Hierarchical and Dynamic Threshold Paillier Cryptosystem without Trusted Dealer

20th Central European Conference on Cryptology

June 24th-26th, 2020

Andreas Klinger[1], Stefan Wüller[1], Giulia Traverso[2], and Ulrike Meyer[1]

[1] RWTH Aachen University

[2] Technische Universität Darmstadt

UnRAVeL Research Training Group – Uncertainty and Randomness in Algorithms, Verification, and Logic

RWTH AACHEN UNIVERSITY

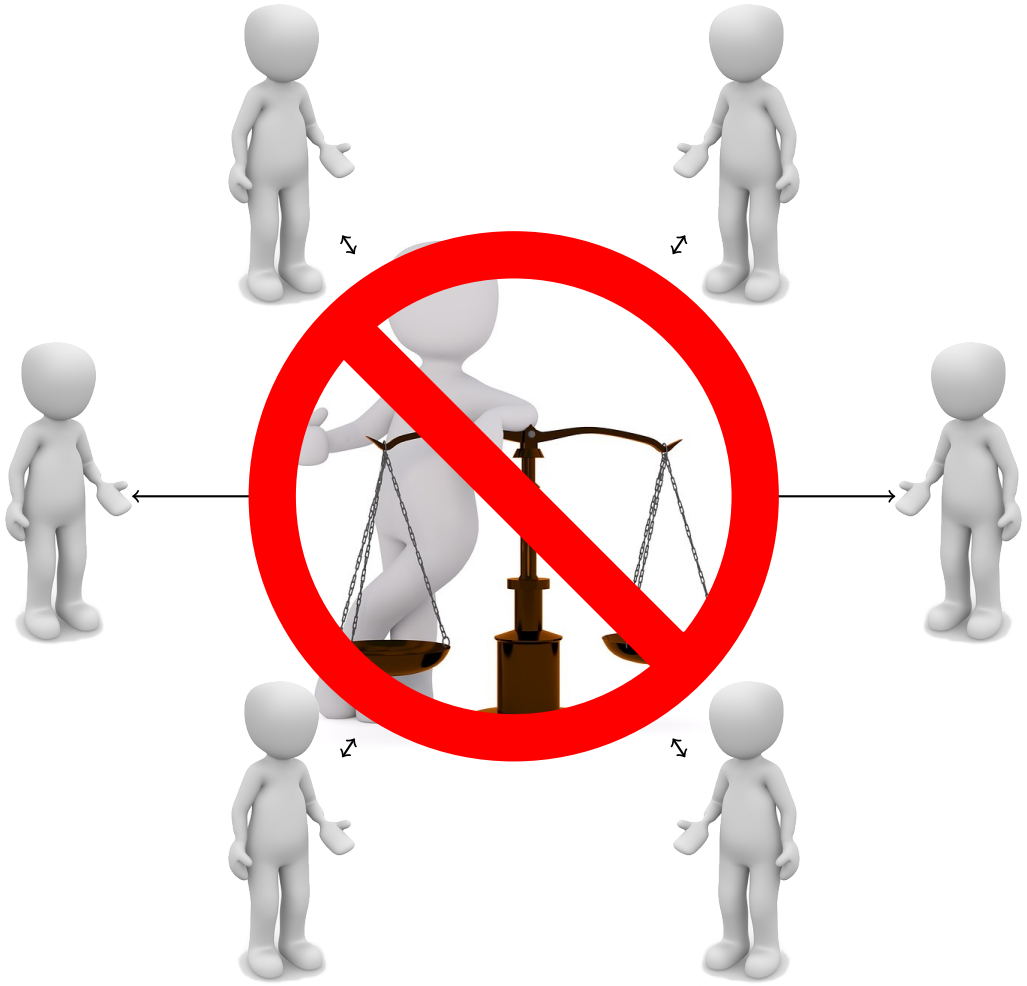
IT SEC Lehr- und Forschungsgebiet IT-Security

RWTH AACHEN UNIVERSITY

Introduction

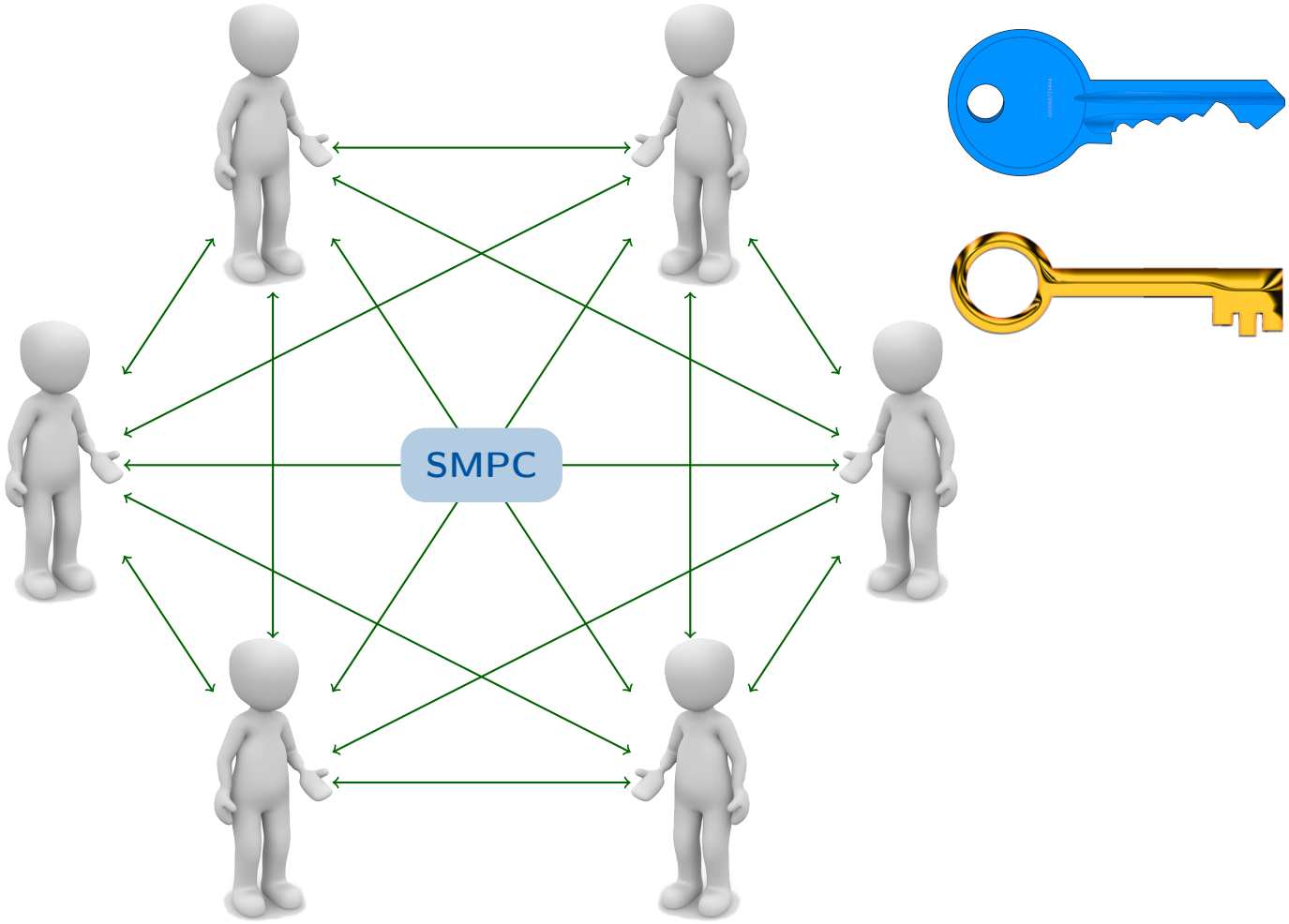
Andreas Klinger, Stefan Wüller, Giulia Traverso, and Ulrike Meyer

Secure Multi Party Computation

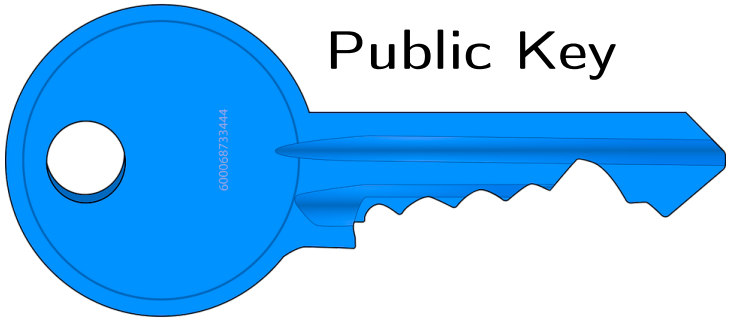


Andreas Klinger, Stefan Wüller, Giulia Traverso, and Ulrike Meyer

Secure Multi Party Computation

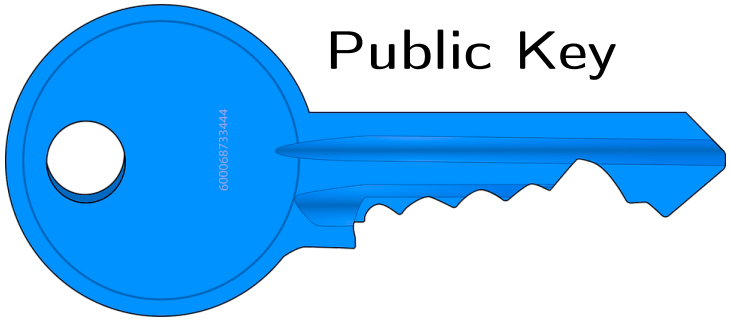


Public Key Cryptography



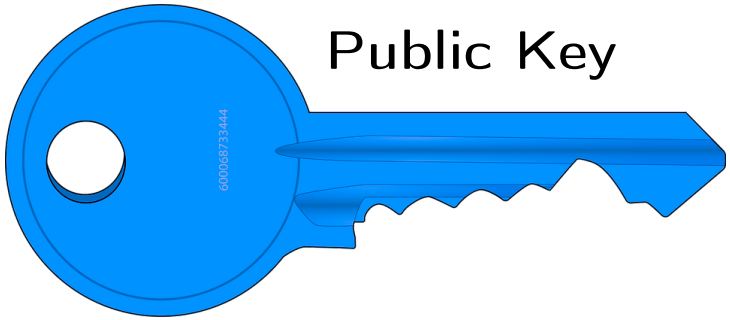
Andreas Klinger, Stefan Wüller, Giulia Traverso, and Ulrike Meyer

Public Key Cryptography



Andreas Klinger, Stefan Wüller, Giulia Traverso, and Ulrike Meyer

Public Key Cryptography

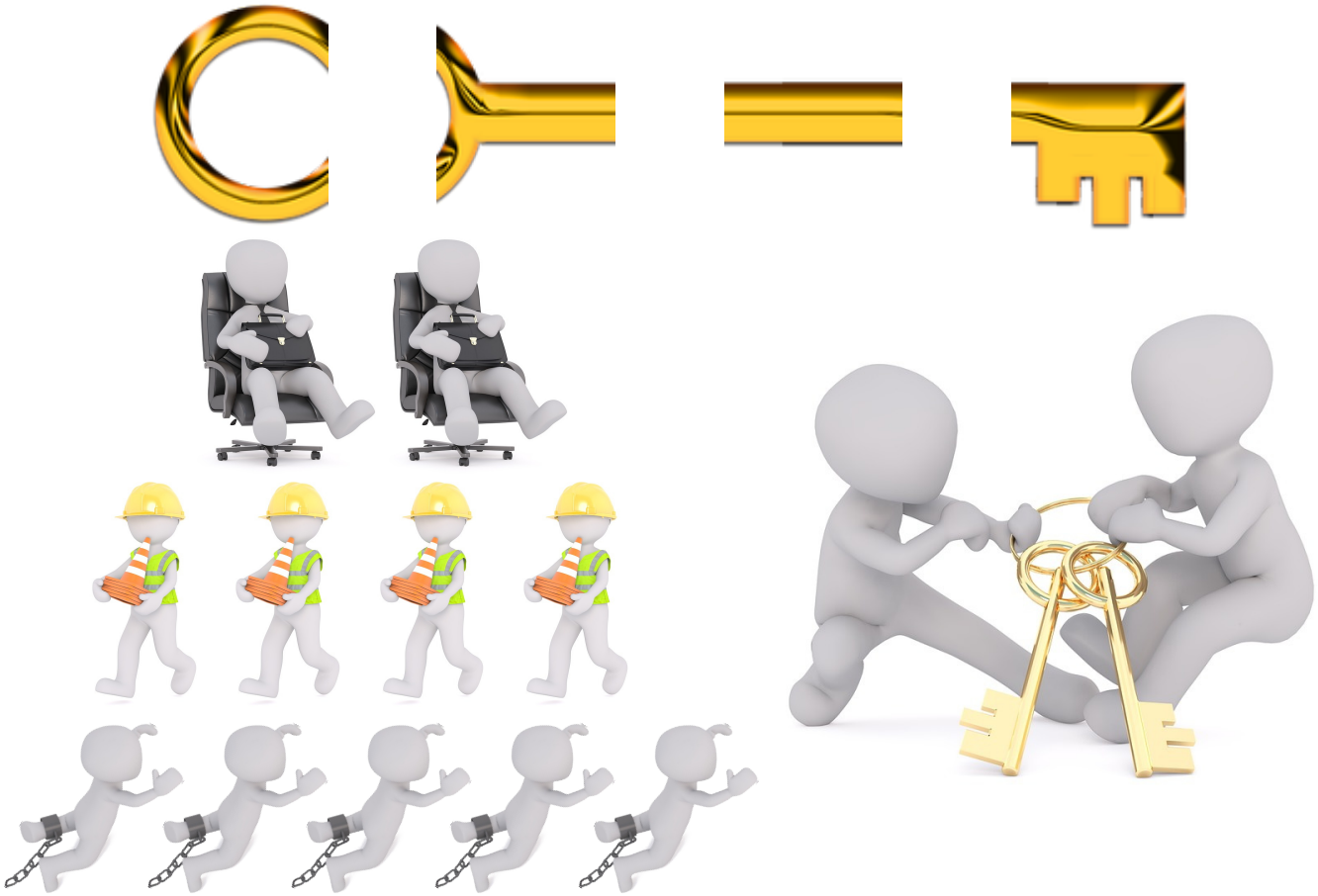


Andreas Klinger, Stefan Wüller, Giulia Traverso, and Ulrike Meyer

Splitting the Key

Andreas Klinger, Stefan Wüller, Giulia Traverso, and Ulrike Meyer

Splitting the Key



Andreas Klinger, Stefan Wüller, Giulia Traverso, and Ulrike Meyer

Hierarchical and Dynamic Threshold Paillier Cryptosystem without Trusted Dealer

Main Properties

- Enables ***hierarchical*** access structures
- Allows to ***add*** and ***remove*** share holders
- No trusted-third party required
- Allows homomorphic ***addition***
- Secure in the presence of a ***malicious*** adversary

Usage Scenarios

- Enforce a certain hierarchy
  → Enforce the presence of certain parties
- Suitable for SMPC
  → Reuse of computations (encrypted results)
  → Audit computations

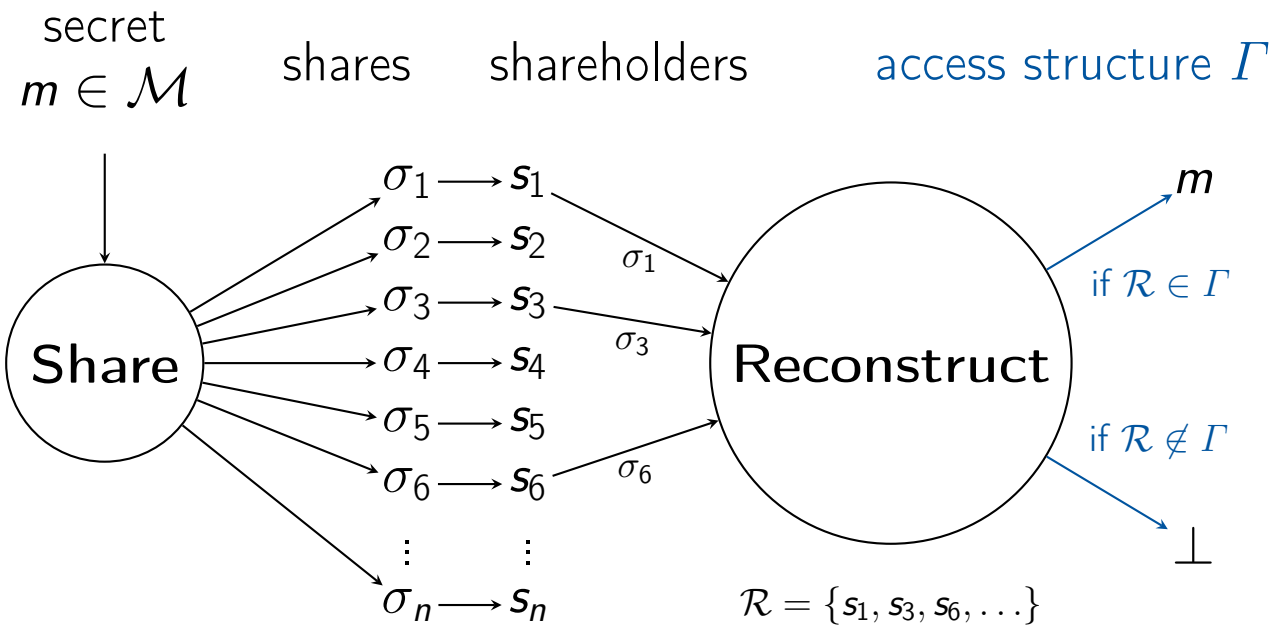
- Government, Electronic Votes
- Companies, Financial system

Secret Sharing Schemes

Secret Sharing Scheme

Definition (Secret Sharing Scheme)

A ***secret sharing scheme*** is a pair of PPT algorithms ***Share*** and *Reconstruct*.

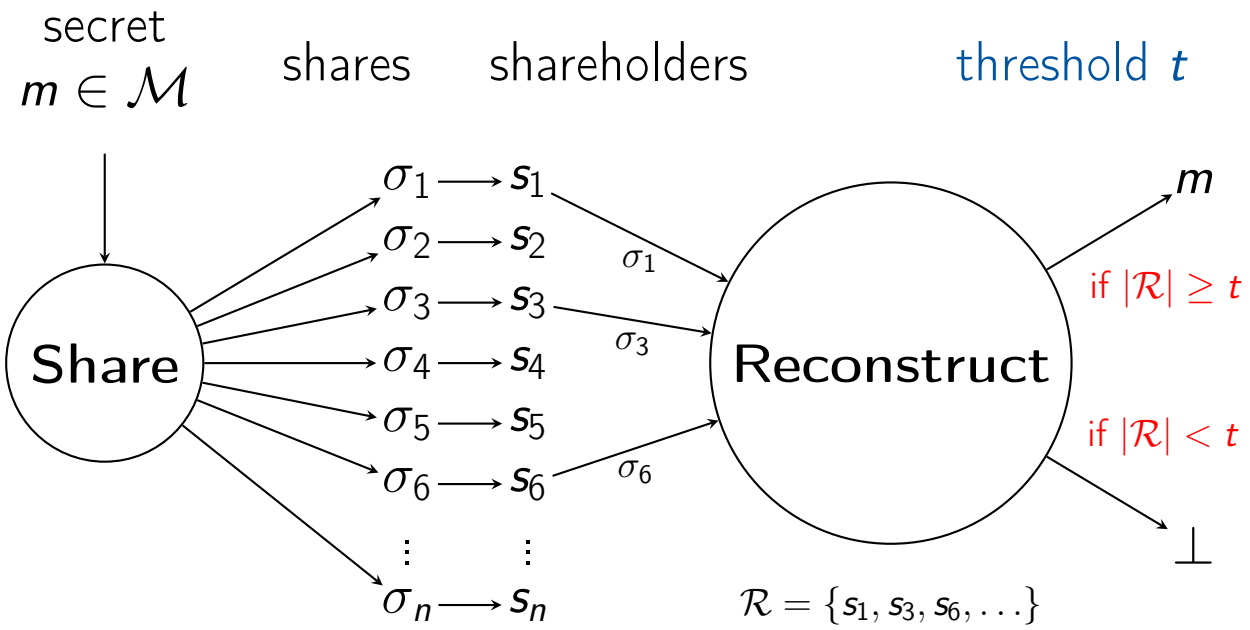


Andreas Klinger, Stefan Wüller, Giulia Traverso, and Ulrike Meyer

Secret Sharing Scheme

Definition (Secret Sharing Scheme)

A ***secret sharing scheme*** is a pair of PPT algorithms ***Share*** and ***Reconstruct***.

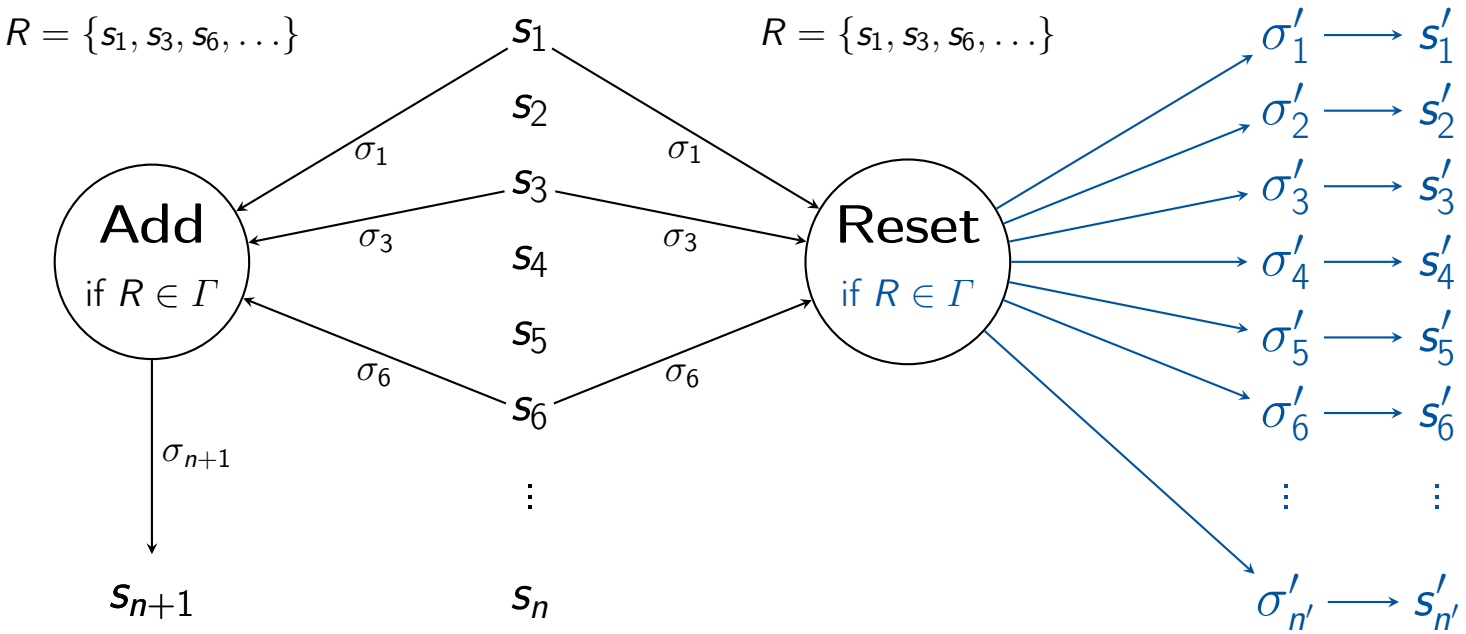


(t, n) Threshold Secret Sharing Scheme

Dynamic Secret Sharing

Definition (Dynamic Secret Sharing)

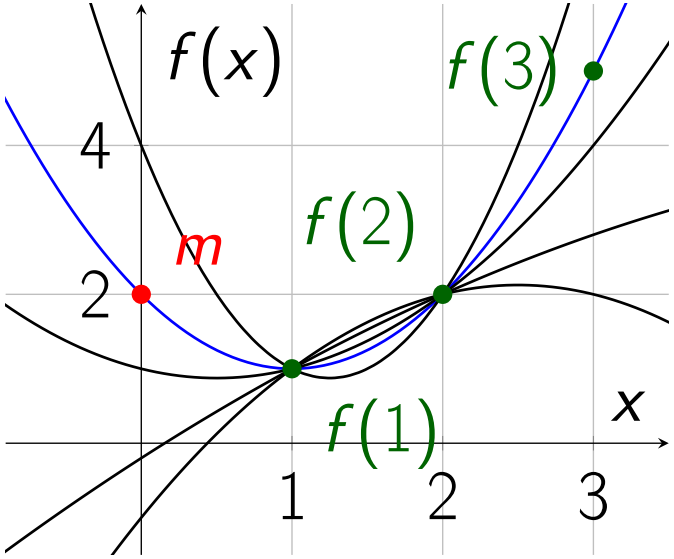
Same as secret sharing scheme (`Share` and `Reconstruct`), but with two additional PPT algorithms ***Add*** and ***Reset***.



(t, n) Threshold Secret Sharing Scheme

Example (Shamir's (t, n) Threshold Secret Sharing Scheme)

- Construct polynomial $f(x)$ of degree $t - 1$ where $f(0) = m$
- Distribute $f(i) = \sigma_i$ to shareholder s_i for $i \in \{1, \ldots, n\}$

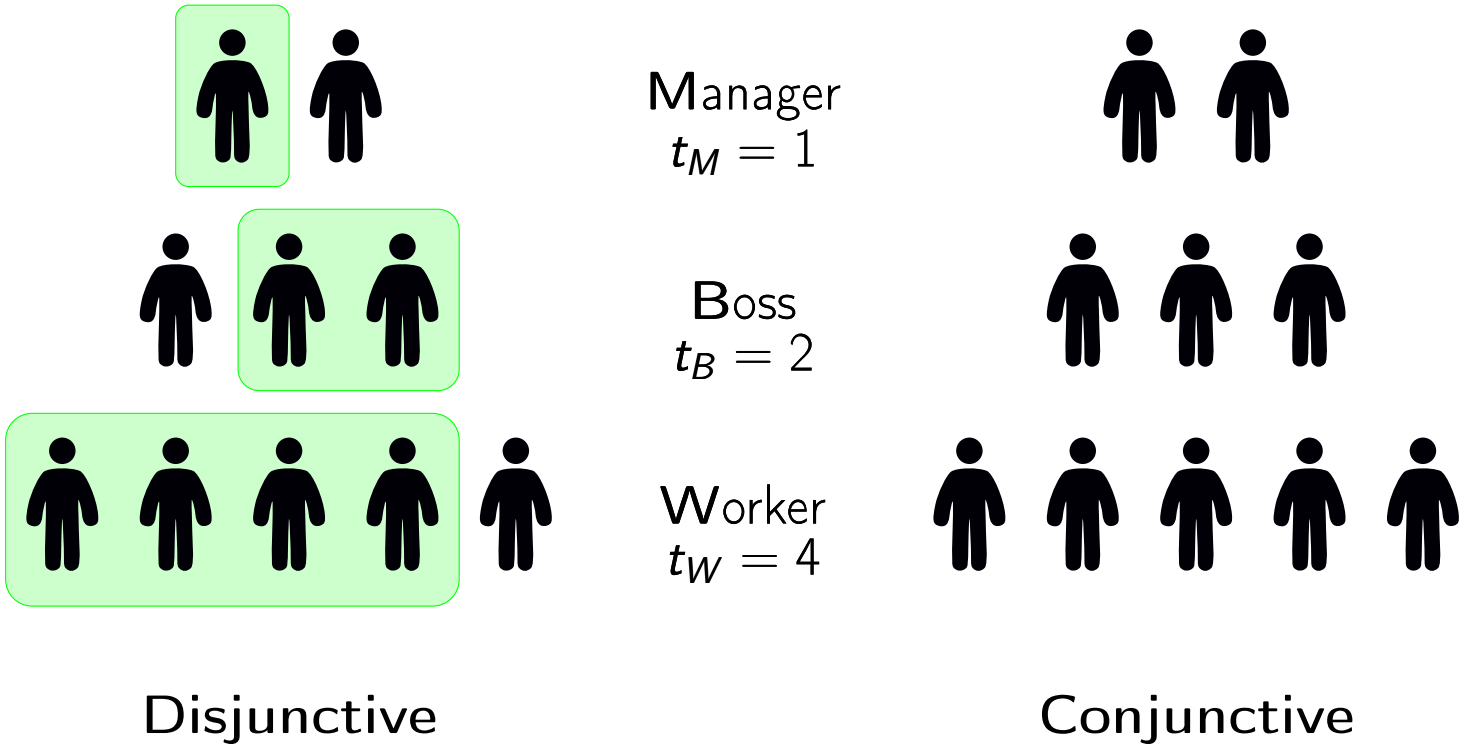


A $(3, 3)$ threshold scheme

$$f(x) = 2 - 2x + x^2$$
$$f(0) = 2 = m$$
$$f(1) = 1 \rightarrow s_1$$
$$f(2) = 2 \rightarrow s_2$$
$$f(3) = 5 \rightarrow s_3$$

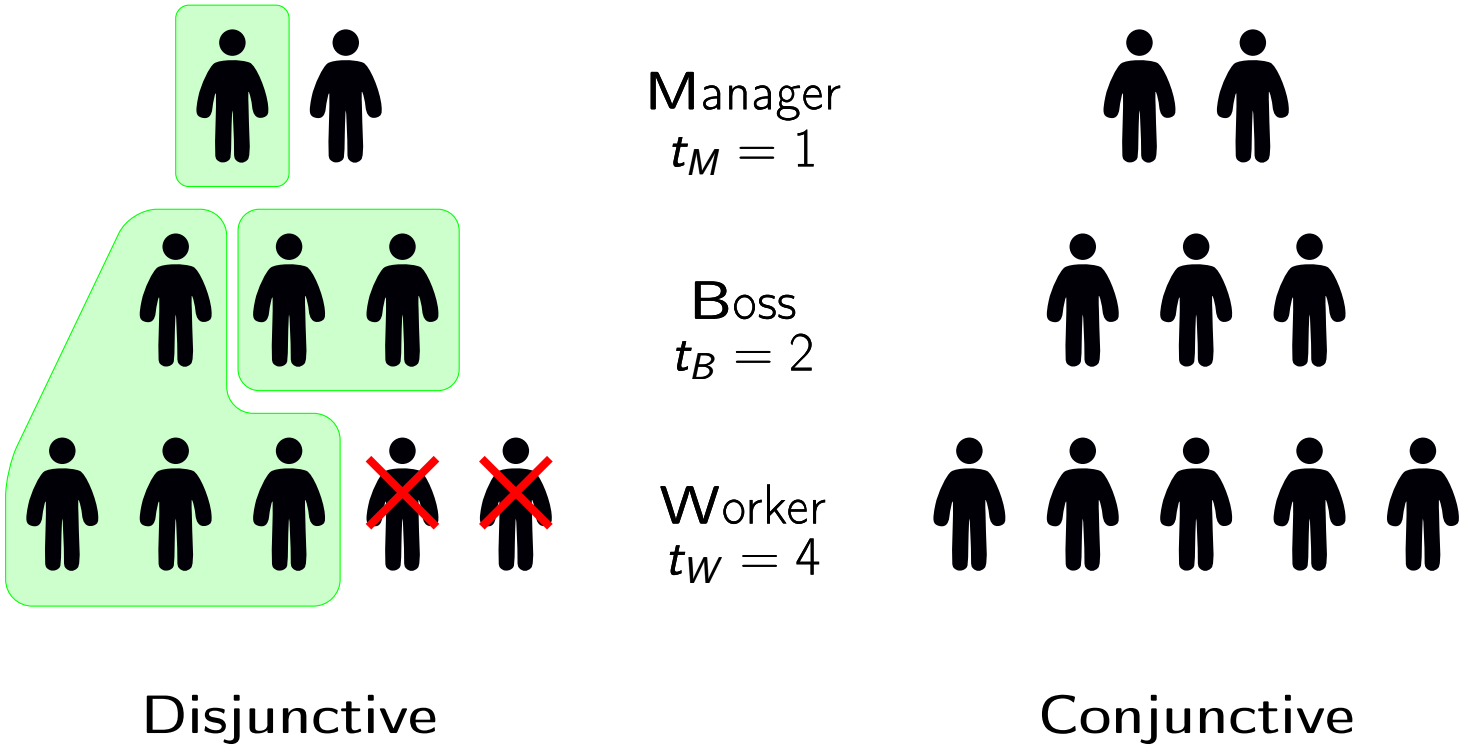
Adi Shamir. "How to Share a Secret". In: *Commun. ACM* 22.11 (1979)

Hierarchical Secret Sharing



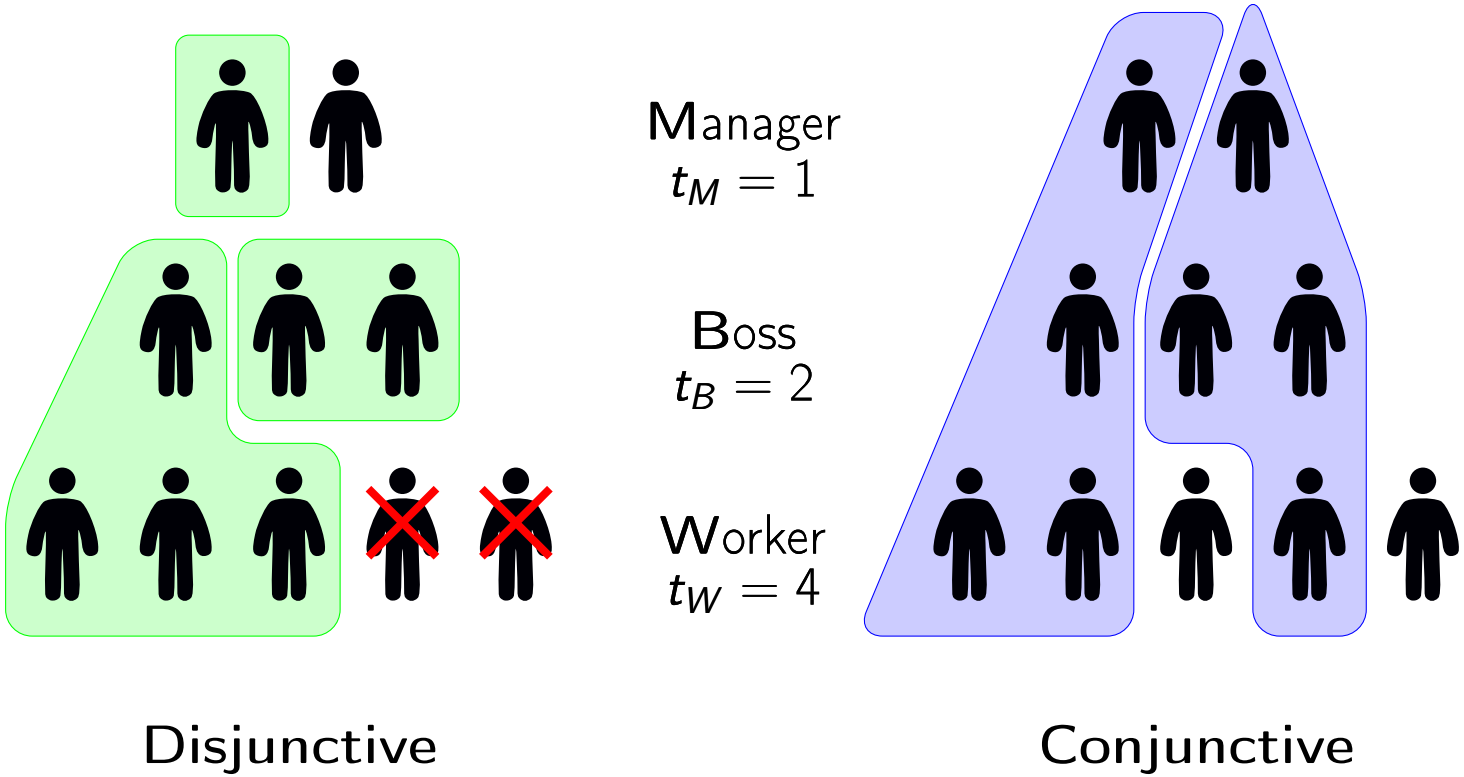
Tamir Tassa. "Hierarchical Threshold Secret Sharing". In: *Journal of Cryptology* 20.2 (2007)

Hierarchical Secret Sharing



Tamir Tassa. "Hierarchical Threshold Secret Sharing". In: *Journal of Cryptology* 20.2 (2007)

Hierarchical Secret Sharing

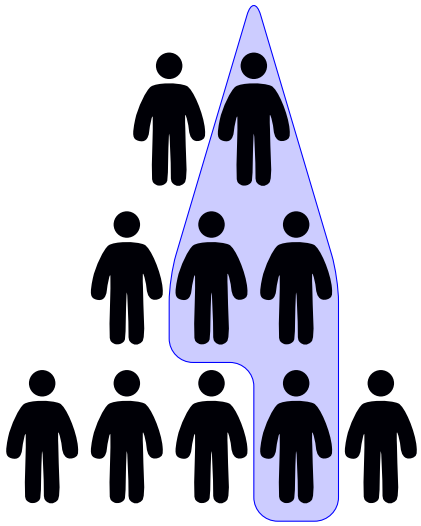


Tamir Tassa. "Hierarchical Threshold Secret Sharing". In: *Journal of Cryptology* 20.2 (2007)

Hierarchical Secret Sharing

Example (Secret Sharing with Birkhoff Interpolation - Conjunctive)

- Setup: Secret $m = a_0$ and thresholds $0 < t_0 < t_1 < \ldots < t_\ell = t$
- Construct polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1}$
- The i-th shareholder on level j gets the **t_{j-1}-th derivative** $f^{t_{j-1}}(i)$



Conjunctive

$t_0 = 1$ $\quad f^0(1)$ $f^0(2)$

$t_1 = 2$ $\quad f^1(1)$ $f^1(2)$ $f^1(3)$

$t_2 = 4$ $\quad f^2(1)$ $f^2(2)$ $f^2(3)$ $f^2(4)$ $f^2(5)$

$$f^0(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$$
$$f^1(x) = a_1 + 2a_2 x + 3a_3 x^2$$
$$f^2(x) = 2a_2 + 6a_3 x$$

Tamir Tassa. "Hierarchical Threshold Secret Sharing". In: *Journal of Cryptology* 20.2 (2007)

Hierarchical Secret Sharing

Reconstruction

- The secret is basically computed as $m = \sum_{i=1}^{4} \frac{\sigma_i \cdot \mathrm{A}_i}{\mathrm{A}}$
- A and A_i are determinants of publicly known matrices
- σ_i is the share of shareholder i

Add Shareholder

- Each shareholder computes a partial interpolation polynomial $f_i(x)$ s. t. $f(x) = \sum_i f_i(x)$
- The new share σ_y is then basically $\sum_i f_i(y)$

Reset Access structure

- Each shareholder computes a partial secret m_i s. t. $m = \sum_i m_i$
- Each shareholder shares m_i with a new polynomial $f_i'(x)$
- The new share σ_y' is then basically $\sum_i f_i'(y)$

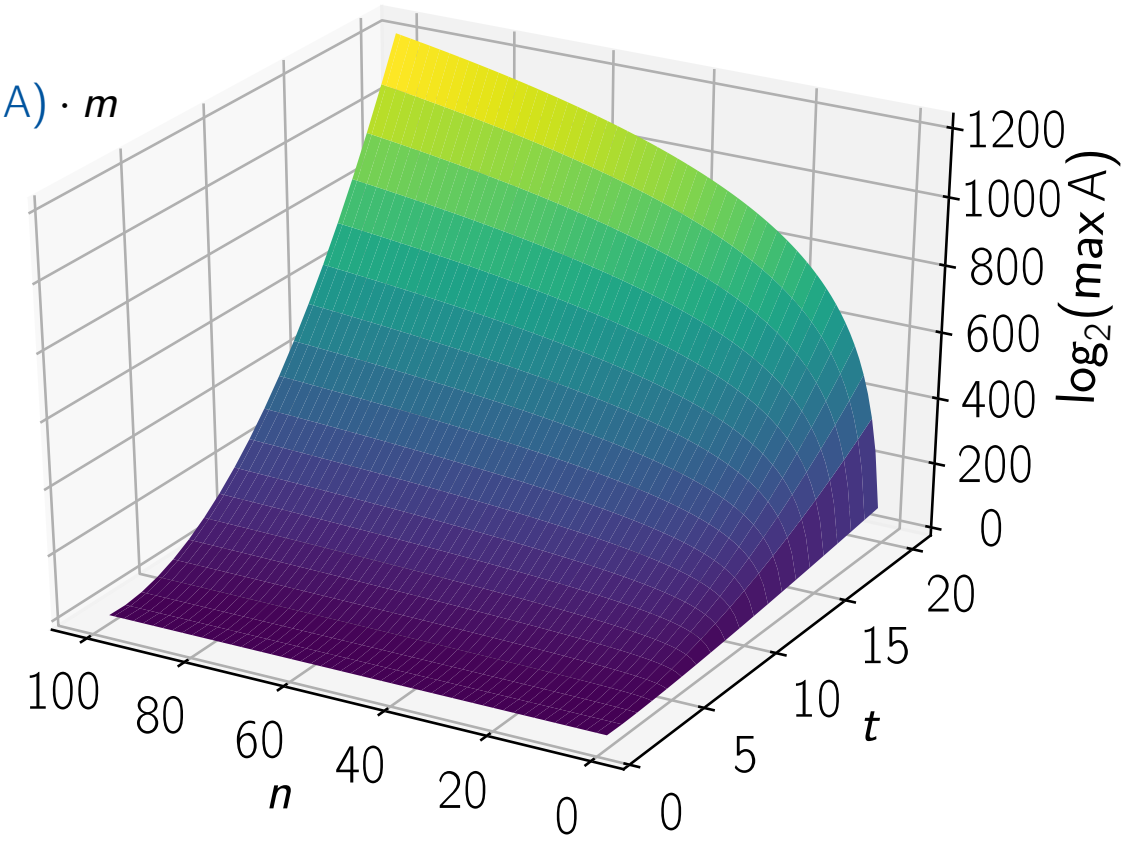
Note, we left out the derivatives/levels that are actually required.

Traverso et al. "Dynamic and Verifiable Hierarchical Secret Sharing". In: *ITS*. LNCS. Springer, 2016

“Secret Sharing” over the Integers

Basic Idea

- Choose coefficients from a **large** interval
- Flat: secret $= n! \cdot m$
- Hierarchical: secret $= \mathrm{lcm}(1, \ldots, A) \cdot m$



Verifiability

- Pedersen Commitments
- Zero-Knowledge Proofs

Paillier Cryptosystem

Paillier Cryptosystem - Properties

- **Asymmetric** and **probabilistic** cryptosystem
- **Semantically secure**
  $\rightarrow$ one message encrypts to many ciphertexts

- **Homomorphic addition**

$$E(m_1) +_h E(m_2) := E(m_1) \cdot E(m_2) = E(m_1 + m_2)$$

  - Homomorphic scalar multiplication

$$E(m) \times_h a := E(m)^a = E(m \cdot a)$$

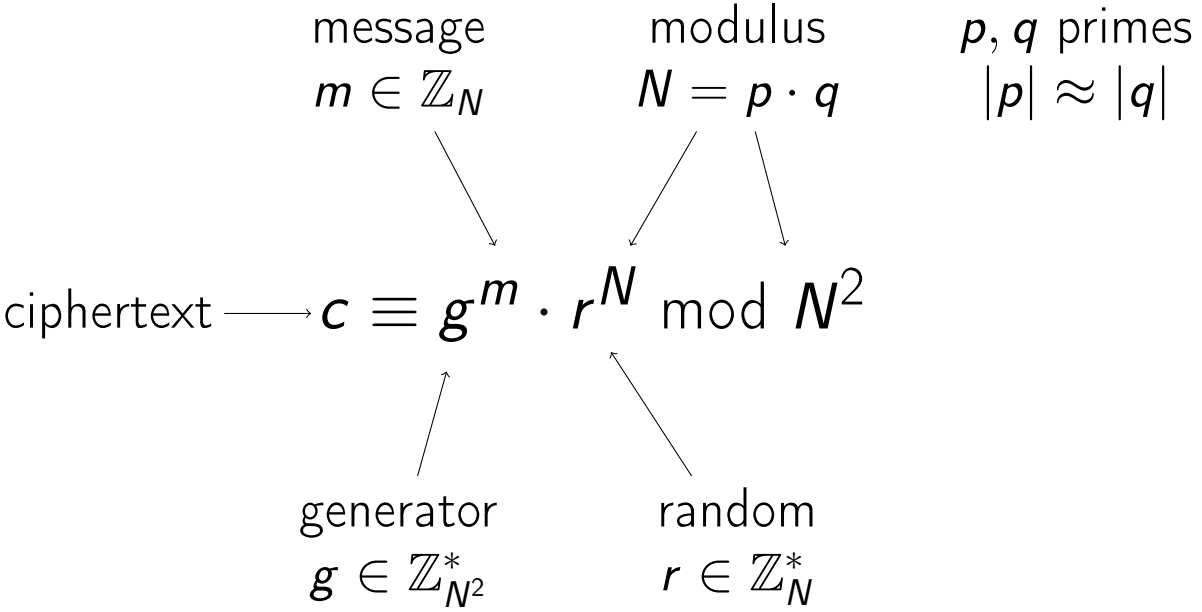
- **Self-Blinding** by adding a fresh encryption of "0"

$$E(m) +_h E(0)$$

Pascal Paillier. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". In: *EUROCRYPT*. Lecture Notes in Computer Science. Springer, 1999

Paillier Cryptosystem - Simplified

Encryption



Decryption (simplified)

with private key $\lambda(N) = \mathsf{lcm}(p-1, q-1)$

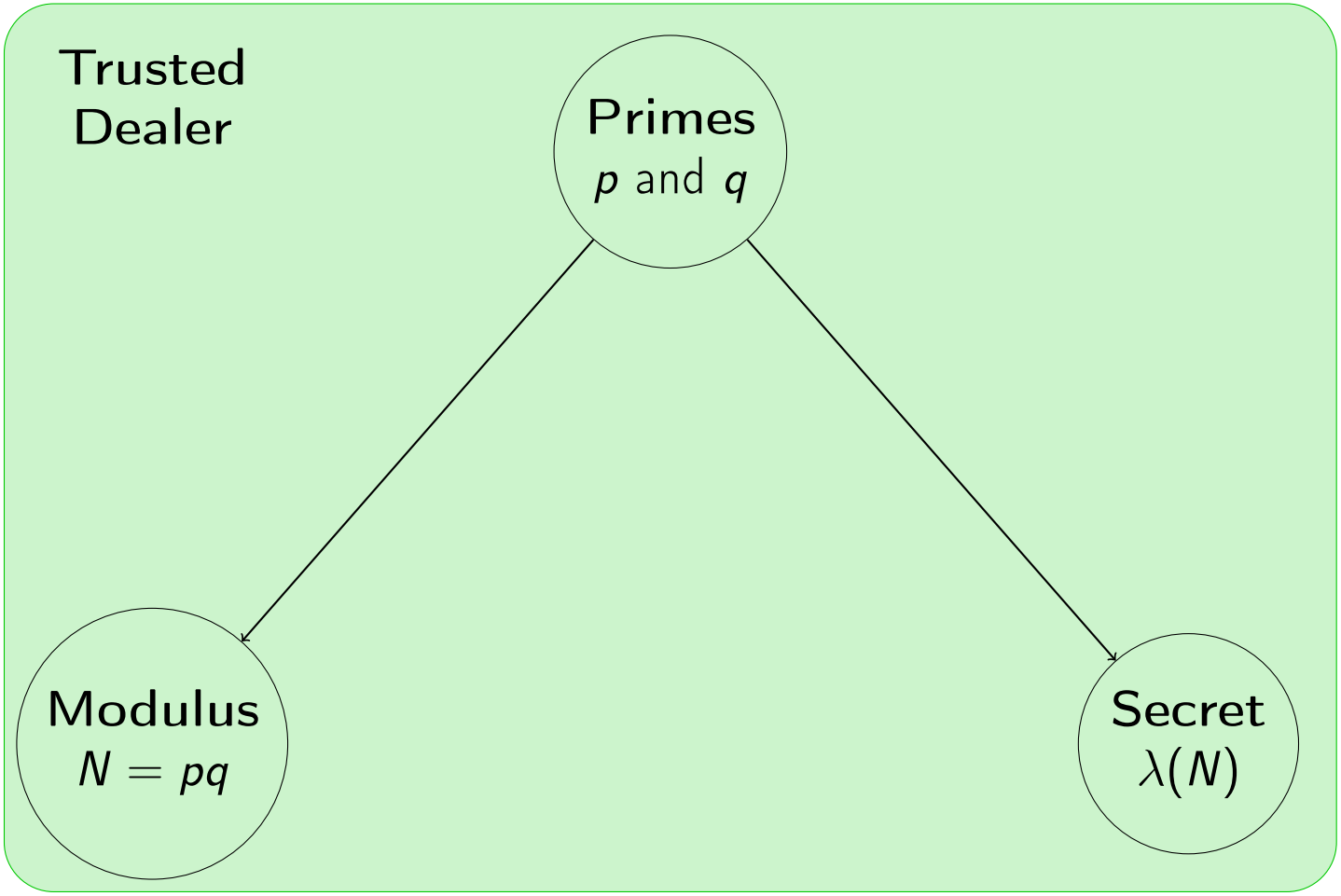
$$c^{\lambda(N)} \rightarrow m$$

Pascal Paillier. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". In: *EUROCRYPT*. Lecture Notes in Computer Science. Springer, 1999

Hierarchical and Dynamic Threshold Paillier Cryptosystem without Trusted Dealer

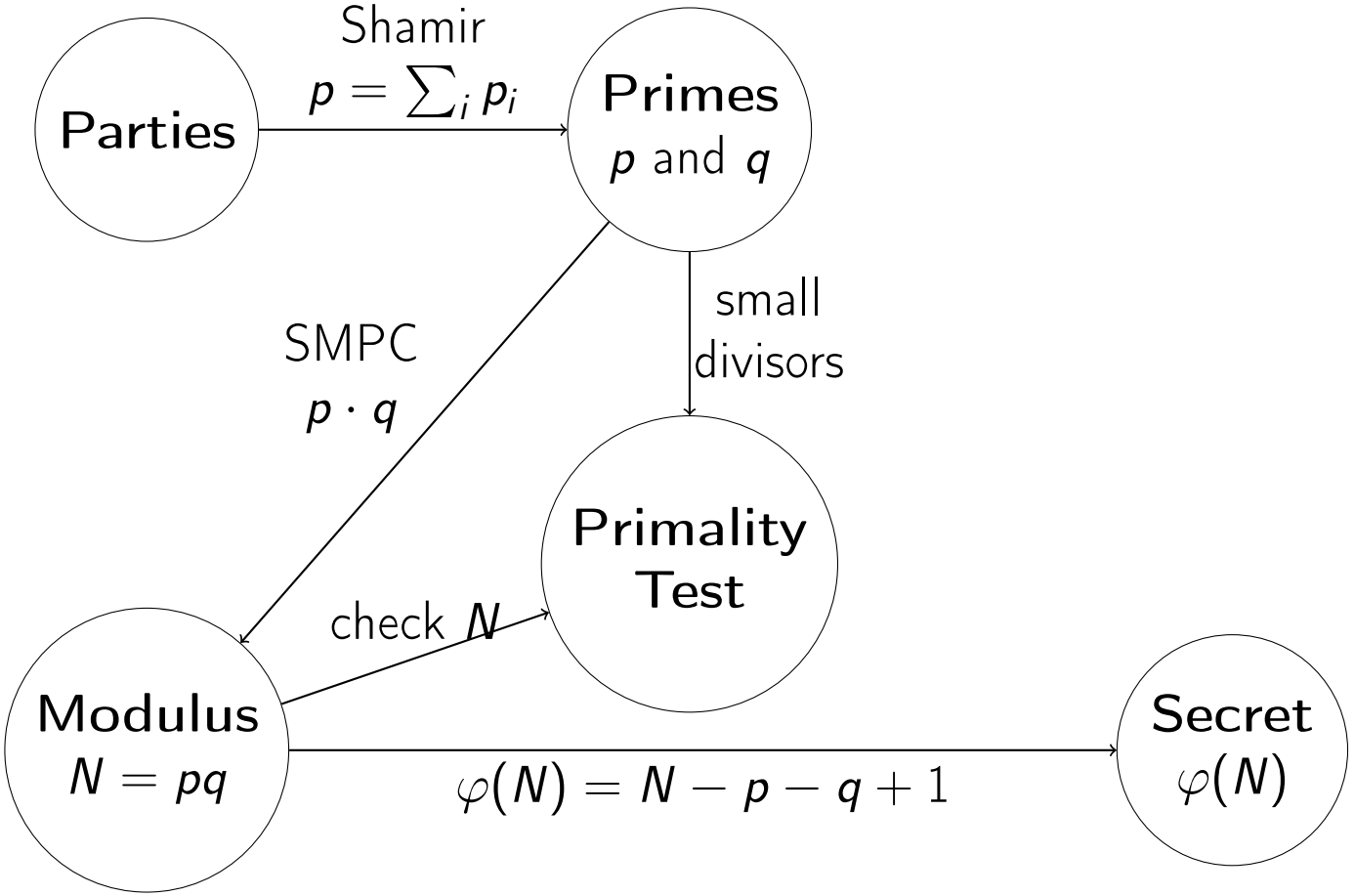
Andreas Klinger, Stefan Wüller, Giulia Traverso, and Ulrike Meyer

Threshold Paillier



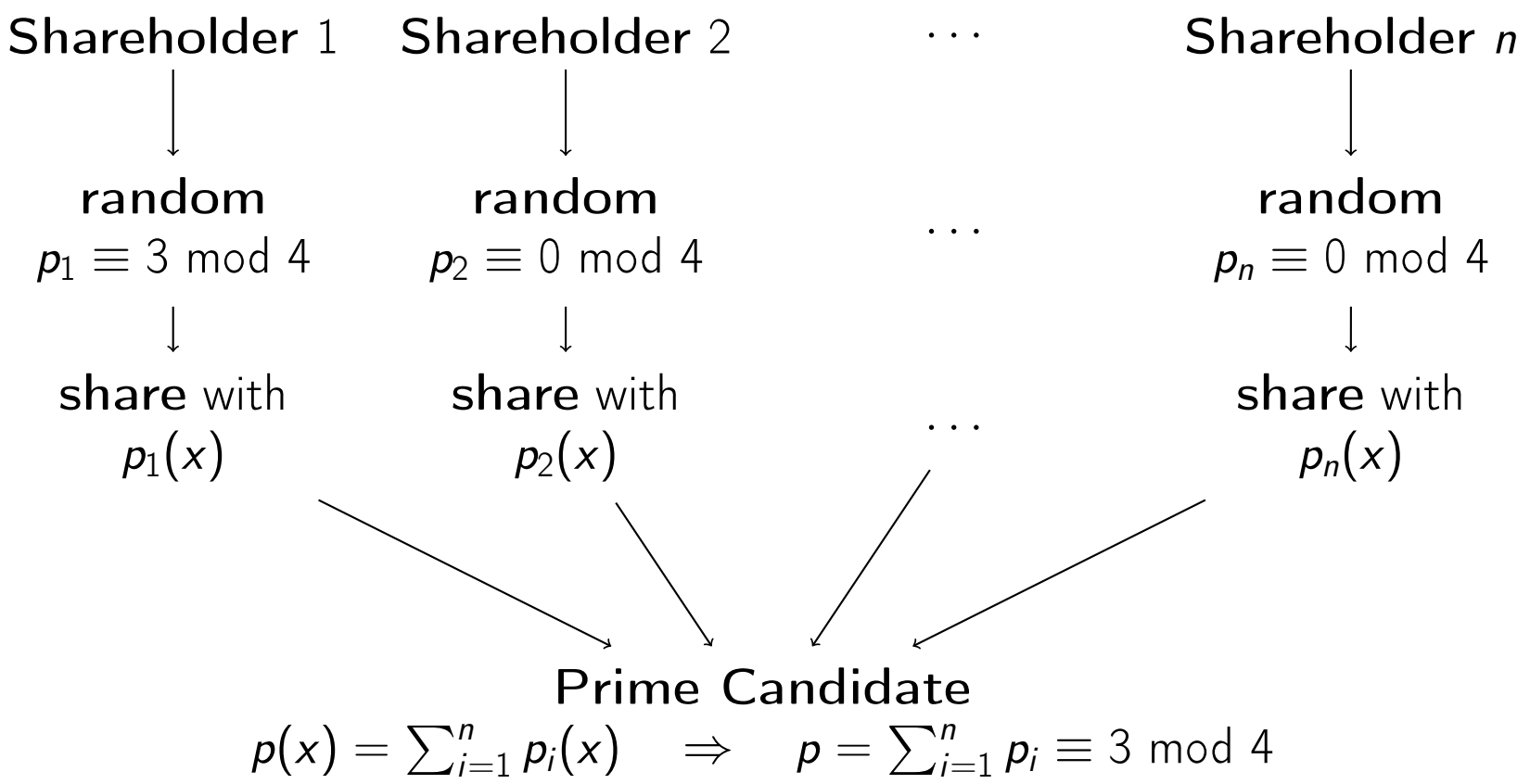
Takashi Nishide and Kouichi Sakurai. "Distributed Paillier Cryptosystem without Trusted Dealer". In: *ISA*. LNCS. Springer, 2010

Threshold Paillier



Takashi Nishide and Kouichi Sakurai. "Distributed Paillier Cryptosystem without Trusted Dealer". In: *ISA*. LNCS. Springer, 2010

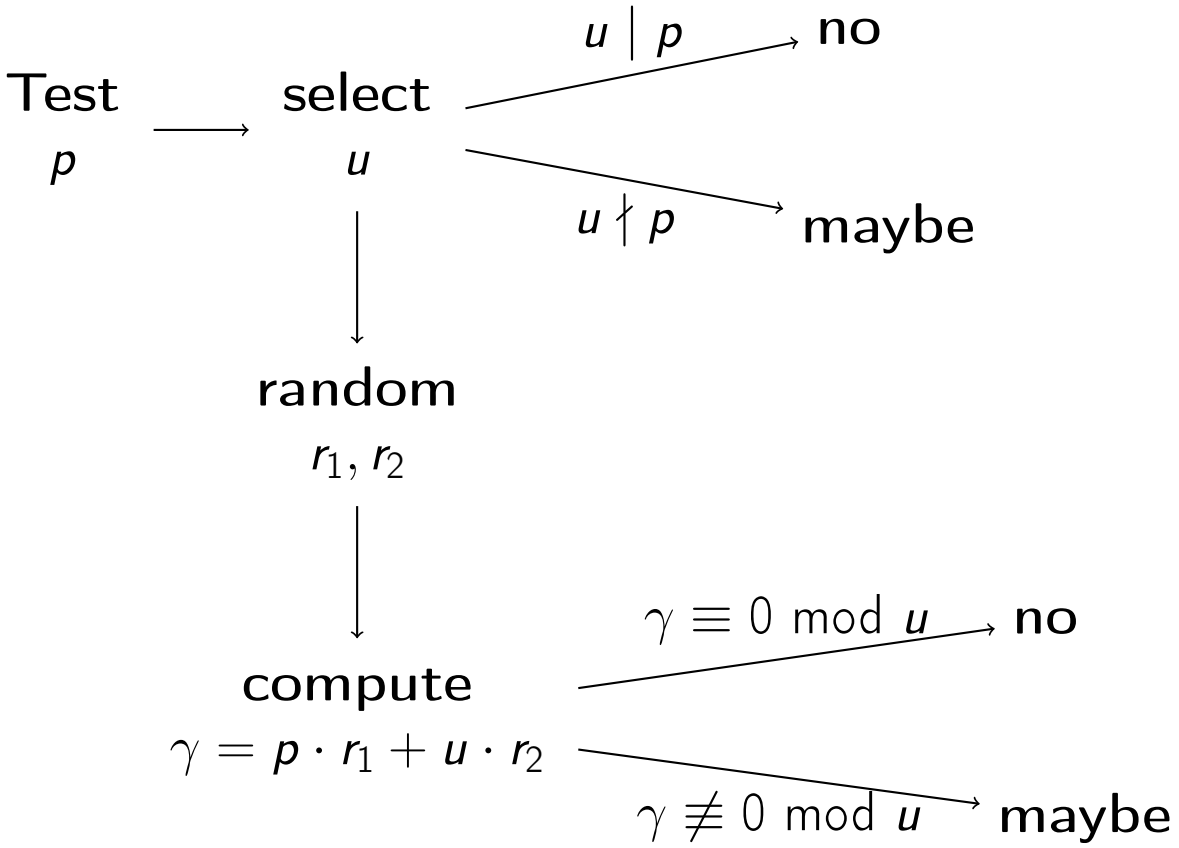
Prime Candidates



Takashi Nishide and Kouichi Sakurai. "Distributed Paillier Cryptosystem without Trusted Dealer". In: *ISA*. LNCS. Springer, 2010

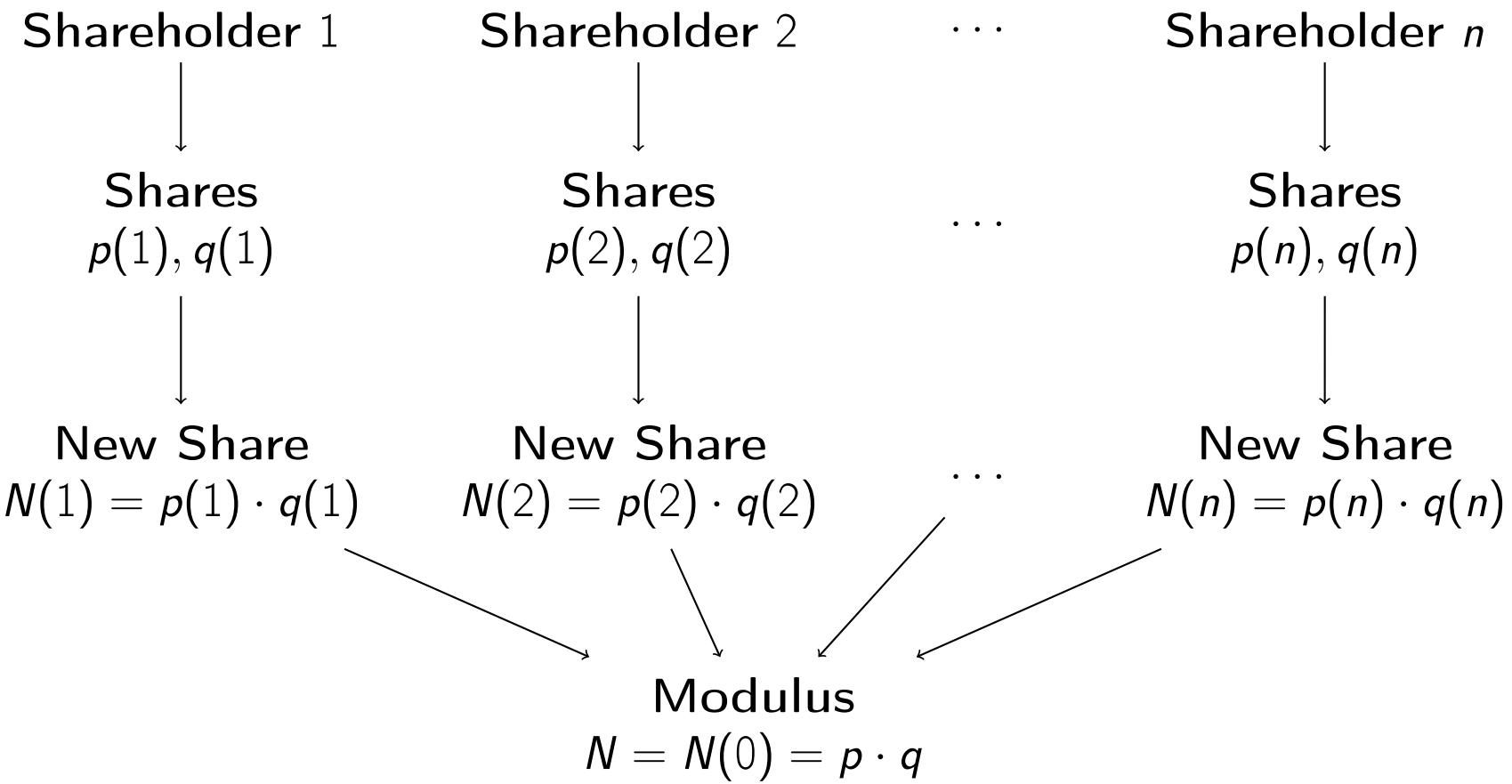
Andreas Klinger, Stefan Wüller, Giulia Traverso, and Ulrike Meyer

Trial Division



Takashi Nishide and Kouichi Sakurai. "Distributed Paillier Cryptosystem without Trusted Dealer". In: *ISA*. LNCS. Springer, 2010

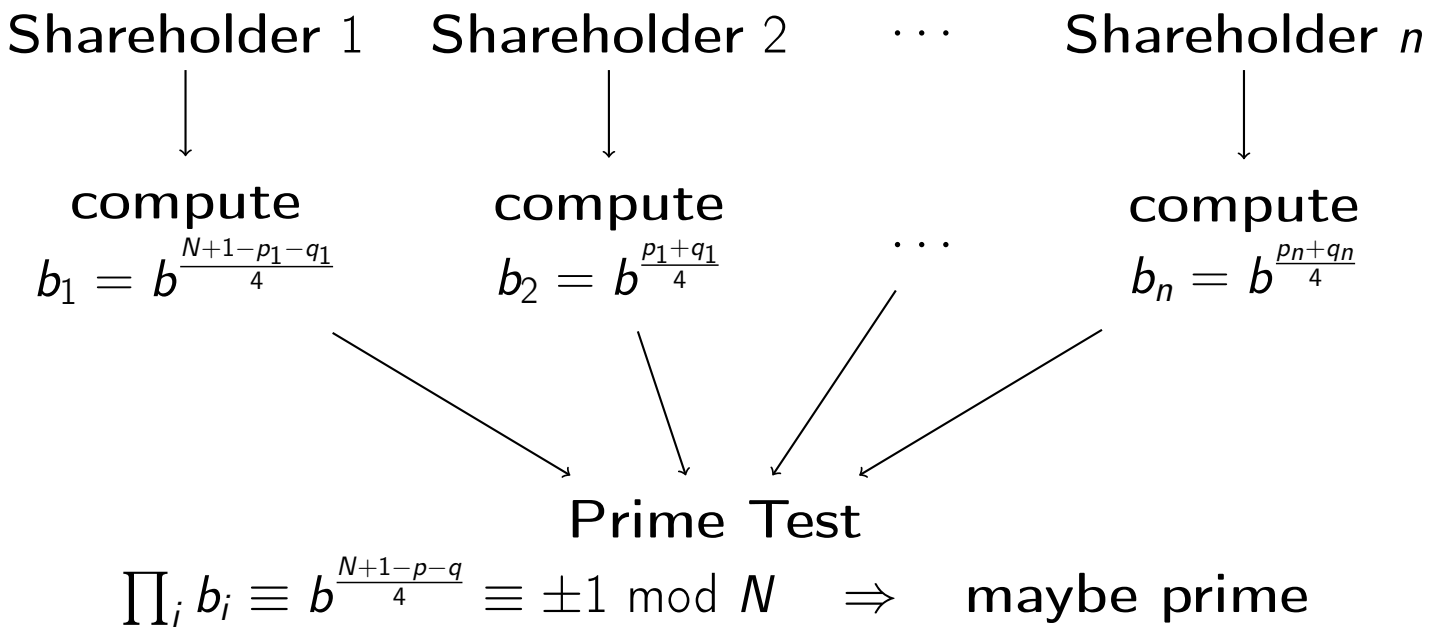
Multiplication - Modulus Generation



Takashi Nishide and Kouichi Sakurai. "Distributed Paillier Cryptosystem without Trusted Dealer". In: *ISA*. LNCS. Springer, 2010

Biprimality Test

$$b^{\frac{N+1-p-q}{4}} \equiv \pm 1 \bmod N \quad \Rightarrow \quad \text{maybe prime}$$



Takashi Nishide and Kouichi Sakurai. "Distributed Paillier Cryptosystem without Trusted Dealer". In: *ISA*. LNCS. Springer, 2010

Final Steps

Private Key $\varphi(N)$

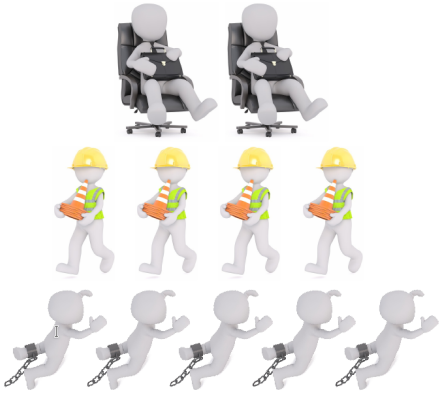
$$\begin{aligned}\varphi(N) &= (p-1)\cdot(q-1)\\ &= N-p-q+1\end{aligned}$$

Shares σ_i

$$\sigma_i = N - p(i) - q(i) + 1$$

Hierarchical Access Structure

Reset algorithm

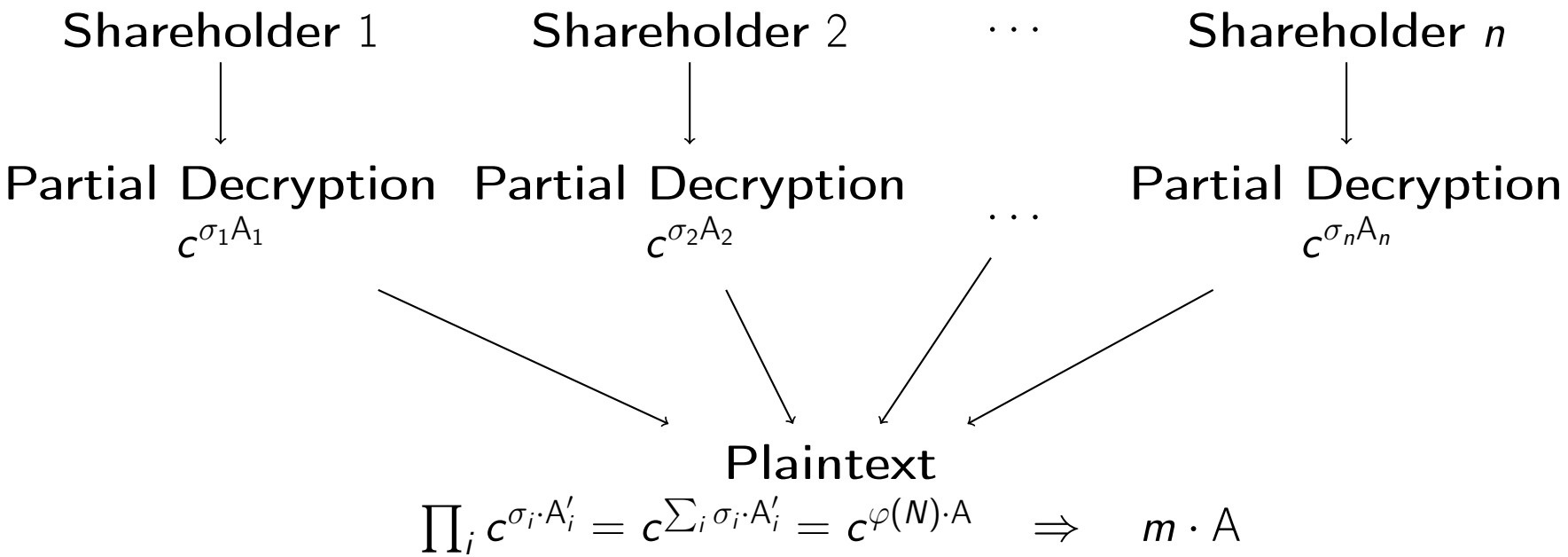


Andreas Klinger, Stefan Wüller, Giulia Traverso, and Ulrike Meyer

Decryption

$$c^{\varphi(N)} \quad \Rightarrow \quad m$$

$$\varphi(N) = \sum_i \frac{\sigma_i \cdot \mathrm{A}_i}{\mathrm{A}} \qquad \Rightarrow \qquad \varphi(N) \cdot \mathrm{A} = \sum_i \sigma_i \cdot \mathrm{A}_i$$



$$\prod_i c^{\sigma_i \cdot \mathrm{A}'_i} = c^{\sum_i \sigma_i \cdot \mathrm{A}'_i} = c^{\varphi(N) \cdot \mathrm{A}} \quad \Rightarrow \quad m \cdot \mathrm{A}$$

Conclusion

Contributions

- Verifiable hierarchical and dynamic secret sharing scheme over the integers
  - Add and remove shareholders
  - Hierarchical access structure
- Hierarchical and dynamic threshold Paillier cryptosystem without trusted dealer
  - Add and remove shareholders
  - Hierarchical access structure
  - No trusted dealer
  - Allows homomorphic addition
  - Secure against malicious adversaries

Future Work

- Implementation and real world performance evaluation
- Develop hierarchical threshold RSA

Discussion

Thank you for your attention!

References

- Takashi Nishide and Kouichi Sakurai. "Distributed Paillier Cryptosystem without Trusted Dealer". In: *ISA*. LNCS. Springer, 2010.
- Pascal Paillier. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". In: *EUROCRYPT*. Lecture Notes in Computer Science. Springer, 1999.
- Adi Shamir. "How to Share a Secret". In: *Commun. ACM* 22.11 (1979).
- Tamir Tassa. "Hierarchical Threshold Secret Sharing". In: *Journal of Cryptology* 20.2 (2007).
- Traverso et al. "Dynamic and Verifiable Hierarchical Secret Sharing". In: *ITS*. LNCS. Springer, 2016.