中国科学: 信息科学 2016 年 第 46 卷 第 6 期: 729–742
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
论 文

OFBNLF 加密工作模式的分析

孙哲蕾[①②③], 王鹏[①③*]

① 中国科学院信息工程研究所, 北京 100093
② 中国科学院大学, 北京 100049
③ 中国科学院数据与通信保护教育中心, 北京 100093
* 通信作者. E-mail: wp@is.ac.cn

收稿日期: 2015–10–15; 接受日期: 2015–11–18; 网络出版日期: 2016–05–27
国家自然科学基金 (批准号: 61272477, 61472415)、国家重点基础研究发展 (973) 计划 (批准号: 2014CB340603) 和中国科学院战略性先导科技专项 (批准号: XDA06010702) 资助项目

摘要 OFBNLF(output feedback with a nonlinear function) 模式是我国分组密码工作模式的国家标准之一, 选择明文攻击不可区分 (IND-CPA) 模型则是用来评判分组密码工作模式的重要安全指标. 迄今为止, 还没有文献对 OFBNLF 模式的安全性进行分析或证明, 也没有文献对其软件实现进行评估. 本文对 OFBNLF 模式的安全性分析进行了研究, 在给出 OFBNLF 模式的在线加密描述的基础上, 采用做游戏 (game-playing) 的技术, 第一次证明了 OFBNLF 模式在逐分组选择明文攻击不可区分 (BW-IND-CPA) 模型下的安全性. 鉴于之前对 BW-IND-CPA 模型的形式定义并没有对一般的加密模式进行在线的形式化处理, 本文在给出在线加密形式定义的基础上, 重新对 BW-IND-CPA 模型进行了定义. 同时还对 OFBNLF 软件实现效率做了评估, 并与国家标准中其他的加密模式在安全性和软件实现效率方面分别进行了对比.

关键词 分组密码工作模式 OFBNLF 安全性分析 逐分组选择明文攻击 性能

1 引言

分组密码作为密码系统的基本部件, 一般通过特定的工作模式 (mode of operation, 以下亦简称模式) 才能实现机密性、完整性等安全功能. 例如, 实现机密性的加密模式, 实现完整性的认证模式, 以及同时实现这两种功能的认证加密模式. 由于其广泛的应用, 各类分组密码工作模式陆续被各国或者国际标准化组织标准化, 其中包括 NIST, ISO (ISO/IEC 10116), IEEE, IETF 等. 就加密模式而言, NIST (美国技术标准局) [1] 早在 DES 算法时期就标准化了 4 种分组密码工作模式: 电码本模式 (electronic codebook, ECB), 密码分组链接模式 (cipher block chaining, CBC), 密码反馈模式 (cipher feedback, CFB) 和输出反馈模式 (output feedback, OFB). 之后随着 AES 算法征集的完成, 越来越多的工作模式被标准化. 2001 年发布的加密模式标准文档 SP-800-38A 中, 在原有 ECB, CBC, CFB, OFB 等模式的基础上, 增加了计数器模式 (counter, CTR). 之后又在 SP-800-38F 文档中标准化了用于磁盘扇区加密的 XTS-AES 模式. ISO, IEEE, IETF 等定义的有关工作模式的标准基本上和 NIST 的标准相似.

引用格式: 孙哲蕾, 王鹏. OFBNLF 加密工作模式的分析. 中国科学: 信息科学, 2016, 46: 729–742, doi: 10.1360/N112015-00163

© 2016《中国科学》杂志社

和现行 NIST, ISO 等标准不同的是, 2008 年我国新颁布的分组密码加密工作模式国家标准 GB/T 17964-2008 [2] 中, 额外又增加了分组链接模式 (block chaining, BC) 和带非线性函数的输出反馈模式 (output feedback with a nonlinear function, OFBNLF) 两种工作模式. OFBNLF 加密模式处理一个分组的消息需要调用两次分组密码, 而其他工作模式只需要调用一次分组密码, 这种方式在影响软件实现效率的同时也增加了安全性分析及证明的难度. 分组密码工作模式安全性证明的研究始于 Bellare 等, 核心思想是在假设底层分组密码是伪随机置换 (pseudorandom permutation, PRP) 的基础上, 在一定的安全模型中, 证明工作模式的安全性. 伪随机置换, 即与随机置换不可区分的置换, 已经成为工作模式研究领域的常用假设. 安全模型刻画了敌手的攻击能力, 例如选择明文攻击, 或者选择密文攻击; 具体的证明则用到了归约的思想, 即论证如果存在对工作模式的攻击, 也一定存在对底层分组密码伪随机性的攻击, 从而反证出工作模式的安全性. 文献 [3] 给出了 CBC, CTR 等工作模式的证明, CFB, OFB 等模式的证明在其他文献中也曾经出现过 [4].

OFBNLF 模式最早出现在文献 [5] 中, 之后文献 [6∼8] 等也涉及一些对 OFBNLF 模式的讨论, 但是迄今为止, 还没有文献对 OFBNLF 模式的安全性进行分析或证明, 也没有文献对其软件实现进行评估.

本文首次对 OFBNLF 模式进行了系统的安全性分析和软件实现效率评估, 具体如下:

(1) 在逐分组选择明文攻击不可区分 (BW-IND-CPA) 模型 [9] 下证明了 OFBNLF 模式的安全性. 在传统的选择明文攻击不可区分 (IND-CPA) 模型中, 敌手在询问加密算法时, 消息只能作为一个整体进行询问, 然后得到相应的整体密文; 在 BW-IND-CPA 模型中, 敌手可以进行逐分组询问, 然后得到相应的密文分组, 当前明文分组的选取可以基于之前的问答. 本文在 BW-IND-CPA 模型下对 OFBNLF 模式进行了分析, 我们证明, 当初始向量不重复时, 逐分组地选择明文对 OFBNLF 模式进行询问, 其结果和得到相同长度的随机比特串的情况无法区分, 即在逐分组选择明文的攻击方式下, 敌手得不到明文的任何信息, 保证了在 BW-IND-CPA 模型下 OFBNLF 模式的机密性.

(2) 在 BW-IND-CPA 模型下的证明使用了做游戏 (game-playing) [10] 的技术. 做游戏的技术对于分散证明的难点以及写出清晰、可读性强的证明很有帮助, 是目前进行安全性证明普遍采用的方法. 之前对 BW-IND-CPA 模型的形式定义 [11], 并没有对一般的加密模式进行在线的形式化处理, 因此早期对一些模式例如 DCBC [11] 的 BW-IND-CPA 证明难以采用做游戏的技术, 导致了这些证明和传统的 IND-CPA 模型下的证明没有太大区别, 没有从证明中反映出逐分组攻击的特点. 我们在给出在线加密形式定义的基础上, 重新对 BW-IND-CPA 模型进行了定义. 这一处理方式使得对 OFBNLF 模式的证明很容易采用做游戏的技术.

(3) 将 OFBNLF 模式的安全性和软件实现与我国国家标准中其他的加密模式进行对比研究. 与 ECB, CBC, CTR, CFB, OFB 和 BC 等加密模式相比, OFBNLF 模式无论是在 IND-CPA 模型下还是在 BW-IND-CPA 模型下都是安全的. 在软件实现性能方面, 我们分别测试了这几种加密模式在 AES 算法和 SM4 算法下的软件实现效率. 实验数据表明不论是以 AES 作为底层分组密码, 还是以 SM4 作为底层分组密码, 模式 OFBNLF 的软件实现性能都不是十分理想.

2 预备知识

2.1 基本符号

$\{0,1\}^n$ 表示长度为 n 的所有比特串的集合. $\{0,1\}^*$ 表示所有比特串的集合. $A \leftarrow B$ 表示将 B 赋

值给 A. $\mathcal{X}$ 是一个集合, $x \xleftarrow{\$} \mathcal{X}$ 表示从集合 $\mathcal{X}$ 中随机选取一个值并赋予 x. $\mathrm{Perm}(n)$ 表示 $\{0,1\}^n$ 上所有置换的集合. $\mathrm{Func}(n)$ 表示 $\{0,1\}^n$ 上所有函数的集合. $|A|$ 表示比特串 A 的比特长度. $\mathcal{A}^{\mathcal{O}} = 1$ 表示敌手 $\mathcal{A}$ 在攻击过程中询问谕言 $\mathcal{O}$ 后输出比特 1.

2.2 初始向量

加密模式一般是带状态的或者随机的 [12], 通常都有一个初始向量 IV (initial vector) [13]. IV 通常无需保密, 随密文一起发送给接收者. IV 可以是由算法生成的随机数; 也可以是由使用者自行选择的不可重复的值 (nonce [1)]). 当 IV 作为 nonce 使用时, 使用者承担了算法随机化的责任, 即每次都必须选取不同的 IV, IV 的重复会破坏模式的安全性. Rogaway 等学者建议在定义安全模型时, 敌手选择不重复的 IV, 即所谓的基于 nonce 的安全性 [14]. NIST 等标准文档中专门讨论了有关生成 IV 的方式, 一般包含作为 nonce 和随机数两种方法.

2.3 加密模式

加密模式一般可表示为三元组 $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. $\mathcal{K}$ 表示密钥的集合; $\mathcal{E}$ 和 $\mathcal{D}$ 分别表示 $\mathcal{SE}$ 的加密过程和解密过程. 对于基于初始向量 IV 的模式 [2)], 加密过程 $\mathcal{E}$ 以密钥 $K \in \mathcal{K}$, IV 和明文 $M \in \{0,1\}^*$ 为输入, 输出密文 C, 记为 $C \leftarrow \mathcal{E}_K(IV, M)$; 解密过程 $\mathcal{D}$ 以密钥 $K \in \mathcal{K}$, IV 和密文 $C \in \{0,1\}^*$ 为输入, 输出明文 M, 记为 $M \leftarrow \mathcal{D}_K(IV, C)$. 我们要求 $M = \mathcal{D}_K(IV, \mathcal{E}_K(IV, C))$.

2.4 可忽略函数 [15]

对于函数 $f : \mathbb{N} \to \mathbb{R}$, 如果对于任意的常数 $a \geqslant 0$, 存在整数 b, 使得当 $x \geqslant b$ 时,

$$f(x) < \frac{1}{x^a},$$

称函数 f 是可忽略的.

2.5 伪随机置换/伪随机函数

如果敌手无法将一个分组密码 ($E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, 密钥随机选取) 和一个随机置换 ($\pi \xleftarrow{\$} \mathrm{Perm}(n)$) 区分开, 称这个分组密码是一个伪随机置换 (PRP, pseudorandom permutation) [16, 17]. 具体地, 假设敌手 $\mathcal{A}$ 能够询问分组密码 E_K ($K \xleftarrow{\$} \{0,1\}^k$) 或随机置换 $\pi \xleftarrow{\$} \mathrm{Perm}(n)$, 并得到相应的输出. $\mathcal{A}$ 区分分组密码 E_K 和 π 的优势定义为

$$\mathrm{Adv}^{\mathrm{prp}}_E(\mathcal{A}) = |\Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{E_K(\cdot)} = 1] - \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n) : \mathcal{A}^{\pi(\cdot)} = 1]|. \tag{1}$$

对于时间复杂度 t, 询问次数 q, 定义攻击 E 的优势为

$$\mathrm{Adv}^{\mathrm{prp}}_E(t, q) = \max\{\mathrm{Adv}^{\mathrm{prp}}_E(\mathcal{A})\}.$$

$\mathrm{Adv}^{\mathrm{prp}}_E(t, q)$ 一般可以表示为分组长度 n 的函数. 当 $\mathrm{Adv}^{\mathrm{prp}}_E(t, q)$ 可忽略时, 称 E 是一个伪随机置换. 类似地, 将上述定义中的 π 替换为随机函数 $\rho \xleftarrow{\$} \mathrm{Func}(n)$, 即给出伪随机函数 (PRF, pseudorandom function) 的定义. 随机置换和随机函数是不可区分的, 在证明过程中经常将随机置换替换为随机函数, 以下是 PRP-PRF 切换引理.

1) nonce 一词一般意味不重复的值.

2) 本文之后的讨论中, 敌手可以选择不能重复的 IV.

引理1 (PRP-PRF 切换引理 [16,18]) 敌手 $\mathcal{A}$ 在询问时间为 t, 询问次数为 q 时, 区分随机函数 $\rho \xleftarrow{\$} \mathrm{Func}(n)$ 和随机置换 $\pi \xleftarrow{\$} \mathrm{Perm}(n)$ 的优势满足

$$|\Pr[\mathcal{A}^{\rho}=1]-\Pr[\mathcal{A}^{\pi}=1]| \leqslant \frac{q(q-1)}{2^{n+1}}. \tag{2}$$

2.6 IND-CPA 模型

在分析工作模式的安全性时, 需要建立相应的安全模型, 其中的三个要素为安全目标、敌手能力和安全指标. 安全目标反映了一个工作模式需要完成的安全功能, 对于加密模式来说, 指的是机密性, 也就是敌手不能获得明文任意比特的信息 [12]. 敌手能力一般分为选择明文攻击 (CPA) 和选择密文攻击 (CCA) 等, 本文采用的是选择明文攻击. 安全指标给出了敌手攻击是否成功的具体度量. 我们经常使用不可区分性 (IND) [3] 给出安全指标的具体定义. 例如在 IND-CPA 安全模型中, 我们将安全指标定义为敌手区分真实的加密模式和理想的加密模式的优势. 在真实的加密模式下, 谕言 (oracle) 是模式的加密过程 $\mathcal{E}_K$ ($K \xleftarrow{\$} \mathcal{K}$); 在理想的加密模式下, 谕言是随机串输出函数 \$. 为了区分真实的加密模式和理想的加密模式, 敌手 $\mathcal{A}$ 选择 IV, 明文 $M \in \{0,1\}^*$, 提交谕言, 此处明文串作为整体提交谕言, 然后得到应答. 在真实的加密模式下, 谕言输出密文 $C \leftarrow \mathcal{E}_K(IV, M)$; 在理想的加密模式下, 谕言输出与在真实加密模式下加密得到的密文等长的随机串. 敌手 $\mathcal{A}$ 区分真实的加密模式与理想的加密模式的优势定义为

$$\mathrm{Adv}_{\mathcal{E}}^{\mathrm{ind-cpa}}(\mathcal{A}) = |\Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\mathcal{E}_K(\cdot,\cdot)}=1] - \Pr[\mathcal{A}^{\$(\cdot,\cdot)}=1]|, \tag{3}$$

其中, 对于时间复杂度 t, 询问次数 q, 询问的消息的总的分组长度 μ, 定义攻击 $\mathcal{E}$ 的优势为

$$\mathrm{Adv}_{\mathcal{E}}^{\mathrm{ind-cpa}}(t,q,\mu) = \max\{\mathrm{Adv}_{\mathcal{E}}^{\mathrm{ind-cpa}}(\mathcal{A})\}.$$

2.7 BW-IND-CPA 模型

在一些实际应用中, 密码设备的存储空间是有限的, 在加密过程中无法做到在处理完所有明文分组后, 再整体输出相应的密文. 在线加密 (online encryption) [9,19~23] 是解决这一问题的有效方法. 在线加密模式将消息进行分组, 然后依次对消息分组进行处理, 每处理一个明文分组, 就输出相应的密文分组. 常见的分组密码加密模式, 例如 CBC, OFB, CFB 等, 都可以用在线加密的方式实现.

然而, 在线加密使得敌手可以逐分组地获得密文信息, 因而导致了新的攻击 —— 逐分组选择明文攻击 [9]. 相应的安全模型可以定义为逐分组选择明文攻击下的不可区分性 (BW-IND-CPA). 这种安全模型与 IND-CPA 大体相同, 但是敌手拥有了更多的能力. 敌手在询问的时候并不是将明文串作为整体一次性地交予谕言, 而是可以在得到当前密文分组后再选择下次提交的明文分组, 因此敌手具有更强的适应性攻击的能力. 文献 [9] 利用这种方式破坏了 CBC, GEM 和 IACBC 等模式在 BW-IND-CPA 模型下的安全. 例如在 CBC 模式中, 敌手在已知 $C[0]=IV$ 的情况下, 询问 $M[1]$ 并实时得到 $C[1]$, 敌手接着询问 $M[2]=C[1]\oplus C[0]\oplus M[1]$, 必将得到 $C[2]=C[1]$, 敌手可以通过这种方式成功将 CBC 模式与随机串区分. 之后在 2003 年, Pierre-Alain Fouque 等 [11] 对 CBC 模式进行修改得到模式 DCBC, 并且证明了这种模式与 CFB 模式在逐分组选择明文攻击下的安全性.

逐分组的攻击方式与加密模式的在线实现方式是紧密相关的. 之前的有关 BW-IND-CPA 模型下安全性都是在传统的加密形式下定义的, 以下先给出在线加密模式的形式定义, 在此基础上自然得到了 BW-IND-CPA 模型的定义. 将在线加密模式 $\mathcal{E}$ 看成两个算法: $\mathcal{E}=(\mathcal{E}_K^{\mathrm{int}}, \mathcal{E}_K^{\mathrm{next}})$. $\mathcal{E}_K^{\mathrm{int}}$ 处理初始向量 IV, 更新内部状态 S, 用 $S \leftarrow I_K(IV)$ 表示, 此过程不输出任何值; $\mathcal{E}_K^{\mathrm{next}}$ 利用当前内部状态 S 处理明

文分组 M, 更新内部状态 S, 得到相应的密文分组 C, 用 $(S', C) \leftarrow N_K(S, M), S \leftarrow S'$ 表示, 同时输出密文 C. 常见工作模式 CBC, OFB, CFB 等的在线加密方式都可以写成这种形式. OFBNLF 模式的在线加密描述见算法 1.

算法 1 OFBNLF 模式的在线加密描述

procedure $\mathcal{E}_K^{\text{OFBNLF}} = (\mathcal{E}_K^{\text{int}}, \mathcal{E}_K^{\text{next}})$
$\mathcal{E}_K^{\text{int}}$ (IV)
    $S \leftarrow E_K(IV)$
$\mathcal{E}_K^{\text{next}}$ (M)
    $C \leftarrow E_S(M)$
    $S \leftarrow E_K(S)$
    return C
end procedure

在在线加密形式定义的基础上, 可以直接定义 BW-IND-CPA 模型下的安全性. 采用常用的方法, 先将在线加密模式理想化, 然后将安全指标定义为敌手区分两种情况的优势. 将 $(\mathcal{E}_K^{\text{int}}, \mathcal{E}_K^{\text{next}})$ 理想化为 $(\$^{\text{int}}, \$^{\text{next}})$, 其中 $\$^{\text{int}}$ 不返回任意值, $\$^{\text{next}}$ 返回一个分组长度的随机值. 在线加密真实和理想情况具体描述见算法 2. 敌手 $\mathcal{A}$ 的优势定义为

$$\text{Adv}_{\mathcal{E}}^{\text{bw-ind-cpa}}(\mathcal{A}) = |\Pr[\mathcal{A}^{\mathcal{E}_K^{\text{int}}(\cdot), \mathcal{E}_K^{\text{next}}(\cdot)} = 1] - \Pr[\mathcal{A}^{\$^{\text{int}}(\cdot), \$^{\text{next}}(\cdot)} = 1]|. \tag{4}$$

对于时间复杂度 t, 询问次数 q, 询问的消息的总的分组长度 μ, 定义攻击 $\mathcal{E}$ 的优势为

$$\text{Adv}_{\mathcal{E}}^{\text{bw-ind-cpa}}(t, q, \mu) = \max\{\text{Adv}_{\mathcal{E}}^{\text{bw-ind-cpa}}(\mathcal{A})\}.$$

算法 2 在线加密真实与理想情况

真实情况 $\mathcal{SE} = (\mathcal{E}_K^{\text{int}}, \mathcal{E}_K^{\text{next}})$	**理想情况** $\mathcal{SE} = (\$^{\text{int}}, \$^{\text{next}})$
$\mathcal{E}_K^{\text{int}}(IV)$	$\$^{\text{int}}(IV)$
$S \leftarrow I_K(IV)$	
$\mathcal{E}_K^{\text{next}}(M)$	$\$^{\text{next}}(M)$
$(S', C) \leftarrow N_K(S, M)$	$C \xleftarrow{\$} \{0,1\}^n$
$S \leftarrow S'$	
return C	**return** C

3 OFBNLF 加密模式的安全性

OFBNLF 模式结合了 OFB 模式和 ECB 模式, 上层采用 OFB 模式, 使用主密钥生成一系列所需的子密钥; 下层类似于 ECB 模式, 利用子密钥进行分组密码加密. OFBNLF 模式分为加密和解密两个过程: $C \leftarrow \mathcal{E}_K^{\text{OFBNLF}}(IV, M)$ 和 $M \leftarrow \mathcal{D}_K^{\text{OFBNLF}}(IV, C)$.

假设底层采用分组密码: $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$. OFBNLF 模式的初始向量 IV 长度为 n; 密钥的长度为 k. OFBNLF 模式只能处理长度为 n 比特的倍数的消息. 如果要处理任意长度的消息, 需要对消息进行填充. 一般采用的填充方式为先填充一个比特 1, 再填充若干比特 0, 使其长度为 n 的倍数. 本文只考虑能完整分组的消息空间. 算法 3 和图 1 描述了 OFBNLF 模式的加解密过程.

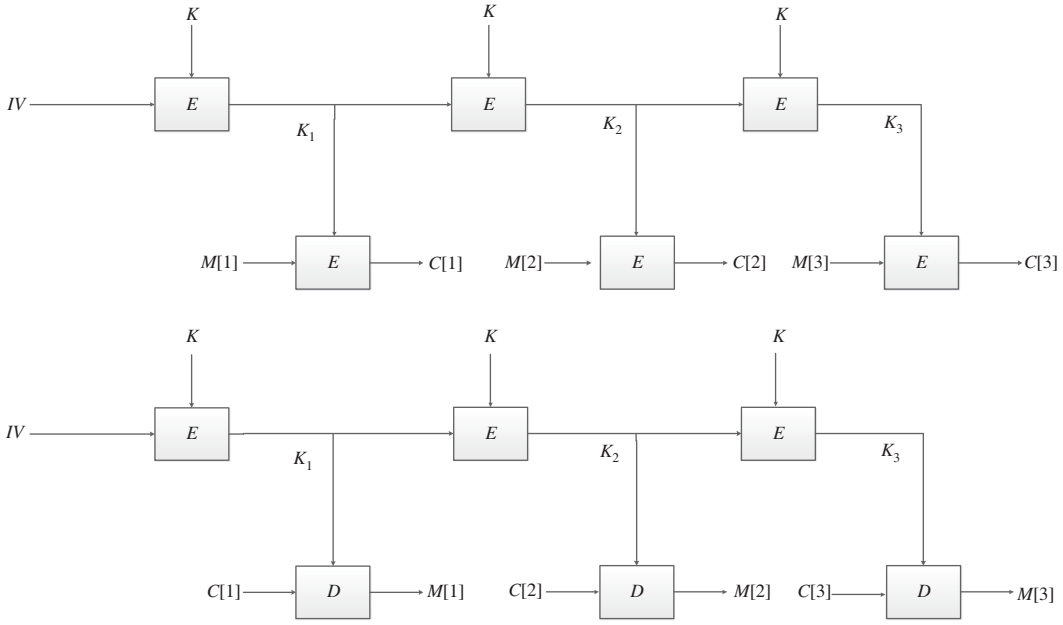

图 1　带非线性函数的输出反馈工作模式 (OFBNLF)

Figure 1　Output feedback with a nonlinear function (OFBNLF)

算法 3 OFBNLF 模式的整体描述

procedure $\mathcal{E}_K^{\mathrm{OFBNLF}}(IV, M)$
　Partition M into $M[1]\cdots M[m]$
　$K_0 \leftarrow IV$
　for $i \leftarrow 1, m$ **do**
　　$K_i \leftarrow E_K(K_{i-1})$
　　$C[i] \leftarrow E_{K_i}(M[i])$
　end for
　$C \leftarrow C[1]\cdots C[m]$
　return C
end procedure

procedure $\mathcal{D}_K^{\mathrm{OFBNLF}}(IV, C)$
　Partition C into $C[1]\cdots C[m]$
　$K_0 \leftarrow IV$
　for $i \leftarrow 1, m$
　　$K_i \leftarrow E_K(K_{i-1})$
　　$M[i] \leftarrow D_{K_i}(C[i])$
　end for
　$M \leftarrow M[1]\cdots M[m]$
　return M
end procedure

定理1　OFBNLF[E] 是使用分组密码 E 作为底层模块的 OFBNLF 模式, 对于同一密钥 K, 敌手 $\mathcal{A}$ 在询问中能选择不重复的 IV 值. 则对于任意的时间复杂度 t, 询问次数 q (即询问左边谕言的次数), 询问消息的总的分组数 μ (即询问右边谕言的次数), 有

$$\mathrm{Adv}^{\text{bw-ind-cpa}}_{\mathrm{OFBNLF}[E]}(t,q,\mu) \leqslant \mathrm{Adv}^{\mathrm{prp}}_{E}(t+O(q+\mu),q+\mu)+\mu\mathrm{Adv}^{\mathrm{prp}}_{E}(t+O(\mu),1)+\frac{\mu(\mu-1)+q\mu}{2^n}. \tag{5}$$

假设分组密码 E 是一个伪随机置换, 所以 $\mathrm{Adv}^{\mathrm{prp}}_{E}(t+O(q+\mu),q+\mu)$ 和 $\mathrm{Adv}^{\mathrm{prp}}_{E}(t+O(\mu),1)$ 都是可忽略的. 除此之外, $\frac{\mu(\mu-1)+q\mu}{2^n}$ 也是可忽略的. 因此上述定义表明, 敌手 $\mathcal{A}$ 在时间复杂度为 t, 询问次数为 q, 询问消息的总的分组数为 μ 时, 对 OFBNLF 模式在 BW-IND-CPA 模型下的区分优势是可忽略的.

利用做游戏 (game-playing) [10] 的技术对定理 1 进行证明. 证明过程用到了 5 个游戏 $G1$, $G2$, $G3$, $G4$ 和 $G5$. 首先将真实方案的上层分组密码替换为随机置换得到游戏 $G1$, 他们之间的区分优势即为分组密码与随机置换之间的区分优势, 这一部分是可忽略的; 之后将方案上层的随机置换替换为随机函数得到游戏 $G2$, 这一替换之间的区分优势为随机置换与随机函数之间的区分优势, 是可忽略的; 然后将上层的随机函数替换为随机串得到游戏 $G3$, 这一步的区分优势的上界是随机函数输入产生碰撞的概率, 是可忽略的; 之后将方案下层的分组密码替换为随机置换得到游戏 $G4$, 这时由于每一把密钥都是独立随机选取的, 使得这种替换是可行的, 这时两个游戏之间的区分优势为一簇分组密码与一簇随机置换之间的区分优势, 同样是可忽略的; 最后将方案的密文生成的部分替换为随机串输出得到游戏 $G5$, 由于 $G4$ 中输出密文的是每次独立选取的随机置换, 这时区分游戏 $G4$ 与 $G5$ 的优势为 0, 这时游戏 $G5$ 已经等价于方案的理想情况. 把这几步之间的优势累加起来, 即得到真实方案与理想方案之间的区分优势的上界, 也是可忽略的. 具体证明过程如下.

证明 将 OFBNLF 模式中上层用于生成子密钥的底层分组密码替换为随机置换 π 得到游戏 $G1$. 在游戏的描述中, 仅给出两个谕言回答攻击者询问的过程, 以下相同.

$$G1: \quad \mathcal{E}_K^{\text{int}}(IV): S \leftarrow \pi(IV); \quad \mathcal{E}_K^{\text{next}}(M): C \leftarrow E_S(M),\ S \leftarrow \pi(S),\ \text{return } C.$$

$(\mathcal{E}^{\text{int}}, \mathcal{E}^{\text{next}})$ 与游戏 $G1$ 唯一的区别在于方案的上层中的分组密码换成了 π, 敌手 $\mathcal{B}$ 调用 $\mathcal{A}$ 模拟其过程, 输出 $\mathcal{A}$ 的输出, 那么敌手 $\mathcal{B}$ 就是一种区分底层分组密码和随机置换 π 的算法. $\mathcal{B}$ 的时间复杂度为 $t + O(q + \mu)$, 询问次数为 $q + \mu$, 则

$$|\Pr[\mathcal{A}^{\mathcal{E}_K^{\text{int}}, \mathcal{E}_K^{\text{next}}} = 1] - \Pr[\mathcal{A}^{G1} = 1]| \leqslant \text{Adv}_E^{\text{prp}}(t + O(q + \mu), q + \mu). \tag{6}$$

再将 OFBNLF 模式中上层用于生成子密钥的底层随机置换 π 替换为随机函数 ρ ($\rho \xleftarrow{\$} \text{Func}(n)$), 得到游戏 $G2$:

$$G2: \quad \mathcal{E}_K^{\text{int}}(IV): S \leftarrow \rho(IV); \quad \mathcal{E}_K^{\text{next}}(M): C \leftarrow E_S(M),\ S \leftarrow \rho(S),\ \text{return } C.$$

敌手 $\mathcal{A}$ 区分游戏 $G1$ 和游戏 $G2$, 敌手 $\mathcal{B}$ 调用 $\mathcal{A}$ 模拟 $\mathcal{A}$ 的过程, 输出 $\mathcal{A}$ 的输出, 对 OFBNLF 模式底层中的随机置换与随机函数进行区分, 其中时间复杂度为 $t + O(q + \mu)$, 询问次数为 $q + \mu$, 其中每次明文串的最后一个明文分组的处理过程中生成的子密钥并没有被使用, 本文忽略了这一部分的处理, 因此 $\mathcal{B}$ 的实际询问次数为 μ, 根据 PRP-PRF 切换引理 [16, 18], 则

$$|\Pr[\mathcal{A}^{G1} = 1] - \Pr[\mathcal{A}^{G2} = 1]| \leqslant \frac{\mu(\mu - 1)}{2^{n+1}}. \tag{7}$$

将模式中的状态值 S 的更新由随机函数的输出值替换为随机串输出, 得到游戏 $G3$:

$$G3: \quad \mathcal{E}_K^{\text{int}}(IV): S \xleftarrow{\$} \{0,1\}^n; \quad \mathcal{E}_K^{\text{next}}(M): C \leftarrow E_S(M),\ S \xleftarrow{\$} \{0,1\}^n,\ \text{return } C.$$

不难看出, $G2$ 和 $G3$ 只有在对 ρ 的输入产生碰撞的时候是不一样的. 输入值是 IV 或是中间状态值 (子密钥), 一共有 q 个 IV 值, μ 个子密钥值. coll 表示在游戏 $G2$ 中这些值至少发生一次碰撞时的事件. 根据做游戏技术 [10], 有

$$|\Pr[\mathcal{A}^{G2} = 1] - \Pr[\mathcal{A}^{G3} = 1]| \leqslant \Pr[\text{coll}].$$

coll1 表示 IV 和子密钥之间发生碰撞, coll2 表示子密钥之间发生碰撞, 那么

$$\Pr[\text{coll}] \leqslant \Pr[\text{coll1}] + \Pr[\text{coll2}].$$

由于一共有 q 个 IV 值, μ 个子密钥值, 每个子密钥与某个 IV 产生碰撞的概率都为 $1/2^n$, 则 IV 和子密钥之间至少发生一次碰撞的概率为

$$\Pr[\text{coll1}] \leqslant \frac{q\mu}{2^n},$$

μ 个子密钥值之间发生碰撞的概率为

$$\Pr[\text{coll2}] \leqslant \frac{1}{2^n} + \frac{2}{2^n} + \cdots + \frac{\mu-1}{2^n} = \frac{\mu(\mu-1)}{2^{n+1}}.$$

因此

$$|\Pr[\mathcal{A}^{G2}=1] - \Pr[\mathcal{A}^{G3}=1]| \leqslant \frac{2q\mu + \mu(\mu-1)}{2^{n+1}}. \tag{8}$$

将模式下层对明文进行加密的分组密码模块 E_S 全部替换为随机置换 π_S, 得到游戏 $G4$:

$$G4: \quad \mathcal{E}_K^{\text{int}}(IV): S \xleftarrow{\$} \{0,1\}^n; \quad \mathcal{E}_K^{\text{next}}(M): C \leftarrow \pi_S(M),\ S \xleftarrow{\$} \{0,1\}^n,\ \text{return } C.$$

敌手 $\mathcal{C}$ 调用 $\mathcal{A}$ 模拟 $\mathcal{A}$ 的过程, 输出 $\mathcal{A}$ 的输出, 即得到区分分组密码 $\{E_{S_i}: i=1,2,\ldots,\mu\}$ 与随机置换 $\{\pi_{S_i}: i=1,2,\ldots,\mu\}$ 的算法, 其中 $S_i, i=1,2,\ldots,\mu$ 是 μ 个随机独立的值. 可以在游戏 $G3$ 和 $G4$ 之间构造一系列的游戏, 使得每次只将一个分组密码替换为随机置换, 如下所示:

$$\begin{aligned}
G3: &\ E_{S_1}\ E_{S_2}\ E_{S_3}\ \cdots\ E_{S_\mu},\\
&\ \pi_{S_1}\ E_{S_2}\ E_{S_3}\ \cdots\ E_{S_\mu},\\
&\ \pi_{S_1}\ \pi_{S_2}\ E_{S_3}\ \cdots\ E_{S_\mu},\\
&\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots,\\
G4: &\ \pi_{S_1}\ \pi_{S_2}\ \pi_{S_3}\ \cdots\ \pi_{S_\mu},
\end{aligned}$$

每两个游戏之间的都只有一个分组密码和一个随机置换的区别, 因此区分优势都以 $\text{Adv}_E^{\text{prp}}(t+O(\mu),1)$ 为上界, 所以

$$|\Pr[\mathcal{A}^{G3}=1] - \Pr[\mathcal{A}^{G4}=1]| \leqslant \mu \text{Adv}_E^{\text{prp}}(t+O(\mu),1). \tag{9}$$

将模式中密文 C 的输出值由随机置换的输出值替换为随机串输出, 得到游戏 $G5$:

$$G5: \quad \mathcal{E}_K^{\text{int}}(IV): S \xleftarrow{\$} \{0,1\}^n; \quad \mathcal{E}_K^{\text{next}}(M): C \xleftarrow{\$} \{0,1\}^n,\ S \xleftarrow{\$} \{0,1\}^n,\ \text{return } C.$$

由于在游戏 $G4$ 和 $G5$ 中的子密钥都是随机独立的值, 对于游戏 $G4$ 来说, 底层模块 π_S 是随机独立的置换, 且只用一次, 因此输出值是随机值; 对于游戏 $G5$ 来说, 输出的也是随机值. 因此在敌手看来, 游戏 $G4$ 和 $G5$ 是一样的, 即

$$|\Pr[\mathcal{A}^{G4}=1] - \Pr[\mathcal{A}^{G5}=1]| = 0. \tag{10}$$

由于游戏 $G5$ 输出的一直是随机串, 则

$$|\Pr[\mathcal{A}^{G5}=1] - \Pr[\mathcal{A}^{\$^{\text{int}}(\cdot),\$^{\text{next}}(\cdot)}=1]| = 0. \tag{11}$$

综合式 (6)~(11), 敌手 $\mathcal{A}$ 在时间复杂度为 t, 询问次数为 q, 询问消息的总的分组数 μ 时, 对 OFBNLF 模式在 BW-IND-CPA 下的区分优势满足

$$\text{Adv}^{\text{bw-ind-cpa}}_{\text{OFBNLF}[E]}(\mathcal{A}) = |\Pr[\mathcal{A}^{\mathcal{E}_K^{\text{int}},\mathcal{E}_K^{\text{next}}}=1] - \Pr[\mathcal{A}^{\$^{\text{int}}(\cdot),\$^{\text{next}}(\cdot)}=1]|$$

表 1 对 OFBNLF, ECB, CBC, CTR, CFB, OFB 和 BC 等加密模式特点的总结 (模式描述参考附录 A, 表中部分数据来源于文献 [24])

Table 1 Summarize the characteristics of OFBNLF, ECB, CBC, CTR, CFB, OFB and BC. (The descriptions of mode refer to appendix, some conclusions are derived from the paper [24])

Characteristics	ECB	CBC	CTR	CFB	OFB	BC	OFBNLF
IV	×	✓	✓	✓	✓	✓	✓
IND-CPA (IV as nonce)	×	×	✓	×	×	×	✓
IND-CPA (IV as a random number)	×	✓	✓	✓	✓	✓	✓
BW-IND-CPA (IV as nonce)	×	×	✓	×	×	×	✓
BW-IND-CPA (IV as a random number)	×	×	✓	✓	✓	×	✓

$$
\begin{aligned}
&\leqslant |\Pr[\mathcal{A}^{\mathcal{E}_K^{\text{int}},\mathcal{E}_K^{\text{next}}}=1]-\Pr[\mathcal{A}^{G1}=1]|+|\Pr[\mathcal{A}^{G1}=1]-\Pr[\mathcal{A}^{G2}=1]|\\
&\quad+|\Pr[\mathcal{A}^{G2}=1]-\Pr[\mathcal{A}^{G3}=1]|+|\Pr[\mathcal{A}^{G3}=1]-\Pr[\mathcal{A}^{G4}=1]|\\
&\quad+|\Pr[\mathcal{A}^{G4}=1]-\Pr[\mathcal{A}^{G5}=1]|+|\Pr[\mathcal{A}^{G5}=1]-\Pr[\mathcal{A}^{\$^{\text{int}}(\cdot),\$^{\text{next}}(\cdot)}=1]|\\
&\leqslant \mathrm{Adv}_E^{\text{prp}}(t+O(q+\mu),q+\mu)+\frac{\mu(\mu-1)}{2^{n+1}}+\frac{2q\mu+\mu(\mu-1)}{2^{n+1}}\\
&\quad+\mu\mathrm{Adv}_E^{\text{prp}}(t+O(\mu),1).
\end{aligned}
$$

因此,

$$
\mathrm{Adv}^{\text{bw-ind-cpa}}_{\text{OFBNLF}[E]}(t,q,\mu)\leqslant\ \mathrm{Adv}_E^{\text{prp}}(t+O(q+\mu),q+\mu)+\mu\mathrm{Adv}_E^{\text{prp}}(t+O(\mu),1)+\frac{q\mu+\mu(\mu-1)}{2^n}.
$$

4 安全性对比

OFBNLF 模式是 OFB 模式和 ECB 模式相结合的一个变体, 用于直接对明文进行加密处理的子密钥随每一个分组改变. 当生成的子密钥产生碰撞的时候, 将产生相同的密钥流, 即对于同一位置相同的明文将产生相同的密文, 这一部分继承了 OFB 的特性. 类似 ECB 模式, OFBNLF 模式没有采用链式的结构, 当前密文分组只与当前明文分组, 此分组在明文串中的位置及初始值 IV 相关, 与之前的明文分组无关.

表 1 有关模式 ECB, CBC, CTR, CFB 和 OFB 的结论来自文献 [24], 同时还包含 BC 及 OFBNLF 两个工作模式的安全性结论. 我们分别对这几种模式在常规安全模型 IND-CPA 和 BW-IND-CPA 下的安全性作了总结和比较, 每种模式分为初始向量 IV 作为随机数和作为 nonce 使用的两种情况. BC 模式在结构上与 CBC 模式相似, 由本文的方法易知 BC 模式的安全性与 CBC 模式也是相似的 —— 只有在 IV 作为随机数时的 IND-CPA 模型下是安全的, 其他情况下都是不安全的. 不安全情况下的攻击过程可参考同情况下对 CBC 模式的攻击. 当 IV 作为随机数时, CFB 和 OFB 模式在 IND-CPA 和 BW-IND-CPA 模型下都是安全的. 不论 IV 是作为随机数还是 nonce 使用, 不论是在 IND-CPA 模型下还是 BW-IND-CPA 模型下, 模式 OFBNLF 都是安全的. 表中的 CTR 模式为附录 A 中描述的模式, 区别于国家标准和国际标准中的 CTR 模式, 表中 CTR 模式的 IV 作为 nonce 或随机数使用, 标准中的 IV 作为带状态的计数器使用或作为 nonce 使用, 这么修改是为了与本文之前对 IV 的定义相

表 2　加密模式的软件实现性能比较. 每一个模式都分别在 128, 256, 512, 1024 和 4096 字节下作了比较. 表中实验数据的单位是时钟周期每字节 (cpb). 实验环境是 Intel(R) Core(TM) i7-2600 CPU @ 3.40 GHz, 在 GCC 的环境下编译. 模式中的分组密码分别使用 AES 以及 SM4

Table 2 The comparison of software performance of modes. We implemented these modes on our PC with Intel(R) Core(TM) i7-2600 CPU (3.40 GHz). Test data are collected under 128, 256, 512, 1024 and 4096 bytes. The block ciphers adopted are AES and SM4

	128		256		512		1024		4096	
	AES	SM4	AES	SM4	AES	SM4	AES	SM4	AES	SM4
CTR	3.71	69.5	2.31	46.86	1.4	46.31	0.86	45.29	0.78	45.21
ECB	3.69	67.05	2.24	44.75	1.33	43.57	0.78	44.05	0.67	42.63
CBC	11.35	67.52	8.56	45.14	5.31	43.81	4.71	43.37	4.64	43.45
CFB	11.27	67.24	8.51	44.82	5.3	44.18	4.71	44	4.63	42.94
OFB	10.84	67.21	8.27	44.82	5.23	43.94	4.67	43.31	4.59	42.59
BC	11.45	67.3	8.61	45.31	5.37	44.66	4.88	44.66	4.8	43.28
OFBNLF	14.53	99.99	11.92	77.48	11.69	76.37	11.5	76.29	11.4	76.1

匹配. 但不论 IV 是作为 nonce 使用、作为带状态的计数器使用, 还是作为随机数使用, CTR 模式在 IND-CPA 模型和 BW-IND-CPA 模型下都是安全的.

5　软件实现性能对比

本节将评估 OFBNLF 模式的软件实现性能, 将其与 CTR, ECB, CBC, CFB, OFB 和 BC 等加密模式进行比较. 底层的分组密码选用应用十分广泛的 AES 算法和我国国家标准 SM4 算法 [25], 并分别测试了在这两种分组密码下 CTR, ECB, CBC, CFB, OFB, BC 和 OFBNLF 等模式的软件实现效率. 其中 AES 算法采用 AES 新指令 (AES-NI) 实现, SM4 的算法实现没有进行优化[3]. 本实验没有采用多核并行计算.

从实验数据 (详见表 2) 中可以看出, ECB 模式和 CTR 模式是软件实现效率最高的加密模式. 这得益于他们可以进行充分的并行运算. 我们将 CTR 模式与 ECB 模式的轮函数展开, 充分利用了计算机的程序并发执行, 发挥了 CPU 的并行工作能力, 从而提高了实现效率. 但是这种方法并不适用于 CBC, CFB, OFB, BC 和 OFBNLF 等模式. 由于 CBC, CFB, OFB, BC 和 OFBNLF 等模式都是链接模式, 即当前处理建立在之前处理的结果上, 这种结构制约了这些模式在程序上实现并发执行. 除此之外, 分组密码 AES 的实现得到 Intel CPU 的指令支持 —— AES-NI. 这种指令方式的实现使得这几种模式在 AES 分组密码下的实现效率高于 SM4 下的实现效率. 但是, 与其他加密模式相比, 不论是以 AES 还是 SM4 作为底层分组密码, OFBNLF 模式的软件实现性能都不是十分理想 (详见图 2 和 3), 我们将原因归结为以下两点:

分组密码的调用过多. 在 OFBNLF 模式中, 每处理一个分组的明文都要有两次的分组密码的调用, 这样大大降低了实现效率;

密钥扩展算法的影响. 在 OFBNLF 模式中, 每一个明文分组的处理都需要进行一次密钥扩展算法的调用, 对 AES 来说, 密钥扩展算法的实现代价在整个的实现代价中占据了大量的时间, 导致大量

3) 由于目前缺乏对 SM4 软件实现的研究, 我们没有对基于 SM4 的 CTR 和 ECB 两种模式进行并行实现的优化, 所以这两种模式的实现效率与其他的串行模式的实现效率相近.

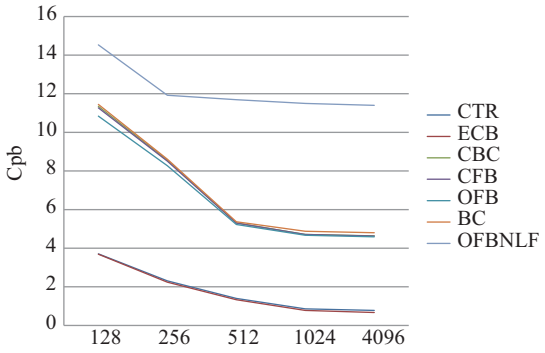

图 2 使用 AES 的加密模式的软件实现效率对比

Figure 2 Comparison of the software implementation efficiency of the encryption modes based on AES

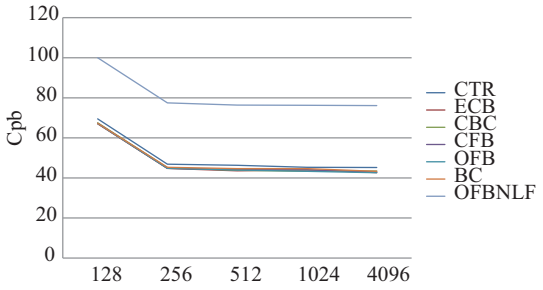

图 3 使用 SM4 的加密模式的软件实现效率对比

Figure 3 Comparison of the software implementation efficiency of the encryption modes based on SM4

的时间被用于密钥扩展算法. 当然也可以选择一次性生成大量的子密钥, 但是存储的代价就相应地提高了.

本文认为 OFBNLF 模式中的每组明文需要两次分组密码调用的设计方式, 不论是从理论角度还是实验结果看, 效率都是比较低的.

6 结束语

本文首次对 OFBNLF 模式进行系统的安全性分析和软件实现效率评估. 本文在给出 OFBNLF 模式在线加密描述的基础上, 利用做游戏的技术第一次证明了 OFBNLF 模式在 BW-IND-CPA 模型下的安全性. 鉴于之前对 BW-IND-CPA 模型的形式定义并没有对一般的加密模式进行在线的形式化处理, 在给出在线加密形式定义的基础上, 重新对 BW-IND-CPA 模型进行了定义. 除此之外, 对 OFBNLF 模式在安全性和软件实现效率方面与我国国家标准中其他的加密模式进行对比研究. 指出与 ECB, CBC, CTR, CFB, OFB 和 BC 等加密模式相比, OFBNLF 模式无论是在 IND-CPA 模型下还是在 BW-IND-CPA 模型下都是安全的, 但是不论是以 AES 作为底层分组密码, 还是 SM4 作为底层分组密码, 模式 OFBNLF 的软件实现性能都不是十分理想.

需要指出的是, 相对于国际标准, 国家标准 GB/T 17964-2008 额外增加了 OFBNLF 模式和 BC 模式. 在国际标准中针对 IV 应该如何生成和使用的问题, 给出了指导性的意见, 这一点在国家标准中没有体现出来. IV 的生成方式一般包括作为 nonce 使用和随机数两种方法, 国际标准还特别讨论了 CTR 模式中作为计数器使用的 IV. 当 IV 作为随机数使用时, 碰撞的概率为生日概率, 并不会破坏模式的安全性证明; 作为 nonce 使用时, 由使用者承担了算法随机化的责任, 使用者必须每次挑选不重复的值作为 IV, IV 的重用会破坏模式的安全, 例如在 CTR 模式和 OFBNLF 模式中, IV 一旦重用, 将生成相同的密钥流. 由于用户可选的缘故, 导致了 CBC, CFB, OFB 和 BC 等模式在 IND-CPA 安全模型下是不安全的. IV 的生成方式及使用方式直接影响了模式的安全性, 对于这部分的描述是非常有必要的. 我们建议将有关 IV 的生成方式及使用方式的描述写进未来的标准中, 以规范 IV 的使用方式, 避免不安全的情况.

参考文献

1 Menezes A J, van Oorschot P C, Vanstone S A. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996
2 中国标准出版社. 信息安全技术分组密码算法的工作模式. GB/T 17964-2008. http://webstore.spc.net.cn/produce/showonebook.asp?strid=36837. 2008
3 Bellare M, Desai A, Jokipii E, et al. A concrete security treatment of symmetric encryption. In: Proceedings of the 38th Annual Symposium on Foundations of Computer Science, Miami Beach, 1997. 394–403
4 Sung J, Lee S, Lim J I, et al. Concrete security analysis of CTR-OFB and CTR-CFB modes of operation. In: Information Security and Cryptology — ICISC 2001. Berlin: Springer, 2001. 103–113
5 Jansen C J, Boekee D E. Modes of blockcipher algorithms and their protection against active eavesdropping. In: Advances in Cryptology — EUROCRYPT'87. Berlin: Springer, 1987. 281–286
6 Jansen C J. Investigations on nonlinear streamcipher systems: construction and evaluation methods. Dissertation for Ph.D. Degree. Delft: Delft University of Technology, 1989
7 Barlow L C. Symmetric encryption with multiple keys: techniques and applications. Dissertation for Master Degree. Corvallis: Oregon State University, 2005
8 Preneel B. Analysis and design of cryptographic hash functions. Dissertation for Ph.D. Degree. Leuven: Katholieke Universiteit te Leuven, 1993
9 Joux A, Martinet G, Valette F. Blockwise-adaptive attackers revisiting the (in) security of some provably secure encryption modes: CBC, GEM, IACBC. In: Advances in Cryptology — CRYPTO 2002. Berlin: Springer, 2002. 17–30
10 Bellare M, Rogaway P. The security of triple encryption and a framework for code-based game-playing proofs. In: Advances in Cryptology — EUROCRYPT 2006. Berlin: Springer, 2006. 409–426
11 Fouque P A, Martinet G, Poupard G. Practical symmetric on-line encryption. In: Fast Software Encryption. Berlin: Springer, 2003. 362–375
12 Goldwasser S, Micali S. Probabilistic encryption. J Comput Syst Sci, 1984, 28: 270–299
13 Namprempre C, Rogaway P, Shrimpton T. Reconsidering generic composition. In: Advances in Cryptology — EUROCRYPT 2014. Berlin: Springer, 2014. 257–274
14 Rogaway P. Nonce-based symmetric encryption. In: Fast Software Encryption. Berlin: Springer, 2004. 348–358
15 Goldwasser S, Bellare M. Lecture notes on cryptography. http://cseweb.ucsd.edu/ mihir/papers/gb.pdf. 2008
16 Bellare M, Kilian J, Rogaway P. The security of the cipher block chaining message authentication code. J Comput Syst Sci, 2000, 61: 362–399
17 Luby M, Rackoff C. How to construct pseudorandom permutations from pseudorandom functions. SIAM J Comput, 1988, 17: 373–386
18 Bellare M, Goldreich O, Mityagin A. The power of verification queries in message authentication and authenticated encryption. Cryptology ePrint Archive, 2004, 2004: 309
19 Hoang V T, Reyhanitabar R, Rogaway P, et al. Online authenticated-encryption and its nonce-reuse misuse-resistance. IACR Cryptology ePrint Archive, 2015, 2015: 189
20 Andreeva E, Bogdanov A, Luykx A, et al. How to securely release unverified plaintext in authenticated encryption. In: Advances in Cryptology — ASIACRYPT 2014. Berlin: Springer, 2014. 105–125
21 Agrawal M, Chang D, Sanadhya S. Sp-AELM: sponge based authenticated encryption scheme for memory constrained devices. In: Information Security and Privacy. Berlin: Springer, 2015. 451–468
22 Hoang V T, Krovetz T, Rogaway P. Robust authenticated-encryption AEZ and the problem that it solves. In: Advances in Cryptology — EUROCRYPT 2015. Berlin: Springer, 2015. 15–44
23 Rogaway P, Zhang H. Online ciphers from tweakable blockciphers. In: Topics in Cryptology — CT-RSA 2011. Berlin: Springer, 2011. 14–18
24 Rogaway P. Evaluation of some blockcipher modes of operation. http://web.cs.ucdavis.edu/ rogaway/papers/modes-cryptrec.pdf. 2011
25 国家商用密码管理办公室. 无线局域网产品使用的 SMS4 密码算法. http://www.oscca.gov.cn/News/200705/News_1106.html

附录 A ECB, CBC, CTR, CFB, BC 和 OFB 模式

ECB, CBC, OFB 和 CFB 是最初作为 DES 的应用被标准化. 后来 CTR 模式在由 DES 过渡到 AES 的过程中被标准化. 下面将简要介绍这 6 种模式. 定义模式中使用的初始值为 IV, 可以作为用户可选的 nonce, 不能重复; 除此之外, IV 也可交由算法随机独立选取, 用户不能干扰参与这个过程. 模式中使用到的底层分组密码统一定义为 $E : K \times \{0,1\}^n \to \{0,1\}^n$, 加密过程: $C = E_K(M)$, 解密过程: $M = D_K(C)$. 明文分组: $M[1], M[2], \ldots$; 密文分组: $C[1], C[2], \ldots$(若有 IV, 则 $C[0] = IV$).

ECB	$C[i] = E_K(M[i])$	$M[i] = D_K(C[i])$,
CBC	$C[i] = E_K(M[i] \oplus C[i-1])$	$M[i] = D_K(C[i]) \oplus C[i-1]$,
CTR	$C[i] = E_K(IV \| i) \oplus M[i]$	$M[i] = E_K(IV \| i) \oplus C[i]$,
CFB	$C[i] = M[i] \oplus E_K(C[i-1])$	$M[i] = C[i] \oplus E_K(C[i-1])$,
OFB	$C[i] = M[i] \oplus T[i]$	$M[i] = C[i] \oplus T[i]$
	$T[i] = E_K(T[i-1])$	$T[0] = C[0]$,
BC	$C[i] = E_K(T_i \oplus M[i])$	$M[i] = D_K(C[i]) \oplus T[i]$
	$T[i] = T[i-1] \oplus C[i-1]$	$T[0] = C[0]$.

6 种模式介绍完毕.

Analysis of the OFBNLF encryption mode of operation

Zhelei SUN[1,2,3] & Peng WANG[1,3*]

1 *Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China*;
2 *University of Chinese Academy of Sciences, Beijing* 100049*, China*;
3 *Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing* 100093*, China*
*E-mail: wp@is.ac.cn

Abstract OFBNLF is one of the national standardized block cipher modes of operation. In this mode, indistinguishability under chosen plaintext attack is an important security index. To the best of our knowledge, to date no analysis of the security and software implementation efficiency of OFBNLF mode has been conducted. In this paper, we analyze the security of OFBNLF and show that OFBNLF is blockwise-IND-CPA (indistinguishability under blockwise-based chosen plaintext attack) using game-playing techniques based on the description of online encryption on OFBNLF. The previous definition of BW-IND-CPA mode was not based on online mode; however, in this paper, we redefine BW-IND-CPA mode on the basis of online encryption. In addition, we compare OFBNLF mode with other encryption modes of the national standard in terms of security and software implementation efficiency.

Keywords block cipher mode of operation, OFBNLF, security analysis, indistinguishability under blockwise-based chosen plaintext attack, efficiency

Zhelei SUN was born in 1989. She received a B.E. degree from Sichuan University in 2011. Currently, she is a Ph.D. candidate at University of Chinese Academy of Sciences. Her research interests include authenticated encryption and universal hash.

Peng WANG was born in 1976. He received a Ph.D. degree in communication systems from University of Chinese Academy of Sciences in 2006. Currently, he is an associate professor at the Institute of Information Engineering (IIE), Chinese Academy of Sciences. His research interests include symmetric cryptography and its applications.