

基于AES算法的 WLAN安全机制分析

Performance Analysis of AES-Based WLAN Security

中图分类号:

TP393.17

文献标识码:

A

文章编号:

1009-6868(2004)06-0042-05

刘永元/LIU Yong-yuan
张联峰/ZHANG Lian-feng
刘乃安/LIU Nai-an

(西安电子科技大学综合业务网国家重点实验室, 西安710071)
(State Key Laboratory of Integrated Service Networks, Xidian University,
Xi'an 710071, China)

摘要: 高级加密标准(AES)加密算法Rijndael采用对称的块加密技术, 提供比WEP/TKIP中RC4算法更高的加密性能, 它将成为取代WEP的新一代的加密技术, 为无线网络带来更强大的安全防护。文章主要讲述了AES加密算法, 在分支编码本(OCB)模式下的AES加密机制原理, AES算法在WLAN中的应用, 以及现有的一些针对AES算法的攻击方法。

关键词: 高级加密标准; 分支编码本模式; 无线局域网; 性能分析; 无线健壮安全认证协议

Abstract: Advanced Encryption Standard (AES) is a symmetric block cipher that is based upon the Rijndael algorithm. It performs better encryption than WEP/TKIP, and is expecting to replace WEP, strengthening wireless information security. This paper describes AES and Rijndael algorithm, a cipher suite based on the AES and Offset Codebook (OCB) mode, the implementation of AES in WLAN, and some attacks on the cipher AES.

Key words: Advanced Encryption Standard; Offset Codebook mode; Wireless LAN; performance analysis; Wireless Robust Authenticated Protocol

随着无线局域网(WLAN)技术的迅速发展, 无线网络安全越来越受到人们的关注。但IEEE802.11协议中包含的有线等效保密(WEP)子协议存在着各种各样的安全缺陷, 无法保证数据的机密性、完整性和对接入用户实现身份认证。

为了修补WEP协议, IEEE802.11工作组制定了TKIP(Temporal Key Integrity Protocol)安全协议。TKIP继续使用RC4算法, 但实现了动态密钥更新, 还增加了一个IV的杂凑函数和一个新的消息完整性校验算法, 极大地提高了加密安全强度。但作为一个临时加密协议, 由于WEP本身的缺陷, TKIP也很容易受到攻击。

为了彻底改善其协议的安全性能, IEEE802.11工作组在IEEE 802.11i中定义了一种基于高级加密标准(AES)的全新加密算法, 以实施更强大的加密和消息完整性检查。

1 AES算法

AES (Advanced Encryption Standard) 是1997年1月美国国家标准和技术研究所(NIST)发布征集的新加密算法。2000年10月2日, 由比利时设计者Joan Daemen和Vincent Rijmen设计的Rijndael算法以其优秀的性能和抗攻击能力, 最终赢得了胜利, 成为新一代的加密标准AES。

1.1 Rijndael加密

Rijndael是一个密钥迭代分组密码, 包含了轮变换对状态的重复作用。轮数 N_r 的值取决于分组和密钥的长度。对于AES, 当密钥长度为128比特时, $N_r = 10$; 当密钥长度为192比特时, $N_r = 12$; 当密钥长度为256比特时, $N_r = 14$ 。

Rijndael算法的加密过程如图1所示。它包括一个初始密钥加法, 记作AddRoundKey, 接着进行 $N_r - 1$ 次轮变换(Round), 最后再使用一个轮变换(FinalRound)。

轮变换由4个步骤组成: SubBytes, ShiftRows, MixColumns和AddRoundKey。最后一轮与前 $N_r - 1$ 次轮变换稍有不同, 省掉了其中的MixColumns步骤。

步骤SubBytes是Rijndael算法中唯一的非线性变换——砖匠置换。

步骤ShiftRows是一个字节换位, 它将状态中的行按照不同的偏移量进行循环移位。使第 i 行第 j 位的字节移动到位置 $(j - C_i) \bmod N_b$, 移动偏移量 C_i 的值依赖于 N_b 的取值。其中 N_b = 分组长度/32, 对于AES, N_b 取固定长度4。

步骤MixColumns是作用在状态各列的砖匠置换。

密钥加法AddRoundKey将状态与一个轮密钥进行异

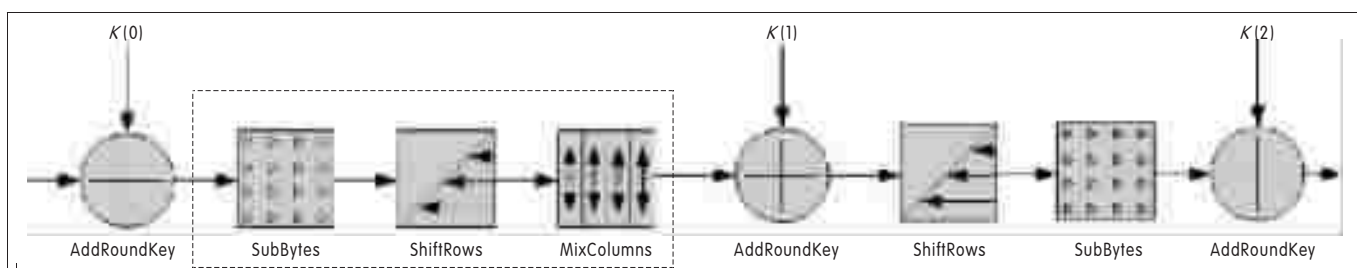


图1 Rijndael算法的加密原理框图(两轮)

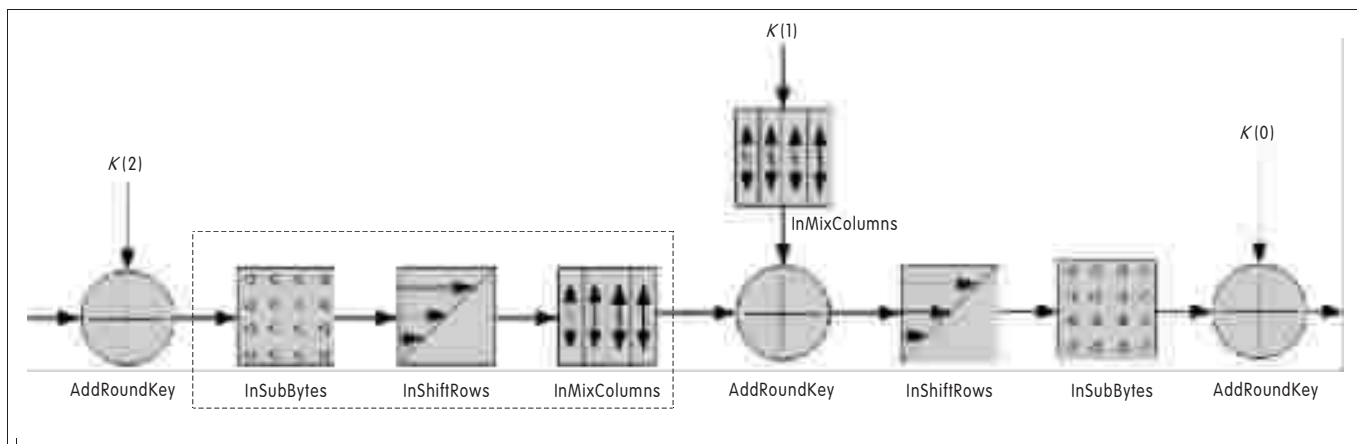


图2 Rijndael算法的等价解密原理框图(两轮)

或。轮密钥是由密码密钥通过密钥编排方案^[1]导出。轮密钥的长度等于分组的长度。

1.2 Rijndael解密

Rijndael解密算法有2种形式。一种是直接解密算法,即直接利用步骤InsubBytes,InvShiftRows,InvMixColumns和AddRoundKey的逆并倒置其次序对数据进行解密。

另一种是等价解密算法,其实现原理如图2所示。等价解密算法有利于有效实现良好的运算次序。

2 基于分支编码本模式的AES保密机制

2.1 AES-OCB加密原理

OCB (Offset Codebook)是802.11健壮安全网络(RSN) AES算法所采用的操作模式。OCB算法使用AES块加密,利用一个临时密钥K和一个随机数(Nonce)完成对数据的保密和完整性检验。

AES-OCB数据加密原理如图3所示。OCB加密算法首先把明文分成m个128比特的数据块,然后分别对m个数据块进行异或、AES加密等运算,生成m个加密数据块,再将m个加密数据块拼接,与重放计数器(Replay Counter)、消息

完整性检验码(MIC)一起作为加密数据负载,完成对明文数据的加密。

如图3所示,分支编码本的值 L_0 可以由密钥K通过对128比特的0字符串进行AES加密运算而获得,其数学表达式为:

$$L_0 = \text{AES_Encrypt}_K(0^{128}) \quad (1)$$

其它分支编码本的值可以由 L_0 通过有限域乘法算出。

在使用OCB模式对数据进行加密的过程中,设备要为每一个加密帧产生一个新的Nonce,用于计算偏移量(Offset)的值:

$$\text{Offset}_0 = \text{AES_Encrypt}_K(\text{Nonce} \oplus L_0) \quad (2)$$

其它偏移量的值可以由 Offset_0 通过递推而得到,其数学表达式为:

$$\text{Offset}_i = \text{Offset}_{i-1} \oplus L_{\text{ntz}(i)} \quad (3)$$

$$\text{加密数据块 } C_i = \text{AES_Encrypt}_K(M_i \oplus \text{Offset}_i) \oplus \text{Offset}_i \quad (4)$$

$$i = 1, 2, \dots, m-1$$

其中, M_i 用来表示第i个明文数据块。

当 $i = m$ 时,

$$Z_m = \text{AES_Encrypt}_K(|M_m| \oplus L_{-1} \oplus \text{Offset}_m) \quad (5)$$

$$C_m = M_m \oplus (\text{the first } |M_m| \text{ bit of } Z_m) \quad (6)$$

其中 $|M_m|$ 表示第m个明文数据块的比特长度。

消息完整性检验码

$MIC = AES_Encrypt_K$

$$(M_1 \oplus M_2 \cdots \oplus M_{m-1} \oplus Z_m \oplus C_m 0^* \oplus Offset_{m+1}) \quad (7)$$

其中 $C_m 0^*$ 表示将加密数据块 C_m 补0生成一个128比特的数据块。

最后将128比特的消息完整性检验码数据块截断,取前64比特作为输出负载MIC。

2.2 AES-OCB解密原理

AES-OCB数据解密原理如图4所示。其初始化过程与

加密时相同。

明文数据块 M_i 为:

$$M_i = AES_Decrypt_K (C_i \oplus Offset_i) \oplus Offset_i \quad i=1,2,\dots,m-1 \quad (8)$$

当 $i=m$ 时,

$$Z_m = AES_Decrypt_K (|C_m| \oplus L_{-1} \oplus Offset_m) \quad (9)$$

$$M_m = C_m \oplus (\text{the first } |C_m| \text{ bit of } Z_m) \quad (10)$$

其中 $|C_m|$ 表示第 m 个密文数据块的比特长度。

消息解密结束后, MIC 的值可以由解密明文计算出来。将计算出来的 MIC 与接收来的 MIC 进行比较,确定OCB密文是否为真^[3]。

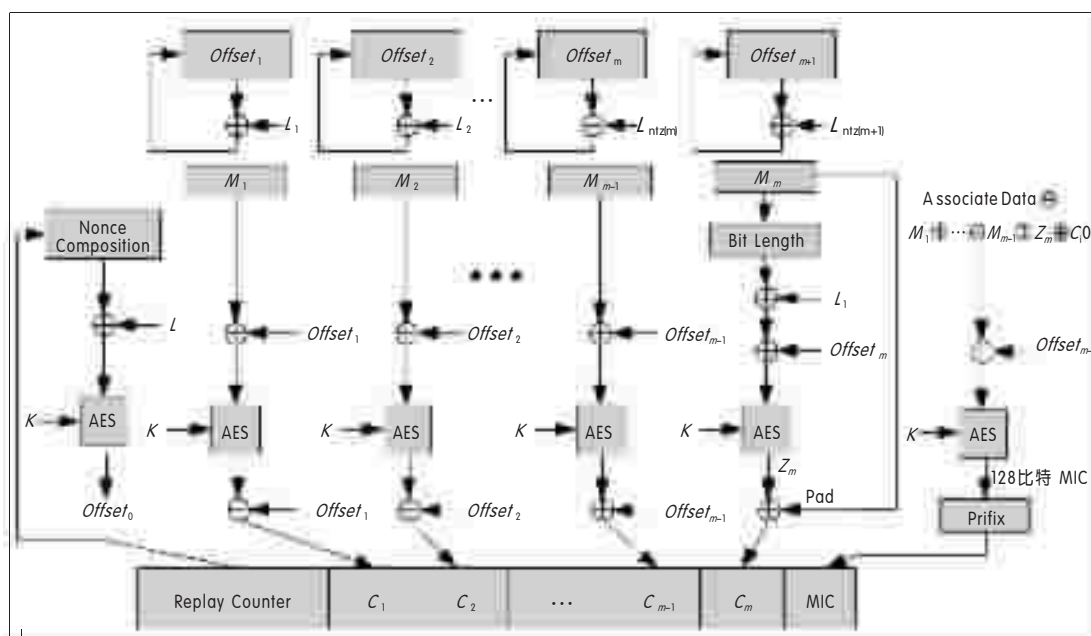


图3 AES-OCB数据加密原理^[2]

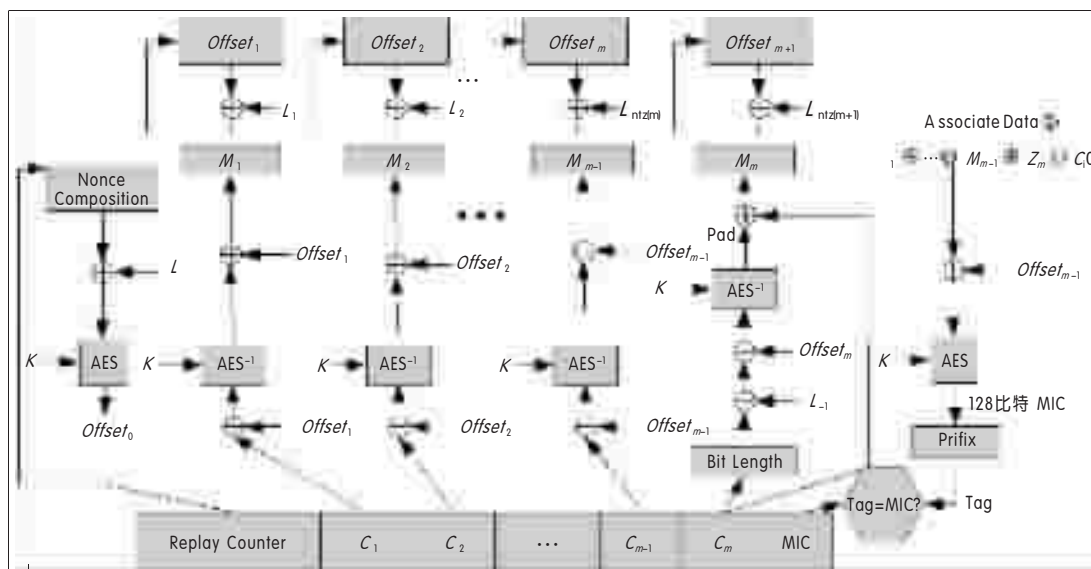


图4 AES-OCB数据解密原理^[2]

3 AES在WLAN中的实现

无线健壮安全认证协议(WRAP)位于802.11重传功能体系结构之上,是一种基于128比特AES OCB模式的加密算法。WRAP的加密过程主要包括三个部分:密钥产生进程、数据封装进程以及数据解封进程。

- 密钥产生进程:通过802.1X协议建立链接,构建临时密钥,然后802.11媒体访问控制(MAC)由联接请求、应答和临时密钥K一起通过密钥产生算法生成加密密钥。

- 数据封装进程:一旦加密密钥被生成,连接状态初始化后,802.11 MAC就会使用WRAP数据封装算法,利用加密密钥对所有即将发送的单MAC服务数据单元

(MSDU, MAC Service Data Unit)进行保护。

- 数据解封进程: 同样, 一旦加密密钥被生成, 连接状态初始化后, 802.11 MAC 就会使用WRAP数据解封算法, 利用加密密钥对所有接收来的单播 MSDU进行解封, 丢弃任何发送端接收来的未经过数据封装算法保护的MSDU。

3.1 WRAP的数据封装过程

WRAP的数据封装过程主要由下面几个步骤构成:

(1) 根据所要发送的MSDU数据选择合适的封装方式

在数据加密之前, 传输端首先要检验所要发送的数据是单播MSDU还是多播/广播MSDU, 从而决定相应设备使用何种方式保护要发送的MSDU。

(2) 递增传输数据分组计数, 选择合适的重放计数器

在选择好封装方式之后, 传输端首先要对所传输的MSDU数据分组个数进行检验。分组个数为:

$$m = \left\lceil \frac{\text{MSDU数据长度}}{\text{AES分组长度}} \right\rceil \quad (11)$$

式中, $\lceil \rceil$ 表示将向上取整, AES分组长度为128比特。

如果将要发送数据分组的个数 m 与已经发送了的数据分组的个数之和大于 2^{48} , 那么密钥就会被认为已经耗尽, 丢弃所有要传输的数据包, 直到原先的密钥被一个新的密钥所取代。

另外, 传输端还要选择一个合适的重放计数器。如果所选重放计数器的值为 $2^{28}-2=268435454$ (或者更大), 那么一个新的有效的Nonce将无法构建, 从而使安全保障失效。在新的密钥到来之前, 发送端不能在该链路或广播/多播通信信道上发送任何MSDU, 数据封装算法也会丢弃所有的数据包。

如果将要发送数据分组的个数 m 与已经发送了的数据分组的个数之和小于 2^{48} , 而且所选重放计数器的值小于 268435454, 那么传输端可以很容易构建出另一个有效的Nonce, 同时将已发送数据分组变量的值加 m , 重复计数器的值加2, 进行下一步操作。

(3) 构造重放计数器字段: 重放计数器占有4个字节的字段长度, 用来传输MSDU序列号。重放计数的主要作用是构造Nonce和检测接收到的MSDU是否被重放。

(4) 构造OCB Nonce:

OCB模式为了保障消息的安全性, 要求用来加密每一条消息的Nonce都是独一无二的。重放计数器、QoS通信类别、MSDU源MAC地址和MSDU目的MAC地址共同作用构成OCB Nonce, 来保证Nonce的唯一性。

(5) 由目的MAC地址构造一个相关的数据分组。

(6) 使用AES-OCB加密算法对MSDU和相关数据进行加密:

设备使用WRAP临时加密密钥 T_k 和Nonce对明文MSDU数据进行加密, 产生两个输出结果:

- 一个OCB加密数据串。该字符串包含的字节数和MSDU明文包含的字节数相同。

- 一个64比特的OCB标识符。

(7) 构造MSDU负载。

3.2 WRAP的数据解封过程

WRAP的数据解封过程主要由下面几个步骤构成:

(1) 根据接收来的MSDU数据选择合适的解封方式

接收端根据发送和接收MAC地址以及KeyID比特值, 为接收来的MSDU选择合适的解封方式。接收地址是广播/多播, 用广播的方式进行解封; 否则, 就用单播的方式进行解封。

(2) 对接收来的MSDU数据进行基本的完整性检验

选择好解封方式后, 对接收来的MSDU负载进行完整性检验, 主要分为两个步骤:

首先检验MSDU负载是否满足15个字节以上的字节长度。如果MSDU负载的长度不够15个字节, 那么接收端就会丢弃该MSDU。MSDU至少包含有3个字节的逻辑链路控制(LLC)头和12个字节的基于协议头字段。

然后检验接收来数据分组的个数:

$$m = \left\lceil \frac{\text{MSDU负载长度}-12}{\text{AES分组长度}} \right\rceil \quad (12)$$

式中, $\lceil \rceil$ 表示向上取整。减去12是考虑到MSDU重放计数器字段和OCB标识符共占有12个字节长度。如果数据分组的个数 m 与WRAP已经接收到的数据分组个数之和大于 2^{48} , 那么接收端将丢弃MSDU。

(3) 从接收来的MSDU数据中提取重放计数器, QoS传输级别, 以及源MAC地址和目的MAC地址的值, 构建OCB Nonce。

(4) 利用构建好了的Nonce和临时密钥对MSDU数据进行解密

MSDU数据的解密是通过Nonce和AES解密密钥的使用来实现的。利用OCB解密算法对MSDU数据进行解密会产生下面两种可能的输出结果:

- 解密成功: 产生一个标识符确认, 解密明文。
- 解密失败: 解密算法检测到MSDU数据发生了改变,

表1 几种攻击方法及其相应的时间和空间复杂度^[5]

攻击方法	攻击轮数	选择明文量	时间复杂度
Square攻击	4	2^9	$2^9 \sim 2^9$
	5	2^{11}	$2^{39} \sim 2^{40}$
	6	2^{32}	$2^{71} \sim 2^{72}$
不可能差分攻击	5	$2^{29.5}$	2^{71}
密钥相关攻击	5	2^{11}	2^{31}
	6	2^{32}	2^{63}
部分和攻击	6	6×2^{32}	2^{44}
	7	$9 \times 2^{32} \sim 21 \times 2^{32}$	$2^{155} \sim 2^{152}$
		$2^{128} \sim 2^{119}$	2^{120}
	8	$2^{128} \sim 2^{119}$	$2^{188} \sim 2^{204}$
	9	2^{85}	2^{224}
冲突攻击	7	2^{32}	2^{140}

丢弃该MSDU。

(5) 单播重放检验

如果接收到的数据帧是单播MSDU,那么接收端就要判断它是一个新帧还是一个重放。如果接收到的数据是多播/广播MSDU,那么接收端就跳过这一步。

重放保护的功能通过对MSDU序列号的检验来实现。若<QoS-Service-Class, SeqNum>对在有效的MSDU中没有作为上下文密钥出现过的话,接收该MSDU;否则,将该MSDU丢弃。

(6) 完成接收

如果接收来的MSDU没有因为上述原因被丢弃,那么接收端将已经接收数据分组(RecvdBlocks)计数器的值加m,整个解密过程完成。

4 AES算法的攻击分析

不管是从学术和理论的角度,还是从实际角度来看,目前尚未存在对Rijndael算法完整版的成功攻击,但提出了几种对Rijndael简化算法的攻击方法。其中最主要的攻击算法是L. Knudsen提出的Square攻击^[4],在混合步骤Mix-Column中的列具有最大分支数,而且字节换位ShiftRows提供最佳扩散性的前提条件下,它对4到6轮的Rijndael简化版本有效。其思想是利用第4轮字节替换前后平衡性的改变来猜测密钥字节。文献[5]中作者在667 MHz奔腾Ⅲ上对4轮Rijndael简化算法实现Square攻击,耗时仅为100 ms。通过对4轮Rijndael简化算法进行初始和末尾扩展可以将攻击扩展到6轮。

N. Ferguson等在文献[6]中提出的Herds攻击将Square攻击更进一步扩展到了8轮,它需要 $2^{128} \sim 2^{119}$ 个选择明文和

2^{104} 比特的存储空间。它不适用于128比特密钥的情况;对于192比特密钥的情况,工作因子相当于 2^{188} 次密码运算;对于256比特密钥的情况,其工作因子相当于 2^{204} 次密码运算。

H. Gilbert和M. Minier开发的四轮区分器,也将对Rijndael简化算法的攻击提高到了7轮。它只适用于128比特的密钥情形,攻击复杂度大约相当于 2^{192} 次密码轮变换。

通过发掘密码设计的其它弱点,采用新的攻击技术,还发展出了一些其它的针对Rijndael简化算法的攻击方法。如密钥相关攻击、部分和攻击、冲突攻击等。表1列出了一些攻击方法及其相应的时间和空间复杂度。

5 结束语

作为一种全新的高级加密标准,AES加密算法采用对称的块加密技术,提供比WEP/TKIP中RC4算法更高的加密性能,它将在IEEE 802.11i最终确认后,成为取代WEP的新一代的加密技术,为无线网络带来更强大的安全防护。

6 参考文献

- [1] Joan Daemen, Vicent Rijmen. 高级加密标准(AES)算法——Rijndael的设计[M]. 谷大武,徐胜波译.北京:清华大学出版社,2003.
- [2] IEEE 802 Committee of the IEEE Computer Society. 802.11i Draft[S].
- [3] Phillip Rogaway. Proposal to NIST for a Block-cipher Mode of Operation which Simultaneously Provides Privacy and authenticity[DB/OL]. <http://www.cs.ucdavis.edu/~rogaway/ocb/ocb.pdf>, 2001-04.
- [4] Daemen J, Knudsen L R, Rijmen V. The Block Cipher Square. In: Biham E, eds. Fast Software Encryption '97, LNCS 1267 [C], Springer-Verlag, 1997:68-87.
- [5] Wei Baodian, Liu Dongsu, Wang Xinmei. The Principle, Implementation and Cryptanalysis of AES Algorithm Rijndael [J]. Communications Technology. 2002(12).
- [6] Ferguson N, Kelsey J, Schneier B, et al. Improved Cryptanalysis of Rijndael. In: Schneier B, eds. Fast Software Encryption 2000, LNCS 1978[C], Springer-Verlag, 2001:213-231.

收稿日期:2004-03-08

作者简介:

刘永元,西安电子科技大学ISN国家重点实验室在读硕士研究生。主要从事无线通信,网络安全方面的研究。

张联峰,毕业于西安电子科技大学,硕士。现为中兴通讯3G平台研发工程师。主要从事无线通信,网络安全方面的研究。

刘乃安,西安电子科技大学ISN国家重点实验室,副教授。撰写并发表论文二十余篇,出版教材和著作四本,译著一本。从事自然科学基金、国家高科技计划“863”及中外合作项目多项。主要从事移动计算网络、扩展频谱通信、无线通信和移动通信研究。

广告索引

A1:《中兴通讯技术》杂志
A2:《信息网络》杂志
A3:《电信网技术》杂志
A4:《中国电信业》杂志
A5:《电信工程技术与标准化》杂志
封底:中兴通讯股份有限公司