华南师範大學
SOUTH CHINA NORMAL UNIVERSITY

本科毕业论文

论文题目：公钥密码量子安全性的分析与证明
指导老师：王立斌 副教授
学生姓名：曾润智
学　　号：20142101028
学　　院：计算机学院
专　　业：网络工程
班　　级：7 班

摘要

设计可抗量子计算机攻击的公钥密码体制是密码学领域的研究热点。本文跟踪量子安全公钥密码学的最新进展，分析现有的量子安全模型、量子安全体制，从而为后续研究奠定基础。具体工作包括：对经典安全模型进行量子分析，指出其可被量子攻击者利用的漏洞；分析现有的量子安全模型，探讨其定义动机、直观、攻击者能力及其合理性；展示量子安全模型下可证明安全的体制实例，探讨安全模型对体制设计的要求及在模型下体制安全性证明的思路。

本文对公钥密码体制的量子安全性进行形式化分析，指出设计新型量子安全模型必须遵循的若干的原则；分析两种量子安全公钥密码体制的设计与证明，为量子安全公钥密码体制的设计指出可借鉴的思路。

关键词　：公钥密码学，量子安全，安全模型，可证明安全性，随机预言机模型

ABSTRACT

Public key cryptosystem that can resist quantum attacks is a research hotspot in the field of public key cryptography. This paper tracks the advances in quantum security public-key cryptography and analyzes the existing quantum security models and quantum secure cryptosystems, which can lay the foundation for subsequent research. Concretely, we show the quantum analysis of the classical security models and argue that there are some flaws in classical model which can be exploited by the quantum attackers; the existing quantum security models are analyzed and the definition motivation、 security intuition、 the ability of attackers and its reasonableness of these quantum models are discussed; we also show two schemes that are secure under the quantum security model, among the proof we discuss how to design quantum secure scheme and how to prove its security under quantum security model.

This work presents a formal analysis of the quantum security of public-key cryptosystems, points out several principles that must be followed to design a new quantum security model, and analyzes the design and security proof of two quantum-secure public-key cryptosystems. Among these studies we point out the ideas to design quantum-secure public-key cryptosystems.

Keywords: public key cryptography, quantum security, security model, provable security, random oracle model

目录

1. 绪论

公钥密码体制的安全性基于某些公认难题的难解性，比如 RSA 公钥加密体制的安全性可规约为大整数分解的难解性。量子计算机的出现与进展威胁着现有公钥密码体制的安全性[1-2],并对公钥密码体制的设计提出新要求：设计可抗量子攻击的公钥密码体制。量子安全公钥密码学逐步受到业界重视，**设计量子安全的公钥密码体制是公钥密码学领域一大研究热点**。

本文将针对量子安全公钥密码学展开研究，重点关注公钥加密体制与数字签名体制的量子安全性，对公钥加密体制与数字签名体制的量子安全模型进行探讨，并对模型下可证明安全的体制进行深入的分析。

1.1 国内外研究现状与分析

以下从三个个方面论述量子安全公钥密码学的研究进展。

1. 量子叠加态攻击与量子安全模型.

在对密码体制进行安全性证明前，需要确定体制要达到的安全目标并选取合适的安全模型。选定安全模型后，在模型下将体制的安全性规约为难题的难解性即完成体制安全性的证明。安全模型严格刻画了攻击者的计算能力与信息交互方式，模型的强度与合理性很大程度上决定了证明的复杂性与体制的安全性。经典安全模型是一类针对经典攻击者攻击能力而定义出的安全模型，比如公钥加密体制的 IND-CCA 模型[3]。“经典”一词对应“量子”，经典攻击者即仅有传统计算能力而没有量子计算能力的攻击者。

在刻画“抗量子攻击”这一安全概念时，**后量子安全**沿用了经典安全模型。**后量子安全即在经典安全模型下，将体制的安全性规约为量子难题难解性**。其中量子难题指公认不存在高效量子算法的问题。现已有相当一部分后量子安全公钥体制，比如基于格难题的密钥封装体制[4]，数字签名体制[5]。

然而，后量子安全无法完全刻画“可抗量子攻击”这一安全概念，因为经典安全模型并不能很好地刻画量子攻击者的攻击能力。**达到后量子安全的体制不必然在现实运行中可抗量子攻击。**Boneh 等人[6]给出了一种在随机预言机模型下达到后量子安全的身份验证协议，该身份验证协议在现实运行中将无法抵抗**量子叠加态攻击**。量子攻击者对体制中的随机预言机进行叠加态问询，从而破解了该身份验证协议。该工作尝试通过提出量子随机预言机模型来刻画攻击者的量子叠加态攻击能力，这开启了量子安全密码体制的研究先河。

其它对体制的量子叠加态分析可见诸文献[7-9]，这些工作都允许攻击者对密码体制的某些预言机进行叠加态问询并指出这种叠加态问询的合理性。因此有必要定义新的安全

模型以进一步描绘量子攻击者的攻击能力，即设计**量子安全模型**。如果一个体制在量子安全模型下其安全性可规约为可抗量子攻击难题的难解性，则称该体制是**量子安全**的。

量子安全模型既考虑攻击者本身的量子计算能力，**也考虑攻击者的量子叠加态攻击能力**[10]。在量子安全模型中，攻击者具有**量子问询能力**，即攻击者可对某些算法进行量子叠加态的问询。现已有部分公钥密码体制的量子安全模型，如公钥加密体制的量子安全模型、数字签名的量子安全模型[7]。然而，其它重要公钥密码构件的量子安全模型还未被提出，比如基于身份的加密体制、密钥封装机制与认证密钥交换。本文的研究主要对量子安全公钥密码体制设计与证明展开研究。

2. 量子安全体制设计与证明

量子安全体制的设计较经典安全体制有更大的复杂性。在量子安全模型下，量子攻击者可对体制中的部分算法作预言机问询，因此在证明体制的量子安全性时，**需要考虑如何高效应答量子攻击者对预言机的问询**，即要考虑如何高效模拟量子预言机。可以借助量子相关的技巧及引理来高效模拟预言机：Zhandry 证明了用 k-wise 独立函数可以模拟随机预言机[11]，这方便了在量子随机预言机模型下使用随机预言机的可编程特性[12]；Zhandry 还提出半常数分布[11]、小域分布[13]等，这些分布给出了相应高效模拟预言机的方法；Unruh 等人提出的 O2H 引理[14]、O2HA[15]技巧及引理给出了对应的抽取量子攻击者信息的方式。

现已有部分量子安全的公钥密码体制被提出，如数字签名体制[7]，公钥加密体制[12]等。然而目前量子安全公钥体制效率不高，且证明相对复杂，尚无法达到现实工程中的效率要求。因此设计高效简洁的量子安全公钥密码体制仍然是一个开放性问题。

3. 国内研究现状

目前可抗量子攻击公钥密码的研究已在国内受到重视并取得一定成果，如公钥加密体制[16]、数字签名体制[17]、密钥交换协议[18]、认证密钥交换协议[19]等。这些体制具有较高的效率，并且其中部分体制还参与到 NIST 的后量子安全密码体制标准的竞争中[20]。值得注意的是，这些体制的后量子安全性已被分析证明，而其量子安全性还未被考虑，因此需要进一步探讨这些体制的量子安全性。

1.2 本文的工作与结构安排

1.2.1 主要工作与意义

本文对量子安全公钥密码学领域的部分研究内容进行若干分析与探讨，主要内容包括：

1. 展示对公钥体制的量子叠加态攻击，指出经典安全模型的局限性，同时论证量子安全概念强于后量子安全；对量子叠加态攻击的合理性进行了一定的讨论。
2. 对现有量子安全模型进行分析探讨，分析这些安全模型与经典安全模型的异同并讨论其中所刻画的安全概念，然后指出在量子安全模型下证明安全性时会遇到的困难并探讨解决方案；对量子安全模型的合理性与量子安全概念的必要性进行了相应的探讨。
3. 展示两种量子安全的公钥密码体制并给出相应的证明，论证在证明中指出经典安全性证明技巧为何失效，探讨如何解决并展示如何使用相关量子技巧与引理来完成安全性证明；探讨量子安全公钥体制相比后量子安全公钥体制的不足，尝试给出解决方案。

本文工作有如下几点意义：

1. 对现有的公钥密码体制量子安全进行形式化分析，为未来设计更多的公钥密码体制量子安全模型奠定基础，比如设计认证密钥交换的量子安全模型。
2. 详细研究了两种量子安全公钥密码体制的安全性证明，指出量子安全性证明可借鉴的思路，便于未来设计更多的量子安全公钥密码体制。
3. 指出现有量子安全公钥密码体制的不足，并尝试给出解决部分不足的方案，为未来设计更实用的量子安全公钥体制提供方向。

1.2.2 结构安排

本文分为七个章节，具体内容如下：

第一章给出相关研究背景、研究现状与本文研究内容与意义。

第二章给出了在本文中必要的数学背景、密码学背景与量子计算知识。

第三章展示了针对密码学协议的量子叠加态攻击，探讨这些在经典模型在面对量子攻击者时可能存在的漏洞，指出经典安全模型无法完全刻画量子攻击者的能力。

第四章分析几个常用公钥密码构件的量子安全模型，指出这些模型与经典模型的异同、刻画的安全概念与证明时会遇到的困难及解决思路。

第五章和第六章分别展示一种量子安全数字签名体制和一种公钥密码体制，同时给出这两种体制的安全性证明，在证明中探讨证明体制量子安全性的方法。

第七章对本文进行总结，并提出今后工作方向。

2. 背景知识与符号表达

为确保本文的可阅读性与完备性，以下介绍一些常用的数学符号与定义，并给出相关的密码学背景知识。

2.1 数学符号与定义

记S是一个集合，$|S|$表示S中元素的个数。设D是在S上的分布，$x \leftarrow D$表示根据分布D从S抽样x。对于有限集合S，$x \leftarrow_R S$表示从S中随机均匀地抽样一个元素x（在意义明确时，箭头下的R将被忽略）。

设$n \in N$(自然数集合),$\{0,1\}^n$表示长度为n的比特串集合，$n = 0$时表示空串。$\{0,1\}^*$表达所有长度的比特串，即$\{0,1\}^* = \bigcup_{i=0}^{\infty}\{0,1\}^i$.

令k为一个自然数，1^k表示 k 个 1 的串。密码体制需要指定参数，用于确定体制所要达到的比特安全性，而安全参数常表达为如1^k的形式（而非k）。

设S为一个比特串，S_l为S的前l位比特串。

事件与概率.记 A、B、C 是三个事件（都包含于某个样本空间内），$Pr\{A\}(\leq 1)$代表事件 A 发生的概率。$Pr\{A|B\}$代表在事件 B 发生的条件下事件 A 发生的概率。设 Y 是随机变量，$E[Y]$表示 Y 的期望。

k-wise 独立函数簇. 令$F: X \to Y$为一个函数簇，其中Y是有限集。若对于任意$l(\leq k)$个互不相同的$x_i \in X$与l个$y_i \in Y(i = 1, \dots, l)$，有:

$$\Pr_{f \leftarrow F}\{f(x_1) = y_1 \cap \dots \cap f(x_l) = y_l\} = \frac{1}{|Y|^l}$$

则称F是一个 k-wise 独立函数簇，从F中均匀抽取的函数f称为 k-wise 独立函数。

统计距离. 设D_1, D_2为同一集合Y的分布，记$|D_1 - D_2| = \sum_{y \in Y}|D_1(y) - D_2(y)|$为$D_1$与$D_2$的统计距离。其中，$D_1(y) = Pr\{y \leftarrow D_1\}$。

渐近界. 设$f(x)$、$g(x)$是两个函数。$f(x) = O(g(x))$表示，存在常数X和正常数M，对于任意的$x > X$，恒有$|f(x)| > M \cdot |g(x)|$(此时||是绝对值符号)。$f(x) = \Omega(g(x))$表示$g(x) = O(f(x))$。$f(x) = \Theta(g(x))$表示$f(x) = O(g(x))$且$f(x) = \Omega(g(x))$。

可忽略量（negligible，简称 negl）. 令$\varepsilon(n)$是一个函数，若ε(n)非负且对于任意多项式$poly(n)$，存在自然数N使得对于任意的$n \geq N$，有$\varepsilon(n) < \frac{1}{poly(n)}$，则称$\varepsilon(n)$是一个可忽略

量。$negl(n)$指某一个关于n的可忽略量。若$\varepsilon(n)$不是可忽略量，则称$\varepsilon(n)$为**不可忽略量**。

几乎接近(negligibly-close). 记A, B为两个事件，若对于任意足够大的参数n，有$|Pr\{A\} - Pr\{B\}| \leq negl(n)$，则称A 和 B是**几乎接近**的。

概率算法与确定性算法. 记 A 为概率算法，其执行可表达为$output \leftarrow A(input)$。若 A 是确定性算法，则其执行表达为$output := A(input)$。通过将运行中选取的随机性显式表达出来，概率算法可表示为确定性算法。 设r为$output \leftarrow A(input)$中选取的随机性，则该过程可表达为$output := A(input; r)$。

概率多项式时间(PPT)算法.若 A 是经典随机算法并且对于其输入的长度n，其运行时间是关于n的多项式，则称 A 为概率多项式时间算法，简称 A 为 PPT 算法。对密码体制的攻击者可看做是攻击密码体制的算法，PPT 攻击者定义与 PPT 算法类似。

预言机(Oracle). 预言机是一种理想化的黑盒算法，问询者向预言机发出问询，预言机返回相对的应答。问询者除了能获得预言机的输出之外，没有任何关于预言机内部的信息。在文献[21]中可获得预言机更具体的预言机定义。

预言机算法. 设算法 A 可访问预言机 O，则称 A 是预言机算法，记为A^O。

2.2 密码学背景

本节给出若干密码学相关背景，重点给出可证明安全、安全模型、随机预言机模型等概念，以方便下文的讨论，更多详细的内容请参考文献[3]。

2.2.1 安全模型

本文将用安全游戏来描述安全模型，并且通过安全游戏的形式对公钥密码体制进行形式化的安全证明。具体地，设$model$是安全模型，A 算法在$model$下攻击密码体制Π，则安全游戏$G_{A,\Pi}^{model}$对该过程进行描述。安全游戏结束前会返回一个比特，返回 1 代表攻击者 A 在安全模型$model$下达到了攻击目标，否则代表攻击者攻击失败。

举例来说，假设有一个攻击者 A，该攻击者可以在安全模型$model$下攻破 RSA 公钥加密协议，那么借助 A 可以构造算法S（称为模拟者，或抽取者），该算法模拟攻击游戏的环境$G_{A,RSA}^{model}$并与环境中的 A 进行信息交互。模拟者最后从与 A 的交互中提取必要的信息，进而解开大整数分解问题。若S能“完美地”模拟$G_{A,RSA}^{model}$，并且该模拟是高效的，那么S即是

对大整数分解的高效算法。由于假设了大整数分解不存在（经典）高效算法，从而反推得，A 是不存在的，从而证明 RSA 加密体制在安全模型$model$下不存在高效攻击者。

2.2.2 公钥密码体制及其安全性

本文给出公钥加密体制与数字签名体制相关的概念与安全模型。公钥加密体制和数字签名体制的定义在附录 A 中给出，更具体的内容可参考文献[3]，以下仅给出相关的安全概念。

选择密文攻击下不可区分性（简称 IND-CCA）是一种衡量公钥加密体制安全性的安全概念，其安全模型描述如图 2.2。

在 IND-CCA 模型中，在攻击者不仅具有公钥pk，还可对**解密预言机**进行问询。解密预言机是一个黑盒子算法，具有解密功能，但攻击者没有关于该算法的内部构造的任何信息。攻击者可通过加密算法或是自己构造得到相应的密文，然后向解密预言机问询该密文，解密预言机会返回密文对应的明文或拒绝解密。

若体制Π满足: 对于任意足够大的n,对于任意的 PPT 攻击者，$Pr\{G_{A,\Pi}^{IND-CCA}(1^n)=1\}$是个关于n的可忽略量，则称Π满足选择密文攻击下不可区分性，也亦即Π是抗选择密文攻击(简称 IND-CCA)的。

$G_{A,\Pi}^{IND-CCA}(1^n)$描述

其中$\Pi=(\mathrm{K},\mathrm{E},\mathrm{D})$

1. 密钥生成阶段

   $(pk,sk)\leftarrow K(1^n)$，发送pk,n给$A^{D(sk,\cdot)}$，A可问询解密预言机$D(sk,\cdot)$: A发送c给模拟者，模拟者返回$D(sk,c)$。

2. 挑战阶段:

   $(m_0,m_1)\leftarrow A^{D(sk,\cdot)}(1^n,pk)$

   $b\leftarrow_R\{0,1\},c^*\leftarrow E(pk,m_b)$

   发送c^*给$A^{D(sk,\cdot)}$, A不允许向解密预言机问询c^*

3. 测试阶段:

$b'\leftarrow A^{D(sk,\cdot)}(1^n,pk,c^*)$

若$b=b'$，返回 1, ；否则返回 0.

图 2.2 $G_{A,\Pi}^{IND-CCA}(1^n)$描述

选择报文攻击下的存在性不可伪造(简称 EUF-CMA)是衡量数字签名的安全性的一种安全概念。图 2.3 给出$G_{A,S}^{EUF-CMA}$的描述。

在$G_{A,S}^{EUF-CMA}$中，攻击者可根据需要获得某报文对应的签名。由于是 PPT 攻击者，攻击者只能获得多项式多的报文-签名对。记集合Q包含攻击者所有问询得到的报文签名对，攻

击者目标为伪造一个报文-签名对，并且该报文签名对不在Q中。

$$G_{A,S}^{EUF-CMA}$$

$$S=(K,Sign,Ver)$$

1. $(pk,sk)\leftarrow K(1^n)$, 初始化列表$Q=\emptyset$，运行攻击者$A^{Sign(sk,\cdot)}(1^n,\mathrm{pk})$。
2. 每当A发出签名问询明文m, 计算$\sigma\leftarrow Sign(sk,m)$，返回$(m,\sigma)$给$A$并且$Q=Q\cup\{(m,\sigma)\}$。
3. A输出(m^*,σ^*), 若$Ver(pk,m^*,\sigma^*)=1$并且$(m^*,\sigma^*)\notin Q$，则返回 1，否则返回 0.

图 2.3 $G_{A,S}^{EUF-CMA}$描述

若数字签名体制S满足: 对于任意足够大的n,对于任意的 PPT 攻击者，$Pr\{G_{A,S}^{EUF-CMA}(1^n)=1\}$是个关于n的可忽略量，则称S满足选择报文攻击下的存在性不可伪造。

哈希函数是公钥密码体制中的重要构件，以下介绍相关的概念。

抗碰撞哈希函数. 设H是一个哈希函数，若有$(x,x'),x\neq x'$使得$H(x)=H(x')$，则称(x,x')是哈希函数 H 的一个碰撞。若对于任意的 PPT 攻击者 A，A 找到哈希函数H的一个碰撞的概率是可忽略的，则称H是抗碰撞的。

对于带键值的哈希函数$H(k,\cdot)$，不同的键值k定义了不同的哈希函数，这意味着不同的键有相应不同的碰撞。

2.2.3 随机预言机模型

随机预言机模型(ROM)[22]是一种常用的密码体制安全证明**技巧**。该模型将体制内的一个或多个哈希函数模型化为一个随机预言机(简称为 RO)，该预言机的输出分布是真随机的。攻击者想对哈希函数进行求值(即选取某个输入x求$H(x)$)，必须要向 RO 问询，即，发送问询输入x给 RO，RO 返回$H(x)$。

模拟者维护一张问询表H，该表记录攻击者问询过的所有输入及其输出。对于一个问询输入x_1，若表中有其对应的输出y_1，则直接返回y_1；否则$y_1\leftarrow_R R$，记录(x_1,y_1)在表H中，然后返回y_1作为$H(x_1)$。

在随机预言机模型中，**模拟者可以得到攻击者对随机预言机发起的所有问询记录，并且模拟者可以选定预言机的输出值（称为可编程特性）**。

随机预言机模型是一种安全证明技巧而非某种特定密码体制的安全模型，任何的密码体制都可以使用随机预言机模型进行安全性证明。关于随机预言机模型的合理性与弊端，本文不做讨论。

2.3 量子计算

本节简要地介绍在本文中必要的量子计算知识与相关符号。要获得更详细的内容可参考文献[23]，详细的线性代数内容可参考文献[24].

记A是一个量子系统， A的状态由一个状态向量$|\varphi_A\rangle \in H_A$所描述，其中$H_A$为一个有限维的希尔伯特空间，$|\varphi_A\rangle$满足$\||\varphi_A\rangle\| = \sqrt{\langle\varphi_A|\varphi_A\rangle} = 1$。

$|\ \rangle$也被称为**寄存器**。寄存器$|\ \rangle$中“存储”着经典信息，比如$|111\rangle$中含有经典信息111。经典信息一般是比特串，用比特串表达的好处在于，经典信息可通过编码转化成比特串，然后表达在量子态中。

量子叠加态常常表达为$\sum_{x,b}\alpha_{x,b}|x\rangle|b\rangle$，叠加态中的$|x\rangle,|b\rangle$可以有多个取值，比如$\sum_{i\in\{0,1\}^n}\alpha_i|i\rangle|0\rangle$，其中的$|i\rangle$就有$2^n$种取值。

测量(Measurements) 量子态可以被测量，测量过程可视为概率抽样，例如对量子态$\sum_{i\in\{0,1\}^n}\alpha_i|i\rangle|0\rangle$测量后可以$|\alpha_i|^2$得到经典信息$i$。量子态被测量后其状态会改变。**只有测量才能从量子态中提取信息。**

量子算法. 量子算法一一对应于一个酉操作子U。对U输入量子态|b⟩，其算法过程可记为: $|b\rangle \to U|b\rangle$。任何经典算法都可实现成量子算法[23]，设f是一个经典算法或预言机，将其定义域与值域进行相对应的编码后，可构造其对应的量子算法（酉矩阵）U_f:

$$U_f: |x\rangle|b\rangle \mapsto |x\rangle|b \oplus f(x)\rangle$$

其中第一个寄存器被称为**输入量子位**，第二寄存器被称为**工作量子位**，一般b可设为0 从而将f(x)的信息直接储存到寄存器中。 f可以是算法也可以是预言机。对于经典概率算法，将随机性显式写出（增加多一个**随机性量子位**）即可构造类似的U_f。若对U_f输入一个**量子叠加态**$\sum_{m,b}|m\rangle|b\rangle$，由线性性，$U_f$输出$\sum_{m,b}|m\rangle|b \oplus f(m)\rangle$。

对于量子攻击者 A 与一个预言机O，若 A 可对O进行**量子叠加态问询**（即 A 可对U_O进行叠加态问询），则可记为$A^{|O\rangle}$。

3. 量子叠加态攻击

为引出量子安全概念与量子安全模型并讨论其合理性与必要性，本章展示两种对密码学体制的量子叠加态攻击实例[6,7]并作出分析与探讨。具体地：3.1 节首先给出一个在 CROM 下可证明安全的身份认证协议，然后论证该协议在实际运行中并不能抵抗量子攻击者，从而指出 CROM 在面对量子攻击者时遇到的刻画能力不足的问题。3.2 节给出了一个经典模型下可证明安全的数字签名体制，然后展示对该签名体制的叠加态攻击，论证具有叠加态问询能力的量子攻击者比没有该问询能力的攻击者更强。3.3 节讨论这些叠加态攻击的合理性与考虑密码体制量子安全的必要性。

3.1 对身份认证协议的叠加态攻击

对身份认证协议的叠加态攻击包括以下步骤：首先通过一个后量子安全的身份认证协议 ID 构造一个在 CROM 下可证明安全的身份认证协议ID*。进而分析出，在此模型下，即使面对量子攻击者，该协议仍然是安全的。必须强调，此时量子攻击者只能对 RO 进行经典的问询。然后，将该协议中的 RO 实例化为抗碰撞哈希函数，并且描述量子攻击者攻破该协议实例的具体过程，从而论证 CROM 不足以刻画量子攻击者的能力，说明定义 QROM 的必要性。

3.1.1 节给出身份认证协议的描述及其安全性概念，另外还给出了l-近似碰撞哈希函数的概念。l-近似碰撞哈希函数是ID*的构造核心，在ID*加入该哈希函数是为了使得该协议有安全漏洞，该安全漏洞在 CROM 下无法被攻击者（即使是量子攻击者）利用，但在实际运行中量子攻击者可通过对哈希函数的量子叠加态求值来利用该漏洞完全攻破该协议。ID*的具体构造与分析分别在 3.1.2 节与 3.1.3 节。

3.1.1 身份认证协议与l−近似碰撞哈希函数

身份认证协议ID包含三个高效算法$(IS.KGen, P, V)$。其中,IS.KGen()是概率算法：给定输入1^n (n 是安全参数)，返回钥匙对(sk,pk)。算法 P 和 V 的运行定义了在该身份认证协议中，证明方(Prover,运行算法 P，拥有 sk 和 pk)与验证方(Verifier,运行算法 V，拥有 pk）的协议交互。证明方需要向验证方验证身份，具体地，证明方运行算法 P(pk,sk)，并将其输出发给验证方；验证方收到信息后，运行算法 V(pk)，输出一个比特 b，b 等于 1 代表验证方确认证明方的身份，否则代表验证方拒绝证明方的身份验证。

一般要求身份认证协议满足**完备性**和**可靠性**。粗略地讲，完备性是指当验证方与诚实证明方（拥有 pk 对应的 sk）进行交互时，验证方最后会以极大的概率输出比特 1，即接受身份认证。攻击身份认证协议时，攻击者首先在诚实方与验证方的交互中获取信息，

然后假冒证明方的角色，尝试使验证方接受其身份验证，即尝试使验证方相信自己就是 pk 和 sk 的拥有者。可靠性指攻击者以可忽略概率使验证方接受。

给定哈希函数$H = (H.KGen, H.Eval)$（假设H的输出定长是n），其中：

- $H.KGen$为 PPT 算法，输入为安全参数1^n，输出为生成哈希函数的键值，运行过程记为$k \leftarrow H.KGen(1^n)$。
- $H.Eval$为确定性算法，输入为键值k与报文m，输出为报文m对应键值k的哈希值h，运行过程记为：$h := H.Eval(k, m)$。

对于任意的键值k，若存在两个报文$M \neq M', H.Eval(k, M)_l = H.Eval(k, M')_l$，即两个哈希值前l位相同，则称$(M, M')$是一对l-近似碰撞(l-near-collision-resistant)。如果对于任意 PPT 攻击者A:

$$\Pr_{k \leftarrow H.KGen(1^n)}\{(M, M')\text{是一对}l\text{-近似碰撞} \mid (M, M') \leftarrow A(1^n, k)\} \leq negl(n)$$

则称 H 是l-近似抗碰撞哈希函数。$l = n$则等价于称 H 是抗碰撞的。

3.1.2 CROM 下可证明安全的身份认证协议ID*

身份认证协议ID*的构造依赖一种后量子安全身份认证协议 ID，图 3.1 描述ID*的执行过程。ID*分为两部分，第一部分为碰撞阶段，第二部分为身份认证阶段。协议假定：证明方P*和验证方V*分别用有公共参数pk,$l \leq \log n$, n是安全参数。私钥 sk 为P*私有。

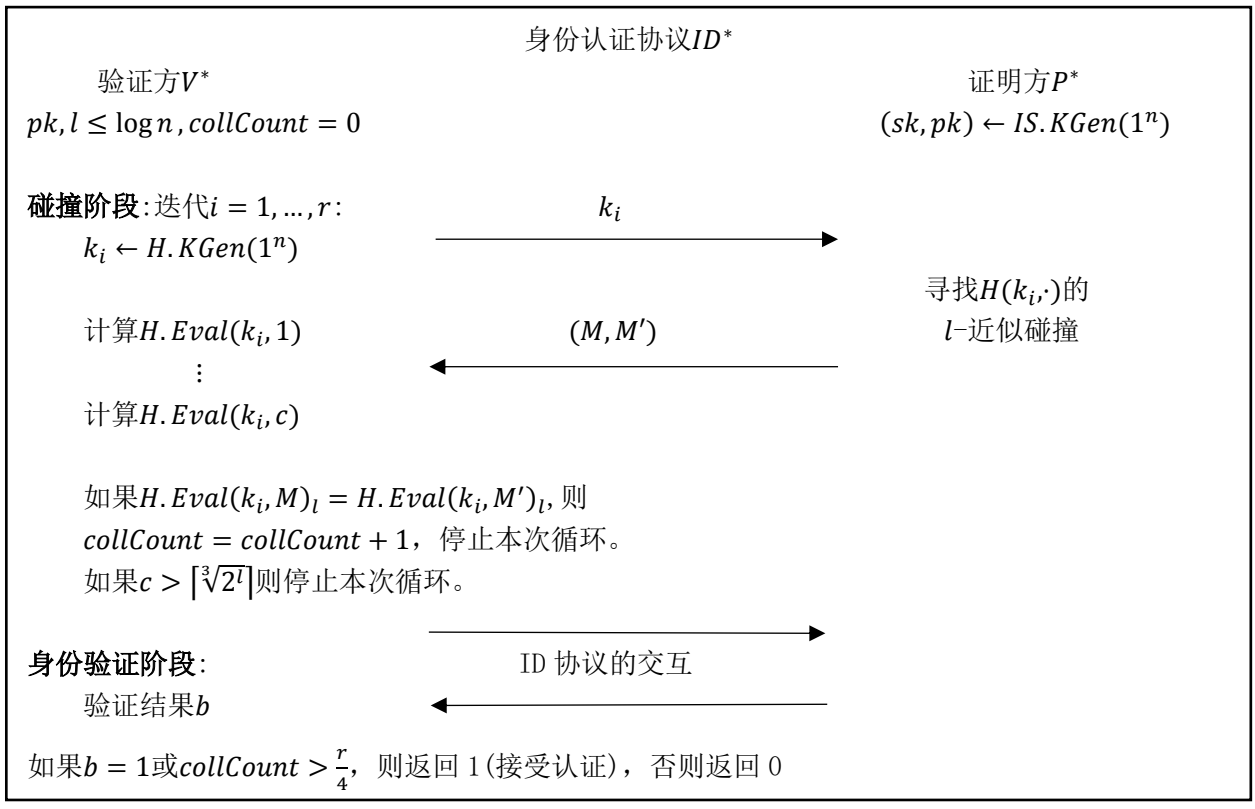

图 3.1 ID^*协议流程图

在碰撞阶段中，V*会执行r（r为关于n的某个多项式:$r = poly(n)$）次循环，同时V*在本地拥有一个内部计数器 collCount。在第i次循环中，V*会先通过 H.KGen 算法抽取一个键值k_i并发给P*，然后V*开始持续进行$c \le \lceil \sqrt[3]{2^l} \rceil$次哈希函数求值。同时，P*根据键值$k_i$开始寻找l-近似碰撞，若找到，则将该碰撞报文对$(M, M')$发给V*。若V*收到$(M, M')$并发现该报文对是l-近似碰撞，则停止此次循环并且对计数值 collCount 加 1，进入$i+1$次循环。若P*没有找到l-近似碰撞，则V*在对哈希函数求值够特定次数后,也进入$i+1$次循环。每一次循环中，V*会对哈希函数求值$\lceil \sqrt[3]{2^l} \rceil$次。

在身份认证阶段，V*和P*执行一次身份认证协议 ID，在此阶段V*会得出一个比特b, b由ID中的算法V运行得出。如果$collCount > \frac{r}{4}$（即P*至少找到$\frac{r}{4}$个l-近似碰撞）**或者** $b = 1$ (即V*在 ID 协议运行中接受了P*的身份验证)，则V*接受P*的身份验证（即输出 1）。

为了简化ID*的分析，给出以下不失一般性的假设。

假设 3.1：假设双方通信信息的时间可忽略不计，且P*求值一次哈希函数所需时间和V*求值一次哈希函数所需时间相同。假设除哈希函数求值以外的操作时间可忽略不计。

在ID*的碰撞阶段中，V*在每一次循环先抽取一个哈希键然后在本地求值$\lceil \sqrt[3]{2^l} \rceil$次哈希函数，由时间假设，攻击者在每一次循环的执行中对哈希函数的求值至多是$\lceil \sqrt[3]{2^l} \rceil$。在 ROM 中，H 将被当做一个随机预言机，每一次循环各自（独立）选择一次k_i可以理解为是每一次循环将重新构造一个随机预言机。**由假设 3.1，在一次循环里攻击者对预言机的问询至多为$\lceil \sqrt[3]{2^l} \rceil$次。**

3.1.3 对ID*的分析

在攻击ID^*时，攻击者欺骗验证方V*接受其身份认证的方法有两种：第一种即是上述所描述的，找到足够的l-近似碰撞数($\frac{r}{4}$个)，另一种则是在执行 ID 协议时欺骗V^*。以下引理说明了，在 CROM 下，ID^*是安全的。

引理 3.1 在经典随机预言机模型下，对于任意的经典攻击者 A，如果 ID 满足完备性和可满足性，那么ID*满足完备性和可靠性。

为了简洁，该引理的详细证明在附录 B 中给出。概括地说，通过分析可得出攻击者在碰撞阶段将以可忽略的概率找到$\frac{r}{4}$个l-近似碰撞，再结合 ID 的可靠性，即攻击者以可忽略概率欺骗V^*，可得出该引理。经典攻击者在 CROM 模型下找到足够l-近似碰撞的概率由生日攻击界所界定。

如果再要求 ID 是后量子安全的，那么由引理 3.1，有推论 3.2。设攻击者具有量子能力，由于仍然是 CROM 下，攻击者在问询 H 时只能进行经典问询（无法叠加态问询），

亦即量子攻击者在每一次循环中仍然是只能进行$\lceil\sqrt[3]{2^l}\rceil$次经典问询，此时量子攻击者无法使用叠加态攻击能力，因此找出足够l-近似碰撞数的概率仍由生日攻击所界定[25]。

推论 3.2 在经典随机预言机模型下，对于任意的量子攻击者 A，如果 ID 满足完备性和可满足性，那么ID*满足完备性和可满足性。

在实例化该协议的哈希函数H时，可使用具有l-近似抗碰撞属性的哈希函数，比如SHA-3。在实例化后，攻击者可以在本地求值哈希函数而不需要问询。**然而由于时间假设，攻击者在碰撞阶段的每一次循环中只能对哈希函数求值$\lceil\sqrt[3]{2^l}\rceil$次**。由实例化哈希函数的l-近似抗碰撞属性，可分析得经典攻击者以可忽略概率在ID^*的碰撞阶段找到足够的l-碰撞。

然而ID^*在实际运行中并不能抗量子攻击。量子攻击者可在本地构造使用量子叠加态求值H的量子算法，并通过 Grover 搜索算法[26]，在每一次循环中，以显著的概率找到一个l-近似碰撞。概率分析显示，在碰撞阶段结束后攻击者将以显著的概率找到$\frac{r}{4}$个l-近似碰撞，因此有引理 3.3。以上分析中仍然假定量子攻击者只能对H进行$\lceil\sqrt[3]{2^l}\rceil$次叠加态求值。

引理 3.3 用任意的抗碰撞哈希函数实例化ID^*后，对于任意的经典攻击者，ID^*满足完备性和可靠性；对于量子攻击者，ID^*不满足可靠性。

引理 3.3 的详细证明将在附录给出。

本节给出了一个在经典模型下可抗量子攻击但在实际运行中被量子攻击者攻破的例子。经典安全模型在刻画量子攻击者能力时存在缺陷：模型没有考虑到攻击者对体制中某些算法进行叠加态求值的能力。为了刻画量子攻击者在实际运行中对哈希函数的量子叠加态求值能力，模型应允许量子攻击者对随机语言预言机进行量子叠加态问询。

3.2 对数字签名体制的叠加态攻击

本节展示对数字签名体制的叠加态攻击。具体地，给出一个数字签名体制$S^* = (K, Sign, Ver)$，该体制在面对经典攻击者时满足选择报文攻击下的存在性不可伪造（EUF-CMA），并且在面对无法进行量子叠加态问询（仅经典问询）的量子攻击者时也仍然满足EUF-CMA 属性。然而，**若允许量子攻击者对签名预言机进行量子叠加态的问询**，则S^*将无法满足 EUF-CMA 属性，即攻击者将以不可忽略的概率伪造出一个S^*的报文-签名对。

在给出S^*的具体构造前先描述构造思路。首先给定一个后量子安全的S_c，即S_c对量子攻击者满足 EUF-CMA 属性。S^*在S_c的基础上，加入了相应的安全漏洞。与 3.1 节类似，该漏洞在 EUF-CMA 模型下无法被攻击者利用，但是如果攻击者可对签名预言机进行量子叠加态问询，则攻击者可利用S^*中的漏洞以一个显著的概率伪造出一个S^*的合法报文-签名对。

具体地，加入漏洞即往体制中加入周期寻找问题(period finding problem)的问题实例，在某些参数下，周期寻找问题不存在经典高效算法，但存在高效量子算法[23]。

$$S^* = (K, Sign, Ver)$$

密钥生成算法$K(1^n)$:

$(sk_c, pk_c) \leftarrow K_c(1^n), k \leftarrow \{0,1\}^n, p \leftarrow RPrime(N')$

返回$sk = (sk_c, k, p), pk = pk_c$

签名算法$Sign((sk_c, k, p), m)$:

$s_1 = PRF(k, m \bmod p)$

$$s_2 = \begin{cases} sk & \text{如果} m = p \\ 0 & \text{如果} m \neq p \end{cases}$$

$\sigma \leftarrow Sign_c(sk_c, (m, s_1, s_2))$

返回(σ, s_1, s_2)

验证算法$Ver(pk, m, (\sigma, s_1, s_2))$:

返回$Ver_c(pk, (m, s_1, s_2), \sigma)$

图 3.2 S^*构造描述

给定两个整数N, N'，设M为整数区间$[0, N)$。设$S_c = (K_c, Sign_c, Ver_c)$是一个数字签名体制，该体制的明文空间为$M$。设 PRF 为一个值域为$M$的伪随机函数。记$RPrime(N')$为一个过程，该过程将从$[\frac{N'}{2}, N')$中随机均匀抽取一个素数。$S^*$构造如图 2.2。**定理 3.4.** 如果$S_c$对量子攻击者满足 EUF-cCMA，且PRF在经典问询下是安全的，则通过合适地选择N, N'，S^*满足 EUF-cCMA 但不满足 EUF-qCMA，即S^*可被量子选择报文攻击攻破。

直观上，如果能找出S^*中的p，则立刻可获得sk（如果$m = p, s_2 = sk$）。对于 cCMA 攻击者（对签名预言机进行经典问询），寻找p的概率是可忽略的。而对于 qCMA 攻击者（对签名预言机进行量子叠加态问询），通过[23]针对周期查找问题的量子算法，攻击者可立刻得到p。

定理 3.4 的证明在附录 B 中给出。

3.3 讨论

3.1 节给出一个模型下安全但是实际运行存在高效量子攻击者的体制，该体制的存在指出经典模型并不能完整刻画量子攻击者的攻击能力。3.2 节论证对体制部分算法拥有量子问询能力的量子攻击者强于没有叠加态问询能力的攻击者。

显然，两节所给出的体制都被设计成某种情况下安全而某种情况下不安全。在实际运行中一般不会使用类似的结构不自然的体制。比如 3.1 节中ID*的碰撞阶段，要求循环中的

c满足$c \leq \sqrt[3]{2^l}$是因为该值能保证经典攻击者无法以显著的概率找到碰撞，而量子攻击者可以以显著概率找到碰撞。3.2 节中S^*的签名算法加上s_1和s_2部分也是为能让其被量子攻击者攻破。即两个体制都是在已有安全体制的基础上加入漏洞。

3.1 节、3.2 节的两个体制的设计具有一定的“不自然”成分，当然对于命题证明来说这是可行的。但如果能找到一些结构更自然的体制并对其进行叠加态攻击，则更具有说服力，比如，对已有的声称达到后量子安全的公钥密码体制进行分析，给出对该体制的量子叠加态攻击，则更能说明量子安全概念的必要性。

以下为 3.1 节与 3.2 节内容上的区别：

- 3.1 节中的身份验证协议ID^*是在模型下安全，但是实际运行不安全，这说明的是随机预言机模型出了问题，因为它无法刻画攻击者在实际运行中的攻击：实际运行中量子攻击者可对哈希函数进行叠加态求值，而经典随机预言机模型仅限攻击者对预言机进行经典求值。因此 3.1 节在一定程度上体现了修改经典随机预言机模型以刻画量子攻击者能力的必要性。
- 3.2 节中的签名体制S^*无法抵抗叠加态攻击，但在实际运行中是否安全则还需讨论。EUF-CMA 模型刻画的安全概念是“攻击者可取得多个报文对应的多个签名，但是仍无法自行伪造出任意一个签名”，允许攻击者对签名预言机进行问询的一个动机是为了考虑“攻击者可获得多个报文对应的多个签名”这一攻击行为。对S^*的叠加态攻击建立于允许攻击者对签名预言机进行量子叠加态问询这一基础之上，**而“允许攻击者对签名预言机进行量子叠加态问询”意味着什么？这对应着实际上攻击者的何种行为？**以上两个疑问对于其它的公钥密码体制，如公钥加密体制，也一样适用，因为在第四章中公钥密码体制的量子安全模型也一样允许攻击者对相关预言机（如解密预言机）进行问询。

关于“允许攻击者对安全模型中的预言机进行量子叠加态问询”这一动机，目前业界已有相关的说法。比如考虑数字签名体制的交互过程，通信的一方具有量子计算机而另一方仅具有经典计算机，显然具有量子计算机的一方只能使用经典的数字签名体制与另一方进行通信。在此情况下，攻击者可以通过各种方式（比如内部攻击、外部截获等行为）获得包含报文与签名的叠加态$\sum_m |m\rangle|\sigma_m\rangle$。“允许攻击者对签名预言机进行量子叠加态问询”在一定程度上描述了这样一种攻击。然而，该情况相对特殊，只有给出更一般、更普适的应用场景与攻击例子才能说明允许攻击者对模型中预言机进行叠加态问询的必要性。

4. 公钥体制量子安全模型

本章展示量子随机预言机模型、数字签名的量子安全模型与公钥加密量子安全模型，并对这些安全模型做出一定的分析，指出在量子安全模型中证明时会遇到的困难并探讨解决思路。

量子随机预言机模型是一种安全性证明技巧而非某种特定密码体制的安全模型，本文为了方便将其整合在该章节中，因为量子随机预言机模型可用在任何安全模型下的安全性证明中。

4.1 量子随机预言机模型

3.1 节指出要证明密码体制在 ROM 下的安全性，需要考虑攻击者对哈希函数(RO)的叠加态问询。量子随机预言机模型建立在经典随机预言机模型的基础上，并且允许攻击者对 RO 进行量子叠加态的问询。

图 4.1 对比了 CROM 与 QROM 交互方式的差别：在 QROM 中，攻击者对随机预言机（标记为 O）的问询步骤变为：**攻击者发送量子叠加态$\sum_{x,b}\alpha_x|x\rangle|b\rangle$，模拟者需要返回$\sum_{x,b}\alpha_x|x\rangle|b\oplus O(x)\rangle$**，而不再是攻击者发送 x 给模拟者，模拟者返回 O(x)给攻击者。攻击者获得该叠加态后，继续进行相应的量子计算（有可能是测量获取信息或是进行某些量子变换）。

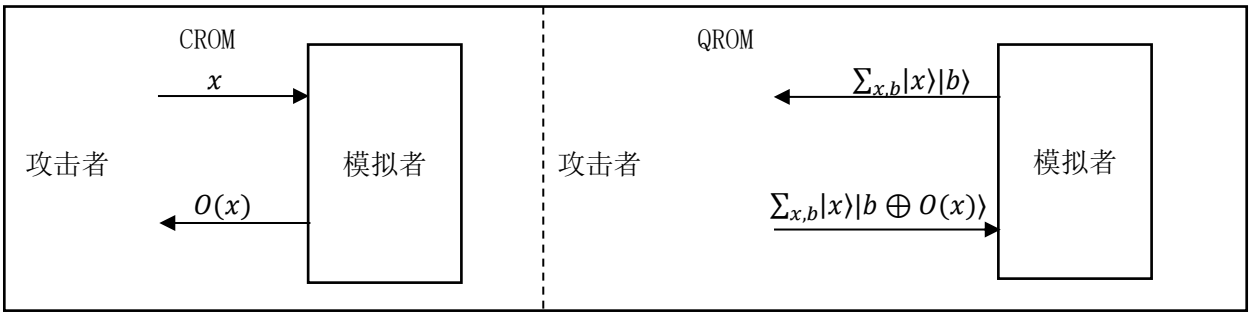

图 4.1 QROM 与 ROM 的区别

模拟量子随机预言机. 由于量子叠加态中可能有指数多个状态的叠加，比如攻击者问询$\sum_{i=0}^{2^n-1}|i\rangle|b\rangle$，因此在应答攻击者的叠加态问询时，需要考虑是否能高效模拟 RO。

在 CROM 下，模拟者不直接构造真随机函数，而是通过惰性抽样来模拟 RO。然而这种方法将无法用在 QROM 中，因为若问询中有指数个状态，模拟者需要均匀抽样指数多个应答，即需要维护一张指数大的问询列表。这将导致模拟者无法高效模拟 QRO。[6]提出使用量子安全的（可量子问询）伪随机函数来模拟 QRO，因为伪随机函数与真随机函数不可区分且伪随机函数可高效执行。另外一种模拟 QRO 方式则是使用 k-wise 独立函数，对于（量子）问询次数为 q 次的攻击者，2q-wise 独立函数足以模拟 QRO[11]（即在

q 次问询攻击者的视野里 2q-wise 独立函数和真随机函数没有区别）。

一些常用在 CROM 的技巧也难以在 QROM 中使用，比如借助 RO 两大特性的技巧。由于无法通过惰性抽样构造函数表，模拟者无法观测攻击者所问询过的内容。在保证高效模拟的情况下，如何利用 QRO 的可编程特性（根据规约适应性地修改一些输出）也是一大难点。Forking lemma[27]等技巧是否能使用在 QROM 中则还是未知的。

4.2 数字签名量子安全模型

图 4.2 给出了数字签名的量子安全模型：**量子选择报文攻击**下存在性不可伪造（简称为 EUF-qCMA）。EUF-qCMA 与经典版本的 EUF-CMA 有较明显的差异:

1. 量子安全模型允许攻击者对签名预言机进行量子叠加态问询。
2. 若攻击者对签名预言机发出q次量子叠加态问询次数，则攻击者的攻击目标为：生成$q+1$个报文-签名对。这与经典模型下的目标不同，经典模型仅要求攻击者伪造一个报文-签名对。

$$G_{A,S}^{EUF-qCMA}$$

$$S=(K,Sign,Ver)$$

1. $(pk,sk)\leftarrow K(1^n)$，运行攻击者$A^{|Sign(sk,\cdot)\rangle}(1^n,\mathrm{pk})$
2. 每当A发出量子叠加态的签名问询$\sum_{m,b}|m\rangle|b\rangle$,模拟者先抽取随机性$r$，返回$\sum_{m,b}|m\rangle|b\oplus Sign(sk,m;r)\rangle$
3. 若A发出了问询q次量子问询，则$\{(m_1,\sigma_1),\dots,(m_{q+1},\sigma_{q+1}\}\leftarrow A^{|Sign(sk,\cdot)\rangle}(1^n,\mathrm{pk})$
4. 若$\forall i,j\in\{1,\dots,q+1\},(m_i,\sigma_i)\neq(m_j,\sigma_j),Ver(m_i,\sigma_i)=1$，则返回 1，否则返回 0。

图 4.2 $G_{A,S}^{EUF-qCMA}$描述

由于攻击者在一次量子叠加态问询里面就能直接潜在地访问所有可能的报文，因此无法类似图 2.3 中所述的，构造一个签名问询列表，这将导致模拟不高效。没有签名问询列表则模拟者无法确定攻击者通过问询得到过哪些报文-签名对，原有的攻击目标不再适用，因此需要重新定义新模型的攻击目标。

对于q次量子叠加态问询的攻击者，其必然可以得到q个报文-签名对（问询获得应答后直接测量即可得到）。因此，为了表达类似“攻击者得到多个报文-签名对，仍然无法构造新的合法签名”的思想，新模型中攻击者的目标变为构造$q+1$个合法明文-签名对。

若数字签名体制S满足: 对于任意足够大的n,对于任意的 PPT 量子攻击者，$Pr\{G_{A,S}^{EUF-qCMA}(1^n)=1\}$是个关于$n$的可忽略量，则称$S$满足量子选择报文攻击下的存在性不可伪造。

显然若一个数字签名体制能满足 EUF-qCMA 属性，其必然满足 EUF-CMA，但满足 EUF-CMA

的数字签名体制不一定可达到 EUF-qCMA 属性（如 3.2 节所展示）。因此，EUF-qCMA 安全属性强于 EUF-CMA。

4.3 公钥加密体制量子安全模型

公钥加密体制的量子安全模型主要考虑量子选择密文攻击，因为公钥（加密密钥）是公开的，量子攻击者可以根据公钥自行构造对应的量子加密算法$U_{Enc_{pk}}:|x\rangle|b\rangle \to |x\rangle|b \oplus Enc_{pk}(x;r)\rangle$（其中$r$作为此次叠加态加密中统一使用的随机性，此处为简略表达）。因此对于公钥密码体制，更加需要关注的是量子叠加态选择密文攻击。图 4.3 给出了量子选择密文攻击(qCCA)下的不可区分性定义。

$G_{A,\Pi}^{IND-qCCA}(1^n)$描述

其中$\Pi = (\mathrm{K},\mathrm{E},\mathrm{D})$

1. 密钥生成阶段

   $(pk,sk) \leftarrow K(1^n)$，发送$pk,n$给$A^{|D^*(sk,\cdot)\rangle}$，$A$可对解密预言机$D^*(sk,\cdot)$进行量子叠加态的问询：$A$发送$\sum_{c,b}|c\rangle|b\rangle$,模拟者返回$\sum_{c,b}|c\rangle|b \oplus D^*(sk,c)\rangle$

   $D^*(sk,\cdot)$在$D(sk,\cdot)$的基础上有一定改动，定义如下：

$$D^*(sk,c) = \begin{cases} \perp & c = c^* \\ D(sk,c) & \text{否则.} \end{cases}$$

2. 挑战阶段:

   $(m_0,m_1) \leftarrow A^{|D^*(sk,\cdot)\rangle}(1^n,pk)$

   $b \leftarrow_R \{0,1\}, c^* \leftarrow E(pk,m_b)$

   发送c^*给$A^{|D^*(sk,\cdot)\rangle}$

3. 测试阶段:

   $b' \leftarrow A^{|D^*(sk,\cdot)\rangle}(1^n,pk,c^*)$

   若$b = b'$，返回 1,；否则返回 0.

图 4.3 $G_{A,\Pi}^{IND-qCCA}(1^n)$描述

IND-qCCA 的定义中涉及了操作:$b \oplus \perp$，为了保证量子操作的可逆性，可将$\perp$编码为不在体制明文空间中的比特串即可。

qIND-qCCA. 相比 IND-CCA，IND-qCCA 允许攻击者对解密预言机进行量子叠加态问询，但在安全性上仍然考虑经典的不可区分性。为了考虑面对量子攻击者的不可区分性（与语义安全），Gagliardoni[10]等人提出了对称加密体制的量子选择明文攻击(qCPA)下的量子不可区分性(qIND)，而针对公钥加密体制的 qIND-qCCA 的概念仍未被研究。为了简洁性，本文仅考虑 IND-qCCA 安全概念。

4.4 其它公钥体制量子安全模型及讨论

重要的公钥密码体制还包括基于身份的加密体制(IBE)、密钥封装机制(KEM)与认证密钥交换(AKE)等。但是关于这三种体制的量子安全模型目前还未被正式定义出。由于 IBE、KEM 在结构上与公钥加密体制（PKE）有一定的相似性，因此可通过适应性地修改 IND-qCCA 模型得出相对应的量子安全模型。

AKE 中常有的（经典）安全模型包括 CK 模型[28]、eCK 模型[29]等。由于 AKE 安全模型中攻击者具有较多的攻击方式，比如侧信道攻击、中间人攻击等，因此相对其他公钥密码体制，AKE 的量子安全模型及其安全定义需要更多的考虑。目前还没有 AKE 的量子安全模型。

接下来对本章内容做一定的讨论。

模型的强度与合理性. 在设计安全模型时，不仅需要考虑安全模型对攻击者是否有足够刻画能力，还需要考虑该安全模型是否过强。所谓过强的安全模型即，攻击者能力过强，体制在该模型下的安全性难以证明，甚至在该模型下不存在可证明安全的体制。比如公钥加密的量子安全模型，除了用不可区分性刻画安全性之外，还可用**全量子不可区分性**(full quantum indistinguishable，简称 fqIND)[7]来刻画体制的安全性。然而，**fqIND 概念被证明是无法达到**，即任意的加密体制都不可能达到 fqIND[7]。4.1.2、4.1.3 节的安全概念被证明是可以达到的，具体的协议实例分别在第五章和第六章。

合理性也是设计安全模型时需要考虑的重要部分。尽管安全模型中攻击者的能力越强，在此模型下可证明安全的密码体制在现实中的安全性也更值得信赖。然而一般情况下，安全性和效率难以兼得，体制安全性过强可能会导致运行效率的不足。单纯地加强攻击者的攻击能力而不考虑这种加强的合理性及与现实的对应性，会导致体制在实际运行中有冗余安全性（即，实际运行中攻击者并没有模型中如此复杂的攻击能力但模型都考虑）同时还效率不足。在实际运行中，是否真的需要如此强安全的体制呢？4.1.2、4.1.3 节的安全概念的合理性与强度在未来研究中还需要进一步的探讨。

模拟预言机. 在安全性证明时，需要考虑如何模拟安全模型中所要求的预言机，比如在 EUF-qCMA 中要考虑如何模拟签名预言机,在 IND-qCCA 中需要考虑如何模拟解密预言机。而在规约证明中，模拟者常常并不具有签名用的私钥或是解密用的私钥，因此在证明中需要考虑如何在没有私钥的情况下模拟安全模型要求的预言机。

在经典模型中有一系列方法可以解决上述模拟预言机的问题。比如巧妙使用 ROM 的可编程特性或是在体制中加入某些具有特殊性质的构件。而在量子情况下，由于攻击者可对预言机进行量子叠加态的问询，因此在证明中需要考虑这些方法是否能够高效模拟预言机。第五章和第六章分别展示量子安全数字签名和量子安全公钥加密，同时也对其中模拟预言机的方法作一定的探讨。

5. 量子安全数字签名

本节将展示一种满足 EUF-qCMA 的数字签名体制S[7],S由一个安全概念较弱的数字签名体制S_c和变色龙哈希函数（Chameleon hash function）构成。相关的概念与引理将在5.1 节给出。5.2 节给出S的构造与证明思路。最后 5.3 节将对S的 EUF-qCMA 属性进行证明并探讨证明中高效模拟量子签名预言机的方法。

5.1 随机明文攻击与变色龙哈希

量子安全签名体制S基于一种较弱的数字签名体制S_c，S_c满足随机报文攻击下的存在性不可伪造(简称 EUF-RMA)。EUF-RMA 相对 EUF-CMA 较弱，定义如下：

随机报文攻击下的存在性不可伪造. 随机报文攻击(Random message attack)指模拟者在安全游戏中随机均匀选取q个报文，生成对应的签名，返回这q个报文-签名对给攻击者。攻击者仅得到这q个报文-签名对,不允许进行签名问询。最后攻击者尝试生成一个伪造（不属于给定的q个报文-签名对）。记S是一个数字签名体制，若对于任意的攻击者A,在随机报文攻击下， A可生成一个S的伪造的概率是可忽略量，则称S满足随机报文攻击下的存在性不可伪造。

S的构造中还包含变色龙哈希函数。在证明中，变色龙哈希函数的性质可使模拟者不需要S的私钥sk也可模拟签名预言机。变色龙哈希函数定义如下：

变色龙哈希函数. 一个变色龙哈希函数由四个算法构成$CH = (G, H, Inv, Sample)$：

- $G(1^n)$:生成公私钥对(pk, sk)。
- $H(pk, m, r)$:对报文m进行哈希。
- $Sample(1^n)$:该算法抽取一个随机性r，r满足如下属性：对于任意的pk, m，$H(pk, m, r)$是均匀分布。
- $Inv(sk, h, m)$:该算法产生随机性r，r满足$H(pk, m, r) = h$并且给定$H(pk, m, r) = h$, 该算法输出分布可忽略地接近于$Sample(1^n)$。

如果对于任意的量子攻击者，仅给定pk，攻击者无法找到H(k,·,·)的碰撞，则称该变色龙哈希函数是抗碰撞的。现已有基于格的量子抗碰撞变色龙哈希函数[30]。而一般达到后量子安全的数字签名体制(可抵抗量子攻击者的 EUF-CMA)即满足 EUF-RMA,比如基于格的数字签名[31]、[30]。

5.2 体制构造与分析

构造 5.1. 记$\mathrm{CH} = (\mathrm{G_H}, \mathrm{H}, \mathrm{Inv}, \mathrm{Sample})$为变色龙哈希函数，$\mathrm{S_c} = (\mathrm{G_c}, \mathrm{Sign_c}, \mathrm{Ver_c})$为一个

数字签名体制。其中哈希函数的值域为S_c的报文空间。设QF, RF为两种两两独立(pair-wise independent)函数簇，这两个函数簇中的函数将签名体制的报文分别映射为Inv和$Sign_c$的随机性输入。现定义如下数字签名体制$S = (G, Sign, Ver)$:

- $G(1^n)$:

  $(sk_H, pk_H) \leftarrow G_H(1^n), (sk_c, pk_c) \leftarrow G_c(1^n)$

  输出$sk = (pk_H, sk_c), pk = (pk_H, pk_c)$

- $Sign\big((pk_H, sk_c), m\big)$:

  $Q \leftarrow_R QF, R \leftarrow_R RF$

  $r \coloneqq Sample\big(1^n; R(m)\big), h \coloneqq H(pk_H, m, r)$

  $s \coloneqq Q(m), \sigma \coloneqq Sign_c(sk_c, h; s)$，输出$(r, \sigma)$

- $Ver\big((pk_H, pk_c), m, (r, \sigma)\big)$:

  $h \coloneqq H(pk_H, m, r)$，输出$Ver_c(pk_c, h, \sigma)$

在体制构造中，CH的私钥sk_H并没有被使用，但在安全性证明中sk_H将被用于模拟签名预言机。

该体制的 EUF-CMA 属性较容易被证明：将对该体制的攻击规约为对S_c的攻击，而通过使用变色龙哈希函数可使模拟者在没有S_c私钥的情况下仍然能够模拟签名预言机。注意，在证明S的 EUF-CMA 时并不需要其中的变色龙哈希函数有抗碰撞属性。

定理 5.1. 如果对于任意量子攻击者，S_c满足 EUF-RMA 属性，并且CH是抗碰撞的变色龙哈希函数，则构造 5.1 的S满足 EUF-qCMA。即对于任意足够大的安全参数n, 对于任意的量子攻击者 A, $Pr\{G_{A,S}^{EUF-qCMA}(1^n) = 1\} \leq negl(n)$。

在给出定理 5.1 的证明前，先证明S满足 EUF-CMA，即对于任意的量子攻击者，如果S_c满足 EUF-RMA 属性，并且CH是变色龙哈希函数(不需要抗碰撞)，则构造 5.1 的S满足 EUF-CMA。给出该证明的目的是给出该体制安全性证明的主要思路，展示变色龙哈希函数在该证明中的作用，为后面 EUF-qCMA 的证明提供一个概观。

S的 EUF-CMA 证明:

G_0:该攻击游戏即$G_{A,S}^{EUF-CMA}$，但是在模拟签名预言机时候，模拟者不需要生成R, Q这两个函数，其生成签名步骤改为：$r \leftarrow Sample(1^n), h \coloneqq H(pk_H, m, r), \sigma \leftarrow Sign(sk_c, h)$，然后返回$(r, \sigma)$。另外模拟者在生成$pk_H$时也将对应的$sk_H$保留下来。

G_0与$G_{A,S}^{EUF-CMA}$实际上是等价的。由于R, Q在每一次问询仅被使用一次，由其两两独立

性，攻击者将无法区分G_0与$G_{A,S}^{EUF-CMA}$。因此$Pr\{G_0 = 1\} = Pr\{G_{A,S}^{EUF-CMA} = 1\}$。

G_1对签名问询的应答方式作了修改。设攻击者问询报文m的签名，模拟者做如下操作：$h \leftarrow MSP^{S_c}$, $\sigma \leftarrow Sign(sk_c, h)$，$r \leftarrow Inv(sk_H, h, m)$，然后返回$(r, \sigma)$。

在变色龙哈希函数的定义中，对于由$Sample$生成的r, $H(pk, m, r)$是一个均匀分布，即可将h视为均匀选取。再由Inv算法的属性，$Inv(sk_H, h, m)$输出的概率分布和Sample的输出分布几乎接近，同时也满足$h = H(pk_H, m, r)$，因此$|Pr\{G_1 = 1\} - Pr\{G_0 = 1\}| \leq negl(n)$。

接下来可直接规约到S_c的 EUF-RMA 属性。具体地，设 A 是任意一个对S的攻击者，该攻击者发起q次签名问询。现构造一个攻击者 B，该攻击者模拟G_1，借助 A 以攻击S_c:

$B\left(1^n, pk_c, \left((h_1, \sigma_1), \ldots, (h_q, \sigma_q)\right)\right)$:

1. $(sk_H, pk_H) \leftarrow G_H(1^n)$，运行$A^{Sign(sk,\cdot)}\left(1^n, (pk_c, pk_H)\right)$
2. 当A发出第i次签名问询（设报文为m_i），执行如下操作:$r_i \leftarrow Inv(sk_H, h_i, m_i)$, 返回$(r_i, \sigma_i)$
3. 当A返回伪造$\left(m^*, (r^*, \sigma^*)\right)$，计算$h^* \leftarrow H(pk_H, m^*, r^*)$，输出$(h^*, \sigma^*)$

容易分析得 B 完美模拟了G_1，并且如果A返回的伪造是合法的，即$Ver(pk_c, h^*, \sigma^*)$输出1，并且不在问询列表当中，则(h^*, σ^*)是S_c的一个合法伪造。因此$Pr\{G_1 = 1\} = Pr\{G_{B,S_c}^{EUF-RMA}\} \leq negl(n)$，易推得$Pr\{G_{A,S}^{EUF-CMA} = 1\} \leq negl(n)$。注意，此时并未要求$CH$具有抗碰撞属性。

以上证明方法难以直接适用在 EUF-qCMA 的证明之中，具体地，在 EUF-qCMA 中，攻击者可对签名预言机进行量子叠加态的问询。由于叠加态中可能有指数多个报文的取值，若模拟者B没有签名私钥，则B从S_c中获得的报文-签名对输入(h, σ)要指数多个才可以成功模拟签名预言机，这将导致G_1模拟不高效。因此要证明该体制满足 EUF-qCMA，则必须考虑**如何仅用多项式个(h, σ)来应答攻击者的量子叠加态签名问询**。如何解决该问题是证明定理 5.1 的关键步骤。

一个解决方案是，通过**小域分布**(small range distribution)[13]，使用多项式个(h, σ)来模拟对叠加态中指数多个报文的签名应答。详细内容在 5.3 节给出。

5.3 安全性证明

接下来给出定理 5.1 的证明，即证明S的 EUF-qCMA 安全性。本文在此证明的重点为展示如何高效模拟签名预言机的一种方法（使用小域分布），因此仅给出部分的证明，剩下的

证明在附录 D 中给出。

证明前先给出证明先给出相关引理：

小域分布. 记X,Y为两个集合，D是Y上的一个分布。设r为一个整数，P是$X \to [r]$的真随机函数。令$(y_1,\dots,y_r)$是根据D抽取的r个样本。$(y_1,\dots,y_r)$和P可构成一个函数的分布$H{:}X \to Y$，该分布由$H(x) \to y_{P(x)}$定义。该分布称为小域分布(关于r个D的样本)。

引理 5.2.([13]) 对于任意的集合X,Y，任意的在Y上的分布D，任意的整数r与任意的量子算法 A（该算法向预言机$H{:}X \to Y$发出q次叠加态问询)，存在常数C_0，A 区分以下两种预言机H的概率小于$\frac{C_0 q^3}{r}$：

- $H(x) = y_x$, 其中$y_x \leftarrow_R D$。
- H根据小域分布(关于r个D的样本)进行构造。

引理 5.3.([7, Lemma2.5]) 记X,Y为集合，对于任意的$x,x' \in X$，令D_x, D_x'为Y上的分布，并且$D_x, D_{x'}$满足$|D_x - D_x'| \le \epsilon$，$\epsilon$独立于$x$的选取。设函数$O{:}X \to Y$满足对于任意的$x$有$O(x) \leftarrow D_x$（即$O(x)$的取值根据$D_x$从Y抽样)，函数$O'{:}X \to Y$满足对于任意的$x$有$O'(x) \leftarrow D_x'$。则对于任意q次叠加态问询的量子攻击者A，A可区分预言机O与预言机O′的概率至多为$\sqrt{8C_0 q^3 \epsilon}$。

对定理 5.1 的证明：设ϵ为攻击者 A（q次问询）在$G_{A,S}^{EUF-qCMA}(1^n)$中的取胜概率，现设ϵ是不可忽略的，即存在多项式$p = p(n)$使得$p(n) > \frac{1}{\epsilon(n)}$。记$\epsilon_i$为在安全游戏$G_i$中攻击者取胜的概率。

G_0. G_0即$G_{A,S}^{EUF-qCMA}$，模拟者按照如下方式模拟签名预言机：在攻击者对签名预言机发出第i次量子叠加态时，模拟者首先分别从RF, QF中抽取两个两两独立函数R^i, Q^i，然后对问询叠加态中所有的明文m，做如下计算：

1. 令$r_m^i = Sample\left(1^n; R^i(m)\right), s_m^i = Q^i(m)$
2. 计算$h_m^i = H\left(pk_H, m, r_m^i\right), \sigma_m^i = Sign_c(sk_c, h_m^i; s_m^i)$
3. 返回应答(r_m^i, σ_m^i)。

（即：$\sum_m |m\rangle|b\rangle \to \sum_m |m\rangle|b \oplus \left(r_m^i, \sigma_m^i\right)\rangle$）

攻击者在最后将生成$q+1$个伪造$\{(m_1^*, r_1^*, \sigma_1^*), \ldots, (m_{q+1}^*, r_{q+1}^*, \sigma_{q+1}^*)\}$。

G_1. G_1对G_0 做了三处改动：

1. RF, QF改为真随机函数簇，即R^i, Q^i是真随机函数。该改动等价于，r_m^i的生成改为$r_m^i \leftarrow Sample(1^n)$，即均匀随机性由算法“内部生成”。注意在量子设定下算法的随机性还要由模拟者选取生成。
2. s_m^i的生成改为均匀随机生成（类似于 EUF-CMA 安全证明中的修改），该改动等价于$\sigma_m^i \leftarrow Sign_c(sk_c, h_m^i)$。
3. 攻击者的成功条件改为:
   a) 生成$q+1$个互不相同的伪造(原本G_0的目标)。
   b) **任意的两个(m_k^*, r_k^*)都不是$H(pk_H, \cdot, \cdot)$的碰撞。**

注意，此时G_1是无法高效模拟的，因为模拟者需要抽取指数多个r_m^i与s_m^i。

由于在G_0中，R,Q仅被攻击者问询一次，由其两两独立性知攻击者无法区分R,Q来自两两独立函数簇还是来自真随机函数簇。又由CH的抗碰撞性，易得$\epsilon_1 \geq \epsilon_0 - negl^{CH}(n)$。

G_2. 在G_1基础上:h_m^i的生成变为均匀随机生成（而非由$H(pk_H, m, r_m^i)$计算）。另外，均匀随机生成随机性t_m^i，计算$r_m^i = Inv(sk_H, h_m^i, m; t_m^i)$。

在攻击者 A 的视野中，两个安全游戏的区别在于r_m^i的分布差异。而由CH中Sample和Inv的性质，对于每一个m，G_2中r_m^i的分布与G_1中r_m^i的分布是可忽略地接近。若攻击者 A 是经典攻击者，则可以直接得出$|\epsilon_2 - \epsilon_1|$是可忽略的。然而此时 A 是量子攻击者，因此需要针对量子攻击者相关的不可区分引理来论证。以引理 5.3 的视角来看，不同的m即引理 5.3 中的x，对于通过$Sample$函数生成的r_m，其分布可看做D_x，而通过Inv生成的r_m，其对应分布可视为D_x'。由CH的属性可知$|D_x - D_x'| \leq negl^{rand}(n)$。由引理 5.3 可知，$\epsilon_2 \geq \epsilon_1 - negl^{rand}(n) = \epsilon_0 - negl^{CH}(n) - negl^{rand}(n)$。注意，此时模拟者开始使用$CH$的私钥$sk_H$。

G_3. 设$l = 2C_0qp$，C_0为引理 5.2 中的常数。在G_2基础上，模拟者在运行攻击者前选定一些列的值：对于$i = 1, \ldots, q$与$j = 1, \ldots, l$，随机均匀抽样$\hat{h}_j^i$并计算$\hat{\sigma}_j^i = Sign_c(sk_c, \hat{h}_j^i)$，再选$q$个真随机函数$O_i$，这些函数将明文m映射到$\{1,\ldots,l\}$中。模拟者还选取q个真随机函数$T_i$。运行攻击者后，**对于每一次问询，令$h_m^i = \hat{h}_{O_i(m)}^i$，$\sigma_m^i = \hat{\sigma}_{O_i(m)}^i$，$t_m^i = T_i(m)$。**

G_3对G_2的改动为：

1. h_m^i用小域分布来生成。图 5.1 指出了h_m^i生成方式的图形描述。由于$\sigma_m^i = \hat{\sigma}_{O(m)}^i =$

$Sign(sk_c, \hat{h}^i_{O(m)}) = Sign(sk_c, h^i_m)$，因此其生成方式类似$h^i_m$，不再赘述。

2. t^i_m的生成方式改成由真随机函数生成。

第一个改动是该证明的核心。如前面所述，在应答攻击者 A 的量子叠加态签名问询时，模拟者需要用到指数多个h^i_m, σ^i_m。在规约中，所有的h_m, σ_m都是在$G^{EUF-RMA}_{A,S_c}$中生成，如果模拟者从$G^{EUF-RMA}_{A,S_c}$中获得指数多个h_m, σ_m，这将导致模拟不高效。在G_3中，模拟者事先抽取多项式个$\hat{h}$并构造其对应的$\hat{\sigma}$，然后所有的h_m, σ_m都从这些$\hat{h}, \hat{\sigma}$中取值。举例来讲，在应答第i次量子签名叠加态问询时，对于叠加态$\sum_m |m\rangle$中所有的报文值m，模拟者需要计算所有这些报文对应的(h^i_m, σ^i_m)。模拟者使用已构造好的l个$\hat{h}, \hat{\sigma}$值$\{(\hat{h}^i_1, \hat{\sigma}^i_1), \dots, (\hat{h}^i_l, \hat{\sigma}^i_l)\}$作为这些$\{(h^i_m, \sigma^i_m)\}_m$的取值。注意，所有的$(h^i_m, \sigma^i_m)$都是合法$S_c$签名。

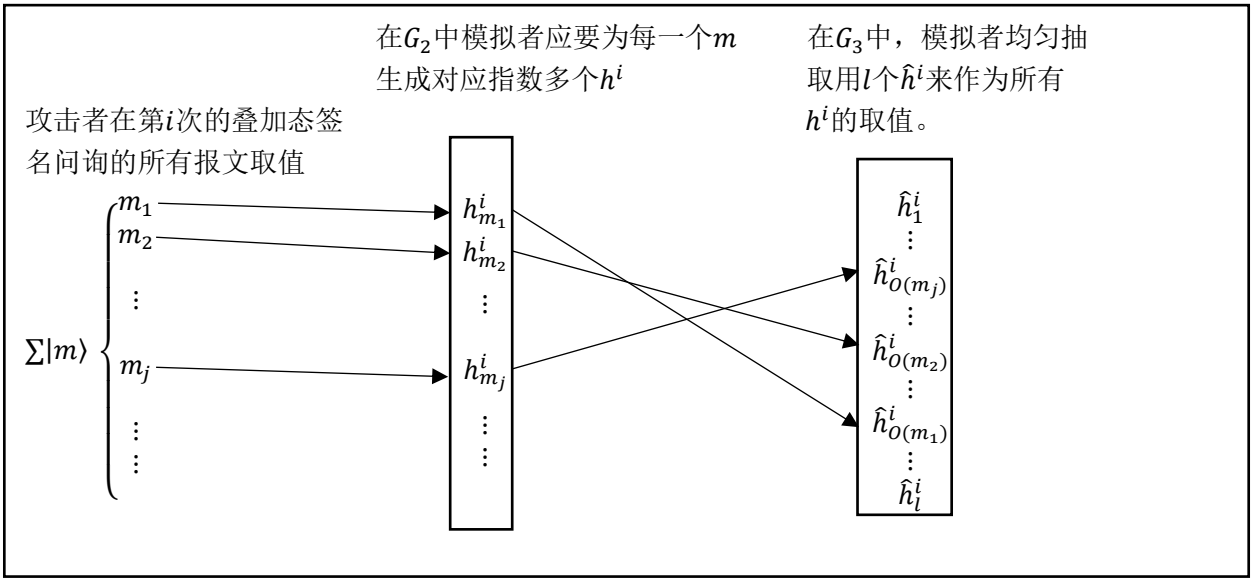

图 5.1 小域分布在G_3中的体现：“小域”体现于，用相对少量的$\hat{h}^i$来作为指数多个h^i的取值。由鸽笼原理，必然存在$m_j \neq m_k, h^i_{m_j} = \hat{h}^i_{O(m_j)} = \hat{h}^i_{O(m_k)} = h^i_{m_k}$。但由引理 C.1，攻击者以小于$\frac{1}{2p}$的概率区分$h^i$生成是随机均匀生成还是通过小域分布生成。

由引理 5.2 与l的取值，在某一次签名问询中攻击者可区分两种分布的概率是$\frac{1}{2qp}$，q次问询后量子攻击者将以小于$\frac{1}{2p}$概率区分两种h, σ的生成方式。显然l是多项式大的，因此模拟者此时可高效模拟签名预言机。

第二个改动实际上和随机均匀抽取t^i_m相同，此改动仅为了方便下一个安全游戏的描述。综上所述，有$\epsilon_3 \geq \epsilon_2 - \frac{1}{2p}$。

G_4. 在G_3的基础上，令O_i, T_i都为两两独立函数。由于O_i, T_i仅用于某一次问询，量子攻击者无法区分O_i, T_i是真随机函数还是两两独立函数[11]，由此得$\epsilon_4 = \epsilon_3$。此时模拟者使用两两独立函数来生成随机性，因此G_4是可高效模拟的（G_1, G_2, G_3都涉及模拟者自选随机性、构造真随机函数等步骤，因此无法高效模拟）。

此时模拟者可以高效模拟G_4，接下来的证明思路类似于S的 EUF-CMA 证明，模拟者可以通过来自S_c的多项式个(h, σ)来作为G_4中的$(\hat{h}, \hat{\sigma})$。模拟者需要借助攻击者来构造出S_c的合法伪造，但由于攻击者返回的是$q+1$个伪造，并且模拟者在应答时使用了小域分布来生成$\hat{h}, \hat{\sigma}$而非直接根据报文m来构造签名应答，因此模拟者无法直接从攻击者的伪造中直接提取信息，比如直接从$q+1$个伪造中均匀抽取一个伪造返回会导致规约不正确，所以还无法直接论证ϵ_4是可忽略量。

剩下的证明则是说明如何用量子相关的引理与技巧来使模拟者从攻击者中抽取出需要的信息，并非本文重点，因此这些证明将放在附录 C 中。

5.4 讨论

本章给出一种量子安全的数字签名体制S，该体制基于一个后量子安全数字签名与变色龙哈希函数。该体制的提出论证了 4.2 节中的 EUF-qCMA 安全是可达到的，因此具有一定的理论意义。注意，由于不同的S_c与CH会组合成不同的S，因此S的构造可视为一种通用转换，该转换可将安全性较弱的数字签名体制转换为安全性较强的数字签名体制。

然而该体制的规约紧致性较差。附录 C 证明了，如果攻击者以ϵ_0的概率攻破，则可构造一个攻击者，该攻击者以$\epsilon_7 \geq \frac{\epsilon_0}{ql^2} - \frac{negl(n)}{ql^2} - \frac{1}{2pql^2}$的概率攻破$S_c$的 EUF-RMA 属性。在安全证明上，这足以论证ϵ_0是可忽略量。然而，该规约是非常不紧致的，因为ql^2可以是一个非常大的值，比如$q \approx 2^{20}, l \approx 2^{50}$，这意味着运行$S$时要选择一个巨大的安全参数才能达到所需的安全性（比如2^{80}比特安全）。安全参数过大会导致体制运行不高效。

除了使用通用转换来构造量子安全数字签名体制，还可以尝试通过某种“通用规约形式”将后量子安全数字签名体制证明为量子安全。比如，Boneh 等人在提出 QROM 的同时还提出了无历史规约(history-free reduction，简称 HFR)[6]，对于特定的数字签名体制，如果可将该体制在 CROM 下的 EUF-CMA 安全性证明构造为 HFR 形式，则该数字签名体制在 QROM 下满足 EUF-CMA 属性。类似地，可尝试提出某种通用规约形式，如果一种数字签名体制的后量子安全性规约证明可构造为该种规约形式，则这种数字签名体制也满足量子安全性。这种通用规约形式的好处在于，在使用现有高效后量子安全数字签名体制的同时避免加入其它构造从而避免效率的降低。

6. 量子安全公钥加密体制

通用转换是设计公钥加密体制的一种常用方法。Fujisaki-Okamoto 转换[32]（简称 FOT）通过使用哈希函数，将安全性较弱的公钥加密体制和对称加密体制组合成一个在 ROM 达到 IND-CCA 安全的公钥加密体制。

然而，通过 FOT 得到的公钥加密体制在 ROM 下的 IND-CCA 安全性证明无法适用于 QROM 下，因此 FOT 的量子变种 QFOT 被提出[12]。QFOT 已被证明在 QROM 下满足 IND-CCA，本文将指出 QFOT 在 QROM 下也满足 IND-qCCA。记Π^{QFO}为通过 QFOT 得到的公钥加密体制。

QFOT 的描述与相关安全性定义将在 6.1 节给出。6.2 节对Π^{QFO}进行分析，指出其安全性证明思路。6.3 节证明Π^{QFO}在 QROM 下满足 IND-qCCA。对Π^{QFO}的讨论在 6.4 节中给出。

6.1 QFOT 构造与相关定义

QFOT 使用三个哈希函数将一个**单向γ-散布**的公钥加密体制和一个**一次安全**对称加密体制组合成一种抗选择密文攻击的公钥加密体制。在介绍 QFOT 前先给出相关的定义。

单向公钥加密. 设$\Pi = (K, E, D)$是一个公钥加密体制。给定安全参数k与攻击者 A，定义如下的安全游戏$G_{A,\Pi}^{OW}(1^k)$:

1. $(pk, sk) \leftarrow K(1^k)$
2. $x \leftarrow_R MSP, y \leftarrow E_{pk}(x)$
3. $y' \leftarrow A(pk, y)$
4. 若$y = y'$，则返回 1；否则返回 0

定义 6.1. 设$\Pi = (K, E, D)$是一个公钥加密体制。如果对于任意的 PPT 攻击者 A 与任意足够大的$k \in N$，恒有:

$$Pr\{G_{A,\Pi}^{OW}(1^k) = 1\} \leq negl(k)$$

则称Π是单向安全的。

单向安全性要求仅给定通过体制加密算法加密得到出来的密文（与安全参数），难以找到该密文对应的明文。攻击者在该安全游戏中是被动的，即无法访问解密预言机。显然，相对于 IND-CPA，单向安全的安全性更弱。

定义 6.2. 设$\Pi = (K, E, D)$是一个公钥加密体制。如果对于任意足够大的协议安全参数$k \in N$，任意的pk，任意的$x \in MSP$与y，恒有:

$$\underset{r \leftarrow COIN}{Pr}\{y = E_{pk}(x; r)\} \leq \frac{1}{2^{\gamma}}$$

则称Π是γ-散布(γ-spread)的。

在γ-散布加密体制中，在加密随机性均匀选取的情况下，任意的明文都至少有2^{γ}个密文与其对应。

一次安全私钥加密. 设$\Pi = (E, D)$是一个私钥加密体制，给定安全参数 k 与攻击者 A，定义如下攻击游戏$G_{A,\Pi}^{OT}(1^k)$:

1. $sk \leftarrow_R KSP$
2. $(m_0, m_1, s) \leftarrow A(1^k)$
3. $b \leftarrow_R \{0,1\}, c \leftarrow E_{sk}(m_b)$
4. $b' \leftarrow A(c, s)$
5. 如果$b' = b$，返回 1;否则返回 0

定义 6.3. 设$\Pi = (E, D)$是一个私钥加密体制，如果对于任意的 PPT 攻击者 A 与任意足够大的$k \in N$，恒有:$Pr\{G_{A,\Pi}^{OT}(1^k) = 1\} \leq \frac{1}{2} + negl(k)$，则称Π是一次安全的。

设$\Pi^{sy} = (E^{sy}, G^{sy})$是私钥加密体制，$\Pi^{asy} = (K^{asy}, E^{asy}, G^{asy})$是公钥加密体制，两个体制的明文空间满足。设哈希函数$G: \{0,1\}^* \to KSP^{sy}, H: \{0,1\}^* \times \{0,1\}^* \to COIN^{asy}, H': MSP^{asy} \to MSP^{asy}$。通过 QFOT 的公钥加密体制记为$\Pi^{QFO} = (K^{QFO}, E^{QFO}, G^{QFO})$。不失一般性，设$MSP^{asy} = \{0,1\}^{n_1}, COIN^{asy} = \{0,1\}^{n_2}, KSP^{sy} = \{0,1\}^{m}$。以下为 QFOT 的描述：

Quantum Fujisaki-Okamoto 转换

- K^{QFO}:输入为1^k，$(pk, sk) \leftarrow K^{asy}(1^k)$，将$(pk, sk)$输出。该过程表示为$(pk, sk) \leftarrow K^{QFO}(1^k)$。

- E^{QFO}:输入为$pk, m \in MSP^{FO}$. 执行如下过程
  1. $r \leftarrow_R COIN^{FO}$
  2. $a := G(r), c \leftarrow E^{sy}(a, m)$
  3. $h := H(r, c), e := E^{asy}(pk, r; h)$

4. $d \coloneqq H'(r)$
5. 输出(e,c,d)

该过程表示为$(e,c,d) \leftarrow E^{QFO}(pk,m)$。

- D^{QFO}:输入为$sk,e \in \{0,1\}^*,c \in \{0,1\}^*,d \in \{0,1\}^*$. 执行如下过程
  1. $\hat{r} \coloneqq D^{asy}(sk,e)$
  2. 如果$\hat{r} \notin MSP^{asy}$，返回⊥.
  3. $\hat{h} \coloneqq H(r,c)$，如果$e \neq E^{asy}(pk,\hat{r};\hat{h})$，返回⊥
  4. 如果$d \neq H'(r)$，返回⊥
  5. $\hat{a} \coloneqq G(\hat{r})$,返回$D^{sy}(\hat{a},c)$

可以证明Π^{QFO}在 QROM 下满足 IND-qCCA 属性。

定理 6.1. 若对于量子攻击者，私钥加密体制Π^{sy}是一次安全的，公钥加密体制Π^{asy}是单向安全且是γ-散布的，则Π^{QFO}在 QROM 下满足 IND-qCCA。

6.2 QFOT 分析

在证明定理 6.1 前，先分析Π^{QFO}以给出其安全性证明思路。

Π^{QFO}的抗选择密文攻击直观. 抗选择密文攻击属性要求解密算法以极大的概率拒绝解密不合法的密文（返回⊥）。合法密文即正常的通过体制加密算法得出的密文，所谓不合法的密文即由攻击者自行构造的密文或是篡改合法密文得到的密文。

对于一个合法密文，攻击者无法知道该密文加密过程使用的随机性r，否则可以规约构造一个对Π^{asy}单向安全性的攻击算法。对于不合法的密文，如果攻击者篡改了(e,c)部分，这要么会导致解密算法在第二步停止，要么在第三步停止。因为修改了(e,c)后，解密算法计算得出的$\hat{r}$将大概率与原本的随机性r不同，这也意味着$\hat{h}$与原有的h不同。因为H是随机预言机，$\hat{h}$与h互相独立且符合均匀分布，由Π^{asy}的γ-散布性质，$Pr\{e = E^{asy}(pk,\hat{r};\hat{h})\}$是一个可忽略量，因此对于修改了$(e,c)$部分的密文，解密算法以极大的概率返回⊥。若攻击者篡改了d部分，那么解密算法将以极大概率在第四步返回⊥。

模拟解密预言机. 在对Π^{QFO}进行 IND-qCCA 证明时，需要考虑如何不使用私钥来模拟解密预言机。对于一个密文(e,c,d)，c部分直接携带了明文的信息，e部分是对加密所用随机性的加密，d部分是随机性的H'哈希值。由体制构造，要解密c，需要加密时使用的r，获

得r则需要用私钥sk对e进行解密。

在没有sk的情况下，可以通过两种方法获得r：

1. **可以通过G,H的问询列表获得r**。在随机预言机模型下，对G,H的求值必须向模拟者问询。因此对于通过加密算法生成的密文，模拟者在本地必然会有此次加密的关于$(r,a:=G(r)),(r,c,h:=H(r,c))$的副本。比如一个合法的密文(e,c,d)，模拟者本地应有$(r,c,h:=H(r,c))$，其中r是得到(e,c,d)过程中所使用的随机性。通过查找到该r，可以直接得到$a:=G(r)$，再而对c进行解密，进而得到(e,c,d)对应的明文。实际上该方法就是经典 FOT 安全性证明中模拟解密预言机的方法。
2. **可以通过H'获得r**。在安全证明时，可使用随机多项式来模拟随机预言机H'。由于$MSP^{asy}=\{0,1\}^{n_1}$，因此H'实际上可用有限域$GF(2^{n_1})$上的随机多项式来模拟。从$d:=H'(r)$得到r实际上是有限域多项式求根问题，即r应在多项式$H'-d$的根集中，只需要从根集中寻找需要的r即可计算回$a:=G(r)$从而解密e得到明文。已知存在高效算法求解有限域多项式的根[33]，因此可以通过此方式高效模拟解密预言机。该思想源于[34]。

两种方法都可用于证明Π^{QFO}在 ROM 下的 IND-CCA 安全性。然而在 QROM 下，第一种方法将导致模拟者无法高效模拟解密预言机：一方面，攻击者发出的是量子叠加态问询，模拟者无法直接观测到收到的叠加态问询中包含什么报文。另一方面，攻击者一次叠加态问询即可“潜在地”问询指数多个报文，而这指数多个报文对应着指数多个随机性，G,H的问询列表会有指数多个的值，模拟者将花费指数时间寻找需要的r。

抽取信息. 除了需要考虑如何高效模拟解密预言机，模拟者还需要考虑如何从攻击者的问询中抽取信息，因为模拟者需要借助攻击者来攻击Π^{asy}的单向安全性与Π^{sy}的一次安全性以完成安全性规约。在量子情况下，模拟者需要借助量子技巧来抽取量子叠加态问询中的信息，并且用相关的引理论证模拟者将以不可忽略概率从叠加态中获得需要的信息。本证明借助了在[14-15]中的“单向隐藏”(One way to hiding，简称 O2H)引理及其适应(adaptive,O2HA)版变种，论证模拟者可从攻击者的问询中以不可忽略概率提取所需的信息。

6.3 安全性证明

在证明定理 6.1 之前，需要用到相关的引理。

引理 6.2.([35]) 设$f:\{0,1\}^{n_1}\to\{0,1\}^{n_2}$为具有最小熵k的函数（即对于任意的x,y，有$Pr\{f(x)=y\}\le 2^{-k}$）。令$H:\{0,1\}^{*}\to\{0,1\}^{n_1}$为一个随机预言机。则对于任意的量子算法 A（该算法对H的问询为q次），A 返回f(H(·))的一个碰撞的概率至多为$O(\frac{q^{9/5}}{2^{k/5}})$。即：

$$Pr\{x \neq x, f(H(x)) = f(H(x')) \mid (x, x') \leftarrow A^H(f)\} \leq O(\frac{q^{9/5}}{2^{k/5}})$$

引理 6.3.（O2H 引理，[15]）令$H:\{0,1\}^* \to \{0,1\}^n$为一个随机预言机。$A_1$为一个预言机算法，其向H进行q次的问询。设C也是一个预言机算法，给定C输入x，C依次执行：1. $i \leftarrow \{1,\dots,q_1\}, y \leftarrow \{0,1\}^m$ 2. 运行$A_1^H(x,y)$，当A_1^H对H发出第i次问询后，C测量该问询并将测量结果输出。令：

$$P_A^1 := Pr\{b' = 1 | x \leftarrow \{0,1\}^n, b' \leftarrow A_1^H(x, H(x))\}$$
$$P_A^2 := Pr\{b' = 1 | x \leftarrow \{0,1\}^n, y \leftarrow \{0,1\}^m, b' \leftarrow A_1^H(x,y)\}$$
$$P_C := Pr\{x' = x \mid x \leftarrow \{0,1\}^n, x' \leftarrow C^H(x,i)\}$$

则有：$$|P_A^1 - P_A^2| \leq 2q_1\sqrt{P_C}$$

由于本节的目的主要为指出在Π^{QFO}在安全性证明中如何高效模拟量子随机预言机、如何不使用sk来模拟解密预言机与如何使用量子预言机的可编程特性，因此仅给出部分的证明，剩下的证明在附录 D 中。

定理 6.1 的证明：

G_0：

1. 分别构造$2(q_G + q_{dec} + 1)$-wise, $2(q_{H'} + q_{dec} + 1)$-wise 独立函数G, H'
2. $(pk, sk) \leftarrow K(1^n)$，$r^* \leftarrow MSP^{asy}$，运行$A^{|H\rangle,|G\rangle,|H'\rangle,|D(sk,\cdot)\rangle}(pk)$
3. $(m_0, m_1) \leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D(sk,\cdot)\rangle}(pk)$
4. $b \leftarrow \{0,1\}, c^* \leftarrow E^{sy}(G(r^*), m_b), e^* := E^{asy}(pk, r^*; H(r^*||c^*)), d := H'(r^*)$
5. $b' \leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D(sk,\cdot)\rangle}(pk, (e^*, c^*, d^*))$

G_0与 IND-qCCA 游戏形式相同，但将G, H′分别修改为$2(q_G + q_{dec} + 1)$-wise, $2(q_{H'} + q_{dec} + 1)$-wise 独立函数（H仍然真随机函数，因此G_0是不高效的），由 QFOT 的构造与G_0的描述知攻击者对G, H′的问询次数分别为 $(q_G + q_{dec} + 1), (q_{H'} + q_{dec} + 1)$，由[11]知对随机预言机进行 k 次叠加态问询的攻击者无法区分随机函数与 2k-wise 独立函数，因此 $Pr\left\{G_{A,\Pi^{QFO}}^{IND-qCCA} = 1\right\} = Pr\{G_0 = 1\}$

由于所有的安全游戏都包括操作：构造$2(q_G + q_{dec} + 1)$-wise 独立函数G、构造$2(q_{H'} + q_{dec} + 1)$-wise 独立函数H′、$(pk, sk) \leftarrow K(1^n)$、$r^* \leftarrow MSP^{asy}$、$b \leftarrow \{0,1\}$。为了简洁以下的安全游戏描述将忽略这些操作。

G_1将G_0中的$D(sk,\cdot)$修改为$D^*(sk,\cdot)$，$D^*(sk,\cdot)$的执行步骤为:对于输入(e,c,d) 如果e^*已定义且$e = e^*$，则返回⊥，否则执行$D(sk,\cdot)$的步骤。注意，改修改可能会使攻击者对G, H'的问询次数改变，但由于其问询次数必然是减小的，因此所构造的G, H'仍能使攻击者无法

区分。另外，对于量子攻击者，$D^*(sk,\cdot)$也可以高效模拟解密预言机。

$\mathbf{G_1}$:

1. $(m_0,m_1)\leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}(pk)$
2. $c^*\leftarrow E^{sy}(G(r^*),m_b),e^*:=E^{asy}\left(pk,r^*;H(r^*||\,c^*)\right)$
3. $b'\leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}\left(pk,(e^*,c^*,H'(r^*))\right)$
4. 如果$b=b'$，返回 1，否则返回 0.

要证明攻击者以可忽略概率区分G_0与G_1（即$|Pr\{G_0=1\}-Pr\{G_1=1\}|$是可忽略的），需要考虑$D^*(sk,\cdot)$与$D(sk,\cdot)$的差异是可忽略的，即若攻击者提交$(e=e^*,c,d)$密文，$D(sk,\cdot)$也会以极大的概率输出⊥。

若$e=e^*$，必然有$r=r^*\left(r为D(sk,e)\right)$，因此必然有$d=d^*$（不满足则两个解密算法都会拒绝），由于攻击者不允许问询挑战密文，**因此仅当$\boldsymbol{e=e^*,c\neq c^*,d=d^*}$时$\boldsymbol{D(sk,\cdot)}$与$\boldsymbol{D^*(sk,\cdot)}$会出现差异。**

而若$e=e^*,c\neq c^*,d=d^*$，这意味着$E^{asy}(pk,r^*;H(r^*||c))=E^{asy}(pk,r^*;H(r^*||c^*))$，由于H是一个真随机函数，$H(r^*||c)$与$H(r^*||c^*)$相互独立并且均匀分布。从引理 6.2 的视角来看，攻击者寻找到了$E^{asy}_{(pk,r^*)}\left(H(\cdot)\right)$的一个碰撞，由构造知攻击者对H(·)的问询次数为$\mathrm{q_H}+\mathrm{q_{dec}}+1$，再由$\mathrm{E^{asy}}$的γ-散布属性可得$E^{asy}(pk,r^*;H(r^*||c))=E^{asy}(pk,r^*;H(r^*||c^*))$的概率为$O(\frac{(q_H+q_{dec}+1)^{9/5}}{2^{\gamma/5}})$，即$|Pr\{G_0=1\}-Pr\{G_1=1\}|\leq O\left(\frac{(q_H+q_{dec}+1)^{\frac{9}{5}}}{2^{\frac{\gamma}{5}}}\right)$。

G_2在G_1的基础上，将H构造为$2(q_H+q_{dec}+1)$-wise 独立函数，并且将对称加密的密钥与$\mathrm{d^*}$的生成修改为随机均匀值而非预言机的输出。

$\mathbf{G_2}$:

1. $a^*\leftarrow KSP^{sy},d^*\leftarrow MSP^{sy}$
2. $(m_0,m_1)\leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}(pk)$
3. $c^*\leftarrow E^{sy}(a^*,m_b),e^*:=E^{asy}\left(pk,r^*;H(r^*||c^*)\right)$
4. $b'\leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}\left(pk,(e^*,c^*,d^*)\right)$
5. 如果$b=b'$，返回 1，否则返回 0.

类似于 CFOT 的证明，如果攻击者可区分G_2与G_1（即攻击者问询过$\mathrm{r^*}$），则可构造攻击者以攻破$\mathrm{\Pi^{asy}}$的单项安全性。然而在量子情况下，模拟者无法直接使用经典情况下的方法来提取相关的信息，因此需要借助引理 6.3 来证明攻击者以可忽略概率区分G_2与G_1。

设$A_1^{|G\times H'\rangle}$为一个预言机算法，该算法运行$\mathrm{A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}}$并可对预言机$G\times H'$发出叠加态问询。给定输入$\left(r^*,(a^*,d^*)\right)$，$A_1^{|G\times H'\rangle}$执行如下操作（见下页）。显然$A_1^{|G\times H'\rangle}$将对$G\times H'$问询$q_{o2h}:=q_G+q_{H'}+2q_{dec}$次。

攻击者$A_1^{|G\times H'\rangle}(r^*,(a^*,d^*))$:

1. 构造$2(q_H+q_{dec}+1)$-wise 独立函数H，$(pk,sk)\leftarrow K(1^n)$，$b\leftarrow\{0,1\}$
2. $(m_0,m_1)\leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}(pk)$
3. $c^*\leftarrow E^{sy}(a^*,m_b),e^*:=E^{asy}\left(pk,r^*;H(r^*||c^*)\right)$
4. $b'\leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}\left(pk,(e^*,c^*,d^*)\right)$
5. 如果$b=b'$，返回 1，否则返回 0.

如果$a^*=G(r^*),d^*=H'(r^*)$，则$A_1^{|G\times H'\rangle}$正在模拟G_1，如果a^*,d^*都是随机值而非预言机的输出，则$A_1^{|G\times H'\rangle}$正在模拟G_2。现构造另一个预言机算法C:

$C^{|G\times H'\rangle}(r^*)$:

1. $i\leftarrow\{1,\dots,q_{o2h}\},(a^*,d^*)\leftarrow KSP^{sy}\times MSP^{asy}$。
2. 运行$A_1^{|G\times H'\rangle}\left(r^*,(a^*,d^*)\right)$直到其对发出第$i$次问询，对第$i$次问询进行测量并输出。

对比$A_1^{|G\times H'\rangle}$、C的构造与引理 6.3 知，$P_A^1=Pr\{G_1=1\},P_A^2=Pr\{G_2=1\}$，以下定义$\mathrm{G}_3$使得$P_C=Pr\{G_3=1\}$。（为了简洁，忽略构造$2(q_H+q_{dec}+1)$-wise 独立函数H的步骤）

$\mathbf{G_3}$:

1. $a^*\leftarrow KSP^{sy},d^*\leftarrow MSP^{sy},i\leftarrow\{1,\dots,q_{o2h}\}$
2. 运行$A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}(pk)$直到$A$对$G\times H'$发出第$i$次问询:
   $(m_0,m_1)\leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}(pk)$
   $c^*\leftarrow E^{sy}(a^*,m_b),e^*:=E^{asy}\left(pk,r^*;H(r^*||c^*)\right)$
   $b'\leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}\left(pk,(e^*,c^*,d^*)\right)$
3. 测量A对$G\times H'$第i次问询中的$\hat{r}$部分，设测量结果为$\hat{r}$。
4. 如果$r^*=\hat{r}$，返回 1，否则返回 0。

由引理 6.3，有$|Pr\{G_1=1\}-Pr\{G_2=1\}|\le 2q_{o2h}\sqrt{Pr\{G_3=1\}}$。

可以证明，如果攻击者在G_2中以显著概率胜出，则模拟者可以以显著的概率攻破Π^{sy}的一次安全性，即引理 6.4。引理 6.4 的证明在附录 D 中给出。

引理 6.4. 如果对称加密体制Π^{sy}是一次安全的，则$Pr\{G_2=1\}\le\frac{1}{2}+negl^{sy}(n)$。

$\mathbf{G_4}$:

1. $a^*\leftarrow KSP^{sy},d^*\leftarrow MSP^{sy},i\leftarrow\{1,\dots,q_{o2h}\}$
2. 运行$A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}(pk)$直到$A$对$G\times H'$发出第$i$次问询:
   $(m_0,m_1)\leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}(pk)$
   $c^*\leftarrow E^{sy}(a^*,m_b),e^*:=E^{asy}\left(pk,r^*;H(r^*||c^*)\right)$
   $b'\leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}\left(pk,(e^*,c^*,d^*)\right)$
3. 测量A对$G\times H'$第i次问询中的$\hat{r}$部分，设测量结果为$\hat{r}$。
4. 如果$r^*=\hat{r}$，返回 1，否则返回 0。

$\mathbf{D^{**}((e,c,d))}$:

1. 如果$e = e^*$，返回⊥
2. 计算$H' - d$的所有的根，设S为所有的根的集合，即$S = \{r|H'(r) = d\}$。
3. 搜索$r \in S\backslash\{r^*\}$，若存在r，使得$e = E^{asy}(pk, r; H(r||c))$，则计算$\hat{a} \coloneqq G(r)$并返回$D^{sy}(\hat{a}, c)$。
4. 若$e = E^{asy}(pk, r^*; H(r^*||c))$，则：
   如果$H'(r^*) = d$，则计算$\hat{a} \coloneqq G(r^*)$并返回$D^{sy}(\hat{a}, c)$。
   否则，返回⊥
5. 返回⊥。

在G_4中，模拟者使用算法$D^{**}(\cdot)$来模拟解密预言机，同时要求H′是$GF(2^{n_1})$上的$2(q_H + q_{dec} + 1) - 1$次随机多项式。由于可用$k - 1$次随机多项式（系数均匀随机选）来构造k-wise独立函数，因此可用$2(q_H + q_{dec} + 1) - 1$次随机多项式来构造H'。根据H'的定义域与值域，构造有限域$GF(2^{n_1})$上的随机多项式即满足H′的要求。对于任意有限域上的多项式，存在经典 PPT 算法求解多项式所有的根[Ben81]，因此$D^{**}(\cdot)$可高效模拟解密预言机，并且不需要使用sk。

以下分析，对于任意的密文$(e \neq e^*, c, d)$，$D^*(sk, \cdot)$与$D^{**}(\cdot)$的输出是相同。设$\hat{r} = D^{asy}(sk, e)$：

1. 若$H'(\hat{r}) \neq d$，则$D^*(sk, (e, c, d))$必然返回⊥（第 4 行）。在$D^{**}(\cdot)$中，由于$\mathrm{H}'(\hat{\mathrm{r}}) \neq \mathrm{d}$，因此$\hat{\mathrm{r}} \notin \mathrm{S}$，即算法会执行到第 4 行。而如果$\hat{r} \neq r^*$，则必然有$e \neq E^{asy}(pk, r^*; H(r^*||c))$，因此算法会在第五行返回⊥。如果$\hat{r} = r^*$，则由于$H'(r^*) \neq d$，算法会在第四行返回⊥。
2. 若$H'(\hat{r}) = d$，则在$D^{**}((e, c, d))$执行中，必有$\hat{\mathrm{r}} \in \mathrm{S}$，即模拟者可得到$\hat{\mathrm{r}}$。
   a) 如果$r \neq r^*$：若$e = E^{asy}(pk, \hat{r}; H(\hat{r}||c))$，$D^*(sk, (e, c, d))$与$D^{**}((e, c, d))$将分别会在其第五行与第三行计算$\hat{a} \coloneqq G(\hat{r})$并返回$D^{sy}(\hat{a}, c)$。否则两者都会返回⊥。
   b) 如果$r = r^*$：若$e = E^{asy}(pk, r^*; H(r^*||c))$，$D^*(sk, (e, c, d))$与$D^{**}((e, c, d))$都会计算$\hat{a} \coloneqq G(\hat{r})$并返回$D^{sy}(\hat{a}, c)$。否则两者都会返回⊥。

因此$\mathrm{D}^*(\mathrm{sk}, \cdot)$与$\mathrm{D}^{**}(\cdot)$的输出是相同，亦即$Pr\{G_3 = 1\} = Pr\{G_4 = 1\}$。

在G_4中，a^*, d^*都与r^*无关，除了e^*部分的生成外，模拟者 B 不会再使用到r^*，因此接下来类似 CFOT 的证明，即在规约中将e^*换成从$G^{OW}_{B,\Pi^{asy}}$中获得的挑战密文。然而，同样地，该证明是在量子设定下，因此必须使用相关的量子引理与技巧来进行证明。此证明剩下的部分在附录 D 中给出。

6.4 讨论

本章描述了 QFOT,并证明由 QFOT 得到的公钥加密体制在 QROM 下满足 IND-qCCA 属性。QFOT 的提出在一定程度上解决了 FOT 是否量子安全这一开放问题。

然而，Π^{QFO}存在如下缺陷：

效率低. Π^{QFO}使用了三个哈希函数，并且密文的长度相比明文长了 2 倍。这加大了通信方的计算耗时和通信耗时。而实际上，由于该公钥加密体制“规约紧致性”较差，因此要使该体制在现实运行中仍然安全会导致其安全系数更大，安全系数越大往往效率越低，这进一步制约了该公钥加密体制的效率。

d在实际运行中作用不明. 原始的 FOT 并没有使用H'函数，QFOT 中加入H'仅为了安全证明能过。由于现代密码学要求可证明安全性，因此要论证 FOT 可抗量子攻击必须给出严谨的证明。没有证明即无法有足够证据说明其安全性，哪怕在实际运行中找不到对 FOT 的攻击。因此在安全证明的角度看，H'是必须的。然而在实际运行中，d对解密密文并无用处，因为要解密密文实际上仅需要解密e得到随机性再解密c即可。Π^{QFO}的抗选择密文性实际上仅通过(e,c)即可达到，d的加入仅为了完成证明中解密预言机的规约。

QFOT 的提出为解决 FOT 的安全性证明提供了一种解决方案,但由上述指出缺陷可知，QFOT 仍然有可修改的地方，比如给出规约紧致性更强的证明、去除密文的d部分仅修改e,c的生成方式以完成证明。

7. 总结与展望

7.1 总结

本文对现有量子安全模型及其相关公钥密码体制展开研究，具体地：

1. 展示两种对后量子安全密码体制的量子叠加态攻击，指出经典安全模型在面对量子攻击者时刻画能力不足的问题，同时对量子叠加态攻击的合理性做出一定的探讨。

2. 研究现有的量子安全模型，探讨其定义动机、直观、攻击者能力定义，同时分析这些量子安全模型的强度与合理性。

3. 展示了两种量子安全模型下可证明安全的体制实例，对这些体制的设计与证明进行了深入的分析与探讨并从中指出量子安全性证明的可借鉴的思路，同时指出这些体制尚且存在的问题。

通过展示对后量子安全密码体制的量子叠加态攻击，本文指出量子叠加态攻击的合理性与不足，即并非所有量子叠加态攻击都具有现实的合理性，比如对针对S^*的叠加态攻击进行质疑：这种叠加态攻击对应于现实的何种攻击行为？量子叠加态攻击的合理性还需要进一步的讨论。

通过对现有量子安全模型进行研究与探讨，本文讨论了量子安全模型设计需要考虑的问题，比如模型中攻击者的行为对应于现实的何种攻击？模型的强度如何？是否存在体制可达到模型所以定义的安全性。对现有量子安全模型的分析为未来设计其它公钥密码构件的量子安全模型奠定了基础。

通过详细研究两种量子安全公钥密码体制，本文指出了量子安全性证明可借鉴的思路，并且指出这些量子安全密码体制的问题，比如效率低、安全证明复杂、证明紧致性差等。这些问题的提出为以后设计更多实用的量子安全公钥密码体制提供了方向。

7.2 展望

根据以上总结，本人从三个方面对未来研究工作进行分析并提出展望。

量子叠加态攻击. 第三章展示的对密码体制的量子叠加态攻击指出经典安全模型对量子攻击者刻画能力不足。在攻击身份验证协议ID^*时，量子攻击者通过对随机预言机的叠

加态问询攻破了该协议，该攻击具有一定的合理性，因为在实际运行中，量子攻击者可在本地对哈希函数进行量子叠加态求值。相对应的，量子随机预言机模型也具有一定的合理性。

在攻击数字签名体制S^*时，攻击者对签名预言机进行叠加态问询。然而，相比于对ID*协议的攻击，对S^*的叠加态攻击则显得合理性不足。尽管业界已给出相关的攻击情形，但这些情形都较为特殊。对签名预言机进行叠加态问询是否合理？**对预言机的叠加态问询对应着现实中的何种攻击？这种攻击是否普适地存在？**以上几个问题的解决将有助于进一步阐述量子叠加态攻击的合理性、量子安全模型的合理性与量子安全概念的必要性。

量子安全模型. 为刻画攻击者的量子叠加态攻击能力，量子安全模型在经典安全模型的基础上允许攻击者对体制中某些算法进行量子叠加态问询。第四章展示了现有的公钥加密体制、数字签名体制的量子安全模型。

设计量子安全模型并非仅简单地在经典安全模型的基础上允许攻击者对体制部分算法进行叠加态问询，因为安全模型的设计需要综合衡量其**强度**与**合理性**。提出某一种体制的量子安全模型时首先需要指出该模型相比于经典模型更强，并且论证该模型的安全性是可达到的。其次还要说明模型合理性，解释模型中攻击者的攻击行为对应着现实中的何种攻击，这种攻击是否合理等等。

还有一部分公钥密码构件的量子安全模型还未被正式提出，比如基于身份的加密体制、密钥封装体制、认证密钥交换。基于身份的加密体制与密钥封装机制在结构上类似于公钥机密体制，因此设计其量子安全性相对容易。而认证考虑了更多的现实攻击，如侧信道分析等，因此其量子安全模型的设计将相对复杂。**为以上公钥密码构件设计强度合适并且合理的量子安全模型是构建其量子安全公钥密码体制的基础**。

量子安全公钥密码体制. 相比于后量子安全公钥体制，量子安全公钥体制往往效率不高，安全证明的紧致性也较差，因此在现实中并不实用，五六章所展示体制的意义更多是理论层面上的，在现实中一般不会使用如此低效的体制。因此，**设计实用的量子安全体制具有较高的实践意义。**

量子安全体制的证明比后量子安全的证明要复杂许多，这使得量子安全公钥密码体制的设计相对较难。为简化密码体制的设计，可考虑使用通用转换。第五章给出的S构造实际上即是一种通用转换，其可将一种后量子安全的数字签名体制转换为量子安全的数字签名体制，这在一定程度上方便了量子安全数字签名体制的设计。因此，可尝试**研究更多可将后量子安全密码体制转换为对应量子安全密码体制的通用转换**。这种通用转换存在将极大地便于量子安全公钥密码体制的设计，因为现已有相当一部分的后量子安全公钥密码体制。

FOT 作为一种重要的通用转换，其不仅可用于公钥加密体制的设计，还可用于密钥封装

机制的设计[37]。相较 FOT，QFOT 的证明紧致性较差，并且结构有一定不自然的地方，因此 QFOT 还需要进一步的研究。

总之，量子安全公钥密码领域仍存在许多亟待解决的问题，某些论题还需要更深入的探讨。根据以上分析，本人今后研究工作重点列举如下：

1. 尝试构造更普适的现实攻击情形以说明量子叠加态攻击的合理性，从而进一步阐述公钥体制满足量子安全的必要性。

2. 研究不同公钥密码体制的量子安全模型，如基于身份加密体制、密钥封装机制与认证密钥交换的量子安全模型，并论证这些量子安全模型的合理性，为进一步设计其量子安全体制奠定基础。

3. 设计实用的量子安全公钥密码体制。尝试从体制结构、体制安全证明紧致性入手，构造高效且证明简洁的量子安全公钥密码体制。

4. 设计将后量子安全体制转为对应量子安全体制的通用构造，比如通用构造；对已有的通用构造进行再分析，如量子 Fujisaki-Okamoto 转换，尝试对这些通用构造进行改进，使其结构更加自然并简化其安全性证明。

参考文献

[1] Shor P W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[M]. Society for Industrial and Applied Mathematics, 1997.

[2] IBM Research. IBM research advances device performance for quantum computing[EB/OL].http://trove.nla.gov.au/work/163372348?q&versionId=178067881

[3] Katz J, Lindell Y. Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)[M]. Chapman & Hall/CRC, 2007.

[4] Bos J, Ducas L, Kiltz E, etc. CRYSTALS–Kyber: a CCA-secure module-lattice-based KEM[J]. IACR Cryptology ePrint Archive, 2017, 2017: 634.

[5] Hoffstein J, Pipher J, Silverman J H. NSS: An NTRU lattice-based signature scheme[C]. International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2001: 211-228.

[6] Dan B, Özgür Dagdelen, Fischlin M, etc. Random Oracles in a Quantum World[M]. Advances in Cryptology – ASIACRYPT 2011. Springer Berlin Heidelberg, 2011:41-69.

[7] Dan B, Zhandry M. Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World[M]. Advances in Cryptology – CRYPTO 2013. Springer Berlin Heidelberg, 2013:361-379.

[8] Dan B, Zhandry M. Quantum-Secure Message Authentication Codes[M]. Advances in Cryptology – EUROCRYPT 2013. Springer Berlin Heidelberg, 2013:592-608.

[9] Damgård I, Funder J, Nielsen J B, etc. Superposition Attacks on Cryptographic Protocols[C]. International Conference on Information Theoretic Security. Springer International Publishing, 2013:142-161.

[10] Gagliardoni T, Hülsing A, Schaffner C. Semantic Security and Indistinguishability in the Quantum World[M]. Advances in Cryptology – CRYPTO 2016. Springer Berlin Heidelberg, 2016.

[11] Zhandry M. Secure Identity-Based Encryption in the Quantum Random Oracle Model[C]. Cryptology Conference on Advances in Cryptology --- CRYPTO. Springer-Verlag New York, Inc. 2012:758-775.

[12] Targhi E E, Unruh D. Post-quantum security of the Fujisaki-Okamoto and OAEP transforms[C]. Theory of Cryptography Conference. Springer, Berlin, Heidelberg, 2016: 192-216.

[13]Zhandry M. How to Construct Quantum Random Functions[C]. Foundations of Computer Science. IEEE, 2012:679-687.

[14]Unruh D. Revocable Quantum Timed-Release Encryption[M]. Advances in Cryptology – EUROCRYPT 2014. Springer Berlin Heidelberg, 2014:1-76.

[15]Unruh D. Quantum Position Verification in the Random Oracle Model[M]. Advances in Cryptology – CRYPTO 2014. Springer Berlin Heidelberg, 2014:1-18.

[16]程海涛, 韩刚, 钱海峰. 常量噪声下带辅助输入的 LPN 公钥密码[J]. 密码学报, 2017, 4(5):506-516.

[17]杨丹婷, 许春根, 徐磊,等. 理想格上基于身份的签名方案[J]. 密码学报, 2015, 2(4):306-316.

[18]Jin Z, Zhao Y. Optimal key consensus in presence of noise[J]. arXiv preprint arXiv:1611.06150, 2016.

[19]Zhang J, Zhang Z, Ding J, etc. Authenticated key exchange from ideal lattices[C]. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2015: 719-751.

[20]NIST. National institute of standards and technology: Post-Quantum Cryptography. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions

[21]Sipser M. Introduction to the Theory of Computation[J]. Acm Sigact News, 2013, 27(1):27-29.

[22]Bellare M, Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols[C]. ACM Conference on Computer and Communications Security. ACM, 1993:62-73.

[23]Nielsen M A, Chuang I L. Quantum Computation and Quantum Information, 10th Anniversary Edition[J]. International Journal of Parallel Emergent & Distributed Systems, 2011, 21(1):1-59.

[24]Strang G. Introduction to linear algebra[M]. Wellesley, MA: Wellesley-Cambridge Press, 1993.

[25]Bellare M, Kilian J, Rogaway P. The Security of Cipher Block Chaining[M]. Advances in Cryptology — CRYPTO ’94. Springer Berlin Heidelberg, 1994:341-358.

[26] Grover L K. A fast quantum mechanical algorithm for database search[C]. Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM, 1996: 212-219.

[27] Pointcheval D, Stern J. Security proofs for signature schemes[C]. International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1996: 387-398.

[28] Ran C, Krawczyk H. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels[M]. Advances in Cryptology — EUROCRYPT 2001. Springer Berlin Heidelberg, 2001:453-474.

[29] Lamacchia B, Lauter K, Mityagin A. Stronger security of authenticated key exchange[C]. International Conference on Provable Security. Springer-Verlag, 2007:1-16.

[30] Cash D, Hofheinz D, Kiltz E, etc. Bonsai Trees, or How to Delegate a Lattice Basis[M]. Advances in Cryptology – EUROCRYPT 2010. Springer Berlin Heidelberg, 2010:523-552.

[31] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions[C]. Proceedings of the fortieth annual ACM symposium on Theory of computing. ACM, 2008: 197-206.

[32] Fujisaki E, Okamoto T. Secure Integration of Asymmetric and Symmetric Encryption Schemes[J]. Journal of Cryptology, 2013, 26(1):80-101.

[33] Benor M. Probabilistic algorithms in finite fields[J]. Siam Journal on Computing, 2006, 9(2):273-280.

[34] Unruh D. Non-Interactive Zero-Knowledge Proofs in the Quantum Random Oracle Model[M]. Advances in Cryptology - EUROCRYPT 2015. Springer Berlin Heidelberg, 2015:755-784.

[35] Ebrahimi E. Quantum Collision-Resistance of Non-uniformly Distributed Functions[C]. Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings. Springer, 2016, 9606: 79.

[36] Brassard G, Høyer P, Tapp A. Quantum cryptanalysis of hash and claw-free functions[J]. Acm Sigact News, 1997, 28(2):14-19.

[37] Hofheinz D, Hövelmanns K, Kiltz E. A Modular Analysis of the Fujisaki-Okamoto Transformation[M]. Theory of Cryptography. 2017:341-371.

[38] Shoup V. Sequences of Games: A Tool for Taming Complexity in Security Proofs[J]. Iacr Cryptology Eprint Archive, 2004, 2004.

附录

A. 相关密码体制定义

伪随机函数. 设PRF: $K \times D \to R$是一个函数，其中K是F的种子(seed)域，D是函数的定义域，R是函数的值域。记RF: $D \to R$是一个包含所有$D \to R$函数的函数簇，从RF均匀抽取得函数称为真随机函数。记A^O是可问询预言机O的攻击者 A。若对于任意足够大的安全参数n，任何 PPT 攻击者A^O都有：

$$\left|\Pr_{k\leftarrow K}\{A^{F(k,\cdot)}(1^n)=1\}-\Pr_{R\leftarrow RF}\{A^{R(\cdot)}(1^n)=1\}\right|\le \mathrm{negl}(n)$$

则称PRF是一个伪随机函数。伪随机体现在，设攻击者原本是与真随机函数交互，当把该真随机函数替换成伪随机函数时，攻击者的行为基本不变（仅出现可忽略的行为变化）。

私钥加密体制. 一个私钥加密（也称对称加密）体制由两个算法(E,D)组成。对于任意一个足够大的参数$k \in N$:

- 加密算法 E 是一个 PPT 算法，其运行时间是关于k的多项式。E 的输入包括密钥$sk \in KSP$，明文$x \in MSP$，输出对应的密文$y \leftarrow Enc_{sk}(x)$（若显式表达随机性，则表示为$r \leftarrow COIN, y := Enc_{sk}(x;r)$）. KSP、MSP、COIN分别为该对称加密的密钥空间、明文空间与随机性空间，三个空间由参数k唯一确定。

- 解密算法 D 是一个确定性的多项式时间算法(运行时间是关于k的多项式)，其输入包括密钥$sk \in KSP$与密文$c \in \{0,1\}^*$，输出明文$x \in MSP$（表示为$x := D_{sk}(c)$）或是特殊符号⊥。

私钥加密体制应满足正确性：对于任意的足够大的k，任意的$sk \in KSP$、$x \in MSP$，有$D_{sk}\left(E_{sk}(x)\right)=x$.

公钥加密体制. 一个公钥加密体制（也称非对称加密）由三个算法(K,E,D)组成.对于任意足够大的参数$k \in N$:

- 密钥生成算法 K 是一个 PPT 算法（运行时间是关于k的多项式），其输入1^k，输出公钥私钥对(pk, sk).该过程表达为$(pk, sk) \leftarrow K(1^n)$

- 加密算法 E 是一个 PPT 算法（运行时间是关于k的多项式），其输入包括公钥pk，明文$x \in MSP$，输出密文$c \leftarrow E_{pk}(x)$（若显式表达随机性，则表示为$r \leftarrow COIN, y := Enc_{pk}(x;r)$）。MSP、COIN分别为该非对称加密的明文空间与随机性空间，两个空间由参数k唯一确定。

- 解密算法 D 是一个确定性算法（运行时间是关于k的多项式），其输入包括密钥sk，密文$y \in \{0,1\}^*$，返回对应的明文$x := D_{sk}(y)$或返回特殊符号$\perp$

公钥加密体制应满足正确性：对于任意的足够大的k，任意的公私钥对(pk, sk)、$x \in MSP$，有$D_{sk}\left(E_{pk}(x)\right) = x$.

数字签名体制. 一个数字签名体制）由三个算法(K,Sign,Ver)组成.对于任意足够大的参数$k \in N$:

- 密钥生成算法 K 是一个 PPT 算法（运行时间是关于k的多项式），其输入1^k，输出公钥私钥对(pk, sk).该过程表达为$(pk, sk) \leftarrow K(1^n)$
- 签名算法 Sign 是一个 PPT 算法（运行时间是关于k的多项式），其输入包括公钥sk，明文$x \in MSP$，输出签名$\sigma \leftarrow Sign_{sk}(x)$（若显式表达随机性，则表示为$r \leftarrow COIN, \sigma := Sign_{sk}(x; r)$）。MSP、COIN分别为该签名体制的明文空间与随机性空间，两个空间由参数k唯一确定。
- 解密算法 Ver 是一个确定性算法（运行时间是关于k的多项式），其输入包括密钥pk，明文签名对(x, σ)，如果σ是m的签名则返回 1，否则返回 0。

数字签名体制应满足正确性：对于任意的足够大的k，任意的公私钥对(pk, sk)、$x \in MSP$，有$Ver_{pk}\left(Sign_{sk}(x)\right) = 1$.

B. 第 3 章命题证明

本节给出第三章相关引理的证明及事件分析。在证明这些引理之前首先给出其它相关的引理：

引理 B.1 (切尔诺夫界) 设$X_1, \ldots, X_n$是n次泊松实验[1]的随机变量，设$X = \sum_{i=1}^{n} X_i$且$E[X] = \mu$，则对于任意的$0 < \delta \leq 1$，有:

$$\Pr\{X \geq (1+\delta)\mu\} < \exp\left(-\frac{\mu\delta^2}{2}\right)$$

$$\Pr\{X \geq (1-\delta)\mu\} < \exp\left(-\frac{\mu\delta^2}{2}\right)$$

引理 B.2（生日攻击界,经典版本[25,命题 A.1]） X，Y是两个集合，其中$|Y| = n$，设 F 是所有$X \to Y$的函数的集合。对于任意的概率多项式经典攻击者 A，给定攻击者对f的问询（至多问询q次），存在常数 c，有如下式子成立：

[1] n 次泊松实验是指独立进行 n 次实验，每次实验的结果X_i是 0-1 二值的布尔随机变量。$X_1, \ldots, X_n$不一定是同分布。

$$\Pr_{f\leftarrow R F}\{f(x_1)=f(x_2)\mid (x_1,x_2)\leftarrow A^f()\}\le c\cdot\frac{q^2}{N}$$

引理 B.2 指出，对于经典攻击者，寻找随机函数的碰撞概率是可忽略的（对函数只求值一次的情况），该定理对部分的碰撞（比如，前l-位的碰撞）也成立。在对函数求值多次的情况下，通过切尔诺夫界可以分析出，适当地选取限定的次数会使找出碰撞的概率也是可忽略的。

对于量子攻击者，也有类似的定理成立：

引理 B.3.（量子碰撞攻击[36,定理 5]）X，Y是两个集合，其中$|Y|=n$，设$f: X\to Y$为一个函数。存在概率多项式量子攻击者 A，A 对f求值（量子叠加态求值）期望次数$\Theta\left(\sqrt[3]{N}\right)$次后，以大于$\frac{1}{2}$的概率找到一个碰撞。

引理 B.3 一定程度上解释了在ID*的碰撞阶段中为何选取$c\le\lceil\sqrt[3]{2^l}\rceil$。通过选取该c值，可以保证在限定求值次数内，经典攻击者以可忽略概率找出碰撞而量子攻击者以显著的概率找出碰撞。

引理 B.4 ([21]) 记A,B,F_1,F_2为定义在同一概率空间中的四个事件。若$\Pr\{F_1\}=\Pr\{F_2\}$并且$\Pr\{A\cap\neg F_1\}=\Pr\{B\cap\neg F_2\}$，则有:

$$|\Pr\{A\}-\Pr\{B\}|\le\Pr\{F_1\}(=\Pr\{F_2\})$$

引理 3.1 在经典随机预言机模型下，对于任意的经典攻击者 A，如果 ID 满足完备性和可满足性，那么ID*满足完备性和可靠性。

证明：

由ID*的构造（设 n 为协议的安全参数）

$$\Pr\{\text{A“攻破”ID*协议}\}=\Pr\{\text{A 至少找出}\tfrac{r}{4}\text{个 H 的l-碰撞}\}+\Pr\{\text{A“攻破”ID 协议}\}$$

(“攻破”是指攻击者 A 欺骗V*通过了身份验证)

由于假设了 ID 协议是安全的（满足可靠性），因此：$\Pr\{\text{A“攻破” ID 协议}\}\le\mathrm{negl}(n)$

接下来绑定 $\Pr\{\text{A 至少找出}\frac{r}{4}\text{个 H 的l-碰撞}\}$。在碰撞阶段中，r次循环里的每一次的预言机都不同（因为选了不同的k_i，每一循环的哈希函数都不同）。第i次循环，定义随机变量X_i为：$X_i=1$指攻击者在此次找到一个以上的l-碰撞,否则$X_i=0$。攻击者在一次循环内只能进行$\lceil\sqrt[3]{2^l}\rceil$次问询，而由于是l-碰撞，这意味着要找碰撞的域的大小为2^l。由引理 B.2 可以得到:$\Pr[X_i=1]\le c\cdot\frac{\left(\sqrt[3]{2^l}\right)^2}{2\cdot 2^l}=c\cdot\frac{1}{2\cdot\sqrt[3]{2^l}}\le c\cdot\frac{1}{2\cdot\sqrt[3]{n}}$

设$X=\sum_{i=1}^{r}X_i$，则在此定义下，$\Pr\{\text{A 至少找出}\frac{r}{4}\text{个 H 的l-碰撞}\}$就等于$\Pr\{X>\frac{r}{4}\}$。

由于r次循环可看作是 r 次泊松实验,由期望的线性属性有$E[X]=\sum_{i=1}^{r}\le c\cdot\frac{r}{2\cdot\sqrt[3]{n}}$,再由引理 B.1 可以得到：

$$\Pr\left\{X\ge\frac{r}{4}\right\}=\Pr\{\left(1+\frac{\sqrt[3]{n}}{2c}-1\right)\cdot\frac{c\cdot r}{2\cdot\sqrt[3]{n}}\}$$

$$<\exp\left(-\frac{\frac{c\cdot r}{2\cdot\sqrt[3]{n}}\cdot\left(\frac{\sqrt[3]{n}}{2c}-1\right)^{2}}{2}\right)$$

$$<\exp(-\frac{r\sqrt[3]{n}}{16c})$$

由于选定了$r=\mathrm{poly}(n)$且为c常数，因此 Pr{ A 至少找出$\frac{r}{4}$个 H 的l-碰撞}是一个可忽略量。综上，Pr{A “攻破” ID*协议}是可忽略量。因此证明ID*在经典随机预言机下是安全的。

引理 3.3 用任意的抗碰撞哈希函数实例化ID*后，对于任意的经典攻击者，ID*满足完备性和可靠性；对于量子攻击者，ID*不满足可靠性，即存在针对ID*的量子攻击。

证明：

由于实例化后的哈希函数具有抗碰撞属性（攻击者以可忽略的概率找到任意一组碰撞）。因此对于经典攻击者，其证明过程与引理 3.1 类似，这里不做赘述。

实例化后的哈希函数可被攻击者在本地进行求值。对于量子攻击者，由[23]，可将哈希函数转换构造为相应的可量子叠加态求值的量子算法。由引理 B.3，存在量子攻击者 A，在ID*碰撞阶段的每一轮以大于$\frac{1}{2}$的概率找出一个l-碰撞，类似引理 3.2，通过切尔诺夫界，有：

$$\Pr\left\{X\ge\frac{r}{4}\right\}=1-\Pr\left\{X<\frac{r}{4}\right\}>1-\Pr\left\{X<\left(1-\frac{r}{2}\right)\cdot\frac{r}{2}\right\}>1-\exp\left(-\frac{r}{16}\right)$$

显然最后一个量是显著概率（$r=\mathrm{poly}(n)$）。因此存在量子攻击者，在限定的求值次数内可找出足够的碰撞，Pr{ A 至少找出$\frac{r}{4}$个 H 的l-碰撞是一个显著量，即 A 以显著的概率攻破ID*。

定理 3.4. 如果S_c对量子攻击者满足 EUF-cCMA，且PRF在经典问询下是安全的，则通过合适地选择N,N'，S*满足 EUF-cCMA 但不满足 EUF-qCMA，即S*可被量子选择明报文攻击攻破。

证明:

令N'为一个关于安全参数n的指数增长的整数（即，$N'=O(\exp(n))$）并且设N是这样一个数：它等于最小的，大于$4N'^2$的某个2的幂次，即$N=2^t,2^t>4N'^2,2^{t-1}\le 4N'^2$。首先通过一系列的安全游戏来证明S*满足 EUF-cCMA。定义事件WIN_i为在安全游戏G_i

中攻击者胜出，即G_i输出 1。设$\Pr\{G_{A,S}^{EUF-CMA}(1^n)=1\}=\varepsilon$。

G_0：令$G_0=G_{A,S}^{EUF-CMA}$，则$\Pr\{WIN_0\}=\varepsilon$。

G_1：在G_0的基础上，在运行攻击者前，先均匀选取一个随机函数R，将S^*中签名算法Sign的$s_1 \leftarrow PRF(k,m \bmod p)$改为$s_1=R(m \bmod p)$。由PRF的伪随机性可知，$\Pr\{WIN_1\}\leq \varepsilon + negl^{PRF}(n)$。

G_2：在G_1的基础上，将$s_1=R(m \bmod p)$改为$s_1=R(m)$且令$s_2=0$（无论p是否等于m）。

定义事件 Bad 为：攻击者问询（对签名预言机问询）过p或问询过两个模p相等的明文m_0,m_1（即$m_0\equiv m_1 \bmod p$）。由协议的构造可知，在G_1和G_2中 Bad 发生的概率是相同的，且如果两个游戏下的 Bad 都不发生那么攻击者 A 在两个游戏中的胜出概率是相同的，因此由引理 B.4，有:

$$|\Pr\{WIN_1\}-\Pr\{WIN_2\}|\leq \Pr\{Bad\}$$

为了简洁，$\Pr\{Bad\}$的概率分析将在后面给出。具体地，对于q次问询的攻击者，$\Pr\{Bad\}\leq O(\frac{q^2\log N'}{N'})$。

现证明$\Pr\{WIN_2\}$是可忽略的。具体地，若$\Pr\{WIN_2\}$是一个显著量，则可构造一个针对S_c的高效经典选择报文攻击，通过反证法（已假设S_c可抗量子攻击者的经典选择明文攻击）可知，$\Pr\{WIN_2\}$是一个可忽略量。

设$B^{Sign_c(sk,\cdot)}$是一个针对S_c的 cCMA 攻击者（B没有pk），B获得pk后，进行如下操作:

- 均匀选取一个随机函数R，$p \leftarrow RPrime(N')$，运行A(pk)
- 若A发出签名问询m，向签名预言机$Sign_c(sk,\cdot)$问询关于m的签名，得到应答σ，返回签名应答$(\sigma,R(m),0)$
- A发出伪造$(m^*,(\sigma^*,s_1^*,s_2^*))$后，B返回伪造$(m^*,\sigma^*)$

$B^{Sign_c(sk,\cdot)}$完美模拟了G_2的环境给A，若A的伪造是一个合法的报文-签名对，那么B返回的伪造也是合法的。由S_c的 EUF-cCMA 属性，可知$\Pr\{WIN_2\}\leq negl^{Sign}(n)$。

综上所述，可知$\varepsilon \leq negl^{PRF}(n)+O\left(\frac{q^2\log N'}{N'}\right)+negl^{Sign}(n)$，即ε也是个可忽略量，从而得到$S^*$是满足 EUF-cCMA 的。

对于可对签名预言机进行量子叠加态问询的量子攻击者 A，由N',N的选择，A 可使用[NC00]中的量子周期查找算法，通过一次对签名预言机的量子叠加态问询即可S^*中的p求出，得到p后向签名预言机问询p的签名，签名中的s_2部分即是私钥，获得私钥的

攻击者可随意构造报文-签名对。所以S^*无法满足 EUF-qCMA。

对事件 Bad 的分析. 事件 Bad 定义为：攻击者问询（对签名预言机问询）过p或问询过两个模p相等的明文m_0, m_1（即$m_0 \equiv m_1 \bmod p$）。现分析 Bad 的发生概率。

设第$i(\in \{1, \dots, q\})$次问询后，Bad 仍未发生。这意味着在前i次问询中对于不同的m，所有的s_1都是均匀随机且互相独立的，所有的s_2都为 0，即攻击者没有关于p的任何信息。现考虑在第$i+1$次问询时 Bad 发生的概率。

在攻击者发出第$i+1$次问询时，该问询与前面i个问询构成i个差，由N的设定知，这些差至多为$8N'^2$，即这些差至多可被在$\left[\frac{N'}{2}, N'\right]$中两个不同的素数除（可被三个以上素数除则意味着某个明文的大小为$O(N'^3)$，这不符合N的设定）。再由素数的分布可知，任意一个差可被p整除的概率为$2 \cdot O\left(\frac{\log N'}{N'}\right) = O\left(\frac{\log N'}{N'}\right)$，因此这些这$i$个差其中一个可被$p$整除的概率为$O(\frac{i \log N'}{N'})$，即在第$i+1$次问询时 Bad 发生的概率为$O(\frac{i \log N'}{N'})$。

由递推知，攻击者发出q次问询后 Bad 仍不发生的概率为：

$$\sum_{i=1}^{q} O\left(\frac{i \log N'}{N'}\right) = O\left(\frac{q^2 \log N'}{N'}\right)$$

C. 第 5 章命题证明

继续对定理 5.1 的证明（从G_4开始）：

设$h_k^* = H(pk, m_k^*, r_k^*)$为攻击者输出伪造$\{(m_1^*, r_1^*, \sigma_1^*), \dots, (m_{q+1}^*, r_{q+1}^*, \sigma_{q+1}^*)\}$对应$m, r$部分的哈希值。由于在$G_1$中已要求任意的两个$(m_k^*, r_k^*)$都不是$H(pk_H, \cdot, \cdot)$的碰撞，因此所有的$(h_k^*, \sigma_k^*)$都各不相同。令$Hash^i$为一个集合，该集合包括所有的用于应答第$i$次问询的$\hat{h}_j^i$值（详见$G_3$），并令集合$Hash = \bigcup_{i=1}^{q} Hash^i$。

$\{h_1^*, \dots, h_{q+1}^*\}$与$Hash$的关系可分为两种情况：1. 所有的$h_k^*$都各不相同并且被包含在$Hash$中 2. 至少一个$h_k^*$不在$Hash$中。为了简洁，分情况 2 的发生概率将在本节的最后给出。可以证明情况 2 以可忽略的概率（记为$negl^{S_c}(n)$）发生，因此情况 1 下攻击者输出$q+1$个伪造的概率为$\epsilon_{4.1} = \epsilon_4 - negl^{S_c}(n) \geq \epsilon_0 - negl^{CH}(n) - negl^{rand}(n) - \frac{1}{2}p - negl^{S_c}(n)$。为了简洁，记为$\epsilon_{4.1} \geq \epsilon_0 - negl(n) - \frac{1}{2}$。

G_5. 在G_4的基础上，模拟者运行攻击者前先猜测一个值i^*，即猜测$Hash^{i^*}$中有两个不同的h_k^*。注意，由鸽笼原理，i^*必然存在。不失一般性，设该不同的h_k^*为h_0^*, h_1^*，设j_b^*为：$h_b^* =$

$\hat{h}_{j_b^*}^{i^*}, b = 0,1$。

由于攻击者进行q次问询，模拟者猜中i^*的概率为$\frac{1}{q}$，所以$\epsilon_5 = \frac{\epsilon_{4.1}}{q}$。

G_6. 在G_5的基础上，在攻击者进行第i^*次问询的时候，测量$O_{i^*}(m)$（定义在G_3中）以获得j^*。注意，在攻击者发出第i^*次问询时，模拟者只需要对$\hat{h}_{j^*}^{i^*}$(设$\hat{h}_{j^*}^{i^*} = h_0$)进行$Sign_c$签名(因为测量了$O_{i^*}(m)$并且测量结果为$j^*$)，模拟者并不需要对$h_1$进行 $Sign_c$签名。

由于O_{i^*}的值域为$\{1, \dots, l\}$，由[7, 引理 2.1]，有$\epsilon_6 \geq \frac{\epsilon_5}{l}$（该引理指出，设量子算法 A 运行结束后以$\varepsilon$的概率输出某一结果x。若在 A 运行中的某一时刻对 A 进行部分测量，其中可能的测量结果有k种，则最后 A 仍然输出x的概率大于等于$\frac{\varepsilon}{k}$）。

G_7. 在G_6的基础上，在运行攻击者 A 前事先猜测j^*，然后检查该猜测是否正确（通过G_6中测量的结果）。显然$\epsilon_7 = \frac{\epsilon_6}{l} \geq \frac{\epsilon_0}{ql^2} - \frac{negl(n)}{ql^2} - \frac{1}{2pql^2}$。

为了方便分析，G_7将完整表述在图 C.1:

G_7

1. $i^* \leftarrow \{1, \dots, q\}, j^* \leftarrow \{1, \dots, l\}$
2. $(sk = (pk_H, sk_c), pk = (pk_H, pk_c)) \leftarrow G(1^n)$, 设$sk_H$为$CH$的私钥（模拟者拥有）
3. 设$l = 2C_0qp$, 对于$i = 1, \dots, q$, $j = 1, \dots, l$，均匀随机抽取$\hat{h}_j^i$，并设$\hat{\sigma}_j^i \leftarrow Sign_c(sk_c, \hat{h}_j^i)$，分别抽取$q$个两两独立函数$O_i, T_i (i = 1, \dots, q)$。
4. 对于第$i \neq i^*$次签名叠加态问询中的每一个m：
   - $h_m^i = \hat{h}_{O_i(m)}^i, \sigma_m^i = \hat{\sigma}_{O_i(m)}^i, t_m^i = T_i(m)$
   - $r_m^i = Inv(sk_H, h_m^i; t_m^i)$
   - 返回(r_m^i, σ_m^i)
5. 对于第$i = i^*$次签名叠加态问询:
   - 测量$O_i(m)$得到j
   - 如果$j = j^*$:进行第 4 步的操作。
   - 否则停止模拟。
6. A 输出$\{(m_1^*, r_1^*, \sigma_1^*), \dots, (m_{q+1}^*, r_{q+1}^*, \sigma_{q+1}^*)\}$

图 C.1 G_7的描述

现构造攻击者 B，B 目标为破坏S_c的 EUF-RMA 属性。B 为攻击者 A 模拟一个G_7的环境并尝试借助 A 以攻击S_c。B 首先获得S_c的pk与$(q-1)l+1$个S_c的明文-签名对，在模拟G_7时，从输入的$(q-1)l+1$个明文-签名对随机抽取一个作为$h_{j^*}^{i^*}, \sigma_{j^*}^{i^*}$。剩下的$(q-1)l$个作为第三

步的$(\hat{h}_j^i, \hat{\sigma}_j^i)(i \neq i^*)$。可以验证 B 完美模拟$G_7$。

假设 A 最后输出$\{(m_1^*, r_1^*, \sigma_1^*), \dots, (m_{q+1}^*, r_{q+1}^*, \sigma_{q+1}^*)\}$且任意的两个$(m_k^*, r_k^*)$都不是$H(pk_H, \cdot, \cdot)$的碰撞。不失一般性，设在$G_7$中模拟者猜中的是$h_0^*$，则模拟者 B 仅需要用到$h_0^*$的签名$\sigma_0^*$而并未用到$h_1^*$的签名$\sigma_1^*$，因此$(h_1^*, \sigma_1^*)$即是一个$S_c$的合法伪造且 B 的输入不包括$(h_1^*, \sigma_1^*)$。所以 B 可以以$\epsilon_7 \geq \frac{\epsilon_0}{ql^2} - \frac{negl(n)}{ql^2} - \frac{1}{2pql^2}$的概率攻破$S_c$的 EUF-RMA 属性，若$\epsilon_0$是不可忽略量，则$\epsilon_7$也是不可忽略量，由反证法知$\epsilon_0$是可忽略量，即对于任意的攻击者 A，有$G_{A,S}^{EUF-qCMA}(1^n) \leq \frac{1}{negl(n)}$，因此S满足 EUF-qCMA 属性。

G_4中情况 2 的分析：情况 2 为：至少一个h_k^*不在Hash中。若情况 2 以不可忽略的概率发生，则可以构造一个攻击者 B，B 模拟为 A 模拟G_4的环境以攻击S_c的 EUF-RMA 属性：B 首先获得S_c的pk与ql个S_c的明文-签名对以作为各个$(\hat{h}_j^i, \hat{\sigma}_j^i)$，在攻击者 A 返回$q+1$个伪造$(m_k^*, r_k^*, \sigma_k^*)$后，B 计算$h_k^* = H(pk_H, m_k^*, r_k^*), k = 1, \dots, q$，然后寻找其中满足$h_k^* \notin Hash$，如果找到满足$h_k^* \notin Hash$的k，B 输出$(h_k^*, \sigma_k^*)$即可。由以上分析知，情况 2 发生的概率可忽略。

D. 第 6 章命题证明

命题 D.1. $k-1$阶随机多项式是k-wise 独立函数簇。

证明：$k-1$阶多项式的形式为$f(x) = a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$，其中系数$a_i$是均匀选取的（设多项式的值域大小为N）。

对于任意k个互不相同的x_i与k个y_i：

$$\Pr_f\{f(x_1) = y_1, \dots, f(x_k) = y_k\}$$

$$= \Pr_f\left\{ \begin{bmatrix} 1 & \cdots & x_1^{k-1} \\ \vdots & \ddots & \vdots \\ 1 & \cdots & x_k^{k-1} \end{bmatrix} \begin{bmatrix} a_0 \\ \vdots \\ a_{k-1} \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_k \end{bmatrix} \right\}$$

记$X = \begin{bmatrix} 1 & \cdots & x_1^{k-1} \\ \vdots & \ddots & \vdots \\ 1 & \cdots & x_k^{k-1} \end{bmatrix}$，$X_i$为将X中第i列替换为$\begin{bmatrix} y_1 \\ \vdots \\ y_k \end{bmatrix}$的矩阵。由范德蒙德矩阵知，$|X| \neq 0$，再由克莱姆法则知，$a_i = \frac{|X_{i+1}|}{|X|}$，由f的构造知，所有的$a_i$都均匀选取且互相独立，所以：

$$\Pr_f\left\{ \begin{bmatrix} 1 & \cdots & x_1^{k-1} \\ \vdots & \ddots & \vdots \\ 1 & \cdots & x_k^{k-1} \end{bmatrix} \begin{bmatrix} a_0 \\ \vdots \\ a_{k-1} \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_k \end{bmatrix} \right\}$$

$$= \Pr_f\left\{a_0 = \frac{|X_1|}{|X|}, \dots, a_{k-1} = \frac{|X_k|}{|X|}\right\} = \frac{1}{N^k}$$

对于$l \le k$，由X的秩有类似结果成立。因此$k-1$阶随机多项式是k-wise 独立函数簇

引理 D. 2. (02HA 引理，[14]) 令$H:\{0,1\}^* \to \{0,1\}^n$为一个随机预言机。令$A_0$是一个预言机算法，其对H进行$q_0$次的问询。设$A_1$也为一个预言机算法，$A_1$使用$A_0$停机后的量子状态并向H进行$q_1$次的问询。设C也是一个预言机算法，给定C输入$(j, B, x)$，C运行$A_1^H(x, B)$，当$A_1^H$对H发出第i次问询后，C测量该问询并将测量结果输出。令:

$$P_A^1 := \Pr\{b' = 1 | m \leftarrow A_0^H(), x \leftarrow \{0,1\}^l, b' \leftarrow A_1^H(x, H(x||m))\}$$

$$P_A^2 := \Pr\{b' = 1 | m \leftarrow A_0^H(), x \leftarrow \{0,1\}^l, B \leftarrow \{0,1\}^n, b' \leftarrow A_1^H(x, B)\}$$

$$P_C := \Pr\left\{x' = x, m = m' \middle| \begin{matrix} m \leftarrow A_0^H, x \leftarrow \{0,1\}^l, B \leftarrow \{0,1\}^n, j \leftarrow \{1, \dots, q_1\} \\ x'||m' \leftarrow C^H(j, B, x) \end{matrix}\right\}$$

则有:

$$\left|P_A^1 - P_A^2\right| \le 2q_1\sqrt{P_C} + q_0 2^{-\frac{l}{2}+2}$$

继续对定理 6. 1 的证明:

由于模拟者不再需要sk来模拟解密预言机，因此对e^*的生成方式作一定的修改即可将该安全性证明规约到Π^{asy}的单向安全性。G_5在G_4基础上，将e^*的生成方式修改为与$H(r^*||c^*)$无关（由于在规约中e^*是作为模拟者的挑战密文，模拟者无法控制该密文加密中生成的随机性）。

G_5:

1. $a^* \leftarrow KSP^{sy}, d^* \leftarrow MSP^{sy}, i \leftarrow \{1, \dots, q_{o2h}\}$
2. 运行$A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}(pk)$直到$A$对$G \times H'$发出第$i$次问询:
   $(m_0, m_1) \leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}(pk)$
   $c^* \leftarrow E^{sy}(a^*, m_b), e^* \leftarrow E^{asy}(pk, r^*)$
   $b' \leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}(pk, (e^*, c^*, d^*))$
3. 测量A对$G \times H'$第i次问询中的$\hat{r}$部分，设测量结果为$\hat{r}$。
4. 如果$r^* = \hat{r}$，返回 1，否则返回 0。

与前面证明攻击者无法区分G_1与G_2的方法类似，此处可借助引理 D.2 来证明$|\Pr\{G_4 = 1\} - \Pr\{G_5 = 1\}|$是可忽略的。首先构造两个预言机算法$A_0^H, A_1^H$（两个算法都需要自行构造独立函数$G, H'$，为了简洁忽略该步骤）:

$\mathbf{A_0^H}$:

1. $(pk, sk) \leftarrow K(1^n), b \leftarrow \{0,1\}, a^* \leftarrow KSP^{sy}, d^* \leftarrow MSP^{asy}, i \leftarrow \{1, \dots, q_{o2h}\}$
2. 运行$A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}(pk)$直到$A$对$G \times H'$发出第$i$次问询:

$(m_0, m_1) \leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}(pk), c^* \leftarrow E^{sy}(a^*, m_b)$

3. 返回c^*。

$\mathbf{A_1^H(r^*, h^*)}$:

1. 如果$i > q_{0GH'}$（$q_{0GH'}$为A_0^H中A对预言机$G \times H'$的问询次数）:

运行$A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}(pk)$直到$A$对$G \times H'$发出第$i - q_{0GH'}$次问询:

$e^* \leftarrow E^{asy}(pk, r^*; h^*)$,

$b' \leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}(e^*, c^*, d^*)$

2. 测量A对$G \times H'$第i次问询中的$\hat{r}$部分，设测量结果为$\hat{r}$。
3. 如果$r^* = \hat{r}$，返回 1, 否则返回 0。

$\mathrm{A_1^H}$使用$\mathrm{A_0^H}$结束时的量子态，这意味着$\mathrm{A_1^H}$拥有$\mathrm{A_0^H}$在运行中生成的随机性与输出。注意，$\mathrm{A_0^H}$有可能会在构造挑战密文$\mathrm{c^*}$之前结束（即$\mathrm{i \le q_{0GH'}}$），在此情况下，$\mathrm{A_1^H}$会直接进行测量而不再与攻击者$\mathrm{A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}}$交互。这是可行的，因为实际上可将$\mathrm{A_0^H}$与$\mathrm{A_1^H}$整合为同一个量子攻击者，分开描述仅为了与引理 D.2 保持形式上的相同性。由$\mathrm{A_0^H, A_1^H}$的构造知，若$\mathrm{(r^*, h^*)}$中的$\mathrm{h^* = H(r^* || c^*)}$，则整个$\mathrm{A_0^H}$与$\mathrm{A_1^H}$在模拟$\mathrm{G_4}$，如果$\mathrm{h^*}$是真随机值，则$\mathrm{A_0^H}$与$\mathrm{A_1^H}$在模拟$\mathrm{G_5}$。即$\mathrm{P_A^1 = Pr\{G_4 = 1\}, P_A^2 = Pr\{G_5 = 1\}}$

为了使用引理 D.2，现构造$\mathrm{G_6}$使得$\mathrm{Pr\{G_6 = 1\} = P_C}$，$\mathrm{G_6}$的描述在图 D.1。由引理 D.2，有$\mathrm{|Pr\{1 \leftarrow G_5\} - Pr\{1 \leftarrow G_6\}| \le 2q_1\sqrt{Pr\{1 \leftarrow G_7\}} + q_0 2^{-\frac{n_1}{2}+2}}$。

可将$\mathrm{G_6, G_7}$规约到$\mathrm{\Pi^{asy}}$的单向安全性，即引理 D.3。

引理 D. 3. 如果公钥加密体制$\mathrm{\Pi^{asy}}$是单向安全的，则$\mathrm{Pr\{G_5 = 1\} \le \frac{1}{2} + negl^{asy}(n)}$且$\mathrm{Pr\{G_6 = 1\} \le \frac{1}{2} + negl^{asy}(n)}$。

引理 D.3 的证明在后面给出。

综上所述，有：

$$\mathrm{Pr\{1 \leftarrow G_0\} \le \frac{1}{2} + negl^{sy}(n) + O\left(\frac{(q_H + q_{dec} + 1)^{\frac{9}{5}}}{2^{\frac{\gamma}{5}}}\right) + 2q_{o2h}\sqrt{negl^{asy}(n) + 2q_1\sqrt{negl^{asy}(n)} + q_0 2^{-\frac{n_1}{2}+2}}}$$

G_6[2]:

1. $a^* \leftarrow KSP^{sy}, d^* \leftarrow MSP^{asy}, i \leftarrow \{1,\dots,q_{o2h}\}$（$q_{0GH'}$为$A_0^H$中$A$对预言机$G \times H'$的问询次数）
2. 构造$2(q_H + q_{dec} + 1)$-wise, $2(q_H + q_{dec} + 1)$-wise，$2(q_{H'} + q_{dec} + 1)$-wise 独立函数
3. 运行$A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}(pk)$直到$A$对$G \times H'$发出第$i$次问询:

$(m_0, m_1) \leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}(pk), c^* \leftarrow E^{sy}(a^*, m_b)$

4. 生成c^*后，$r^* \leftarrow MSP^{asy}, h^* \leftarrow COIN^{asy}, j \leftarrow \{1,\dots,q_1\}$（$q_1$为$A_1^H$中$A$对预言机$H$的问询次数）
5. 继续运行$A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}$直到 A对H发出第j次问询：

   如果$i > q_{0GH'}$：

   运行$A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}(pk)$直到$A$对$G \times H'$发出第$i - q_{0GH'}$次问询:

   $e^* \leftarrow E^{asy}(pk, r^*; h^*)$

   $b' \leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^*(sk,\cdot)\rangle}(e^*, c^*, d^*)$

   测量A对$G \times H'$第i次问询中的$\hat{r}$部分。

   测量A对H第j次问询中的$\hat{r}||\hat{c}$部分，设测量结果为$(\hat{r}, \hat{c})$
6. 如果$\hat{r} = r^*$且$\hat{c} = c^*$, 则返回 1，否则返回 0。

图 D.1 G_6的描述

即Π^{QFO}满足 IND-qCCA 属性，定理 5.6 得证。

引理 6.4. 如果对称加密体制Π^{sy}是一次安全的，则$\Pr\{\mathrm{G}_2 = 1\} \le \frac{1}{2} + \mathrm{negl}^{\mathrm{sy}}(\mathrm{n})$。

证明：现构造攻击者A^{sy}，该攻击者满足$\Pr\{\mathrm{G}^{\mathrm{OT}}_{\mathrm{A}^{\mathrm{sy}},\Pi^{\mathrm{sy}}} = 1\} = \Pr\{\mathrm{G}_2 = 1\}$：

$\mathrm{A}^{\mathrm{sy}}(1^{\mathrm{n}})$:

1. 运行$\mathrm{G}^{\mathrm{asy}}(1^{\mathrm{n}})$得到$(\mathrm{pk}, \mathrm{sk})$，构造$2(\mathrm{q_H} + \mathrm{q_{dec}} + 1)$-wise、$2(\mathrm{q_{H'}} + \mathrm{q_{dec}} + 1)$-wise、$2(\mathrm{q_G} + \mathrm{q_{dec}} + 1)$-wise 独立函数$\mathrm{H}, \mathrm{H}', \mathrm{G}$，运行$\mathrm{A}^{|\mathrm{H}\rangle,|\mathrm{G}\rangle,|\mathrm{H}'\rangle,|\mathrm{D}^*(\mathrm{sk},\cdot)\rangle}(\mathrm{pk})$。
2. A输出挑战明文$(\mathrm{m}_0, \mathrm{m}_1)$后，$\mathrm{A}^{\mathrm{sy}}$输出$(\mathrm{m}_0, \mathrm{m}_1)$，收到$\mathrm{c}^*$后，依次执行：
   a) $\mathrm{r}^* \leftarrow \mathrm{MSP}^{\mathrm{asy}}, \mathrm{d}^* \leftarrow \{0,1\}^{\mathrm{n}_1}$
   b) $\mathrm{e}^* \coloneqq \mathrm{E}^{\mathrm{asy}}(\mathrm{pk}, \mathrm{r}^*; \mathrm{H}(\mathrm{r}^*||\mathrm{c}^*))$
   c) 返回$(\mathrm{e}^*, \mathrm{c}^*, \mathrm{d}^*)$给A
3. A输出b'后，A^{sy}也输出b'。

在$\mathrm{G}^{\mathrm{OT}}_{\mathrm{A}^{\mathrm{sy}},\Pi^{\mathrm{sy}}}$中，$\mathrm{c}^*$的生成步骤为：$\mathrm{a}^* \leftarrow \mathrm{KSP}^{\mathrm{sy}}, \mathrm{b} \leftarrow \{0,1\}, \mathrm{c}^* \leftarrow \mathrm{E}^{\mathrm{sy}}(\mathrm{a}^*, \mathrm{m_b})$，因此$\mathrm{A}^{\mathrm{sy}}$完美模拟了$\mathrm{G}_2$，因此$\Pr\{\mathrm{G}_2 = 1\} = \Pr\{\mathrm{G}^{\mathrm{OT}}_{\mathrm{A}^{\mathrm{sy}},\Pi^{\mathrm{sy}}} = 1\} \le \frac{1}{2} + \mathrm{negl}^{\mathrm{sy}}(\mathrm{n})$。

[2] 为了安全游戏之间的一致性，G_6的描述包括了i的选取、对$G \times H'$的测量等，实际上在此安全游戏中可以不包含这些操作。

引理 D.3. 如果公钥加密体制Π^{asy}是单向安全的，则$\Pr\{G_5=1\}\leq\frac{1}{2}+\mathrm{negl}^{asy}(n)$且$\Pr\{G_6=1\}\leq\frac{1}{2}+\mathrm{negl}^{asy}(n)$。

证明：现构造攻击者A_5^{asy}，该攻击者满足$\Pr\left\{G^{OW}_{A_5^{asy},\Pi^{asy}}=1\right\}=\Pr\{G_5=1\}$。

$A_5^{asy}(1^n,pk,y)$:

1. $i\leftarrow\{1,\dots,q_{o2h}\}$
2. 构造$2(q_H+q_{dec}+1)$-wise、$2(q_{H'}+q_{dec}+1)$-wise、$2(q_G+q_{dec}+1)$-wise 独立函数H,H',G，使用$D^{**}(\cdot)$算法来模拟解密预言机。
3. 运行$A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}(pk)$直到A对$G\times H'$发出第i次问询:

   若$(m_0,m_1)\leftarrow A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}(pk)$，则：

   a) $b\leftarrow\{0,1\},a^*\leftarrow KSP^{sy},d^*\leftarrow\{0,1\}^{n_1}$
   b) $c^*\leftarrow E^{sy}(a^*,m_b),e^*:=y$
   c) 返回(e^*,c^*,d^*)给A
4. 测量A对$G\times H'$第i次问询中的$\hat{r}$部分，设测量结果为$\hat{r}$
5. 返回$\hat{r}$。

由于在$G^{OW}_{A_5^{asy},\Pi^{asy}}$中，y的生成方式为：$r^*\leftarrow MSP^{asy},h^*\leftarrow COIN^{asy},y:=E^{asy}(pk,r^*;h^*)$，因此有$\Pr\left\{G^{OW}_{A_5^{asy},\Pi^{asy}}=1\right\}=\Pr\{G_5=1\}$。

接下来构造攻击者A_6^{asy}，该攻击者满足$\Pr\left\{G^{OW}_{A_6^{asy},\Pi^{asy}}=1\right\}=\Pr\{G_5=1\}$：

$A_6^{asy}(1^n,pk,y)$：

1. 构造$2(q_H+q_{dec}+1)$-wise、$2(q_{H'}+q_{dec}+1)$-wise、$2(q_G+q_{dec}+1)$-wise 独立函数H,H',G，使用$D^{**}(\cdot)$算法来模拟解密预言机。
2. 运行$A^{|H\rangle,|G\rangle,|H'\rangle,|D^{**}(\cdot)\rangle}(pk)$直到A对H发出第$j+q_0$次问询（$q_0$为$c^*$生成前A对H的问询次数,j在$c^*$生成后选取:）:

   a) $b\leftarrow\{0,1\},a^*\leftarrow KSP^{sy},d^*\leftarrow\{0,1\}^{n_1}$
   b) $c^*\leftarrow E^{sy}(a^*,m_b),j\leftarrow\{1,\dots,q_1\},e^*:=y$
   c) 返回(e^*,c^*,d^*)给A
3. 测量A对H的第$j+q_0$次问询叠加态，设测量结果为$\hat{r},\hat{c}$
4. 返回$\hat{r}$。

同样的，在$G^{OW}_{A_6^{asy},\Pi^{asy}}$中，y的生成方式为：$r^*\leftarrow MSP^{asy},h^*\leftarrow COIN^{asy},y:=E^{asy}(pk,r^*;h^*)$，因此有$\Pr\left\{G^{OW}_{A_6^{asy},\Pi^{asy}}=1\right\}=\Pr\{G_6=1\}$。

致谢

首先我要衷心感谢我的导师王立斌副教授。从大一到现在，王老师一直给我悉心无比的教导。在学习上，王老师引领我进入计算机科学的大门，带领我学习算法、代数、计算理论等计算机基础课程，并带领我学习密码学、复杂性理论、量子计算等进阶课程。王老师经常与我讨论各种计算机科学的开放性问题，在这些讨论中我收获了大量本科课程外的知识，并且逐渐从中领会到作为一名研究者所应有的素质。这一切都为我未来的科研道路奠定了坚实的基础。在生活上，在我迷茫的时候老师总是能诚恳地给予我一针见血的意见，在我犯错时老师总是给予严厉而又中肯的批评。王老师也经常与我讨论文学、音乐、电影等，这极大地扩展了我的视野，丰富了我专业之外的学识，而与王老师交流所获得的这些智慧又潜移默化地促进了我的专业学习。总之，我一路走来，都离不开老师的悉心指导与辛勤点拨。

其次我要感谢我的几位师兄：潘嘉昕师兄、温伟强师兄、李灏师兄、杨景添师兄与林宣耿师兄。已在国外的潘师兄与温师兄在学院作了多次研究报告，我从中受益匪浅并扩展了科研视野，其中温师兄还多次在邮件中详细回答我量子计算相关的问题。李师兄、杨师兄、林师兄经常和我与王老师讨论密码学，我在这些讨论中获得了各种知识与观点，在生活上，这三位师兄也都给予过我许多帮助。

我还要感谢教过我的所有老师，包括黄煜廉老师、马昌社老师、陈卫东老师、张奇支老师、龚征老师等，也感谢在生活上给予我帮助的所有领导、辅导员。

最后我要感谢我的父母。爸爸妈妈一直给予我无条件的支持，在他们的支持下我才得以专心做自己想做的事、追求自己的理想。

太多感激之情无法一一言表！谨以此文献给所有爱我和我爱的人！