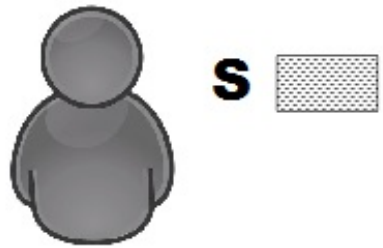
How to Split a Secret into Unknown Shares

Ruxandra F. Olimid

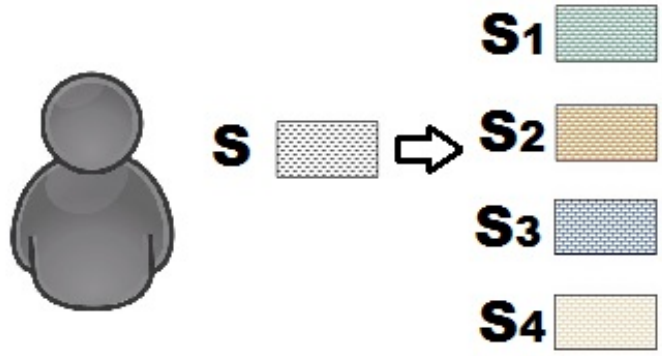
University of Bucharest

RCD - September 23, 2015

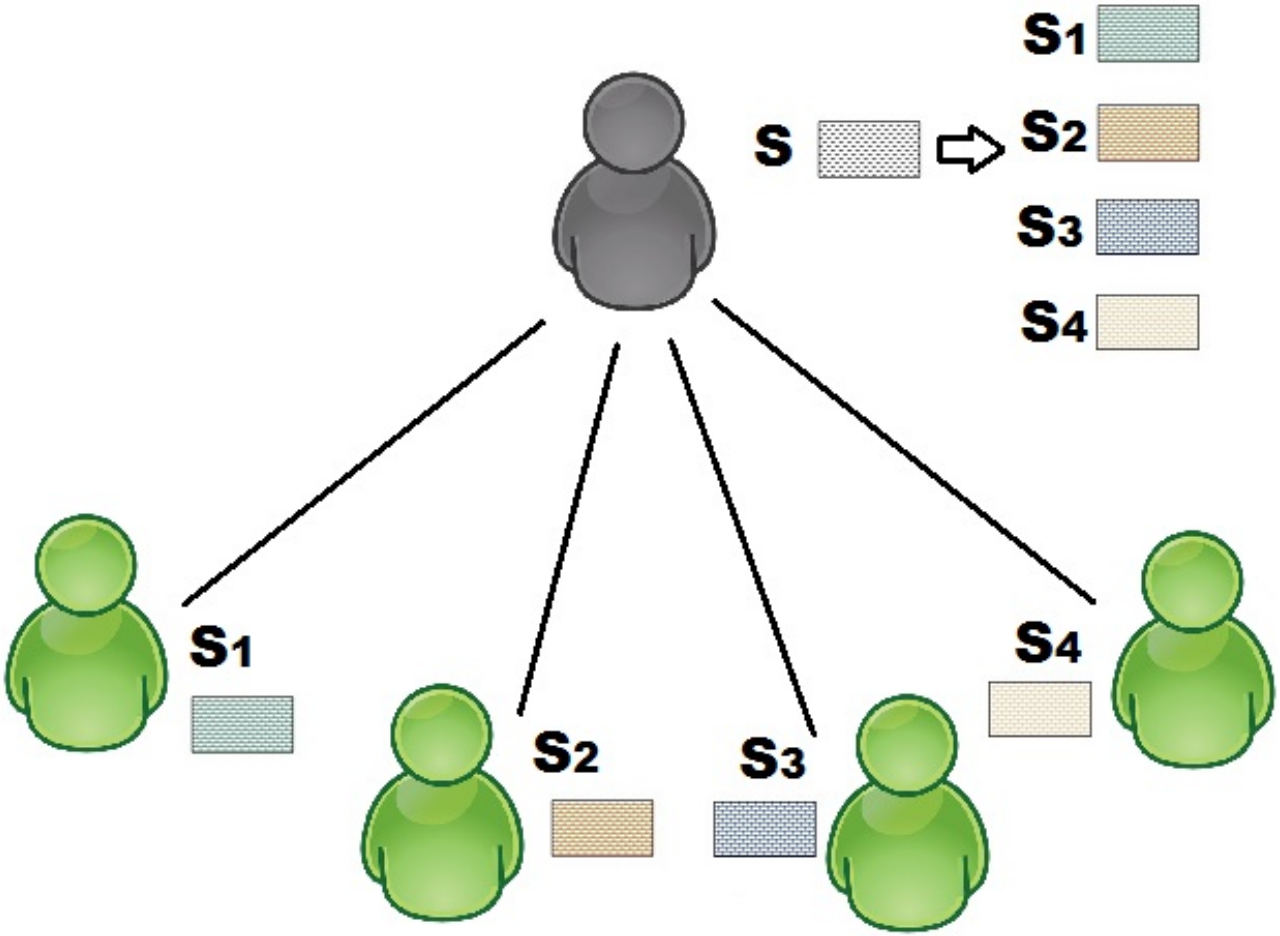
Secret Sharing



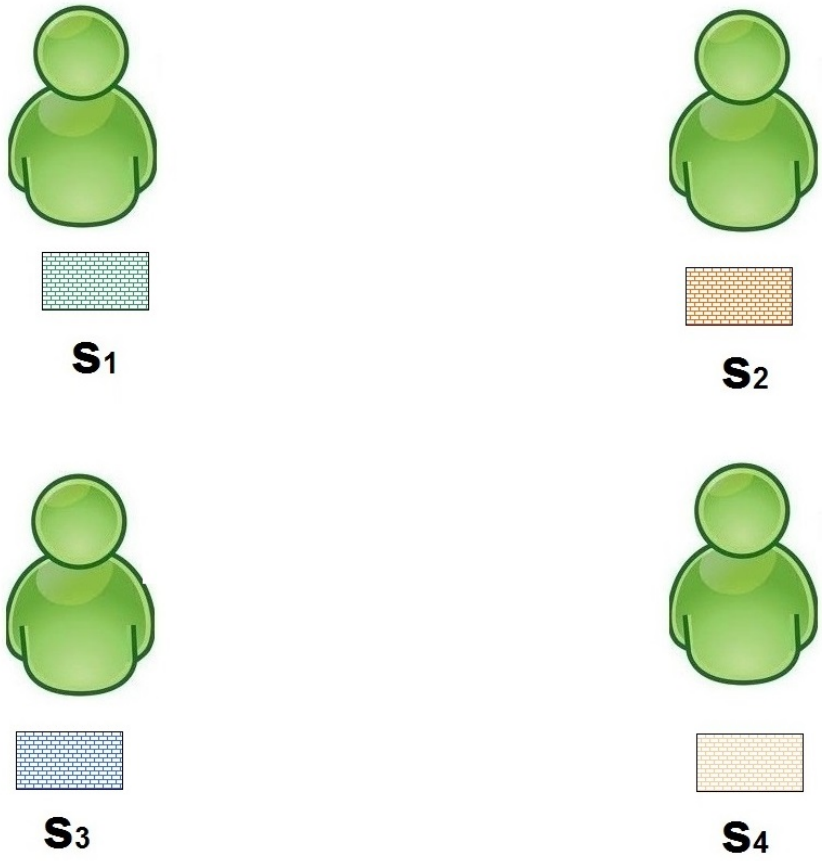
Secret Sharing



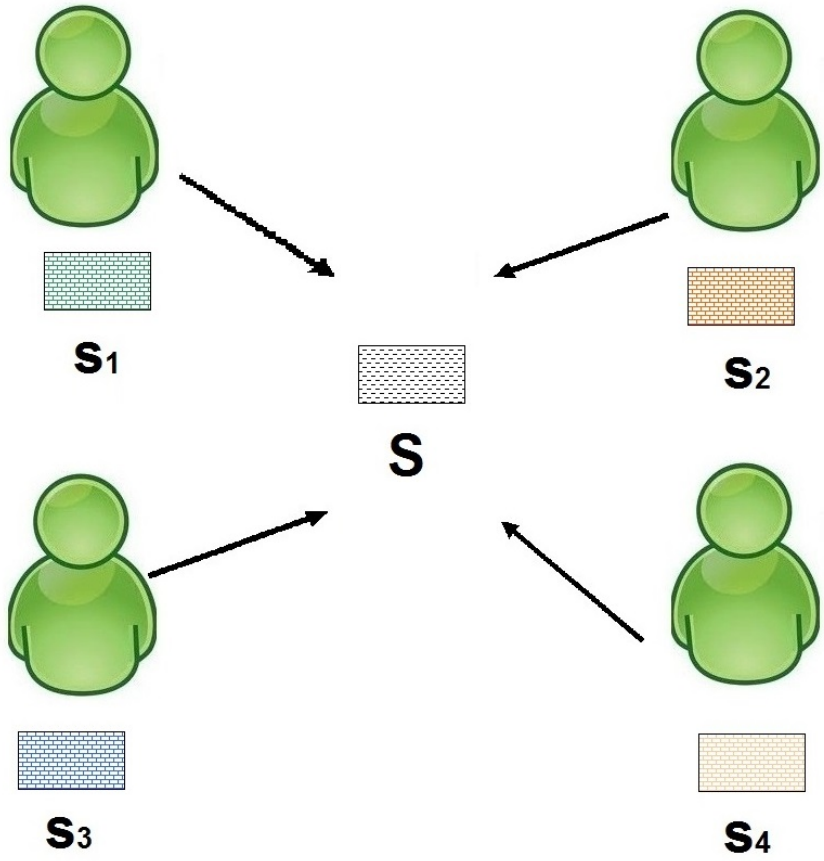
Secret Sharing



Secret Sharing



Secret Sharing



Cryptographic Anonymity

- Controversial reconstruction: it is argued if the secret should be reconstructed or not
- Coalition statistics: it is not desired to have any information about coalitions that are more likely to reconstruct

[Guillermo, Martin, O'Keefe 2003]

Cryptographic Anonymity

- Controversial reconstruction: it is argued if the secret should be reconstructed or not
- Coalition statistics: it is not desired to have any information about coalitions that are more likely to reconstruct

[Guillermo, Martin, O'Keefe 2003]

What about the dealer?

Cryptographic Anonymity w.r.t. Dealer

- Existing work: all-or-nothing secret sharing

[Grigoriev, Shpilrain 2013]

- Our contribution: threshold secret sharing (Shamir's scheme)

Shamir's Secret Sharing Scheme [S'79]

1. *Secret Sharing Phase.* *The dealer picks a* $t-1$ *degree random polynomial*

$$f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \pmod{q} \tag{1}$$

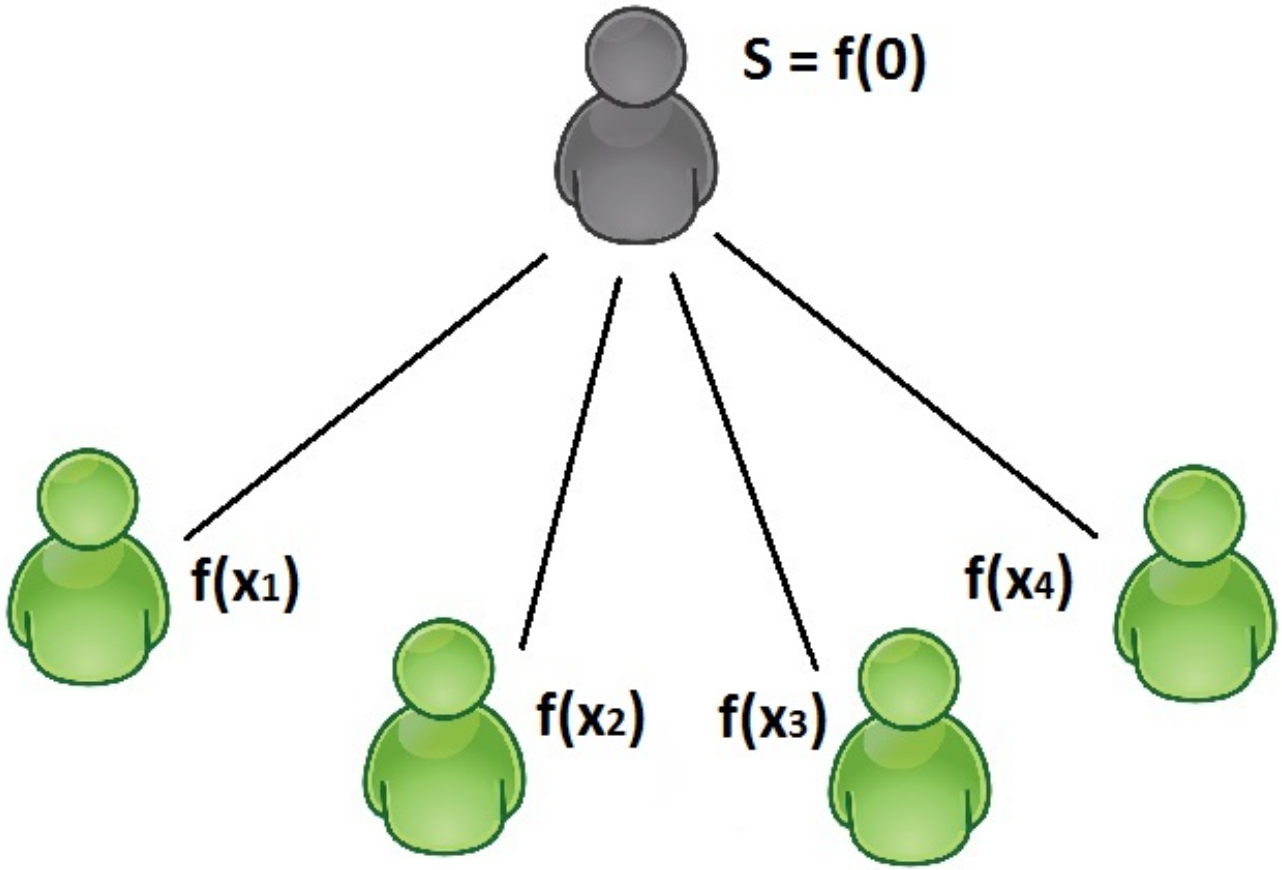
s.t. $a_0 = S$ *and* $a_i \in \mathbb{Z}_q, i = 1, \ldots, t-1$.

2. *Shares Distribution Phase.* *The dealer transmits the share* $f(x_i)$ *to the participant* U_i, $i = 1, \ldots, n$, *via a secure channel.*

3. *Reconstruction Phase.* *Given at least* t *points* $(x_i, f(x_i))$ *with distinct* x_i*'s, the unique polynomial* $f(x)$ *can be found as:*

$$f(x) = \sum_{i=1}^{t} f(x_i) \prod_{1 \le j \le t, i \ne j} \frac{x - x_j}{x_i - x_j} \tag{2}$$

Shamir's Secret Sharing Scheme [S'79]



Simple Proposals

- Solution 1: the dealer *knows* the polynomial, but does *NOT know* the values where the polynomial is evaluated in
- Solution 2: the dealer does *NOT know* the polynomial, but *knows* the values where the polynomial is evaluated in

First Proposal

First Proposal

Correctness and secrecy hold from construction.

First Proposal

Correctness and secrecy hold from construction.

The dealer does not learn the shares (from the security of OPE)

Second Proposal

$$S = \sum_{i=1}^{n} s_i \qquad f_i(0) = s_i \qquad f(x_i) = \sum_{j=1}^{n} f_j(x_i)$$

Reconstr.: $S = \sum_{i=1}^{t+1} f(x_i) \prod_{1 \le j \le t+1, i \neq j} \frac{x_j}{x_j - x_i}$

Second Proposal

$$S = \sum_{i=1}^{n} s_i \qquad f_i(0) = s_i \qquad f(x_i) = \sum_{j=1}^{n} f_j(x_i)$$

Reconstr.: $S = \sum_{i=1}^{t+1} f(x_i) \prod_{1 \le j \le t+1, i \neq j} \frac{x_j}{x_j - x_i}$

Correctness and secrecy hold from construction.

Second Proposal

$$S = \sum_{i=1}^{n} s_i \qquad f_i(0) = s_i \qquad f(x_i) = \sum_{j=1}^{n} f_j(x_i)$$

Reconstr.: $S = \sum_{i=1}^{t+1} f(x_i) \prod_{1 \le j \le t+1, i \ne j} \frac{x_j}{x_j - x_i}$

Correctness and secrecy hold from construction.

The dealer does not learn the final shares.

Work in progress ...

Thank you!

This work was supported by the strategic grant POSDRU/159/1.5/S/137750, Project Doctoral and Postdoctoral programs support for increased competitiveness in Exact Sciences research cofinanced by the European Social Found within the Sectorial Operational Program Human Resources Development 2007 2013.