基于广义猫映射的组播密钥管理方案研究*)

杨 军[1] 覃伯平[2] 雷开彬[1]

(西南民族大学计算机科学与技术学院 成都 610041)[1] (北京理工大学 北京 100081)[2]

摘 要 为处理组密钥管理中的"1影响n问题",曹国梁等人提出了组密钥与个体密钥之间存在广义猫映射关系的组播加密算法及其密钥管理方案。我们进一步分析其密码强度、前向/后向保密性和可扩展性问题。解析结果表明:对已知明文攻击的脆弱性使该密码不适合提供组播数据保密性安全服务;通信开销以组规模为渐近下界,使该方案不满足大型组播组中密钥管理低带宽开销的QoS要求。分析方法对其他密码算法转化为组密钥更新协议的研究亦有积极作用。

关键词 组播安全,组密钥管理,广义猫映射,对称密钥分组密码,穷举密码分析

Study of a Multicast Key Management Scheme Based on the Generalized Cat Map

YANG Jun[1] QIN Bo-Ping[2] LEI Kai-Bin[1]

(College of Computer Science and Technology, Southwest University for Nationalities, Chengdu 610041)[1]

(Beijing Institute of Technology, Beijing 100081)[2]

Abstract Aiming to deal with "the 1-affects-n problem" in group key management, a multicast encryption algorithm and its corresponding key management scheme where there is a relation of the generalized cat map between the group key and individual keys were proposed by Cao et al.. We further analyze the cipher strength, forward /backward secrecy and scalability problems. The analytical results demonstrate that the cipher is not suitable to provide the security service of multicast data confidentiality due to its vulnerability to the known-plaintext attack, and the scheme does not meet the QoS requirement of low bandwidth overhead for key management in a large multicast group because the group size is an asymptotic lower bound for the communication overhead. The analytical methods will also have positive effect on the research into converting other encryption algorithms into group rekeying protocols.

Keywords Multicast security, Group key management, Generalized cat map, Symmetric-key block cipher, Exhaustive cryptanalysis

1 引言

组播是下一代Internet应用的重要支撑技术,而组播的安全性是成功部署组通信应用所必须解决的重要课题之一。为提供组播数据的组访问控制、保密性及组认证,基本的安全挑战围绕可扩展、安全和可靠的组密钥管理(Group Key Management,GKM)[1,2]。已有研究表明,不存在一个万能的GKM方案满足各种应用的安全需求。现有的GKM解决方案可分为两大类[2]:共享TEK法和独立子组TEK法(组密钥也称为业务加密密钥(Traffic Encryption Key,TEK))。在第一类方法中,所有组成员共享一个组密钥。这种单一密钥的管理按体系结构分为三个子类:集中式、分散式和分布式。其中,集中式方案还可进一步分为两两密钥(Pairwise Keys)、广播秘密(Broadcast Secrets,如Secure Lock)及密钥层次(Keys Hierarchy,如LKH)。共享TEK法的一个共同缺点是"1影响n问题"。为缓解该问题,第二类方法不采用整体的组密钥而把组成员分成若干子组,每个子组拥有它自己独立的TEK。如Iolus[1,2]、Chiu等人[3]利用单向ElGamal代理加密的安全组播方案。独立子组TEK法的局限性包括数据转换增加数据包传送的延迟及可信第三方问题等。

在基于星形密钥图模型[4]的传统两两密钥管理方案(如[2,5]GKMP,Proovendran等人方案、Dunigan-Cao协议、Chu等人协议、Canetti等人的最小存储方案)中,因组密钥与个体密钥之间尚未建立函数关系,当有成员离开时,只能采用多次的安全单播(或组播一条组合在一起的加密消息[4])进行组密钥更新,故其通信开销都随组规模线性增长,缺乏可扩展性。另一方面,在组密钥与密钥加密密钥(Key Encryption Keys,KEKs)之间引入某种有效的函数关系来构造密钥更新消息,确为GKM研究的一条重要途径(如OFT,OFC,嵌套加密)[1~6],但安全性等问题需深入研究。

2003年,马等人[7]在研究图像加密系统时,把猫映射推广成广义猫映射。2005年,曹等人[8]利用其中一种广义猫映射的矩阵,选择特殊的模数$m=2^n(n\geq 128)$,构造了一种n比特分组对称密码(简称C密码),用于提供组播数据保密性安全服务,同时提出与C密码配套使用的两两密钥管理方案(简称C方案)。由于在组密钥与各个个体密钥之间建立了一种新型的函数关系,该方案区别于所有传统两两密钥管理方案的特点是:密钥服务器采用组播方式公开发送一条密钥更新消息,让每个合法组成员利用自己的个体密钥(素数)来计算新的组密钥。但尚未严格论证其密码强度以及是否满足

*)国家自然科学基金资助(编号:60573050)。杨 军 副教授,博士研究生,主研方向:信息安全、应用密码学和组密钥管理;覃伯平 博士后,主研方向:计算机应用技术、网络安全和传感器网络;雷开彬 副教授,硕士,主研方向:计算机图形学和计算机辅助几何设计。

GKM的特有要求、如可扩展性。在概述C密码和C方案的基础上(第2节),我们在第3节比较它们与Hill密码在安全方面的一些相似性和特性;通过考察一切素数在既约剩余系$\{1,3,5,\cdots,m-1\}$上的平均分布情况,确定C密码的密钥空间大小;揭示C密码解密充要条件与C方案中前向/后向保密性的关系,并由此提出一种密钥组合攻击方法;通过刻画影子密钥概念,研究个体密钥在模运算下的同余碰撞问题;对C密码的已知明文攻击以及C方案在大型组播通信中的应用可行性分析。最后给出全文总结。

2 C密码及C方案:简要回顾

2.1 C密码

对给定的$m\in N=\{1,2,3,\cdots\}$,记剩余类环$Z_m=\{0,1,\cdots,m-1\}$。一个广义猫映射[7]是由满足条件$\det D=1$的矩阵$D=\begin{pmatrix}a & b\\ c & d\end{pmatrix}(a,b,c,d\in Z_m)$所确定的一个线性变换:

$\Psi:Z_m\times Z_m\to Z_m\times Z_m$

$(x_1,x_2)\mathrm{a}(y_1,y_2)=(x_1,x_2)D \bmod m$

为把面向点对点通信的广义猫映射推广成一种组播加密算法,曹等人[8]选择明文空间$P=$密文空间$C=Z_m\times Z_m$,并选定模数$m=2^n(n\geqslant 128)$,提出了一种n比特分组密码(简称C密码)。对有w个组成员的安全组播组$U=\{u_1,u_2,\cdots,u_w\}$,密钥空间的选择如下(记$P_m=\{$大于m的一切素数$\}$):

1)任意选取$(a_t,b_t)\in P_m\times P_m(t=1,2,\cdots,w)$满足$\{a_1,a_2,\cdots,a_w\}\cap\{b_1,b_2,\cdots,b_w\}=\varnothing$;

2)$(I_1,I_2)\leftarrow(\prod_{t=1}^{w}a_t,\prod_{t=1}^{w}b_t\}$;

3)$(r_1,r_2)\leftarrow(I_1,I_2) \bmod m$。

所有满足上述条件的序对(r_1,r_2)组成的一个有限集K_1称为种子密钥空间。定义密钥空间

$$K_2=\left\{D=\begin{pmatrix}r_1 & r_1r_2-1\\ 1 & r_2\end{pmatrix} \bmod m:(r_1,r_2)\in K_1\right\}$$

对任意的密钥$D\in K_2$,定义加密变换为

$$(y_1,y_2)=(x_1,x_2)D \bmod m$$

明文单元$(x_1,x_2)\in P$ (1)

解密变换为

$$(x_1,x_2)=(y_1,y_2)D^{-1} \bmod m$$

密文单元$(y_1,y_2)\in C$ (2)

据带余除法,令

$$I_i=mn_i+r_i(0\leqslant r_i<m,i=1,2) \tag{3}$$

各成员计算种子密钥如下:

$$\left\{\begin{array}{l}r_1\leftarrow a_t-(mn_1 \bmod a_t)\\ r_2\leftarrow b_t-(mn_2 \bmod b_t)\end{array}\right\} \tag{4}$$

2.2 C方案

·初始化:假定组控制器和密钥服务器(Group Controller and Key Server,GCKS)与每个用户已完成一对一的互认证及注册过程[1,4],初始的组播组为$U=\{u_1,u_2,\cdots,u_w\}$。用GCKS$\to u:k$表示GCKS通过安全单播通道向组成员u分发密钥素材k;用GCKS$\Rightarrow U:M$表示GCKS以组播方式向U发送明文消息M。GCKS执行如下操作:

1)按照C密码随机地生成w个个体密钥(a_t,b_t),种子密钥(r_1,r_2)及公开消息(n_1,n_2);

2)GCKS$\to u_t:(a_t,b_t),t=1,2,\cdots,w$;

3)GCKS$\to u_1:(r_1,r_2)$,这里假定u_1为请求成为组播源的组成员;

4)GCKS$\Rightarrow U:(n_1,n_2)$。

·成员离开的密钥更新:假定$U=\{u_{i+1},u_{i+2},\cdots,u_w\}$同时离开$U$,新的安全组播组$U'=\{u_1,u_2,\cdots,u_i\}$。对此,GCKS进行如下操作:

1)查询注册表,确定以前所有使用过或泄露过的个体密钥的集合K_0;

2)随机选取秘密的"新鲜因子"

$(a',b')\in P_m\times P_m-K_0$;

3)$(I'_1,I'_2)\leftarrow(a'\prod_{t=1}^{i}a_t,b'\prod_{t=1}^{i}b_t)$;

4)按C密码生成新的种子密钥(r'_1,r'_2)和更新消息(n'_1,n'_2);

5)GCKS$\to u_1:(r'_1,r'_2)$,仍假定u_1为组播源;

6)GCKS$\Rightarrow U:(n'_1,n'_2)$。

·成员加入的密钥更新:类似于离开情形,但首先在步骤1)与2)之间插入一步:为j个新成员生成及分发新的个体密钥$(a_t,b_t),t=w+1,w+2,\cdots,w+j$。然后,步骤3)变为

$(I'_1,I'_2)\leftarrow(a'\prod_{t=1}^{w+j}a_t,b'\prod_{t=1}^{w+j}b_t)$。

3 对C密码及C方案的密码分析

在本节,我们证明C密码及C方案的若干安全性质,分析其弱点及可扩展性等问题。

3.1 种子密钥空间K_1的结构

C密码是一种与Hill密码既有联系也有区别的多表代换密码:C密码把基于Z_{26}上模算术的2阶Hill密码[9]扩大到Z_m上,但其密钥空间K_2仅为线性群$L_2(Z_m)$的一个真子集[10]。对称密码系统的安全需求包括"密钥量要足够大以能抵抗穷举密钥攻击"这一必要条件[11]。易见(r_1,r_2)a D是K_1与K_2之间的一个一一对应,故$|K_1|=|K_2|$,对K_2可归结为对K_1的研究。我们首先建立:

引理1 对给定的$m=2^n$,一切素数的模m剩余平均分布在既约剩余系$\{1,3,5,\cdots,m-1\}$上。

证明:对任意给定的模$m\in N$,环Z_m的乘法群$Z_m^*=\{r\in Z_m:\gcd(r,m)=1\}$也是一组既约剩余系。当$m>2$,由算术数列之素数定理[12],所有的素数平均地分布在$\varphi(m)$个算术数列$(mq+r)_{q=0}^{+\infty}$之中,其中φ为Euler函数,$r\in Z_m^*$。特别地,当$m=2^n$时,一切素数的模m剩余平均分布在$Z_m^*=\{1,3,5,\cdots,m-1\}$上。引理1获证。□

基于引理1,我们建立K_1之结构。

定理1 $K_1=Z_m^*\times Z_m^*$。

证明:为简洁计,用符号"$s\to S$"表示变量s能够遍历(跑遍)集合S。由(3)式的奇偶性,得$K_1\subseteq Z_m^*\times Z_m^*$。还需证明,按C密码生成的余数对$(r_1,r_2)\to Z_m^*\times Z_m^*$即可。由$K_1$的定义,有

$$r_1=((c \bmod m)(a_w \bmod m)) \bmod m \tag{5}$$

这里视$c=a_1a_2\cdots a_{w-1}$为常量。因$\gcd(c,m)=1$,据既约剩余系的遍历性质[12],当变量$q\to Z_m^*$时,有

$$((c \bmod m)q) \bmod m\to Z_m^* \tag{6}$$

与此同时,当$a_w\to P_m$时,由于小于m的素数只有有限个,由引理1知,$a_w \bmod m\to Z_m^*$。接着由(6)及(5)式,即得$r_1\to Z_m^*$。

注意到对给定的m和w,$P_m-\{a_1,a_2,\cdots,a_w\}$仍含无穷多个素数,同理可证,$r_2\to Z_m^*$。综上所述,$(r_1,r_2)\to Z_m^*\times Z_m^*$。

由定理1,C密码的密钥量$|K_2|=|K_1|\geqslant m^2/4=2^{254}$。DES的密钥量为$2^{56}$;AES的密钥量最小为$2^{128}$,最大为$2^{256}$。

因此，C密码能较好地抵抗针对对称密钥系统最有效的攻击[11]——穷举密钥攻击。

3.2 密钥组合攻击及同余碰撞攻击

先看敌手可能利用的C密码解密的充要条件。

定理2 设 $N'=\{2,3,4,\cdots\}$，则在(4)式中以 x,y 为未知量的整数方程组

$$\begin{cases} r_1=x-(mn_1 \bmod x) \\ r_2=y-(mn_2 \bmod y) \end{cases} \tag{7}$$

在 $N'\times N'$ 内的解集 $R=\{(x,y)\in N'\times N': x\mid I_t$ 且 $y\mid I_2\}$，而且 $|R|=(2^w-1)^2$。

证明：由(3)式，组(7)的第一式⇔

$x-r_1=(I_1-r_1) \bmod x=(I_1-r_1)-\lfloor (I_1-r)/x \rfloor x$

$\Leftrightarrow x\mid I_1$，其中 $\lfloor v \rfloor$ 表示不超过 v 的最大整数。

同理可证，组(7)的第二式⇔$x\mid I_2$。接着，

$$|R|=\binom{w}{1}+\binom{w}{2}+\cdots+\binom{w}{w}^2=(2^w-1)^2。$$

定理2既表明了C密码的解密原理(即U的所有个体密钥的集合 $K_U\subset R$)，同时 $|K_U|=w=|R|$ 又揭示了C方案的安全隐患：敌手利用R的任一元素都能计算出种子密钥 (r_1,r_2)。我们称这种穷举密码分析为密钥组合攻击。下面估计其成功的概率。

称整数对 (x,y) 为奇数对，若 x 与 y 同为奇数。定理2启发敌手在格点区域 $(m,mn_1)\times(m,mn_2)$ 中的 $\frac{1}{2}(mn_1-m)\cdot\frac{1}{2}(mn_2-m)$ 个奇数对范围内穷举搜索 R 的 $\binom{w}{1}+\binom{w}{2}+\cdots+\binom{w}{w-1}^2=(2^w-2)^2$ 个元素之一。搜索成功的概率

$$p_1(w)=4(2^w-2)^2/(I_1-r_1-m)(I_2-r_2-m)$$
$$<4^{w+1}/(m^w-2m)^2<(2^{w+1}/(2^{128w}-2^{129}))^2$$

不难证明，函数 $f(x)=2^{x+1}/(2^{128x}-2^{129})$ 在 $[3,+\infty)$ 上单调递减。于是，

$p_1(w)<f^2(3)=1/2^{250}(2^{255}-1)^2=\delta$

(δ 可视为足够小的常数)。上述数学分析表明：尽管C方案不具备严格意义上的前向/后向保密性，但它对上述密钥组合攻击是计算上安全的。

下面考察个体密钥与种子密钥的关系。(5)式蕴涵的结果 $r_1=(\prod_{t=1}^{w}(a_t \bmod m)) \bmod m$ 表明：每个模剩余 $a_t \bmod m$ (记为 $\overline{a_t}$，以下类同)才是个体密钥 a_t 对种子密钥 r_1 的实质性贡献份额。对 r_2 有类似考虑。$(\overline{a_t},\overline{b_t})$ 称为 (a_t,b_t) 的影子密钥。两个密钥称为是同余碰撞的，若其影子密钥重合。例如，$(233,1009) \bmod 2^4=(41,49)=(617,1201) \bmod 2^4$。

定理3 敌手直接利用种子密钥算法(4)式、公开的密钥更新消息 (n'_1,n'_2)、影子密钥以及同余碰撞都不能攻击C方案的前向/后向保密性。

证明：假定 u_t 是被驱除或新加入的成员，其个体密钥为 (a_t,b_t)。

(i)直接攻击：若 u_t 非法利用 (a_t,b_t) 计算 $a_t-(mn'_1 \bmod a_t)$ 及 $b_t-(mn'_1 \bmod b_t)$，试图获取新种子密钥 (r'_1,r'_2)，则由密钥更新算法知 $a_t\square I'_1$ 及 $b_t\square I'_2$，再由定理2，必有 $r'_1\neq a_t-(mn'_1 \bmod a_t)$ 及 $r'_2\neq b_t-(mn' \bmod b_t)$。

(ii)间接攻击1：虽影子密钥 $(\overline{a_t},\overline{b_t})$，$(r'_1,r'_2)$ 都同在 $Z_m^*\times Z_m^*$ 之内，但据定理1，u_t 利用 $(\overline{a_t},\overline{b_t})$ 碰撞(即与之重合) (r'_1,r'_2) 在计算上是不可行的。

(iii)间接攻击2：假定 $(\overline{a_t},\overline{b_t})=(\overline{a_s},\overline{b_s})$，后者为某一合法组成员的影子密钥。我们证明 u_t 不能由此导出 (a_s,b_s)；这是集中式GKM的一项基本要求[1,2]：一个组成员的个体密钥只能与GCKS共享。事实上 $\forall r\in Z_m^*$，写 $[r]=\{x\in P_m: x\equiv r \pmod m\}$，则一切的子集 $[r]$ 构成 P_m 的一个分类。由引理1知，任何一类 $[r]$(包括 $[\overline{a_s}]$ 和 $[\overline{b_s}]$)均含无穷多个素数。故 u_t 不能导出 (a_s,b_s)。定理3获证。

3.3 已知明文攻击及应用可行性分析

DES和AES能够成功抵御某些类型的攻击主要归功于它们含有非线性运算的S盒[9,11]，而C密码则没有。与Hill密码类似，对C密码采用惟密文攻击是很难攻破的，然而我们证明它对已知明文攻击是脆弱的。事实上，假定敌手拥有一对明文-密文单元 (x_1,x_2)，$(y_1,y_2)\in Z_m\times Z_m$，则敌手基于(1)式，视 r_1 和 r_2 为未知量，可建立如下同余方程组

$$x_1r_1\equiv y_1-x_2 \pmod{2^n} \tag{8}$$
$$y_1r_2\equiv y_2+x_1 \pmod{2^n} \tag{9}$$

当 $(x_1,y_1)=$(奇数，奇数)时，敌手可高效地(如利用扩展的Euclidean算法[9,11])求出惟一解为

$$\begin{cases} r_1\equiv x_1^{-1}(y_1-x_2) \pmod{2^n} \\ r_2\equiv y_1^{-1}(y_2+x_1) \pmod{2^n} \end{cases}$$

由此即达到密码分析的基本目的——确定密钥(加密密钥 D 和解密密钥 D^{-1})。

当 $(x_1,y_1)\neq$(奇数，奇数)时，敌手从(8)及(9)式仍能求出若干个解，从而也可列举出若干个候选的加密密钥。

下面计算随机事件“$(x_1,y_1)=$(奇数，奇数)”发生的概率 p_2。在(8)式中，记事件“$x_1=$奇数”，“$y_1=$奇数”依次为 E_1,E_2。由于 x_1,x_2 在 Z_m 中取奇数的概率均为1/2，且 r_1,r_2 恒为奇数，故

$$p_2=P(E_1,E_2)=P(E_1)P(E_2\mid E_1)=(1/2)(1/2)=1/4$$

上述分析表明：平均而言，对C密码试验4次已知明文攻击，而且每次仅需一对明文-密文单元，即可确定密钥。

为抵御已知明文攻击，文[8]试图在一种密码操作模式下使用迭代法，但在应用时提出了“迭代次数足够多或密文序列足够长”的额外要求。实际上，大型动态组播组的安全解决方案除追求安全性外，还有各种计算/存储/通信开销、可靠性等工程目标需要折中与权衡。

第一，从“迭代的C密码”的每一次加密看，它采用的是在大多数应用中都有缺陷的电码本(ECB)模式[11]。具体地分析，在不可靠、不安全的IP组播通信环境下，在密文丢失或被注入一些数据位时，整个密文序列将不能被正确地解密，即同步错误不可恢复。而且当消息长度超出分组长度，或者重复使用同一密钥加密多个单组消息时，该模式容易受到重放攻击和密码分析。因此，C密码不适于对IP组播数据提供保密性安全服务。

第二，鉴于在C方案中GCKS和所有组成员必须始终共享一个动态变化的种子密钥，其实质就是组密钥。除采用周期或批处理等安全策略外，组密钥必须随组成员资格变化而更新。换言之，C方案并非采用独立子组TEK方法，文[8]为其断言“无需组密钥更新”的特点不真。

第三，设组密钥更新时的组规模为自变量 w，则由密钥更新算法及(3)式，有

$$m^w<I_i<m(n'_i+1),\ i=1,2$$

故当 $w\geqslant n$ 时，有

(下转第107页)

最多维护 $\log_m N$ 个 GNP 坐标的信息。假定 $N=2^{20}$，$m=4$，$\log_m N=10$。在每个代理增加了 10 个辅助的 GNP 坐标索引的存储开销。这种搜索效率优于分布式系统中通常采用的网络层拓扑感知方法，例如扩展环搜索、启发式搜索，$O(n)$的搜索效率。

在文[13]以及其它发布订阅系统中，通常采用度量所有相邻代理的 RTT(Round-Trip-Time)的方法来解决应用层路由中存在的问题。但在大规模系统中，这种方法需要在每跳路由进行 $O(m)$次度量，m 是相邻代理的数量，效率比较低。本文的方法通过获取 GNP 坐标，取消了每跳度量 RTT 产生的开销。

结束语 在基于 K-D 树划分信息空间实现发布订阅系统的基础上，Spanhop 路由算法和相关拓扑感知策略不仅减少了消息在系统中的转发次数，同时通过网络层的拓扑感知减少了网络层的实际转发距离。同时，算法对于解决扁平层叠网络中的消息路由问题具有一定的参考作用。存在的主要问题是，对信息空间划分方法的依赖性比较强，目前适用的范围有限。后续的工作是进一步研究在信息空间划分基础上的多播通知路由策略以及基于发布订阅中间件系统的实现相关问题。

参 考 文 献

1 Eugster Patrick T H, Felber P, Guerraoui R, et al. The Many Faces of Publish/Subscribe [J]. ACM Computing Surveys, 2003, 35(2): 114～131

2 Carzaniga A, Rosenblum D S, Wolf A L. Archieving scalability and expressiveness in an Internet-Scale event notification service [A]. In: Proceedings of 19th ACM Symposium on Principles of Distributed Computing(PODC2000)[C], 2000. 219～227

3 Wang Y M, Qiu L, Achlioptas D, et al. Subscription partitioning and routing in content-based publish/subscribe networks [A]. In: Dahlia Malkhi, ed. 16th International Symposium on Distributed Computing [C]. Berlin: Springer- Verlag, 2002. 28～30

4 逯鹏，刘旭东，林学练，等. 基于兴趣划分的内容发布订阅系统关键算法[J]. 北京航空航天大学学报，2006，32(8)：992～997

5 Eugene Ng T S, Zhang Hui. Towards Global Network Positioning [A]. In: Proceedings of the ACM SIGCOMM Internet Measurement Workshop [C]. New York: ACM Press, 2001. 25～29

6 Cao F, Singh J P. MEDYM: An architecture for content-based publish-subscribe networks. In: Proceedings of ACM SIGCOMM, Portland, OG, Aug. 2004

7 Cugola G, Nitto E D, Fuggetta A. The JEDI event-based infrastructure and its application to the development of the OPSS WFMS. IEEE Trans. on Software Engineering, 2001, 27(9): 827～850

8 Carzaniga A, Rutherford M J, Wolf A L. A routing scheme for content-based networking. In: Proceedings of IEEE INFOCOM, Hongkong, China, Mar. 2004

9 Mühl G. Large-Scale content-based publish/subscribe systems: [Ph. D Thesis]. Darmstadt University of Technology, 2002

10 薛涛，冯博琴. 内容发布订阅系统路由算法和自配置策略研究[J]. 软件学报，2005, 16(2): 251～259

11 Pietzuch P R. Hermes: A scalable event-based middleware: [Ph D Thesis]. University of Cambridge, 2004

12 Castro M, Druschel P, et al. SCRIBE: A large-scale and decentralized application-level multicast infrastructure [J]. IEEE Journal on Selected Areas in communications (JSAC), 2002, 20(8): 1489～1499

13 Baldoni R, Marchetti C, Virgillito A. Content-based Publish-Subscribe over Structured Overlay Networks [A]. In: Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICSCS'05)[C], 2005. 437～446

14 Banavar G, Chandra T, Mukherjee B, et al. An efficient multicast protocol for content-based publish-subscribe systems [A]. In: Dahlin M, ed. International Conference on Distributed Computing Systems [C], Washington, DC USA: IEEE Computer Society, 1999. 262～272

(上接第 82 页)

$$\log_2 n'_i \geqslant n(w-1) \geqslant (n-1)w \geqslant 0$$

于是，作为密钥更新开销的一部分，密钥更新消息(n'_1, n'_2)的比特长度为 $\log_2 n'_1 + \log_2 n'_2 = \Omega(w)$。这使得 C 方案仍未摆脱传统两两密钥类方案的一个共同局限性——承受不可扩展的通信开销。

结束语 本文研究了 C 密码和 C 方案的安全性及其在安全组播通信中的应用可行性问题。计算出的密钥量表明 C 密码能较好地抵抗穷举密钥攻击；尽管 C 方案不具备严格意义上的前向/后向保密性，但对密钥组合攻击和同余碰撞攻击是计算上安全的。然而，C 密码对已知明文攻击的脆弱性使得它不适于对组播通信提供保密性安全服务；尽管 C 方案是与传统两两密钥管理不同的新方案，但仍未摆脱通信开销不可扩展的传统局限性。

鉴于 C 密码是图像加密系统中广义猫映射的运用和 Hill 密码的变种、对称密码学中的置换密码又可视为 Hill 密码的特款[9]、影子密钥概念包含公钥密码学中起着基础作用的大素数模运算，本文的方法与结果将对 GKM 的研究产生一定积极作用。

参 考 文 献

1 Hardjono T, Dondeti L R. Multicast and Group Security. Norwood [M]. MA: Artech House, INC, 2003

2 Challal Y, Bouabdallah A, Seba H. A Taxonomy of Group Key Management Protocols: Issues and Solutions [J]. Transactions on Engineering, Computing and Technology, 2005, 6 (2): 5～17

3 Chiu Y P, Lei C L, Huang C Y. Secure Multicast Using Proxy Encryption [C]. In: Proceedings of the 7th International Conference on Information and Communications Security (ICICS '05, Beijing), Springer LNCS 3783, 2005. 280～290

4 Wong C K, Gouda M, Lam S S. Secure Group Communications Using Key Graphs [J]. IEEE/ ACM Trans on Networking, 2000, 8(1): 16～31

5 Canetti R, Malkin T, Nissim K. Efficient communication storage tradeoffs for multicast encryption [C]. In: Advances in Cryptology-EUROCRYPT'99, LNCS 1592. Berlin: Springer- Verlag, 1999. 459～474

6 Snoeink J, Suri S, Varghese G. A lower bound for multicast key distribution [J]. Computer Networks, 2005, 47(3): 429～441

7 马在光，丘水生. 基于广义猫映射的一种图像加密系统[J]. 通信学报，2003, 24(2): 51～57

8 曹国梁，周杰. 一种适用于安全多播的加密算法及密钥管理方案[J]. 通信学报，2005, 26(1A): 100～105

9 Stinson D R 著. 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

10 Jacbson N. Basic Algebra I. 2nd edition [M]. New York: W H Freeman and Company, 1989

11 Menezes A J, van Oorschot P, Vanstone S 著. 应用密码学手册[M]. 胡磊，等译. 北京：电子工业出版社，2005

12 潘承洞，潘承彪. 初等数论. 第二版[M]. 北京：北京大学出版社，2003