



# 现代密码学

## 可证明安全性与Elgamal加密方案简介

王煜宇

信息与软件工程学院

电子科技大学



# 目录

---

- 密码游戏与规约
  - **CDH**假设
  - 加密方案的定义
  - 具体的加密方案
  - 加密方案的安全性证明
-



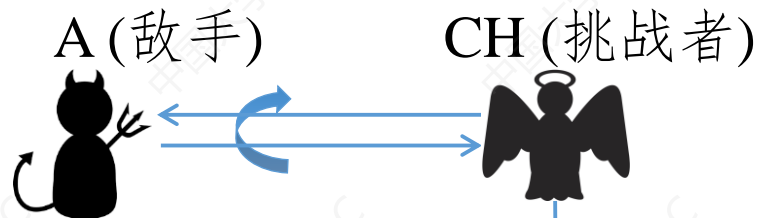
# 目录

---

- 密码游戏与规约
  - **CDH假设**
  - 加密方案的定义
  - 具体的加密方案
  - 加密方案的安全性证明
-



# 密码游戏



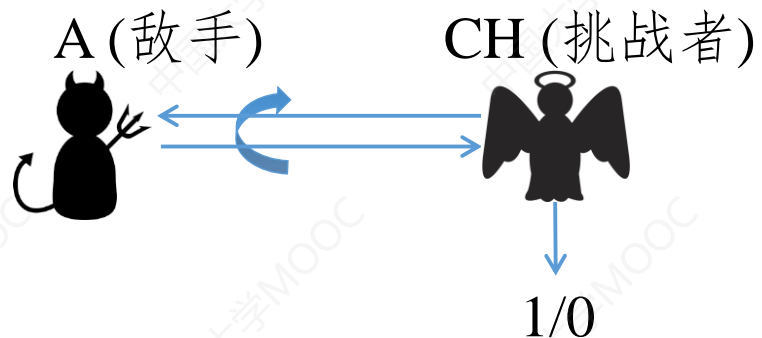
敌手能攻破密码游戏  $\Leftrightarrow$  挑战者输出 1

1/0

$\Pr[\text{CH 输出 } 1] = \text{negl} \Rightarrow \text{密码游戏是安全的}$



# 密码游戏

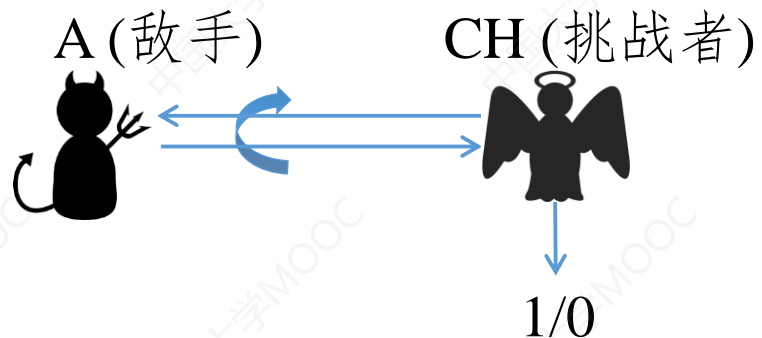


$\Pr[\text{CH 输出 } 1] = \text{negl} \Rightarrow \text{密码游戏是安全的}$

可忽略的概率



# 密码游戏



几乎所有的计算性的假设和安全性都能用密码游戏来表示

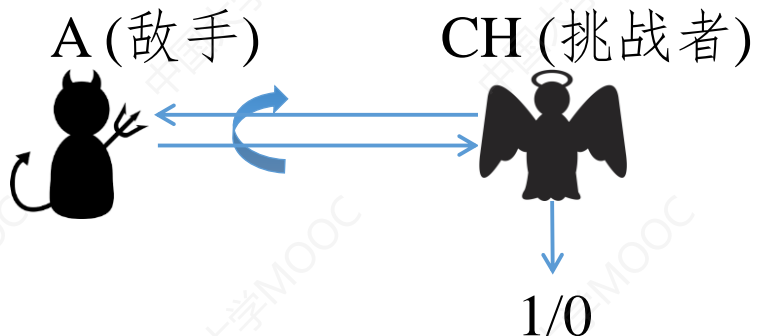
$\Pr[\text{CH 输出 } 1] = \text{negl} \Rightarrow \text{密码游戏是安全的}$



# 规约

假设

$G_1$ 的可证明安全性：基于 $G_2$ 证明 $G_1$ 的安全性

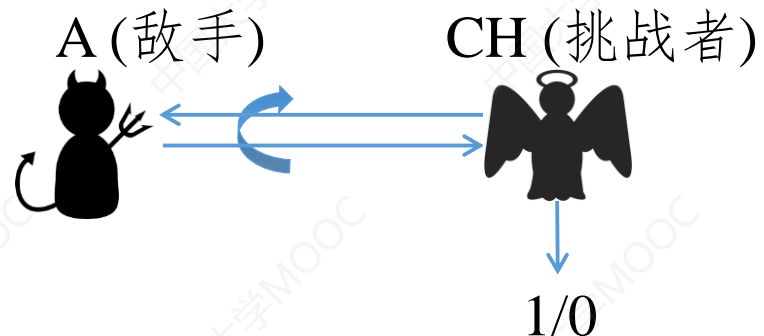


$\Pr[\text{CH 输出 } 1] = \text{negl} \Rightarrow \text{密码游戏是安全的}$



# 规约

假设



$\Pr[\text{CH 输出 } 1] = \text{negl} \Rightarrow \text{密码游戏是安全的}$

$G_1$ 的可证明安全性：基于 $G_2$ 证明 $G_1$ 的安全性



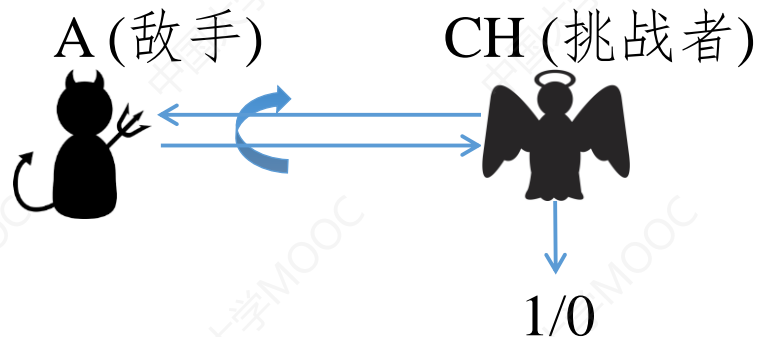
$G_2 \text{ 安全} \implies G_1 \text{ 安全}$





# 规约

假设



$\Pr[\text{CH 输出 } 1] = \text{negl} \Rightarrow \text{密码游戏是安全的}$

$G_1$ 的可证明安全性：基于 $G_2$ 证明 $G_1$ 的安全性

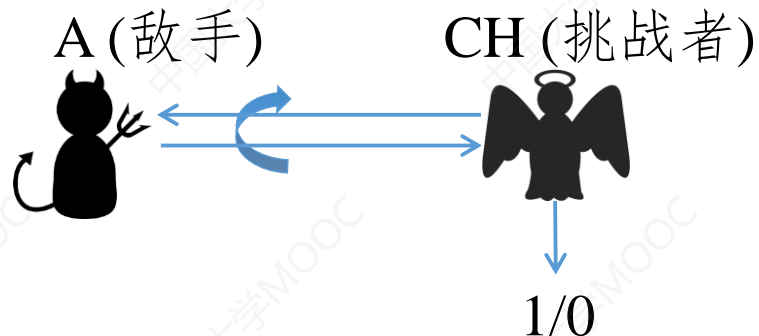
$G_2 \text{ 安全} \implies G_1 \text{ 安全}$

$G_1 \text{ 不安全} \implies G_2 \text{ 不安全}$



# 规约

假设



$\Pr[\text{CH 输出 } 1] = \text{negl} \Rightarrow \text{密码游戏是安全的}$

$G_1$ 的可证明安全性：基于 $G_2$ 证明 $G_1$ 的安全性

$G_2 \text{ 安全} \implies G_1 \text{ 安全}$

$G_1 \text{ 不安全} \implies G_2 \text{ 不安全}$

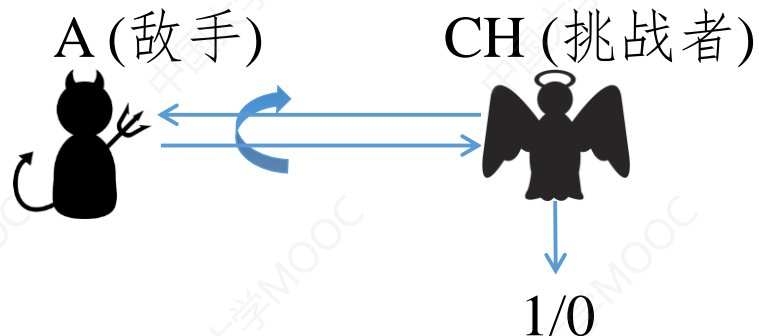
存在敌手攻破 $G_1 \implies$ 存在敌手攻破 $G_2$



# 规约

假设

$G_1$ 的可证明安全性：基于 $G_2$ 证明 $G_1$ 的安全性



$\Pr[\text{CH 输出 } 1] = \text{negl} \Rightarrow \text{密码游戏是安全的}$

$G_2 \text{ 安全} \implies G_1 \text{ 安全}$

$G_1 \text{ 不安全} \implies G_2 \text{ 不安全}$

存在敌手攻破 $G_1 \implies$ 存在敌手攻破 $G_2$

$G_1$ 到 $G_2$ 的规约

攻破 $G_1$ 的敌手

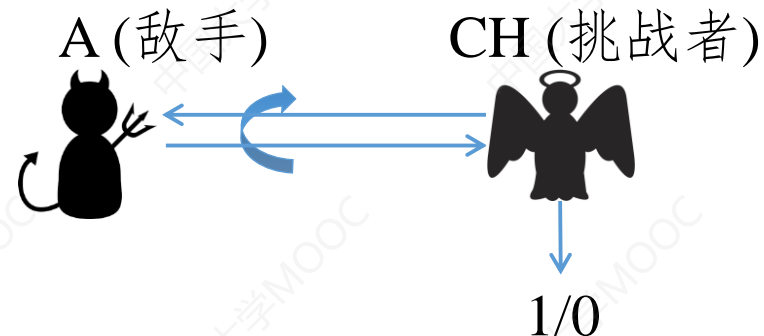




# 规约

假设

$G_1$ 的可证明安全性：基于 $G_2$ 证明 $G_1$ 的安全性



$\Pr[\text{CH 输出 } 1] = \text{negl} \Rightarrow \text{密码游戏是安全的}$

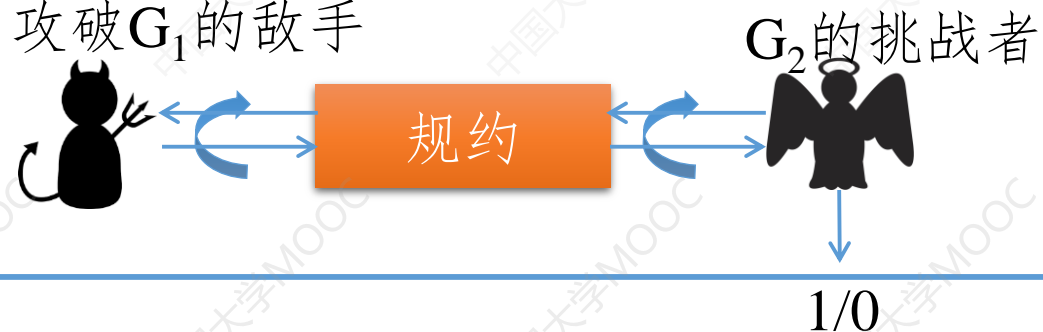
$G_2 \text{ 安全} \Rightarrow G_1 \text{ 安全}$

$G_1 \text{ 不安全} \Rightarrow G_2 \text{ 不安全}$

存在敌手攻破 $G_1 \Rightarrow$ 存在敌手攻破 $G_2$

$G_1$ 到 $G_2$ 的规约

攻破 $G_1$ 的敌手





# 目录

---

- 密码游戏与规约
  - **CDH假设**
  - 加密方案的定义
  - 具体的加密方案
  - 加密方案的安全性证明
-

A decorative blue horizontal bar with a series of vertical lines of varying heights, creating a striped effect.

# CDH假设 [DH76]

---

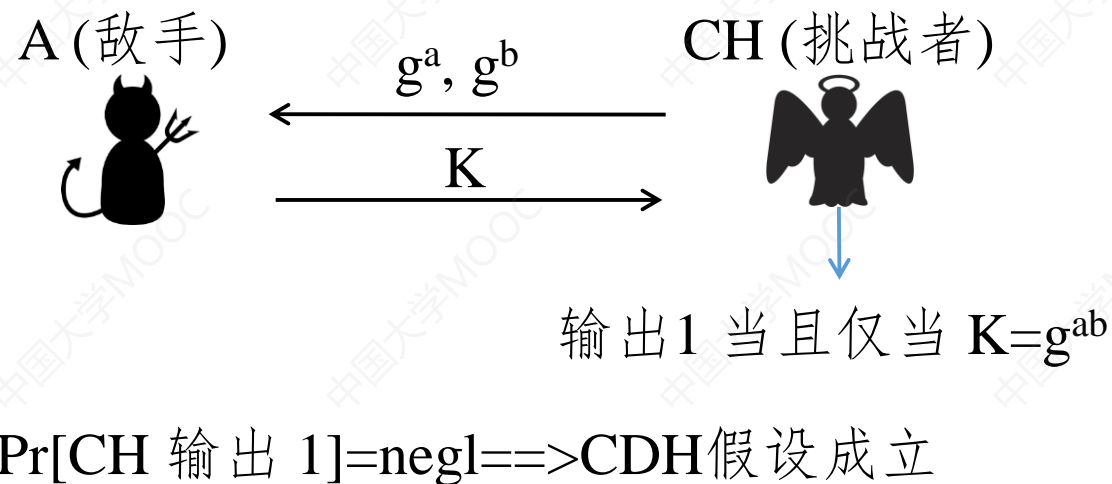
$G$ : 阶为 $q$ 的循环群  
 $\{g^1, g^2, \dots, g^q\}$

$Z_q = \{1, 2, \dots, q\}$

# CDH假设 [DH76]

$G$ : 阶为 $q$ 的循环群  
 $\{g^1, g^2, \dots, g^q\}$

$Z_q = \{1, 2, \dots, q\}$





# 目录

---

- 密码游戏与规约
  - **CDH假设**
  - 加密方案的定义
  - 具体的加密方案
  - 加密方案的安全性证明
-





# 加密

---

$\text{Gen}(1^k) \rightarrow (\text{pk}, \text{sk})$

$\text{Enc}(\text{pk}, m) \rightarrow \text{ct}$

$\text{Dec}(\text{sk}, \text{ct}) = m$

正确性:  $\text{Dec}(\text{sk}, (\text{Enc}(\text{pk}, m))) = m$



# 加密

$$\text{Gen}(1^k) \rightarrow (\text{pk}, \text{sk})$$

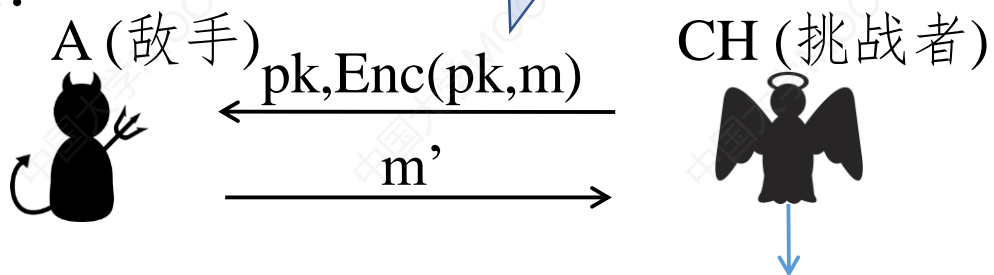
$$\text{Enc}(\text{pk}, m) \rightarrow \text{ct}$$

$$\text{Dec}(\text{sk}, \text{ct}) = m$$

$$\text{正确性: } \text{Dec}(\text{sk}, (\text{Enc}(\text{pk}, m))) = m$$

随机生成的密文

单向性:



1 当且仅当  $m=m'$

$\Pr[\text{CH 输出 } 1] = \text{negl} \Rightarrow \text{加密方案满足单向性}$



# 目录

---

- 密码游戏与规约
  - **CDH假设**
  - 加密方案的定义
  - 具体的加密方案
  - 加密方案的安全性证明
-

# Elgama1加密方案 [Elgama184]

---

$\text{Gen}(1^k): x \leftarrow Z_q, pk=g^x, sk=x$

$\text{Enc}(pk,m): r \leftarrow Z_q, ct=(c=mg^{xr}, c'=g^r)$

$\text{Dec}(sk,ct=(c,c')): m=cc'^{-x}$

正确性:  $cc'^{-x}=mg^{xr}g^{-rx}=m$



# 目录

---

- 密码游戏与规约
  - **CDH假设**
  - 加密方案的定义
  - 具体的加密方案
  - 加密方案的安全性证明
-

# E1gama1加密基于CDH假设的单向性

$\text{Gen}(1^k): x \leftarrow \mathbb{Z}_q, \text{pk}=g^x, \text{sk}=x$

$\text{Enc}(\text{pk}, m): r \leftarrow \mathbb{Z}_q, \text{ct}=(c=mg^{xr}, c'=g^r)$

$\text{Dec}(\text{sk}, \text{ct}=(c, c')): m=cc'^{-x}$

单向性到CDH的规约

以大概率攻破单向性的敌手A

CDH的挑战者



# Elgamal加密基于CDH假设的单向性

从敌手的视角看，规约算法给出的公钥和密文与单向性的挑战者是一致的

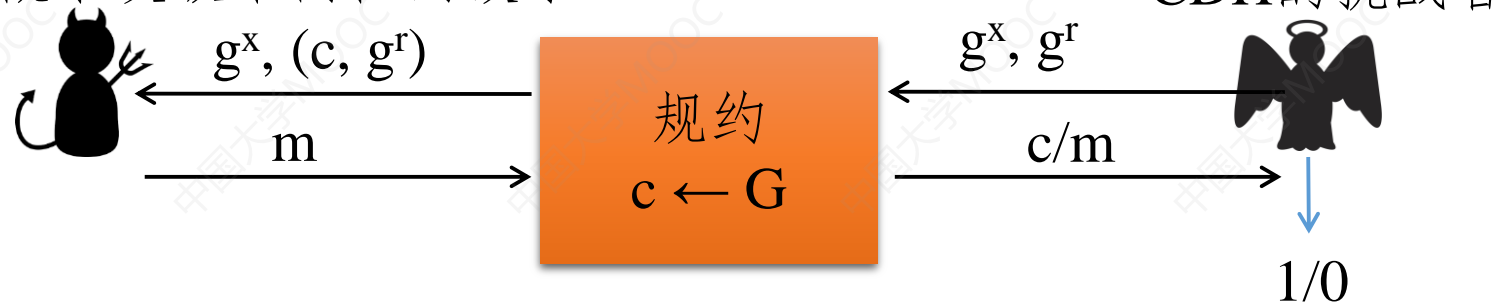
$\text{Gen}(1^k): x \leftarrow \mathbb{Z}_q, \text{pk}=g^x, \text{sk}=x$

$\text{Enc}(\text{pk}, m): r \leftarrow \mathbb{Z}_q, \text{ct}=(c=mg^{xr}, c'=g^r)$

$\text{Dec}(\text{sk}, \text{ct}=(c, c')): m=cc'^{-x}$

单向性到CDH的规约

以大概率攻破单向性的敌手A



# Elgama1加密基于CDH假设的单向性

从敌手的视角看，规约算法给出的公钥和密文与单向性的挑战者是一致的

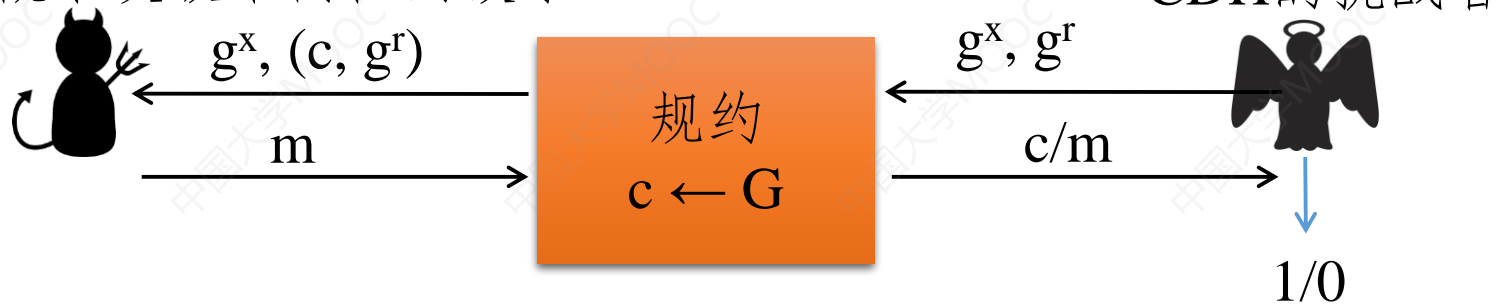
$$\text{Gen}(1^k): x \leftarrow \mathbb{Z}_q, \text{pk}=g^x, \text{sk}=x$$

$$\text{Enc}(\text{pk}, m): r \leftarrow \mathbb{Z}_q, \text{ct}=(c=mg^{xr}, c'=g^r)$$

$$\text{Dec}(\text{sk}, \text{ct}=(c, c')): m=cc'^{-x}$$

单向性到CDH的规约

以大概率攻破单向性的敌手A



$$\Pr[\text{规约算法解决CDH困难问题}] = \Pr[c/m = g^{rx}] = \Pr[c = mg^{rx}] = \Pr[\text{敌手A打破单向性}]$$

=====> 如果CDH假设成立，不存在敌手能打破Elgama1加密的单向性。





# 总结

---

- **CDH**安全性
  - **Elgamal**加密方案
  - 安全性证明: **CDH**安全性 $\rightarrow$ 加密方案安全性 (证明方法: 构造**规约**)
-



感谢聆听!

wangyuyu@uestc.edu.cn