# 可证明安全 - 密码学中的安全性证明

钱宸
网络空间安全学院
山东大学

2025.09.17

# Contents

# 基于安全游戏的证明

# 基于安全游戏的证明

我们给出一个混合 [Shoup, 2004] 和 [Bellare and Rogaway, 2006] 的基于安全游戏的证明模式.

## 基本标记

- $x \leftarrow \mathcal{D}(X)$: 从集合 $X$ 上的分布 $\mathcal{D}$ 中随机采样 $x$, $\mathsf{U}(X)$ 表示集合 $X$ 上的均匀分布.

# 基于安全游戏的证明

我们给出一个混合 [Shoup, 2004] 和 [Bellare and Rogaway, 2006] 的基于安全游戏的证明模式.

## 基本标记

- $x \hookleftarrow \mathcal{D}(X)$: 从集合 $X$ 上的分布 $\mathcal{D}$ 中随机采样 $x$, $\mathsf{U}(X)$ 表示集合 $X$ 上的均匀分布.
- $y \xleftarrow{\$} A(x)$: 运行算法 $A$ 并输入 $x$, 输出 $y$. 其中 $A$ 为一个 PPT (Probabilistic Polynomial Turing Machine). 上述 $\mathcal{D}(X)$ 也可以看作是一个 PPT.

# 基于安全游戏的证明

我们给出一个混合 [Shoup, 2004] 和 [Bellare and Rogaway, 2006] 的基于安全游戏的证明模式.

## 基本标记

- $x \hookleftarrow \mathcal{D}(X)$: 从集合 $X$ 上的分布 $\mathcal{D}$ 中随机采样 $x$, $\mathsf{U}(X)$ 表示集合 $X$ 上的均匀分布.
- $y \xleftarrow{\$} A(x)$: 运行算法 $A$ 并输入 $x$, 输出 $y$. 其中 $A$ 为一个 PPT (Probabilistic Polynomial Turing Machine). 上述 $\mathcal{D}(X)$ 也可以看作是一个 PPT.
- $y := A(x)$: 运行算法 $A$ 并输入 $x$, 输出 $y$. 其中 $A$ 为一个确定性多项式时间算法.

# 基于安全游戏的证明

我们给出一个混合 [Shoup, 2004] 和 [Bellare and Rogaway, 2006] 的基于安全游戏的证明模式.

## 基本标记

- $x \hookleftarrow \mathcal{D}(X)$: 从集合 $X$ 上的分布 $\mathcal{D}$ 中随机采样 $x$, $\mathsf{U}(X)$ 表示集合 $X$ 上的均匀分布.
- $y \xleftarrow{\$} A(x)$: 运行算法 $A$ 并输入 $x$, 输出 $y$. 其中 $A$ 为一个 PPT (Probabilistic Polynomial Turing Machine). 上述 $\mathcal{D}(X)$ 也可以看作是一个 PPT.
- $y := A(x)$: 运行算法 $A$ 并输入 $x$, 输出 $y$. 其中 $A$ 为一个确定性多项式时间算法.
- $\Pr\left[\phi(x_1, \ldots, x_n) \;\middle|\; x_1 \xleftarrow{\$} X_1, x_2 \xleftarrow{\$} X_2(x_1), \cdots, X_n(x_1, \ldots, x_{n-1})\right]$: 用来标记事件 $\phi(x_1, \ldots, x_n)$ 在 $x_1, \ldots, x_n$ 分别从 $X_1, \ldots, X_n$ 中随机采样时发生的概率.

# 基于安全游戏的证明

## 需要证明的断言

$\forall \mathcal{A} \in \mathsf{PPT} : \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}}(1^\lambda) = \Pr[\mathbf{G}_{\mathcal{A}} \Rightarrow 1] \leq \mathsf{negl}(\lambda)$.

然而, 直接证明上述断言往往比较困难. 我们通过构造一系列中间游戏来简化证明过程.

## 中间游戏

$\mathbf{G}_0, \mathbf{G}_1, \ldots, \mathbf{G}_n$, 其中 $\mathbf{G}_0$ 为原始安全游戏, $\mathbf{G}_n$ 为显然安全的游戏.

因为 $\mathbf{G}_n$ 显然安全, 所以 $\forall \mathcal{A} \in \mathsf{PPT} : \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_n}(1^\lambda) = \Pr[\mathbf{G}_{n,\mathcal{A}} \Rightarrow 1] \leq \mathsf{negl}(\lambda)$.

## 记号

对于所有 $i \in [n]$, 我们将 $\Pr\left[\mathbf{G}_(i, \mathcal{A}) \Rightarrow 1\right]$ 记作 $\mathsf{pr}_i$.

# 切换方式

- 什么样的切换方式是允许的?
- 为什么中间有些的引入可以简化证明流程?
- 需要注意什么?

# 中间游戏切换-为什么?

## 中间游戏

$\mathbf{G}_0, \mathbf{G}_1, \ldots, \mathbf{G}_n$, 其中 $\mathbf{G}_0$ 为原始安全游戏, $\mathbf{G}_n$ 为" 显然安全的游戏".

- 因为 $\mathbf{G}$ 显然安全, 所以 $\forall \mathcal{A} \in \mathsf{PPT} : \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_n}(1^\lambda) = \Pr[\mathbf{G}_{n,\mathcal{A}} \Rightarrow 1] = 0.$

# 中间游戏切换-为什么?

## 中间游戏

$\mathbf{G}_0, \mathbf{G}_1, \ldots, \mathbf{G}_n$, 其中 $\mathbf{G}_0$ 为原始安全游戏, $\mathbf{G}_n$ 为" 显然安全的游戏".

- 因为 $\mathbf{G}$ 显然安全, 所以 $\forall \mathcal{A} \in \mathsf{PPT} : \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_n}(1^\lambda) = \Pr[\mathbf{G}_{n,\mathcal{A}} \Rightarrow 1] = 0$.
- 如果证明了: $\forall i \in [n] : \forall \mathcal{A} \in \mathsf{PPT} : |\mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_i}(1^\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_{i-1}}(1^\lambda)| \leq \mathsf{negl}(\lambda)$.

# 中间游戏切换-为什么?

## 中间游戏

$\mathbf{G}_0, \mathbf{G}_1, \ldots, \mathbf{G}_n$, 其中 $\mathbf{G}_0$ 为原始安全游戏, $\mathbf{G}_n$ 为" 显然安全的游戏".

- 因为 $\mathbf{G}$ 显然安全, 所以 $\forall \mathcal{A} \in \mathsf{PPT} : \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_n}(1^\lambda) = \Pr[\mathbf{G}_{n,\mathcal{A}} \Rightarrow 1] = 0$.
- 如果证明了: $\forall i \in [n] : \forall \mathcal{A} \in \mathsf{PPT} : |\mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_i}(1^\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_{i-1}}(1^\lambda)| \leq \mathsf{negl}(\lambda)$.
- 因为概率空间是一个度量空间, 所以概率函数 $\Pr[\cdot]$ 满足三角不等式.

# 中间游戏切换-为什么?

## 中间游戏

$\mathbf{G}_0, \mathbf{G}_1, \ldots, \mathbf{G}_n$, 其中 $\mathbf{G}_0$ 为原始安全游戏, $\mathbf{G}_n$ 为" 显然安全的游戏".

- 因为 $\mathbf{G}$ 显然安全, 所以 $\forall \mathcal{A} \in \mathsf{PPT} : \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_n}(1^\lambda) = \Pr[\mathbf{G}_{n,\mathcal{A}} \Rightarrow 1] = 0$.
- 如果证明了: $\forall i \in [n] : \forall \mathcal{A} \in \mathsf{PPT} : |\mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_i}(1^\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_{i-1}}(1^\lambda)| \leq \mathsf{negl}(\lambda)$.
- 因为概率空间是一个度量空间, 所以概率函数 $\Pr[\cdot]$ 满足三角不等式.
- 所以,

$$\begin{aligned}\forall \mathcal{A} \in \mathsf{PPT} : \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_0}(1^\lambda) &\leq |\mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_0}(1^\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_n}(1^\lambda)| + \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_n}(1^\lambda) \\ &\leq \sum_{i=0}^{n-1} |\mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_i}(1^\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_{i+1}}(1^\lambda)| \leq n \cdot \mathsf{negl}(\lambda) = \mathsf{negl}(\lambda).\end{aligned}$$

# 中间游戏切换-为什么?

## 中间游戏

$\mathbf{G}_0, \mathbf{G}_1, \ldots, \mathbf{G}_n$, 其中 $\mathbf{G}_0$ 为原始安全游戏, $\mathbf{G}_n$ 为" 显然安全的游戏".

- 因为 $\mathbf{G}$ 显然安全, 所以 $\forall \mathcal{A} \in \mathsf{PPT} : \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_n}(1^\lambda) = \Pr[\mathbf{G}_{n,\mathcal{A}} \Rightarrow 1] = 0$.
- 如果证明了: $\forall i \in [n] : \forall \mathcal{A} \in \mathsf{PPT} : |\mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_i}(1^\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_{i-1}}(1^\lambda)| \leq \mathsf{negl}(\lambda)$.
- 因为概率空间是一个度量空间, 所以概率函数 $\Pr[\cdot]$ 满足三角不等式.
- 所以,

$$\begin{aligned}\forall \mathcal{A} \in \mathsf{PPT} : \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_0}(1^\lambda) &\leq |\mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_0}(1^\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_n}(1^\lambda)| + \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_n}(1^\lambda) \\ &\leq \sum_{i=0}^{n-1} |\mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_i}(1^\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_{i+1}}(1^\lambda)| \leq n \cdot \mathsf{negl}(\lambda) = \mathsf{negl}(\lambda).\end{aligned}$$

- 综上, $\forall \mathcal{A} \in \mathsf{PPT} : \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_0}(1^\lambda) = \Pr[\mathbf{G}_{0,\mathcal{A}} \Rightarrow 1] \leq \mathsf{negl}(\lambda)$.

# 切换方式

[Shoup, 2004] 中给出了三种常用的切换方式:

## 常用切换方式

**不可区分性:** $\forall \mathcal{A} \in \mathsf{PPT} : |\mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_i}(1^\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_{i-1}}(1^\lambda)| \leq \mathsf{negl}(\lambda)$.

**失败事件:** $\mathbf{G}_i$ 与 $\mathbf{G}_{i+1}$ 完全相同, 直到一个特殊事件 $F$ 发生.

**桥接步骤:** 通常用来表示在 $\mathbf{G}_i$ 和 $\mathbf{G}_{i+1}$ 之间的唯一区别就是某个变量是用两种不同但等价的方式计算.

# 切换方式 - 不可区分性

**不可区分性**

$\forall \mathcal{A} \in \mathsf{PPT} : |\mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_i}(1^\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_{i-1}}(1^\lambda)| \leq \mathsf{negl}(\lambda)$.

- 通常是基于某个密码学假设 (如: 离散对数假设, RSA 假设, CDH 假设, DDH 假设, XDH 假设等) 来证明的.

# 切换方式 - 不可区分性

**不可区分性**

$\forall \mathcal{A} \in \mathsf{PPT} : |\mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_i}(1^\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_{i-1}}(1^\lambda)| \leq \mathsf{negl}(\lambda)$.

- 通常是基于某个密码学假设 (如: 离散对数假设, RSA 假设, CDH 假设, DDH 假设, XDH 假设等) 来证明的.
- **证明思路通常是:** 假设存在一个 PPT 算法 $\mathcal{A}$ 可以在 $\mathbf{G}_i$ 和 $\mathbf{G}_{i-1}$ 之间区分, 那么我们可以构造一个 PPT 算法 $\mathcal{B}$ 来攻击某个密码学假设. **(规约)**

# 切换方式 - 不可区分性

**不可区分性**

$\forall \mathcal{A} \in \mathsf{PPT} : |\mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_i}(1^\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\mathbf{G}_{i-1}}(1^\lambda)| \leq \mathsf{negl}(\lambda)$.

- 通常是基于某个密码学假设 (如: 离散对数假设, RSA 假设, CDH 假设, DDH 假设, XDH 假设等) 来证明的.
- **证明思路通常是:** 假设存在一个 PPT 算法 $\mathcal{A}$ 可以在 $\mathbf{G}_i$ 和 $\mathbf{G}_{i-1}$ 之间区分, 那么我们可以构造一个 PPT 算法 $\mathcal{B}$ 来攻击某个密码学假设. **(规约)**
- **例如:** $\mathbf{G}_{i-1}$ 中使用了 DDH 对 $(p, g, g^a, g^b, g^{ab})$, 而 $\mathbf{G}_i$ 中使用了一个真正的随机对 $(p, g, g^a, g^b, g^c)$. 如果存在一个 PPT 算法 $\mathcal{A}$ 可以区分这两个游戏, 那么我们可以构造一个 PPT 算法 $\mathcal{B}$ 来区分这两个对, 从而攻击 DDH 假设.

# 切换方式 - 失败事件

**失败事件**

$\mathbf{G}_i$ 与 $\mathbf{G}_{i+1}$ 完全相同, 直到一个特殊事件 $F$ 发生.

为了使得过程简洁, 我们通常要求事件 $F$ 与 $\mathbf{G}_{i,\mathcal{A}} \Rightarrow 1$, $\mathbf{G}_{i+1,\mathcal{A}} \Rightarrow 1$ 在同一个概率空间下.


概率空间 (概率论基础):

样本空间 $\Omega$: 所有可能的结果的集合.

# 切换方式 - 失败事件

**失败事件**

$\mathbf{G}_i$ 与 $\mathbf{G}_{i+1}$ 完全相同, 直到一个特殊事件 $F$ 发生.

为了使得过程简洁, 我们通常要求事件 $F$ 与 $\mathbf{G}_{i,\mathcal{A}} \Rightarrow 1$, $\mathbf{G}_{i+1,\mathcal{A}} \Rightarrow 1$ 在同一个概率空间下.


概率空间 (概率论基础):

**样本空间** $\Omega$: 所有可能的结果的集合.

**事件空间** $\mathcal{E} \subseteq 2^{\Omega}$: 一个事件是样本空间的子集.

# 切换方式 - 失败事件

**失败事件**

$\mathbf{G}_i$ 与 $\mathbf{G}_{i+1}$ 完全相同, 直到一个特殊事件 $F$ 发生.

为了使得过程简洁, 我们通常要求事件 $F$ 与 $\mathbf{G}_{i,\mathcal{A}} \Rightarrow 1$, $\mathbf{G}_{i+1,\mathcal{A}} \Rightarrow 1$ 在同一个概率空间下.


概率空间 (概率论基础):

**样本空间** $\Omega$: 所有可能的结果的集合.

**事件空间** $\mathcal{E} \subseteq 2^{\Omega}$: 一个事件是样本空间的子集.

**概率测度** $\Pr[\cdot]$: 对事件空间中每个事件的发生概率的度量.

# 切换方式 - 失败事件

**失败事件**

$\mathbf{G}_i$ 与 $\mathbf{G}_{i+1}$ 完全相同, 直到一个特殊事件 $F$ 发生.

上述定义等价于

$$\forall \mathcal{A} \in \mathsf{PPT} : (\mathbf{G}_{i,\mathcal{A}} \Rightarrow 1 \wedge \neg F) \Leftrightarrow (\mathbf{G}_{i+1,\mathcal{A}} \Rightarrow 1 \wedge \neg F)$$

# 切换方式 - 失败事件 (差异引理)

**定理 (差异引理 [Shoup, 2004])**

对于 $A, B, F \in \mathcal{E}$ 为概率空间 $(\Omega, \mathcal{E}, \Pr[\cdot])$ 中的三个事件, 如果 $(A \wedge \neg F) \Leftrightarrow (B \wedge \neg F)$ 则有

$$|\Pr[A] - \Pr[B]| \leq \Pr[F].$$

**证明.**

$$\begin{aligned} |\Pr[A] - \Pr[B]| &= |(\Pr[A \wedge F] + \Pr[A \wedge \neg F]) - (\Pr[B \wedge F] + \Pr[B \wedge \neg F])| \\ &= |\Pr[A \wedge F] - \Pr[B \wedge F]| \\ &\leq \Pr[F]. \end{aligned}$$

□

# 切换方式 - 失败事件 (注意事项)

- 事件 $F$ 可能是 PPT 不可判定的. (这一点在基于模拟的证明中不一定为真).

# 切换方式 - 失败事件 (注意事项)

- 事件 $F$ 可能是 PPT 不可判定的. (这一点在基于模拟的证明中不一定为真).
- 事件 $F$ 的概率 $\Pr[F]$ 必须是**可忽略**的, 否则无法保证切换的正确性.

# 切换方式 - 失败事件 (注意事项)

- 事件 $F$ 可能是 PPT 不可判定的. (这一点在基于模拟的证明中不一定为真).
- 事件 $F$ 的概率 $\Pr[F]$ 必须是**可忽略**的, 否则无法保证切换的正确性.
- 通常 $F$ 应该在 $\mathbf{G}_{i,\mathcal{A}}$ 或者 $\mathbf{G}_{i+1,\mathcal{A}}$ 中能够求出上界.

# 切换方式 - 失败事件 (注意事项)

- 事件 $F$ 可能是 PPT 不可判定的. (这一点在基于模拟的证明中不一定为真).
- 事件 $F$ 的概率 $\Pr[F]$ 必须是可忽略的, 否则无法保证切换的正确性.
- 通常 $F$ 应该在 $\mathbf{G}_{i,\mathcal{A}}$ 或者 $\mathbf{G}_{i+1,\mathcal{A}}$ 中能够求出上界.
- 也有可能事件 $F$ 会一直无法求出上界, 直到一个后续的游戏 $\mathbf{G}_j$ 中才可以求出上界.

# 切换方式 - 桥接事件

## 桥接步骤

通常用来表示在 $\mathbf{G}_i$ 和 $\mathbf{G}_{i+1}$ 之间的唯一区别就是某个变量是用两种不同但等价的方式计算.

- **例如:** $a = \mathbf{k}^\intercal(\mathbf{A}\mathbf{w}) = (\mathbf{k}^\intercal\mathbf{A})\mathbf{w}$.

# 切换方式 - 桥接事件

## 桥接步骤

通常用来表示在 $\mathbf{G}_i$ 和 $\mathbf{G}_{i+1}$ 之间的唯一区别就是某个变量是用两种不同但等价的方式计算.

- **例如:** $a = \mathbf{k}^\intercal(\mathbf{A}\mathbf{w}) = (\mathbf{k}^\intercal\mathbf{A})\mathbf{w}$.
- 这种切换方式通常是显然正确的, 因为两种计算方式是等价的.

# 切换方式 - 桥接事件

## 桥接步骤

通常用来表示在 $\mathbf{G}_i$ 和 $\mathbf{G}_{i+1}$ 之间的唯一区别就是某个变量是用两种不同但等价的方式计算.

- **例如:** $a = \mathbf{k}^\intercal(\mathbf{A}\mathbf{w}) = (\mathbf{k}^\intercal\mathbf{A})\mathbf{w}$.
- 这种切换方式通常是显然正确的, 因为两种计算方式是等价的.
- 这种切换方式主要是为后续的不可区分性切换或者失败事件切换做铺垫.

# 样例：哈希 El-Gamal 加密方案

- El-Gamal 加密方案加密了一个群元素，
  **如何加密一个消息比特串？**

# 样例：哈希 El-Gamal 加密方案

- El-Gamal 加密方案加密了一个群元素，**如何加密一个消息比特串？**
- El-Gamal 加密方案的一个变种.

# 样例：哈希 El-Gamal 加密方案 - 回顾：IND-CPA


- IND-CPA 安全性

# 样例：哈希 El-Gamal 加密方案 - 回顾：IND-CPA


- IND-CPA 安全性
- $\mathbf{Exp}^{\text{IND-CPA}}_{\mathbf{\Pi},\mathcal{A}}(1^\lambda)$ :

# 样例：哈希 El-Gamal 加密方案 - 回顾：IND-CPA


- IND-CPA 安全性
- $\mathbf{Exp}^{\text{IND-CPA}}_{\mathbf{\Pi},\mathcal{A}}(1^\lambda)$ :
  1. $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathbf{\Pi}.\mathsf{KGen}(1^\lambda)$

# 样例：哈希 El-Gamal 加密方案 - 回顾：IND-CPA


- IND-CPA 安全性
- $\mathbf{Exp}^{\text{IND-CPA}}_{\mathbf{\Pi},\mathcal{A}}(1^\lambda)$ :
  1. $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathbf{\Pi}.\mathsf{KGen}(1^\lambda)$
  2. $(m_0, m_1) \xleftarrow{\$} \mathcal{A}(\mathsf{pk})$, 其中 $|m_0| = |m_1|$

# 样例：哈希 El-Gamal 加密方案 - 回顾：IND-CPA


- IND-CPA 安全性
- $\mathbf{Exp}^{\text{IND-CPA}}_{\mathbf{\Pi},\mathcal{A}}(1^\lambda)$ :
  1. $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathbf{\Pi}.\mathsf{KGen}(1^\lambda)$
  2. $(m_0, m_1) \xleftarrow{\$} \mathcal{A}(\mathsf{pk})$, 其中 $|m_0| = |m_1|$
  3. $b \xleftarrow{\$} \{0,1\}$; $\mathsf{ct}^\star \xleftarrow{\$} \mathbf{\Pi}.\mathsf{Enc}(\mathsf{pk}, m_b)$

# 样例：哈希 El-Gamal 加密方案 - 回顾：IND-CPA


- IND-CPA 安全性
- $\mathbf{Exp}^{\text{IND-CPA}}_{\mathbf{\Pi},\mathcal{A}}(1^\lambda)$ :
  1. $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathbf{\Pi}.\mathsf{KGen}(1^\lambda)$
  2. $(m_0, m_1) \xleftarrow{\$} \mathcal{A}(\mathsf{pk})$, 其中 $|m_0| = |m_1|$
  3. $b \xleftarrow{\$} \{0,1\}$; $\mathsf{ct}^\star \xleftarrow{\$} \mathbf{\Pi}.\mathsf{Enc}(\mathsf{pk}, m_b)$
  4. $b' \xleftarrow{\$} \mathcal{A}(\mathsf{ct}^\star)$

# 样例：哈希 El-Gamal 加密方案 - 回顾：IND-CPA


- IND-CPA 安全性
- $\mathbf{Exp}^{\text{IND-CPA}}_{\mathbf{\Pi},\mathcal{A}}(1^\lambda)$ :
  1. $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathbf{\Pi}.\mathsf{KGen}(1^\lambda)$
  2. $(m_0, m_1) \xleftarrow{\$} \mathcal{A}(\mathsf{pk})$, 其中 $|m_0| = |m_1|$
  3. $b \xleftarrow{\$} \{0,1\}$; $\mathsf{ct}^\star \xleftarrow{\$} \mathbf{\Pi}.\mathsf{Enc}(\mathsf{pk}, m_b)$
  4. $b' \xleftarrow{\$} \mathcal{A}(\mathsf{ct}^\star)$
  5. **return** $[\![b' = b]\!]$

# 样例: 哈希 El-Gamal 加密方案 - 熵平滑哈希 (Entropy Smoothing Hash)

需要一个特殊性质的哈希函数, 要求当 $k, X$ 均随机采样时, $(k, \mathsf{H}_k(X))$ 与随机采样的 $(k, h)$ 不可区分.

# 样例: 哈希 El-Gamal 加密方案 - 熵平滑哈希 (Entropy Smoothing Hash)

需要一个特殊性质的哈希函数, 要求当 $k, X$ 均随机采样时, $(k, \mathsf{H}_k(X))$ 与随机采样的 $(k, h)$ 不可区分.

## 熵平滑哈希

设 $\mathcal{H} = \{\mathsf{H}_k : \mathbb{G} \to \{0,1\}^\ell\}_{k \in \mathcal{K}}$ 为一个哈希函数族. 对于任意 PPT 敌手 $\mathcal{A}$, 定义下列熵平滑优势:

$$\mathsf{Adv}^{\mathsf{ES}}_{\mathcal{H},\mathcal{A}}(1^\lambda) = \Big|\Pr\Big[\mathcal{A}(k,h) = 1 \;\Big|\; k \xleftarrow{\$} \mathcal{K}, x \xleftarrow{\$} \mathbb{Z}_p, h \hookleftarrow \mathsf{U}\left(\{0,1\}^\ell\right)\Big] - \Pr\Big[\mathcal{A}(k,h) = 1 \;\Big|\; k \xleftarrow{\$} \mathcal{K}, x \xleftarrow{\$} \mathbb{Z}_p, h \xleftarrow{\$} \mathsf{H}_k(g^x)\Big]\Big|.$$

如果存在这样的哈希函数族 $\mathcal{H}$, 使得对于任意 PPT 敌手 $\mathcal{A}$, 都有 $\mathsf{Adv}^{\mathsf{ES}}_{\mathcal{H},\mathcal{A}}(1^\lambda) \le \mathsf{negl}(\lambda)$, 则称 $\mathcal{H}$ 为熵平滑哈希族.

# 样例：哈希 El-Gamal 加密方案

## 哈希 El-Gamal

$\mathsf{KGen}(1^\lambda)$:

1. $x \xleftarrow{\$} \mathbb{Z}_p;\ k \xleftarrow{\$} \mathcal{K}$
2. $X := g^x$
3. $\mathsf{pk} := (X, k);\ \mathsf{sk} := (x, k)$
4. **return** $(\mathsf{pk}, \mathsf{sk})$

$\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$ :

1. **parse** $(\mathsf{sk}, \mathsf{ct})$ as $(x, (R, C))$
2. $K := \mathsf{H}_k(R^x)$
3. $m := K \oplus C$
4. **return** $m$

$\mathsf{Enc}(\mathsf{pk}, m)$:

1. $r \xleftarrow{\$} \mathbb{Z}_p;\ R := g^r;\ Z = X^r$
2. $K := \mathsf{H}_k(Z)$
3. $\mathsf{ct} := (R, K \oplus m)$
4. **return** $\mathsf{ct}$

# 样例: 哈希 El-Gamal 加密方案

**定理**

如果 $\mathcal{H}$ 为熵平滑哈希族, 则哈希 El-Gamal 加密方案在 DDH 假设下满足 IND-CPA 安全性.

- $\mathbf{G}_0$: 原始安全游戏. $\mathsf{pr}_0 = \mathbf{Exp}_{\mathcal{A}}^{\text{IND-CPA}}(1^\lambda)$.

# 样例: 哈希 El-Gamal 加密方案

**定理**

如果 $\mathcal{H}$ 为熵平滑哈希族, 则哈希 El-Gamal 加密方案在 DDH 假设下满足 IND-CPA 安全性.

- $\mathbf{G}_0$: 原始安全游戏. $\mathsf{pr}_0 = \mathbf{Exp}_{\mathcal{A}}^{\text{IND-CPA}}(1^\lambda)$.
- $\mathbf{G}_1$: 将挑战密文中的 $Z = X^r$ 替换为随机采样的 $Z \xleftarrow{\$} \mathbb{G}$.**(不可区分性)**

$$|\mathsf{pr}_0 - \mathsf{pr}_1| \leq \mathsf{Adv}^{\mathsf{DDH}}_{\mathbb{G},\mathcal{B}_1}(1^\lambda).$$

# 样例: 哈希 El-Gamal 加密方案

**定理**

如果 $\mathcal{H}$ 为熵平滑哈希族, 则哈希 El-Gamal 加密方案在 DDH 假设下满足 IND-CPA 安全性.

- $\mathbf{G}_0$: 原始安全游戏. $\mathsf{pr}_0 = \mathbf{Exp}_{\mathcal{A}}^{\text{IND-CPA}}(1^\lambda)$.
- $\mathbf{G}_1$: 将挑战密文中的 $Z = X^r$ 替换为随机采样的 $Z \xleftarrow{\$} \mathbb{G}$.**(不可区分性)**

$$|\mathsf{pr}_0 - \mathsf{pr}_1| \leq \mathsf{Adv}^{\mathsf{DDH}}_{\mathbb{G},\mathcal{B}_1}(1^\lambda).$$

- $\mathbf{G}_2$: 将挑战密文中的 $K = \mathsf{H}_k(Z)$ 替换为随机采样的 $K \xleftarrow{\$} \{0,1\}^\ell$.**(不可区分性)**

$$|\mathsf{pr}_1 - \mathsf{pr}_2| \leq \mathsf{Adv}^{\mathsf{ES}}_{\mathcal{H},\mathcal{B}_2}(1^\lambda).$$

# 样例: 哈希 El-Gamal 加密方案

**定理**

如果 $\mathcal{H}$ 为熵平滑哈希族, 则哈希 El-Gamal 加密方案在 DDH 假设下满足 IND-CPA 安全性.

- $\mathbf{G}_0$: 原始安全游戏. $\mathsf{pr}_0 = \mathbf{Exp}_{\mathcal{A}}^{\text{IND-CPA}}(1^\lambda)$.
- $\mathbf{G}_1$: 将挑战密文中的 $Z = X^r$ 替换为随机采样的 $Z \xleftarrow{\$} \mathbb{G}$.**(不可区分性)**

$$|\mathsf{pr}_0 - \mathsf{pr}_1| \leq \mathsf{Adv}^{\mathsf{DDH}}_{\mathbb{G},\mathcal{B}_1}(1^\lambda).$$

- $\mathbf{G}_2$: 将挑战密文中的 $K = \mathsf{H}_k(Z)$ 替换为随机采样的 $K \xleftarrow{\$} \{0,1\}^\ell$.**(不可区分性)**

$$|\mathsf{pr}_1 - \mathsf{pr}_2| \leq \mathsf{Adv}^{\mathsf{ES}}_{\mathcal{H},\mathcal{B}_2}(1^\lambda).$$

- $\mathbf{G}_3$: 将挑战密文中的 $C = K \oplus m_b$ 替换为随机采样的 $C \xleftarrow{\$} \{0,1\}^\ell$.**(不可区分性)**

$$|\mathsf{pr}_2 - \mathsf{pr}_3| = 0.$$

# 样例 2: 弱 Cramer-Shoup 加密方案

**背景:** Cramer-Shoup 加密方案是第一个基于标准假设 (DDH 假设) 的公钥加密方案, 并且满足 IND-CCA 安全性 [Cramer and Shoup, 1998].
**弱 Cramer-Shoup 加密方案**是 Cramer-Shoup 加密方案的一个简化版本.

- $\text{IND-CPA}^{\text{Cor}}$ 安全性 (indistinguishability under chosen-plaintext attack with corruption)

# 样例 2: 弱 Cramer-Shoup 加密方案

**背景:** Cramer-Shoup 加密方案是第一个基于标准假设 (DDH 假设) 的公钥加密方案, 并且满足 IND-CCA 安全性 [Cramer and Shoup, 1998].
**弱 Cramer-Shoup 加密方案**是 Cramer-Shoup 加密方案的一个简化版本.

- $\text{IND-CPA}^{\text{Cor}}$ 安全性 (indistinguishability under chosen-plaintext attack with corruption)
- $\text{IND-CPA}^{\text{Cor}}$ 要求首先给敌手提供 $(\mathsf{pk}_1, \ldots, \mathsf{pk}_N)$, 敌手选择两个消息 $m_0, m_1$ 进行对 $\mathsf{pk}_{\mathcal{I}}$ 进行挑战, 其中 $\mathcal{I} \subseteq [N]$.

# 样例 2: 弱 Cramer-Shoup 加密方案

**背景:** Cramer-Shoup 加密方案是第一个基于标准假设 (DDH 假设) 的公钥加密方案, 并且满足 IND-CCA 安全性 [Cramer and Shoup, 1998].
**弱 Cramer-Shoup 加密方案**是 Cramer-Shoup 加密方案的一个简化版本.

- $\text{IND-CPA}^{\text{Cor}}$ 安全性 (indistinguishability under chosen-plaintext attack with corruption)
- $\text{IND-CPA}^{\text{Cor}}$ 要求首先给敌手提供 $(\mathsf{pk}_1, \ldots, \mathsf{pk}_N)$, 敌手选择两个消息 $m_0, m_1$ 进行对 $\mathsf{pk}_{\mathcal{I}}$ 进行挑战, 其中 $\mathcal{I} \subseteq [N]$.
- 敌手还可以选择获取任意一个私钥 $\mathsf{sk}_j$, 但不能选择挑战私钥 $\mathsf{sk}_{i^\star \in \mathcal{I}}$.

# 样例 2: 弱 Cramer-Shoup 加密方案

## $\mathcal{O}_{\mathsf{Cor}}(i)$

1. $\mathcal{L}_{\mathsf{sk}} \xleftarrow{\$} \mathcal{L}_{\mathsf{sk}} \cup \{i\}$
2. **return** $\mathsf{sk}_i$

## $\text{IND-CPA}^{\mathsf{Cor}}$ 安全性

$\mathbf{Exp}^{\text{IND-CPA}^{\mathsf{Cor}}}_{\mathbf{\Pi},\mathcal{A}}(1^\lambda)$ :

1. $b \hookleftarrow \mathsf{U}(\{0,1\})$ ; $\mathsf{pp} \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$; **for** $i \in [N]$ : $(\mathsf{pk}_i, \mathsf{sk}_i) \xleftarrow{\$} \mathcal{O}_{\mathsf{KGen}}(i, \mathsf{pp})$
2. $(\mathsf{m}_0, \mathsf{m}_1, \mathcal{I}) \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\mathsf{Cor}}}(\mathsf{pk}_{[N]})$
3. $\mathbf{C} = (\mathcal{O}_{\mathsf{Enc}}(i, \mathsf{m}_b))_{i\in[\mathcal{I}]} = (\mathsf{Enc}(\mathsf{pk}_i, \mathsf{m}_b))_{i\in[\mathcal{I}]}$
4. $b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\mathsf{Cor}}}(\mathbf{C})$
5. **return** $[\![b' = b \wedge \mathcal{I} \cap \mathcal{L}_{\mathsf{sk}} = \emptyset]\!]$

# 样例 2: 弱 Cramer-Shoup 加密方案

## 弱 Cramer-Shoup 加密方案

$\mathsf{Setup}(1^\lambda)$ :

1. $a \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$ ; $\left[\mathbf{A}\right] := \begin{bmatrix} 1 & a \end{bmatrix}^\intercal \in \mathbb{G}^2$
2. **return** $\mathsf{pp} := \left[\mathbf{A}\right]$

$\mathsf{KGen}(1^\lambda)$:

1. $k_1, k_2 \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$
2. $\mathbf{k} := \begin{pmatrix} k_1 & k_2 \end{pmatrix}^\intercal \in \mathbb{Z}_p^2$
3. $\mathsf{pk} := \mathbf{k}^\intercal \left[\mathbf{A}\right]$ ; $\mathsf{sk} := \mathbf{k}$
4. **return** $(\mathsf{pk}, \mathsf{sk})$

$\mathsf{Enc}(\mathsf{pk}, \mathsf{m} \in \mathbb{G})$ :

1. $r \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$
2. $\mathbf{x} = \left[\mathbf{A}\right] r \in \mathbb{Z}_p^2$
3. $\mathsf{ct} := \mathsf{pk} \cdot r + \mathsf{m} \in \mathbb{G}$
4. **return** $\mathsf{ct}$

# 样例 2: 弱 Cramer-Shoup 加密方案

## 弱 Cramer-Shoup 加密方案 (安全性规约)

$\mathsf{Setup}(1^\lambda)$ :

1. $a \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$ ; $\left[\mathbf{A}\right] := \begin{bmatrix} 1 & a \end{bmatrix}^\mathsf{T} \in \mathbb{G}^2$
2. **return** $\mathsf{pp} := \left[\mathbf{A}\right]$

$\mathcal{O}_{\mathsf{KGen}}(i)$:

1. $\mathbf{k}_i := \begin{pmatrix} k_1 & k_2 \end{pmatrix}^\mathsf{T} \hookleftarrow \mathsf{U}\left(\mathbb{Z}_p^2\right)$
2. $\mathsf{pk}_i := \mathbf{k}_i^\mathsf{T} \left[\mathbf{A}\right]$ ; $\mathsf{sk}_i := \mathbf{k}_i$
3. **return** $(\mathsf{pk}_i, \mathsf{sk}_i)$

$\mathcal{O}_{\mathsf{Enc}}(i, \mathsf{m} \in \mathbb{G})$ :

1. $r \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$
2. $\mathbf{x} = \left[\mathbf{A}\right] r \in \mathbb{Z}_p^2$
3. $\mathsf{ct} := \mathsf{pk}_i \cdot r + \mathsf{m} \in \mathbb{G}$
4. **return** ct

# 样例 2: 弱 Cramer-Shoup 加密方案

## 弱 Cramer-Shoup 加密方案 (安全性规约)

$\mathsf{Setup}(1^\lambda)$ :

1. $a \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$ ; $\left[\mathbf{A}\right] := \begin{bmatrix} 1 & a \end{bmatrix}^\mathsf{T} \in \mathbb{G}^2$
2. **return** $\mathsf{pp} := \left[\mathbf{A}\right]$

$\mathcal{O}_{\mathsf{KGen}}(i)$:

1. $\mathbf{k}_i := \begin{pmatrix} k_1 & k_2 \end{pmatrix}^\mathsf{T} \hookleftarrow \mathsf{U}\left(\mathbb{Z}_p^2\right)$
2. $\mathsf{pk}_i := \mathbf{k}_i^\mathsf{T} \left[\mathbf{A}\right]$ ; $\mathsf{sk}_i := \mathbf{k}_i$
3. **return** $(\mathsf{pk}_i, \mathsf{sk}_i)$

$\mathcal{O}_{\mathsf{Enc}}(i, \mathsf{m} \in \mathbb{G})$ :

1. $r \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$
2. $\mathbf{x} = \left[\mathbf{A}\right] r \in \mathbb{Z}_p^2$
3. $\mathsf{ct} := \mathbf{k}_i \cdot \mathbf{x} + \mathsf{m} \in \mathbb{G}$
4. **return** ct

# 样例 2: 弱 Cramer-Shoup 加密方案

## 弱 Cramer-Shoup 加密方案 (安全性规约)

$\mathsf{Setup}(1^\lambda)$ :

1. $a \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$ ; $\left[\mathbf{A}\right] := \begin{bmatrix} 1 & a \end{bmatrix}^\mathsf{T} \in \mathbb{G}^2$
2. **return** $\mathsf{pp} := \left[\mathbf{A}\right]$

$\mathcal{O}_{\mathsf{KGen}}(i)$:

1. $\mathbf{k}_i := \begin{pmatrix} k_1 & k_2 \end{pmatrix}^\mathsf{T} \hookleftarrow \mathsf{U}\left(\mathbb{Z}_p^2\right)$
2. $\mathsf{pk}_i := \mathbf{k}_i^\mathsf{T} \left[\mathbf{A}\right]$ ; $\mathsf{sk}_i := \mathbf{k}_i$
3. **return** $(\mathsf{pk}_i, \mathsf{sk}_i)$

$\mathcal{O}_{\mathsf{Enc}}(i, \mathsf{m} \in \mathbb{G})$ :

1. $\mathbf{x} \hookleftarrow \mathsf{U}\left(\mathbb{Z}_p^2\right)$
2. $\mathsf{ct} := \mathbf{k}_i \cdot \mathbf{x} + \mathsf{m} \in \mathbb{G}$
3. **return** $\mathsf{ct}$

# 样例 2: 弱 Cramer-Shoup 加密方案

## 弱 Cramer-Shoup 加密方案 (安全性规约)

$\mathsf{Setup}(1^\lambda)$ :

1. $a \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$ ; $\left[\mathbf{A}\right] := \begin{bmatrix} 1 & a \end{bmatrix}^\intercal \in \mathbb{G}^2$
2. **return** $\mathsf{pp} := \left[\mathbf{A}\right]$, $\mathbf{h} := \begin{pmatrix} -a & 1 \end{pmatrix}^\intercal$

$\mathcal{O}_{\mathsf{KGen}}(i)$:

1. $\mathbf{k}_i := \begin{pmatrix} k_1 & k_2 \end{pmatrix}^\intercal \hookleftarrow \mathsf{U}\left(\mathbb{Z}_p^2\right)$
2. $\mathsf{pk}_i := \mathbf{k}_i^\intercal \left[\mathbf{A}\right]$ ; $\mathsf{sk}_i := \mathbf{k}_i$
3. **return** $(\mathsf{pk}_i, \mathsf{sk}_i)$

$\mathcal{O}_{\mathsf{Enc}}(i, \mathsf{m} \in \mathbb{G})$ :

1. $\mathbf{x} \hookleftarrow \mathsf{U}\left(\mathbb{Z}_p^2\right)$
2. $\mathsf{ct} := \mathbf{k}_i \cdot \mathbf{x} + \mathsf{m} \in \mathbb{G}$
3. **return** ct

# 样例 2: 弱 Cramer-Shoup 加密方案

## 弱 Cramer-Shoup 加密方案 (安全性规约)

$\mathsf{Setup}(1^\lambda)$ :

1. $a \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$ ; $\left[\mathbf{A}\right] := \begin{bmatrix} 1 & a \end{bmatrix}^\intercal \in \mathbb{G}^2$
2. **return** $\mathsf{pp} := \left[\mathbf{A}\right]$, $\mathbf{h} := \begin{pmatrix} -a & 1 \end{pmatrix}^\intercal$

$\mathcal{O}_{\mathsf{KGen}}(i)$:

1. $\mathbf{k}_i := \begin{pmatrix} k_1 & k_2 \end{pmatrix}^\intercal \hookleftarrow \mathsf{U}\left(\mathbb{Z}_p^2\right)$
2. $\ell \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$
3. $\mathsf{pk}_i := \mathbf{k}_i^\intercal \left[\mathbf{A}\right]$ ; $\mathsf{sk}_i := \mathbf{k}_i + \ell \cdot \mathbf{h}$
4. **return** $(\mathsf{pk}_i, \mathsf{sk}_i)$

$\mathcal{O}_{\mathsf{Enc}}(i, \mathsf{m} \in \mathbb{G})$ :

1. $\mathbf{x} \hookleftarrow \mathsf{U}\left(\mathbb{Z}_p^2\right)$
2. $\mathsf{ct} := \mathbf{k}_i \cdot \mathbf{x} + \mathsf{m} \in \mathbb{G}$
3. **return** ct

# 样例 2: 弱 Cramer-Shoup 加密方案

## 弱 Cramer-Shoup 加密方案 (安全性规约)

$\mathsf{Setup}(1^\lambda)$ :

1. $a \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$ ; $\left[\mathbf{A}\right] := \begin{bmatrix} 1 & a \end{bmatrix}^\intercal \in \mathbb{G}^2$
2. **return** $\mathsf{pp} := \left[\mathbf{A}\right]$, $\mathbf{h} := \begin{pmatrix} -a & 1 \end{pmatrix}^\intercal$

$\mathcal{O}_{\mathsf{KGen}}(i)$:

1. $\mathbf{k}_i := \begin{pmatrix} k_1 & k_2 \end{pmatrix}^\intercal \hookleftarrow \mathsf{U}\left(\mathbb{Z}_p^2\right)$
2. $\ell \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$
3. $\mathsf{pk}_i := \mathbf{k}_i^\intercal \left[\mathbf{A}\right]$ ; $\mathsf{sk}_i := \mathbf{k}_i + \ell \cdot \mathbf{h}$
4. **return** $(\mathsf{pk}_i, \mathsf{sk}_i)$

$\mathcal{O}_{\mathsf{Enc}}(i, \mathsf{m} \in \mathbb{G})$ :

1. $\mathbf{x} \hookleftarrow \mathsf{U}\left(\mathbb{Z}_p^2\right)$
2. $\mathsf{ct} := \mathbf{k}_i \cdot \mathbf{x} + \mathsf{m} + \ell \cdot \mathbf{h}$
3. **return** $\mathsf{ct}$

# 样例 2: 弱 Cramer-Shoup 加密方案

## 弱 Cramer-Shoup 加密方案 (安全性规约)

$\mathsf{Setup}(1^\lambda)$ :

1. $a \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$ ; $\left[\mathbf{A}\right] := \begin{bmatrix} 1 & a \end{bmatrix}^\intercal \in \mathbb{G}^2$
2. **return** $\mathsf{pp} := \left[\mathbf{A}\right]$, $\mathbf{h} := \begin{pmatrix} -a & 1 \end{pmatrix}^\intercal$

$\mathcal{O}_{\mathsf{KGen}}(i)$:

1. $\mathbf{k}_i := \begin{pmatrix} k_1 & k_2 \end{pmatrix}^\intercal \hookleftarrow \mathsf{U}\left(\mathbb{Z}_p^2\right)$
2. $\ell \hookleftarrow \mathsf{U}(\mathbb{Z}_p)$
3. $\mathsf{pk}_i := \mathbf{k}_i^\intercal \left[\mathbf{A}\right]$ ; $\mathsf{sk}_i := \mathbf{k}_i + \ell \cdot \mathbf{h}$
4. **return** $(\mathsf{pk}_i, \mathsf{sk}_i)$

$\mathcal{O}_{\mathsf{Enc}}(i, \mathsf{m} \in \mathbb{G})$ :

1. $\mathbf{x} \hookleftarrow \mathsf{U}\left(\mathbb{Z}_p^2\right)$
2. $\mathsf{ct} \hookleftarrow \mathsf{U}(\mathbb{G})$
3. **return** ct

# References


Bellare, M. and Rogaway, P. (2006).
The security of triple encryption and a framework for code-based game-playing proofs.
In Vaudenay, S., editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 409–426. Springer, Berlin, Heidelberg.

Cramer, R. and Shoup, V. (1998).
A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack.
In Krawczyk, H., editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 13–25. Springer, Berlin, Heidelberg.

Shoup, V. (2004).
Sequences of games: a tool for taming complexity in security proofs.
Cryptology ePrint Archive, Report 2004/332.