

矩阵分析与应用

- 秘密共享

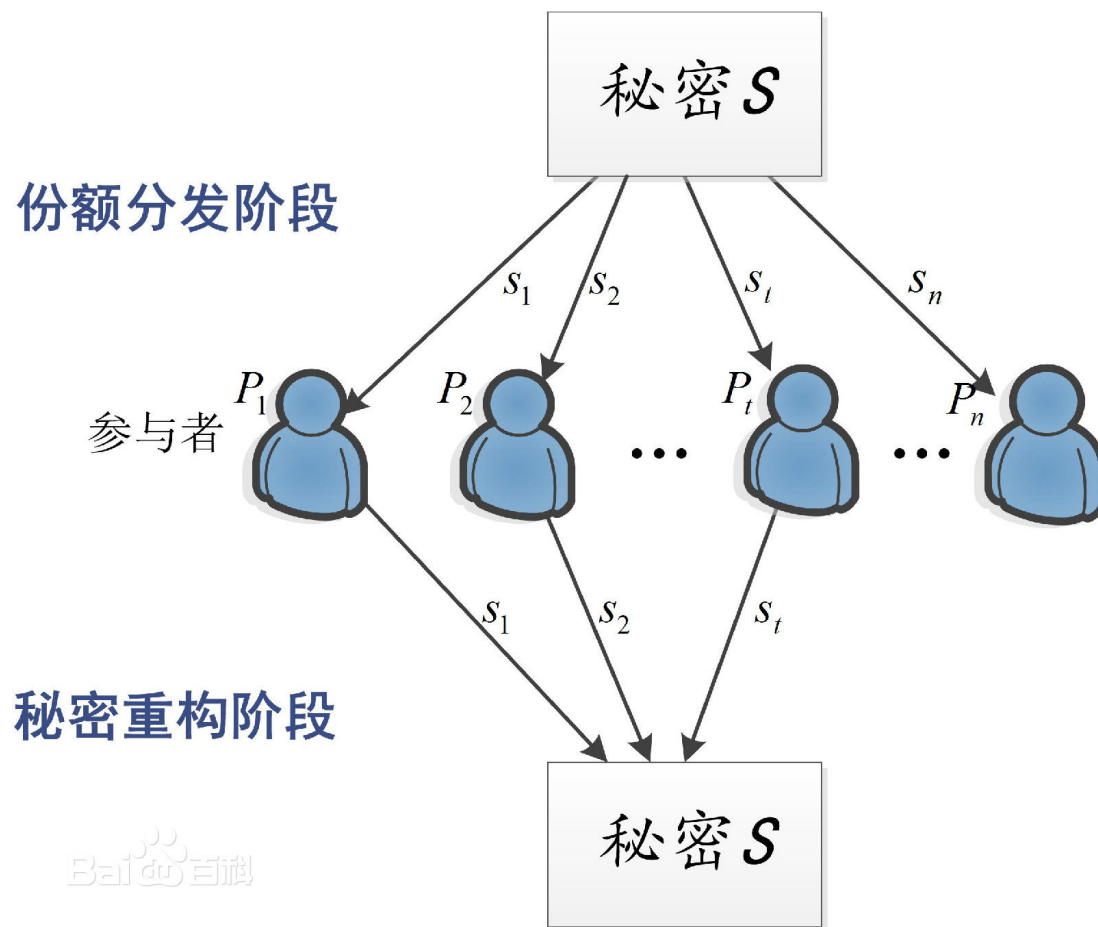
林宪正

参考文献：庞辽军等，" 秘密共享技术及其应用，" 人民邮电出版社

秘密共享

- 秘密共享：将秘密以适当的方式拆分，拆分后的每一个份额由不同的参与者管理，单个参与者无法恢复秘密信息，只有若干个参与者一同协作才能恢复秘密消息。
- 秘密共享是一种将秘密分割存储的密码技术，目的是阻止秘密过于集中，以达到分散风险和容忍入侵的目的，是信息安全和数据保密中的重要手段。

秘密共享



门限秘密共享

-Shamir 门限方案

- 数学基础：多项式内插
- (t, n) 秘密分发：
 - 输入：秘密 $s \in F_q$
 - 随机选择 $f(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1}$ ，使 $a_0 = s$
 - 计算 $(w_1, f(w_1)), (w_2, f(w_2)), \dots, (w_n, f(w_n))$
- 秘密恢复：
 - 当获得任何 t 秘密份额时，可以通过多项式插值方法计算出 $f(x)$ ，其常数项为秘密 s

门限秘密共享

-Shamir 门限方案

- 任意 $t-1$ 份秘密份额无法获取 s 的任何信息。
- 减小秘密份额大小
 - $f(x)$ 全部系数为秘密信息 (计算安全的秘密共享)
 - $f(x)$ 部份系数为秘密信息 (Ramp Scheme)
- 侦测错误的秘密份额。
- 可否将 Shamir 门限方案建立在环上？

访问结构

- 访问结构用於指出哪些参与者可以合作恢复出所共享的秘密，而哪些参与者合作不能恢复秘密。
- 例子：在 $(t=2, n=3)$ 门限秘密共享中，令参与者集合为 $P=\{P_1, P_2, P_3\}$ ，则
$$\Gamma=\{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3\}, \{P_1, P_2, P_3\}\} ,$$
$$\bar{\Gamma}=\{\{P_1\}, \{P_2\}, \{P_3\}\} .$$

访问结构

- 访问结构的单调性。如果 $X \in \Gamma$ 且 $X \subseteq A \subseteq \Pi$ ，那么 $A \in \Gamma$ 。
- 极小访问结构。 $\Gamma_{\mu} = \{A | A \in \Gamma \text{ 且 } \forall B \subset A \Rightarrow B \notin \Gamma\}$ 。
- 极大非访问结构。

完备的秘密共享

- 完备的秘密共享方案。令 π 为实现访问结构 Γ 的一个秘密共享方案，在 n 个参与者中共享了秘密 s ，如果满足：
 - 任何集合 $\gamma \in \Gamma$ 中的参与者将他们的秘密份额放在一起能够确定秘密 s
 - 任何集合 $\eta \subseteq P$ 且 $\eta \notin \Gamma$ 中的参与者将他们的秘密份额放在一起不能得到关于秘密 s 的任何信息

秘密共享的应用

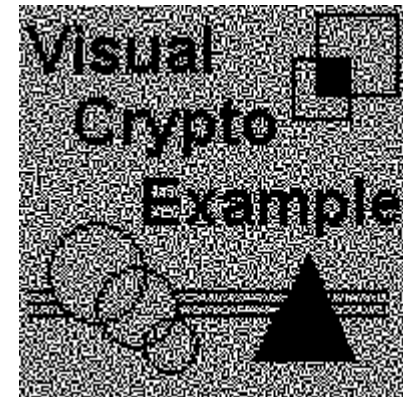
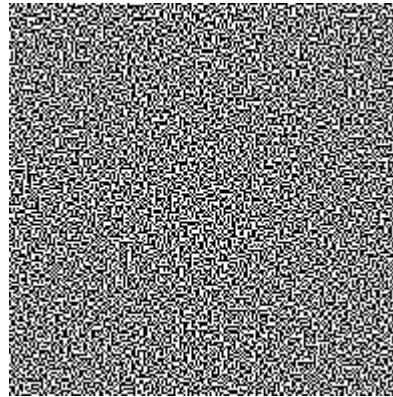
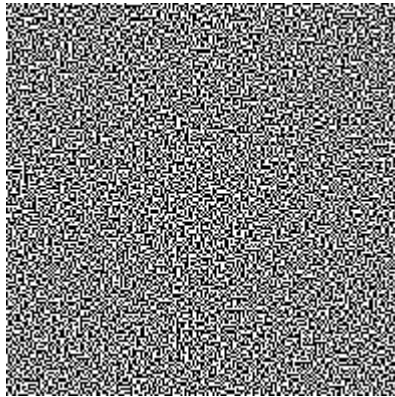
- 门限数字签名
- 多方安全计算













探讨问题

- 分級的秘密共享
- 基於 MDS 码的秘密分享方案
 - X-Codes, P-Codes, Star Codes,...
- 基於信道编码的秘密分享方案
 - Product Codes
 - Generalized Reed-Muller Codes

秘密共享

- 视觉密码 (Visual Cryptography)



pixel		share #1	share #2	superposition of the two shares
	$p = .5$			
	$p = .5$			
	$p = .5$			
	$p = .5$			

半色调技术

- 误差扩散法 Error Diffusion

