分组密码工作模式的应用安全问题

王 鹏　　郭婷婷
（信息安全国家重点实验室（中国科学院信息工程研究所） 北京 100093）
（中国科学院数据与通信保护研究教育中心 北京 100093）
（中国科学院大学网络空间安全学院 北京 100049）
（wp@is.ac.cn）

Application Security of Block Cipher Mode of Operation

Wang Peng and Guo Tingting
（*State Key Laboratory of Information Security*（*Institute of Information Engineering*, *Chinese Academy of Sciences*）, *Beijing* 100093）
（*Data Assurance and Communication Security Research Center*, *Chinese Academy of Sciences*, *Beijing* 100093）
（*School of Cyber Security*, *University of Chinese Academy of Sciences*, *Beijing* 100049）

Abstract The block cipher mode of operation has a nearly perfect theoretical system—as long as the underlying block cipher is secure, the upper mode of operation can be proved to be secure. However, there is a huge gap between theory and reality. In reality, various application security issues have repeatedly appeared. This paper focuses on a series of problems including IV misuse, online attack, RUP problem, padding oracle attack, birthday attack, etc. IV misuse means the IV value which produced by programmers doesn't meet the random strength in cryptography. This problem can be avoided by using the nonce-based schemes. The data in some mode of operations is processed online. Therefore, the operations will suffer block-wise attack, which is also called online attack. The solution is to use the authenticatd encryption mode which is secure online. The RUP problem means the operations output unverified plaintext, which doesn't satisfy data integrity. Abed and Ashur et al. have improved relevant mode of operation to solve this problem. Padding oracle attack means the enemy using error messages which are returned by the receiver to attack the operations. To avoid such attack, the authenticatd encryption mode can be used. The birthday attack takes advantage of the collision in the middle state of the block cipher mode to forge. The secure strength of the block cipher whose block length is 64 bits will be reduced to 32 bits due to this attack, which is un-secure for them. Therefore, we'd better design the mode of operations which is beyond birthday bound. In this paper, we will analyze the causes of the above problems, the research status and solutions in detail. Finally, we will give some useful suggestions.

Key words block cipher; mode of operation; initial vector; online attack; RUP problem; padding oracle; birthday attack

收稿日期：2018-11-15

摘　要　分组密码工作模式有着近乎完美的理论体系：只要底层分组密码是安全的，上层工作模式就可以被证明是安全的.但是理论与现实之间存在巨大差距，现实情况中分组密码工作模式往往会出现各种各样的应用安全问题.主要梳理了其中的IV误用、在线攻击、RUP问题、填充谕示攻击、生日攻击等一系列问题，其中IV误用是指程序员生成的IV值没有达到密码学要求的随机强度，对此可以使用基于Nonce的方案来避免；在线攻击是指一些情况下数据采用在线处理的方式而受到的逐分组攻击，解决方法是使用在线安全的认证加密模式；RUP问题是指工作模式输出未验证的明文，使得数据完整性得不到满足，对此Abed和Ashur等人对相关模式进行了改进；填充谕示攻击是指敌手利用接收方对不正确密文返回的错误提示信息进行攻击，对此可以使用认证加密模式来避免；生日攻击利用工作模式中间状态的碰撞进行伪造的攻击，在此攻击下分组长度为64 b的分组密码的安全强度会降为32 b，为了避免这个问题，需要设计超生日界的工作模式.详细分析了以上问题出现的原因、关于它们的研究现状及相应的解决办法，最后给出几点具体的建议.

关键词　分组密码；工作模式；初始向量；在线攻击；RUP问题；填充谕示；生日攻击

中图法分类号　TP309

分组密码算法是研究较为成熟的密码模块.从形式上看，分组密码是就在密钥控制下进行置换，它能将定长的明文变换成相同长度的密文.如果把实现了机密性、完整性等安全性功能的密码方案看作是高楼大厦，分组密码就是构建这些高楼大厦的砖头.我们把用分组密码构造的密码方案称为分组密码工作模式，以下简称为工作模式或者模式.按照功能划分，分组密码工作模式主要包括：1)加密模式，例如CBC，OFB，CFB，CTR等，实现的是机密性，即敌手无法从密文得到明文任一比特的信息；2)认证模式，例如CBC-MAC，PMAC，CMAC，实现的是完整性，即敌手无法伪造能通过验证的消息；3)认证加密模式，例如GCM，OCB，COPA等，同时实现了机密性和完整性.

现代分组密码的设计近乎苛刻，设计的分组密码要经过差分攻击、线性攻击、不可能差分攻击、中间相遇攻击等一系列已知攻击的检验，在没有找到比穷搜密钥攻击更为有效的攻击的情况下才被认为是安全的.一大批密码学家都为此倾尽心力.如果一个分组密码是安全的分组密码，那么当密钥随机选取时，可以将其看作是一个伪随机置换(PRP).一般情况下，分组密码工作模式的安全性都是在假设分组密码是伪随机置换的基础上，给出相应安全模型下的严格证明.安全模型包含敌手能力、安全目标以及安全指标等内容：敌手能力刻画了攻击者的能力，例如计算能力、攻击方式(已知明文攻击、选择明文攻击、选择密文攻击、在线攻击等)、获得的信息等；安全目标是机密性、完整性等要实现的安全功能；安全指标是对安全目标的进一步量化，是攻击者优势的具体度量.

分组密码工作模式有近乎完美的安全理论体系：只要底层分组密码是安全的，上层工作模式就可以被证明是安全的.然而，理论和现实之间却存在着巨大的差距.工作模式在应用中经常出现安全问题.原因主要源自3个方面：1)安全证明的前提条件不成立.例如，在某些工作模式中，要求每次重新随机选取初始向量(IV)才能推出证明结果，但是在实际应用中程序员往往简单地生成IV，达不到随机性的要求，导致工作模式的安全性出现问题.2)超出了安全结论的适用范围.安全结论并不是无条件成立的，例如对工作模式的生日攻击已经超出了安全结论的适用范围.3)安全模型和现实存在差异.比如填充谕示攻击、在线攻击、RUP攻击，它们都和经典的安全模型存在差异.

本文梳理了分组密码工作模式的IV误用、在线攻击、RUP问题、填充谕示攻击、生日攻击等一系列应用安全问题，分析了这些问题出现的原因、关于它们的研究现状及对应的解决办法，最后给出几点具体的建议.

1　IV误用

加密模式或者认证加密模式通常会使用初始向量(IV)，IV的主要作用是使密文随机化，其最

低要求是不能重复使用，以保证即使加密相同的明文也能得到不同的密文，甚至得到的密文是随机独立的. 不同工作模式对 IV 的使用有不同的要求. 例如 CBC 加密模式要求每次加密时都随机选取新的 IV. 因此，原则上需要有一个随机数生成器不断地生成 IV，这对算法的实现提出了很高的要求. 在实现过程中，很多程序员只是简单地调用类似于 C 语言标准库中的 random() 函数来生成 IV，但实际上这些函数达不到密码学中要求的随机强度. 在 SSL v3 和 TLS v1. 0 这 2 个协议中，将 CBC 模式当前 IV 值取为前一次密文的最后一个分组，这使得当前 IV 值是可预测的. Duong 等人[1]利用这一特征，进一步发展出针对 CBC 模式的、能有效恢复明文的攻击. 随后 TLS v1. 1 和 v1. 2 明确要求在每次加密时 IV 值必须是随机生成的.

在各种实际使用的安全协议中，因为 IV 值没有严格按照要求生成，从而造成 CBC 模式出现严重安全问题的例子多不胜数. IV 的误用一直是工作模式的一大问题. Rogaway 等人[2]认为应该在工作模式设计中降低对 IV 的使用要求，降为只要求其满足不重复的最低要求，并且攻击者除了可以选择明文/密文，还可以选择不重复的 IV 进行攻击，由此提出了基于 Nonce 的方案. 然而 CBC 模式在 Nonce 下是不安全的，于是 Rogaway 等人[2]将 CBC 模式改进为 CBC2 模式，并证明了基于 Nonce 的 CBC2 模式在在线安全模型下的安全性. 目前有很多工作模式都是基于 Nonce 的方案，例如 GCM，OCB 等认证加密模式. 这些模式在实现过程中，只需要保证 IV 不重复即可保证安全性，降低了 IV 实现的代价.

2 在线攻击

在传统的工作模式中一般将数据作为一个整体进行处理. 但是在存储、通信等资源受限的轻量级应用中，有时数据需要以在线的方式进行处理. 例如，在加解密过程中需要先将数据进行分组，然后一边输入分组数据，一边输出加密后的分组数据. 但是这种在线数据处理方式带来了一种新的攻击：逐分组攻击. 2002 年，Joux 等人[3]对在线加密的方式进行了研究，提出了逐分组（block-wise）攻击模型，即敌手可以根据在线得到的密文分组选择当前的明文分组，进行逐分组攻击. 在这一攻击下，CBC，GEM 和 IACBC 等一系列工作模式都是不安全的.

2003 年，Fouque 等人[4]在这一攻击模型下，证明 2 个在线加密模式 Delayed-CBC 和 CFB 是安全的；随后对各种逐分组安全模型及其之间的关系进行了研究[5]. 2004 年，Boldyreva 等人[6]对选择密文攻击下的逐分组安全模型进行了研究，提出了一种更实用的安全模型. 2006 年，Bard[5]指出 SSL 和 TLS 协议的早期版本中存在逐分组攻击可利用的弱点，并对逐分组安全模型作了进一步的研究[8]. 文献[9-10]对我国国家标准 GB/T 17964—2008 中 2 个新增加的分组密码工作模式 OFBNLF 和 BC 进行了研究，给出了 OFBNLF 模式在逐分组攻击下的安全性证明[9]，对于不安全的 BC 模式给出了修改方案[10].

在线工作模式的研究激发了在线密码（online cipher）的研究. 在线密码可以看作是分组密码的推广，是一个可以在线处理多个分组数据的分组密码. 由于要实现在线计算，在线密码当前输入的分组数据只会对当前和之后输出的分组数据产生影响. 这一对象的定义最初是由 Bellare 等人[11]在 2001 年给出，他们构造了 2 种基于泛哈希函数和分组密码的在线密码：HCBC1 和 HCBC2，并给出了在线加密在认证加密中的应用. 2008 年，Nandi[12]给出了另外 2 种在线密码构造：MHCBC 和 MCBC，其中 MHCBC 是对 HCBC2 的改进，但 MCBC 不需要泛哈希函数. 2011 年，Rogaway 等人[13]用可调分组密码重新梳理了以上构造，给出了 TC1，TC2 和 TC3 这 3 种在线密码的设计. 2016 年，Bhaumik[14]设计了 OleF 在线密码模式，它利用 Feistel 结构，并且加解密只用到底层分组密码，该模式具有选择密文攻击下的安全性.

在线密码是在线处理分组数据的理想模块，逐渐成为在线认证加密（online authenticated encryption）的核心模块. 2012 年，Fleischmann 等人[15]提出了 McOE 认证加密模式，其核心就是在线密码，这一模式还可以解决初始向量重复使用的问题. 2013 年，Andreeva 等人[16]设计了 COPA 认证加密模式，它具有一定的并行计算能力. 2015 年，Hoang 等人[17]提出将在线密码作为在线认证

加密的安全性定义中的一部分是不合理的，在给出的新的定义中，用户可以任意选择在线处理数据的分割方式和密文扩展方式，适用范围更广. 2016年，Endignoux等人[18]进一步研究了在线认证加密和逐分组安全性之间的关系，并指出很多情况下二者的要求是等价的.

3 RUP问题

一般的认证加密工作模式的解密过程需要先判断密文是否有效，当密文有效时才输出明文. 但是在资源受限时解密过程会先逐个输出明文分组，最后再作判断. 这就是所谓的输出未验证明文(released unverified plaintext, RUP)的问题. 由于在线认证加密方法的解密是在线进行的，这一问题在这种认证加密中尤为突出. 2014年，Andreeva等人[19]首次对RUP问题进行了系统研究，结果发现大多数在线认证加密工作模式包括GCM，OCB，COPA等一系列模式，在RUP下完整性都存在问题. 2016年，Chakraborti等人[20]通过对iFeed模式的分析，对一种类型的认证加密模式给出了RUP下的有效伪造攻击. 2017年，Datta等人[21]的研究指出只要COPA，ELmE，ELmD和COLM等模式的中间链接层是线性的，就能在RUP下进行有效的伪造攻击.

针对RUP下产生的完整性问题，2016年，Abed等人[22]对SIV模式进行了改进，2017年，Ashur等人[23]对GCM模式进行了改进，Zhang等人[24]对OCB模式进行了改进，在一定程度上解决了这一问题.

4 填充谕示攻击

在选择明文攻击下，CBC等加密工作模式被证明是安全的. 在这一安全模型中攻击者只拥有选择明文得到相应密文的能力，但是在现实应用环境中攻击者往往能获得其他一些关键的信息. 例如，在使用CBC模式时，由于分组密码只能处理固定分组长度的数据，因此消息在进行加密时都要先经过填充的步骤，然后再分成若干个分组的数据，最后再用CBC模式进行加密. 当接收方得到密文数据后进行解密可以得到填充后的消息. 如果发现填充是不正确的，那么密文在传输过程可能出现了问题. 因此，这时某些协议会发出一条信息告诉发送方消息的填充出现问题. 并且允许发送方重新发送密文，直到接收方收到正确的消息. 在公开的信道上攻击者很容易截获这类填充不正确的信息. Vaudenay的研究表明，如果攻击者能够获取这些信息，那么就可以进行有效的恢复明文攻击. 这种攻击被称为填充谕示(padding oracle)攻击[25-27].

我们看到，攻击者获取这些信息已经超出标准安全模型定义的敌手能力. 填充是否正确，是解密过程中产生的信息，是对消息填充有效性的一种判断，然而这一信息在通常的选择明文攻击下是无法获取的. 安全协议中返回对消息填充有效性的判断，说明具体应用中有对完整性这一安全功能的需求. 但是这种判断填充有效性的机制还不足以形成密码学意义上的完整性，比如如果我们只改变密文中的IV，那么得到的消息填充依旧正确，这相当于伪造了能够通过填充验证的密文信息. 为抵抗这种攻击最直接有效的方法就是改为使用认证加密模式，用认证加密模式中的解密算法来进行有效性的判断.

5 生日攻击

生日攻击是一种针对工作模式的常见攻击方式. 一般的工作模式都存在生日攻击问题. 生日攻击没有利用到任何分组密码的算法细节，只用到工作模式的结构或者将分组密码作为置换的特征. 工作模式的生日攻击一般利用工作模式中间状态的碰撞，将其转化为针对机密性的区分攻击或者针对完整性的伪造攻击. 对于n比特的分组长度，其工作模式的安全强度往往只有$n/2$比特，生日攻击只需要$2^{n/2}$的复杂度即可攻击成功. 例如，认证模式一般设计成一个输入是变长的伪随机函数(pseudorandom function, PRF). 认证模式OMAC[28]的安全界为$O(l^2q^2/2^n)$，其中n是分组密码的分组长度，q是敌手询问的次数，l是每次询问的消息的最长长度. 我们可以看到，当$q=2^{n/2}$时，安全界将趋近于1. 另一方面，的确存在具体的攻击只需要$2^{n/2}$次询问就可以区分OMAC和完全随机的函数[29]，甚至可以进行有效的伪造攻

击[30]. 我们将类似的攻击都称为生日攻击，将其安全界称为生日界. 我们注意到，生日攻击并没有违反 OMAC 的可证明安全结果.

如果是 128 b 分组密码的工作模式，生日攻击带来的问题不大，但是如果分组长度只有 64 b，那么其工作模式的安全强度只有 32 b. 现实生活中为了节省硬件资源，轻量级分组密码的分组长度一般都设置为 64 b，甚至更短. 同时由于历史原因，现实中还在使用一些 64 b 分组长度的分组密码，例如 Triple DES(3DES)算法. 如果我们直接对这些轻量级分组密码套用一些常见的工作模式，生日攻击将变成一种现实的攻击. 在 CCS 2016 会议上，Bhargavan 等人[31]在 TSL，OpenVPN 等安全协议中，展示了生日攻击对经典的 CBC 加密模式产生的威力. 对于 64 b 分组密码的工作模式，为保障其应用安全就不得不频繁地更换密钥，这又会给密钥管理带来极大的麻烦.

同时，密码学界一直都在致力于抗生日攻击的研究，设计了一批超越生日界(beyond birthday bound，BBB)的工作模式. 例如，SUM-ECBC，3kf9，PMAC_Plus 等认证模式和 CHM，CIP 等认证加密模式.

6 结　论

分组密码工作模式有着近乎完美的理论体系，却屡次出现各种应用安全问题. 任何理论体系只是对现实的部分抽象，无法完全反映真正的世界. 在工作模式的应用中我们不能盲目相信可证明安全理论的结果，而应该了解证明的含义和局限性，了解模式实现应该注意的问题，分析理论结果和现实的差异，真正做到对工作模式的安全性心中有数. 具体注意以下几点：

1) 在实现分组密码工作模式时严格按照要求生成 IV，特别对于随机 IV，要生成密码学意义下随机的 IV；如果没有办法达到 IV 的要求，选择使用基于 Nonce 的工作模式；

2) 对于在线使用的工作模式选择在线安全的工作模式，对于有完整性要求的应用场景，选择在线安全的认证加密工作模式；

3) 对于一般的认证加密模式，例如 GCM，OCB 等应该先判断密文的完整性，然后再决定是否输出明文，避免输出未验证明文(RUP)的情况发生；如果确实因为存储有限等原因不可避免，应该选择 RUP 下安全的工作模式；

4) 在有完整性信息交互的安全协议中使用认证加密模式，用认证加密模式中的解密算法作完整性的判断；

5) 对于 64 b 或者更短分组长度的分组密码，注意安全界的适用范围，选择抗生日攻击的工作模式；

6) CBC 模式是目前出问题最多的一种工作模式，如果没有特别的安全把握避免使用 CBC 模式.

参　考　文　献

[1] Duong T, Rizzo J. Here come the ⊕ ninjas [J/OL]. 2011 [2018-11-15]. http://www.hpcc.ess.soton.ac.uk/~dan/talks/bullrun/Beast.pdf

[2] Rogaway P. Nonce-based symmetric encryption [C] //Proc of Int Workshop on Fast Software Encryption. Berlin: Springer, 2004: 348-358

[3] Joux A, Martinet G, Valette F. Blockwise-adaptive attackers revisiting the (In) security of some provably secure encryption modes: CBC, GEM, IACBC [C] // Advances in Cryptology—CRYPTO 2002. Berlin: Springer, 2002: 231-248

[4] Fouque P A, Martinet G, Poupard G. Practical symmetric on-line encryption [C] //Proc of Int Workshop on Fast Software Encryption. Berlin: Springer, 2003: 362-375

[5] Fouque P A, Joux A, Poupard G. Blockwise adversarial model for on-line ciphers and symmetric encryption schemes [G] //Selected Areas in Cryptography. Berlin: Springer, 2004: 212-226

[6] Boldyreva A, Taesombut N. Online encryption schemes: New security notions and constructions [C] //Proc of Cryptographers' Track at the RSA Conf. Berlin: Springer, 2004: 1-14

[7] Bard G V. A challenging but feasible blockwise-adaptive chosen-plaintext attack on SSL [C] //Proc of Int Conf on Secrypt. Berlin: Springer, 2010: 7-10

[8] Bard G V. Blockwise-adaptive chosen-plaintext attack and online modes of encryption [C] //Proc of IMA Int Conf on Cryptography and Coding. Berlin: Springer, 2007: 129-151

[9] 孙哲蕾，王鹏. OFBNLF 加密工作模式的分析[J]. 中国科学：信息科学，2016，46(6)：729-742

[10] 郑凯燕，王鹏. BC加密模式的分析及其改进[J]. 信息安全学报，2017，2(3)：61-78

[11] Bellare M，Boldyreva A，Knudsen L，et al. Online ciphers and the Hash-CBC construction [C] //Proc of Int Cryptology Conf. Berlin：Springer，2001：292-309

[12] Nandi M. Two new efficient CCA-secure online ciphers：MHCBC and MCBC [C] //Progress in Cryptology—INDOCRYPT 2008. Berlin：Springer，2008：350-362

[13] Rogaway P，Zhang H. Online ciphers from tweakable blockciphers [C] //Topics in Cryptology—CT-RSA 2011. Berlin：Springer，2011：237-249

[14] Bhaumik R，Nandi M. Olef：An inverse-free online cipher. an online SPRP with an optimal inverse-free construction [J]. IACR Trans on Symmetric Cryptol，2016，2016(2)：30-51

[15] Fleischmann E，Forler C，Lucks S. McOE：A foolproof on-line authenticated encryption scheme [C] //Proc of Int Workshop on Fast Software Encryption. Berlin：Springer，2012：196-215

[16] Andreeva E，Bogdanov A，Luykx A，et al. Parallelizable and authenticated online ciphers [C] //Advances in Cryptology—ASIACRYPT 2013. Berlin：Springer，2013：424-443

[17] Hoang V T，Reyhanitabar R，Rogaway P，et al. Online authenticated-encryption and its nonce-reuse misuse-resistance [C] //Advances in Cryptology—CRYPTO 2015. Berlin：Springer，2015：493-517

[18] Endignoux G，Vizár D. Linking online misuse-resistant authenticated encryption and blockwise attack models [J]. IACR Trans on Symmetric Cryptol，2016，2016(2)：125-144

[19] Andreeva E，Bogdanov A，Luykx A，et al. How to securely release unverified plaintext in authenticated encryption [C] //Proc of Int Conf on the Theory and Application of Cryptology and Information Security. Berlin：Springer，2014：105-125

[20] Chakraborti A，Datta N，Nandi M. INT-RUP analysis of block-cipher based authenticated encryption schemes [C] //Proc of RSA Conf on Topics in Cryptology—Ct-RSA. Berlin：Springer，2016：39-54

[21] Datta N，Luykx A，Mennink B，et al. Understanding RUP integrity of COLM [J]. IACR Trans on Symmetric Cryptol，2017，2017(2)：143-161

[22] Abed F，Forler C，List E，et al. RIV for robust authenticated encryption [C] //Proc of Int Workshop on Fast Software Encryption. Berlin：Springer，2016：23-42

[23] Ashur T，Dunkelman O，Luykx A. Boosting authenticated encryption robustness with minimal modifications [C] //Proc of Int Cryptology Conf. Berlin：Springer，2017：3-33

[24] Zhang P，Wang P，Hu H，et al. INT-RUP security of checksum-based authenticated encryption [C] //Proc of Int Conf on Provable Security. Berlin：Spinger，2017：147-166

[25] Vaudenay S. Security flaws induced by CBC padding-applications to SSL，IPSEC，WTLS… [C] //Proc of Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin：Springer，2002：534-545

[26] Canvel B，Hiltgen A，Vaudenay S，et al. Password interception in a SSL/TLS channel [C] //Proc of Int Cryptology Conf. Berlin：Springer，2003：583-599

[27] Rizzo J，Duong T. Practical padding oracle attacks [C] //Proc of USENIX Conf on Offensive Technologies. Berkeley，CA：USENIX Association，2010：1-8

[28] Iwata T，Kurosawa K. OMAC：One-key CBC MAC [J]. Pre-proceedings of Fast Software Encryption，2003，20(1)：129-153

[29] Yuan Z，Wang W，Jia K，et al. New birthday attacks on some MACs based on block ciphers [G] //Proc of Int Cryptology Conf on Advances in Cryptology—CRYPTO 2009. Berlin：Springer，2009：209-230

[30] Jia K，Wang X，Yuan Z，et al. Distinguishing and second-preimage attacks on CBC-like MACs [C] //Proc of Int Conf on Cryptology and Network Security. Berlin：Springer，2009：349-361

[31] Bhargavan K. On the practical (in-) security of 64-bit block ciphers：Collision attacks on HTTP over TLS and OpenVPN [C] //Proc of ACM SIGSAC Conf on Computer and Communications Security. New York：ACM，2016：456-467

王 鹏

博士，副研究员，主要研究方向为对称密码方案的设计与分析.

wp@is.ac.cn

郭婷婷

博士研究生，主要研究方向为对称密码方案的设计与分析.

guotingting@is.ac.cn