对称加密的具体安全性处理

M. BELLARE*
A. DESAI*
E. JOKIPII*
P. ROGAWAY†

2000年9月

摘要

我们在具体安全性框架下研究对称（即私钥）加密的安全概念与方案。

我们给出了几种不同的安全概念，并分析了它们之间归约的具体复杂度。接着，我们对使用分组密码进行加密的各种方法进行了具体安全性分析，包括两种最流行的方法：密码分组链接模式和计数器模式。我们针对敌手成功率与其资源之间的函数关系，建立了紧密的界限（即匹配的上界和下界）。

目录

1 引言 3
2 安全概念 6
3 概念间的归约 10
4 有限域PRF与PRP 17
5 XOR与CTR方案的分析 18
6 CBC方案的分析 23
参考文献 30

1 引言

加密方案使得Alice能够向Bob发送消息，同时对手Eve无法获得关于消息内容的显著信息。这是密码学的经典问题。通常在两种场景之一中考虑：在对称（私钥）场景中，加密和解密在发送方和接收方共享的密钥下进行；在非对称（公钥）场景中，发送方拥有一些公开信息，而接收方持有相应的秘密信息。

本文有两个目标。第一个是在具体安全性框架下研究对称加密的安全概念。这意味着我们将考察不同概念间归约的具体复杂度。我们希望同时证明上界和下界。通过这种方式，我们可以建立概念间的紧密关系，并可以比较概念（即使它们可以多项式归约到彼此）的强弱。

第二个目标是提供一些特定对称加密方案的具体安全性分析。我们考虑的方案正在广泛使用，但尚未在可证明安全的传统下得到任何形式化的分析（无论是具体的还是渐近的）。我们希望弥补这一点。再次强调，目标是找到敌手成功率作为其消耗资源的函数的紧密界限。这既需要证明上界，也需要证明匹配的下界。

背景。Goldwasser和Micali的开创性工作[15]首次为加密引入了形式化的安全概念。具体来说，他们为非对称加密提出了两个安全概念：“语义安全性”和“多项式安全性”，并证明了它们在多项式时间归约下是等价的。Micali, Rackoff和Sloan[22]表明（这些概念的适当版本）也等价于Yao[26]提出的另一个概念。Goldreich[11]给出了非对称加密概念的均匀复杂度处理。Luby在[20, 第11-12章]中提出了这些概念在对称设置下的一些适配。

Goldwasser和Micali[15]还指定了一个非对称加密方案，其安全性（在上述意义上）多项式时间归约于二次剩余问题。随后出现了许多其他方案（例如[9, 1, 26, 13, 7]），基于各种困难问题。

具体安全性。上述所有工作的观点是：如果两个安全概念之间存在多项式时间归约，则它们是等价的；如果存在从某个困难问题到方案的多项式时间归约，则该方案被宣布为可证明安全的。这些当然是基本问题，但我们相信，一旦答案已知，以更精确的方式对概念和方案进行分类就很重要。

做个类比，在密码学中只关心多项式时间可归约性有点像只关心一个计算问题是否在P中。然而我们知道，许多有趣的问题（包括算法领域的绝大部分，以及复杂性理论的大部分）都围绕着获取关于已知在P中的问题的进一步信息展开。这些信息有助于更好地理解问题，并且对实际应用也至关重要。

在密码学中关注多项式等价概念的具体复杂度有类似的收益。特别是，当归约不是保持安全性时，意味着为了安全必须使用更大的安全参数，从而降低效率。因此，最终，人们需要为低效的归约付出安全性或运行时间的代价。

我们采用Bellare、Kilian和Rogaway[6]的方法进行具体安全性分析，其中参数化所涉及的资源，并通过关于它们的显式函数来度量敌手的成功率。该方法是非渐近的，适用于具有有限域的函数。

我们不仅关心通过展示具体界限来证明安全性，还关心证明这些界限是最优的，这通过展示匹配的攻击来完成。

我们遵循Bellare等人[5, 3]的工作，他们曾针对某些消息认证方案做过此类分析。

尽管本文关注对称加密的具体安全性，但我们相信，总体而言，具体安全性是理论密码学中富有成效研究的主要新兴途径之一。

安全概念。我们将考虑对称加密的四种安全定义，并检查它们之间归约的复杂度。我们的每个定义实际上包含两个概念：一个是针对选择明文攻击（CPA）的，另一个是针对选择密文攻击（CCA）的。第一个定义，我们称之为“左或右不可区分性”（LOR）是新的；第二个定义，“实或随机不可区分性”（ROR）是它的一个变体。接下来的两个定义，“找然后猜安全性”（FTG）和“语义安全性”（SEM）是将Goldwasser和Micali[15]的定义适配到对称设置的结果。[1]

为了建模CPA，我们必须赋予敌手查看密文的能力。在公钥设置中，敌手可以利用公钥自行创建密文，但在对称密钥设置中，加密密钥是秘密的，因此我们必须修改模型并为敌手提供一个加密函数预言机。加密预言机的存在是为什么不能将对称加密概念视为非对称加密特例的一个原因。为了建模CCA，我们必须给予敌手，除了加密预言机外，还有一个解密函数预言机。

如上所述，我们通过参数化敌手A的资源来进行具体安全性分析。我们区分A的运行时间t（按照惯例，这包括A程序的空间以及回答A所有预言机查询的时间）；A向加密预言机发出的查询数量q_e；A从其加密预言机查询的响应中看到的密文量μ_e；以及在CCA的情况下，还包括A向解密预言机发出的查询数量q_d；以及A从其解密预言机查询的响应中看到的明文量μ_d。着眼于实际应用，重要的是要分开处理所有这些资源。（以前的工作会忽略q_e, μ_e, q_d, μ_d，因为它们以t为界。但作为资源，它们非常不同，因为通常获取合法的明文-密文对比执行本地计算更成问题。）任何概念下的方案安全性通过给出该方案“优势函数”的界限来规定。优势函数是在所有限制在某些指定资源内的敌手中，敌手“攻破”方案的“优势”（与简单猜测相比）的最大值。当然，“攻破”方案的含义因不同概念而异。

概念间的归约。在这项工作中，我们只考察相同攻击下概念间归约的复杂度，$\mathrm{ATK} \in \{\mathrm{CPA}, \mathrm{CCA}\}$。也就是说，进行比较的两个概念要么都是针对CPA定义的，要么都是针对CCA定义的。根据我们这里的结果以及[4, 10, 19]的工作，可以得出，不可能存在从任何CPA安全性概念到任何CCA安全性概念的归约。

我们证明LOR-ATK和ROR-ATK是等价的，归约中的常数因子很小。（也就是说，它们之间存在保持安全性的归约。）我们还证明了从这些概念到FTG-ATK的保持安全性的归约。然而，从FTG-ATK到LOR-ATK（或ROR-ATK）的归约不是保持安全性的。但我们证明了我们给出的归约是紧密的；无法做得更好。我们通过证明SEM-ATK和FTG-ATK是等价的来完成整个图景。

从上述结果可以清楚地看出，当人们想要证明某个加密方案$\mathcal{SE}$的安全性时，最好给出从ROR-ATK或LOR-ATK出发的紧密归约，因为这意味着对其它概念也有良好的归约。

图1：$\mathsf{ATK} \in \{\mathsf{CPA}, \mathsf{CCA}\}$时概念间的关系。从概念$\mathbf{A}$到概念$\mathbf{B}$的实线表示存在从$\mathbf{A}$到$\mathbf{B}$的保持安全性的归约。虚线表示归约不是保持安全性的。

尽管以前在方案分析中考虑过具体安全性[6, 5, 3, 8]，但这是首次为了关联不同安全概念而考虑它。也就是说，这是首次根据概念间归约的复杂度将概念分类为较弱或较强。

实际上，这些结果很容易推广到非对称设置。我们主要关注对称设置，因为这是我们想要分析的方案所在的领域。

加密方案的安全性。我们分析了一些经典对称加密方案的安全性。具体来说，我们研究了使用分组密码（例如DES）的三种不同加密模式：CBC（密码分组链接模式）；CTR（计数器模式）；以及XOR（CTR模式的一种无状态变体）。

在这些方案中，底层原语是一个伪随机函数（PRF）族或伪随机置换（PRP）族F，其中由密钥K指定的特定函数F_K将l比特映射到L比特，l, L是固定的。（对于置换，$l = L$。）为了加密消息，以某种依赖于方案的方式迭代应用F_K。我们希望了解加密方案的安全性如何依赖于所假定的PRF族的安全性。我们按照[6]中的方式定义PRF和PRP族的具体安全性，通过参数化时间t'和预言机查询次数q'。我们为PRF或PRP族定义优势函数，类似于为加密方案定义的优势函数。问题在于：假设F是一个“好”的PRF族（意味着对于合理的t', q'值，其优势函数很小），那么对于加密方案，使得其优势函数在那些资源下很小的t, q_e, μ_e值是多少？我们寻求上界和下界。（后者代表了已知的最佳攻击。）

对于CTR方案，我们证明如果底层PRF族对于资源t', q'的优势函数值为ϵ'，那么该方案的优势函数值至多为$2\epsilon'$，对于资源$t = t', \mu = q'l$和任何q。对于XOR方案，我们证明在上述意义下，方案的优势函数值至多为$2\epsilon' + \delta_{\mathrm{XOR}}$，其中$\delta_{\mathrm{XOR}} = \mu(q-1)/(L2^l)$，其他资源如前所述。我们分析CBC时假设底层族是PRP族，因为该方案确实必须与置换一起使用。将t', q', ϵ'现在理解为与F作为PRP族相关的值，我们证明对于CBC，相应的优势函数值至多为$2\epsilon' + \delta_{\mathrm{CBC}}$，其中$\delta_{\mathrm{CBC}} = (\mu^2 - \mu l)/(l^2 2^l)$，其他资源如前所述。在所有情况下，我们都证明这些结果在常数因子内是紧密的。注意，即使底层PRF（或PRP）族是理想的（意味着

$\epsilon' = 0$），攻击XOR或CBC方案的敌手仍然可能获得一些优势。这对于CTR并不成立，因此我们得出结论，它具有最佳的安全性。

以上所有安全性都是在LOR-CPA意义下的。根据我们之前的说明，这给出了针对CPA的任何其他三个概念的可比较的界限。存在简单的（且众所周知的）攻击表明，我们研究的这三种方案中没有一种是抗CCA的。

更多相关工作。我们已经提到了最重要的相关工作，即[15]。这里我们提供一些更详细的比较和历史，并讨论其他工作。

由于我们的结果意味着所考虑的概念在多项式时间归约下是等价的，它们在一个层面上可以视为提供了对称情况下的[15]的类似物。Luby[20]定义了本质上是对称加密的找然后猜安全性，并且他提到使用输出长度等于待加密比特数的伪随机函数进行加密。在处理非对称设置时，[11]提到对称情况可以类似处理。这种观点中缺少的一个要素是，为了建模CPA，在对称设置中必须为敌手提供某种加密手段。我们通过为敌手提供加密预言机来扩展多项式和语义安全性。比[15, 22]更强的非对称加密概念已经出现，例如不可延展性[10]和选择密文安全性[24, 25]。从这项研究之后的结果[4, 10, 19]可以推断，FTG-CCA意味着所有这些其他概念。

像[20, 12, 16]这样的工作在一定程度上关注具体安全性，但并未真正“走到底”，因为在某种程度上，他们的概念仍然只关心某些东西是否是多项式的。此外，风味与我们不同，因为他们的关注点更多是对于一定的随机性投资能获得多少安全性，并且处理方式仍然是渐近的。奇怪的是，一些早期的工作有更具体的处理：在非对称加密领域，Alexi等人[1]仔细指定了他们的归约复杂度，这一习惯后来许多工作不幸地放弃了。

从单向函数构造伪随机生成器[17]提供了一种从单向函数开始的对称加密解决方案。在当前工作中，存在性不是问题；我们感兴趣的是具体安全性和某些特定方案的分析。

[6]提供了CBC MAC的具体安全性分析。（CBC MAC不应与CBC加密混淆：前者是一种消息认证码。）我们建立在他们技术的基础上，但这些技术不能直接解决这里的问题。CBC模式加密在[2, 18, 23]中标准化。

2 安全概念

如果$A(\cdot,\cdot,\ldots)$是任何概率算法，那么$a \leftarrow A(x_1, x_2, \ldots)$表示运行$A$于输入$x_1, x_2, \ldots$并令$a$为结果的实验，概率取自$A$的随机选择。类似地，如果$A$是一个集合，那么$a \leftarrow A$表示从$A$中均匀选择一个点并赋值给$a$的实验。

（对称）加密方案的语法。一个（对称）加密方案$\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$由三个算法组成。随机化的密钥生成算法$\mathcal{K}$以安全参数$k \in \mathbb{N}$为输入，返回一个密钥$K$；我们写作$K \xleftarrow{R} \mathcal{K}(k)$。加密算法$\mathcal{E}$可以是随机的或有状态的。它以密钥$K$和明文$M$为输入，返回密文$C$；我们写作$C \xleftarrow{R} \mathcal{E}_K(M)$。（如果是随机的，它每次调用时都重新掷币。如果是有状态的，它使用并更新跨调用维护的状态。）解密算法$\mathcal{D}$是确定性的和无状态的。它以密钥K和一个字符串C为输入，返回相应的明文M或符号$\perp$；我们写作$x \leftarrow \mathcal{D}_K(C)$，其中$x \in \{0,1\}^* \cup \{\perp\}$。我们要求对所有$M \in \{0,1\}^*$有$\mathcal{D}_K(\mathcal{E}_K(M)) = M$。

现在我们给出四个安全定义，每个定义都建模选择明文攻击和选择密文攻击（Rackoff和Simon[25]的意义上）。在每种情况下，我们允许敌手以某种形式访问加密预言机；这是这些定义与先前定义区别的一个特征。我们将为无状态加密方案描述我们的定义，稍后指出如何修改它们以适应有状态方案。

左或右不可区分性。允许敌手进行形式为(x_0, x_1)的查询，其中x_0, x_1是等长的消息。考虑两种游戏。在第一种中，每个查询通过加密左消息来响应；在第二种中，加密右消息。形式化地，我们定义左或右预言机$\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,b))$，其中$b \in \{0,1\}$，它接受输入$(x_0, x_1)$并执行以下操作：如果$b = 0$，它计算$C \leftarrow \mathcal{E}_K(x_0)$并返回$C$；否则计算$C \leftarrow \mathcal{E}_K(x_1)$并返回$C$。我们认为一个加密方案是“好的”，如果“合理的”敌手在给定左或右预言机访问权限的情况下，无法获得“显著的”优势来区分$b = 0$和$b = 1$的情况。

为了建模选择密文攻击，我们还允许敌手拥有解密预言机的访问权限。注意，如果敌手在左或右预言机输出的密文上查询解密预言机，那么它显然可以轻易赢得游戏。因此，我们禁止它这样做。任何其他查询都是允许的。

定义 1 [LOR-CPA, LOR-CCA] 令 $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ 为对称加密方案。令 $b \in \{0,1\}$ 且 $k \in \mathbb{N}$。令 A_{cpa} 为可以访问预言机 $\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,b))$ 的敌手，A_{cca} 为可以访问预言机 $\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,b))$ 和 $\mathcal{D}_K(\cdot)$ 的敌手。现在，我们考虑以下实验：

$\mathbf{Experiment}\ \mathbf{Exp}^{\text{lor-cpa-}b}_{\mathcal{SE},A_{\text{cpa}}}(k)$	$\mathbf{Experiment}\ \mathbf{Exp}^{\text{lor-cca-}b}_{\mathcal{SE},A_{\text{cca}}}(k)$
$K \xleftarrow{R} \mathcal{K}(k)$	$K \xleftarrow{R} \mathcal{K}(k)$
$d \leftarrow A_{\text{cpa}}^{\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,b))}(k)$	$d \leftarrow A_{\text{cca}}^{\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,b)),\mathcal{D}_K(\cdot)}(k)$
$\mathbf{Return}\ d$	$\mathbf{Return}\ d$

上述要求 A_{cca} 从不在 $\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,b))$ 预言机输出的密文 C 上查询 $\mathcal{D}_K(\cdot)$，并且查询 $\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,b))$ 的两个消息总是等长。我们通过以下方式定义敌手的优势：

$$\mathbf{Adv}^{\text{lor-cpa}}_{\mathcal{SE},A_{\text{cpa}}}(k) = \Pr[\mathbf{Exp}^{\text{lor-cpa-1}}_{\mathcal{SE},A_{\text{cpa}}}(k) = 1] - \Pr[\mathbf{Exp}^{\text{lor-cpa-0}}_{\mathcal{SE},A_{\text{cpa}}}(k) = 1]$$

$$\mathbf{Adv}^{\text{lor-cca}}_{\mathcal{SE},A_{\text{cca}}}(k) = \Pr[\mathbf{Exp}^{\text{lor-cca-1}}_{\mathcal{SE},A_{\text{cca}}}(k) = 1] - \Pr[\mathbf{Exp}^{\text{lor-cca-0}}_{\mathcal{SE},A_{\text{cca}}}(k) = 1].$$

我们如下定义方案的优势函数。对于任意整数 $t, q_e, \mu_e, q_d, \mu_d$，

$$\mathbf{Adv}^{\text{lor-cpa}}_{\mathcal{SE}}(k, t, q_e, \mu_e) = \max_{A_{\text{cpa}}}\{\mathbf{Adv}^{\text{lor-cpa}}_{\mathcal{SE},A_{\text{cpa}}}(k)\}$$

$$\mathbf{Adv}^{\text{lor-cca}}_{\mathcal{SE}}(k, t, q_e, \mu_e, q_d, \mu_d) = \max_{A_{\text{cca}}}\{\mathbf{Adv}^{\text{lor-cca}}_{\mathcal{SE},A_{\text{cca}}}(k)\}$$

其中最大值取自所有时间复杂性为 t 的 A_{cpa}，A_{cca}，每个敌手至多向 $\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,b))$ 预言机进行 q_e 次查询，总计至多 $\mu_e/2$ 比特，并且在 A_{cca} 的情况下，还至多向 $\mathcal{D}_K(\cdot)$ 预言机进行 q_d 次查询，总计至多 μ_d 比特。如果对于任何时间复杂性在 k 中是多项式的敌手 A，函数 $\mathbf{Adv}^{\text{lor-cpa}}_{\mathcal{SE},A}(\cdot)$（相应地 $\mathbf{Adv}^{\text{lor-cca}}_{\mathcal{SE},A}(\cdot)$）是可忽略的，则称方案 $\mathcal{SE}$ 是LOR-CPA安全（相应地LOR-CCA安全）的。

“时间复杂性”是在某种固定的RAM计算模型中，实验的最坏情况总执行时间加上敌手代码的大小。我们强调实验的总执行时间包括实验中所有操作的时间，包括密钥生成和计算预言机查询答案的时间。因此，当时间复杂性是多项式有界时，所有其他参数也是多项式有界的。这种测量敌手时间复杂性及其他资源的约定适用于本文中的所有定义。优势函数是使用指定资源的敌手能够破坏方案 $\mathcal{SE}$ 安全性的最大概率。

实或随机不可区分性。思想是敌手无法区分文本的加密与等长垃圾字符串的加密。（通过传递性，敌手无法区分任意两个等长字符串的加密。）形式化地，我们定义实或随机预言机 $\mathcal{E}_K(\mathcal{RR}(\cdot,b))$，其中 $b \in \{0,1\}$，它接受输入 x 并执行以下操作：如果 $b = 1$ 它计算 $C \leftarrow \mathcal{E}_K(x)$ 并返回 C；否则它计算 $C \leftarrow \mathcal{E}_K(r)$，其中 $r \xleftarrow{R} \{0,1\}^{|x|}$ 并返回 C。（理解该预言机会选取 $\mathcal{E}$ 可能需要的任何随机性，如果 $\mathcal{E}$ 是随机的，或者如果 $\mathcal{E}$ 是有状态的，则适当地更新其状态。）如果没有任何“合理的”敌手在给定该预言机访问权限下能够获得“显著的”优势来区分 $b = 0$ 和 $b = 1$ 的情况，则该加密方案是“好的”。

定义 2 [ROR-CPA, ROR-CCA] 令 $\mathcal{SE}=(\mathcal{K},\mathcal{E},\mathcal{D})$ 为对称加密方案。令 $b\in\{0,1\}$ 且 $k\in\mathbb{N}$。令 A_{cpa} 为可以访问预言机 $\mathcal{E}_K(\mathcal{RR}(\cdot,b))$ 的敌手，A_{cca} 为可以访问预言机 $\mathcal{E}_K(\mathcal{RR}(\cdot,b))$ 和 $\mathcal{D}_K(\cdot)$ 的敌手。现在，我们考虑以下实验：

Experiment Expror-cpa-b(S,E,Acpa)(k)	Experiment Expror-cca-b(S,E,Acca)(k)
K←R K(k)	K←R K(k)
d←AεK(RR(·,b))(k)	d←AεK(RR(·,b)),D_K(·)(k)
Return d	Return d

上述要求 A_{cca} 从不在 $\mathcal{E}_K(\mathcal{RR}(\cdot,b))$ 预言机输出的密文 C 上查询 $\mathcal{D}_K(\cdot)$。我们通过以下方式定义敌手的优势：

$$\mathbf{Adv}^{\text{ror}-\text{cpa}}_{\mathcal{SE},A_{\text{cpa}}}(k)=\Pr[\mathbf{Exp}^{\text{ror}-\text{cpa}-1}_{\mathcal{SE},A_{\text{cpa}}}(k)=1]-\Pr[\mathbf{Exp}^{\text{ror}-\text{cpa}-0}_{\mathcal{SE},A_{\text{cpa}}}(k)=1]$$

$$\mathbf{Adv}^{\text{ror}-\text{cca}}_{\mathcal{SE},A_{\text{cca}}}(k)=\Pr[\mathbf{Exp}^{\text{ror}-\text{cca}-1}_{\mathcal{SE},A_{\text{cca}}}(k)=1]-\Pr[\mathbf{Exp}^{\text{ror}-\text{cca}-0}_{\mathcal{SE},A_{\text{cca}}}(k)=1].$$

我们如下定义方案的优势函数。对于任意整数 t,q_e,μ_e,q_d,μ_d，

$$\mathbf{Adv}^{\text{ror}-\text{cpa}}_{\mathcal{SE}}(k,t,q_e,\mu_e)=\max_{A_{\text{cpa}}}\{\mathbf{Adv}^{\text{ror}-\text{cpa}}_{\mathcal{SE},A_{\text{cpa}}}(k)\}$$

$$\mathbf{Adv}^{\text{ror}-\text{cca}}_{\mathcal{SE}}(k,t,q_e,\mu_e,q_d,\mu_d)=\max_{A_{\text{cca}}}\{\mathbf{Adv}^{\text{ror}-\text{cca}}_{\mathcal{SE},A_{\text{cca}}}(k)\}$$

其中最大值取自所有时间复杂性为 t 的 $A_{\text{cpa}},A_{\text{cca}}$，每个敌手至多向 $\mathcal{E}_K(\mathcal{RR}(\cdot,b))$ 预言机进行 q_e 次查询，总计至多 μ_e 比特，并且在 A_{cca} 的情况下，还至多向 $\mathcal{D}_K(\cdot)$ 预言机进行 q_d 次查询，总计至多 μ_d 比特。如果对于任何时间复杂性在 k 中是多项式的敌手 A，函数 $\mathbf{Adv}^{\text{ror}-\text{cpa}}_{\mathcal{SE},A}(\cdot)$（相应地 $\mathbf{Adv}^{\text{ror}-\text{cca}}_{\mathcal{SE},A}(\cdot)$）是可忽略的，则称方案 $\mathcal{SE}$ 是ROR-CPA安全（相应地ROR-CCA安全）的。

找然后猜安全性。这是[15, 22]中给出的多项式安全性概念的适配。我们设想一个在两个阶段运行的敌手。在找阶段，敌手努力提出一对等长消息 x_0 和 x_1，它试图区分它们的加密。它还保留一些状态信息 s，可能希望保存下来以后帮助它。在猜阶段，它获得一个随机密文 y，对应于明文 x_0,x_1 之一，连同状态信息 s。如果敌手正确识别出哪个明文与 y 对应，则它“获胜”。如果“合理的”敌手无法以显著超过一半的概率获胜，则该加密方案是“好的”。

定义 3 [FTG-CPA, FTG-CCA] 令 $\mathcal{SE}=(\mathcal{K},\mathcal{E},\mathcal{D})$ 为对称加密方案。令 $b\in\{0,1\}$ 且 $k\in\mathbb{N}$。令 A_{cpa} 为可以访问预言机 $\mathcal{E}_K(\cdot)$ 的敌手，A_{cca} 为可以访问预言机 $\mathcal{E}_K(\cdot)$ 和 $\mathcal{D}_K(\cdot)$ 的敌手。现在，我们考虑以下实验：

Experiment Expftg-cpa-b(k)K←R K(k)	Experiment Expftg-cca-b(k)K←R K(k)
(x0,x1,s)←AεK(·)	(x0,x1,s)←AεK(·),D_K(·)
(k,find)y←E_K(xb)d←AεK(·)	(k,find)y←E_K(xb)d←AεK(·),D_K(·)
(k,guess,y,s)Return d	(k,guess,y,s)Return d

上述要求 A_{cca} 不在猜阶段查询 $\mathcal{D}_K(\cdot)$ 于密文 y 上，并且两个消息 (x_0,x_1) 等长。我们通过以下方式定义敌手的优势：

$$\mathbf{Adv}^{\text{ftg}-\text{cpa}}_{\mathcal{SE},A_{\text{cpa}}}(k)=\Pr[\mathbf{Exp}^{\text{ftg}-\text{cpa}-1}_{\mathcal{SE},A_{\text{cpa}}}(k)=1]-\Pr[\mathbf{Exp}^{\text{ftg}-\text{cpa}-0}_{\mathcal{SE},A_{\text{cpa}}}(k)=1]$$

$$\mathbf{Adv}^{\text{ftg}-\text{cca}}_{\mathcal{SE},A_{\text{cca}}}(k)=\Pr[\mathbf{Exp}^{\text{ftg}-\text{cca}-1}_{\mathcal{SE},A_{\text{cca}}}(k)=1]-\Pr[\mathbf{Exp}^{\text{ftg}-\text{cca}-0}_{\mathcal{SE},A_{\text{cca}}}(k)=1].$$

我们如下定义方案的优势函数。对于任意整数 t,q_e,μ_e,q_d,μ_d，

$$\mathbf{Adv}^{\mathrm{ftg-cpa}}_{\mathcal{SE}}(k,t,q_e,\mu_e)=\max_{A_{\mathrm{cpa}}}\{\mathbf{Adv}^{\mathrm{ftg-cpa}}_{\mathcal{SE},A_{\mathrm{cpa}}}(k)\}$$

$$\mathbf{Adv}^{\mathrm{ftg-cca}}_{\mathcal{SE}}(k,t,q_e,\mu_e,q_d,\mu_d)=\max_{A_{\mathrm{cca}}}\{\mathbf{Adv}^{\mathrm{ftg-cca}}_{\mathcal{SE},A_{\mathrm{cca}}}(k)\}$$

其中最大值取自所有时间复杂性为 t 的 A_{cpa} , A_{cca} ，每个敌手至多向 $\mathcal{E}_K(\cdot)$ 预言机进行 q_e 次查询，总计至多 $(\mu_e-|x_0|)$ 比特，并且在 A_{cca} 的情况下，还至多向 $\mathcal{D}_K(\cdot)$ 预言机进行 q_d 次查询，总计至多 μ_d 比特。如果对于任何时间复杂性在 k 中是多项式的敌手 A ，函数 $\mathbf{Adv}^{\mathrm{ftg-cpa}}_{\mathcal{SE},A}(\cdot)$ （相应地 $\mathbf{Adv}^{\mathrm{ftg-cca}}_{\mathcal{SE},A}(\cdot)$ ）是可忽略的，则称方案 $\mathcal{SE}$ 是FTG-CPA安全（相应地FTG-CCA安全）的。

语义安全性。Goldwasser和Micali[15]解释语义安全性为：给定密文可以有效计算的关于明文的任何信息，在没有密文的情况下也能计算。我们将[15, 22]的形式化适配到对称设置。

我们的敌手将在两个阶段运行。在选择阶段，它努力提出一个有利的消息分布 $\mathcal{M}$。我们假设消息分布是有效的，意味着 $\mathcal{M}$ 中所有具有非零概率的字符串都有相同的长度。在敌手的预测阶段，它被给予一个随机密文 y，对应于根据分布 $\mathcal{M}$ 选择的明文 x_1，并且它必须输出一个函数 f 和一个函数值 α。它希望 $\alpha=f(x)$。如果没有合理的敌手能够以显著优于概率 $\alpha=f(x_0)$ 的概率猜出 $f(x)$，其中 x_0 是从 $\mathcal{M}$ 中随机抽取的隐藏值，则加密方案是语义安全的。这种比较性的测量敌手优势的方法遵循了Bellare等人[4]用来捕捉不可延展性概念的方法。

先前的形式化要求该条件对所有函数 f 成立。在我们的具体处理中，我们允许函数 f 和概率分布 $\mathcal{M}$ 由敌手选择。

定义 4 [SEM-CPA, SEM-CCA] 令 $\mathcal{SE}=(\mathcal{K},\mathcal{E},\mathcal{D})$ 为对称加密方案。令 $k\in\mathbb{N}$。令 A_{cpa} 为可以访问预言机 $\mathcal{E}_K(\cdot)$ 的敌手，A_{cca} 为可以访问预言机 $\mathcal{E}_K(\cdot)$ 和 $\mathcal{D}_K(\cdot)$ 的敌手。现在，我们考虑以下实验：

$$\mathbf{Exp}^{\mathrm{sem-cpa-b}}_{\mathcal{SE},A_{\mathrm{cpa}}}(k)$$

$$K\xleftarrow{R}\mathcal{K}(k)$$

$$(\mathcal{M},s)\leftarrow A^{\mathcal{E}_K(\cdot)}_{\mathrm{cpa}}(k,\mathrm{select})$$

$$x_0\leftarrow\mathcal{M};x_1\leftarrow\mathcal{M}$$

$$y\leftarrow\mathcal{E}_K(x_1)$$

$$(f,\alpha)\leftarrow A^{\mathcal{E}_K(\cdot)}_{\mathrm{cpa}}(k,\mathrm{predict},y,s)$$

$$If\alpha=f(x_b)thend\leftarrow 1;elsed\leftarrow 0$$

$$\mathbf{Return}d$$

$$\mathrm{Experim}\mathbf{Exp}^{\mathrm{sem-cca-b}}_{\mathcal{SE},A_{\mathrm{cca}}}(k)$$

$$K\xleftarrow{R}\mathcal{K}(k)$$

$$(\mathcal{M},s)\leftarrow A^{\mathcal{E}_K(\cdot),\mathcal{D}_K(\cdot)}_{\mathrm{cca}}(k,\mathrm{select})$$

$$x_0\leftarrow\mathcal{M};x_1\leftarrow\mathcal{M}$$

$$y\leftarrow\mathcal{E}_K(x_1)$$

$$(f,\alpha)\leftarrow A^{\mathcal{E}_K(\cdot),\mathcal{D}_K(\cdot)}_{\mathrm{cca}}(k,\mathrm{predict},y,s)$$

$$If\alpha=f(x_b)thend\leftarrow 1;elsed\leftarrow 0$$

Return d

上述要求 A_{cca} 不在预测阶段查询 $\mathcal{D}_K(\cdot)$ 于密文 y 上。我们通过以下方式定义敌手的优势：

$$\mathbf{Adv}^{\text{sem-cpa}}_{\mathcal{SE},A_{\text{cpa}}}(k) = \Pr[\mathbf{Exp}^{\text{sem-cpa-1}}_{\mathcal{SE},A_{\text{cpa}}}(k) = 1] - \Pr[\mathbf{Exp}^{\text{sem-cpa-0}}_{\mathcal{SE},A_{\text{cpa}}}(k) = 1]$$

$$\mathbf{Adv}^{\text{sem-cca}}_{\mathcal{SE},A_{\text{cca}}}(k) = \Pr[\mathbf{Exp}^{\text{sem-cca-1}}_{\mathcal{SE},A_{\text{cca}}}(k) = 1] - \Pr[\mathbf{Exp}^{\text{sem-cca-0}}_{\mathcal{SE},A_{\text{cca}}}(k) = 1]$$

我们如下定义方案的优势函数。对于任意整数 $t, q_e, \mu_e, q_d, \mu_d$，

$$\mathbf{Adv}^{\text{sem-cpa}}_{\mathcal{SE}}(k, t, q_e, \mu_e) = \max_{A_{\text{cpa}}}\{\mathbf{Adv}^{\text{sem-cpa}}_{\mathcal{SE},A_{\text{cpa}}}(k)\}$$

$$\mathbf{Adv}^{\text{sem-cca}}_{\mathcal{SE}}(k, t, q_e, \mu_e, q_d, \mu_d) = \max_{A_{\text{cca}}}\{\mathbf{Adv}^{\text{sem-cca}}_{\mathcal{SE},A_{\text{cca}}}(k)\}$$

其中最大值取自所有时间复杂性为 t 的 A_{cpa} , A_{cca} ，每个敌手至多向 $\mathcal{E}_K(\cdot)$ 预言机进行 q_e 次查询，总计至多 $(\mu_e - |x_0|)$ 比特，并且在 A_{cca} 的情况下，还至多向 $\mathcal{D}_K(\cdot)$ 预言机进行 q_d 次查询，总计至多 μ_d 比特。如果对于任何时间复杂性在 k 中是多项式的敌手 A ，函数 $\mathbf{Adv}^{\text{sem-cpa}}_{\mathcal{SE},A}(\cdot)$ （相应地 $\mathbf{Adv}^{\text{sem-cca}}_{\mathcal{SE},A}(\cdot)$ ）是可忽略的，则称方案 $\mathcal{SE}$ 是SEM-CPA安全（相应地SEM-CCA安全）的。

为有状态情况修改定义。通过以上述定义的自然方式进行修改来调整回答预言机查询的方式，可以获得有状态加密方案的安全定义。例如，在定义2中，$A^{\mathcal{E}_K(\mathcal{RR}(\cdot,0))}_{\text{cpa}}$ 现在表示 A_{cpa} 拥有一个维护状态 σ 的预言机，初始为 ε。在收到查询 x 后，它选择随机性 r 并设置 (σ', y) 为 $\mathcal{E}_K(x, \sigma, r)$。它返回 y 作为预言机查询的答案，并通过 $\sigma \leftarrow \sigma'$ 更新状态。注意（密文 y ）被返回，但更新后的状态不被返回。（因此当我们写作 $A^{\mathcal{E}_K(\mathcal{RR}(\cdot,0))}_{\text{cpa}}$ 时，我们是在滥用符号；我们应该写作 $A^{\mathcal{E}^2_K(\mathcal{RR}(\cdot,0))}_{\text{cpa}}$。）注意加密预言机现在具有“记忆”：在调用之间，状态被修改和保留。符号 $A^{\mathcal{E}_K(\mathcal{RR}(\cdot,1))}_{\text{cpa}}$ 可以类似地重新解释，同样的方法适用于其他定义。

3 概念间的归约

这里我们考察不同安全概念间的归约。我们同时考察上界和下界。由于我们关注具体安全性界限，我们可以用我们的结果来决定一个安全概念相对于其他它可以多项式归约的概念有多强。这个信息是有用的，因为它帮助我们识别归约最理想的起点。当我们通过从左或右不可区分性出发的归约来证明方案安全性时，我们隐含地使用了这个信息。

我们使用符号 $A \Rightarrow B$ 表示从概念 A 到概念 B 的保持安全性的归约。$A \to B$ 表示从 A 到 B 的归约（不一定是保持安全性的）。$A \neq B$ 和 $A \not\to B$ 是上述的自然解释。为简洁和清晰起见，我们同时关联 CPA 和 CCA 下的概念。我们让字符串 atk 实例化为形式符号 cpa, cca，而 ATK 则是来自 CPA, CCA 的相应形式符号。在我们断言的证明中，我们使用约定：如果 $\text{atk} = \text{cpa}$ 则 $\mathcal{O}^{-1} = \epsilon$。（当我们说 $\mathcal{O}^{-1} = \epsilon$ 时，意思是 $\mathcal{O}^{-1}$ 是在任何输入上都返回空字符串的函数。）

前两个定理表明，我们的前两个概念，左或右不可区分性和实或随机不可区分性，在任何攻击下本质上强度相同。

定理 1 [ROR-ATK $\Rightarrow$ LOR-ATK] 对于任何方案 $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$

$$\mathbf{Adv}^{\text{lor-cpa}}_{\mathcal{SE}}(k, t, q_e, \mu_e) \leq 2 \cdot \mathbf{Adv}^{\text{ror-cpa}}_{\mathcal{SE}}(k, t, q_e, \mu_e)$$

$$\mathbf{Adv}^{\text{lor-cca}}_{\mathcal{SE}}(k, t, q_e, \mu_e, q_d, \mu_d) \leq 2 \cdot \mathbf{Adv}^{\text{ror-cca}}_{\mathcal{SE}}(k, t, q_e, \mu_e, q_d, \mu_d).$$

证明：假设 A_1 是在 LOR-ATK 意义上攻击 $\mathcal{SE}=(\mathcal{K},\mathcal{E},\mathcal{D})$ 的敌手。我们构造一个新的敌手 A_2，使用 A_1，在 ROR-ATK 意义上攻击 $\mathcal{SE}$。

令 $\mathcal{O}_2(\cdot)$ 是 A_2 的加密预言机，$\mathcal{O}^{-1}(\cdot)$ 是其解密预言机。$A_2^{\mathcal{O}_2(\cdot),\mathcal{O}^{-1}(\cdot)}$ 将运行 A_1，使用其预言机来模拟 A_1 的预言机。

对于 $b\in\{0,1\}$ 且 $|x_0|=|x_1|$，定义 $\mathcal{O}_1(\mathcal{LR}(x_0,x_1,b))$ 为 $\mathcal{O}_2(x_b)$。

算法 $A_2^{\mathcal{O}_2(\cdot),\mathcal{O}^{-1}(\cdot)}(k)$

(1) 令 $b\xleftarrow{R}\{0,1\}$

(2) 如果 $b=0$ 则 $d\leftarrow A_1^{\mathcal{O}_1(\mathcal{LR}(\cdot,\cdot,0)),\mathcal{O}^{-1}(\cdot)}(k)$，否则 $d\leftarrow A_1^{\mathcal{O}_1(\mathcal{LR}(\cdot,\cdot,1)),\mathcal{O}^{-1}(\cdot)}(k)$。

(3) 如果 $b=d$ 则返回 1 否则返回 0。

从以上描述很容易看出时间和查询复杂性如声称那样。

我们现在计算 A_2 的优势。我们考虑 $\mathbf{Exp}^{\mathrm{ror-atk-b}}_{\mathcal{SE},A_2}(k)$，自由地引用这个实验背后的随机变量。我们有，

$$\mathbf{Adv}^{\mathrm{ror-atk}}_{\mathcal{SE},A_2}(k)=\mathrm{Pr}[\mathbf{Exp}^{\mathrm{ror-atk-1}}_{\mathcal{SE},A_2}(k)=1]-\mathrm{Pr}[\mathbf{Exp}^{\mathrm{ror-atk-0}}_{\mathcal{SE},A_2}(k)=1]$$

当 $\mathcal{O}_2(\cdot)=\mathcal{E}_K(\mathcal{RR}(\cdot,0))$ 时，我们有 $\mathcal{O}_1(\mathcal{LR}(\cdot,\cdot,0))$ 和 $\mathcal{O}_1(\mathcal{LR}(\cdot,\cdot,1))$ 返回相同分布的答案。所以，$\mathrm{Pr}[\mathbf{Exp}^{\mathrm{ror-atk-0}}_{\mathcal{SE},A_2}(k)=1]=1/2$。因此，

$$\begin{aligned}
&\mathbf{Adv}^{\mathrm{ror-atk}}_{\mathcal{SE},A_2}(k)=\mathrm{Pr}\left[\mathbf{Exp}^{\mathrm{ror-atk-1}}_{\mathcal{SE},A_2}(k)=1\right]-1/2\\
&=1/2\cdot\mathrm{Pr}\left[\mathbf{Exp}^{\mathrm{lor\text{-}atk\text{-}1}}_{\mathcal{SE},A_1}(k)=1\right]+1/2\cdot\mathrm{Pr}\left[\mathbf{Exp}^{\mathrm{lor\text{-}atk\text{-}0}}_{\mathcal{SE},A_1}(k)=0\right]-1/2\\
&=1/2\cdot\mathrm{Pr}\left[\mathbf{Exp}^{\mathrm{lor\text{-}atk\text{-}1}}_{\mathcal{SE},A_1}(k)=1\right]+1/2\cdot\left(1-\mathrm{Pr}\left[\mathbf{Exp}^{\mathrm{lor\text{-}atk\text{-}0}}_{\mathcal{SE},A_1}(k)=1\right]\right)-1/2\\
&=1/2\cdot\left(\mathrm{Pr}\left[\mathbf{Exp}^{\mathrm{lor\text{-}atk\text{-}1}}_{\mathcal{SE},A_1}(k)=1\right]-\mathrm{Pr}\left[\mathbf{Exp}^{\mathrm{lor\text{-}atk\text{-}0}}_{\mathcal{SE},A_1}(k)=1\right]\right)\\
&=1/2\cdot\mathbf{Adv}^{\text{lor-atk}}_{\mathcal{SE},A_1}(k)
\end{aligned}$$

由于 A_1 是任意敌手，优势函数中的声称关系成立。

定理 2 [LOR-ATK $\Rightarrow$ ROR-ATK] 对于任何方案 $\mathcal{SE}=(\mathcal{K},\mathcal{E},\mathcal{D})$

$$\mathbf{Adv}^{\mathrm{ror\text{-}cpa}}_{\mathcal{SE}}(k,t,q_e,\mu_e)\le\mathbf{Adv}^{\mathrm{lor\text{-}cpa}}_{\mathcal{SE}}(k,t,q_e,\mu_e)$$

$$\mathbf{Adv}^{\mathrm{ror-cca}}_{\mathcal{SE}}(k,t,q_e,\mu_e,q_d,\mu_d)\le\mathbf{Adv}^{\mathrm{lor-cca}}_{\mathcal{SE}}(k,t,q_e,\mu_e,q_d,\mu_d).$$

证明：假设 A_2 是在 ROR-ATK 意义上攻击 $\mathcal{SE}=(\mathcal{K},\mathcal{E},\mathcal{D})$ 的敌手。我们构造一个新的敌手 A_1，使用 A_2，在 LOR-ATK 意义上攻击 $\mathcal{SE}$。

令 $\mathcal{O}_1(\cdot,\cdot)$ 是 A_1 的加密预言机，$\mathcal{O}^{-1}(\cdot)$ 是其解密预言机。$A_1^{\mathcal{O}_1(\cdot,\cdot),\mathcal{O}^{-1}(\cdot)}$ 将运行 A_2，使用其预言机来模拟 A_2 的预言机。

对于任何字符串 x，定义 $\mathcal{O}_2(x)$ 为 $\mathcal{O}_1(r,x)$，其中 $r\xleftarrow{R}\{0,1\}^{|x|}$ 在每次调用预言机时重新选择。

算法 $A_1^{\mathcal{O}_1(\cdot,\cdot),\mathcal{O}^{-1}(\cdot)}(k)$

(1) 返回 $A_2^{\mathcal{O}_2(\cdot),\mathcal{O}^{-1}(\cdot)}(k)$

显然，时间和查询复杂性如声称那样。对于 A_1 的优势，我们有，

$$\mathbf{Adv}^{\mathrm{lor-atk}}_{\mathcal{SE},A_1}(k) = \mathrm{P\,r}[\mathbf{Exp}^{\mathrm{ror-atk}-1}_{\mathcal{SE},A_2}(k)=1] - \mathrm{P\,r}[\mathbf{Exp}^{\mathrm{ror-atk}-0}_{\mathcal{SE},A_2}(k)=1] = \mathbf{Adv}^{\mathrm{ror-atk}}_{\mathcal{SE},A_2}(k)$$

由于 A_2 是任意敌手，优势函数中的声称关系成立。

左或右不可区分性和实或随机不可区分性构成了比传统的找然后猜概念更强的安全概念。直观地说，在找然后猜中敌手的工作更难，因为它必须挑出一对消息来执行区分。定理3、4和命题5说明了这一点。

第一个定理表明，具有某种左或右安全性的方案在找然后猜意义上具有基本相同的安全性。

定理 3 [LOR-ATK $\Rightarrow$ FTG-ATK] 对于任何方案 $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$

$$\mathbf{Adv}^{\mathrm{ftg-cpa}}_{\mathcal{SE}}(k,t,q_e,\mu_e) \le \mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathcal{SE}}(k,t,q_e+1,\mu_e)$$

$$\mathbf{Adv}^{\mathrm{ftg-cca}}_{\mathcal{SE}}(k,t,q_e,\mu_e,q_d,\mu_d) \le \mathbf{Adv}^{\mathrm{lor-cca}}_{\mathcal{SE}}(k,t,q_e+1,\mu_e,q_d,\mu_d).$$

证明：假设 A_3 是在 FTG-ATK 意义上攻击 $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ 的敌手。我们构造一个新的敌手 A_1，使用 A_3，在 LOR-ATK 意义上攻击 $\mathcal{SE}$。

令 $\mathcal{O}_1(\cdot,\cdot)$ 是 A_1 的加密预言机，$\mathcal{O}^{-1}(\cdot)$ 是其解密预言机。$A_1^{\mathcal{O}_1(\cdot,\cdot),\mathcal{O}^{-1}(\cdot)}$ 将运行 A_3，使用其预言机来模拟 A_3 的预言机。

对于任何字符串 x，定义 $\mathcal{O}_3(x)$ 为 $\mathcal{O}_1(x,x)$。我们假设，不失一般性，A_3 不在它先前通过查询 $\mathcal{O}_3(\cdot)$ 获得的任何密文上查询 $\mathcal{O}^{-1}(\cdot)$。

算法 $A_1^{\mathcal{O}_1(\cdot,\cdot),\mathcal{O}^{-1}(\cdot)}(k)$

(1) 令 $(x_0, x_1, s) \leftarrow A_3^{\mathcal{O}_3(\cdot),\mathcal{O}^{-1}(\cdot)}(k, \mathrm{find})$

(2) 令 $d \leftarrow A_3^{\mathcal{O}_3(\cdot),\mathcal{O}^{-1}(\cdot)}(k, \mathbf{guess}, \mathcal{O}_1(x_0,x_1), s)$

(3) 如果 $d = 0$ 则返回 0，否则返回 1。

显然，时间和查询复杂性如声称那样。对于 A_1 的优势，我们有，

$$\mathbf{Adv}^{\mathrm{lor-atk}}_{\mathcal{SE},A_1}(k) = \mathrm{P\,r}[\mathbf{Exp}^{\mathrm{ftg-atk}-1}_{\mathcal{SE},A_3}(k)=1] - \mathrm{P\,r}[\mathbf{Exp}^{\mathrm{ftg-atk}-0}_{\mathcal{SE},A_3}(k)=1] = \mathbf{Adv}^{\mathrm{ftg-atk}}_{\mathcal{SE},A_3}(k)$$

由于 A_3 是任意敌手，优势函数中的声称关系成立。

下一个定理表明，如果一个方案具有某种找然后猜安全性，那么它在左或右意义上是安全的，但所显示的安全性在数量上较低。

定理 4 [FTG-ATK $\rightarrow$ LOR-ATK] 对于任何方案 $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$

$$\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathcal{SE}}(k,t,q_e,\mu_e) \le q_e \cdot \mathbf{Adv}^{\mathrm{ftg-cpa}}_{\mathcal{SE}}(k,t,q_e,\mu_e)$$
$$\mathbf{Adv}^{\mathrm{lor-cca}}_{\mathcal{SE}}(k,t,q_e,\mu_e,q_d,\mu_d) \le q_e \cdot \mathbf{Adv}^{\mathrm{ftg-cca}}_{\mathcal{SE}}(k,t,q_e,\mu_e,q_d,\mu_d).$$

证明：假设 A_1 是在 LOR-ATK 意义上攻击 $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ 的敌手。我们构造一个新的敌手 A_3，使用 A_1，在 FTG-ATK 意义上攻击 $\mathcal{SE}$。

令 $\mathcal{O}_3(\cdot)$ 是 A_3 的加密预言机，$\mathcal{O}^{-1}(\cdot)$ 是其解密预言机。对于 $b \in \{0,1\}$ 且 $|x_0| = |x_1|$，定义 $\mathcal{O}_1(\mathcal{LR}(x_0, x_1, b))$ 为 $\mathcal{O}_3(x_b)$。

算法 $A_3^{\mathcal{O}_3(\cdot),\mathcal{O}^{-1}(\cdot)}(k, \text{find})$

(1) 令 $i \xleftarrow{R} \{1, \ldots, q_e\}$

(2) 运行 A_1，使用 $\mathcal{O}_1(\mathcal{LR}(\cdot,\cdot,0))$ 回答其加密预言机查询，使用 $\mathcal{O}^{-1}(\cdot)$ 回答其解密预言机查询，直到它进行第 i 次加密预言机查询，我们将其记为 (x_0^i, x_1^i)。（也就是说，A_1 现在已提出此查询，正在等待加密预言机的响应。）令 s 为此刻 A_1 的运行状态。

(3) 返回 (x_0^i, x_1^i, s)

算法 $A_3^{\mathcal{O}_3(\cdot),\mathcal{O}^{-1}(\cdot)}(k, \mathbf{guess}, y, s)$

(1) 通过回答其第 i 次加密预言机查询（即 (x_0^i, x_1^i)）为 y 来恢复 A_1 在状态 s 下的执行，并在它进行另一次预言机查询之前停止。

(2) 继续执行 A_1，现在通过 $\mathcal{O}_1(\mathcal{LR}(\cdot,\cdot,1))$ 回答所有加密预言机查询，通过 $\mathcal{O}^{-1}(\cdot)$ 回答解密预言机查询，直到 A_1 停止。

(3) 如果 A_1 输出 1 则返回 0，否则返回 1。

显然，时间和查询复杂性如所给出。我们使用标准的混合论证计算 A_3 的优势。为此，我们定义 $q_e + 1$ 个实验的序列：对于 $j = 0 \ldots q_e$，定义 $\mathbf{Exp}^{\text{hyb-atk}-j}_{\mathcal{SE},A_1}(k)$ 为一个实验，其中选择 $K \xleftarrow{R} \mathcal{K}(k)$ 并运行 A_1，通过 $\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,0))$ 回答 A_1 的前 j 次加密预言机查询，其余通过 $\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,1))$ 回答，此外，如果 $\text{atk} = \text{cca}$，通过 $\mathcal{D}_K(\cdot)$ 回答其解密预言机查询。实验的输出定义为 A_1 的输出。

现在考虑实验 $\mathbf{Exp}^{\text{fg-atk-b}}_{\mathcal{SE},A_3}(k)$，其中 A_3 是上述算法。在这个实验中，如果 $b = 0$ 则 $y = \mathcal{E}_K(x_0^i)$ 并且在模拟中，A_1 的输出将是 $\mathbf{Exp}^{\text{hyb-atk}-(i+1)}_{\mathcal{SE},A_1}(k)$ 的输出。另一方面，如果 $b = 1$ 则 $y = \mathcal{E}_K(x_1^i)$ 并且在模拟中，A_1 的输出将与 $\mathbf{Exp}^{\text{hyb-atk-i}}_{\mathcal{SE},A_1}(k)$ 相同。由于 i 是 A_3 从 $\{1, \ldots, q_e\}$ 中随机选择的，我们有，

$$\begin{aligned}
&\mathbf{Adv}^{\text{ftg-atk}}_{\mathcal{SE},A_3}(k) = (1/q_e) \cdot \textstyle\sum_{i=0}^{q_e-1} \left(\Pr\left[\mathbf{Exp}^{\text{hyb-atk-i}}_{\mathcal{SE},A_1}(k) = 1\right] - \Pr\left[\mathbf{Exp}^{\text{hyb-atk-(i+1)}}_{\mathcal{SE},A_1}(k) = 1\right] \right) \\
&= (1/q_e) \cdot \left(\Pr\left[\mathbf{Exp}^{\text{hyb-atk-0}}_{\mathcal{SE},A_1}(k) = 1\right] - \Pr\left[\mathbf{Exp}^{\text{hyb-atk-q_e}}_{\mathcal{SE},A_1}(k) = 1\right] \right) \\
&= (1/q_e) \cdot \mathbf{Adv}^{\text{lor-atk}}_{\mathcal{SE},A_1}(k)
\end{aligned}$$

由于 A_1 是任意敌手，优势函数中的声称关系成立。

以下命题表明，上述安全性的下降并非由于归约的任何弱点，而是固有的——我们展示了一个方案，其在找然后猜意义上的安全性高于左或右意义上的安全性，其差距与上述定理相同。显然，如果根本不存在安全的加密方案，我们无法做出这样的陈述，因此该定理假设存在一个安全方案，然后构造一个展示所需差距的不同方案。

命题 5 [FTG-ATK $\not\Rightarrow$ LOR-ATK] 假设 $\mathcal{SE}$ 是一个无状态加密方案，消息空间包含 $\{0,1\}$。那么，存在一个无状态加密方案 $\mathcal{SE}'$，使得，

$$\begin{aligned}
&\mathbf{Adv}^{\text{lor-cpa}}_{\mathcal{SE}'}(k, t, q_e, q_e) = \mathbf{Adv}^{\text{lor-cca}}_{\mathcal{SE}'}(k, t, q_e, q_e, 0, 0) \geq 0.632 \\
&\mathbf{Adv}^{\text{ftg-cpa}}_{\mathcal{SE}'}(k, t, q_e, \mu_e) \leq \mathbf{Adv}^{\text{ftg-cpa}}_{\mathcal{SE}}(k, t, q_e, \mu_e) + 1/q_e \\
&\mathbf{Adv}^{\text{ftg-cca}}_{\mathcal{SE}'}(k, t, q_e, \mu_e, q_d, \mu_d) \leq \mathbf{Adv}^{\text{ftg-cca}}_{\mathcal{SE}}(k, t, q_e, \mu_e, q_d, \mu_d) + 1/q_e
\end{aligned}$$

此外，那么存在一个有状态加密方案 $\mathcal{SE}''$，使得，

$$\begin{aligned}
&\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathcal{SE}''}(k,t,q_e,q_e) = \mathbf{Adv}^{\mathrm{lor-cca}}_{\mathcal{SE}''}(k,t,q_e,q_e,0,0) = 1\\
&\mathbf{Adv}^{\mathrm{ftg-cpa}}_{\mathcal{SE}''}(k,t,q_e,\mu_e) \le \mathbf{Adv}^{\mathrm{ftg-cpa}}_{\mathcal{SE}}(k,t,q_e,\mu_e) + 1/q_e\\
&\mathbf{Adv}^{\mathrm{ftg-cca}}_{\mathcal{SE}''}(k,t,q_e,\mu_e,q_d,\mu_d) \le \mathbf{Adv}^{\mathrm{ftg-cca}}_{\mathcal{SE}}(k,t,q_e,\mu_e,q_d,\mu_d) + 1/q_e.
\end{aligned}$$

证明：令 $\mathcal{SE} = (\mathcal{E},\mathcal{D},\mathcal{K})$ 为给定的加密方案。我们现在定义 $\mathcal{SE}' = (\mathcal{E}',\mathcal{D}',\mathcal{K}')$ 并证明它具有所声称的性质。设 $\mathcal{K}' = \mathcal{K}$。定义加密为：

算法 $\mathcal{E}'_K(x)$

(1) 选取 $i \xleftarrow{R} \{1,\ldots,q_e\}$

(2) 如果 $i = 1$ 则返回 $0 \,\|\, x$，否则返回 $1 \,\|\, \mathcal{E}_K(x)$

$\mathcal{D}'$ 如预期那样。现在考虑以下在 LOR-ATK 意义上攻击 $\mathcal{SE}'$ 的敌手 A_1。令 $\mathcal{O}_1(\cdot,\cdot)$ 是 A_1 的加密预言机，$\mathcal{O}^{-1}(\cdot)$ 是其解密预言机。

算法 $A_1^{\mathcal{O}_1(\cdot,\cdot),\mathcal{O}^{-1}(\cdot)}(k)$

(1) 固定一对不同的等长消息 x_1, x_2。（具体取 $x_0 = 0$ 和 $x_1 = 1$，我们假设它们在 $\mathcal{SE}$ 的消息空间中。）

(2) 对于 $j = 1,\ldots,q_e$ 执行：$y_j \leftarrow \mathcal{O}_1(x_0,x_1)$

(3) 如果存在某个 j 使得 $y_j = 0 \,\|\, x_0$，则返回 0；否则返回 1。

可以验证，A_1 的优势是 $\mathcal{E}'_K$ 选择的 i 值在至少一次加密中为 1 的概率，即 $\mathbf{Adv}^{\mathrm{lor-atk}}_{\mathcal{SE},A_1}(k) = 1 - (1-1/q_e)^{q_e} \approx 1 - 1/e$。

注意 A_1 进行了 q_e 次查询，每次包含两个 1 比特的消息，所以其复杂性如声称的那样。

一个进行 q_e 次查询的找然后猜敌手必须希望其在猜阶段的挑战 y 以 0 开头。如果不是，它无法获得超过攻击 $\mathcal{SE}$ 的敌手的优势。以 $1/q_e$ 的概率 y 以 0 开头，所以 $\mathbf{Adv}^{\mathrm{ftg-cpa}}_{\mathcal{SE}'}(k,t,q_e,\mu_e)$（相应地，$\mathbf{Adv}^{\mathrm{ftg-cca}}_{\mathcal{SE}'}(k,t,q_e,\mu_e,q_d,\mu_d)$）至多为 $\epsilon' + (1-\epsilon')/q_e \le \epsilon' + 1/q_e$，其中 ϵ' 是 $\mathbf{Adv}^{\mathrm{ftg-cpa}}_{\mathcal{SE}}(k,t,q_e,\mu_e)$（相应地，$\mathbf{Adv}^{\mathrm{ftg-cca}}_{\mathcal{SE}}(k,t,q_e,\mu_e,q_d,\mu_d)$）。

注意 $\mathcal{SE}'$ 是无状态的（只要 $\mathcal{SE}$ 是无状态的）。如果我们允许构造的方案是有状态的，我们可以稍微改进安全性之间差距的常数因子，使 ϵ' 恰好为 1。为此，我们定义一个有状态加密方案 $\mathcal{SE}'' = (\mathcal{E}'', \mathcal{D}'', \mathcal{K}'')$，它维护一个计数器 ctr，初始为 0。密钥生成器 $\mathcal{K}''$ 输出 (i,a)，其中 $i \xleftarrow{R} \{1,\ldots,q_e\}$ 且 $K \xleftarrow{R} \mathcal{K}(k)$。$\mathcal{E}''$ 如下：

算法 $\mathcal{E}''_{i,K}(x,ctr)$

(1) $ctr \leftarrow ctr + 1$

(2) 如果 $i = ctr$ 则返回 $(ctr, 0\|x)$，否则返回 $(ctr, 1\|\mathcal{E}_K(x))$

（请记住，根据我们对有状态方案的语法，加密算法的输出是一个包含新状态（这里是更新后的计数器）和实际密文的二元组。）$\mathcal{D}''$ 如预期那样。如果我们考虑与上面相同的左或右敌手 A_1，现在与方案 $\mathcal{SE}''$ 一起执行，我们看到它保证在其 q_e 次查询中收到一个第一位为 0 的响应。所以 $\mathcal{SE}''$ 在 LOR-ATK 意义上的优势函数现在是 1，而它在 FTG-ATK 意义上保持不变。

在上述中，将 $\mathcal{SE}$ 的优势函数值视为非常小（几乎为零）。构造的方案 $\mathcal{SE}'$ 可以使用 q_e 次查询以 $\epsilon' = 0.632$ 的概率被攻破，在左或右意义上，意味着它在这个概念下完全不安全。然而，在找然后猜意义上（使用可比较的资源）攻破它的概率是 $\epsilon \approx 1/q_e$。概率满足关系 $q_e\epsilon = \Theta(\epsilon')$，表明定理 4 本质上是紧密的。此外，如果允许方案是有状态的，可以使 ϵ' 恰好为 1，使得 $q_e\epsilon \approx \epsilon'$。

语义安全性过于复杂，不适合作为证明方案安全的良好起点。尽管如此，如下一个定理所示，从语义安全性到找然后猜安全性存在一个强归约是很好的。注意，这只要求语义安全性对一个特定且简单的函数（恒等函数）和一个特定且简单的消息空间分布成立。这个定理在[15]中对非对称设置是隐含的，他们的证明很容易适配到对称设置。

定理 6 [SEM-ATK $\Rightarrow$ FTG-ATK] 对于任何方案 $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$

$$\mathbf{Adv}^{\mathrm{ftg-cpa}}_{\mathcal{SE}}(k, t, q_e, \mu_e) \leq \mathbf{Adv}^{\mathrm{sem-cpa}}_{\mathcal{SE}}(k, t, q_e, \mu_e)$$

$$\mathbf{Adv}^{\mathrm{ftg-cca}}_{\mathcal{SE}}(k, t, q_e, \mu_e, q_d, \mu_d) \leq \mathbf{Adv}^{\mathrm{sem-cca}}_{\mathcal{SE}}(k, t, q_e, \mu_e, q_d, \mu_d).$$

证明：假设 A_3 是在 FTG-ATK 意义上攻击 $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ 的敌手。我们构造一个新的敌手 A_4，使用 A_3，在 SEM-ATK 意义上攻击 $\mathcal{SE}$。我们使用[15]的标准归约，很容易扩展以考虑到预言机的存在。

令 $\mathcal{O}_4(\cdot)$ 是 A_4 的加密预言机，$\mathcal{O}^{-1}(\cdot)$ 是其解密预言机。

算法 $A_4^{\mathcal{O}_3(\cdot),\mathcal{O}^{-1}(\cdot)}(k, \mathrm{select})$

(1) 令 $(x_0, x_1, s) \leftarrow A_3^{\mathcal{O}_4(\cdot),\mathcal{O}^{-1}(\cdot)}(k, \mathsf{find})$

(2) 返回 $((x_0, x_1), (s, (x_0, x_1)))$

也就是说，$\mathcal{M}$ 是二元组 (x_0, x_1)，每个 x_0 和 x_1 被分配概率 $1/2$。

算法 $A_4^{\mathcal{O}_4(\cdot),\mathcal{O}^{-1}(\cdot)}(k, \mathrm{predict}, y, (s, (x_0, x_1)))$

(1) 令 $d \leftarrow A_3^{\mathcal{O}_4(\cdot),\mathcal{O}^{-1}(\cdot)}(k, \mathrm{guess}, y, s)$

(2) 返回 (f, x_d)，其中 f 是恒等函数。

对于 A_4 的优势，我们有，

$$\mathbf{Adv}^{\mathrm{sem-atk}}_{\mathcal{SE},A_4}(k) = \mathrm{Pr}[\mathbf{Exp}^{\mathrm{ftg-atk-1}}_{\mathcal{SE},A_3}(k) = 1] - \mathrm{Pr}[\mathbf{Exp}^{\mathrm{ftg-atk-0}}_{\mathcal{SE},A_3}(k) = 1] = \mathbf{Adv}^{\mathrm{ftg-atk}}_{\mathcal{SE},A_3}(k)$$

利用这个，我们得到了优势函数中的声称关系。

结合这个定理和定理4，得到了从语义安全性到左或右安全性的归约，但这个归约继承了定理4归约的安全性损失。和之前一样，结果证明这种损失是固有的：左或右安全性是一个更强的概念。看到这一点的例子基本上与命题5证明中的相同，但设置变得更加复杂。我们在此不再进一步讨论。

定理 7 [FTG-ATK $\Rightarrow$ SEM-ATK] 对于任何方案 $\mathcal{SE}=(\mathcal{K},\mathcal{E},\mathcal{D})$

$$\begin{aligned}\mathbf{Adv}^{\mathrm{sem\text{-}cpa}}_{\mathcal{SE}}(k,t,q_e,\mu_e) &\le 2\cdot\mathbf{Adv}^{\mathrm{ftg\text{-}cpa}}_{\mathcal{SE}}(k,t,q_e,\mu_e)\\ \mathbf{Adv}^{\mathrm{sem-cca}}_{\mathcal{SE}}(k,t,q_e,\mu_e,q_d,\mu_d) &\le 2\cdot\mathbf{Adv}^{\mathrm{ftg-cca}}_{\mathcal{SE}}(k,t,q_e,\mu_e,q_d,\mu_d).\end{aligned}$$

证明：假设 A_4 是在 SEM-ATK 意义上攻击 $\mathcal{SE}=(\mathcal{K},\mathcal{E},\mathcal{D})$ 的敌手。我们构造一个新的敌手 A_3，使用 A_4，在 FTG-ATK 意义上攻击 $\mathcal{SE}$。

令 $\mathcal{O}_3(\cdot)$ 是 A_3 的加密预言机，$\mathcal{O}^{-1}(\cdot)$ 是其解密预言机。

算法 $A_3^{\mathcal{O}_3(\cdot),\mathcal{O}^{-1}(\cdot)}(k,\mathrm{find})$

(1) 令 $(\mathcal{M},s)\leftarrow A_4^{\mathcal{O}_3(\cdot),\mathcal{O}^{-1}(\cdot)}(k,\mathrm{select})$

(2) 令 $x_0\leftarrow\mathcal{M}$；$x_1\leftarrow\mathcal{M}$

(3) 令 $s'\leftarrow(\mathcal{M},s,x_0,x_1)$

(4) 返回 (x_0,x_1,s')

算法 $A_3^{\mathcal{O}_3(\cdot),\mathcal{O}^{-1}(\cdot)}(k,\mathrm{guess},y,(\mathcal{M},s,x_0,x_1))$

(1) 令 $(f,z)\leftarrow A_4^{\mathcal{O}_3(\cdot),\mathcal{O}^{-1}(\cdot)}(k,\mathrm{predict},y,s)$

(2) 如果 $z=f(x_1)$ 则返回 1；否则返回一个随机比特。

对于 A_3 的优势，我们有，

$$\mathbf{Adv}^{\mathrm{ftg-atk}}_{\mathcal{SE},A_3}(k)=\Pr[\mathbf{Exp}^{\mathrm{sem-atk-1}}_{\mathcal{SE},A_4}(k)=1]-\Pr[\mathbf{Exp}^{\mathrm{sem-atk-0}}_{\mathcal{SE},A_4}(k)=1]=\mathbf{Adv}^{\mathrm{sem-atk}}_{\mathcal{SE},A_4}(k)$$

利用这个，我们得到了优势函数中的声称关系。

在早期工作[15, 22, 11]中，没有对 f 的复杂性做任何限制；甚至允许它是不可计算的。显然，针对如此复杂函数的语义安全性并没有被定义4捕捉到。存在替代的定义和定理（遵循[11]的技术），可用于讨论复杂函数 f（但在讨论简单函数时用处较小）。我们目前不进一步探讨这一点，因为正如我们上面所指出的，其他安全概念更适合实践。

综上所述，展示一个加密方案左或右安全或实或随机安全意味着到所有其他概念的紧密归约。展示一个加密方案找然后猜安全或语义安全则不然。因此，如果界限相等，最好用前两个概念之一来证明安全性，因为这立即转化为其他概念同样良好的界限。

渐近安全性。上述定理意味着所考虑的所有定义（在相同攻击下）在多项式时间归约下是等价的，因为正如定理所示，所有转换只涉及多项式因子。我们只是在说一些更强的东西。

非对称加密。以上所有定义和结果都适用于非对称设置。在那个设置中，为了促进选择明文攻击，没有必要给予敌手加密预言机（但加密预言机仍然保留，用于左或右不可区分性和实或随机不可区分性，以测试敌手的有效性）。对于所有四个定义，重要的是为敌手提供公钥。那么即使在非对称设置中，从具体安全性的角度来看，证明左或右不可区分性的良好界限，也比提供同等良好的找然后猜安全性界限要“更好”。

4 有限域PRF与PRP

我们在本文中研究的对称加密方案基于有限伪随机函数[6]，这是原始伪随机函数概念[14]的具体安全性版本。因此，我们回顾[6]中一些必要的定义。

一个函数族是一个映射 $F\colon \mathrm{Keys}(F) \times \mathrm{Dom}(F) \to \mathrm{Ran}(F)$。这里 $\mathrm{Keys}(F)$ 是 F 的密钥空间；$\mathrm{Dom}(F)$ 是 F 的定义域；$\mathrm{Ran}(F)$ 是 F 的值域。二输入函数 F 接受一个密钥 $K \in \mathrm{Keys}(F)$ 和一个输入 $x \in \mathrm{Dom}(F)$，返回一个点 $F(K,x) \in \mathrm{Ran}(F)$。如果 $\mathrm{Keys}(F) = \{0,1\}^k$ 对于某个整数 k，那么我们称 k 为密钥长度。如果 $\mathrm{Dom}(F) = \{0,1\}^l$ 对于某个整数 l，那么我们称 l 为输入长度。如果 $\mathrm{Ran}(F) = \{0,1\}^L$ 对于某个整数 L，那么我们称 L 为输出长度。在本文中，$\mathrm{Keys}(F), \mathrm{Dom}(F),$ 和 $\mathrm{Ran}(F)$ 总是有限的。对于每个密钥 $K \in \mathrm{Keys}(F)$，我们定义映射 $F_K\colon \mathrm{Dom}(F) \to \mathrm{Ran}(F)$，对所有 $x \in \mathrm{Dom}(F)$ 令 $F_K(x) = F(K,x)$。因此，F 指定了从 $\mathrm{Dom}(F)$ 到 $\mathrm{Ran}(F)$ 的映射集合，每个映射与一个密钥相关联。这就是为什么 F 被称为函数族。我们将 F_K 称为 F 的一个实例。我们经常谈论从 $\mathrm{Keys}(F)$ 中均匀选择随机密钥 K。这个操作写作 $K \xleftarrow{R} \mathrm{Keys}(F)$。我们写作 $f \xleftarrow{R} F$ 表示操作 $K \xleftarrow{R} \mathrm{Keys}(F)$；$f \leftarrow F_K$。也就是说，$f \xleftarrow{R} F$ 表示从族 F 中随机选择一个函数的操作。当 f 被这样选择时，它被称为 F 的随机实例。如果 $\mathrm{Dom}(F) = \mathrm{Ran}(F)$，并且对于每个密钥 $K \in \mathrm{Keys}(F)$，F_K 是 $\mathrm{Dom}(F)$ 上的一个置换（即双射），那么我们说 F 是一个置换族。

为了定义PRF和PRP，我们首先需要固定两个函数族。一个是 $\mathrm{Rand}^{l \to L}$，所有从 $\{0,1\}^l$ 到 $\{0,1\}^L$ 的函数的族，另一个是 Perm^l，所有在 $\{0,1\}^l$ 上的置换的族。

定义 5 [PRF 和 PRP 族, [6]] 令 F 为具有输入长度 l 和输出长度 L 的函数族，P 为具有长度 l 的置换族。令 $b \in \{0,1\}$。令 $D_{\mathrm{fn}}, D_{\mathrm{pn}}$ 为可以访问预言机 $\mathcal{O}_b(\cdot)$ 的区分器。现在，我们考虑以下实验：

Experiment Expprf-bF, Dfn	Experiment Expprp-bP, Dpn
O0←R Randl→L; O1←R F	O0←R Perml; O1←R P
d←DOb(·)	d←DpnOb(·)
Return d	Return d

我们通过以下方式定义区分器的优势：

$$\mathbf{Adv}^{\mathrm{prf}}_{F,D_{\mathrm{fn}}} = \Pr\left[\mathbf{Exp}^{\mathrm{prf}-1}_{F,D_{\mathrm{fn}}} = 1\right] - \Pr\left[\mathbf{Exp}^{\mathrm{prf}-0}_{F,D_{\mathrm{fn}}} = 1\right]$$

$$\mathbf{Adv}^{\mathrm{prp}}_{P,D_{\mathrm{pn}}} = \Pr\left[\mathbf{Exp}^{\mathrm{prp}-1}_{P,D_{\mathrm{pn}}} = 1\right] - \Pr\left[\mathbf{Exp}^{\mathrm{prp}-0}_{P,D_{\mathrm{pn}}} = 1\right].$$

我们如下定义函数族的优势函数。对于任意整数 t, q，

$$\mathbf{Adv}^{\mathrm{prf}}_{F}(t,q) = \max_{D_{\mathrm{fn}}}\{\mathbf{Adv}^{\mathrm{prf}}_{F,D_{\mathrm{fn}}}\}$$

$$\mathbf{Adv}^{\mathrm{prp}}_{P}(t,q) = \max_{D_{\mathrm{pn}}}\left\{\mathbf{Adv}^{\mathrm{prp}}_{P,D_{\mathrm{pn}}}\right\}$$

其中最大值取自所有时间复杂性为 t 的 $D_{\mathrm{fn}}, D_{\mathrm{pn}}$，每个区分器至多对预言机进行 q 次查询。

注意，由于我们讨论的是有限族 F, P，所以没有固定或形式化的“安全”PRF或PRP族概念。每个族都有作为PRF或PRP族的某种相关的不安全性。我们仅在非正式讨论中使用术语“F 是安全的PRF”，来表示 $\mathbf{Adv}^{\mathrm{prf}}_{F}(t,q)$ 对于“合理的” t, q 值是“低的”。还要注意，与Luby和Rackoff[21]不同，我们相对于随机置换族而不是随机函数族来衡量PRP族的质量。这的动机

是，正如我们所定义的，PRPs是比PRFs更好的分组密码模型。（当然，区别仅在于具体安全性，但这确实是我们关心的。）尽管如此，以下两个概念之间的关系通常是足够的：

命题 8 [PRPs 是 PRFs] 对于任何具有长度 l 的置换族 P，

$$\mathbf{Adv}^{\mathrm{prf}}_{P}(t,q) \leq \mathbf{Adv}^{\mathrm{prp}}_{P}(t,q) + q^2 2^{-l-1}.$$

分组密码是一个（有限）置换族。例如，DES是一个置换族，其中 Keys(DES) = {0,1}56 且 Dom(DES) = Ran(DES) = {0,1}64。对分组密码估计的密码分析强度为我们提供了 t, q 的值，对于这些值，该分组密码可被视为PRP族。使用命题8，我们得到了它可以被视为PRF族的界限。

5 XOR与CTR方案的分析

固定一个具有输入长度 l、输出长度 L 和密钥长度 k 的函数族 F。我们令 K 表示运行加密方案的双方共享的密钥。它将用于指定函数 $f = F_K$。实际上，所有方案都只依赖于这个函数，因为它们可以在给定该函数预言机的情况下实现。

CTR方案是有状态的（基于计数器且确定性的）。XOR方案是CTR的一种无状态（随机化）变体。

规范。方案 $\mathrm{XOR}[F] = (\mathcal{E}\text{-XOR}, \mathcal{D}\text{-XOR}, \mathcal{K}\text{-XOR})$ 工作如下。密钥生成算法 $\mathcal{K}$-XOR 只是输出一个随机的 k 比特密钥 K 用于底层PRF族 F，从而指定一个从 l 比特到 L 比特的函数 $f = F_K$。要加密的消息 x 被视为一系列 L 比特块（如有必要，首先进行填充），$x = x_1 \cdots x_n$。我们定义 $\mathcal{E}\text{-XOR}_K(x) = \mathcal{E}\text{-XOR}^{F_K}(x)$ 和 $\mathcal{D}\text{-XOR}_K(z) = \mathcal{D}\text{-XOR}^{F_K}(z)$，其中：

function $\mathcal{E}$-XORf(x)

$r \leftarrow \{0,1\}^l$

for $i = 1, \ldots, n$ do $y_i = f(r + i) \oplus x_i$

return $r \parallel y_1 y_2 \ldots y_n$

function $\mathcal{D}$-XORf(z)

Parse z as $r \parallel y_1 \ldots y_n$

for $i = 1, \ldots, n$ do $x_i = f(r + i) \oplus y_i$

return $x = x_1 \cdots x_n$

我们称 r 为现时值。上面的加法是模 2^l 的，结果以通常的方式编码为 l 比特字符串。

这个方案的有状态变体是 $\mathrm{CTR}[F] = (\mathcal{E}\text{-CTR}, \mathcal{D}\text{-CTR}, \mathcal{K}\text{-CTR})$。这里 r 的角色由一个 l 比特计数器扮演，记为 ctr，初始为 -1，每次加密后增加加密的块数。注意只有发送方维护计数器，并且它作为密文的一部分输出。对方案的一个限制是加密块的总数不超过 2^l。

密钥生成算法 $\mathcal{K}$-CTR 和之前一样，意思是只输出一个用于PRF族的随机密钥 K。采用与上面相同的格式约定，我们定义 $\mathcal{E}\text{-CTR}_K(x, ctr) = \mathcal{E}\text{-CTR}^{F_K}(x, ctr)$ 和 $\mathcal{D}\text{-CTR}_K(z) = \mathcal{D}\text{-CTR}^{F_K}(z)$，其中：

function $\mathcal{E}$-CTRF(x,ctr)

for $i = 1, \ldots, n$ do $y_i = f(ctr + i) \oplus x_i$

$ctr \leftarrow ctr + n$

return (ctr, ctr $\| y_1 y_2 \ldots y_n$)

function $\mathcal{D}$-CTRf(z)

Parse z as $ctr \| y_1 \ldots y_n$

for $i = 1, \ldots, n$ do $x_i = f(ctr + i) \oplus y_i$

return $x = x_1 \ldots x_n$

方案特点。注意解密不需要反转 $f = F_K$ 的能力。因此 F_K 不必是置换。

XOR和CTR方案比更常见的操作模式有一些计算上的优势。即，不同块上的 F_K 计算可以并行完成，因为一个块上的计算独立于其他块。这种可并行性优势可以通过硬件或软件支持实现。如果每个块都带有其索引标签，则解密不必按顺序进行。这些方案也支持离线处理，因为 F_K 计算可以在它们要使用的消息可用之前的空闲时间完成。

XOR的安全性。我们给出 XOR $[F]$ 方案优势函数的界限，假设 F 是有限PRF族。由于这种情况下没有渐近性，我们在表示中去掉了安全参数 k。对于我们在本工作中研究的所有其他方案，也遵循这个约定。

我们首先推导一个试图在LOR-CPA意义上攻破 XOR $[F]$ 方案的敌手成功率的下界。在常见的密码学术语中，这意味着我们只是提供一个攻击。我们指定的攻击是针对“理想”方案 XOR[Rand $^{l \to L}$] 的。

命题 9 [使用随机函数的XOR不安全性的下界] 假设 $R = \text{Rand}^{l \to L}$。那么，对于任何满足 $\mu_e q_e / L \leq 2^l$ 的 q_e, μ_e，

$$\mathbf{Adv}^{\text{lor-cpa}}_{\text{XOR}[R]}(\cdot, t, q_e, \mu_e) \geq 0.316 \cdot \frac{\mu_e \cdot (q_e - 1)}{L \cdot 2^l}.$$

这是一个“生日”攻击。如果我们令 $\bar{n} = \mu_e / (L q_e)$ 为每次查询的平均块数，使得 $\mu_e = L q_e \cdot \bar{n}$，可能更容易衡量。然后我们看到优势函数是 $\Omega(q_e^2 / 2^l) \cdot \bar{n}$，这是典型的生日行为，显示了对查询数量的二次依赖。

由于我们在随机函数模型中证明了下界，我们不讨论时间复杂性。但从策略上可以清楚地看出，时间复杂性除了进行预言机调用的时间外，只是一点开销。这对于所有下界都是正确的，我们不再提及。命题9表明，即使底层分组密码 F 非常好（它不能比真正随机更好），XOR方案在加密越来越多的数据时也会泄露一些信息。接下来，我们证明上述攻击本质上是可能的最佳攻击：无法获得更好的优势，除了一个常数因子。

引理 10 [使用随机函数的XOR不安全性的上界] 假设 $R = \text{Rand}^{l \to L}$。那么，对于任何 t, q_e, μ_e，

$$\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{XOR}[R]}(\cdot, t, q_e, \mu_e) \le \frac{\mu_e \cdot (q_e - 1)}{L \cdot 2^l}.$$

当然，在理想模型中的安全性指示并不意味着使用分组密码时的安全性指示。然而，“真实世界”的情况很容易从上述推导出来：

定理 11 [使用伪随机函数的XOR的安全性] 假设 F 是一个具有输入长度 l 和输出长度 L 的 PRF 族。那么，对于任何 t, q_e 和 $\mu_e = q' L$，

$$\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{XOR}[F]}(\cdot, t, q_e, \mu_e) \le 2 \cdot \mathbf{Adv}^{\mathrm{prf}}_{F}(t, q') + \frac{\mu_e \cdot (q_e - 1)}{L \cdot 2^l}.$$

CTR的安全性。该方案的有状态版本具有更好的安全性。敌手在理想情况下没有优势：

引理 12 [使用随机函数的CTR的安全性] 假设 $R = \mathrm{Rand}^{l \to L}$。那么，对于任何 t, q_e 和 $\mu_e \le L 2^l$，

$$\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{CTR}[R]}(\cdot, t, q_e, \mu_e) = 0.$$

这转化为以下“真实世界”的安全性：

定理 13 [使用伪随机函数的CTR的安全性] 假设 F 是一个具有输入长度 l 和输出长度 L 的 PRF 族。那么，对于任何 t, q_e 和 $\mu_e = \min(q' L, L 2^l)$，

$$\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{CTR}[F]}(\cdot, t, q_e, \mu_e) \le 2 \cdot \mathbf{Adv}^{\mathrm{prf}}_{F}(t, q').$$

证明。以下在各种估计中会有用：

事实 14 对于任何满足 $0 \le x \le 1$ 的实数 x，我们有 $(1 - e^{-1})x \le 1 - e^{-x} \le x$

我们在整个证明中使用以下符号。如果 x 是一个长度是 L 的倍数的字符串，我们将其视为一系列 L 比特块。我们令 $n = |x|_L$ 表示块数，$x[i]$ 表示第 i 块，使得 $x = x[1] \dots x[n]$。对于一个整数 m，令 $[m] = \{1, \dots, m\}$。在证明中，我们令 q 表示 q_e，μ 表示 μ_e。

命题9的证明：通过构造一个达到给定安全参数的敌手来证明。回想一下，LOR-CPA意义上的敌手进行由消息对组成的加密预言机查询，试图区分是加密对中的左半部分还是右半部分。我们的敌手 A 寻找底层方案使用的随机函数 f 的输入碰撞。

算法 $A^{\mathcal{O}(\cdot,\cdot)}(k)$

(1) 令 $n = \mu/(Lq)$。（这将是所有查询消息中的块数。）

(2) 选择消息 $N_1, \dots, N_q$，全部 n 块长，使得对于所有 $i, j = 1, \dots, q$ 和 $k, k' = 1, \dots, n$ 满足 $(i, k) \ne (j, k')$，有 $N_i[k] \ne N_j[k']$。（例如，对于 $i = 1, \dots, q$ 和 $k = 1, \dots, n$，设 $N_i[k]$ 为整数 $n(i-1) + k$ 的 L 比特二进制编码。）

(3) 对于 $i = 1, \dots, q$ 执行：$(r_i, y_i[1] \dots y_i[n]) \leftarrow \mathcal{O}(0^{nl}, N_i)$。我们称 r_i 为第 i' 个现时值。

(4) 如果存在 $i \ne j$ 使得 $|r_i - r_j| < n$（这里将 r_i, r_j 视为整数！）则确定值 $k, k' \in \{1, \dots, n\}$ 使得 $r_i + k = r_j + k'$。如果 $y_i[k] = y_j[k']$ 则输出1，否则输出2。

(5) 如果不存在 $i \ne j$ 使得 $|r_i - r_j| < n$，则输出抛硬币的结果。

令 OverlapNonce 为对于某个 $i \neq j$ 有 $|r_i - r_j| < n$ 的事件。每当这个事件发生时，我们就说发生了现时值重叠。我们声称 A 的优势恰好是 OverlapNonce 的概率。为了看到这一点，首先观察到该事件的概率在两个游戏中是相同的，因为它只涉及随机现时值。令 p 为这个概率。令 $\Pr_b[A=1]$ 为 A 声明它在玩游戏0时的概率，而实际上它在玩游戏 $b \in \{0,1\}$ 。我们有

$$\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{XOR}[R],A}(\cdot) = \mathrm{P}_1\mathrm{r}[A=1] - \mathrm{P}_0\mathrm{r}[A=1] = \left(p \cdot 1 + (1-p)\cdot\frac{1}{2}\right) - \left(p \cdot 0 + (1-p)\cdot\frac{1}{2}\right) = p$$

现在我们想下界 p。令 D_i 为直到第 i 次查询（包括第 i 次查询）都没有发生现时值重叠的事件。我们观察到，要使 D_{i+1} 为真，第 $(i+1)$ 次查询的现时值不能与先前任何 i 次查询的现时值重叠。就第 $(i+1)$ 个现时值可以假设的值而言，我们注意到至少有 in 个值会导致现时值重叠。（通常可能有多达 $i(n-1)$ 个这样的值，但我们现在可以忽略它们，因为我们的兴趣是 p 的下界。）因此我们有

$$\Pr\left[\mathsf{D}_{i+1} \mid \mathsf{D}_i\right] \leq \frac{2^l - in}{2^l} = 1 - \frac{in}{2^l}.$$

在第 q 次查询结束时没有现时值重叠的概率现在可以计算如下

$$\Pr\left[\mathsf{D}_q\right] = \prod_{i=1}^{q-1} \Pr\left[\mathsf{D}_{i+1} \mid \mathsf{D}_i\right] \leq \prod_{i=1}^{q-1}\left(1 - \frac{in}{2^l}\right) \leq \prod_{i=1}^{q-1} e^{-in/2^l} = e^{-nq(q-1)/2^{l+1}}.$$

最后一个不等式来自事实14。继续，

$$p = \mathrm{P}\,\mathrm{r}[\mathsf{OverlapNonce}] = 1 - \mathrm{P}\,\mathrm{r}[\mathsf{D}_q] \geq 1 - e^{-nq(q-1)/2^{l+1}} = 1 - e^{-(1/2)\cdot\mu(q-1)/(L2^l)}.$$

我们假设了 $\mu q/L \leq 2^l$。这意味着 $x \stackrel{\mathrm{def}}{=} \mu(q-1)/(L2^l) \leq 1$，我们可以应用事实14的不等式 $1 - e^{-x} \geq (1-e^{-1})x$ 得到

$$p \geq \left(1 - \frac{1}{e}\right)\cdot\frac{1}{2}\cdot\frac{\mu(q-1)}{L2^l},$$

这就证明了该命题。

引理10的证明：令 $(M_1, N_1), \ldots, (M_q, N_q)$ 为敌手 A 的预言机查询，每个查询根据定义由一对等长消息组成。这些查询是依赖于 A 的随机选择和预言机对先前查询的响应的随机变量。令 $r_i \in \{0,1\}^l$ 为与 (M_i, N_i) 相关联的现时值，由预言机随机选择，$i = 1, \ldots, q$。令 n_i 为第 i 次查询中的块数。在回答第 i 次查询时，预言机将底层函数 f 应用于 n_i 个字符串 $r_i + 1, \ldots, r_i + n_i \in \{0,1\}^l$。我们称这些字符串为第 i 个序列，$r_i + k$ 是该序列中的第 k 个点，$k = 1, \ldots, n_i$。

令 D 为以下事件，定义为针对任一游戏：每当 $(i,k) \neq (j,k')$ 时，有 $r_i + k \neq r_j + k'$，对于所有 $i, j = 1, \ldots, q$ 和 $k = 1, \ldots, n_i$ 以及 $k' = 1, \ldots, n_j$。也就是说，D 是在所有查询中随机函数的输入上没有发生碰撞的事件（或者等价地，没有重叠序列）。我们还定义 $\Pr_0[\cdot]$ 为事件在游戏0中的概率，$\Pr_1[\cdot]$ 为事件在游戏1中的概率。

声称 1. $\Pr_0\left[\overline{\mathsf{D}}\right] = \Pr_1\left[\overline{\mathsf{D}}\right]$

证明：对于任一游戏，事件 D 仅取决于为每个查询选择的现时值。现时值本身是随机选择的，因此独立于正在进行的游戏（或给予预言机的消息）。 □

声称 2. $\Pr_0\left[A=1 \mid \mathsf{D}\right] = \Pr_1\left[A=1 \mid \mathsf{D}\right]$

证明：给定事件 D，在任一游戏中，每次调用函数 f 时，它都是在一个新点上求值，因此输出随机且均匀地分布在 $\{0,1\}^L$ 上，独立于其他任何东西。因此每个密文块是一个消息块与一个随机值的异或。由此得出的一个结果是，每个密文块的分布独立于任何先前的密文块和消息。

我们现在上界 A 的优势如下：

$$\begin{aligned}&\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{XOR}[R],A}(\cdot) = \mathrm{P\ r}_1[A=1] - \mathrm{P\ r}_0[A=1]\\ &= \mathrm{Pr}_1\left[A=1 \mid \overline{\mathsf{D}}\right]\cdot\mathrm{Pr}_1\left[\overline{\mathsf{D}}\right] + \mathrm{Pr}_1\left[A=1 \mid \mathsf{D}\right]\cdot\mathrm{Pr}_1\left[\mathsf{D}\right] -\\ &\mathrm{P\ r}_0\left[A=1 \mid \overline{\mathsf{D}}\right]\cdot\mathrm{P\ r}_0\left[\overline{\mathsf{D}}\right] - \mathrm{P\ r}_0[A=1 \mid \mathsf{D}]\cdot\mathrm{P\ r}_0[\mathsf{D}]\end{aligned}$$

使用声称1和声称2，我们有，

$$\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{XOR}[R],A}(\cdot) = \left(\mathrm{P}_1\mathrm{r}\left[A=1 \mid \overline{\mathsf{D}}\right] - \mathrm{P}_0\mathrm{r}\left[A=1 \mid \overline{\mathsf{D}}\right]\right)\cdot\mathrm{P}_1\mathrm{r}\left[\overline{\mathsf{D}}\right] \le \mathrm{P}_1\mathrm{r}\left[\overline{\mathsf{D}}\right]$$

根据声称1，我们去掉谈论 D 概率时的下标，将上式写作 $\mathrm{Pr}[\overline{\mathsf{D}}]$。现在我们想上界 $\mathrm{Pr}[\overline{\mathsf{D}}]$。我们观察到，在选择第 i 个现时值时发生碰撞的概率，如果所有先前的 $i-1$ 次查询导致 $i-1$ 个输入序列与 f 的距离不小于 $n_i - 1$ 块，则是最大的。如果第 i 个序列开始于任何其他先前序列 j 之前 $n_i - 1$ 块的块位置，或者开始于该序列 j 占据的块位置，就会发生碰撞。现在令第 i 个序列与任何先前序列碰撞的概率为 p_i。那么我们有，对于 $i > 1$

$$p_i \le \frac{\sum_{j=1}^{i-1}(n_j + n_i - 1)}{2^l} = \frac{(i-1)(n_i-1) + \sum_{j=1}^{i-1} n_j}{2^l}.$$

因此

$$\mathrm{P\ r}[\overline{\mathsf{D}}] \le \sum_{i=1}^{q} p_i \le \sum_{i=1}^{q} \frac{\left((i-1)(n_i-1) + \sum_{j=1}^{i-1} n_j\right)}{2^l} = \frac{\frac{\mu}{L}(q-1) - \frac{q(q-1)}{2}}{2^l} \le \frac{\mu(q-1)}{L\cdot 2^l}.$$

将所有内容放在一起，我们有 $\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{XOR}[R],A}(\cdot) \le \frac{\mu(q-1)}{L\cdot 2^l}$。

定理11的证明：直观上，引理10说 $\mathrm{XOR}\,[R]$ 是安全的。如果 $\mathrm{XOR}\,[F]$ 不安全，这将意味着 F 作为PRF函数族不好。形式上，我们通过矛盾论证来证明该定理。假设 A 是在 LOR-CPA 意义上攻击 $\mathrm{XOR}\,[F]$ 的敌手，并且其优势大于 $\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{XOR}[F]}(k,t,q_e,\mu_e)$。我们构建一个区分器 D，使用 A，其优势优于 $\mathbf{Adv}^{\mathrm{prf}}_{F}(t,q')$，对于某个合理的 q' 值，这与 F 作为伪随机函数族假定的安全性相矛盾。我们的区分器只是运行 A，并试图观察 A 是否攻破了加密方案。如果是，它打赌 f 来自 F，否则打赌 f 来自 R。为了运行 A，它通过查询自己的预言机 f 来模拟 A 的预言机 $\mathcal{O}(\cdot,\cdot)$，使用后者作为加密方案的底层函数。更详细地说：

算法 $D^f(k)$

(1) $b \leftarrow \{0,1\}$。（这代表为 A 选择左或右预言机的选择。）

(2) 运行 A，如下响应其预言机查询。当 A 进行预言机查询 (M_1, M_2) 时，令 $z \leftarrow \mathcal{E}\text{-}\mathrm{XOR}^f(M_b)$，并将 z 作为预言机查询的答案返回给 A。（这里重要的是，D 在给定 f 的预言机时可以实现加密函数。）

(3) 最终 A 停止并输出一个猜测 d，以指示它认为其预言机是左预言机还是右预言机。如果 $d = b$ 则输出 1，否则输出 0。

在响应预言机查询 (M_1, M_2) 时，区分器 D 对 f 进行 n 次预言机查询，其中 $n = |M_1|/L = |M_2|/L$ 是消息中的块数。所以 D 进行的预言机查询总数至多为 μ/L，根据假设是 q'。

为了计算 $\mathbf{Adv}^{\mathrm{prf}}_{F,D}$，我们首先需要一些符号。对于 $G \in \{F, R\}$，令 $\mathsf{Correct}(G)$ 为当加密方案底层函数为 $f \leftarrow G$ 时 A 正确识别其预言机的概率。可以验证 $\mathsf{Correct}(G) = (1/2) \cdot [1 + \mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{XOR}(G),A}]$。现在注意

$$\mathbf{Adv}^{\mathrm{prf}}_{F,D} = \mathrm{Correct}(F) - \mathrm{Correct}(R) = (1/2) \cdot \left[\mathbf{Adv}^{\mathrm{lor\text{-}cpa}}_{\mathrm{XOR}[F],A}(\cdot) - \mathbf{Adv}^{\mathrm{lor\text{-}cpa}}_{\mathrm{XOR}[R],A}(\cdot)\right].$$

引理10为我们提供了 $\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{XOR}[R],A}(\cdot)$ 的界限。利用这个，我们看到为了避免矛盾，我们必须如定理陈述中那样界定优势函数。

引理12的证明：与引理10的证明类似。区别在于对于 $\mu/L \leq 2^l$，有 $\Pr_0\left[\overline{\mathsf{D}}\right] = \Pr_1\left[\overline{\mathsf{D}}\right] = 0$。这是因为计数器在加密了 2^l 个块之前不会重复。

定理13的证明：与定理11的证明类似，略。

6 CBC方案的分析

对于CBC方案，我们要求 $l = L$（F 的输入长度和输出长度相同）并且每个 F_K 是一个置换，使得给定 K 我们不仅可以计算 F_K 还可以计算 F_K^{-1}。

规范。方案 $\mathrm{CBC}[F] = (\mathcal{E}\text{-CBC}, \mathcal{D}\text{-CBC}, \mathcal{K}\text{-CBC})$ 具有与先前方案相同的密钥生成算法，意味着加密密钥是指定 $f = F_K$ 的密钥 K。要加密的消息 x 被视为一系列 l 比特块，$x = x_1 \ldots x_n$。我们定义 $\mathcal{E}\text{-CBC}_K(x) = \mathcal{E}\text{-CBC}^{F_K}(x)$ 和 $\mathcal{D}\text{-CBC}_K(z) = \mathcal{D}\text{-CBC}^{F_K}(z)$，其中：

function E-CBCf(x) y0←{0,1}l for i=1,...,n do yi=f(yi-1 ⊕ xi) return y0‖y1y2···yn	function D-CBCf(z) Parse z as y0 // y1···yn for i=1,...,n do xi=f-1(yi) ⊕ yi-1 return x=x1...xn

值 y_0 称为初始向量或现时值。关于计数器变体的讨论见下文。

方案特点。我们已经提到XOR和CTR方案相对于CBC方案的计算优势。然而，CBC方案比这些其他方案具有更好的错误传播和错误恢复特性。CBC是自同步的，因为几个密文块的损坏甚至丢失只会妨碍几个明文块的正确解密，而不需要显式的重新同步。

CBC的安全性。$\mathrm{CBC}[F]$ 方案的分析应假设 F 是PRP族，而不是PRF族，因为该方案确实必须与置换一起使用，而不是函数。然而，使用函数而不是置换进行分析要简单得多。因此，我们的方法如下。对于上界（关于 $\mathrm{CBC}[F]$ 的不安全性），我们首先分析 $\mathrm{CBC}[\mathrm{Rand}^{l \to l}]$（即使用随机函数的方案）。然后，类似于定理11，我们推导 $\mathrm{CBC}[F]$ 的安全性，假设 F 是PRF族。最后，使用命题8，我们将其转化为当 F 被视为PRP族时的安全性。然而，对于下界，这种方法行不通。因此我们直接推导下界。

命题 15 [使用随机置换的CBC不安全性的下界] 假设 $R = \mathrm{Perm}^l$。那么，对于 $\mu_e \leq l \cdot 2^{\frac{l}{2}}$ 且 $q_e = \mu_e / l$，

$$\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{CBC}[R]}(\cdot, t, q_e, \mu_e) \geq 0.316 \cdot \left(\frac{\mu_e^2}{l^2} - \frac{\mu_e}{l}\right) \cdot \frac{1}{2^l}.$$

接下来，我们证明这是除常数因子外可能的最佳攻击。

引理 16 [使用随机函数的CBC不安全性的上界] 假设 $R = \mathrm{Rand}^{l \to l}$。那么，对于任何 t, q_e, μ_e，

$$\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{CBC}[R]}(\cdot, t, q_e, \mu_e) \leq \left(\frac{\mu_e^2}{l^2} - \frac{\mu_e}{l} \right) \cdot \frac{1}{2^l}.$$

“真实世界”的安全性如下：

定理 17 [使用伪随机置换的CBC的安全性] 假设 F 是一个具有长度 l 的 PRP 族。那么，对于任何 t, q_e 和 $\mu_e = ql$，

$$\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{CBC}[F]}(\cdot, t, q_e, \mu_e) \leq 2 \cdot \mathbf{Adv}^{\mathrm{prp}}_{F}(t, q) + q^2 2^{-l-1} + \left(\frac{\mu_e^2}{l^2} - \frac{\mu_e}{l} \right) \cdot 2^{-l}.$$

带计数器的CBC。很诱人去制作CBC的计数器变体，并希望安全性提高（或至少保持）。确实，在各种书籍中建议初始化向量可以是一个计数器。但这不起作用；知道计数器的下一个值，敌手可以选择一个消息查询，强制 f 的输入发生碰撞，从而攻破方案（在任何定义下）。

要制作CBC的合适计数器版本，可以让初始化向量为 $y_0 = f(ctr)$，并在每次加密后将 ctr 增加一。该方案最多能加密 2^l 条消息。然后可以有一个类似于定理17的类比。如果用于确定 y_0 的密钥与用于CBC加密其余部分的密钥分开，这个结果最容易（作为定理17的推论）得出。

证明。我们从对 $\mathrm{CBC}[\mathrm{Perm}^l]$ 的攻击开始。

命题15的证明：思路是，只需在初始向量（现时值）中找到碰撞。细节如下。

敌手设 $q = \mu/l$。然后对于 $i = 1, \ldots, q$，设 $M_i = 0^l$，并选择 $N_1, \ldots, N_q$ 为不同的非零 l 比特字符串。它进行 q 次查询，由消息对 $(M_1, M_1'), \ldots, (M_q, M_q')$ 组成。令 $C_i[0] C_i[1]$ 表示对第 i 次查询的响应。如果 $C_1[0], \ldots, C_q[0]$ 全部不同，则敌手抛硬币决定其输出。否则，令 $i \neq j$ 使得 $C_i[0] = C_j[0]$。敌手在 $C_i[1] = C_j[1]$ 时输出 1，否则输出 2。很容易看出，优势恰好是初始向量中出现碰撞的概率。我们使用事实14中的下界来界定这个优势。

注意在上述攻击中，给定 μ_e，我们允许敌手选择一个方便的 q_e。结果证明是 $q_e = \mu_e/l$。有可能证明更强的东西，即对于任何给定的 q_e 值都可以发起攻击。这个的证明，再次是通过构造一个达到给定安全参数的敌手。我们的敌手 A 寻找底层方案使用的随机函数 f 的输入碰撞。

算法 $A^{\mathcal{O}(\cdot,\cdot)}$

(1) 令 $n = \mu/(lq)$。（这将是所有查询消息中的块数。）令 $T = [q] \times [n]$。

(2) 选择消息 $M_1, \ldots, M_q$，全部 n 块长，使得对于所有不同的 $(i,k), (j,k') \in T$，有 $M_i[k] \neq M_j[k']$。（例如，对于所有 $(i,k) \in T$，设 $M_i[k]$ 为整数 $n(i-1)+k$ 的 l 比特二进制编码。）同时设 $M_i'[k] = 0^l$ 且 $M_i' = M_i'[1] \ldots M_i'[n]$，对于所有 $(i,k) \in T$。

(3) 对于 $i = 1, \ldots, q$ 执行：$(C_i[0], C_i[1] \ldots C_i[n]) \leftarrow \mathcal{O}(M_i, M_i')$。我们称 $C_i[0]$ 为第 i' 个初始向量。

(4) 如果 D 为真，则输出抛硬币的结果并停止。否则（意味着 D 为假）继续执行下面的算法其余部分。

(5) 令 $(j,k) \in T$ 为使得 $\mathsf{D}_{j,k}$ 为假的最小对。（意思是如果存在其他对 $(j',k') \in T$ 使得 $\mathsf{D}_{j',k'}$ 为假，则 $(j,k) \prec (j',k')$。）

(6) 如果存在 $(j',k') \prec (j,k)$ 使得 $C_j[k-1] \oplus M_j[k] = C_{j'}[k'-1] \oplus M_{j'}[k']$，则设 $b_0 = 1$ 并测试 $C_j[k] = C_{j'}[k']$。如果测试通过则设 $a_0 = 1$ 否则设 $a_0 = 0$。否则设 $b_0 = 0$。

(7) 如果存在 $(j',k') \prec (j,k)$ 使得 $C_j[k-1] = C_{j'}[k'-1]$，则设 $b_1 = 1$ 并测试 $C_j[k] = C_{j'}[k']$。如果测试通过则设 $a_1 = 1$ 否则设 $a_1 = 0$。否则设 $b_1 = 0$。

(8) 如果 $b_1 = 1$ 则：如果 $a_1 = 1$ 则输出 1，否则输出 0。

(9) 否则（意味着 $b_1 = 0$）必须 $b_0 = 1$。那么如果 $a_0 = 1$ 则输出 0，否则输出 1。

我们省略了这个攻击的分析细节，注意到允许选择方便的 q_e 的攻击所推导出的相同下界在这种情况下也成立。

接下来，我们给出一个引理，该引理在证明引理16时会有用。

考虑一个任意敌手 A，在 LOR-CPA 意义上攻击 $\mathrm{CBC}[R]$（其中 $R = \mathrm{Rand}^{l \to l}$）。它向其预言机 $\mathcal{O}(\cdot,\cdot)$ 进行至多 q 次查询，总计至多 μ 比特。令 $(M_1, M_1'), \ldots, (M_q, M_q')$ 为敌手 A 的预言机查询，每个查询根据定义由一对等长消息组成。这些查询是依赖于 A 的随机选择和预言机对先前查询的响应的随机变量。令 $n_i = |M_i|_l = |M_i'|_l$ 为第 i 次查询中消息的块数，$i = 1, \ldots, q$。令 $C_i = C_i[0] \ldots C_i[n_i]$ 为随机变量，它是预言机对查询 (M_i, M_i') 的响应，$i = 1, \ldots, q$。

一些符号将有用。令 $T = \{(j,k) : j \in [q] \text{ 且 } k \in [n_j]\}$ 且 $T' = \{(j,k) : j \in [q] \text{ 且 } k = 0, \ldots, n_j\}$ 且 $T'' = \{(j,k) : j \in [q] \text{ 且 } k = 0, \ldots, n_j + 1\}$。我们在 T'' 上定义一个顺序 $\prec$ 如下：

$$(j,k) \prec (j',k') \quad \text{当且仅当} \quad \left(\sum_{i=1}^{j-1}(n_i+2)\right) + k < \left(\sum_{i=1}^{j'-1}(n_i+2)\right) + k',$$

对于任意 $(j,k),(j',k') \in T''$。如果 $(j,k) \prec (j',k')$ 或 $(j,k) = (j',k')$，我们写作 $(j,k) \preceq (j',k')$。当然，这个顺序继承到 T'' 的任何子集，我们最常在 T 或 T' 上使用它。

我们令 $\Pr_b[\cdot]$ 表示游戏 $b \in \{0,1\}$ 中的概率分布，其中游戏 b 是 $\mathcal{O}(\cdot,\cdot) = \mathcal{E}\text{-}\mathrm{CBC}^f(\mathcal{LR}(\cdot,\cdot,b))$ 的游戏，$f \leftarrow R$。我们知道在游戏0中 $C_j[k] = C_j[k-1] \oplus M_j[k]$，在游戏1中 $C_j[k] = C_j[k-1] \oplus M_j'[k]$，对于所有 $j \in [q]$ 和 $k \in [n_j]$。以下定义了一个事件，针对任一游戏，表示在任一游戏中直到指定点，f 的输入没有碰撞。

定义 6 [事件 Distinct] 在上述设定中，固定敌手 A，对于 $i \in [q]$ 和 $u \in [n_i]$，定义事件 $D_{i,u}$（称为 distinct）为真，如果

$$C_j[k-1] \oplus M_j[k] \neq C_{j'}[k'-1] \oplus M_{j'}[k'] \text{且} C_j[k-1] \oplus M_j'[k] \neq C_{j'}[k'-1] \oplus M_{j'}'[k']$$

对于满足 $(j',k') \prec (j,k) \preceq (i,u)$ 的 $(j,k),(j',k') \in T$。

令 $\mathsf{D} \equiv \mathsf{D}_{q,n_q}$。同时令 $\mathsf{D}_{1,0}$ 为总是真的事件，对于 $i \geq 2$ 令 $\mathsf{D}_{i,0} \equiv \mathsf{D}_{i-1,n_{i-1}}$。最后对于 $i \in [q]$ 令 $\mathsf{D}_{i,n_i+1} \equiv \mathsf{D}_{i,n_i}$。

事实证明，D 的概率几乎告诉了我们关于敌手优势的所有信息。

引理 18 [主 CBC 引理] 令 A 为上述设定中 $\mathrm{CBC}[R]$ 的敌手。那么

(1) $\Pr_0\left[\overline{\mathsf{D}}\right] = \Pr_1\left[\overline{\mathsf{D}}\right]$。

此外，令 p 为该概率的（共同）值，我们有

(2) $\frac{1}{2}\left(1-\frac{1}{e}\right)\cdot\left(\frac{\mu^2}{l^2}-\frac{\mu}{l}\right)\cdot\frac{1}{2^l}\le p\le\left(\frac{\mu^2}{l^2}-\frac{\mu}{l}\right)\cdot\frac{1}{2^l}$, 且

(3) $\mathbf{Adv}^{\text{lor}-\text{cpa}}_{\text{CBC}[R],A}(\cdot)=\left(\Pr_1\left[A=1\mid\overline{\mathsf{D}}\right]-\Pr_0\left[A=1\mid\overline{\mathsf{D}}\right]\right)\cdot p.$

我们首先在给定主CBC引理的情况下证明我们的结果，然后返回引理的证明。

引理16的证明：从引理18 (3) 我们有

$$\mathbf{Adv}^{\text{lor-cpa}}_{\text{CBC}[R],A}(\cdot)=\left(\Pr_1\left[A=1\mid\overline{\mathsf{D}}\right]-\Pr_0\left[A=1\mid\overline{\mathsf{D}}\right]\right)\cdot p\le p.$$

现在应用引理18 (2) 的上界。

定理17的证明：与定理11的证明类似。这里的增加是，一旦我们得到假设 F 为PRF族的安全性，我们必须使用命题8将其转化为假设 F 为PRP族的安全性。

引理18的证明：对于 $i\in[q]$ 和 $u\in\{0,\dots,n_i\}$ 令 $C_{i,u}=(C_j[k]:(j,k)\in T'$ 且 $(j,k)\preceq(i,u))$ 为直到并包括 $C_i[u]$ 的所有密文块序列。

令 $c_j[k]$ 为 l 比特字符串，$j\in[q]$ 且 $k\in\{0,\dots,n_j\}$。对于 $i\in[q]$ 和 $u\in\{0,\dots,n_i\}$ 令 $c_{i,u}=(c_j[k]:(j,k)\in T'$ 且 $(j,k)\preceq(i,u))$ 为直到并包括 $c_i[u]$ 的所有字符串的“下方”序列。

对于 $(i,u)\in T$，对于固定的密文块集合 c_{q,n_q}，我们定义集合 $\mathsf{Proh}_{i,u}(c_{q,n_q})$ 由以下所有 l 比特字符串组成：

(1) $c_j[k-1]\oplus M_j[k]\oplus M_i[u]$ 对于所有满足 $(j,k)\prec(i,u)$ 的 $(j,k)\in T$

(2) $c_j[k-1]\oplus M'_j[k]\oplus M'_i[u]$ 对于所有满足 $(j,k)\prec(i,u)$ 的 $(j,k)\in T$

也就是说，$\mathsf{Proh}_{i,u}(c_{q,n_q})$ 是 $C_i[u-1]$ 可能取的值的集合，这些值在给定我们对所有 $(j,k)\prec(i,u-1)$ 有 $C_j[k]=c_j[k]$ 的情况下会导致 $\overline{\mathrm{D}_{i,u}}$。

我们从 $\mathsf{Proh}_{i,u}(c_{q,n_q})$ 的定义观察到

$$(n_1+\cdots+n_{i-1}+u-1)\le\left|\mathrm{Proh}_{i,u}\left(c_{q,n_q}\right)\right|\le 2\cdot(n_1+\cdots+n_{i-1}+u-1).\quad(1)$$

我们注意到我们已经计算了 $\mathsf{Proh}_{i,u}(c_{q,n_q})$ 基数的界限。通常，集合的大小可能介于两者之间。

记住游戏之间的区别在于，在游戏0中我们有 $C_j[k]=C_j[k-1]\oplus M_j[k]$，在游戏1中我们有 $C_j[k]=C_j[k-1]\oplus M'_j[k]$，对于所有 $j\in[q]$ 和 $k\in[n_j]$。我们的第一个声称是，尽管如此，以 D 为条件的概率分布是相等的。

声称 1：令 c_{q,n_q} 为上述固定的密文块序列。那么

$$\Pr_0\left[C_{i,u-1}=c_{i,u-1}\mid\mathrm{D}_{i,u}\right]=\Pr_1\left[C_{i,u-1}=c_{i,u-1}\mid\mathrm{D}_{i,u}\right]\qquad(2)$$

对于所有 $i\in[q]$ 和 $u\in[n_i+1]$。

证明：通过归纳法。基本情况是 $(i,u)=(1,1)$。这里 $C_{1,0}=C_1[0]$ 是均匀分布的，因为它是随机选择的初始向量，所以声称成立。

现在假设 $(1,1) \prec (i,u)$。归纳假设是

$$\Pr_0[C_{j,k-1} = c_{j,k-1} \mid \mathsf{D}_{j,k}] = \Pr_1[C_{j,k-1} = c_{j,k-1} \mid \mathsf{D}_{j,k}]$$

对于所有满足 $j \in [q]$ 和 $k \in [n_j]$ 的 $(j,k) \prec (i,u)$。

令 $\Pr'_b[\cdot] = \Pr_b[\cdot|\mathsf{D}_{i,u}]$，$b = 0, 1$。我们考虑两种情况。

首先假设 $u \geq 2$，所以 $u \in \{2, \ldots, n_i + 1\}$。那么

$$\Pr'_b[C_{i,u-1} = c_{i,u-1}] = \Pr'_b[C_i[u-1] = c_i[u-1] \mid C_{i,u-2} = c_{i,u-2}] \cdot \Pr'_b[C_{i,u-2} = c_{i,u-2}]. \quad (3)$$

我们逐个分析右边的两项，并证明每一项都独立于 b。（论证在 $u \leq n_i$ 和 $u = n_i + 1$ 的情况下略有不同，但声称在两种情况下都成立。）从第二项开始。我们以 $\mathsf{D}_{i,u}$ 为条件。对于这一项，以 $\mathsf{D}_{i,u-1}$ 为条件没有区别，因为概率表达式中的量不涉及 $C_{i,u-1}$ 或 $c_{i,u-1}$。也就是说，

$$\Pr'_b[C_{i,u-2} = c_{i,u-2}] = \Pr_b[C_{i,u-2} = c_{i,u-2} \mid D_{i,u-1}].$$

现在根据归纳假设，这一项独立于 b。

对于方程(3)右边的第一项，观察

$$\Pr'_b[C_i[u-1] = c_i[u-1] \mid C_{i,u-2} = c_{i,u-2}] = \begin{cases} 0 & \text{如果} c_i[u-2] \in \mathrm{Proh}_{i,u-1}(c_{q,n_q}) \\ 2^{-l} & \text{否则。} \end{cases} \quad (4)$$

我们这样看方程(4)。第一种情况（概率为0）为真，因为我们以 $\mathsf{D}_{i,u}$ 为条件，这恰好禁止了所述事件。对于第二种情况，注意在游戏0中 $C_i[u-1] = f(C_i[u-2] \oplus M_i[u-1])$，在游戏1中 $C_i[u-1] = f(C_i[u-2] \oplus M'_i[u-1])$。然而，如果我们知道 $c_i[u-2]$ 不在禁止集合中，那么无论进行哪个游戏，$C_i[u-2] \oplus M_i[u-1]$ 和 $C_i[u-2] \oplus M'_i[u-1]$ 都是 f 之前未被调用过的点。因此所述概率如声称的那样，并且特别是独立于 b。因此我们已经完成了证明方程(3)中的量独立于 b。

现在我们必须处理 $u = 1$ 的情况，即证明

$$\Pr_0[C_{i,0} = c_{i,0} \mid \mathsf{D}_{i,1}] = \Pr_1[C_{i,0} = c_{i,0} \mid \mathsf{D}_{i,1}]. \quad (5)$$

我们可以假设 $i \geq 2$，因为情况 $(i,u) = (1,1)$ 在归纳法的基础情况中已经涵盖。我们有

$$\Pr'_b[C_{i,0} = c_{i,0}] = \Pr'_b[C_i[0] = c_i[0] \mid C_{i-1,n_{i-1}} = c_{i-1,n_{i-1}}] \cdot \Pr'_b[C_{i-1,n_{i-1}} = c_{i-1,n_{i-1}}]. \quad (6)$$

第一项是 2^{-l}，因为 $C_i[0]$ 是随机初始向量。对于第二项，我们可以以 $D_{i-1,n_{i-1}+1}$ 为条件而不是 $D_{i,1}$ 而不改变结果。然后我们可以应用归纳假设来看到该项独立于 b。

声称 2. $\Pr_0[A = 1 \mid \mathsf{D}] = \Pr_1[A = 1 \mid \mathsf{D}]$。

以下是引理18陈述中的第一个声称。

声称 3. $\Pr_0\left[\overline{\mathsf{D}}\right] = \Pr_1\left[\overline{\mathsf{D}}\right]$。

证明：我们将通过归纳证明对于每个 $(i,u) \in T$ 我们有

$$\Pr_1\left[\overline{\mathsf{D}_{i,u}}\right] = \Pr_2\left[\overline{\mathsf{D}_{i,u}}\right].$$

显然当 $(i,u)=(1,1)$ 时两个概率都是零，所以假设 $(1,1) \prec (i,u) \in T$。归纳假设 $\Pr_0\left[\overline{\mathsf{D}_{j,k}}\right] = \Pr_1\left[\overline{\mathsf{D}_{j,k}}\right]$ 对于所有 $(j,k) \prec (i,u)$ 成立。对于任何 $b=0,1$，

$$\Pr_b\left[\overline{\mathsf{D}_{i,u}}\right] = \Pr_b\left[\overline{\mathsf{D}_{i,u}} \mid \overline{\mathsf{D}_{i,u-1}}\right] \cdot \Pr_b\left[\overline{\mathsf{D}_{i,u-1}}\right] + \Pr_b\left[\overline{\mathsf{D}_{i,u}} \mid \mathsf{D}_{i,u-1}\right] \cdot \Pr_b[\mathsf{D}_{i,u-1}].$$

在和的第一个项中，第一项是 1，第二项根据归纳独立于 b。在和的第二项中，第二项根据归纳独立于 b。剩下的就是证明

$$\Pr_0\left[\overline{\mathsf{D}_{i,u}} \mid \mathsf{D}_{i,u-1}\right] = \Pr_1\left[\overline{\mathsf{D}_{i,u}} \mid \mathsf{D}_{i,u-1}\right]. \tag{7}$$

我们将方程(7)的证明分为两种情况。

首先假设 $u \geq 2$。写作

$$\Pr_b\left[\overline{\mathsf{D}_{i,u}} \mid \mathsf{D}_{i,u-1}\right] = \\ \sum_{c_{i,u-2}} \Pr_b\left[\overline{\mathsf{D}_{i,u}} \mid \mathsf{D}_{i,u-1} \wedge C_{i,u-2} = c_{i,u-2}\right] \cdot \Pr_b[C_{i,u-2} = c_{i,u-2} \mid \mathsf{D}_{i,u-1}].$$

我们声称和中的每一项都独立于 b。为此固定 c_{q,n_q} 并考虑项

$$\Pr_b\left[\overline{\mathsf{D}_{i,u}} \mid \mathsf{D}_{i,u-1} \wedge C_{i,u-2} = c_{i,u-2}\right] \cdot \Pr_b\left[C_{i,u-2} = c_{i,u-2} \mid \mathsf{D}_{i,u-1}\right]. \tag{8}$$

方程(8)的第二项根据声称1独立于 b。对于第一项，我们声称：

$$\Pr_b\left[\overline{\mathsf{D}_{i,u}} \mid \mathsf{D}_{i,u-1} \wedge C_{i,u-2} = c_{i,u-2}\right] = \frac{\left|\mathrm{Proh}_{i,u}\left(c_{q,n_q}\right)\right|}{2^l}. \tag{9}$$

要看到方程(9)，注意 $\overline{\mathsf{D}_{i,u}}$ 发生在 $C_i[u-1]$ 落在禁止集合中时。我们知道在游戏0中 $C_i[u-1] = f(C_i[u-2] \oplus M_i[u-1])$，在游戏1中 $C_i[u-1] = f(C_i[u-2] \oplus M'_i[u-1])$。给定 $\mathsf{D}_{i,u-1}$ 为真，在任一游戏中，f 之前都没有在 $C_i[u-2] \oplus M_i[u-1]$ 或 $C_i[u-2] \oplus M'_i[u-1]$ 上调用过，因此 $C_i[u-1]$ 是均匀分布的。因此它落在禁止集合中的概率如声称的那样。最后，注意 $\mathsf{Proh}_{i,u}(c_{q,n_q})$ 仅涉及 $c_{i,u-2}$ 中的密文。这意味着它的大小是固定的，特别是独立于游戏。因此我们已经完成了证明方程(8)中的量独立于 b。

剩下的就是证明 $u=1$ 情况的方程(7)。我们类似地进行，主要只是符号的变化。我们可以假设 $i \geq 2$，因为情况 $(i,u)=(1,1)$ 在归纳法的基础情况中已经涵盖。写作

$$\Pr_b\left[\overline{\mathsf{D}_{i,1}} \mid \mathsf{D}_{i,0}\right] = \\ \sum_{c_{i-1,n_{i-1}}} \Pr_b\left[\overline{\mathsf{D}_{i,1}} \mid \mathsf{D}_{i,0} \wedge C_{i-1,n_{i-1}} = c_{i-1,n_{i-1}}\right] \cdot \Pr_b[C_{i-1,n_{i-1}} = c_{i-1,n_{i-1}} \mid \mathsf{D}_{i,0}].$$

再次，逐项分析上述和。固定 c_{q,n_q}，从而固定和中的一项。在这一项中（它本身是两个项的乘积），首先考虑第二项。我们同样可以以 $D_{i-1,n_{i-1}+1}$ 为条件而不改变概率。然后，我们看到量 i 根据声称1独立于 b。对于第一项，类似于上面根据禁止集合进行论证。注意 $C_i[u-1]$ 是随机的（作为初始向量），而禁止集合及其大小仅取决于我们通过条件固定的量。因此这一项也独立于 b。这就完成了声称3的证明。

我们现在令 $p \stackrel{\text{def}}{=} \Pr_0\left[\overline{\mathsf{D}}\right] = \Pr_1\left[\overline{\mathsf{D}}\right]$。以下是引理18陈述中第二个声称的上界。

$$\text{声称 } 4. \quad p \leq \left(\frac{\mu^2}{l^2} - \frac{\mu}{l}\right) \cdot \frac{1}{2^l}.$$

证明：标准的条件概率和边界表明

$$\Pr_0\left[\overline{\mathsf{D}}\right] \le \sum_{i=1}^{q}\sum_{u=1}^{n_i}\Pr_0\left[\overline{\mathsf{D}_{i,u}} \mid \mathsf{D}_{i,u-1}\right].$$

当 $C_i[u-1]$ 落在 $\mathsf{Proh}_{i,u}(\cdot)$ 中时发生碰撞。现在我们可以应用方程(1)来上界上述和

$$\begin{aligned}&\textstyle\sum_{i=1}^{q}\sum_{u=1}^{n_i}\frac{2(n_1+\ldots+n_{i-1}+u-1)}{2^l} = \frac{2}{2^l}\sum_{i=1}^{q}\left(n_i(n_1+\ldots+n_{i-1})+\frac{(n_i-1)n_i}{2}\right)\\ =&\frac{1}{2^l}\left[\frac{\mu^2}{l^2}-\frac{\mu}{l}\right].\end{aligned}$$

这就完成了声称4的证明。 □

以下是引理18陈述中第二个声称的下界。

$$\text{声称 } 5: p \ge \frac{1}{2}\left(1-\frac{1}{e}\right)\cdot\frac{1}{2^l}\left(\frac{\mu^2}{l^2}-\frac{\mu}{l}\right).$$

证明：我们使用方程(1)上界互补事件：

$$\begin{aligned}&\mathrm{P\,r}_0[\mathsf{D}] = \textstyle\prod_{i=1}^{q}\prod_{u=1}^{n_i}\mathrm{P\,r}_0[\mathsf{D}_{i,u}\mid\mathsf{D}_{i,u-1}]\\ &\le \textstyle\prod_{i=1}^{q}\prod_{u=1}^{n_i}\frac{2^l-(n_1+\ldots+n_{i-1}+u-1)}{2^l}\\ &= \textstyle\prod_{i=1}^{q}\prod_{u=1}^{n_i}\left(1-\frac{n_1+\ldots+n_{i-1}+u-1}{2^l}\right).\end{aligned}$$

使用事实14的不等式 $1-x\le e^{-x}$，我们可以上界上述为 e^{-M}，其中

$$M = \sum_{i=1}^{q}\sum_{u=1}^{n_i}\frac{n_1+\ldots+n_{i-1}+u-1}{2^l} = \frac{1}{2}\frac{1}{2^l}\left[\frac{\mu^2}{l^2}-\frac{\mu}{l}\right].$$

但是 $p\ge 1-e^{-M}$。现在应用事实14的不等式 $1-e^{-M}\ge(1-e^{-1})M$ 得到

$$p \ge \frac{1}{2}\left(1-\frac{1}{e}\right)\cdot\frac{1}{2^l}\left[\frac{\mu^2}{l^2}-\frac{\mu}{l}\right].$$

这就完成了声称5的证明。 □

以下是引理18陈述中的第三个声称。

$$\text{声称 } 6: \mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{CBC}[R],A}(\cdot) = \left(\Pr_1\left[A=1\mid\overline{\mathsf{D}}\right]-\Pr_0\left[A=1\mid\overline{\mathsf{D}}\right]\right)\cdot p.$$

证明：通过条件概率，我们有

$$\begin{aligned}&\mathbf{Adv}^{\mathrm{lor-cpa}}_{\mathrm{CBC}[R],A}(\cdot) = \mathrm{Pr}_1[A=1]-\mathrm{Pr}_0[A=1]\\ &=\mathrm{Pr}_1\left[A=1\mid\overline{\mathrm{D}_{q,n_q}}\right]\mathrm{Pr}_1\left[\overline{\mathrm{D}_{q,n_q}}\right]+\mathrm{Pr}_1\left[A=1\mid\mathrm{D}_{q,n_q}\right]\mathrm{Pr}_1\left[\mathrm{D}_{q,n_q}\right]\\ &-\mathrm{Pr}_0\left[A=1\mid\overline{\mathrm{D}_{q,n_q}}\right]\mathrm{Pr}_0\left[\overline{\mathrm{D}_{q,n_q}}\right]-\mathrm{Pr}_0\left[A=1\mid\mathrm{D}_{q,n_q}\right]\mathrm{Pr}_0\left[\mathrm{D}_{q,n_q}\right].\end{aligned}$$

声称6的证明通过应用声称2和3完成。 □

这就完成了引理18的证明。

致谢

我们感谢 Ran Canetti，他对早期草稿提出了一些有益的意见，以及 Jim Gray，他建议了定义2的变体，该变体现在出现在这里。

参考文献

[1] W. ALEXI, B. CHOR, O. GOLDREICH, C. SCHNORR, "RSA and Rabin functions: Certain parts are as hard as the whole," SIAM Journal on Computing Vol. 17, No. 2, 1988, pp. 194-209.

[2] ANSI X3.106, “American National Standard for Information Systems – Data Encryption Algorithm – Modes of Operation,” American National Standards Institute, 1983.

[3] M. BELLARE, R. CANETTI AND H. KRAWczyk "Psuedorandom functions revisited: The cascade construction and its concrete security," Proceedings of the 37th Symposium on Foundations of Computer Science, IEEE, 1996.

[4] M. BELLARE, A. DESAI, D. POINTCHEVAL AND P. ROGAWAY, “Relations among notions of security for public-key encryption schemes,” Advances in Cryptology - Crypto '98, LNCS Vol. 1462, H. Krawczyk ed., Springer-Verlag, 1998.

[5] M. BELLARE, R. GUÉRIN AND P. ROGAWAY, “XOR MACs: New methods for message authentication using finite pseudorandom functions,” Advances in Cryptology - Crypto '95, LNCS Vol. 963, D. Coppersmith ed., Springer-Verlag, 1995.

[6] M. BELLARE, J. KILIAN AND P. ROGAWAY, "The security of the cipher block chaining message authentication code," Advances in Cryptology - Crypto '94, LNCS Vol. 839, Y. Desmedt ed., Springer-Verlag, 1994.

[7] M. BELLARE AND P. ROGAWAY, “Optimal asymmetric encryption – How to encrypt with RSA,” Advances in Cryptology - Eurocrypt '95, LNCS Vol. 921, L. Guillou and J. Quisquater ed., Springer-Verlag, 1995.

[8] M. BELLARE AND P. ROGAWAY, “The exact security of digital signatures: How to sign with RSA and Rabin,” Advances in Cryptology - Eurocrypt '96, LNCS Vol. 1070, U. Maurer ed., Springer-Verlag, 1996.

[9] M. BLUM AND S. GOLDWASSER, “An efficient probabilistic public-key encryption scheme which hides all partial information,” Advances in Cryptology - Crypto '84, LNCS Vol. 196, R. Blakely ed., Springer-Verlag, 1984.

[10] D. DOLEV, C. DWORK AND M. NAOR, “Non-malleable cryptography,” SIAM J. of Computing, to appear. Preliminary version in Proceedings of the 23rd Annual Symposium on the Theory of Computing, ACM, 1991.

[11] O. GOLDREICH “A uniform complexity treatment of encryption and zero-knowledge,” Journal of Cryptology, Vol. 6, 1993, pp. 21-53.

[12] O. GOLDREICH, R. IMPAGLIAZZO, L. LEVIN, R. VENKATESAN AND D. ZUCKERMAN, "Security preserving amplification of hardness," Proceedings of the 31st Symposium on Foundations of Computer Science, IEEE, 1990.

[13] O. GOLDREICH AND L. LEVIN, “A hard-core predicate for all one-way functions,” Proceedings of the 21st Annual Symposium on the Theory of Computing, ACM, 1989.

[14] O. GOLDREICH, S. GOLDWASSER AND S. MICALI, “How to construct random functions,” Journal of the ACM, Vol. 33, No. 4, 1986, pp. 210–217.

[15] S. GOLDWASSER AND S. MICALI, “Probabilistic encryption,” J. of Computer and System Sciences, Vol. 28, April 1984, pp. 270–299.

[16] A. HERZBERG AND M. LUBY, “Public randomness in cryptography,” Advances in Cryptology - Crypto '92, LNCS Vol. 740, E. Brickell ed., Springer-Verlag, 1992.

[17] J. HÅSTAD, R. IMPAGLIAZZO, L. LEVIN AND M. LUBY, “Construction of a pseudo-random generator from any one-way function,” ICSI Technical Report, No. 91-068, submitted to SICOMP.

[18] ISO 8372, "Information processing - Modes of operation for a 64-bit block cipher algorithm," International Organization for Standardization, Geneva, Switzerland, 1987.

[19] J. KATZ AND M. YUNG, “Complete characterization of security notions for probabilistic private-key encryption,” Proceedings of the 32nd Annual Symposium on the Theory of Computing, ACM, 2000.

[20] M. Luby, Pseudorandomness and Cryptographic Applications, Princeton University Press, 1996.

[21] M. Luby AND C. RACKOFF, "How to construct pseudorandom permutations from pseudorandom functions," SIAM J. Computation, Vol. 17, No. 2, April 1988.

[22] S. MICALI, C. RACKOFF AND R. SLOAN, “The notion of security for probabilistic cryptosystems,” SIAM J. of Computing, April 1988.

[23] National Bureau of Standards, NBS FIPS PUB 81, “DES modes of operation,” U.S Department of Commerce, 1980.

[24] M. NAOR AND M. YUNG, "Public-key cryptosystems provably secure against chosen ciphertext attacks," Proceedings of the 22nd Annual Symposium on the Theory of Computing, ACM, 1990.

[25] C. RACKOFF AND D. SIMON, “Non-interactive zero-knowledge proof of knowledge and chosenciphertext attack,” Advances in Cryptology - Crypto '91, LNCS Vol. 576, J. Feigenbaum ed., Springer-Verlag, 1991.

[26] A. C. YAO, “Theory and applications of trapdoor functions,” Proceedings of the 23rd Symposium on Foundations of Computer Science, IEEE, 1982.

专业术语英文中文对照表

英文术语	中文翻译
Symmetric Encryption	对称加密
Concrete Security	具体安全性
Pseudorandom Function (PRF)	伪随机函数
Pseudorandom Permutation (PRP)	伪随机置换
Chosen-Plaintext Attack (CPA)	选择明文攻击
Chosen-Ciphertext Attack (CCA)	选择密文攻击
Left-or-Right Indistinguishability (LOR)	左或右不可区分性

英文术语	中文翻译
Real-or-Random Indistinguishability (ROR)	实或随机不可区分性
Find-then-Guess Security (FTG)	找然后猜安全性
Semantic Security (SEM)	语义安全性
Block Cipher	分组密码
Cipher Block Chaining (CBC)	密码分组链接模式
Counter Mode (CTR)	计数器模式
XOR Scheme	XOR方案
Nonce	现时值
Initialization Vector (IV)	初始向量
Advantage Function	优势函数
Reduction	归约
Tight Reduction	紧密归约
Security-Preserving	保持安全性的
Adversary	敌手
Oracle	预言机
Distinguisher	区分器
Random Function	随机函数
Random Permutation	随机置换
Birthday Attack	生日攻击
Overlap	重叠/碰撞
Stateless	无状态的
Stateful	有状态的
Parallelizability	可并行性
Self-Synchronizing	自同步的
Key Generation	密钥生成
Encryption Algorithm	加密算法
Decryption Algorithm	解密算法
Polynomial-Time	多项式时间
Asymptotic Security	渐近安全性
Public-Key Encryption	公钥加密
Private-Key Encryption	私钥加密
Provable Security	可证明安全