研究报告

基于双重分组和密钥计数的并行认证模式

黄玉划，胡爱群，宋宇波
（东南大学信息安全研究中心，南京 210096）

[摘要] 由于 CBC－MAC 模式不可并行处理，提出了一种基于双重分组的并行认证模式（PKCB）。PKCB 模式同并行认证模式 PMAC 相比，安全性和速率都有显著提高，PKCB 认证模式与 CTR（计数器）加密模式结合可构成分组密码算法的一种全工作模式。在此基础上提出了一种基于密钥计数的并行认证模式（KCTR－MAC）。KCTR－MAC 模式安全性比 PMAC 模式高得多，而速率未降低，KCTR－MAC 认证模式和 CTR 加密模式结合也可构成分组密码算法的一种全工作模式（2CTR），2CTR 模式的综合性能不亚于标准模式 CCM（CTR with CBC－MAC），是一种安全快速的实用模式。

[关键词] 认证模式；CBC－MAC 模式；PMAC 模式；CTR 模式；CCM 模式
[中图分类号] TN918，TP309 [文献标识码] A [文章编号] 1009－1742（2004）07－0070－05

1 引言

对称密钥算法分为序列密码算法和分组密码算法。分组密码算法的主要优势是可并行处理。由于分组密码算法本身只定义了将一个分组明文加密成密文的变换，而实际应用中要加密和认证的数据长度远远大于一个分组，这就需要为分组密码算法选择工作模式，避免采用固定格式带来的安全隐患[1]。笔者主要讨论认证模式。

在 128 MB 内存环境下，AES（Rijndael）算法[2]的速率约为 50～70 Mb/s；而 MD5 算法[3]的速率将近 120 Mb/s，SHA1[4]，SHA256[5]的速率可达 80 Mb/s。也就是说，由 AES 构成的 CBC－MAC 算法[6]速率低于常用散列函数。CBC－MAC 有很多变体，实质上只是增加了一些进程，例如 XCBC－MAC[7]和 RMAC[8]，其综合性能和 CBC－MAC 差不多。

R. Housley 等提出的 CCM（CTR with CBC－MAC）模式[9]是分组密码算法的一个标准工作模式。CCM 分别采用 CTR 和 CBC－MAC 作为加密和认证模式；IEEE802.15.3（WPAN）已经采用 CCM 模式，IPSec 考虑采用 CTR 模式，HP 支持 CBC－MAC 模式[1]。

CTR（计数器）模式[10]是个性能很好的模式。CCM 模式的主要缺点是采用 CBC－MAC 模式作为认证模式，不可并行处理，这使得 CTR 模式的速率优势化为乌有。笔者主要从这方面进行改进。

现有的并行认证模式主要是 P. Rogaway 提出的 PMAC（并行 MAC）模式[11]。

2 CCM 模式简介

CTR 模式包含 CTR 模式和 CBC－MAC 模式。

2.1 CCM 的加密模式——CTR（计数器）模式

定义 $C = E_K(P)$ 表示用密钥 K 把明文 P 加密成密文 C，$P = D_K(C)$ 表示用密钥 K 把密文 C 解密成明文 P；假设单个分组长度为 T 位，明文分组为 $P_1, \cdots, P_n$；密文分组为 $C_1, \cdots, C_n$；最后一组明文

[收稿日期] 2003－07－10；修回日期 2003－11－09
[基金项目] “八六三”高技术计划资助项目（2002AA143010；2003AA143040）
[作者简介] 黄玉划（1975－），男，江西高安市人，东南大学无线电工程系博士生

长度为 τ 位，信息认证码（MAC）长度为 m 位。

CTR 模式是由 Diffie 和 Hellman 于 1979 年提出的，加州大学的 P. Rogaway 等强烈推荐此模式为标准[12]，现已发展成标准加密模式之一[1]，其算法过程为[1, 10, 12]：

for $i = 1$ to n do { $\mathrm{IV}_i = \mathrm{IV} + i$;

$S_i = E_K(\mathrm{IV}_i)$;}（可预处理）

（初始向量 IV 一般为计数器，或为不重复的伪随机数，IV_i 可扩展至所需长度）

for $i = 1$ to $n-1$ do $C_i = P_i \oplus S_i$;

$C_n = P_n \oplus \mathrm{MSB}_\tau(S_n)$;（加密）

for $i = 1$ to $n-1$ do $P_i = C_i \oplus S_i$;

$P_n = C_n \oplus \mathrm{MSB}_\tau(S_n)$;（解密）

其中，$\mathrm{MSB}_\tau(S_n)$ 表示截取 S_n 的前 τ 位。由上述算法可知，CTR 模式是通过将明（密）文同密码流相异或进行加（解）密的。因此，CTR 模式没有完整性[12]，只能作为加密模式，不能同时作为认证模式。

2.2 CCM 的认证模式——CBC－MAC 模式

CBC（密码分组链接）模式算法为[13~15]：

for $i = 1$ to n do $Y_i = E_K(P_i \oplus Y_{i-1})$;

（Y_0 一般为计数器，或为不重复的伪随机数）

$Y_n = E_{K_1}(Y_n)$;（可选进程）

$\mathrm{MAC} = \mathrm{MSB}_m(Y_n)$;

当最后一组明文长度 τ 小于分组长度 T 时，可采用补位或密文挪用等措施。当 $m = T$ 时，一般要采用可选进程，以减轻穷举攻击的威胁。CBC 模式既可作为加密模式，又可作为认证模式，还可同时实现加密和认证。当 CBC 模式同时作为加密和认证模式时，需要采用可选进程。CBC 模式作为认证模式时称为 CBC－MAC 模式[13~15]。

3 基于双重分组的并行认证模式及其与 PMAC 模式的性能比较

3.1 基于双重分组的并行认证模式（PKCB）

双重分组思想最初是用来构造散列长度为分组长度 2 倍的单向散列函数，然而这些方案已被证明是不安全的[14, 15]。不过，双重分组思想用来构造快速认证模式还是可取的。

以 AES 为例。众所周知，FIPS 197[16]定义的 AES 算法的分组长度为 16 B，密钥长度可以是 16 B，24 B 或 32 B，而密钥长度为 32 B 的算法速率只比密钥长度为 16 B 的略慢一些。当然，Rijndael 算法[17]本身定义的分组长度也可以是 16 B，24 B 或 32 B[1]。利用这一特点，可以得到一个串行速率约为 CBC－MAC 的 2～3 倍的并行模式。首先把明文按 48 B（40 B 或 32 B）分成 n 组：M_1，…，M_n。如果最后一组明文长度小于 48 B（40 B 或 32 B），可采用补位或密文挪用等措施。每组又分为 2 组：P_{i1}，P_{i2}。不妨令 P_{i1} 为 16 B，P_{i2} 为 32 B（24 B 或 16 B）。则并行算法为：

for $i = 1$ to n do {$\mathrm{IV}_i = i \parallel \mathrm{IV}$;

（初始向量 IV 一般为计数器，或为不重复的伪随机数，$\parallel$ 表示串联）

$K_i = P_{i2} \oplus \mathrm{IV}_i$;

（明文当密钥，不能作为加密模式，IV_i 可扩展至所需长度）

$Y_i = E_{K_i}(P_{i1})$;}

$Y_n = E_{K_A}(Y_n)$;（可选进程，K_A 可与 K 相同）

$\Sigma = \bigoplus_{i=1}^{n} Y_i$;$\mathrm{MAC} = \mathrm{MSB}_m[E_K(\Sigma)]$;

该并行模式的思路是部分明文当密钥，可称为 PKCB（并行密钥密码分组）模式。在 128 MB 内存环境下，AES－PKCB 算法的串行速率可达 140～170 Mb/s，比常用散列函数快。PKCB（并行双重分组）模式在思想上与 P. Rogaway 提出的 PMAC（并行 MAC）模式[11]有类似之处，不过 PKCB 模式对明文进行双重分组，计算量约为 PMAC 模式的 1/2～1/3。

3.2 PMAC 模式

PMAC 是 P. Rogaway 提出的并行认证模式[11]。该模式用到了 GF（2^n）域，以 $n = 128$ 为例。不可约多项式为

$$p_{128}(x) = x^{128} + x^7 + x^2 + x + 1$$

定义 $a(x) + b(x) = a(x) \oplus b(x)$，

$$a(x)\, b(x) = [a(x) \odot b(x)] \bmod p_{128}(x),$$

$\odot$ 表示模乘，$\mathrm{ntz}(i)$ 表示二进制数 i 从右边数连 0 的个数，$f(L, i)$ 表示 $L \odot x^i$，$|P|$ 表示取输入信息 P 的位数，γ_0，…，γ_{2^n-1} 是相邻码元相差 1 位的格雷编码，且 $\gamma_0 = 0$，则 $\gamma_i \odot L = (\gamma_{i-1} \odot L) \oplus L[\mathrm{ntz}(i)]$。PMAC 模式的算法过程为[11, 12]：

$L = E_K(0)$;

for $i = 1$ to $n-1$ do { $Z_i = \gamma_i \odot L$;

$Y_i = E_K(P_i \oplus Z_i)$;}

if $|P_n| = T$ then $Y_n = P_n \oplus L \odot x^{-1}$;

else $Y_n = P_n 10^{T-|P_n|-1}$;（0* 表示用 0 补位）

$\Sigma = \bigoplus_{i=1}^{n} Y_i$;$\mathrm{MAC} = \mathrm{MSB}_m[E_K(\Sigma)]$。

3.3 PMAC模式的安全性

PMAC模式是一种高效的并行认证模式，安全性较高。

分析认证模式的安全性必须结合加密模式。假设分组密码算法分别采用CTR和PMAC作为加密和认证模式。

令 $\delta_{ij} = Z_i \oplus Z_j, \Delta_{ij} = S_i \oplus S_j \oplus \delta_{ij}$；

$$C_i^* = C_j \oplus \Delta_{ij},$$

$C_j^* = C_i \oplus \Delta_{ij}$（密文差分互换）。

解密得 $P_i^* = C_i^* \oplus S_i = P_j \oplus \delta_{ij}$，

$$P_j^* = C_j^* \oplus S_j = P_i \oplus \delta_{ij},$$

则 $Y_i^* = E_K(P_i^* \oplus Z_i) = Y_j$，

$$Y_j^* = E_K(P_j^* \oplus Z_j) = Y_i。$$

即密文差分互换后MAC值不变。

虽然 Δ_{ij} 是个伪随机数，但任意2组密文（最后一组或最后2组除外）满足线性差分互换关系，是其不足之处。因此，PMAC模式的安全性明显低于CBC－MAC。假设PMAC模式中密文篡改成功的概率为 P_{PMAC}。

3.4 PKCB认证模式的安全性

假设分组密码算法分别采用CTR和PKCB作为加密和认证模式，不管可选进程，以AES－128为例，$P_{2i-1} = P_{i1}, P_{2i} = P_{i2}$。

令 $\Delta_{2i-1,2j-1} = S_{2i-1} \oplus S_{2j-1}$，

$\Delta_{2i,2j} = S_{2i} \oplus S_{2j} \oplus i \oplus j$，$\delta_{ij} = i \oplus j$，

$$C_{2i-1}^* = C_{2j-1} \oplus \Delta_{2i-1,2j-1},$$

$$C_{2j-1}^* = C_{2i-1} \oplus \Delta_{2i-1,2j-1},$$

$$C_{2i}^* = C_{2j} \oplus \Delta_{2i,2j},$$

$C_{2j}^* = C_{2i} \oplus \Delta_{2i,2j}$（密文差分互换），

解密得

$$P_{2i-1}^* = C_{2i-1}^* \oplus S_{2i-1}^* = P_{2j-1},$$

$$P_{2j-1}^* = C_{2j-1}^* \oplus S_{2j-1}^* = P_{2i-1},$$

$$P_{2i}^* = C_{2i}^* \oplus S_{2i}^* = P_{2j} \oplus \delta_{ij},$$

$$P_{2j}^* = C_{2j}^* \oplus S_{2j}^* = P_{2i} \oplus \delta_{ij},$$

则 $K_i^* = P_{2i}^* \oplus \mathrm{IV}_i = K_j$，

$$K_j^* = P_{2j}^* \oplus \mathrm{IV}_j = K_i,$$

$$Y_i^* = E_{K_i^*}(P_{2i-1}^*) = Y_j,$$

$$Y_j^* = E_{K_j^*}(P_{2j-1}^*) = Y_i。$$

也就是说，要同时猜测2个伪随机数 $\Delta_{2i,2j}$ 和 $\Delta_{2i-1,2j-1}$，才能确保密文篡改成功。因此，PKCB认证模式采用AES－128算法时密文篡改成功的概率约为 $P_{\mathrm{PKCB}} = P_{\mathrm{PMAC}}^2$。类似地，可求得采用AES－192算法时密文篡改成功的概率约为 $P_{\mathrm{PKCB}} = P_{\mathrm{PMAC}}^{2.5}$；采用AES－256算法时密文篡改成功的概率约为 $P_{\mathrm{PKCB}} = P_{\mathrm{PMAC}}^3$。由此可以说明，PKCB与PMAC算法相比，安全性和速率都有显著提高。

4 计数器认证模式及其与PMAC，PKCB模式的性能比较

4.1 计数器认证模式（KCTR－MAC）

由于CTR模式是纯加密模式，不能同时作为认证模式，可将它改造成认证模式（如果最后一组明文长度小于分组长度，可采用补位或密文挪用等措施）：

for $i = 1$ to n do { $\mathrm{IV}_i = i \,||\, \mathrm{IV}$;

（IV为计数器，或为不重复的伪随机数）

$K_i = K \oplus \mathrm{IV}_i$;

（可预处理，IV_i 可扩展至所需长度）

$Y_i = E_{K_i}(P_i)$;}

$Y_n = E_{K_A}(Y_n)$;（可选进程）

$\sigma = \bigoplus_{i=1}^{n} Y_i$

（密文可互换，不能同时作为加密模式）

$\Sigma = E_K(\sigma)$;

$\mathrm{MAC} = \mathrm{MSB}_m(\Sigma)$;

该模式只能作为认证模式，采用密钥计数思想，可称为密钥计数认证（KCTR－MAC）模式。CBC－MAC算法采用相同密钥加密，而KCTR－MAC算法采用变密钥加密，因此，KCTR－MAC模式的安全性更高些。KCTR－MAC模式描述比PMAC模式简单，但KCTR－MAC模式需进行多次密钥编排（可预处理），计算量和PMAC模式差不多。

4.2 KCTR－MAC模式的安全性

由于CTR加密模式是通过将明（密）文同密码流相异或进行加（解）密的，而PMAC和PKCB认证模式又有一定的差分线性，这样就可通过密文差分互换实现明文差分互换，而MAC值不变。

假设分组密码算法分别采用CTR和KCTR－MAC作为加密和认证模式。KCTR－MAC模式对不同顺序的明文采用不同的密钥进行处理，即采用密钥计数方式对数据进行定位，可以抵抗密文的增删和互换攻击。虽然密钥的计数是线性的，但经过

加密算法的非线性处理，数据的偏移不存在差分线性关系，可以抵抗密文差分互换攻击。虽然 PKCB 认证模式也采用不同的密钥对不同顺序的明文进行处理，但引入部分明文当密钥，可通过修改数据控制密钥。因此，KCTR－MAC 模式的安全性比 PMAC 和 PKCB 模式高。不过，KCTR－MAC 模式不能与相同的加密模式共存（PMAC 模式也不能与相同的加密模式共存）。

PMAC 模式中的伪随机序列 Z_i 实质上是计数值的伪随机变换；PMAC 模式实质上也是一种计数器模式。因此，KCTR－MAC 模式是 PMAC 模式的改进模式。当然，也可把 PMAC 模式中的伪随机序列 Z_i 引入到 KCTR－MAC 模式中，以增强复杂度；这样需增加存储空间以便预处理。

KCTR－MAC 算法是陷门单向函数，不能作为无陷门单向散列函数，可采用它来构造并行的无陷门单向散列函数。另外，KCTR－MAC 模式可扩展为同时实现加密和认证的全工作模式。

5　CCM 并行模式

CCM 模式[18~21]把 CTR 和 CBC－MAC 有机结合，前者用于加密，而后者用于认证。该模式在不少地方已被标准化[1]。CTR 模式是个性能很好的模式，但 CBC－MAC 模式不可并行处理，这使得 CTR 模式的速率优势荡然无存。

5.1　CCM 并行模式 1（CTR with PKCB－MAC）

将 PKCB 认证模式与 CTR 加密模式结合构成分组密码算法的一种全工作模式，称为 CPK 模式。CPK 模式加解密和认证都可并行处理，但安全性明显低于 CCM 模式。

5.2　CCM 并行模式 2（2CTR）

KCTR－MAC 只能作为认证模式，而 CTR 只能作为加密模式，将 KCTR－MAC 与 CTR 结合构成分组密码算法的一种全工作模式，称为 2CTR（双计数器）模式。2CTR（CTR with KCTR－MAC）模式与 CCM 模式相比，安全性未降低，至少未明显降低，而加解密和认证都可并行处理，因此，2CTR 模式的综合性能不亚于标准模式 CCM。

6　结语

笔者给出了一种基于双重分组的并行认证模式（PKCB）；PKCB 模式与 PMAC 模式相比，安全性和速率都有显著提高；PKCB 认证模式与 CTR 加密模式结合可构成分组密码算法的一种全工作模式（CPK）；CPM 模式加解密和认证都可并行处理，但安全性明显低于 CCM 模式。在此基础上给出了一种基于密钥计数的并行认证模式（KCTR－MAC）；KCTR－MAC 模式安全性比 PMAC 模式高得多，而速率未降低；KCTR－MAC 认证模式和 CTR 加密模式结合也可构成分组密码算法的一种全工作模式（2CTR）；2CTR 模式解决了 CCM 认证（CBC－MAC）不可并行处理的问题。2 种新工作模式描述简单，便于性能评估，其中 2CTR 模式的综合性能不亚于标准模式 CCM。

参考文献

[1] 耿　嘉. 无线局域网中加密技术的研究 [D]. 南京：东南大学，2002

[2] Gladman B. A specification for Rijndael, the AES algorithm (V3.3) [EB/OL]. http://fp.gladman.plus.com/cryptography-technology/rijndael/aesspec.pdf, 2002

[3] Touch J. Report on MD5 Performance [EB/OL]. RFC1810, http://www.china-pub.com/computers/emook/aboutemook.htm, 1995

[4] NIST. Secure Hash Standard [S]. FIPS 180－1, 1995

[5] NIST. Secure Hash Standard [S]. FIPS 180－2, 2002

[6] ISO/IEC/JTC 1/SC 27. Information processing — modes of operation for a 64 bit block cipher algorithm [S]. ISO8372, http://www.eos.org.eg/web-en/cat/items/d15530.html, 1987

[7] Black J, Rogaway P. XCBC MAC [EB/OL]. http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/, 2001

[8] Jaulmes E, Joux A, Valette F. RMAC [EB/OL]. http://csrc.nist.gov/CryptoToolkit/modes/, 2001

[9] Housley R, Whiting D, Ferguson N. CCM: AES Mode of Operation [EB/OL]. http://csrc.nist.gov/encryption/modes/proposedmodes/, 2002

[10] Lipmaa H, Rogaway P, Wagner D. CTR Mode Encryption [EB/OL]. http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/, 2001

[11] Rogaway P, Black J. PMAC [EB/OL]. http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/, 2001

[12] 吴文玲. 简评 AES 工作模式 [J]. 中国科学院研究生院学报，2002，19(3)：324～333

[13] Stinson D R. 密码学原理与实践(第二版) [M]. 冯登国译. 北京：电子工业出版社，2003

[14] 王育民，刘建伟. 通信网的安全——理论与技术[M]. 西安：西安电子科技大学出版社，1999

[15] Schneier B. 应用密码学——协议、算法与C源程序[M]. 吴世忠. 北京：机械工业出版社，2000

[16] NIST. Announcing the AES [S]. FIPS 197, http://csrc. ncsl. nist. gov/publications/fips/fips197/fips - 197.pdf, 2001

[17] Daemen J, Rijmen V. AES Proposal: Rijndael (V2) [EB/OL]. http://csrc. nist. gov/encryption/aes/rijndael/Rijndael.pdf, 1999

[18] Walker J. Proposed TGi D1. 8 Clause 8 Editing Changes [EB/OL]. IEEE802.11 - 02/178r0, http://grouper.ieee.org/groups/802/11/Reports/tgi-update.htm, 2002

[19] Letanche O, Stanley D. Proposed Tgi D2.2 Clause 8 AES - CCM text [EB/OL]. IEEE802. 11 - 02/144r4, http://grouper. ieee. org/groups/802/11/Reports/tgi-update.htm, 2002

[20] Whiting D, Housley R, Ferguson N. AES Encryption & Authentication Using CCM Mode [EB/OL]. IEEE802. 11 - 02/001r2, http://grouper. ieee. org/groups/802/11/Reports/tgi-update.htm, 2002

[21] Tgi. WLAN Enhanced Security [EB/OL]. IEEE P802. 11i/D3. 0, http://grouper. ieee. org/groups/802/11/Reports/tgi-update.htm, 2002

Parallel Authentication Modes Based on Double Blocks or Key Counter

Huang Yuhua, Hu Aiqun, Song Yubo

(*Research Center of Information Security, Southeast University, Nanjing* 210096, *China*)

[**Abstract**] The CBC - MAC mode is not a parallel one. A parallel authentication mode (PKCB) based on double blocks was put forward in this paper. The PKCB mode had a marked improvement on security & speed over parallel authentication mode, PMAC. And it may be combined with the CTR (counter) encryption mode to form a full block cipher mode. On this ground, another parallel authentication mode (KCTR - MAC) based on key counter was advanced. As compared with the PMAC mode, the KCTR - MAC mode had a marked improvement on security, while its speed did not become lower. The KCTR - MAC authentication mode may be combined with the CTR (counter) encryption mode to form a full block cipher mode (2CTR), too. The 2CTR mode had a performance advantage over the standard mode, CCM (CTR with CBC - MAC). And it was a fast, practicable mode with security.

[**Key words**] authentication mode; CBC - MAC mode; PMAC mode; CTR mode; CCM mode