

对基于广义猫映射的组播密钥管理方案的改进

王全迪¹, 李金凤¹, 周杰²

(1. 华南理工大学 理学院, 广州 510640; 2. 华南理工大学 计算机科学与工程学院, 广州 510006)

(qdwang@scut.edu.cn)

摘要:通过分析指出曹国梁等人给出的基于广义猫映射的组播密钥管理方案不满足组成员私钥独立性的安全性要求。利用单向函数对基于广义猫映射的组播密钥管理方案进行改进,改进方案满足组成员私钥独立性的安全性要求,且比曹国梁等人的组播密钥管理方案具有更高的安全性,同时还具有较低的计算开销和通信开销。

关键词:组播安全;组播密钥管理;私钥独立性;广义猫映射;单向函数

中图分类号: TP309.7 **文献标志码:** A

Modification of Cao's multicast key management scheme based on generalized cat map

WANG Quan-di¹, LI Jin-feng¹, ZHOU Jie²

(1. School of Sciences, South China University of Technology, Guangzhou Guangdong 510640, China;

2. School of Computer Science and Engineering, South China University of Technology, Guangzhou Guangdong 510006, China)

Abstract: It is indicated that Cao Guoliang et al's multicast key management scheme based on generalized cat map does not satisfy the independent security requirement of individual keys of group members. A modification scheme was proposed by using one way function. The presented scheme satisfies the independent security requirement of individual keys of group members. Compared with Cao Guoliang et al's scheme, this modification scheme has higher security and lower computation and communication overheads.

Key words: multicast security; multicast key management; independence of individual key; generalized cat map; one way function

组播通信是一种高效的多目标传输机制,在视频会议、视频点播、网络电视等业务中有广泛的应用。随着基于组播通信应用的不断发展,安全组播成为当前计算机网络安全领域研究的热点问题之一,吸引了众多研究者的关注^[1-4]。安全组播通信主要包括保证传输数据的机密性和完整性、对源和组成员的身份认证以及访问控制等^[2]。实现安全组播通信的主要方法之一是采用密码技术^[2-3]:所有组成员(或组成员子组)共享一个组密钥(业务加解密密钥),运用某种对称加密算法加密和解密传输的信息。在安全群组通信过程中,组成员身份是动态变化的。当组成员身份变化时,为了满足前向或后向机密性,需要更新组密钥。通常每个组成员持有一个或多个私钥用于有效更新组密钥。如何安全有效地对组密钥和组成员的私钥进行管理,是组播密钥管理的核心问题^[2-5]。

组播密钥管理的安全性要求包括组密钥保密性、组密钥独立性、前向保密性、后向保密性和组成员私钥独立性等安全属性。其中前向保密、后向保密和组成员私钥独立性是组播密钥管理特有的需求^[3]。近年来国内外研究者已经提出了许多组播密钥管理方案,已有的组播密钥管理方案可分为集中式、分布式和分层分组式^[2]。

曹国梁等人^[6]基于整数乘积和模运算,结合一种广义猫映射,构造了一种集中式组播密钥管理方案(以下简称曹方案)。杨军等人文献^[7]中分析了该组播密钥管理方案的密码强度、前向/后向保密性和可扩展性等问题,对方案的已知明文攻击以及在大型组播通信中的应用的可行性进行了分析。由于在组密钥与组成员私钥之间建立了一种新型的函数

关系,该组播密钥管理方案区别于传统的组播密钥管理方案:组管理中心采用组播方式公开发送一条密钥更新消息,每个组成员利用自己的私钥计算新的组密钥,因而极大地减少了通信开销。

本文指出曹方案^[6]给出的基于广义猫映射的组播密钥管理方案不满足组成员私钥独立性的安全性要求。利用单向函数给出该方案的一种改进,讨论了改进方案的安全性和性能。

1 曹方案简介与分析

Arnold 猫映射是 Anosov 散射的一个最著名实例。对 Arnold 猫映射在正整数范围内进行推广,将像空间从 $[0,1] \times [0,1]$ 推广到 $\{0,1,\dots,N\} \times \{0,1,\dots,N\}$,称为广义猫映射^[8]。广义猫映射和逆映射的矩阵方程分别为:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = D \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \bmod N = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \bmod N$$

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = D^{-1} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \bmod N = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \bmod N$$

其中: N 是一个充分大的正整数, a, b, c, d 为正整数,矩阵 D 满足 $|D| = 1$,即 $ad - bc = 1$ 。

曹方案以素数对作为组成员的私钥,利用整数乘积和模运算的性质,借助广义猫映射,给出一种集中式组播密钥管理方案。下面首先介绍这一方案,然后指出该方案不满足组成员私钥独立性的安全性要求。

收稿日期:2010-10-11;修回日期:2010-11-28。 **基金项目:**国家科技支撑计划项目(2008BAH37B08)。

作者简介:王全迪(1963-),女,吉林集安人,教授,博士,主要研究方向:应用数学、信息安全; 李金凤(1981-),女,山东聊城,硕士研究生,主要研究方向:信息安全; 周杰(1964-),男,吉林双辽人,教授,博士,主要研究方向:高性能网络技术、信息安全。

设一个安全组播系统包含一个组管理中心负责管理组成员和分发组密钥。组管理中心选取正整数 $N = 2^{128}$ 并公开。假设某次安全组播通信中初始组播组为 $U = \{u_1, u_2, u_3, \dots, u_m\}$, 其中 u_1 为组播信息发送者。组管理中心与每个组成员完成一对一的互认证及注册过程。对组成员 $u_i (i \in \{1, 2, \dots, m\})$, 组管理中心随机选取与其他组成员不同的素数对 $(a_i, b_i) (a_i, b_i > N)$ 作为其私钥, 并通过安全单播通道发送给 u_i 。安全组播通信过程如下。

1) 组管理中心利用组成员的私钥 $(a_i, b_i) (i = 1, 2, \dots, m)$, 计算乘积 $I_1 = a_1 a_2 \dots a_m a_p$ 和 $I_2 = b_1 b_2 \dots b_m b_p$ 。其中 (a_p, b_p) 是随机选取地与其他所有组成员的私钥均不相同的一对素数, 称为扰乱密钥。

2) 令 $n_1 = \lfloor I_1/N \rfloor, r_1 = I_1 \bmod N; n_2 = \lfloor I_2/N \rfloor, r_2 = I_2 \bmod N$, 其中 $\lfloor x \rfloor$ 为取整符号。显然有 $I_1 = n_1 N + r_1, I_2 = n_2 N + r_2$ 。 (r_1, r_2) 为组密钥, (n_1, n_2) 为辅助密钥。

3) 组管理中心销毁 I_1 和 I_2 , 将 (r_1, r_2) 通过安全单播通道发送给 u_1 , 将 (n_1, n_2) 组播给组成员。

4) 组成员 u_1 收到 (r_1, r_2) 后, 令广义猫映射的矩阵为 $D = \begin{bmatrix} r_1 & r_1 r_2 - 1 \\ 1 & r_2 \end{bmatrix}$, 利用广义猫映射加密整数对 $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ (组播明文信息), $x_1, x_2 \in [0, N]$, 得到密文:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = D \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \bmod N = \begin{bmatrix} r_1 & r_1 r_2 - 1 \\ 1 & r_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \bmod N$$

5) 将 $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ 组播给组成员。

6) 组成员 $u_i (i \in \{2, 3, \dots, m\})$ 收到密文 $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ 后, 首先利用其私钥 (a_i, b_i) 、辅助密钥 (n_1, n_2) 和 N , 计算出组密钥 $(r_1, r_2): r_1 = a_i - (n_1 N \bmod a_i), r_2 = b_i - (n_2 N \bmod b_i)$ 。这是根据如下的推导过程得到的:

$$\begin{aligned} n_1 N \bmod a_i &= (I_1 - r_1) \bmod a_i = \\ &= ((I_1 \bmod a_i) - (r_1 \bmod a_i)) \bmod a_i = \\ &= ((a_i \bmod a_i) - (r_1 \bmod a_i)) \bmod a_i = \\ &= (a_i - r_1) \bmod a_i = a_i - r_1 \end{aligned}$$

类似可得 $n_2 N \bmod b_i = b_i - r_2$ 。

然后, 利用广义猫映射的逆映射矩阵方程恢复出明文:

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = D^{-1} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \bmod N = \begin{bmatrix} r_2 & 1 - r_1 r_2 \\ -1 & r_1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \bmod N$$

7) 在组播通信过程中, 有新的组成员加入组播组, 或组播组中的组成员退出组播组时, 重新触发安全组播通信过程 1) ~ 6) 更新组密钥。

下面说明如上的组播密钥管理方案不满足组成员私钥独立性的安全性要求。

假设在两次组播通信中只有两个成员是公共的成员。如设两次组播通信的组成员分别为: $\{u_1, u_2, u_{i_1}, \dots, u_{i_k}\}$ 和 $\{u_1, u_2, u_{j_1}, \dots, u_{j_l}\}$, 且 $\{u_1, u_2, u_{i_1}, \dots, u_{i_k}\} \cap \{u_1, u_2, u_{j_1}, \dots, u_{j_l}\} = \{u_1, u_2\}$ 。在第一次组播通信中, u_1 和 u_2 利用其私钥及公开的信息可计算出:

$$\begin{aligned} I_1^1 &= n_1^1 N + r_1^1 = a_1 a_2 a_{i_1} \dots a_{i_k} a_p^1 \\ I_2^1 &= n_2^1 N + r_2^1 = b_1 b_2 b_{i_1} \dots b_{i_k} b_p^1 \end{aligned}$$

在第二次组播通信中, u_1 和 u_2 可计算出:

$$\begin{aligned} I_1^2 &= n_1^2 N + r_1^2 = a_1 a_2 a_{j_1} \dots a_{j_l} a_p^2 \\ I_2^2 &= n_2^2 N + r_2^2 = b_1 b_2 b_{j_1} \dots b_{j_l} b_p^2 \end{aligned}$$

其中 (a_p^1, b_p^1) 和 (a_p^2, b_p^2) 分别是两次组播通信中的扰乱密钥。

由于 $\gcd(I_1^1, I_1^2) = a_1 a_2, \gcd(I_2^1, I_2^2) = b_1 b_2$, 因此, 组成员 u_1 利用两次组播获得的信息, 通过式 $a_2 = \frac{\gcd(I_1^1, I_1^2)}{a_1}$ 和 $b_2 = \frac{\gcd(I_2^1, I_2^2)}{b_1}$ 可获得组成员 u_2 的私钥 (a_2, b_2) ; 组成员 u_2 利用两次组播获得的信息, 通过式 $a_1 = \frac{\gcd(I_1^1, I_1^2)}{a_2}$ 和 $b_1 = \frac{\gcd(I_2^1, I_2^2)}{b_2}$ 可获得组成员 u_1 的私钥 (a_1, b_1) 。这里可以用广义欧几里得除法计算两个整数的最大公因数 $\gcd(x, y)$ 。如上分析可知, 在两次组播通信中恰好有两个成员是公共的成员时, 这两个成员利用获得的组播信息就可得到对方的私钥。因此, 曹方案不满足组成员私钥独立性要求。

例如某次组播通信的组播组有三个成员 $\{u_1, u_2, u_3\}$, 接下来的组播通信中组成员 u_3 退出组播组, 新组成员 u_4 加入组播组。于是, 根据上面的计算过程可知, 经过两次不同的组播通信后, u_1 可获得 u_2 的私钥, u_2 可获得 u_1 的私钥。如果在后面的组播通信中, u_1 被强制退出组播组, 而 u_2 仍在新的组播组中, 由于 u_1 具有 u_2 的私钥, 因此 u_1 可继续获得组播信息, 破坏了组播的安全性要求。

2 对曹方案的改进

2.1 改进方案描述

利用单向函数, 借鉴文献[9]的方法对曹方案进行改进, 描述如下。

设一个安全组播系统包含一个组管理中心负责管理组成员和分发组密钥。组管理中心选取正整数 $N = 2^{128}$ 并公开, 同时公布一个单向函数 H (设 H 的输出为 128 b)。假设某次安全组播通信中初始组播组为 $U = \{u_1, u_2, u_3, \dots, u_m\}$, 其中 u_1 为组播信息发送者。组管理中心与每个组成员完成一对一的互认证及注册过程。对组成员 $u_i (i \in \{1, 2, \dots, m\})$, 组管理中心随机选取与其他组成员不同的正整数对 $(a_i, b_i) (a_i, b_i > N)$ 作为其私钥, 并通过安全单播通道发送给 u_i 。安全组播通信过程如下:

1) 组管理中心随机选取正整数对 (c_1, c_2) 和 (r_1, r_2) , (r_1, r_2) 为组密钥。这里要求 $r_1 < \min\{H(a_i \| c_1) : 1 \leq i \leq m\}, r_2 < \min\{H(b_i \| c_2) : 1 \leq i \leq m\}$ 。利用组成员的私钥 $(a_i, b_i) (i = 1, 2, \dots, m)$ 和单向函数 H , 计算: $I_1 = \prod_{i=1}^m H(a_i \| c_1) + r_1$ 和 $I_2 = \prod_{i=1}^m H(b_i \| c_2) + r_2$ 。

2) 将 (c_1, c_2) 和 (I_1, I_2) 组播给组成员。

3) 组成员 u_i 收到 (c_1, c_2) 和 (I_1, I_2) 后, 利用其私钥 $(a_i, b_i), (c_1, c_2), (I_1, I_2)$ 和单向函数 H , 计算组密钥 $(r_1, r_2): r_1 = I_1 \bmod H(a_i \| c_1), r_2 = I_2 \bmod H(b_i \| c_2)$ 。

令广义猫映射的矩阵为 $D = \begin{bmatrix} r_1 & r_1 r_2 - 1 \\ 1 & r_2 \end{bmatrix}$, 利用广义猫

映射加密整数对 $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ (组播明文信息), $x_1, x_2 \in [0, N]$, 得到密文:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = D \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \bmod N = \begin{bmatrix} r_1 & r_1 r_2 - 1 \\ 1 & r_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \bmod N$$

4) 将 $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ 组播给组成员。

5) 组成员 $u_i (i \in \{2, 3, \dots, m\})$ 收到密文 $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ 后, 首先

利用其私钥 (a_i, b_i) 、 (c_1, c_2) 、 (I_1, I_2) 和单向函数 H , 计算组密钥 (r_1, r_2) : $r_1 = I_1 \bmod H(a_i \parallel c_1)$, $r_2 = I_2 \bmod H(b_i \parallel c_2)$ 。然后, 利用广义猫映射的逆映射矩阵方程恢复出明文:

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = D^{-1} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \bmod N = \begin{bmatrix} r_2 & 1 - r_1 r_2 \\ -1 & r_1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \bmod N$$

6) 在组播通信过程中, 有新的组成员加入组播组, 或组播组中的组成员退出组播组时, 重新触发安全组播通信过程 1) 至 5) 更新组密钥。

2.2 安全性和性能分析

首先, 改进的组播密钥管理方案满足前向和后向保密性要求。对于组播组 U , 在组播通信过程中, 有新的组成员 $u_j (u_j \notin U)$ 加入组播组, 或组成员 $u_i (u_i \in U)$ 退出组播组。加入 (或退出) 组播组的组成员 $u_j (u_i)$ 可能获得其加入组播组之前 (退出组播组之后) 的组播信息 (c_1, c_2) 和 (I_1, I_2) ((c_1', c_2') 和 (I_1', I_2'))。但由于 $u_j (u_i)$ 的私钥没有参与计算 I_1 和 I_2 (I_1' 和 I_2'), 因此无法获得其加入组播组之前 (退出组播组之后) 的组密钥 (r_1, r_2) ((r_1', r_2')), 从而无法恢复出相应的组播明文。

其次, 改进的组播密钥管理方案满足组成员私钥独立性的安全性要求。1) 组成员的私钥由组管理中心随机选取, 并且互不相同, 因此是相互独立的。2) 从 I_1 和 I_2 的定义可知, 由 I_1 或 I_2 计算 $H(a_i \parallel c_1)$ 或 $H(b_i \parallel c_2)$ 的一种方法是: 先确定 (r_1, r_2) , 然后对 $I_1 - r_1$ 或 $I_2 - r_2$ 进行因式分解, 因此这一方法在计算上是不可行的, 由于 $H(a_i \parallel c_1)$ 和 $H(b_i \parallel c_2)$ 不一定是素数, 更增加了这一方法在计算上的难度。3) 组管理中心在分发组密钥时使用单向函数, 即使在某次组播通信时组成员 u_i 能够获得 $H(a_j \parallel c_1)$ 和 $H(b_j \parallel c_2)$ ($j \neq i$), 由于 (c_1, c_2) 的选取以及 H 的单向性, u_i 也很难获得 u_j 的私钥 (a_j, b_j) 。

利用与杨军等人^[7]类似的分析方法可知, 改进的组播密钥管理方案能抵抗穷举密钥攻击。同样改进方案也是采用与 Hill 密码类似的多表代换密码实现的一种组播密钥管理方案, 因此采用唯密文攻击是很难攻破的, 然而对已知明文攻击相对脆弱。

与曹方案在性能上比较: 1) 在分发组密钥时, 改进方案需要组管理中心先计算单向函数值, 一方面由于单向函数的计算时间与大整数相乘的计算时间相比相对较小, 另一方面单向函数值小于相应私钥分量的值, 因此, 组管理中心的计算量并没有增加; 2) 组管理中心不需要计算辅助密钥 (n_1, n_2)

和组密钥 (r_1, r_2) , 相对减少了组管理中心和组成员的计算量; 3) 组管理中心在分发组密钥时, 不需要安全单播通道给组播信息发送者发送组密钥, 减少了通信开销, 增加了系统的安全性。

3 结语

组成员私钥独立性是组播密钥管理方案特有的安全需求。本文指出曹国梁等人在文献[6]中给出的基于广义猫映射的组播密钥管理方案不满足组成员私钥独立性的安全性要求, 并利用单向函数设计了一种改进方案。改进方案满足组成员私钥独立性的安全性要求, 且比曹方案具有更高的安全性, 同时具有较低的计算开销和通信开销。

参考文献:

- [1] SUN Y L, RAY LIU K J. Analysis and protection of dynamic membership information for group key distribution schemes [J]. IEEE Transactions on Information Forensics and Security, 2007, 2(2): 213–226.
- [2] CHALLAL Y, SEBA H. Group key management protocols: A novel taxonomy [J]. International Journal of Information Technology, 2005, 2(1): 105–118.
- [3] PHAM T, WATTERS P. The efficiency of periodic rekeying in dynamic group key management [C]// ECUMN'07: Proceedings of the Fourth European Conference on Universal Multiservice Networks. Washington, DC: IEEE Computer Society, 2007: 425–432.
- [4] KAPLAN S, HUTCHISON D. A survey of key management for secure group communication [J]. ACM Computing Surveys, 2003, 35(2): 309–329.
- [5] HAJYVAHABZADEH M, EIDKHANI E, MORTAZAVI S A, et al. A new group key management protocol using code for key calculation: CKC [C]// ICISA: International Conference on Information Science and Applications. Seoul: [s. n.], 2010: 1–6.
- [6] 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.
- [7] 杨军, 覃伯平, 雷开彬. 基于广义猫映射的组播密钥管理方案研究 [J]. 计算机科学, 2008, 35(1): 80–83.
- [8] 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.
- [9] CHANG C-C, SU Y-W, LIN I-C. A broadcast encryption based key management scheme for dynamic multicast communications work in progress [C]// The Second International Conference on Scalable Information Systems. Suzhou: [s. n.], 2007: 69–70.
- [2] KITAGAKI K, OTO T. New address-generation-unit architecture for video signal processing [C]// Visual Communications and Image Processing. Boston: SPIE, 1991: 891–900.
- [3] DESOLI G. Instruction assignment for clustered VLIW DSP compilers: A new approach, HPL-98-13 [R]. Palo Alto: Hewlett-Packard Company, 1998.
- [4] CHU M. Region based hierarchical operation partitioning for multi-cluster processors [C]// PLDI'03: Proceedings of the ACM SIGPLAN 2003 Conference on Programming Language Design and Implementation. New York: ACM, 2003: 300–311.
- [5] HWU W W. The IMPACT research group [EB/OL]. [2010–07–10]. <http://impact.crhc.illinois.edu/>.
- [6] OZER E, BANERJIA S, CONTE T. United assign and schedule: A new approach to scheduling for clustered register file microarchitectures [C]// Proceedings of the 31th Annual International Symposium on Microarchitecture. Dallas: Microarchitecture, 1998: 308–315.
- [7] LAPINSKII V, JACOME M, de VECIANA G. High-quality operation binding for clustered VLIW datapaths [C]// Proceedings of the 2001 Design Automation Conference. New York: ACM, 2001: 702–707.
- [8] FIELDS B, BODIK R, HILL M D. Slack: Maximizing performance under technological constraints [C]// Proceedings of the 29th Annual International Symposium on Computer Architecture. Anchorage: ISCA, 2002: 47–58.
- [9] DSPstone [EB/OL]. (2006–05–23) [2010–04–12]. <http://www.ert.rwth-aachen.de/Projekte/Tools/DSPSTONE/dspstone.htm>.
- [10] RAU B. Iterative modulo scheduling: An algorithm for software pipelining loops [C]// MICRO 27: Proceedings of the 27th Annual International Symposium on Microarchitecture. New York: ACM, 1994: 63–74.

(上接第 937 页)