Probabilistic Secret Sharing

Paolo D’Arco, Roberto De Prisco, Alfredo De santis, Angel Perez del Pozo, Ugo Vaccaro

2019-06-12

Presented by: Dimcho Karakashev

UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Outline

- Introduction
- Previous Work
- Models in the paper
- Probabilistic scheme for finite threshold
- A probabilistic $(2,\infty)$-threshold construction
- Transforms for general schemes from simpler ones
  - From (k,∞)-threshold scheme to $(k+1,\infty)$-threshold scheme
  - From $(j,\infty)_{j=\{2,..,k\}}$-threshold scheme where to $(k+1,\infty)$-threshold scheme
- A probabilistic (k,∞)-threshold construction with constant size of shares

Introduction

- Secret Sharing

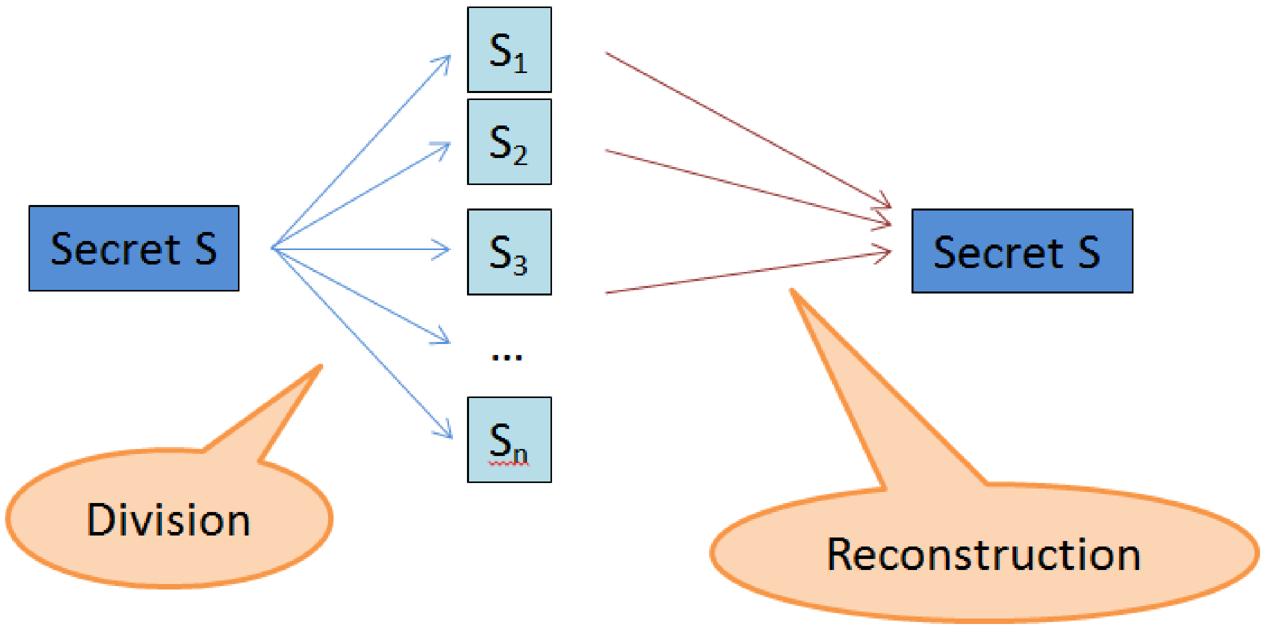


Figure 1. Secret sharing scheme

http://robinsnippet.blogspot.com/2017/12/shamirs-secret-sharing-scheme.html

Introduction

- Visual cryptography schemes

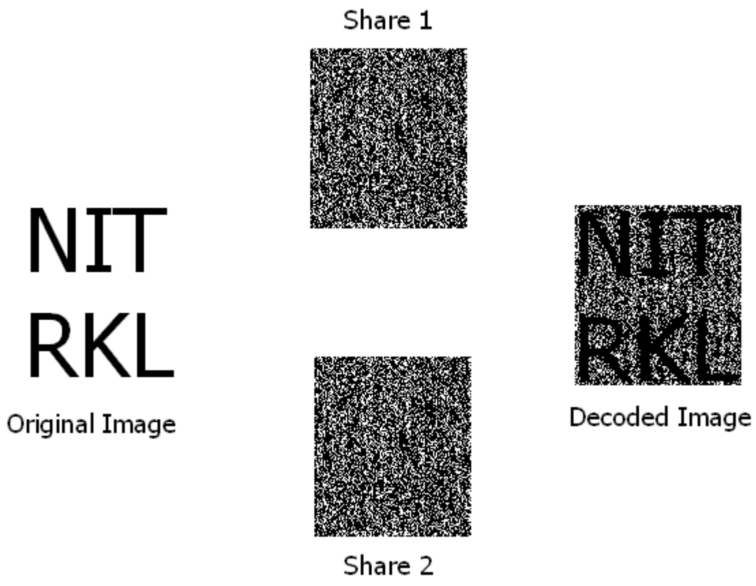


Figure 2. Visual Cryptography

https://www.researchgate.net/figure/Working-of-visual-cryptography_fig1_261163761

Introduction

- Evolving access structures – (k,∞)-threshold scheme
- Open questions in secrete sharing schemes
- This paper:
  - No study has focused on the analysis and the design of secret sharing scheme in which the secret can be reconstructed with high probability. (except visual cryptography)
  - “Can we reduce the size of the shares held by the participants if we allow a small probability of error in the reconstruction phase?”

Related Work

- Perfect
- Non-perfect
  - (d,t,n)-ramp scheme
  - Statistical relaxation – the privacy is not information-theoretic (some probability of information leakage)
  - Computational relaxation – guarantees only against computationally bounded adversary.

Model

- Probabilistic secret sharing scheme:

  ▶ **Definition 2.** Let S be a set of secrets such that $|S| \geq 2$, and let α be a positive real value such that $0 < \alpha \leq 1$. An α-probabilistic secret sharing scheme Π for an access structure $\mathcal{A}$ on the set of participants $\mathcal{P}_n$ and set of secrets S consists of a pair of probabilistic polynomial time algorithms $(\mathsf{Share}, \mathsf{Recon})$ where

  - Share(s) = $\{sh_1,\ldots,sh_n\}$
  - Recon($\{sh_i\}_{i\in A}$) = s
- α-correctness: Prob[Recon($\{sh_i\}_{i\in A}$)=s] ≥α
- Perfect privacy

Model(evolving schemes)

- Access structure:

  ▶ **Definition 5.** [26, 27] Let $\mathbb{N}$ be the set of the natural numbers. A (possibly infinite) sequence of access structures $\{\mathcal{A}_t\}_{t\in\mathbb{N}}$ is called evolving if, for every $t \in \mathbb{N}$, the following conditions hold:
  - $\mathcal{A}_t$ is an access structure over $\mathcal{P}_t$
  - $\mathcal{A}_t|_{t-1}$ is equal to $\mathcal{A}_{t-1}$.

- Probabilistic secret sharing for evolving access structures:
  - $\mathrm{Share}(s,\{sh_1,\ldots,sh_{t-1}\}) = sh_t$
  - $\mathrm{Recon}(\{sh_i\}_{i\in A}) = s$

Probabilistic schemes for the threshold finite case

- (3,4)-threshold deterministic scheme:

$$B_0 = \begin{bmatrix} 000111 \\ 001011 \\ 001101 \\ 001110 \end{bmatrix} \qquad B_1 = \begin{bmatrix} 000111 \\ 100110 \\ 010110 \\ 001110 \end{bmatrix}$$

Probabilistic schemes for the threshold finite case

- (3,4)-threshold deterministic scheme:

$$B_0 = \begin{bmatrix} \boxed{000111} \\ 001011 \\ 001101 \\ 001110 \end{bmatrix} \qquad B_1 = \begin{bmatrix} 000111 \\ 100110 \\ 010110 \\ 001110 \end{bmatrix}$$

Probabilistic schemes for the threshold finite case

- (3,4)-threshold deterministic scheme:

$$B_0 = \begin{bmatrix} 000111 \\ \boxed{001011} \\ 001101 \\ 001110 \end{bmatrix} \qquad B_1 = \begin{bmatrix} 000111 \\ 100110 \\ 010110 \\ 001110 \end{bmatrix}$$

Probabilistic schemes for the threshold finite case

- (3,4)-threshold deterministic scheme:

$$B_0 = \begin{bmatrix} 000111 \\ 001011 \\ 001101 \\ 001110 \end{bmatrix} \qquad B_1 = \begin{bmatrix} 000111 \\ 100110 \\ 010110 \\ 001110 \end{bmatrix}$$

sh_1: 000111
sh_2: 001011
sh_3: 001101
sh_4: 001110

Probabilistic schemes for the threshold finite case

- Deterministic (3,4)-threshold scheme:

$$B_0 = \begin{bmatrix} 000111 \\ 001011 \\ 001101 \\ 001110 \end{bmatrix} \qquad B_1 = \begin{bmatrix} 000111 \\ 100110 \\ 010110 \\ 001110 \end{bmatrix}$$

- Superposing when s=0 - 4 ones and 2 zeros
- Superposing when s=1 - 5 ones and 1 zero

Probabilistic schemes for the threshold finite case

- Probabilistic visual cryptography scheme:

$$\mathcal{C}_0 = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right\} \qquad \mathcal{C}_1 = \left\{ \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\}$$

- Shares of the participants are randomly selected vectors(or function):
  - 0 is reconstructed correctly $\frac{1}{3}$ of the times
  - 1 is reconstructed correctly $\frac{5}{12}$ of the times
  - Overall $\frac{7}{12}$ of the times

Probabilistic schemes for the threshold finite case

- Probabilistic visual cryptography scheme:

$$\mathcal{C}_0 = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right\} \qquad \mathcal{C}_1 = \left\{ \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\}$$

- Shares of the participants are randomly selected vectors(xor function):
  - 0 is reconstructed correctly $\frac{5}{6}$ of the times
  - 1 is reconstructed correctly $\frac{5}{6}$ of the times
  - Overall $\frac{5}{6}$ of the times

$(2,\infty)$-threshold construction

- Construction:
  - Share(i) = sh_{pi}
    - First participant receives a random bit b_1
    - For all other participants:
      - If $s = 0$, then participant p_i receives the same as given to b_1
      - If $s = 1$, then participant p_i receives new random bit
  - Recon(sh_i,sh_j):
    - If $sh_i = sh_j$, then output is 0
    - If $sh_i \neq sh_j$, then output is 1

(2,∞)-threshold construction

- The construction is $\frac{1+p}{2}$ -probabilistic (2,∞)-threshold scheme, where (p,1-p) is the distribution of the secret bit
- Security
- $\frac{1+p}{2}$ - correctness

$$
\begin{aligned}
Prob[\mathsf{Recon}(\{sh_i\}_{i\in A}) = s] \quad = \quad & p \cdot \overset{1}{\boxed{Prob[\mathsf{Recon}(\{sh_i\}_{i\in A}) = 0 | s = 0]}} + \\
& (1-p) \cdot \underset{\frac{1}{2}}{\boxed{Prob[\mathsf{Recon}(\{sh_i\}_{i\in A}) = 1 | s = 1]}}
\end{aligned}
$$

Transforms for general schemes from simple ones

- From (k,∞)-threshold to $(k+1,\infty)$-threshold
- From $\{(j,\infty)\text{-threshold}\}_{\{j=2,..,k\}}$ to $(k+1,\infty)$-threshold

From (k,∞)-threshold to (k+1,∞)-threshold

- Let Π be auxiliary (k,∞)-threshold scheme
- Let Λ be $(k+1,\infty)$-threshold scheme
- The share sh_t is computed the following way:
  - $r_t \in \{0,1\}$ is chosen at random
  - For every $j \in \{1,\dots,t\text{-}1\}$, a new share $w_{t,j}$ of r_t is computed using Π.
  - The share of party t is(scheme Λ):
    - $sh_t=\{s \oplus r_t\} \cup \{w_{t,j}\}_{j=\{1,\dots,t-1\}}$

From (k,∞)-threshold to (k+1,∞)-threshold

- Let Π be auxiliary (k,∞)-threshold scheme
- Let Λ be $(k+1,\infty)$-threshold scheme
- Recon algorithm for scheme Λ:
  - It assumes k+1 parties: $P_{to},P_{t1},\ldots,P_{tk}$ (chronologically ordered)
  - The last k parties run the Recon algorithm of Π with inputs: $(w_{t1,to},w_{t2,to},\ldots,w_{tk,to})$ to recover r_{to}
  - $r_{to} \oplus s \oplus r_{to} = s$

Probabilistic (k,∞)-threshold scheme with constant share size

- Sharmir's secret sharing scheme - (k,q)-threshold scheme
- Upon arrive of new participant t, r_t is chosen at random
- The share is $(r_t, p(r_t))$
- Recon algorithm:
  - Check if all parties have different first components in their shares
  - If so, then Reconstruct the secret

Conclusion

- Formalized the notion of probabilistic secret sharing scheme
- Provided a construction for:
  - probabilistic (3,4)-threshold secret sharing scheme
  - probabilistic $(2,\infty)$-threshold scheme
  - probabilistic (k,∞)-threshold scheme with constant share size
- Transforms for general schemes from simpler ones

THANK YOU

Questions for Discussion

- Is one bit secret realistic?
  - Can you think of any scenarios?
  - Extending the schemes to more bits?
- Do you have any ideas how to make the transformation more efficient?
- Do you think probabilistic secret sharing scheme will be useful?
  - How would you choose α?
- Does the “translation” from visual cryptographic scheme always improve the correctness property for a secret sharing scheme?

ADDITIONAL SLIDES

From {(j,∞)-threshold}$_{j \text{ from2 to } k}$ to (k+1,∞)-threshold

- Let j∈{1,...,k}, Π_j auxiliary (j,∞)-threshold scheme
- Let Λ be (k+1,∞)-threshold scheme to construct
- Generation(g_1>k):

$G_m = g_m$ | G_{m+1}

$P_1,\dots,P_{gm}$ | $P_{g(m+1)},\dots,P_{g(2m+2)}$

From $\{(j,\infty)\text{-threshold}\}_{j \text{ from2 to } k}$ to $(k+1,\infty)$-threshold

G_m

$r_2^{(m)} \longrightarrow s \oplus r_2^{(m)} \xrightarrow{\text{shared by}} (2,g_m)$-threshold scheme

$r_3^{(m)} \longrightarrow s \oplus r_3^{(m)} \longrightarrow (3,g_m)$-threshold scheme

$\ldots \longrightarrow \qquad \longrightarrow$

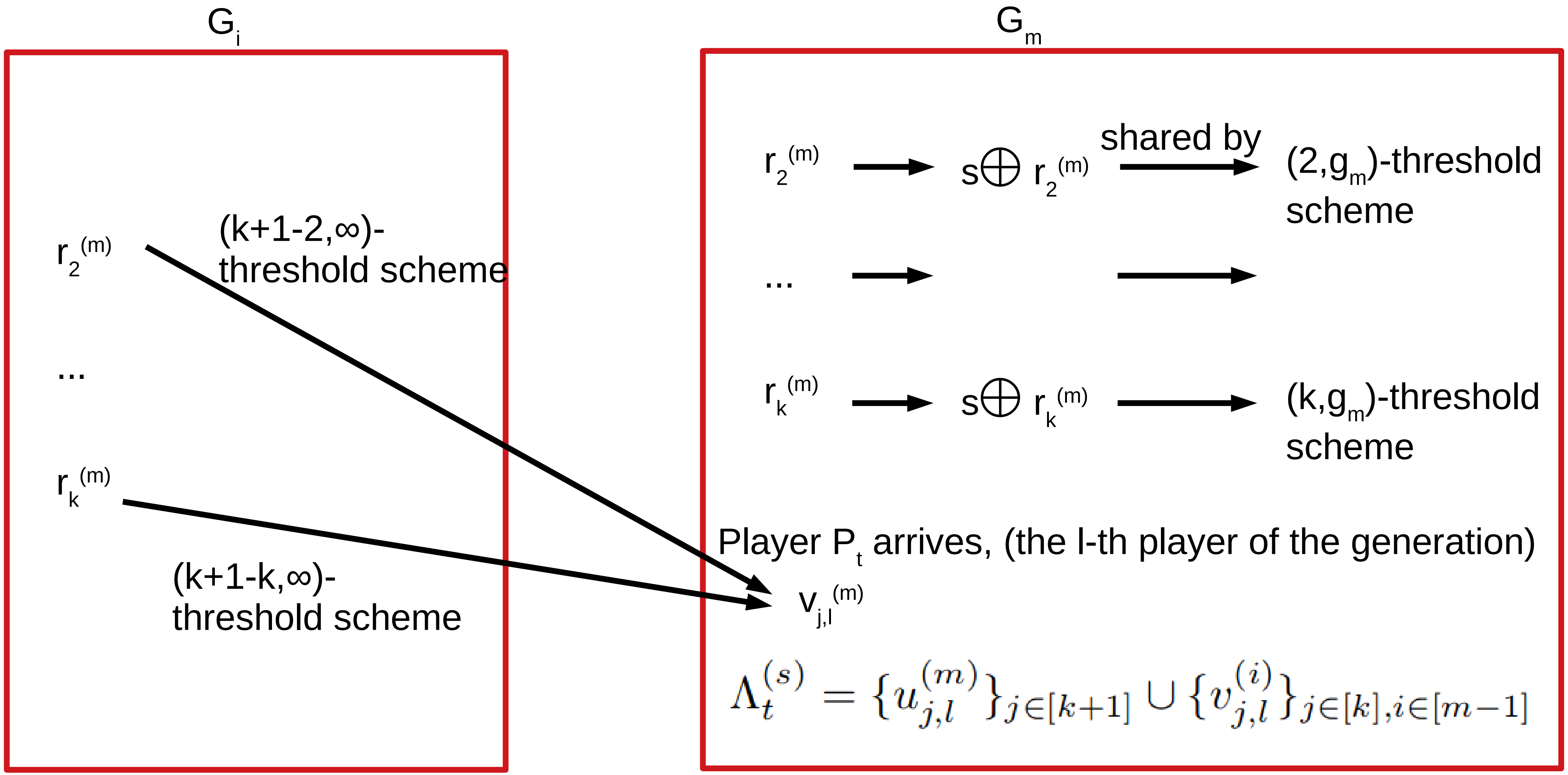
$r_k^{(m)} \longrightarrow s \oplus r_k^{(m)} \longrightarrow (k,g_m)$-threshold scheme

$s \longrightarrow (k+1,g_m)$-threshold scheme

Addtional notation:
$u_{j,l}^{(m)}$ is the l-th share

Addtional notation:
$u_{k+1,l}^{(m)}$ is the l-th share

From $\{(j,\infty)\text{-threshold}\}_{j=\{2,\dots,k\}}$ to $(k+1,\infty)$-threshold



From {(j,∞)-threshold}$_{j \text{ from2 to } k}$ to (k+1,∞)-threshold

- Recon:
  - If there are no subsequent generations, then use $(k+1,g_m)$-threshold scheme.
  - If there are subsequent generation:
    - Recover $s \oplus r_{ko}^{(m)}$ within the generation using (ko,g_m)-threshold scheme
    - Parties of subsequent generations recover $r_{ko}^{(m)}$ using $(k1,\infty)$-threshold scheme
    - $s = s \oplus r_{ko}^{(m)} \oplus r_{ko}^{(m)}$

Note: g_m + parties in subsequent generations = k+1