# BC 加密模式的分析及其改进

郑凯燕 [1,2,3], 王 鹏 [1,2,3]

[1] 中国科学院信息工程研究所信息安全国家重点实验室, 北京 100093
[2] 中国科学院数据与通信保护研究教育中心, 北京 100093
[3] 中国科学院大学网络空间安全学院, 北京 100049

**摘要** 本文首次对国家标准 GB/T 17964-2008 中的 BC 加密模式进行了分析。在密文和随机串的不可区分 (ROI-IND)的定义下, 研究表明在常规的选择明文攻击下 BC 模式的机密性完全依赖于 IV 值的随机性; 而在逐分组攻击(blockwise attack)下 BC 模式是不安全。因此, 从具体应用角度来看, BC 模式的实用性受限, 例如其 IV 值不能作为 Nonce 使用, 不能应用于在线消息处理场景, 等等。针对这些问题, 本文对 BC 加密模式进行了改进, 提出了一种实用性更强的加密模式——基于 Nonce 的 XBC 模式, 并证明了其在并发的逐分组适应的选择明文攻击下的机密性。

**关键词** BC 加密模式; 逐分组攻击; 加密模式/工作模式; 不可区分性; Nonce; 选择明文攻击
**中图法分类号** TP309.7 DOI 号 10.19363/j.cnki.cn10-1380/tn.2017.07.004

# The concrete security of BC mode and its improvement

ZHENG Kaiyan [1,2,3], WANG Peng [1,2,3]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100093, China
[3] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

**Abstract** In this paper, we analyze the confidential security of the Block Chaining operation mode (BC mode) proposed in Chinese national standard GB/T 17964-2008. We define the *real-or-ideal* indistinguishability in the sense of distinguishing the ciphertext with random bits. Using this ROI-IND concept, we prove that: 1) the CPA-security of BC mode totally depends on the randomness of IV, suffering easily misuse in practical implementations; 2) BC mode can't resist the blockwise adptive attack, and fails to provide confidentiality in real on-line applications. To fix the defects of BC mode, we propose an improved encryption mode – nonce-respected XBC mode, which is proved to be confidential against the concurrent blockwise adaptive chosen plaintext attack. Compared to the original BC mode, this nonce-respected XBC mode is easier to correct use, even in on-line applications.

**Key words** block chaining operation mode; concurrent blockwise (adaptive) attack; encryption mode; indistinguishability; nonce; chosen plaintext attack

## 1 引言

分组密码工作模式(block cipher mode of operation)是通过调用分组密码(block cipher)处理消息, 以实现各种安全功能的密码方案, 如实现机密性的加密模式、实现完整性的认证模式、以及同时实现机密性和完整性的认证加密模式等[1]。

分组密码工作模式应用广泛, 各国及各国际标准化组织陆续发布了相应的标准文档, 包括 NIST, ISO, IEEE, IETF 等组织。以加密模式为例, 早在 DES 算法时期, NIST(National Institute of Standard Technology, 美国国家技术标准局)就提出了 4 个经典的加密模式, 分别为 ECB(Electronic Codebook, 电码本模式)、CBC(Cipher Block Chaining, 密码分组链接模式)、CFB(Cipher Feedback, 密码反馈模式)、OFB(Output Feedback, 输出反馈模式)。随后, NIST 在 2001 年发布的标准文档 SP-800-38A 中增加了 CTR(Counter, 计算器模式), 在之后的 SP-800-38F 文档中加入了磁盘扇区加密模式 XTS-AES。基本上, ISO、IEEE、IETF 等组织发布的关于加密模式的标

**通讯作者:** 王鹏, 博士, 副研究员, Email: wp@is.ac.cn。
本课题得到国家自然科学基金(Nos. 61272477, 61472415)、国家重点基础研究发展(973)计划(No.2014CB340603)和中国科学院战略性先导科技专项(No.XDA06010702)资助。
收稿日期: 2016-04-28; 修改日期: 2016-08-07; 定稿日期: 2017-03-24

准文档都包括了这些经典的加密模式。我国也于 2008 年发布了名为《信息安全技术分组密码的工作模式》的国家标准 GB/T 17964-2008[2], 该标准文档共发布了 7 种加密模式, 包括上述 5 个经典加密模式(ECB、CBC、CFB、OFB、CTR)和 2 个额外增加的加密模式, 即 BC 模式和 OFBNLF 模式。

目前有大量研究这些分组密码工作模式的文献。例如, CBC、OFB、CFB、CTR 等经典加密模式都有相应的安全性归约证明。在选择明文攻击(Chosen Plaintext Attack, 以下简称 CPA)下, 文献[3]对 CBC 模式、CTR 模式的 CPA 机密性进行了证明, 文献[4,5]对 CFB 模式、OFB 模式的机密性进行了讨论。归约证明将上层工作模式的安全强度归约到底层密码模块(cryptographic primitives)的安全性上。以 CBC 模式为例, 文献[3]中证明了如果底层的分组密码是一个伪随机置换(PRP-CPA), 那么基于随机 IV 值的 CBC 模式是安全的。但是我们发现, BC 模式是一个全新的加密模式, 目前还没有任何文献对其进行研究。因此, 国家标准 GB/T 17964-2008 的使用者会有诸多的疑惑: BC 模式适用于什么场合? BC 模式的安全性如何?为确保 BC 模式的安全实现应该注意哪些问题?

本文将对上述问题给以解答。我们系统分析 BC 加密模式的特点和其采用不同实现方式和使用于不同应用场景下的安全性, 同时针对其出现的安全隐患, 给出了 BC 加密模式的一个改进方案。对于 BC 加密模式的安全分析, 我们从初始向量(IV)的不同使用方式入手, 分别讨论其在常规模型和逐分组攻击模型下的安全性。

### 1.1 IV 的使用方式及安全性

为了实现概率算法[6], 许多密码方案往往定义了一个重要参数——初始向量(Initialization Vector, 以下简称 IV 值), 该 IV 值的使用方式对整个密码方案的安全性至关重要。如文献[3]中 CBC 模式、CTR 模式的机密性证明是基于随机 IV 值的假设, 即每次加密时 IV 值是随机生成的。

然而, 从具体实现的角度分析, 基于随机 IV 值的密码方案容易出现误用。比如, 在 SSL/TLS 协议中, 基于随机 IV 值的 CBC 模式因被误用而使其 CPA 机密性受到严重损害。当前 Web 浏览器与服务器之间的身份认证和加密数据传输中广泛使用的安全协议是 SSL v3 和 TLS v1.0, 这两个协议版本均将 CBC 模式的 IV 值定义为前一次加密时所得的最后一个密文分组。这使得该 IV 值可被敌手预测, 进而被扩展成一个对 CBC 模式实际的恢复明文攻击[7], Paterson 将其称为“BEAST 攻击”[8]。随后 TLS v1.1 和 v1.2 对该定义进行修改了, 明确要求在每次加密时 IV 值必须随机生成。在 TCP/IP 网络的各安全协议中, 因 IV 值的误用而损害 CBC 模式的 CPA 机密性, 进而攻击整个安全协议的案例多不胜数[7-12]。

另外, 生成随机 IV 值的难度较大, 包括获得随机种子的代价大、随机值的实现方法难以保证, 等等。在文献[13]中, Rogaway 指出在 NIST、ISO、IEEE 等组织发布的各标准文档中, 一些关于随机 IV 值生成方式的建议是不正确的, 其中包括 ISO/IEC 10116:2006[14]、SP-800-38A[15]。

针对随机 IV 值容易出现误用这一问题, Rogaway[16]提出了基于 Nonce 的密码方案设计, 其 IV 值作为 Nonce 使用, 并且敌手能力更强, 可以选择不重复的 IV 值。我们也称这种方案为基于 Nonce 的方案。在文献[16]中, Rogaway 分析得基于 Nonce 的 CBC 模式在 CPA 下不安全, 而基于 Nonce 的 CTR 模式的 CPA 机密性则不受影响。针对基于 Nonce 的 CBC 模式不安全这一问题, Rogaway 将 CBC 模式改进为 CBC2 模式, 并证明了基于 Nonce 的 CBC2 模式在 CPA 下的安全性, 但是 CBC2 模式的密钥长度是原来的两倍, 这给 CBC2 模式的使用带来不便。

### 1.2 常规攻击模型与逐分组攻击模型

在常规的选择明文攻击模型(以下简称 CPA)下, 密码方案所处理的消息都是作为一个整体(atomic entities)一次性提交的, 但在一些实际在线应用中, 消息的提交和处理是逐分组(blockwise)进行的。比如在实时应用中, 由于实时事件的随机性和系统工作状态的不确定性, 处理消息无法整体一次性提交。又如, 一些资源受限的密码设备, 如智能卡, 在处理长消息时, 因设备自身的存储空间有限, 需将长消息分段处理。

需要注意的是, 这类在线处理消息的应用场景导致了一类新的攻击方式——逐分组攻击(blockwise adaptive attack)。与常规攻击模型相比, 逐分组攻击模型下的敌手可以在一次询问过程中控制消息以逐分组方式输入并获得应答。以逐分组适应的选择明文攻击(BlockWise adaptive Chosen-Plaintext Attack, 以下简称 BW-CPA)为例, 敌手在进行加密询问时可以逐分组提交消息, 这一能力是常规攻击模型下敌手没有的。因此, 有些具有 CPA 安全的密码方案在 BW-CPA 下依然是安全的, 如基于随机 IV 值的 CFB 模式和 CTR 模式[17-18], 而有些则不然, 如 CBC、GEM 和 IACBC[19-20]。

针对一些基于分组密码的工作模式在 BW-CPA

下不安全这一问题, Fouque 等人在文献[17]提出了将密文输出延迟(delayed)一个分组的通用方法, 并将其应用到 CBC 模式中, 得到了具有 BW-CPA 机密性的 DCBC(Delayed CBC)模式。但这种延迟密文分组输出的方法存在延长系统响应时间等效率问题。

逐分组攻击模型和密码方案的在线实现方式密切关联, 从具体实现的角度分析, 若密码方案无法抵抗逐分组攻击, 则其不能被应用于实时系统、资源受限设备等消息在线处理的应用场景。

针对上述两种应用场景, 我们对 BC 加密模式的安全性进行系统研究, 分别分析了该加密模式在 CPA、BW-CPA 下的机密性, 包括基于随机 IV 值和基于 Nonce 两种假设, 并针对其安全缺陷进行改进, 提出了基于 Nonce 的 XBC 模式。本文的主要内容如下:

1) 总结了 BC 模式的模式特点, 包括运行效率、差错扩散、自同步、并行处理、预计算等, 并将其与标准文档 GB/T 17964-2008[2]中的另外 6 个加密模式进行了比较。从表 3 可知, BC 模式的运行效率较优, 其平均每处理一个明文分组需要调用分组密码一次, 但该模式存在差错扩散的现象, 且不能实现自同步、并行处理、预计算, 其解密过程需要调用分组密码的解密过程。

2) 分析了 BC 模式的 CPA 机密性。本文从区分密文和等长随机比特串的角度定义了 ROI-IND(现实情况和理想情况的不可区分性), 并在该定义下分析 BC 模式的机密性。由表 6 可知, BC 模式的 CPA 机密性完全依赖于 IV 值的随机性, 基于不重复 Nonce 的 BC 模式在 CPA 下不安全。与各经典加密模式类似的, 基于随机 IV 值的 BC 模式误用性较高。

3) 分析了 BC 模式的 BW-CPA 机密性, 在 ROI-IND 定义下, BC 模式在 BW-CPA 下存在高效的区分攻击。由表 6 可知, BC 模式以在线方式实现是不安全的, 其实用性受限。

4) 改进了 BC 模式, 提出了一个实用性较高的加密模式——基于 Nonce 的 XBC 模式。本文将 ROI-IND 的定义扩展到并发的逐分组适应的选择明文攻击(Concurrent BlockWise adaptive Chosen Plaintext Attack, 以下简称 CBW-CPA)下, 得到 ROI-IND-CBW-CPA 的安全定义, 并在该定义下证明了基于 Nonce 的 XBC 模式的机密性。

本文的具体内容安排为: 第 2 节介绍文中涉及的预备知识和符号记法; 第 3 节回顾 BC 模式的具体描述, 并总结其模式特点; 第 4 节分别分析 BC 模式的 CPA 机密性和 BW-CPA 机密性; 第 5 节提出基于 Nonce 的 XBC 模式, 并证明其 CBW-CPA 机密性; 第 6 节总结全文。

## 2 预备知识

本节将简要介绍本文采用的一些符号记法, 同时回顾一些文中涉及的理论知识, 包括安全定义、安全模型和 PRP-PRF 切换引理等。

### 2.1 基本符号

用 $\{0,1\}^*$ 和 $\{0,1\}^n$ 分别表示任意长度和 $n$ 比特的比特串的集合, 用 $\varepsilon$ 表示空串, 用 $(\{0,1\}^n)^+$ 表示所有长度为 $n$ 的正整数倍的比特串的集合, $(\{0,1\}^n)^*$ 表示 $(\{0,1\}^n)^+$ 和空串 $\varepsilon$ 的并集。$s \xleftarrow{\$} S$ 表示从集合 $S$ 中随机选取一个元素赋值给变量 $s$。

$Perm(n)$ 表示所有 $\{0,1\}^n$ 映射到 $\{0,1\}^n$ 的置换集合, 若 $\pi \xleftarrow{\$} Perm(n)$, 则称 $\pi$ 是随机置换。用 $Func(n_1,n_2)$ 表示所有 $\{0,1\}^{n_1}$ 映射到 $\{0,1\}^{n_2}$ 的函数集合, 用 $Func(n)$ 表示 $Func(n,n)$, 若 $\rho \xleftarrow{\$} Func(n_1,n_2)$, 则称 $\rho$ 是随机函数。

### 2.2 分组密码

$E:\{0,1\}^k\times\{0,1\}^n \to \{0,1\}^n$ 是一个分组大小为 $n$ 比特的分组密码(block cipher), 其中, 密钥空间为 $\{0,1\}^k$, 明文空间和密文空间均为 $\{0,1\}^n$。假设密钥 $K \xleftarrow{\$} \{0,1\}^k$, 则加密算法 $E_K(\cdot)\in Perm(n)$, 解密算法 $D_K(\cdot)\in Perm(n)$, 且其满足:

$\forall M\in\{0,1\}^n, D_K(E_K(M))=M$。

### 2.3 可忽略函数

若函数 $\epsilon$: N→R 满足 $\forall c, \exists n_0, \forall n>n_0, \epsilon(n)\leqslant n^{-c}$, 则称函数 $\epsilon(\cdot)$ 为可忽略函数(negligible function)[21]。从直观上看, 可忽略函数小于任意一固定的多项式函数的倒数, 常见的例子有 $2^{-n}$, $n^{-\log\log n}$, 等等。

### 2.4 区分优势

密码学中常用区分优势表示敌手区分两个对象的概率, 这里将给出其一般性的定义。

假设有两个概率算法 $\mathcal{O}_1$、$\mathcal{O}_2$, 敌手 $\mathcal{A}$ 能够询问某 oracle(可译为谕言) $\mathcal{O}\in\{\mathcal{O}_1,\mathcal{O}_2\}$, 假设其询问次数最多不超过 $q$ 次, 总运行时间为 $t$, 则该敌手 $\mathcal{A}$ 对 $\mathcal{O}_1$、$\mathcal{O}_2$ 的区分概率 $\boldsymbol{Dist}_{\mathcal{O}_1}^{\mathcal{O}_2}(\mathcal{A}(q,t))$ 定义为

$$\boldsymbol{Dist}_{\mathcal{O}_1}^{\mathcal{O}_2}(\mathcal{A}(q,t)) = \left|\Pr\left[\mathcal{A}^{\mathcal{O}_1}=1\right]-\Pr\left[\mathcal{A}^{\mathcal{O}_2}=1\right]\right|,$$

其中, $\Pr\left[\mathcal{A}^{\mathcal{O}}=1\right]$表示敌手 $\mathcal{A}$ 在与概率算法 $\mathcal{O}$ 交互的情况下输出 1 的概率。

由上定义可知, $\boldsymbol{Dist}_{\mathcal{O}_1}^{\mathcal{O}_2}(\mathcal{A}(q,t))$ 的值越大(接近 1), 表明 $\mathcal{O}_1$、$\mathcal{O}_2$ 两者间的差异越明显; 反之, $\boldsymbol{Dist}_{\mathcal{O}_1}^{\mathcal{O}_2}(\mathcal{A}(q,t))$ 的值越小(为可忽略函数), 表明 $\mathcal{O}_1$、$\mathcal{O}_2$ 两者间的差异越小。

进一步定义区分优势 $\boldsymbol{Adv}_{\mathcal{O}_1}^{\mathcal{O}_2}(q,t)$ 如下:

$$\boldsymbol{Adv}_{\mathcal{O}_1}^{\mathcal{O}_2}(q,t) = \max_{\mathcal{A}}\left\{\boldsymbol{Dist}_{\mathcal{O}_1}^{\mathcal{O}_2}(\mathcal{A}(q,t))\right\}$$

当 $\boldsymbol{Adv}_{\mathcal{O}_1}^{\mathcal{O}_2}(q,t)$ 是可忽略函数时, 我们称运行时间不超过 $t$ 的任意敌手 $\mathcal{A}$, 当其最多进行 $q$ 次询问时, $\mathcal{O}_1$、$\mathcal{O}_2$ 是不可区分(indistinguishable)的。

## 2.5 PRP (伪随机置换)和 PRF (伪随机函数)

假设 $E:\{0,1\}^k\times\{0,1\}^n\to\{0,1\}^n$ 是一个分组密码, $K\xleftarrow{\$}\{0,1\}^k$, $E_K(\cdot)$、$D_K(\cdot)$ 分别表示其加解密算法。假设 $\pi$ 是随机置换, 即 $\pi\xleftarrow{\$}Perm(n)$。

假设 CPA 敌手 $\mathcal{A}$, 能够询问加密 oracle $\mathcal{O}(\cdot)\in\{E_K(\cdot),\pi(\cdot)\}$, 若其询问次数最多 $q$ 次, 总运行时间为 $t$, 则敌手 $\mathcal{A}$ 对 $E$、$\pi$ 二者的区分概率定义如下:

$$\boldsymbol{Dist}_E^{\pi}(\mathcal{A}(q,t)) \tag{1}$$
$$=\left|\Pr\left[K\xleftarrow{\$}\{0,1\}^k:\mathcal{A}^{E_K(\cdot)}=1\right]-\Pr\left[\mathcal{A}^{\pi(\cdot)}=1\right]\right|$$

对任意 CPA 敌手 $\mathcal{A}$, $\boldsymbol{Adv}_E^{prq-cpa}(q,t)$ 定义如下:

$$\boldsymbol{Adv}_E^{prq-cpa}(q,t) = \max_{\mathcal{A}}\left\{\boldsymbol{Dist}_E^{\pi}(\mathcal{A}(q,t))\right\} \tag{2}$$

若 $\boldsymbol{Adv}_E^{prq-cpa}(q,t)$ 是可忽略函数, 则称 $E$ 是一个在选择明文攻击下的伪随机置换(PseudoRandom Permutation in the Chosen Plaintext Attack, PRP-CPA)[3,22]。即对任意询问加密 oracle 次数不超过 $q$ 次的 CPA 敌手, 分组密码 $E$ 和一个随机置换是不可区分的。

将上述 PRP-CPA 的定义中的随机置换 $\pi\xleftarrow{\$}Perm(n)$ 替换为随机函数 $\rho\xleftarrow{\$}Func(n)$。可得到在选择明文攻击下的伪随机函数(PseudoRandom Function in the Chosen Plaintext Attack, PRF-CPA)定义, 具体定义如下:

假设 CPA 敌手 $\mathcal{A}$, 能够询问加密 oracle $\mathcal{O}(\cdot)\in\{E_K(\cdot),\rho(\cdot)\}$, 若其询问次数最多 $q$ 次, 总运行时间为 $t$, 则敌手 $\mathcal{A}$ 对 $E$、$\rho$ 二者的区分概率定义如下:

$$\boldsymbol{Dist}_E^{\rho}(\mathcal{A}(q,t)) \tag{3}$$
$$=\left|\Pr\left[K\xleftarrow{\$}\{0,1\}^k:\mathcal{A}^{E_K(\cdot)}=1\right]-\Pr\left[\mathcal{A}^{\rho(\cdot)}=1\right]\right|$$

对任意 CPA 敌手 $\mathcal{A}$, $\boldsymbol{Adv}_E^{prf-cpa}(q,t)$ 定义如下:

$$\boldsymbol{Adv}_E^{prf-cpa}(q,t) = \max_{\mathcal{A}}\left\{\boldsymbol{Dist}_E^{\rho}(\mathcal{A}(q,t))\right\} \tag{4}$$

若 $\boldsymbol{Adv}_E^{prf-cpa}(q,t)$ 是可忽略函数, 则称 $E$ 是 PRF-CPA。

类似地, 可以定义选择密文攻击下的 PRP-CCA、PRF-CCA[3,22]。

## 2.6 PRP/PRF 切换引理[4-5]

在选择明文攻击下, 随机置换和随机函数之间存在着一个生日界的统计距离, 具体内容见下文 PRP/PRF 切换引理(PRP/PRF Switching Lemma)。

**PRP/PRF 切换引理.** 假设随机置换 $\pi\xleftarrow{\$}Perm(n)$, 随机函数 $\rho\xleftarrow{\$}Func(n)$, 对任意 CPA 敌手 $\mathcal{A}$ 询问加密 oracle $\mathcal{O}(\cdot)\in\{\pi(\cdot),\rho(\cdot)\}$ 次数最多 $q$ 次, 总运行时间为 $t$, 则有:

$$\boldsymbol{Adv}_{\pi}^{\rho}(q,t) \leqslant q^2/2^{n+1} \tag{5}$$

## 2.7 现实情况和理想情况的不可区分性定义

假设对称密码方案 $\mathcal{SE}:\mathcal{K}\times\mathcal{M}\to\mathcal{C}$, 其中 $\mathcal{K}$、$\mathcal{M}$ 和 $\mathcal{C}$ 分别是密钥空间、明文空间和密文空间, 则现实情况的加密 oracle 定义为 $\mathcal{SE}_K(\cdot), K\xleftarrow{\$}\mathcal{K}$, 其计算过程为 $\forall M\in\mathcal{M}, C=\mathcal{SE}_K(\cdot)$; 理想情况的加密 oracle 定义为 $Ran\Pi(\cdot)$, 其计算过程定义为 $\forall M\in\mathcal{M}, C\xleftarrow{\$}\{0,1\}^{|M|}$。显然的, $Ran\Pi(\cdot)$ 定义了一个与现实情况的密文等长的随机串生成函数。

现任意 CPA 敌手 $\mathcal{A}$, 若其询问加密 oracle 次数最多 $q$ 次, 总运行时间为 $t$, 则敌手 $\mathcal{A}$ 对现实情况和理想情况的区分概率 $\boldsymbol{Dist}_{\mathcal{SE}}^{Ran\Pi}(\mathcal{A}(q,t))$ 定义如下:

$$\boldsymbol{Dist}_{\mathcal{SE}}^{Ran\Pi}(\mathcal{A}(q,t)) \tag{6}$$
$$=\left|\Pr\left[K\xleftarrow{\$}\mathcal{K}:\mathcal{A}^{\mathcal{SE}_K(\cdot)}=1\right]-\Pr\left[\mathcal{A}^{Ran\Pi(\cdot)}=1\right]\right|$$

对任意 CPA 敌手 $\mathcal{A}$, $\boldsymbol{Adv}_{\mathcal{SE}}^{roi-ind-cpa}(q,t)$ 定义如下:

$$\boldsymbol{Adv}_{\mathcal{SE}}^{roi-ind-cpa}(q,t) = \max_{\mathcal{A}}\left\{\boldsymbol{Dist}_{\mathcal{SE}}^{Ran\Pi}(\mathcal{A}(q,t))\right\} \tag{7}$$

当 $\boldsymbol{Adv}_{\mathcal{SE}}^{roi-ind-cpa}(q,t)$ 是可忽略函数时, 我们称对称密码方案 $\mathcal{SE}$ 在 CPA 下满足现实情况和理想情况

的不可区分性(Real-Or-Ideal Indistinguishability against Chosen Plaintext Attack, ROI-IND-CPA)。从直观上理解, 若 $\boldsymbol{Adv}_{\mathcal{SE}}^{roi-ind-cpa}(q,t)$ 是可忽略函数, 则当密码方案 $\mathcal{SE}$ 的加密次数不超过 $q$ 次时, 其生成的密文可以近似看作随机比特串。

因本文不涉及 CCA 安全, 故上述定义只考虑 CPA 模型。

## 3 BC 模式的介绍

分组链接模式(Block Chaining operation mode), 简称 BC 模式, 是国家标准文档 GB/T 17964-2008[2] 提出的一种分组密码工作模式。本节先介绍 BC 模式的具体描述, 随后归纳其模式特点。

### 3.1 BC 模式的描述

为了便于描述 BC 模式, 引入下列变量:

1) 分组密码 $E:\{0,1\}^k\times\{0,1\}^n\to\{0,1\}^n$, $E_K(\cdot)$、$D_K(\cdot)$ 分别表示加解密, $K\xleftarrow{\$}\{0,1\}^k$。

2) 初始向量值 $IV\in\{0,1\}^n$;

3) 明文消息 $M=M_1M_2\cdots M_l$, 其中 $|M_i|=n$, 即将明文消息按 $n$ 比特进行划分, 共划分成 $l$ 个明文分组。对于任意长度的消息, 一般都要进行消息填充。这里我们为了便于论证, 假设明文消息长度刚好是 $n$ 比特的整数倍;

4) 类似地, 将密文消息表示为 $C=C_1C_2\cdots C_l$。

采用上述各变量, 将 BC 模式记为 $\mathcal{BC}:\{0,1\}^k\times\{0,1\}^n\times\left(\{0,1\}^n\right)^+\to\{0,1\}^n\times\left(\{0,1\}^n\right)^+$, 其中 BC 模式的密钥空间为 $\{0,1\}^k$, 假设 $K\xleftarrow{\$}\{0,1\}^k$, 则 BC 模式的加解密分别如图 1、图 2 所示, 具体描述如表 1、表 2 所示。

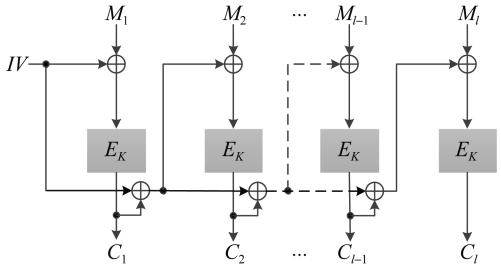



**图 1 BC 模式的加密过程**

**表 1 BC 模式的加密过程**

$\Sigma=IV$;
for $i=1$ to $l$
  $C_i\leftarrow E_K(M_i\oplus\Sigma)$;
  $\Sigma\leftarrow\Sigma\oplus C_i$;

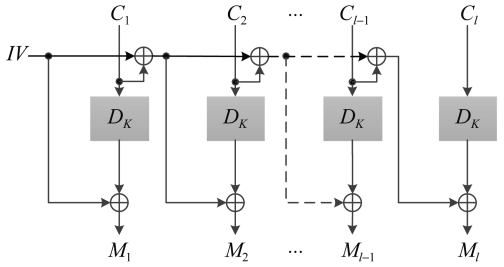



**图 2 BC 模式的解密过程**

**表 2 BC 模式解密过程的描述**

$\Sigma=IV$;
for $i=1$ to $l$
  $M_i\leftarrow D_K(C_i\oplus\Sigma)$;
  $\Sigma\leftarrow\Sigma\oplus C_i$;

### 3.2 BC 模式的特点

BC 模式的设计与传统的加密模式(如 ECB、CBC、CFB、OFB、CTR)类似, 表 2 给出了 BC 模式和各经典的加密模式的特点比较, 该表中所列出的模式特点包括:

运行效率, 即每处理一个消息分组(即 $n$ 比特)需要调用分组密码的平均次数;

差错扩散(error-propagation), 指一个密文分组中发生的比特错误将同时导致其他若干密文分组无法正确解密;

自同步(self-synchronous), 指若解密过程出现不同步问题, 如比特丢失导致分组边界不同步、密文分组丢失等, 加密模式能自动调整;

并行计算(parallelizable), 指并发地处理若干个明文分组, 这里限于分析其加密过程;

预处理(preprocessing), 指加密模式的加解密过程中有些复杂操作可预先进行计算, 并将所得结果存储起来;

不含逆(inverse-free), 指加密模式在加解密过程中均不需要调用分组密码的解密算法。

## 4 BC 模式的安全分析

BC 模式是标准文档 GB/T 17964-2008[2]提出一个基于分组密码的加密模式, 目前还没有任何文献对其进行安全分析。接下来, 本节将分别从常规 CPA、BW-CPA 分析 BC 模式的机密性。

与各经典加密模式类似的, 初始向量 IV 的选取方式对 BC 模式的机密性至关重要。但标准文档 GB/T 17964-2008[2]中没有对 IV 值的使用方式进行说明, 仅将其解释为“在密码变换中, 为增加安全

**表 3　7 种加密模式的特点对比**

| 模式特点 | BC | OFBNLF | ECB | CBC | OFB | CFB | CTR |
|---|---|---|---|---|---|---|---|
| 运行效率 | 1 | 2 | 1 | 1 | 1 | ⩾1 | 1 |
| 差错扩散 | ✓ | ✓ | × | ✓ | × | ✓ | × |
| 自同步 | × | × | × | × | × | ✓ | × |
| 并行计算 | × | ✓ | ✓ | × | × | × | ✓ |
| 预处理 | × | ✓ | × | × | ✓ | × | ✓ |
| 不含逆 | × | × | × | × | ✓ | ✓ | ✓ |

(注: ✓表示满足; ×表示不满足)

该表中所比较的加密模式是标准文档 GB/T 17964-2008[2]所建议的 7 种分组密码工作模式, 其中关于各加密模式特点的详细说明可参考该标准的附录 A、文献[13]的第一部分。

性或使密码设备同步而引入的用于数据变换的起始数据”。

为了分析 BC 模式的安全性, 我们将 IV 值的选取方式分成随机值和不重复的 Nonce 值两类进行讨论。表 4 和表 5 分别给出了在两种不同的 IV 值选取方式下 BC 模式的加密 oracle 的表述, 其中, 基于随机 IV 值的 BC 模式的加密 oracle 为 $\$BC[E]_K(M)$, $M$ 是敌手选择的明文消息, 这里 IV 值是 BC 模式随机生成的, 敌手无法控制; 而基于 Nonce 的 BC 模式的加密 oracle 记为 $\#BC[E]_K(N,M)$, $N,M$ 分别是敌手选择的Nonce值和明文消息, 这里Nonce值要求每次加密时都不重复, 即敌手在选择 Nonce 值时不是任意的, 其必须选择不重复的 $N$ 值。

**表 4　基于随机 IV 的 BC 模式的加密 oracle**

$\$BC[E]_k(M)$

$M=M_1M_2\cdots M_l$;

$\mathrm{IV}\xleftarrow{\$}\{0,1\}^n$; $C_0\leftarrow\mathrm{IV}$;

$\Sigma\leftarrow 0^n$;

**for** $i=1$ **to** $l$

　　$\Sigma\leftarrow\Sigma\oplus C_{i-1}$;

　　$C_i\leftarrow E_K(M_i\oplus\Sigma)$;

**return** $C_0C_1C_2\cdots C_l$

经分析, BC 模式在不同 IV 值假设下的机密性如表 6 所示: 在 CPA 模型下, 基于随机 IV 值的 BC 模式是安全的, 而基于 Nonce 值的 BC 模式则不安全; 在 BW-CPA 模型下, 不论 IV 值的假设如何, BC 模式均是不安全的。因此, 尽管 BC 模式的链式结构具有在线特性, 但其以在线方式实现是不安全的, 不适用于在线消息的应用场景。

接下来, 本节将对 BC 模式的机密性进行详细分析, 对其安全的情况给予证明, 对其不安全的情况则给出具体的攻击方法。

**表 5　基于 Nonce 的 BC 模式的加密 oracle**

$\#BC[E]_k(N,M)$

$M=M_1M_2\cdots M_l$;

$C_0\leftarrow N$;

$\Sigma\leftarrow 0^n$;

**for** $i=1$ **to** $l$

　　$\Sigma\leftarrow\Sigma\oplus C_{i-1}$;

　　$C_i\leftarrow E_K(M_i\oplus\Sigma)$;

**return** $C_1C_2\cdots C_l$

**表 6　BC 模式的机密性**

| | CPA | BW-CPA |
|---|---|---|
| 基于随机 IV 的 BC 模式 | ✓ | × |
| 基于 Nonce 的 BC 模式 | × | × |

## 4.1　常规 CPA 模型下 BC 模式的安全性

本小节我们将采用 ROI-IND 定义来分析 BC 模式在常规 CPA 模型下的机密性。在常规 CPA 下, 基于随机 IV 值的 BC 模式的机密性如下文定理 1 所示, 我们将采用做游戏的证明方法对定理 1 进行证明; 而基于 Nonce 的 BC 模式是不安全的, 下文攻击 1 给出了一个简单高效的区分攻击。

根据ROI-IND定义, 易知现实情况的加密oracle为 BC 模式的加密 oracle, 分别如表 4 和表 5 所示。而基于随机IV值的BC模式(即 $\$BC[E]_K(\cdot)$ 所对应的理想情况的加密 oracle 为 $\Pi(\cdot)$, 具体定义如表 7 所示。$\Pi(\cdot)$ 为随机比特串生成函数, 其与 $\$BC[E]_K(\cdot)$ 的区分优势如下文定理 1 所示。

**表 7　CPA 下基于随机 IV 值的理想情况**

$\Pi(M)$

$C\xleftarrow{\$}\{0,1\}^n\times\{0,1\}^{|M|}$;

**return** $C$

对常规 CPA 敌手 $\mathcal{A}$, 假设其询问加密 oracle $\mathcal{O}(\cdot)\in\{\$BC[E]_K(\cdot),\Pi(\cdot)\}$ 的次数不超过 $q$ 次,

总运行时间为 $t$，则敌手 $\mathcal{A}$ 对现实情况和理想情况的区分概率定义如下

$$\boldsymbol{Dist}^{\Pi}_{\$BC[E]}(\mathcal{A}(q,t)) \tag{8}$$
$$=\left|\Pr\left[K\xleftarrow{\$}\mathcal{K}:\mathcal{A}^{\$BC[E]_K(\cdot)}=1\right]-\Pr\left[\mathcal{A}^{\Pi(\cdot)}=1\right]\right|$$

对任意CPA敌手$\mathcal{A}$，$\boldsymbol{Adv}^{roi-ind-cpa}_{\$BC[E]}(q,t)$ 定义如下:

$$\boldsymbol{Adv}^{roi-ind-cpa}_{\$BC[E]}(q,t) \tag{9}$$
$$=\max_{\mathcal{A}}\left\{\boldsymbol{Dist}^{\Pi}_{\$BC[E]}(\mathcal{A}(q,t))\right\}$$

下面定理 1 给出了 $\boldsymbol{Adv}^{roi-ind-cpa}_{\$BC[E]}(q,t)$ 的上界，由其结论可知，$\boldsymbol{Adv}^{roi-ind-cpa}_{\$BC[E]}(q,t)$ 的上界主要由底层分组密码 $E$ 的伪随机性决定，而分组密码 $E$ 假设为一个 PRP-CPA，故 $\boldsymbol{Adv}^{roi-ind-cpa}_{\$BC[E]}(q,t)$ 是可忽略函数。也就是说，当 $\sigma\leqslant 2^{n/2}$ 时，任意 CPA 敌手无法区分 $\$BC[E]_K(\cdot)$ 和 $\Pi(\cdot)$，即基于随机 IV 值的 BC 模式生成的密文可近似看作随机比特串。

**定理 1.** 假设分组密码 $E$ 满足 PRP-CPA，对任意 CPA 敌手 $\mathcal{A}$ 总有下式成立:

$$\boldsymbol{Adv}^{roi-ind-cpa}_{\$BC[E]}(q,t) \tag{10}$$
$$\leqslant \boldsymbol{Adv}^{prp-cpa}_{E}(q',t')+\sigma^2/2^n$$

其中，$\mathcal{A}$ 询问次数最多为 $q$ 次，且询问的消息分组总数为 $\sigma$，总运行时间为 $t$，且 $q'=\sigma=\mathrm{O}(q)$，$t'=t+\mathrm{O}(q)$。

证明. 下面采用做游戏(game- playing)[23-24]的技术来证明定理 1。当前，有许多密码方案都采用做游戏的方式进行证明，如 CBC-MAC、OAEP、Luky-Rackoff 结构、Hashed ElGamal 等[23-24]。在采用做游戏的方式进行证明过程中，敌手与加密 oracle 进行交互并最终输出判断结果的过程常常被描述为游戏过程，随后证明者将借助一些差异较小的辅助游戏过程一步步推导出证明目标。

根据前面的讨论，我们将 CPA 敌手 $\mathcal{A}$ 分别与现实情况、理想情况的加密 oracle 交互并输出判断结果的过程描述为游戏 1、游戏 4。则有下式成立:

$$\Pr\left[K\xleftarrow{\$}\mathcal{K}:\mathcal{A}^{\$BC[E]_K(\cdot)}=1\right]=\Pr[Game_1=1] \tag{11}$$

$$\Pr\left[\mathcal{A}^{\Pi(\cdot)}=1\right]=\Pr[Game_4=1] \tag{12}$$

其中，$\Pr[Game_i=1]$ 表示敌手 $\mathcal{A}$ 在 $Game_i\ (i=1,2,3,4)$ 中输出判断结果为 1 的概率。

故由公式(8)(11)(12)得，$\mathcal{A}$ 区分 $\$BC[E]$ 和 $\Pi$ 的成功概率 $\boldsymbol{Dist}^{\Pi}_{\$BC[E]}(\mathcal{A}(q,t))$ 如下:

$$\boldsymbol{Dist}^{\Pi}_{\$BC[E]}(\mathcal{A}(q,t)) \tag{13}$$
$$=\left|\Pr[Game_1=1]-\Pr[Game_4=1]\right|$$

由游戏 1、游戏 4 的具体描述可知，这两个游戏过程的差异比较大，无法直观得出公式(13)的结果。因此，我们在采用做游戏技巧进行证明过程中，借助游戏 2、游戏 3 这两个中间游戏一步步导出游戏 1、游戏 4 间的关系。

其中，游戏 2、游戏 3 分别描述了 CPA 敌手 $\mathcal{A}$ 与 $\$BC[\pi]$、$\$BC[\rho]$ 交互并输出判断结果的过程，$\$BC[\pi]$、$\$BC[\rho]$ 的定义见表 8、表 9。这两个方案将基于随机 IV 值的 BC 模式调用的分组密码 $E$ 分别替换成随机置换 $\pi$、随机函数 $\rho$。接下来，我们将说明如何借助这些游戏导出 $\boldsymbol{Dist}^{\Pi}_{\$BC[E]}(\mathcal{A}(q,t))$ 的上界。

**游戏 1.**($Game_1$)

1.1: $K\xleftarrow{\$}\{0,1\}^k$;
1.2: FOR $j=1$ TO $q$
1.3: $M^j\leftarrow\mathcal{A}\left(\left(M^1,C^1\right),\cdots,\left(M^{j-1},C^{j-1}\right)\right)$;
1.4: $C^j\leftarrow\$BC[E]_K\left(M^j\right)$;
1.5: $b\leftarrow\mathcal{A}\left(\left(M^1,C^1\right),\cdots,\left(M^q,C^q\right)\right)\in\{0,1\}$

**游戏 2.**($Game_2$)

2.1: $\pi\xleftarrow{\$}Perm(n)$;
2.2: FOR $j=1$ TO $q$
2.3: $M^j\leftarrow\mathcal{A}\left(\left(M^1,C^1\right),\cdots,\left(M^{j-1},C^{j-1}\right)\right)$;
2.4: $C^j\leftarrow\$BC[\pi]\left(M^j\right)$;
2.5: $b\leftarrow\mathcal{A}\left(\left(M^1,C^1\right),\cdots,\left(M^q,C^q\right)\right)\in\{0,1\}$

**游戏 3.**($Game_3$)

3.1: $\rho\xleftarrow{\$}Func(n)$;
3.2: FOR $j=1$ TO $q$
3.3: $M^j\leftarrow\mathcal{A}\left(\left(M^1,C^1\right),\cdots,\left(M^{j-1},C^{j-1}\right)\right)$;
3.4: $C^j\leftarrow\$BC[\rho]\left(M^j\right)$;
3.5: $b\leftarrow\mathcal{A}\left(\left(M^1,C^1\right),\cdots,\left(M^q,C^q\right)\right)\in\{0,1\}$

**游戏 4.**( $Game_4$ )

4.1:
4.2: FOR $j=1$ TO $q$
4.3: $M^j \leftarrow \mathcal{A}\left(\left(M^1,C^1\right),\cdots,\left(M^{j-1},C^{j-1}\right)\right)$;
4.4: $C^j \leftarrow \Pi\left(M^j\right)$;
4.5: $b \leftarrow \mathcal{A}\left(\left(M^1,C^1\right),\cdots,\left(M^q,C^q\right)\right) \in \{0,1\}$

**表 8** $\$BC[\pi]$ 的描述

$\$BC[\pi](M)$ // $\pi \xleftarrow{\$} Perm(n)$
$M=M_1M_2\cdots M_l$;
$IV \xleftarrow{\$} \{0,1\}^n$; $C_0 \leftarrow IV$;
$\Sigma \leftarrow 0^n$;
**for** $i=1$ **to** $l$
  $\Sigma \leftarrow \Sigma \oplus C_{i-1}$;
  $C_i \leftarrow \pi(M_i \oplus \Sigma)$;
**return** $C_0C_1C_2\cdots C_l$

**表 9** $\$BC[\rho]$ 的描述

$\$BC[\rho](M)$ // $\pi \xleftarrow{\$} Perm(n)$
$M=M_1M_2\cdots M_l$;
$IV \xleftarrow{\$} \{0,1\}^n$; $C_0 \leftarrow IV$;
$\Sigma \leftarrow 0^n$;
**for** $i=1$ **to** $l$
  $\Sigma \leftarrow \Sigma \oplus C_{i-1}$;
  $C_i \leftarrow \pi(M_i \oplus \Sigma)$;
**return** $C_0C_1C_2\cdots C_l$

$Game_1$ V.S. $Game_2$

这两个游戏的区别在于 BC 模式底层调用的算法不同, 分别见 $Game_1$ 中第 1.4 行和 $Game_2$ 中第 2.4 行, 其中 $Game_1$ 使用的是分组密码 $E$, 而 $Game_2$ 使用的是随机置换 $\pi$。若 CPA 敌手 $\mathcal{A}$ 能够区分 $\$BC[E]$ 和 $\$BC[\pi]$, 则必然存在相应 CPA 敌手 $\mathcal{B}_{\mathcal{A}}$ 可通过调用 $\mathcal{A}$ 来区分 $E$ 和 $\pi$, 故有下式成立:

$$\left|\Pr\left[Game_1=1\right]-\Pr\left[Game_2=1\right]\right| \quad (14)$$
$$=\left|\Pr\left[K \xleftarrow{\$} \mathcal{K}: \mathcal{A}^{\$BC[E]_K(\cdot)}=1\right]-\Pr\left[\mathcal{A}^{\$BC[\pi](\cdot)}=1\right]\right|$$
$$=\boldsymbol{Dist}_{\$BC[E]}^{\$BC[\pi]}(\mathcal{A}(q,t)) \leqslant \boldsymbol{Dist}_E^{\pi}(\mathcal{B}_{\mathcal{A}}(q',t'))$$

其中, $\mathcal{A}$ 的 $q$ 询问中消息分组总数是 $\sigma$, 故 BC 模式对底层算法进行了 $\sigma$ 次调用, $q'=\sigma=\mathrm{O}(q)$, $t'=t+\mathrm{O}(q)$。

因分组密码 $E$ 满足 PRP-CPA, 即对任意 CPA 敌手 $\mathcal{B}_{\mathcal{A}}$, 有:

$$\boldsymbol{Dist}_E^{\pi}(\mathcal{B}_{\mathcal{A}}(q',t')) \leqslant \boldsymbol{Adv}_E^{prp-cpa}(q',t') \quad (15)$$

由(14)(15)得, 对任意 CPA 敌手 $\mathcal{A}$,

$$\left|\Pr\left[Game_1=1\right]-\Pr\left[Game_2=1\right]\right| \quad (16)$$
$$\leqslant \boldsymbol{Adv}_E^{prp-cpa}(q',t')$$

其中, $q'=\sigma=\mathrm{O}(q)$, $t'=t+\mathrm{O}(q)$。

$Game_1$ 和 $Game_2$ 间刻画的是 $\$BC[E]$ 和 $\$BC[\pi]$ 两方案间的差异, 由(16)可知, $\$BC[E]$ 和 $\$BC[\pi]$ 的差异最终归约到底层调用的分组密码 $E$ 和 $\pi$ 之间的差异上。

$Game_2$ V.S. $Game_3$

这两个游戏的区别在于: $Game_2$ 中 BC 模式调用了随机置换 $\pi$ (见第 2.4 行), 而 $Game_3$ 中 BC 模式调用了随机函数 $\rho$ (见第 3.4 行)。同理, 一旦敌手 $\mathcal{A}$ 能够区分 $\$BC[\pi]$ 和 $\$BC[\rho]$, 则必然存在相应 CPA 敌手可通过调用 $\mathcal{A}$ 来区分随机置换 $\pi$ 和随机函数 $\rho$。由 PRP/PRF 切换引理可得, 对任意 CPA 敌手 $\mathcal{A}$, 有

$$\left|\Pr\left[Game_2=1\right]-\Pr\left[Game_3=1\right]\right| \quad (17)$$
$$\leqslant \boldsymbol{Adv}_{\pi}^{\rho}(q',t') \leqslant \sigma^2/2^{n+1}$$

其中, $\mathcal{A}$ 的 $q$ 次询问中消息分组总数是 $\sigma$, 即 BC 模式对底层算法进行了 $\sigma$ 次调用, $q'=\sigma=\mathrm{O}(q)$, $t'=t+\mathrm{O}(q)$。

$Game_3$ V.S. $Game_4$

这两个游戏的区别在于: $Game_3$ 中 BC 模式通过调用随机函数 $\rho$ 计算返回值(见第 3.4 行), 而 $Game_4$ 中直接由随机串生成函数 $\Pi$ 得到返回值(见第 4.4 行)。为了清晰地看出这两个游戏的区别, 表 10、表 11 中分别将 $Game_3$ 第 3.4 行和 $Game_4$ 第 4.4 行的代码展开了。其中, 表 10 的左列是将 $\$BC[\rho]$ 按其定义(见表 9)展开; 右列是将 $\Pi$ 生成随机串的方式(见表 7)进行改写, 由“一次性生成所需随机串”改写为“逐分组生成随机串”, 这两种表达方式是一致的。

**表 10** $Game_3$ **第 3.4 行的代码展开**

3.4: $C^j \leftarrow \$BC[\rho](M^j)$
3.41: $M^j=M_1^jM_2^j\cdots M_l^j$;
3.42: $IV^j \xleftarrow{\$} \{0,1\}^n$; $C_0^j \leftarrow IV^j$;
3.43: $\Sigma^j \leftarrow 0^n$;
3.44: **for** $i=1$ **to** $lj$
3.45: $\Sigma^j \leftarrow \Sigma^j \oplus C_{i-1}^j$;
3.46: $C_i^j \leftarrow E_K(M_i^j \oplus \Sigma^j)$;
3.47: $C^j=C_0^jC_1^jC_2^j\cdots C_l^j$

**表 11 $Game_4$ 第 4.4 行的代码展开**

| |
|---|
| 4.4: $C^j \leftarrow \Pi(M^j)$ |
| 4.41: $M^j=M_1^jM_2^j\cdots M_l^j$; |
| 4.42: |
| 4.43: $C_0^j \xleftarrow{\$} \{0,1\}^n$; |
| 4.44: **for** $i=1$ **to** $lj$ |
| 4.45: |
| 4.46: $C_i^j \xleftarrow{\$} \{0,1\}^n$; |
| 4.47: $C^j=C_0^jC_1^jC_2^j\cdots C_l^j$ |

由表 10、表 11 易知, $Game_3$、$Game_4$ 的区别体现在第 3.46 行和第 4.46 行。在 $Game_3$ 中, $C_i^j$ $(j=1,\cdots,q;i=1,\cdots,l_j)$ 是由 $M_i^j\oplus\Sigma^j$ 经过随机函数 $\rho$ 映射得到的, 一旦 $\rho$ 的输入值出现碰撞, 则输出值也将发生碰撞。而在 $Game_4$ 中, 每一个 $C_i^j$ 均是分组大小的随机比特串, 其与 $M_i^j\oplus\Sigma^j$ 无关, 故任意 $C_i^j$ 均是随机独立的, $j=1,\cdots,q;i=1,\cdots,l_j$。

接下来, 我们定义事件 $BAD_1$ 如下:

$$BAD_1 \overset{def}{=} \{\exists(j,i)\neq(j',i'), M_i^j\oplus\Sigma^j=M_{i'}^{j'}\oplus\Sigma^{j'} \mid j,j'=1,\cdots,q;i=1,\cdots,l_j;i'=1,\cdots,l_{j'}\}$$

为了求 $BAD_1$ 事件的发生概率, 需要对 $M_i^j\oplus\Sigma^j$ 的碰撞进行分析, 现将该位置计算得到的结果记为集合 $IN=\{\{M_u^v\oplus\Sigma^v\}_{(u,v)}\}$, 则在计算当前 $M_i^j\oplus\Sigma^j$ 时, $(u,v)$ 应满足 $v\in\{1,\cdots,j-1\}$, $u\in\{1,\cdots,l_v\}$ 或 $v=j$, $u\in\{1,\cdots,i\}$。

用 $col(j,i)$ 表示在 $M_i^j\oplus\Sigma^j$ 位置首次发生碰撞的事件, 即在 $M_i^j\oplus\Sigma^j$ 计算之前, $\{\{M_u^v\oplus\Sigma^v\}_{(u,v)}\}$ 中没有出现碰撞, 且 $M_i^j\oplus\Sigma^j$ 的值与 $\{\{M_u^v\oplus\Sigma^v\}_{(u,v)}\}$ 发生碰撞。则有 $\forall(j,i), j=1,\ldots,q;i=1,\ldots,l_j$,

1) $|IN|=\sum_{v=1}^{j-1}l_v+i-1$;

2) $\Pr[col(j,i)]=|IN|/2^n$。

综上, 有

$$\begin{aligned}&\Pr[BAD_1]\\ &\leqslant\sum_{j=1}^{q}\sum_{i=1}^{l_j}\Pr[col(j,i)]\\ &=\sigma(\sigma-1)/2^{n+1}\leqslant\sigma^2/2^{n+1}\end{aligned}\tag{18}$$

其中, $\sigma$ 是 $\mathcal{A}$ 的 $q$ 次询问中消息分组总数, 即 $\sum_{j=1}^{q}l_j=\sigma$。

易知, 当 $BAD_1$ 事件发生, 在 $Game_3$ 中有, $\rho(M_i^j\oplus\Sigma^j)=\rho(M_{i'}^{j'}\oplus\Sigma^{j'})$, 即 $C_i^j=C_{i'}^{j'}$, 而在 $Game_4$ 中, 任意 $C_i^j$、$C_{i'}^{j'}$ 是独立随机的, 则在这两个游戏中敌手 $\mathcal{A}$ 经过 $q$ 次询问获得的信息不一致。而当 $BAD_1$ 事件没有发生时, 在 $Game_3$、$Game_4$ 中敌手 $\mathcal{A}$ 在 $q$ 次询问中获得的返回值都是随机比特串, 则 $\mathcal{A}$ 的表现是一致的, 即

$$\begin{aligned}&\Pr[Game_3=1\mid\overline{BAD_1}]\\ &=\Pr[Game_4=1\mid\overline{BAD_1}]\end{aligned}\tag{19}$$

故由(18)(19)可得, 对任意 CPA 敌手 $\mathcal{A}$,

$$\begin{aligned}&\left|\Pr[Game_3=1]-\Pr[Game_4=1]\right|\\ &\leqslant\left|\Pr[Game_3=1\mid\overline{BAD_1}]-\Pr[Game_4=1\mid\overline{BAD_1}]\right|\cdot\Pr[\overline{BAD_1}]\\ &+\left|\Pr[Game_3=1\mid BAD_1]-\Pr[Game_4=1\mid BAD_1]\right|\cdot\Pr[BAD_1]\\ &\leqslant\Pr[BAD_1]\leqslant\sigma^2/2^{n+1}\end{aligned}\tag{20}$$

结论

综上所述, 由(13)(16)(17)(20)得, 对任意 CPA 敌手 $\mathcal{A}$, 有

$$\begin{aligned}&\boldsymbol{Dist}^{\Pi}_{\$BC[E]}(\mathcal{A}(q,t))\\ &=\left|\Pr[Game_1=1]-\Pr[Game_4=1]\right|\\ &\leqslant\left|\Pr[Game_1=1]-\Pr[Game_2=1]\right|\\ &+\left|\Pr[Game_2=1]-\Pr[Game_3=1]\right|\\ &+\left|\Pr[Game_3=1]-\Pr[Game_4=1]\right|\\ &\leqslant\boldsymbol{Adv}_E^{prp-cpa}(q',t')+\sigma^2/2^n\end{aligned}\tag{21}$$

即有,

$$\begin{aligned}&\boldsymbol{Adv}^{roi-ind-cpa}_{\$BC[E]}(q,t)\\ &\leqslant\boldsymbol{Adv}_E^{prp-cpa}(q',t')+\sigma^2/2^n\end{aligned}\tag{22}$$

至此, 定理 1 的证明结束。

ROI-IND 定义是从密文与随机比特串区分的角度来刻画密码方案的机密性, 根据该定义, 当 BC 模式的输出密文出现不随机的现象, 即可将其作为 BC 模式的密文与随机比特串的区分依据进行区分攻击(distinguish attack)。故下文列举的区分攻击将给出 BC 模式输出密文不随机的简单实例。

**攻击 1.** 在常规 CPA 模型下对基于 Nonce 的 BC 模式的区分攻击:

记常规 CPA 敌手为 $\mathcal{A}_{cpa}$, 其可以询问基于 Nonce 的 BC 模式的加密 oracle $\#BC[E]_K(\cdot,\cdot)$(见表 5), 且其可以选择不重复的 N 值。现 $\mathcal{A}_{cpa}$ 先询问任意消

息 $(N, M_1)$，$M_1$ 仅为一个分组长度，记其返回值为 $C_1$；接着询问 $(N', M_1')$，其中 $N' \neq N$，$M_1' = N' \oplus N \oplus M_1$，记其返回值为 $C_1'$。易知，当加密 oracle 为 $\#BC[E]_K(\cdot,\cdot)$，$K \xleftarrow{\$} \{0,1\}^k$ 时，一定有 $C_1' = C_1$。

### 4.2 逐分组攻击模型下 BC 模式的安全性

BW-CPA 敌手的能力比常规 CPA 敌手更强，尽管基于随机 IV 值的 BC 模式在常规 CPA 下是安全的，但其在 BW-CPA 下存在十分简单高效的区分攻击，下文攻击 2 给出了一个实例。而基于 Nonce 值的 BC 模式在常规 CPA 下已不安全了，则在 BW-CPA 下其同样不安全，上文所给的攻击 1 在 BW-CPA 下同样是成立的。

**攻击 2.** 在 BW-CPA 模型下对基于 IV 的 BC 模式的区分攻击:

记 BW-CPA 敌手为 $\mathcal{A}_{bw-cpa}$，其可以在询问基于随机 IV 的加密 oracle $\$BC[E]_K(\cdot)$ (见表 4)时逐分组地提交消息分组并获得相应返回值，但其不可选择 IV 值。现 $\mathcal{A}_{bw-cpa}$ 询问任意消息 $(M_1 M_2)$，其先提交消息分组 $M_1$，得到返回值 $(C_0 C_1)$，其中 $C_0$ 是 BC 模式随机选择的 IV 值；接着 $\mathcal{A}_{bw-cpa}$ 修改 $M_2 = C_1 \oplus M_1$，提交 $M_2$ 并得到其返回值 $C_2$。易知，当加密 oracle 为 $\$BC[E]_K(\cdot)$，$K \xleftarrow{\$} \{0,1\}^k$ 时，一定有 $C_2 = C_1$。

由上讨论可知，基于 Nonce 的 BC 模式十分脆弱，在常规 CPA 下已经不安全了；而基于随机 IV 值的 BC 模式尽管在常规 CPA 下具有较好的机密性，但其在 BW-CPA 下是不安全的。因此，从具体应用的角度分析得，BC 模式因依赖于随机 IV 值而容易被误用，且其应用于在线环境是不安全的。针对该问题，本文在 BC 模式上进行改进得到一个新的加密模式——基于 Nonce 的 XBC 模式，该模式不易被误用，且能够满足在线应用的需求。

## 5 BC 模式的改进方案: 基于 Nonce 的 XBC 模式

由第 4 节的分析可知，BC 模式的机密性完全依赖于 IV 值的随机性，其不仅容易出现误用，且实用性受限。因此，本节将探讨如何在 BC 模式的基础上进行改进，得到一个基于 Nonce 的新工作模式，以抵抗逐分组攻击，满足在线应用的需求。

在尝试改进 BC 模式时，我们首先借鉴和比较已有的改进方法，从中吸取经验。针对 CBC 模式的机密性依赖于 IV 值的随机性这一点，Rogaway 在原始的 CBC 基础进行改进，提出了基于 Nonce 的 CBC2 模式[16] (图 4)。与原始 CBC 模式比较，CBC2 模式使用了两个密钥，其中一个密钥先用于加密 Nonce 值，所得密文作为反馈变量(The Feedback)的初始值使用，另一个密钥则用作明文消息处理时加密密钥。CBC2 模式的其运行效率接近原来 CBC 模式。借鉴 CBC2 模式的设计，可以在 BC 模式的基础上改进得到一个基于 Nonce 的 BC2 模式，但该方法所需的密钥量大，且不能抵抗 BW-CPA。

在文献[17]，针对 CBC 不能抵抗 BW-CPA，Fouque 等人提出了一个通用方法——将密文输出延迟一个分组，并证明了 DCBC(Delayed CBC)模式能够抵抗 BW-CPA。类似地，BC 模式可以通过延迟密文分组输出的方式来达到抵抗 BW-CPA 的目的，但该方法得到的新模式安全性仍然依赖于 IV 值的随机性，且可能降低了应用系统的响应效率。

由上讨论可知，直接套用已有的改进方法无法同时解决基于 Nonce 的安全性和抵抗 BW-CPA 这两点。在 BC 模式中，一旦密钥随机选定了，底层的分组密码可以看作一个确定性算法，第 4 节给出的区分攻击正好利用这一点，通过让分组密码的输入值中出现碰撞而达到预测密文输出的目的。实际上，目前许多经典的工作模式(如 ECB、CBC 等)都存在同样的问题。本文借鉴了 Rogaway 提出的 XE 结构[25]对 BC 模式进行改进，以使底层调用的算法具有足够的不确定性。

我们将改进后的工作模式称为基于 Nonce 的 XBC(eXtended Block Chaining operation mode)模式。接下来，我们将给出基于 Nonce 的 XBC 模式的详细定义，并证明其具有 ROI-IND-CBW-CPA 机密性，其中 ROI-IND-CBW-CPA 是指 CBW-CPA 下现实情况和理想情况不可区分性。

### 5.1 基于 Nonce 的 XBC 模式

在描述 XBC 模式的过程中，将沿用 BC 模式的记法，其中还增加了下列变量:

1) Nonce 值 $N \in \{0,1\}^n$，这里要求每次加密时该值不可重复;

2) 定义为有限域 $\mathbb{F}_{2^n}$ 上的乘法，2 是有限域上的生成元，有时在不引起歧义情况下可省略该符号。$2^i$ 表示 $i$ 个因子为 2 进行 $i-1$ 次有限域乘法。

同样地，为了便于阐述，假设 XBC 模式处理的明文消息长度刚好是 $n$ 比特的整数倍。则 XBC 模式的映射关系可表示为 $\mathcal{XBC}: \{0,1\}^k \times \{0,1\}^n \times \left(\{0,1\}^n\right)^+ \to \left(\{0,1\}^n\right)^+$，其中密钥空间为 $\{0,1\}^k$，假设 $K \xleftarrow{\$} \{0,1\}^k$，则 XBC 模

式的加解密过程分别如图 3、图 4 所示, 具体描述分别见表 12、表 13(其中, 加□的运算较原始 BC 模式增加的运算操作)。

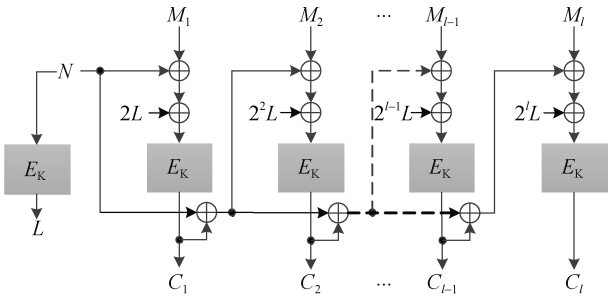



**图 3　XBC 模式的加密过程**

**表 12　基于 Nonce 的 XBC 模式的加密过程**

$M=M_1M_2\cdots M_l$ ;
$\Sigma\leftarrow N$ ;
$\boxed{L\leftarrow E_K(N)}$;
$\boxed{\Delta\leftarrow 2\cdot L}$;
**for** $i=1$ **to** $l$
　　$C_i\leftarrow E_K(M_i\oplus\Sigma\oplus\Delta)$ ;
　　$\Sigma\leftarrow\Sigma\oplus C_i$ ;
　　$\boxed{\Delta\leftarrow 2\cdot\Delta}$;
**return** $C_1C_2\cdots C_l$

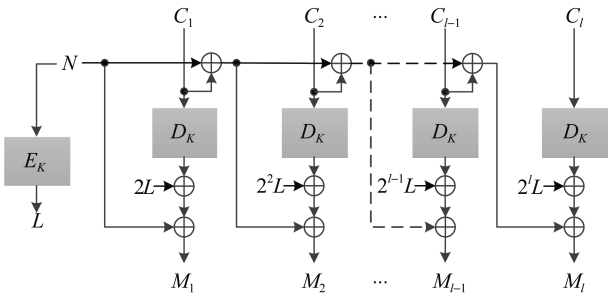



**图 4　XBC 模式的解密过程**

**表 13　基于 Nonce 的 XBC 模式的解密过程**

$C=C_1C_2\cdots C_l$ ;
$\Sigma\leftarrow N$ ;
$\boxed{L\leftarrow E_K(N)}$;
$\boxed{\Delta\leftarrow 2\cdot L}$;
**for** $i=1$ **to** $l$
　　$M_i\leftarrow D_K(C_i)\oplus\Sigma\oplus\Delta$ ;
　　$\Sigma\leftarrow\Sigma\oplus C_i$ ;
　　$\boxed{\Delta\leftarrow 2\cdot\Delta}$;
**return** $M_1M_2\cdots M_l$

基于 Nonce 的 XBC 模式较原始的 BC 模式改动不大, 其每次加解密增加了一次分组密码的调用和计算 $2^iL$ 的有限域运算 (分别见表 12、表 13 加□部分)。二者从运算效率上看相差不大, 因为 $2^iL$ 的计算可以采用累加计算(accumulated compute)的方式, 即 $2^iL$ 的计算可利用 $2^{i-1}L$ 的结果。与 CBC2 模式的改进方法相比, XBC 模式仅需要一个密钥; 与 DCBC 模式的改进方法相比, XBC 模式的密文输出及时, 且其安全性是基于不重复的 Nonce 值。

同时需要强调的是 $L$ 对 XBC 模式的机密性至关重要, 在进行加解密过程中要保证 $2^iL$ 等中间状态值不被泄漏。本文在对 XBC 模式进行安全性分析时, 假设其计算过程是一个黑盒(black-box), 除了明密文分组, 敌手是无法获取任何中间状态值的。

由下面定理 2 可知, 基于 Nonce 的 XBC 模式能够抵抗 CBW-CPA 攻击, 故从具体应用角度分析, 其安全性比原始的 BC 模式好, 误用率低, 实用性高, 于在线环境的应用不受限。

## 5.2　ROI-IND-CBW-CPA 定义

为了论证基于 Nonce 的 XBC 模式能够抵抗 CBW-CPA 攻击, 我们将 ROI-IND-CPA 的定义扩展到 CBW-CPA 下, 得到一个新的安全定义——在并发逐分组适应的选择明文攻击下的现实情况和理想情况不可区分性 (Real-Or-Ideal INDistinguishability against Concurrent BlockWise adaptive Chosen Plaintext Attack, 以下简称 ROI-IND-CBW- CPA)。这里的 CBW-CPA 敌手可以在不同的消息询问过程中并发地进行逐分组控制。在实际应用中, 并发的多任务系统很常见, 故刻画拥有并发控制能力的敌手具有现实意义, 有利于分析密码方案在并发的多任务系统中的安全强度。文献[17-18]中也涉及了 CBW-CPA 敌手。

在 CBW-CPA 下, 敌手能够询问一个特殊的加密 oracle——具有并发性的可逐分组提交消息分组的加密 oracle(Concurrent BlockWise adaptive encryption oracle), 以下简称 CBW-oracle。

假设对称密码方案 $\mathcal{SE}$: $\mathcal{K}\times\mathcal{M}\to\mathcal{C}$, 其中 $\mathcal{K}$、$\mathcal{M}$ 和 $\mathcal{C}$ 分别是密钥空间、明文空间和密文空间, 则现实情况的 CBW-oracle 定义为 $\mathcal{SE}_K^{seq,i}(\cdot)$, 其中 $K\xleftarrow{\$}\mathcal{K}$, $seq$ 是并发询问的序列号, $i$ 指第 $seq$ 个询问的第 $i$ 个分组, 其计算过程为 $\forall M_i^{seq}$, $C_i^{seq}=\mathcal{SE}_K^{seq,i}\left(M_i^{seq}\right)$; 理想情况的 CBW-oracle 定义为 $Con\Pi_K^{seq,i}(\cdot)$, 其计算过程为 $\forall M_i^{seq}$, $C_i^{seq}\xleftarrow{\$}\{0,1\}^{bl}$ 其中 $bl$ 为分组大小。显然的, $Con\Pi^{seq,i}(\cdot)$ 总是返回长度为 $bl$ 的随机比特串。

现 CBW-CPA 敌手 $\mathcal{A}$, 若其询问 CBW- oracle 次数最多 $q$ 次, 总运行时间为 $t$, 则其对现实情况和理

想情况的区分概率为

$$\boldsymbol{Dist}_{\mathcal{SE}^{seq,i}}^{Con\Pi^{seq,i}}\left(\mathcal{A}(q,t)\right) \tag{23}$$

$$=\left|\Pr[K\xleftarrow{\$}\{0,1\}^k:\mathcal{A}^{\mathcal{SE}_K^{seq,i}(\cdot)}=1]\right.$$

$$\left.-\Pr\left[\mathcal{A}^{Con\Pi^{seq,i}(\cdot)}=1\right]\right|$$

对任意 CBW-CPA 敌手 $\mathcal{A}$，定义下式

$$\boldsymbol{Adv}_{\mathcal{SE}}^{roi-ind-cbw-cpa}(q,t) \tag{24}$$

$$=\max_{\mathcal{A}}\left\{\boldsymbol{Dist}_{\mathcal{SE}^{seq,i}}^{Con\Pi^{seq,i}}\left(\mathcal{A}(q,t)\right)\right\},$$

当 $\boldsymbol{Adv}_{\mathcal{SE}}^{roi-ind-cbw-cpa}(q,t)$ 是可忽略函数时，我们称对称密码方案 $\mathcal{SE}$ 在 CBW-CPA 下满足现实情况和理想情况的不可区分性(Real-Or-Ideal Indistinguishability against CBW-CPA, ROI-IND-CBW-CPA)。从直观上理解，当 $\boldsymbol{Adv}_{\mathcal{SE}}^{roi-ind-cbw-cpa}(q,t)$ 是可忽略函数时，可以认为在 $q$ 次加密中，对称密码方案 $\mathcal{SE}$ 生成的每一个密文分组都是完全独立随机的比特串。

因本文不涉及 CCA 安全，故上述定义只考虑了 CPA 安全。

对分组密码 $E$ 而言，CBW-CPA 敌手、BW-CPA 敌手和标准的 CPA 敌手能力是完全一致的，故可将 PRP/PRF-CPA 定义直接扩展为 PRP/PRF-CBW-CPA、PRP/PRF-BW- CPA，即有

$$\boldsymbol{Adv}_E^{prp-cbw-cpa}(q,t)=\boldsymbol{Adv}_E^{prp-bw-cpa}(q,t) \tag{25}$$

$$=\boldsymbol{Adv}_E^{prp-cpa}(q,t)$$

$$\boldsymbol{Adv}_E^{prf-cbw-cpa}(q,t)=\boldsymbol{Adv}_E^{prf-bw-cpa}(q,t) \tag{26}$$

$$=\boldsymbol{Adv}_E^{prf-cpa}(q,t)$$

另外，PRP/PRF 切换引理在 CBW-CPA、BW-CPA 下同样成立。

### 5.3 基于 Nonce 的 XBC 模式满足 ROI-IND-CBW-CPA 性质

在本小节，我们将采用做游戏的方式证明基于不重复 Nonce 值的 XBC 模式满足 ROI-IND-CBW-CPA 性质。为了比较 XBC 模式和 BC 模式， XBC 模式的证明同样采用了基于分组密码(PRP-CPA)的假设。

**表 14　现实情况的 CBW-oracle**

| $XBC[E]_K^{j,i}(N^j, M_i^j)$ |
|---|
| $C_i^j\leftarrow E_K(M_i^j\oplus\Sigma^j\oplus\Delta^j)$; |
| $\Sigma^j\leftarrow\Sigma^j\oplus C_i^j$; |
| $\Delta^j\leftarrow 2\cdot\Delta^j$; |
| **return** $C_i^j$; |

**表 15　理想情况的 CBW-oracle**

| $X\Pi^{j,i}(N^j, M_i^j)$ |
|---|
| $C_i^j\xleftarrow{\$}\{0,1\}^n$; |
| **return** $C_i^j$; |

易知，现实情况的 CBW-oracle 为表 14 中所定义的 $XBC[E]_K^{j,i}(\cdot,\cdot)$，其中 $K\xleftarrow{\$}\{0,1\}^k$，$j$ 表示并发询问中的第 $j$ 个询问，$i$ 表示第 $j$ 个询问中的第 $i$ 个消息分组。为了正确计算，在每个询问，$XBC[E]_K^{j,i}(\cdot,\cdot)$ 需要记录并适时更新其中间状态值 $\Sigma^j$、$\Delta^j$，且当计算 $XBC[E]_K^{j,1}(N^j, M_1^j)$ 时，其初始值分别 $\Sigma^j\leftarrow N^j$，$\Delta^j\leftarrow 2\cdot E_K(N^j)$，$(j=1,\cdots,q)$。

相应地，理想情况的 CBW-oracle 为表 15 中所定义的 $X\Pi^{j,i}(\cdot,\cdot)$，其对任意输入值均返回 $n$ 比特的随机比特串。

这里我们限定在同一个询问中，询问的消息分组是逐分组有序的，即敌手先询问 $(N^j, M_i^j)$ 后才询问 $(N^j, M_{i+1}^j)$。

假设 CBW-CPA 敌手 $\mathcal{A}$ 对 CBW-oracle $\mathcal{O}^{j,i}(\cdot,\cdot)\in\left\{XBC[E]_K^{j,i}(\cdot,\cdot), X\Pi^{j,i}(\cdot,\cdot)\right\}$ 的并发询问不超过 $q$ 次，总运行时间为 $t$，则 $\mathcal{A}$ 对 $XBC[E]_K^{j,i}$ 和 $X\Pi^{j,i}$ 的区分概率定义如下:

$$\boldsymbol{Dist}_{XBC[E]^{j,i}}^{X\Pi^{j,i}}\left(\mathcal{A}(q,t)\right) \tag{27}$$

$$=\left|\Pr\left[K\xleftarrow{\$}\mathcal{K}:\mathcal{A}^{XBC[E]_K^{j,i}(\cdot,\cdot)}=1\right]\right.$$

$$\left.-\Pr\left[\mathcal{A}^{X\Pi^{j,i}(\cdot,\cdot)}=1\right]\right|$$

其中，$j=1,\cdots,q$，$i=1,\cdots,l_j$。

对任意 CBW-CPA 敌手 $\mathcal{A}$，定义下式:

$$\boldsymbol{Adv}_{XBC[E]}^{roi-ind-cbw-cpa}(q,t) \tag{28}$$

$$=\max_{\mathcal{A}}\left\{\boldsymbol{Dist}_{XBC[E]^{j,i}}^{X\Pi^{j,i}}\left(\mathcal{A}(q,t)\right)\right\}$$

定理 2 给出了 $\boldsymbol{Adv}_{XBC[E]}^{roi-ind-cbw-cpa}(q,t)$ 的上界，由其结论知，$\boldsymbol{Adv}_{XBC[E]}^{roi-ind-cbw-cpa}(q,t)$ 的上界主要由底层分组密码 $E$ 的机密性决定，而分组密码 $E$ 是一个 PRP(-CBW)-CPA，则 $\boldsymbol{Adv}_E^{prp-cbw-cpa}(q,t)=\boldsymbol{Adv}_E^{prp-cpa}(q,t)$ 是可忽略函数。也就是说，当

$\sigma+q\ll 2^{n/2}$ 时, 基于Nonce的XBC模式生成的任一密文分组均可看作完全随机独立的比特串。

**定理 2.** 假设分组密码 $E$ 满足 PRP-CPA, 对任意 CBW-CPA 敌手 $\mathcal{A}$ 总有下式成立:

$$\boldsymbol{Adv}_{XBC[E]}^{roi-ind-cbw-cpa}(q,t) \tag{29}$$
$$\leqslant \boldsymbol{Adv}_{E}^{prp-cpa}(q',t') + (\sigma+q)^2/2^n$$

其中, $\mathcal{A}$ 询问次数最多为 $q$ 次, 且询问的消息分组总数为 $\sigma$, 总运行时间为 $t$, 且 $q'=\sigma+q=\ \mathrm{O}(q)$, $t'=t+\mathrm{O}(q)$。

证明. 下面仍然采用做游戏的技术来证明定理 2。根据 ROI-IND-CBW-CPA 定义, 将 CBW-CPA 敌手 $\mathcal{A}$ 分别与现实情况、理想情况的 CBW-oracle 交互并输出判断结果的过程描述为游戏 5、游戏 8, 则有下式成立:

$$\Pr[K\xleftarrow{\$}\mathcal{K}:\mathcal{A}^{XBC[E]_K^{j,i}(\cdot,\cdot)}=1]=\Pr[Game_5=1] \tag{30}$$

$$\Pr\left[\mathcal{A}^{X\Pi^{j,i}(\cdot,\cdot)}=1\right]=\Pr[Game_8=1] \tag{31}$$

为了保证在同一个消息询问中, 敌手询问的消息分组是逐分组有序的, 这里假设在各游戏中 $\mathcal{A}$ 生成的 $(j,i)$ 满足以下(1)或(2):

(1) $i=1$;

(2) $(j,1),\cdots,(j,i-1)$ 已经被询问过。

由式(27)(30)(31)得:

$$\boldsymbol{Dist}_{XBC[E]^{j,i}}^{X\Pi^{j,i}}(\mathcal{A}(q,t)) \tag{32}$$
$$=\left|\Pr[Game_5=1]-\Pr[Game_8=1]\right|$$

由游戏 5、游戏 8 的具体过程描述可知, 这两个游戏间的差异比较大, 无法直观得出公式(32)的结果。因此, 我们在进行做游戏证明过程中, 借助游戏 6、游戏 7 这两个中间游戏一步步导出游戏 5 和游戏 8 的关系。

其中, 游戏 6、游戏 7 分别描述了敌手 $\mathcal{A}$ 与 $XBC[\pi](\cdot,\cdot)$、$XBC[\rho](\cdot,\cdot)$ 交互并输出判断结果的过程, $XBC[\pi](\cdot,\cdot)$、$XBC[\rho](\cdot,\cdot)$ 的 CBW-oracle 的定义分别如表 16、表 17 所示。实际上, $XBC[\pi](\cdot,\cdot)$、$XBC[\rho](\cdot,\cdot)$ 分别是将 XBC 模式调用的分组密码 $E$ 替换成随机置换 $\pi$、随机函数 $\rho$。接下来, 我们将说明如何借助这些游戏导出式子(32)的上界。

$Game_5$ V.S. $Game_6$

这两个游戏的区别在于 XBC 模式底层调用的算法不同, 分别见 $Game_5$ 第 5.10、5.12 行和 $Game_6$ 中第 6.10、6.12 行, 其中 $Game_5$ 调用的是分组密码 $E$, 而 $Game_6$ 使用的是随机置换 $\pi$。一旦 CBW-CPA 敌手 $\mathcal{A}$ 能够区分 $XBC[E]^{j,i}$ 和 $XBC[\pi]^{j,i}$, 则必然存在相应(CBW-)CPA 敌手 $\mathcal{B}_A$ 可通过调用 $\mathcal{A}$ 来区分 $E$ 和 $\pi$, 即有下式成立:

$$\Pr[Game_5=1]-\Pr[Game_6=1] \tag{33}$$
$$=\Pr[K\xleftarrow{\$}\mathcal{K}:\mathcal{A}^{XBC[E]_K^{j,i}(\cdot,\cdot)}=1]-\Pr\left[\mathcal{A}^{XBC[\pi]^{j,i}(\cdot,\cdot)}=1\right]$$
$$=\boldsymbol{Dist}_{XBC[E]^{j,i}}^{XBC[\pi]^{j,i}}(\mathcal{A}(q,t))\leqslant \boldsymbol{Dist}_{E}^{\pi}(\mathcal{B}_{\mathcal{A}}(\sigma+q,t'))$$

其中, $\mathcal{A}$ 的 $q$ 次询问中消息分组总数是 $\sigma$, 故 XBC 模式对底层算法进行了 $\sigma+q$ 次调用。

因分组密码 $E$ 满足PRP-CPA, 由(2)(25)可得, 对任意(CBW-)CPA 敌手 $\mathcal{B}_A$, 有下式:

$$\boldsymbol{Dist}_{E}^{\pi}(\mathcal{B}_{\mathcal{A}}(\sigma+q,t')) \tag{34}$$
$$\leqslant \boldsymbol{Adv}_{E}^{prp-cpa}(\sigma+q,t')。$$

由(33)(34)得, 对任意 CBW-CPA 敌手 $\mathcal{A}$,

$$\Pr[Game_5=1]-\Pr[Game_6=1] \tag{35}$$
$$\leqslant \boldsymbol{Adv}_{E}^{prp-cpa}(\sigma+q,t')$$

$Game_5$ 、 $Game_6$ 之间刻画的是 $XBC[E]$ 和 $XBC[\pi]$ 两方案在 CBW-CPA 下的差异, 由(35)可知, $XBC[E]$ 和 $XBC[\pi]$ 的差异最终归约到分组密码 $E$ 和随机置换 $\pi$ 的差异上。

$Game_6$ V.S. $Game_7$

这两个游戏的区别在于: $Game_6$ 中 XBC 模式调用了随机置换 $\pi$ (见第 6.10、6.12 行), 而 $Game_7$ 中 XBC 模式调用了随机函数 $\rho$ (见第 7.10、7.12 行) 。同理, 若敌手 $\mathcal{A}$ 在这两个游戏中表现有差异, 则 $\mathcal{A}$ 能够区分 $XBC[\pi]$ 和 $XBC[\rho]$, 则必然存(CBW-)CPA

**游戏 5.**( $Game_5$ )

5.1: $K\xleftarrow{\$}\{0,1\}^k$;
5.2: FOR $j=1$ TO $q$
5.3: $(N^j,M^j,C^j)\leftarrow(\varepsilon,\varepsilon,\varepsilon)$;
5.4: $count=0$;
5.5:WHILE $(count<\sigma)$ DO
5.6: $(j,i)\leftarrow\mathcal{A}\left(\left\{(N^j,M^j,C^j)\right\}_q\right)$;
5.7: IF $(i=1)$ THEN

5.8: $N^j \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right)$;

5.9: $\Sigma^j \leftarrow N^j$;

5.10: $\Delta^j \leftarrow 2 \cdot E_K(N^j)$;

5.11: $M_i^j \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right)$;

5.12: $C_i^j \leftarrow XBC[E]_K^{j,i}(N^j, M_i^j)$;

5.13: $(N^j, M^j, C^j) \leftarrow (N^j, M^j \| M_i^j, C^j \| C_i^j)$;

5.14: $count = count + 1$;

5.15: $b \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right) \in \{0,1\}$

**游戏 6.**( $Game_6$ )

6.1: $\pi \xleftarrow{\$} Perm(n)$;

6.2: FOR $j=1$ TO $q$

6.3: $(N^j, M^j, C^j) \leftarrow (\varepsilon, \varepsilon, \varepsilon)$;

6.4: $count = 0$;

6.5:WHILE $(count < \sigma)$ DO

6.6: $(j,i) \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right)$;

6.7: IF $(i=1)$ THEN

6.8: $N^j \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right)$;

6.9: $\Sigma^j \leftarrow N^j$;

6.10: $\Delta^j \leftarrow 2 \cdot E_K(N^j)$;

6.11: $M_i^j \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right)$;

6.12: $C_i^j \leftarrow XBC[\pi]^{j,i}(N^j, M_i^j)$;

6.13: $(N^j, M^j, C^j) \leftarrow (N^j, M^j \| M_i^j, C^j \| C_i^j)$;

6.14: $count = count + 1$;

6.15: $b \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right) \in \{0,1\}$

**表 16** $XBC[\pi](\cdot,\cdot)$ 的 **CBW-oracle** 描述

$XBC[\pi]^{j,i}(N^j, M_i^j)$ // $\pi \xleftarrow{\$} Perm(n)$

$C_i^j \leftarrow \pi(M_i^j \oplus \Sigma^j \oplus \Delta^j)$;

$\Sigma^j \leftarrow \Sigma^j \oplus C_i^j$;

$\Delta^j \leftarrow 2 \cdot \Delta^j$;

**return** $C_i^j$;

(初始时 $\Sigma^j \leftarrow N^j$ 、 $\Delta^j \leftarrow 2 \cdot \pi(N^j)$ )

**游戏 7.**( $Game_7$ )

7.1: $\rho \xleftarrow{\$} Func(n)$;

7.2: FOR $j=1$ TO $q$

7.3: $(N^j, M^j, C^j) \leftarrow (\varepsilon, \varepsilon, \varepsilon)$;

7.4: $count = 0$;

7.5:WHILE $(count < \sigma)$ DO

7.6: $(j,i) \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right)$;

7.7: IF $(i=1)$ THEN

7.8: $N^j \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right)$;

7.9: $\Sigma^j \leftarrow N^j$;

7.10: $\Delta^j \leftarrow 2 \cdot E_K(N^j)$;

7.11: $M_i^j \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right)$;

7.12: $C_i^j \leftarrow XBC[\rho]^{j,i}(N^j, M_i^j)$;

7.13: $(N^j, M^j, C^j) \leftarrow (N^j, M^j \| M_i^j, C^j \| C_i^j)$;

7.14: $count = count + 1$;

7.15: $b \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right) \in \{0,1\}$

**游戏 8.**( $Game_8$ )

8.1:

8.2: FOR $j=1$ TO $q$

8.3: $(N^j, M^j, C^j) \leftarrow (\varepsilon, \varepsilon, \varepsilon)$;

8.4: $count = 0$;

8.5:WHILE $(count < \sigma)$ DO

8.6: $(j,i) \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right)$;

8.7: IF $(i=1)$ THEN

8.8: $N^j \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right)$;

8.9:

8.10:

8.11: $M_i^j \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right)$;

8.12: $C_i^j \leftarrow X\Pi^{j,i}(N^j, M_i^j)$;

8.13: $(N^j, M^j, C^j) \leftarrow (N^j, M^j \| M_i^j, C^j \| C_i^j)$;

8.14: $count = count + 1$;

8.15: $b \leftarrow \mathcal{A}\left(\left\{(N^j, M^j, C^j)\right\}_q\right) \in \{0,1\}$

**表 17 $XBC[\rho](\cdot,\cdot)$ 的 CBW-oracle 描述**

| $XBC[\rho]^{j,i}(N^j, M_i^j) // \rho \xleftarrow{\$} Func(n)$ |
|---|
| $C_i^j \leftarrow \rho(M_i^j \oplus \Sigma^j \oplus \Delta^j)$; |
| $\Sigma^j \leftarrow \Sigma^j \oplus C_i^j$; |
| $\Delta^j \leftarrow 2\cdot\Delta^j$; |
| **return** $C_i^j$; |
| (初始时 $\Sigma^j \leftarrow N^j$ 、 $\Delta^j \leftarrow 2\cdot\rho(N^j)$) |

敌手 $\mathcal{B}_A$ 可通过调用 $\mathcal{A}$ 成功地区分随机置换 $\pi$ 和随机函数 $\rho$。由 PRP/PRF 切换引理可得, 对任意 CBW-CPA 敌手 $\mathcal{A}$,

$$\Pr[Game_6=1]-\Pr[Game_7=1] \leqslant (\sigma+q)^2/2^{n+1} \tag{36}$$

其中, $\mathcal{A}$ 的 $q$ 次询问中消息分组总数是 $\sigma$, 故 XBC 模式对底层算法进行了 $\sigma+q$ 次调用。

$Game_7$ V.S. $Game_8$

这两个游戏的区别在于: $Game_7$ 中 XBC 模式调用了随机函数 $\rho$ (见第 7.10、7.12 行), 一旦 $\rho$ 的输入值产生碰撞, 其输出值也必然产生碰撞, 要么敌手可预测 $\Delta$ 值(见第 7.10 行), 要么敌手观察到输出的密文分组产生碰撞(见第 7.12 行); 而 $Game_8$ 中任意密文输出都是完全独立随机比特串。

为了便于说明, 我们引入几个记法: 用 $cnt$ 表示 $Game_7$ 中当前对 $\rho$ 进行调用的次数, 则 $cnt$ 是 $1,\cdots,\sigma+q$ 的有序列。用 $Dom(\rho)$ 表示 $Game_7$ 中 $\rho$ 在第 $cnt$ 次调用前所有的输入值的集合, 则有 $Dom(\rho)=\{N^v\}_v \cup \{M_u^v \oplus \Sigma_u^v \oplus \Delta_u^v\}_{(v,u)}$, 其 $\Sigma_u^v$、$\Delta_u^v$ 表示计算 $XBC[\rho]^{j,i}(N^j, M_i^j)$ 时 $\Sigma^v$、$\Delta^v$ 的取值, 且 $(v,u)$ 满足 $v\in\{1,\cdots,q\}$, $u\in\{1,\cdots,l_v\}$。现用 $ccol(cnt)$ 表示第 $cnt$ 次调用时 $\rho$ 输入值首次出现碰撞的事件, 即 $|Dom(\rho)|=cnt-1$, 且在第 $cnt$ 次调用时 $\rho$ 输入值与 $Dom(\rho)$ 中的元素发生碰撞, 则

(I) 若 $\rho$ 的输入值是 Nonce 值, 则有 $\Pr[ccol(cnt)] \leqslant |Dom(\rho)|/2^n$;

(II) 若 $\rho$ 的输入值是 $M_i^j \oplus \Sigma^j \oplus \Delta^j$, 同样有 $\Pr[ccol(cnt)] \leqslant |Dom(\rho)|/2^n$。

综合(I) (II)两种情况, 有下式

$$\Pr[ccol(cnt)] \leqslant |Dom(\rho)|/2^n = (cnt-1)/2^n \text{。} \tag{37}$$

其中(II)的结果不是很直接, 根据 $Dom(\rho)$ 中元素的来源, $ccol(cnt)$ 可分成如 $E1$、$E2$ 两种情况, 其定义分别如下:

$$E1 \overset{def}{=} \{\exists N^s = M_i^j \oplus \Sigma^j \oplus \Delta^j \mid N^s \in \{N^v\}_v\};$$

$$E2 \overset{def}{=} \{\exists M_w^s \oplus \Sigma_w^s \oplus \Delta_w^s = M_i^j \oplus \Sigma^j \oplus \Delta^j \mid M_w^s \oplus \Sigma_w^s \oplus \Delta_w^s \in \{M_u^v \oplus \Sigma_u^v \oplus \Delta_u^v\}_{(v,u)}\}$$

易知, $\Pr[E1] \leqslant |\{N^v\}_v|/2^n$。

由表 14 中伪代码可知, $M_w^s \oplus \Sigma_w^s \oplus \Delta_w^s$、$M_i^j \oplus \Sigma^j \oplus \Delta^j$ 表达式分别如下:

$$M_w^s \oplus \Sigma_w^s \oplus \Delta_w^s = M_w^s \oplus N^s \oplus \left(\oplus_{r=1}^{w-1} \rho(M_r^s \oplus \Sigma_r^s \oplus \Delta_r^s)\right) \oplus 2^w \cdot \rho(N^s) \tag{38}$$

$$M_i^j \oplus \Sigma^j \oplus \Delta^j = M_i^j \oplus N^j \oplus \left(\oplus_{r=1}^{i-1} \rho(M_r^j \oplus \Sigma_r^j \oplus \Delta_r^j)\right) \oplus 2^i \cdot \rho(N^j) \tag{39}$$

若 $s \neq j$, 即碰撞发生在并发的不同询问的消息分组之间, 则有 $N^s \neq N^j$ 由式子(38)(39)可知, $N^s$、$N^j$ 分别经过随机函数 $\rho$ 的映射, 故 $\Pr[M_w^s \oplus \Sigma_w^s \oplus \Delta_w^s = M_i^j \oplus \Sigma^j \oplus \Delta^j] = 2^{-n}$。

若 $s=j$ 则碰撞发生在同一个询问的不同消息分组之间, 而同一个询问间消息分组是有序的, 故 $w<i$, $N^s=N^j$, $M_r^s \oplus \Sigma_r^s \oplus \Delta_r^s = M_r^j \oplus \Sigma_r^j \oplus \Delta_r^j$, $s,j \in \{1,\cdots,w-1\}$。则将式子 (38)(39) 代入 $M_w^s \oplus \Sigma_w^s \oplus \Delta_w^s = M_i^j \oplus \Sigma^j \oplus \Delta^j$ 可简化得下式

$$M_i^j \oplus M_w^s \oplus \left(\oplus_{r=w}^{i-1} \rho(M_r^j \oplus \Sigma_r^j \oplus \Delta_r^j)\right) = 2^w \cdot \rho(N^s) \oplus 2^i \cdot \rho(N^j) \tag{40}$$

由随机函数 $\rho$ 的性质可知(40)成立的概率为 $2^{-n}$, 即 $\Pr[M_w^s \oplus \Sigma_w^s \oplus \Delta_w^s = M_i^j \oplus \Sigma^j \oplus \Delta^j] = 2^{-n}$ 同样成立。

由上讨论, 得:

$$\forall M_w^s \oplus \Sigma_w^s \oplus \Delta_w^s \in \{M_u^v \oplus \Sigma_u^v \oplus \Delta_u^v\}_{(v,u)},$$

$$\Pr[M_w^s \oplus \Sigma_w^s \oplus \Delta_w^s = M_i^j \oplus \Sigma^j \oplus \Delta^j] = 2^{-n}$$

故当 $\rho$ 的输入值是 $M_i^j \oplus \Sigma^j \oplus \Delta^j$ 时, $\Pr[ccol(cnt)] = \Pr[E1] + \Pr[E2] \leqslant |Dom(\rho)|/2^n$, 即(II)成立。

接下来, 我们将 $BAD_2$ 定义为 $Game_7$ 中随机函数 $\rho$ 的输入值出现碰撞, 则由(37)得

$$\Pr[BAD_2] \tag{41}$$
$$\leqslant \sum_{cnt=1}^{\sigma+q} \Pr[ccol(cnt)]$$
$$\leqslant \sum_{cnt=1}^{\sigma+q} (cnt-1)/2^n \leqslant (\sigma+q)^2/2^{n+1}$$

其中, $\mathcal{A}$ 的中消息分组总数是 $\sigma$, 故 XBC 模式对底层算法进行了 $\sigma+q$ 次调用。

易知, 当 $BAD_2$ 事件发生, 在 $Game_7$ 中, 要么 $\Delta$ 可被敌手预测, 要么出现密文分组碰撞; 而在 $Game_8$ 中, 任意两个密文分组都是完全随机的比特串。明显的当 $BAD_2$ 事件发生, 在这两个游戏中敌手 $\mathcal{A}$ 经过 $q$ 次询问获得的信息不一致。反之, 当 $BAD_2$ 事件没有发生, 在这两个游戏中敌手 $\mathcal{A}$ 在 $q$ 次询问获得的返回值都是随机比特串, 则 $\mathcal{A}$ 的表现是一致的, 即

$$\Pr\left[ Game_7 = 1 \middle| \overline{BAD_2} \right] \tag{42}$$
$$= \Pr\left[ Game_8 = 1 \middle| \overline{BAD_2} \right]$$

故由(41)(42)可得, 对任意 CBW-CPA 敌手 $\mathcal{A}$

$$\Pr[Game_7 = 1] - \Pr[Game_8 = 1] \tag{43}$$
$$\leqslant \left| \Pr[Game_7 = 1 | \overline{BAD_2}] - \Pr[Game_8 = 1 | \overline{BAD_2}] \right| \cdot \Pr[\overline{BAD_2}]$$
$$+ \left| \Pr[Game_7 = 1 | BAD_2] - \Pr[Game_8 = 1 | BAD_2] \right| \cdot \Pr[BAD_2]$$
$$\leqslant \Pr[BAD_2] \leqslant (\sigma+q)^2/2^{n+1}$$

结论

综上所述, 由 (32)(35)(36)(43) 得, 对任意 CBW-CPA 敌手 $\mathcal{A}$,

$$\boldsymbol{Dist}_{XBC[E]^{j,i}}^{XII^{j,i}}(\mathcal{A}(q,t))$$
$$= \left| \Pr[Game_5 = 1] - \Pr[Game_8 = 1] \right|$$
$$\leqslant \left| \Pr[Game_5 = 1] - \Pr[Game_6 = 1] \right|$$
$$+ \left| \Pr[Game_6 = 1] - \Pr[Game_7 = 1] \right|$$
$$+ \left| \Pr[Game_7 = 1] - \Pr[Game_8 = 1] \right|$$
$$\leqslant \boldsymbol{Adv}_E^{prp-cpa}(\sigma+q, t') + (\sigma+q)^2/2^n$$

由(28)得,

$$\boldsymbol{Adv}_{XBC[E]}^{roi-ind-cbw-cpa}(q,t) \tag{44}$$
$$\leqslant \boldsymbol{Adv}_E^{prp-cpa}(\sigma+q, t') + (\sigma+q)^2/2^n$$

至此, 定理 2 的证明结束。

## 6 结束语

本文首次对国家标准 GB/T 17964-2008[2]中额外增加的 BC 模式进行了分析, 包括了理论和具体应用的安全性分析。由表 6 的分析结果可知, BC 模式的机密性完全依赖于 IV 值的随机性, 且不能抵抗逐分组攻击。因此, 使用 BC 模式时需注意: (1) 确保 IV 值是完全随机生成的, 否则 BC 模式的机密性将受到损害; (2) BC 模式不能用于在线消息处理的应用场景, 如实时系统、资源受限密码设备等; (3) 若在线应用中需要使用加密模式, 可采用本文提出的抗逐分组攻击的改进方案——基于 Nonce 的 XBC 模式, 其运算效率与 BC 模式十分接近, 每次加解密时增加了一次分组密码的调用和少量简单的有限域运算。

本文在分析 BC 模式、XBC 模式时均假设了其明文消息是分组大小的整数倍, 而实际应用中处理的明文消息是任意长度的, 因此 BC 模式、XBC 模式的应用还需解决这一矛盾。一般而言, 这一矛盾可采用适当的填充规则(padding rules)进行解决, 如标准文档 ISO/IEC 9797-1[26]的“10”填充方法(padding method #2)、消息长度填充方法(padding method #3), PKCS #7[27]的填充字节长度填充方法, 等等。

为了能正确地恢复出明文消息, 这些填充规则必须满足单射的性质。具体地说, 假设填充规则 $pad(\cdot):\{0,1\}^* \to (\{0,1\}^n)^+$, 对任意长度的明文消息 $M$ 填充后, 得到填充消息 $M'=pad(M)$, $M'$ 的长度为分组大小的整数倍。则采用填充规则 $pad(\cdot)$ 后, BC 模式、XBC 模式对填充消息 $M'$ 进行加解密运算, 为了正确地恢复出消息 $M$, $pad(\cdot)$ 必须具有单射性。

本文的分析假设了明文消息的长度是分组大小的整数倍, 则 CPA 敌手可选择的明文消息空间为 $(\{0,1\}^n)^+$。当 BC 模式、XBC 模式采用了适当的填充规则后, CPA 敌手可选择的明文消息空间仅为 $(\{0,1\}^n)^+$ 的子集, 比如若采用“10”填充方法[26] (padding method #2), 则 CPA 敌手是无法通过选择某个 $M$ 使得填充后 $M'$ 为全 0。也即采用填充规则后, CPA 敌手选择明文消息的能力降低了。故对于任意明文消息的处理, 采用适当的填充规则, 定理 1、定理 2 结论同样成立。

遗憾的是, 填充处理不当将导致工作模式出现安全问题。例如, 和 CBC 模式一样, BC 模式和 XBC 模式都不能抵抗利用“解密后填充是否正确”这一信息的攻击, 即填充预言(Padding Oracle)攻击[28-30]。这是由 BC 模式、XBC 模式固有的反馈方式决定的, 目前还没有办法克服这种攻击。因此在使用 BC 模式或 XBC 模式时, 应该避免泄露解密后消息填充是否正确这一信息。

另外, 大多数基于分组密码的加密模式都不能抵抗选择密文攻击, 包括 ECB、CBC、CFB、OFB、CTR 等。BC 模式和 XBC 模式也无法抵抗选择密文攻击。

## 参考文献


[1] Wu W L and Feng D G, “The State-of-The-Art of Research on Block Cipher Mode of Operation,” *Chinese Journal of Computers*, vol. 29, no. 1, pp. 21-36, 2006.
(吴文玲, 冯登国, “分组密码工作模式的研究现状”, *计算机学报*, 2006, 29(1): 21-36。)

[2] GB/T 17964-2008. 信息安全技术分组密码的工作模式, 2008.

[3] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, “A concrete security treatment of symmetric encryption”, in *Proc. IEEE 38th Annual Symposium on Foundations of Computer Science(FOCS 1997)* , pp. 394-403, 1997.

[4] J. Sung, S. Lee, J. Lim, and O. Yi, “Concrete security analysis of CTR-OFB and CTR-CFB modes of operation” in *Proc. Information Security and Cryptology(ICISC 2001)*, pp. 103-113, 2001.

[5] A. Alkassar, A. Geraldy, B. Pfitzmann, and A. R. Sadeghi, “Optimized self-synchronizing mode of operation”, in *Proc. Fast Software Encryption(FSE’01)*, pp. 78-91, 2001.

[6] S. Goldwasser and S. Micali, “Probabilistic encryption,” *Journal of computer and system sciences*, vol. 28, no. 2, pp. 270-299, Apr. 1984.

[7] T. Duong and J. Rizzo, “Here come the XOR Ninjas,” *White paper, Netifera*, 2011.

[8] K. Paterson, “Authenticated Encryption in TLS”, Invited talk, In *Proc. Directions in Authenticated Ciphers(DIAC 2013)*, 2013.

[9] G V. Bard, “The Vulnerability of SSL to Chosen Plaintext Attack,” *IACR Cryptology ePrint Archive*, 2004, 2004: 111.

[10] W. Dai, “An attack against SSH2 protocol,” *Email to the SECSH Working Group ietf-ssh@ netbsd. org ftp://ftp. ietf. org/ietf-mail-archive/secsh/2002-02*. mail, 2002.

[11] B. Moeller, “Security of CBC ciphersuites in SSL/TLS: Problems and countermeasures,” *Unpublished manuscript*, May, 2004.

[12] P. Rogaway, “Problems with proposed IP cryptography,” *Unpublished paper*, http://www. cs. ucdavis. edu/rogaway/papers/draftrogaway-ipsec-comments-00. txt, 1996.

[13] P. Rogaway, “Evaluation of some blockcipher modes of operation,” *Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan*, 2011.

[14] International organization for standardization and international electrotechnical commission. ISO/IEC 10116:2006. Information technology - Security techniques - Modes of operation for an *n*-bit block cipher. International Standard, 2006.

[15] M. Dworkin, NIST Special Publication 800-38A. Recommendation for block cipher modes of operation: Modes and techniques, Dec. 2001.

[16] P. Rogaway, “Nonce-based symmetric encryption,” In *Proc. Fast Software Encryption(FSE’04)*, pp. 348-358, 2004.

[17] P. A. Fouque, G. Martinet and G. Poupard, “Practical symmetric on-line encryption,” In *Proc. Fast Software Encryption(FSE’03)*, pp. 362-375, 2003.

[18] P. A. Fouque, A. Joux and G. Poupard, “Blockwise adversarial model for on-line ciphers and symmetric encryption schemes,” In *Proc. Selected Areas in Cryptography(SAC’04)*, pp. 212-226, 2004.

[19] A. Joux, G. Martinet and F. Valette, “Blockwise-Adaptive Attackers Revisiting the (in) security of some provably secure Encryption Modes: CBC, GEM, IACBC,” In *Proc. Cryptology(CRYPTO 2002)*, pp. 17-30, 2002.

[20] G. V. Bard, “A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL,” In Proc. *SECRYPT 2006*, pp. 99-109, 2006.

[21] R. Pass and A. Shelat, “A Course in Cryptography,” 2010.

[22] M. Bellare, J. Kilian and P. Rogaway, “The security of cipher block chaining,” In *Proc. Cryptology(CRYPTO’94)*, pp. 341-358, 1994.

[23] M. Bellare and P. Rogaway, “The security of triple encryption and a framework for code-based game-playing proofs,” In *Proc. Cryptology-EUROCRYPT 2006(eurocrypt2006)*, pp. 409-426, 2006.

[24] V. Shoup, “Sequences of games: a tool for taming complexity in security proofs,” http://eprint.iacr.org/2004/332, 2004.

[25] P. Rogaway, “Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC,” In *Proc. Cryptology-ASIACRYPT 2004(AsiaCrypt2004)*, pp. 16-31, 2004.

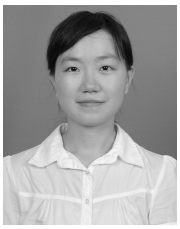
[26] International organization for standardization and international electrotechnical commission. ISO/IEC 9797-1:2011, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher. International Standard, 2011.

[27] RSA Laboratories. PKCS #7 Cryptographic Message Syntax Standard: ASCII, MS-Word, PostScript and Gzip PostScript. Version 1.5.

[28] S. Vaudenay, “Security Flaws Induced by CBC Padding— Applications to SSL, IPSEC, WTLS..,” In *Proc. Cryptology—EUROCRYPT 2002*, pp. 534-545, 2002.

[29] K. G. Paterson and A.Yau, “Padding oracle attacks on the ISO CBC mode encryption standard”, (Topics) In *Proc. Cryptology–CT-RSA 2004*, pp. 305-323, 2004.

[30] A. K. L. Yau, K. G. Paterson and C. J. Mitchell, “Padding oracle attacks on CBC-mode encryption with secret and random IVs” In *Proc. Fast Software Encryption 2005(FSE’2005)*, pp. 299-319, 2005.



**郑凯燕** 于 2010 年在中山大学信息安全专业获得学士学位。现在中国科学院大学信息工程研究所信息安全专业攻读博士学位。研究领域为密码学。研究兴趣包括: 加密方案、哈希函数。Email: zhengkaiyan@ iie.ac.cn

**王鹏** 于 2005 年在中国科学院院研究生院通信与信息系统专业获得博士学位。现任中国科学院院信息工程研究所副研究员。研究领域为密码学。研究兴趣包括: 分组密码工作模式、认证加密方案等。Email: wp@is.ac.cn