现代密码学

可证明安全性与Elgamal加密方案简介

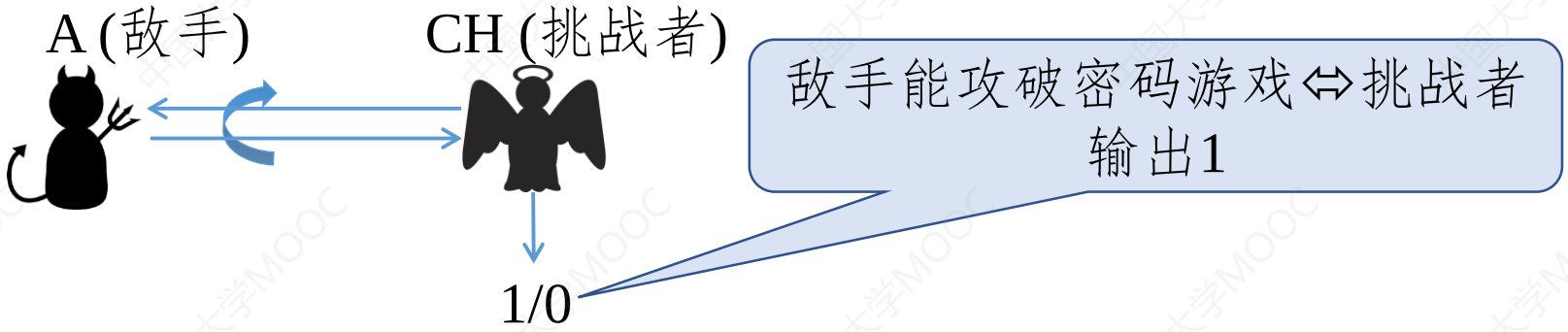
王煜宇
信息与软件工程学院
电子科技大学

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

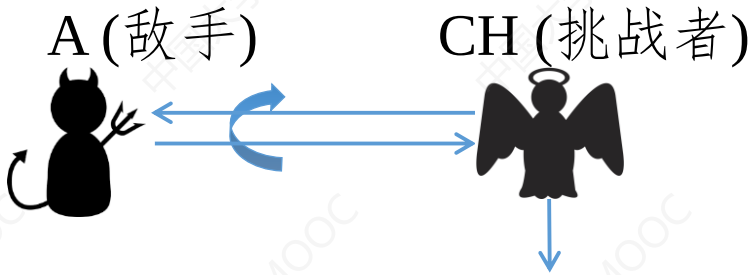
目录

密码游戏



Pr[CH 输出 1]=negl=>密码游戏是安全的

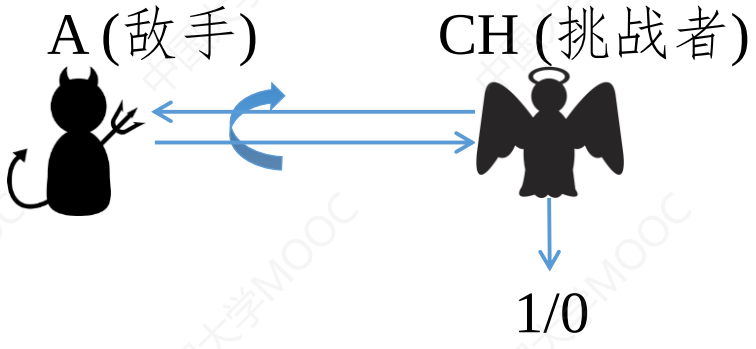
密码游戏



Pr[CH 输出 1]=negl=>密码游戏是安全的

可忽略的概率

密码游戏



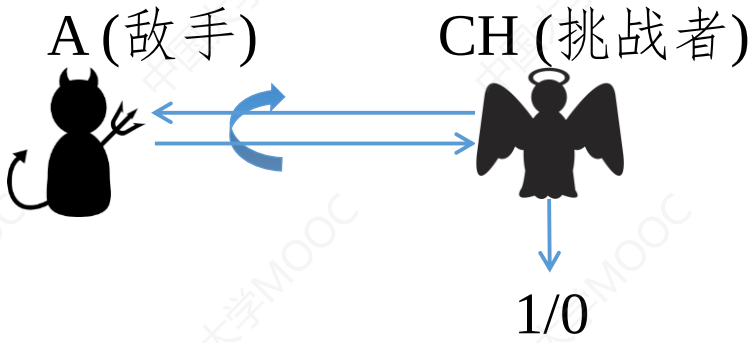
几乎所有的计算性的假设和安全性都能用密码游戏来表示

Pr[CH 输出 1]=negl=>密码游戏是安全的

规约

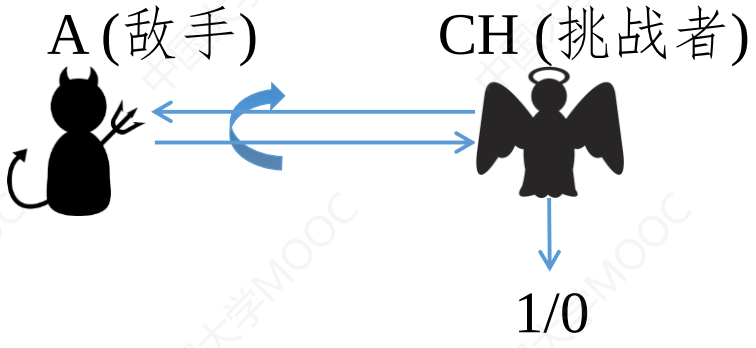
假设

G_1的可证明安全性：基于G_2证明G_1的安全性



Pr[CH 输出 1]=negl=>密码游戏是安全的

规约



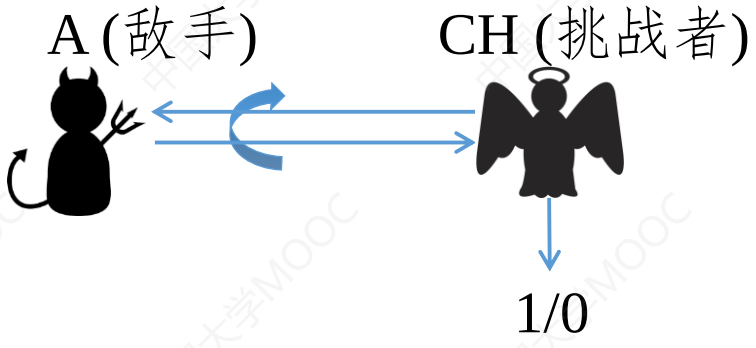
Pr[CH 输出 1]=negl=>密码游戏是安全的

假设

G_1的可证明安全性：基于G_2证明G_1的安全性

G_2安全====> G_1安全

规约



Pr[CH 输出 1]=negl=>密码游戏是安全的

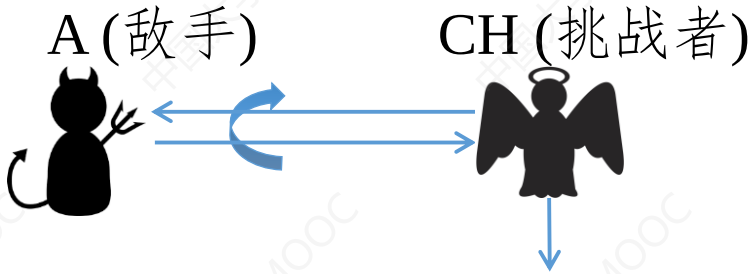
假设

G_1的可证明安全性：基于G_2证明G_1的安全性

G_2安全====> G_1安全

G_1不安全=====> G_2不安全

规约



Pr[CH 输出 1]=negl=>密码游戏是安全的

假设

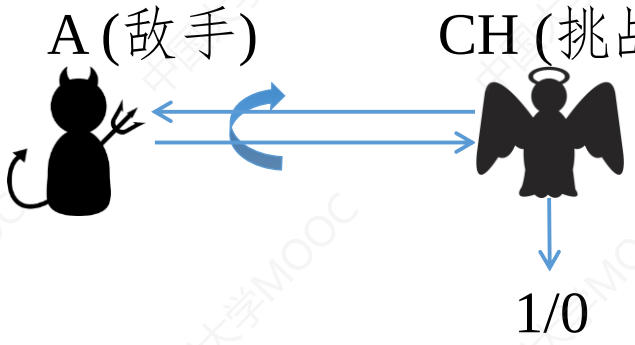
G_1的可证明安全性：基于G_2证明G_1的安全性

G_2安全====> G_1安全

G_1不安全====> G_2不安全

存在敌手攻破G_1====>存在敌手攻破 G_2

规约



Pr[CH 输出 1]=negl=>密码游戏是安全的

假设

G_1的可证明安全性：基于G_2证明G_1的安全性

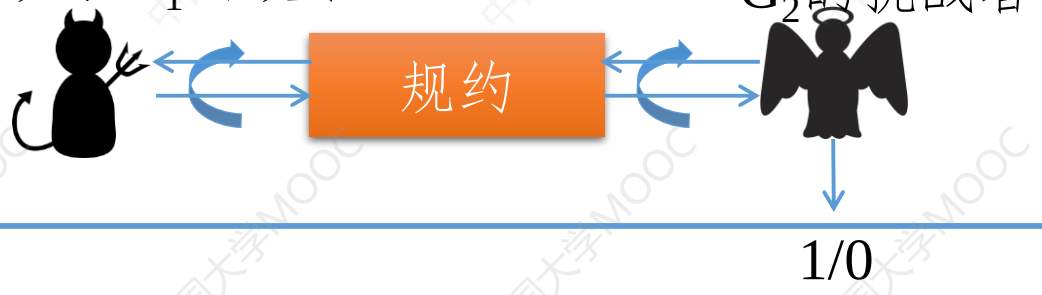
G_2安全====> G_1安全

G_1不安全====> G_2不安全

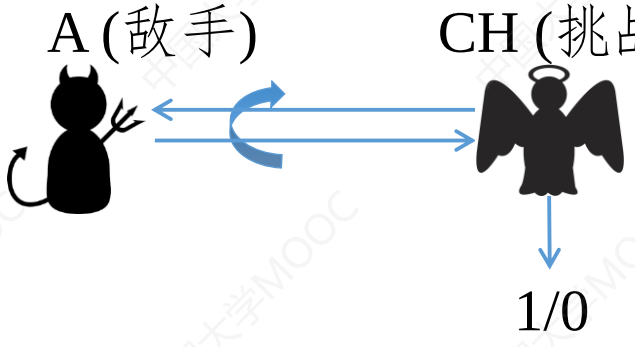
存在敌手攻破G_1====>存在敌手攻破 G_2

G_1到G_2的规约

攻破G_1的敌手



规约



Pr[CH 输出 1]=negl=>密码游戏是安全的

假设

G_1的可证明安全性：基于G_2证明G_1的安全性

G_2安全====> G_1安全

G_1不安全=====> G_2不安全

存在敌手攻破G_1====>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

CDH假设[DH76]

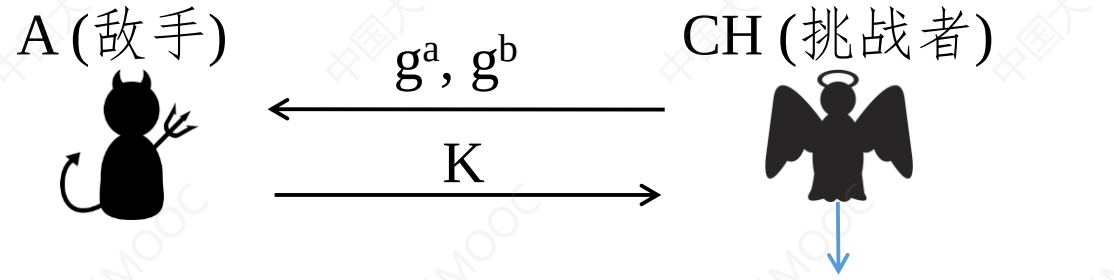
G: 阶为q的循环群
$\{g^1, g^2, \ldots, g^q\}$

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

CDH假设[DH76]

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

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



Pr[CH 输出 1]=negl==>CDH假设成立

目录

加密

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

$Enc(pk,m) \rightarrow ct$

$Dec(sk,ct) = m$

正确性：$Dec(sk,(Enc(pk,m)))=m$

加密

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

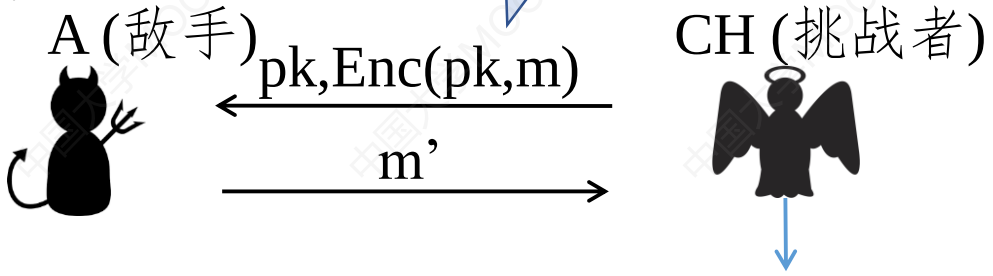
$Enc(pk,m) \rightarrow ct$

$Dec(sk,ct) = m$

正确性：$Dec(sk,(Enc(pk$ $=m$

随机生成的密文

单向性：



Pr[CH 输出 1]=negl=>加密方案满足单向性

目录

Elgamal加密方案[Elgamal84]

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

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

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

正确性：$cc'^{-x}=mg^{xr}g^{-rx}=m$

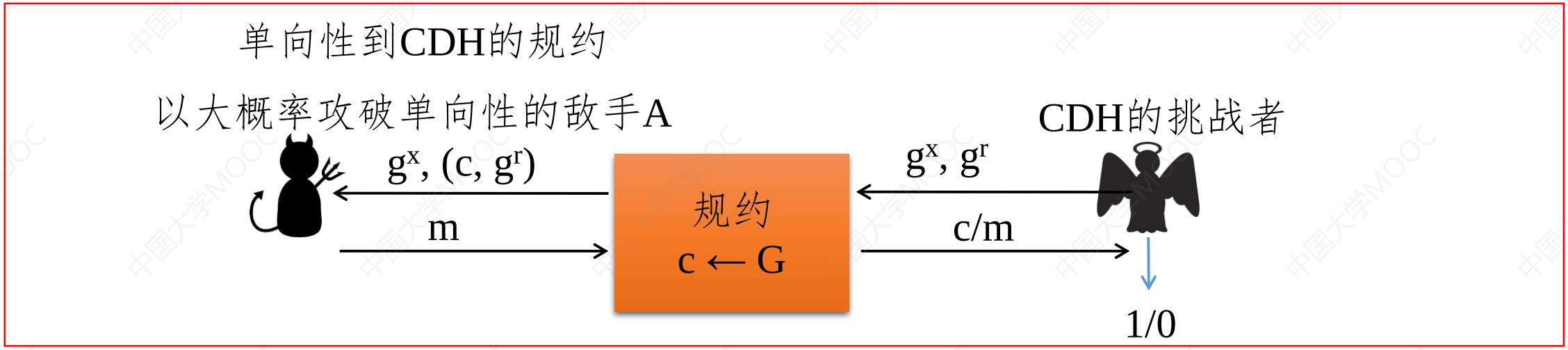
目录

Elgamal加密基于CDH假设的单向性

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

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

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



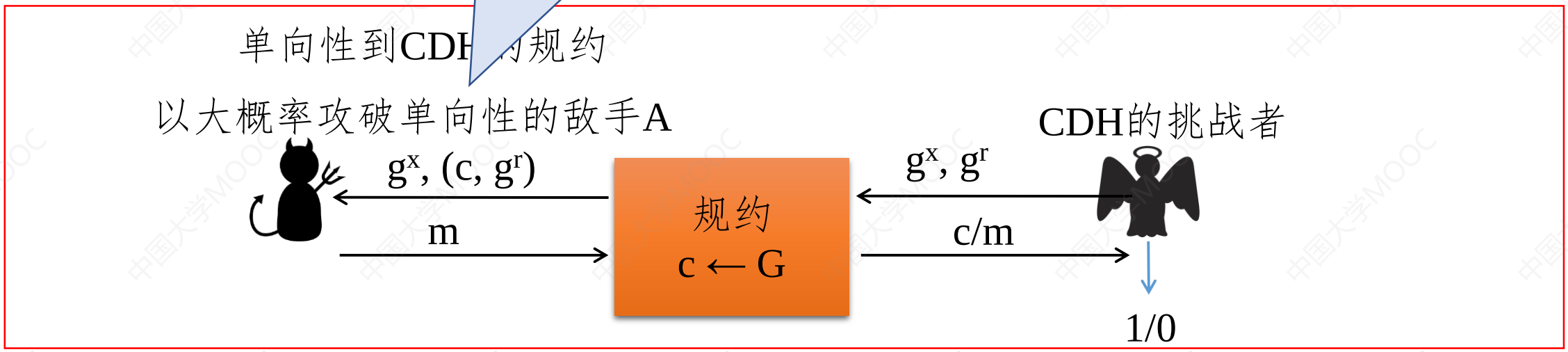
Elgamal加密基于CDH假设的单向性

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

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

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

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



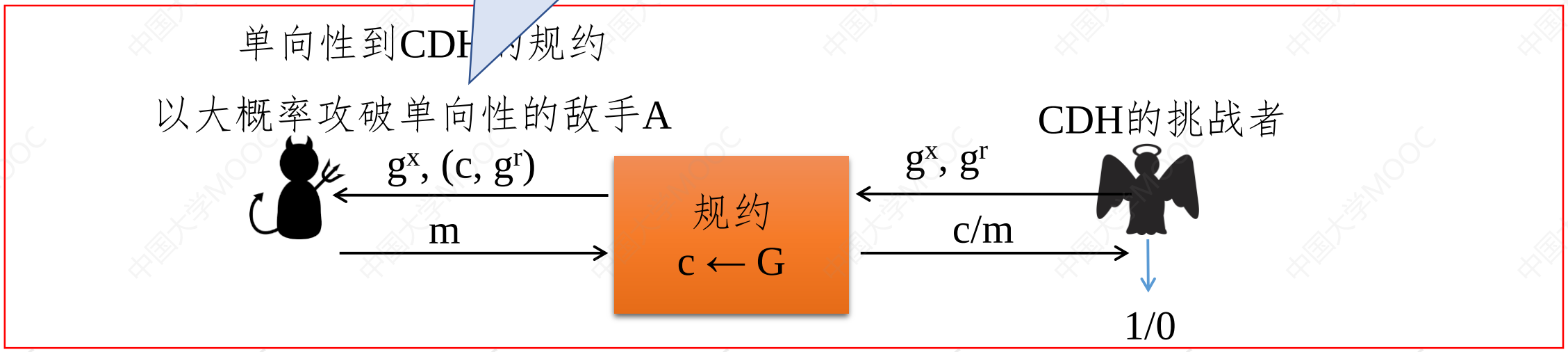
Elgamal加密基于CDH假设的单向性

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

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

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

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



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

=====> 如果CDH假设成立，不存在敌手能打破Elgamal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→加密方案安全性（证明方法：构造规约）

感 谢 聆 听!

wangyuyu@uestc.edu.cn