctive)
  - Compartmented (with lower or upper bounds)
  - Multisecret

Generic Construction for $(t+1,n)$-threshold Schemes

Parameter setup

- $m_0 < \cdots < m_n$ sequence of co-primes
- possible various constraints on the sequence
- $t, n, m_0, \ldots, m_n$ are public parameters

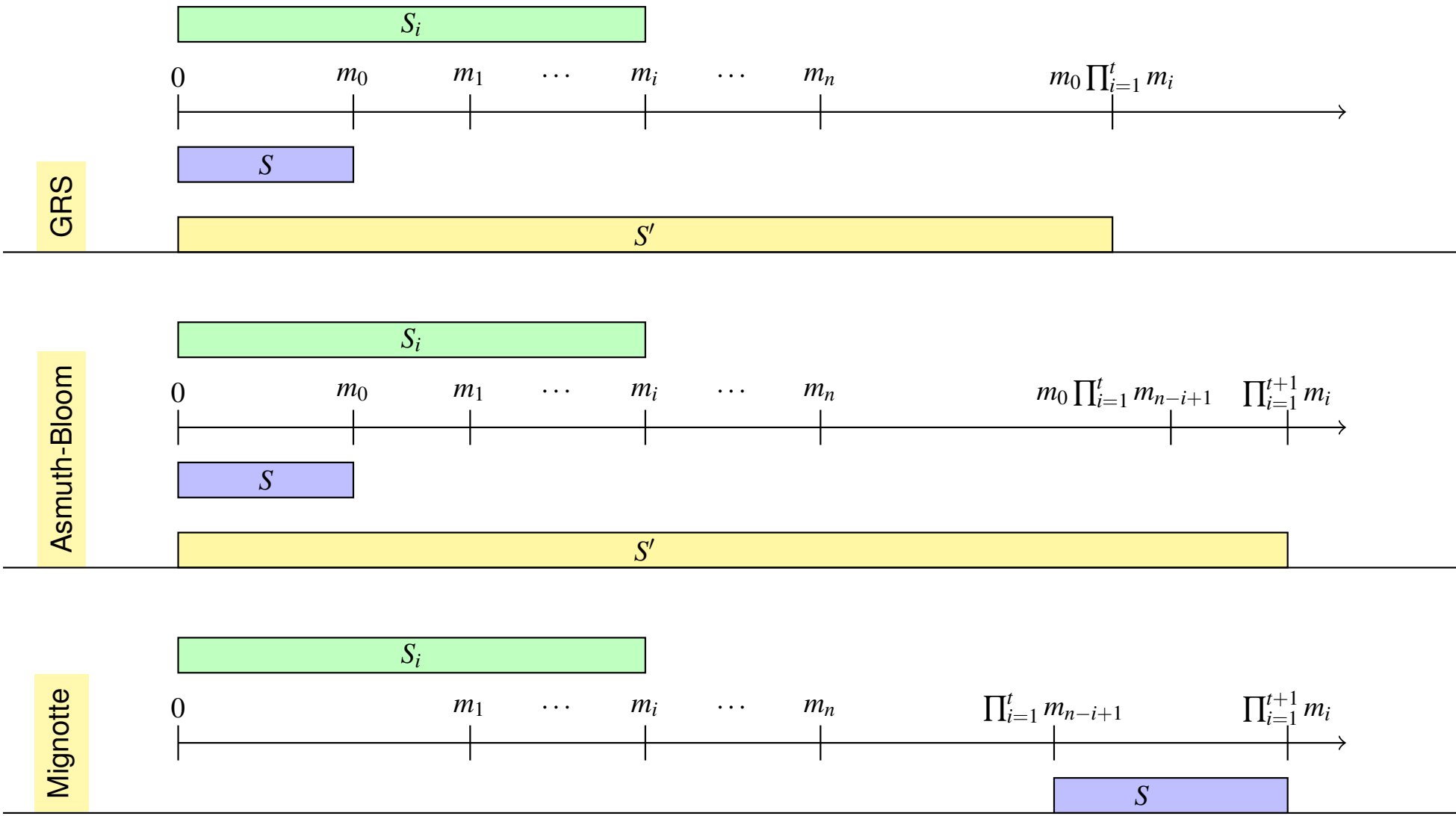
Secret and share spaces

- $[\alpha, \beta)$, where α and β depend on the public parameters
- $\mathbb{Z}_{m_i}$, for all $1 \leq i \leq n$

Secret sharing and reconstruction

- $S_i = S' \ mod \ m_i$, for all $1 \leq i \leq n$, where S' is obtained from S in some way
- Any $t+1$ distinct shares should allow an easy reconstruction of the secret

Instances: GRS, Asmuth-Bloom, Mignotte

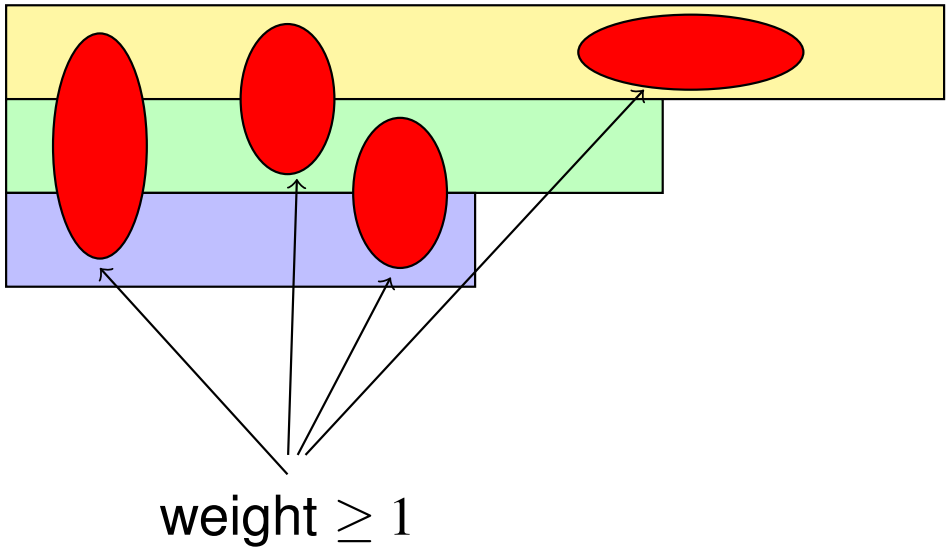


Distributive Weighted Threshold Access Structures

Council Staff $(1/t_3)$

Vice-Directors $(1/t_2)$

Directors $(1/t_1)$



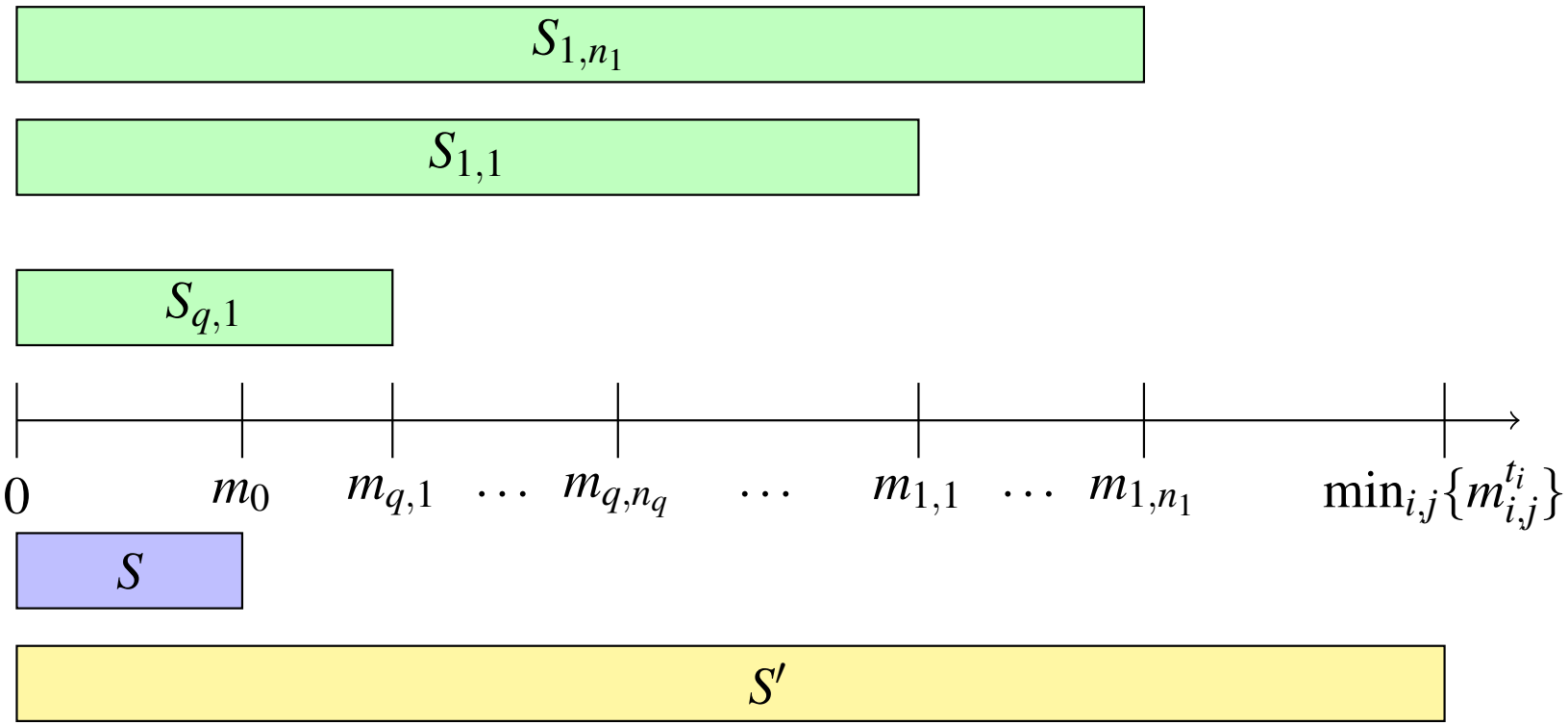
(t_3, n_3)

(t_2, n_2)

(t_1, n_1)

Distributive weighted TAS are neither conjunctive nor disjunctive MAS

CRT-realization of DWTAS



ε-sequence of co-primes: $m_0 \cdot \max_{i,j}\{m_{i,j}^{t_i-\varepsilon}\} < \min_{i,j}\{m_{i,j}^{t_i}\}$

Asymptotic Security

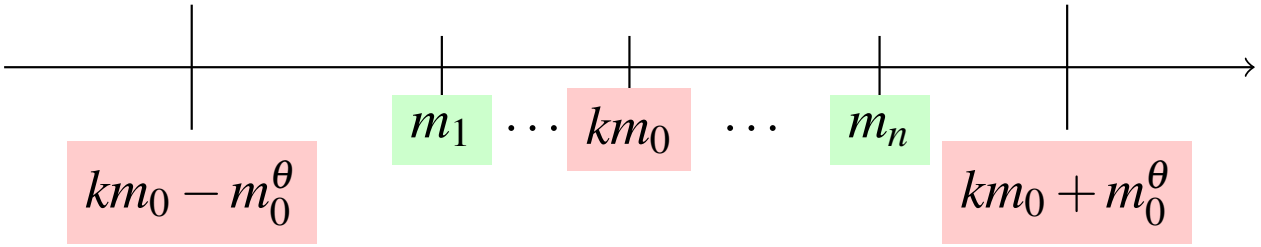
- Loss of entropy: $\Delta(y_I) = H(X) - H(X|Y_I = y_I)$, where $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$
- Asymptotic perfectness
  - $H(X) \neq 0$
  - $|\Delta(y_I)| \to 0$ as m_0 goes to infinity
- Information rate goes asymptotically to $r > 0$ if

$$\left| \frac{|\mathbb{Z}_{m_i}|}{|\mathbb{Z}_{m_0}|} - r \right| \to 0 \quad \text{as } m_0 \text{ goes to infinity}$$

- Asymptotic idealness : $r = 1$
- Perfect zero-knowledge : $\sum_{y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}} \left| P(Y_{S,I} = y_I) - P(Y_{S',I} = y_I) \right| \to 0$ as m_0 goes to infinity

Compact Sequences of Co-primes

- k-compact sequence of co-primes : $m_0, m_1 \ldots, m_n$ such that
  - $m_1 < \cdots < m_n$
  - $km_0 - m_0^\theta < m_i < km_0 + m_0^\theta$ for all $1 \leq i \leq n$ and some real number $k > 0$



- Density : $(x, x + x^\theta)$ contains compact sequences of co-primes whose length ℓ satisfies

$$\ell > \ell(x,\theta) + \left\lfloor \sum_{i=2}^{k} \frac{2ix^{\theta_i/i}}{5\log(x+x^\theta)} \right\rfloor$$

$$\ell(x,\theta) = \pi(x+x^\theta) - \pi(x) > \frac{2x^\theta}{5\log(x+x^\theta)}$$

Security of the GRS Threshold Scheme

Theorem 1

Let $k \geq 1$ be a real number. The GRS threshold scheme, under the uniform distribution on the secret space, is asymptotically perfect and its information rate goes asymptotically to k if and only if it is based on k-compact sequences of co-primes.

Corollary 2

The GRS threshold scheme, under the uniform distribution on the secret space, is asymptotically ideal if and only if it is based on 1-compact sequences of co-primes.

Theorem 3

Let $k \geq 1$ be a real number. The GRS threshold scheme based on k-compact sequences of co-primes, under the uniform distribution on the secret space, is perfect zero-knowledge.

Security of the Asmuth-Bloom Threshold Scheme

Theorem 4

Let $k \geq 1$ be an integer. The Asmuth-Bloom threshold scheme, under the uniform distribution on the secret space, is asymptotically perfect and its information rate goes asymptotically to k if and only if it is based on k-compact sequences of co-primes.

Corollary 5

The Asmuth-Bloom threshold scheme is asymptotically ideal with respect to the uniform distribution on the secret space if and only if it is based on 1-compact sequences of co-primes.

Theorem 6

Let $k \geq 1$ be an integer. The Asmuth-Bloom threshold scheme based on k-compact sequences of co-primes, under the uniform distribution on the secret space, is perfect zero-knowledge.

Security of the Mignotte Threshold Scheme

- The loss of entropy cannot be bounded from above

$$\Delta(y_I) \geq \log \frac{\beta - \alpha - 1}{\left\lfloor \frac{\beta - \alpha + \prod_{i \in I} m_i}{\prod_{i \in I} m_i} \right\rfloor}$$

- The information rate goes to 0

$$\frac{m_i}{\beta - \alpha - 1} \to 0 \quad \text{as } m_1 \text{ goes to infinity}$$

- The scheme is not perfect zero-knowledge

$$\sum_{y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}} \left| P(Y_{S,I} = y_I) - P(Y_{S',I} = y_I) \right| = 2$$

Security of Distributive Weighted TAS

Theorem 7

Distributive weighted threshold schemes do not have ideal realizations.

Theorem 8

Distributive weighted threshold schemes are asymptotically perfect if the secret is chosen uniformly from the secret space.

Theorem 9

Distributive weighted threshold schemes are perfect zero-knowledge if the secret is chosen uniformly from the secret space.

Extensions

- Verifiability (interactive, non-interactive, public) : allows participants to verify their shares for consistency
- Proactivity allows recovering of lost shares by running a share refreshment protocol
- Anonymity allows secret reconstruction without knowledge of which participants hold which shares
- Threshold changeability allows increasing the threshold parameter after the share distribution phase without further communication between the dealer and the shareholder

Concluding Remarks

1. Review of results
   - GRS and Asmuth-Bloom schemes are asymptotically ideal if and only if the schemes are based on 1-compact sequences
   - Mignotte scheme does not satisfy none of the security properties
   - DWTAS are motivated practically, and satisfy the asymptotic perfectness and perfect zero-knowledge properties
2. "Almost perfect"
3. Convergence rate