基于中国剩余定理的秘密共享组播密钥管理方案

席国宝 陈惠芳 赵问道
(浙江大学信电系 杭州 310027)

摘 要 该文结合中国剩余定理和Shamir秘密共享方法，提出了一种新的组播密钥管理方案——基于中国剩余定理的秘密共享(CRTSS)组播密钥管理方案，并把所提出的CRTSS方案与GKMP方案进行比较和分析。结果表明，CRTSS方案克服了传统集中式平面型管理方式更新开销大的通病，提升了整体性能，是一种可靠的、新型的集中式平面型组播密钥管理方案。

关键词 秘密共享，中国剩余定理，密钥管理，组密钥管理协议，基于中国剩余定理的秘密共享
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2006)12-2378-04

Chinese Remainder Theorem-Based Secret Sharing Scheme

Xi Guo-bao Chen Hui-fang Zhao Wen-dao
(*Information Science and Electronic Engineering Department, Zhejiang University, Hangzhou* 310027, *China*)

Abstract This paper proposes Chinese Remainder Theorem-based Secret Sharing (CRTSS) scheme, a new Multicast Key Management (MKM) scheme, which adopts the Chinese remainder theorem and Shamir's secret sharing method. With comparing and analyzing GKMP and CRTSS schemes, the results show that CRTSS scheme overcomes high rekeying cost, the defect of conventional centralized flat schemes, improves the performance. It is a new reliable centralized flat MKM scheme.

Key words Secret sharing, Chinese Remainder Theorem (CRT), Key management, Group Key Management Protocol (GKMP), Chinese Remainder Theorem-based Secret Sharing (CRTSS)

1 引言

随着Internet的迅速普及和爆炸性发展，组播技术应运而生。组播传输提高了数据传送效率，减少了网络出现拥塞的可能性[1]。然而，目前的组播协议缺乏安全机制来满足组播应用的安全性要求，采用明文传输的组播报文在网络上很容易被窃听、冒充和篡改。组播安全问题包括：数据保密、组管理和源认证等多个方面。组播密钥管理的功能是解决组管理的安全问题，主要包括两个方面：一个方面是密钥的分发；另一个方面是对密钥进行管理以适应组成员关系的变化。组播密钥管理为参与组播的成员生成、分发和更新组密钥(Group Key，GK)[2]。

相比单播密钥管理，前向加密(forward confidentiality)和后向加密(backward confidentiality)是组播密钥管理特有的问题[3]。前向加密：主动退出组播的节点或被强制退出的节点(比如恶意节点)无法利用它们所知的密钥解密后继的组播报文或生成有效的加密报文。后向加密：新加入的组成员无法破解它加入之前的组播报文。迄今为止，已经出现了许多组播密钥管理方案，如集中式层次型的集中式基于树的密钥管理(Centralized Tree-based Key Management，CTKM)方案[4]；集中式平面型的组密钥管理协议(Group Key Management Protocol，GKMP)方案[5]；集中式分组型的Iolus[6]方案。本文提出了一种新型的集中式平面型的组播密钥管理方案——基于中国剩余定理的秘密共享(Chinese Remainder Theorem-based Secret Sharing，CRTSS)方案。CRTSS方案是基于中国剩余定理和Shamir的秘密共享的组播密钥管理方案，该方案克服了传统集中式平面型管理方式更新开销大的通病，大大降低了更新开销，是一种可靠的、新型的集中式平面型组播密钥管理方案。

2005-03-28 收到，2005-09-30 改回

2 中国剩余定理

中国剩余定理[7]：设 $p_1, p_2, \cdots, p_k$ 是互为素数的k个正整数，$k \ge 2$，令 $P = p_1 p_2 \cdots p_k = p_1 P_1 = p_2 P_2 = \cdots = p_k P_k$，其中 $P_i = P / p_i$，$i = 1,2,\cdots,k$，则同时满足同余方程组：

$$\left\{\begin{array}{l} c \equiv y_1 \mod p_1 \\ c \equiv y_2 \mod p_2 \\ \quad\vdots \\ c \equiv y_k \mod p_k \end{array}\right\} \tag{1}$$

的正整数解是：$c \equiv y_1 P_1' P_1 + y_2 P_2' P_2 + \cdots + y_k P_k' P \bmod P$。其中 P_i' 是满足同余方程：$P_i' P_i \equiv 1 \mod p_i$，$i = 1,2,\cdots,k$ 的正整数解。

3 CRTSS 方案

基于中国剩余定理的秘密共享 CRTSS 组播密钥管理方案是一种集中式平面型组播密钥管理方案，但它与传统的集

中式平面型组播密钥管理方案只是在结构上相同，密钥管理方法完全不同。

3.1 密钥生成

在CRTSS方案中，组控制者(Group Controller，GC)和成员节点之间不存在密钥层次树结构，CRTSS方案的结构是一种平面型结构(如图 1 所示)，与GKMP方案[5]的体系结构完全相同。

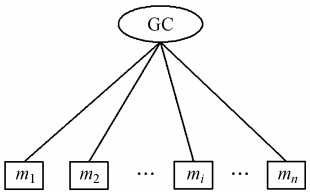

图 1　CRTSS 方案的体系结构

Fig. 1　Structure of CRTSS scheme

成员 m_i 拥有自己的私有素数 p_i，GC 拥有所有成员的私有素数和组密钥。成员 m_i 加入组时，GC 和 m_i 通过密钥交换协议产生的 m_i 的私有密钥 K_i，而私有素数 p_i 是 GC 通过计算得到并用 K_i 加密发送给成员 m_i 的。

GC：利用(2, n)Shamir 秘密共享方法，创建两个一次多项式 $f_1(x)=a_{11}x+a_{10}$ 和 $f_2(x)=a_{21}x+a_{20}$，其中，多项式 $f_1(x)$ 的常数项 a_{10} 就是组密钥 K_g，GC 使用两个不等的随机正整数，利用 $f_1(x)$ 计算得到两个秘密共享份额 AS_1 和 S_g，S_g 称为组密钥 K_g 的盲密钥；而多项式 $f_2(x)$ 的常数项 a_{20} 就是盲密钥 S_g。GC 分别将 $p_1,p_2,\cdots,p_n$ 作为多项式 $f_2(x)$ 的变量进行计算，可以得到 n 个对应的函数值，即 n 个秘密共享份额：

$$\left.\begin{aligned} y_1 &= f_2(p_1)=a_{21}p_1+a_{20}\\ y_2 &= f_2(p_2)=a_{21}p_2+a_{20}\\ &\vdots\\ y_n &= f_2(p_n)=a_{21}p_n+a_{20} \end{aligned}\right\} \tag{2}$$

并且，GC用一其他变量值$x(x\neq 0)$，通过 $f_2(x)$ 计算得到一个有效共享份额AS_2。

GC 按照中国剩余定理计算数值 $P=p_1p_2\cdots p_k=p_1P_1=p_2P_2=\cdots=p_nP_n$，其中：$P_i=P/p_i$，$i=1,2,\cdots,n$，得到同时满足同余方程组式(1)的正整数解是：$c\equiv y_1P_1'P_1+y_2P_2'P_2+\cdots+y_nP_n'P_n \bmod P$。其中 P_i' 是满足同余方程：$P_i'P_i\equiv 1 \bmod p_i$，$i=1,2,\cdots,n$ 的正整数解。

GC 将 c，AS_1 和 AS_2 组播发送到所有成员：$\mathrm{GC}\rightarrow\{m_1,m_2,\ldots,m_n\}:\{c,\mathrm{AS}_1,\mathrm{AS}_2\}$。成员 m_i ($i=1,2,\cdots,n$)接收到 c，AS_1 和 AS_2 后利用 $c\equiv y_i \bmod p_i$ 得到 y_i，即一个秘密共享份额，利用 y_i 和 AS_2，按照 Shamir 秘密共享方法恢复出组密钥 K_g 的盲密钥 S_g；然后利用 S_g 和 AS_1 恢复出组密钥 K_g。

3.2 密钥更新

在 CRTSS 方案中，有 3 种情况需要进行密钥更新：成员加入、成员离开和周期性更新。成员在加入组播组时向 GC 发送加入请求，GC 验证请求通过后，允许成员加入，更新密钥。成员离开组播组时向 GC 发送离开请求，GC 删除成员并更新密钥。而且 GC 还可以周期性更新组密钥。通过成员加入、成员离开和周期性更新 3 种密钥更新情况来说明 CRTSS 方案的密钥更新方法。

3.2.1 成员加入

假设成员 m_{n+1} 要求加入组，此时组有 n 个成员 $m_1,m_2,\cdots,m_n$，如图 2 所示。

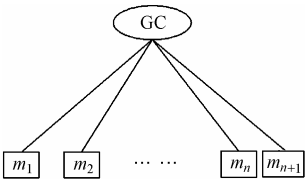

图 2　成员m_{n+1}加入

Fig.2　Member m_{n+1} joins

成员 m_{n+1} 向 GC 发送加入请求，GC 接收到成员的加入请求后，进行成员身份验证或加入验证工作，决定是否接受该成员加入这个组播组。如果决定接受这个成员加入组，GC 需要进行密钥更新。成员加入时的密钥更新过程：

(1)GC 和要求加入的新成员 m_{n+1} 通过密钥交换协议产生 m_{n+1} 的私有密钥 K_{n+1}，同时，GC 生成 m_{n+1} 的私有素数 p_{n+1}；

(2)GC 更新组密钥 K_g 为 K_g'；

(3)GC 更新多项式 $f_1(x)=a_{11}x+a_{10}$ 为 $f_1'(x)=a_{11}'x+a_{10}'$，常数项 $a_{10}'=K_g'$；计算得到 $f_1'(x)$ 的两个秘密共享：AS_1' 和 S_g'；

(4)GC 更新多项式 $f_2(x)=a_{21}x+a_{20}$ 为 $f_2'(x)=a_{21}'x+a_{20}'$，常数项 $a_{20}'=S_g'$；利用原有 n 个成员和新加入成员的 n+1 个私有素数 p_i，($i=1,2,\cdots,n,n+1$)生成 n+1 个新 $f_2'(x)$ 的函数值 $y_i'=f_2'(p_i)$，($i=1,2,\cdots,n,n+1$)以及 AS_2'；

(5)GC 按照中国剩余定理计算 $P'=p_1p_2\cdots p_np_{n+1}=Pp_{n+1}=p_1P_1=p_2P_2=\cdots=p_nP_n=p_{n+1}P_{n+1}$，其中：$P=p_1p_2\ldots p_n$ 是新成员加入前，原来成员的私有素数计算得到的数值；p_{n+1} 是新加入成员的私有素数；$P_i=P/p_i$，$i=1,2,\cdots,n,n+1$；

(6)GC 计算 $c'\equiv y_1'P_1'P_1+y_2'P_2'P_2+\cdots+y_n'P_n'P_n+y_{n+1}'P_{n+1}'P_{n+1} \bmod P'$，其中 P_i' 是满足同余方程：$P_i'P_i\equiv 1 \bmod p_i$，$i=1,2,\cdots,n,n+1$ 的正整数解；

(7) $\mathrm{GC}\rightarrow\{m_1,m_2,\cdots,m_n\}:\{c',\mathrm{AS}_1',\mathrm{AS}_2'\}_{K_g}$；

(8) $\mathrm{GC}\rightarrow\{m_{n+1}\}:\{p_{n+1},c',\mathrm{AS}_1',\mathrm{AS}_2'\}_{K_{n+1}}$。

成员 m_i ($i=1,2,\cdots,n,n+1$)接收到 c',AS_1' 和 AS_2' 后，利用 $c'\equiv y_i' \bmod p_i$ 得到 y_i'，用 y_i' 和 AS_2' 恢复出新盲密钥 S_g'；然后利用 S_g' 和 AS_1' 恢复出新组密钥 K_g'。这样就完成了成员加入的整个密钥更新工作。

3.2.2 成员离开

假设成员 m_j 要求离开组，此时组有 n 个成员 $m_1,m_2,\cdots,m_n$，如图 3 所示。

成员 m_j 向 GC 发送离开请求，GC 接收到成员的离开请求后，进行密钥更新。成员离开时的密钥更新过程：

(1) GC 删除成员 m_j 的节点；

(2) GC 更新组密钥 K_g 为 K_g'；

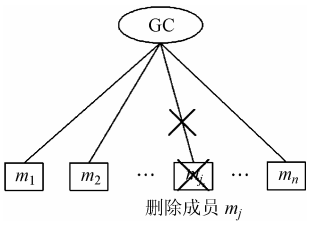

图 3 成员m_j离开组

Fig.3 Member m_j leaves

(3)GC 更新多项式 $f_1(x)=a_{11}x+a_{10}$ 为 $f_1'(x)=a_{11}'x+a_{10}'$，常数项 $a_{10}'=K_g'$；计算得到 $f_1'(x)$ 的两个秘密共享份额： AS_1' 和 S_g'；

(4)GC 更新多项式 $f_2(x)=a_{21}x+a_{20}$ 为 $f_2'(x)=a_{21}'x+a_{20}'$，常数项 $a_{20}'=S_g'$；在原有的 n 个私有素数 $p_i\ (i=1,2,\cdots,n)$中，删除离开成员 m_j 的私有素数 p_j，利用剩余的 n–1 个私有素数 p_i，$(i=1,2,\cdots,n,i\neq j)$生成 n–1 个 $f_2'(x)$ 的函数值 $y_i'=f_2'(p_i)$，$(i=1,2,\cdots,n,i\neq j)$以及 AS_2'；

(5)GC 按照中国剩余定理计算 $P'=p_1p_2\cdots p_n=P/p_j=p_1P_1=p_2P_2=\cdots=p_nP_n$，其中 $P=p_1p_2...p_n$，p_j 是离开成员 m_j 的私有素数；$P_i=P'/p_i$，$i=1,2,\cdots,n,i\neq j$；

(6)GC 计算 $c'\equiv y_1'P_1'P_1+y_2'P_2'P_2+\cdots+y_n'P_n'P_n \bmod P'$，其中 P_i' 是满足同余方程：$P_i'P_i\equiv 1 \bmod p_i$，$i=1,2,\cdots,n,i\neq j$ 的正整数解；

(7) $\mathrm{GC}\rightarrow\{m_1,m_2,\cdots,m_n\}:\{c',\mathrm{AS}_1',\mathrm{AS}_2'\}_{K_g}$。

成员 $m_i\ (i=1,2,\cdots,n,i\neq j)$接收到 c',AS_1' 和 AS_2' 后，利用 $c'\equiv y_i' \bmod p_i$ 得到 y_i'，用 y_i' 和 AS_2' 恢复出新盲密钥 S_g'；然后利用 S_g' 和 AS_1' 恢复出新组密钥 K_g'。这样就完成了成员离开的整个密钥更新工作。

由于 GC 没有使用素数 p_j 生成对应的新函数值 y_j'，计算 P' 和 c' 时也没有使用 p_j，所以，即使成员 m_j 能够得到 $c',\mathrm{AS}_1',\mathrm{AS}_2'$ 后，但也不能够得到正确的 y_j'，因而无法恢复正确的新盲密钥 S_g' 以及新组密钥 K_g'。

3.2.3 *周期性更新* 周期性更新时，GC 以一定的时间间隔生成新的组密钥，并进行更新。周期性密钥更新过程：

(1)GC 更新组密钥 K_g 为 K_g'；

(2)GC 利用原来的盲密钥 S_g 更新多项式 $f_1(x)=a_{11}x+a_{10}$ 为 $f_1'(x)=a_{11}'x+a_{10}'$，常数项 $a_{10}'=K_g'$，且 $S_g=f_1'(x_g)=a_{11}'x_g+a_{10}'$ (x_g是盲密钥S_g所对应的变量值)；计算得到 $f_1'(x)$ 的 1 个秘密共享份额 AS_1'；

(3) $\mathrm{GC}\rightarrow\{m_1,m_2,\cdots,m_n\}:\{\mathrm{AS}_1'\}_{K_g}$。

成员 $m_i\ (i=1,2,\cdots,n)$接收到 AS_1' 后，利用原来的盲密钥 S_g 和 AS_1' 恢复出新组密钥 K_g'，这样就完成了整个周期性密钥更新工作。

4 比较与分析

为了评价 CRTSS 方案的性能，我们把更新开销、计算开销、存储开销和安全性这 4 个方面的性能指标作为衡量组播密钥管理方案性能优劣的标准，对 GKMP 和 CRTSS 这两种组播密钥管理方案进行综合评价。其中，更新开销指的是密钥更新时在网络上所传输的更新消息数量或更新消息大小；计算开销指的是为了达到密钥更新而所需要的计算次数或计算时间；存储开销指的是密钥管理方案需要的存储空间大小；安全性指的是组播密钥管理方案的抗攻击能力。

4.1 更新开销、计算开销和存储开销

对 GKMP 和 CRTSS 两种组播密钥管理方案进行比较，如表 1，表 2 和表 3 所示。其中，表 1 表示成员变动引起密钥更新时，各方案的更新开销和计算开销；表 2 表示周期性密钥更新时，各方案的更新开销和计算开销；表 3 表示各方案的存储开销。

表 1 成员变动

Tab.1 Members change

	GKMP	CRTSS
更新开销(bit)	nK	$3K$
GC 计算开销	nC_e+C_r	$C_r+(n+3)Css+2Cc+Cp+Ccc+3Ce$
成员计算开销	C_e	$3Ce+2Cs$

表 2 周期性更新

Tab.2 Periodic rekey

	GKMP	CRTSS
更新开销(bit)	nK	K
GC 计算开销	nC_e+C_r	$C_r+C_{ss}+C_c+C_e$
成员计算开销	C_e	C_e+C_s

表 3 存储开销

Tab.3 Memory cost

	GKMP	CRTSS
GC 存储开销	$(n+1)K$	$(n+7)K$
成员存储开销	$2K$	$3K$

表中符号意义：K为密钥大小(比特)，n为组规模(成员数量)，C_e为一次加密/解密的计算开销，C_r为生成一个新密钥的计算开销，C_s为一次秘密恢复的计算开销，C_{ss}为得到一个共享份额的计算开销，C_c为重新生成一个多项式的计算开销，C_p为按照中国剩余定理计算一次P值的计算开销，C_{cc}为按照中国剩余定理计算一次c值的计算开销。

从上面的分析可以看出，CRTSS 方案消除了 GKMP 方案在成员变动更新密钥时更新开销较大，周期性更新密钥时更新过程复杂，更新开销大，计算开销高的缺陷；具有在周期性更新密钥时更新开销小，计算开销低，在成员变动引起密钥更新时更新开销小的优势，在更新开销性能上有了相当的改进。

4.2 安全性

一般传统的组播密钥管理方案都是利用密钥来加密新密钥进行传送，例如 GKMP 方案。CRTSS 方案引入了中国剩余定理和(2, n)Shamir 秘密共享方法。中国剩余定理是以大素数为基础的密码体系，其安全性在于将几个大素数的乘积重新分解因数往往十分困难。利用Shamir秘密共享方法，能

够通过只传送秘密共享份额来进行密钥更新，避免了传送真实密钥进行密钥更新，降低了真实密钥被截获并破解的概率，增强了CRTSS方案的抗攻击性。只要攻击者未获得用户的私有素数，即使攻击者掌握当前的组密钥K_g，通过密钥更新，攻击者能够得到c', AS_1'和AS_2'，但由于其没有正确的私有素数，仍无法得到新的组密钥K_g'，保证了方案的安全性。CRTSS方案利用中国剩余定理和(2, n)Shamir秘密共享方法来替代传统方案中的真实密钥，大大降低了密钥被截获的可能性，增强了自身的抗攻击性和安全性。

5　结束语

组播密钥管理为组播提供安全保障，为组播应用铺平了道路。传统的集中式平面型组播密钥管理方案具有更新开销大的致命缺陷，导致其可扩展性较弱。本文提出了 CRTSS 组播密钥管理方案，并对 GKMP 和 CRTSS 方案进行了比较和分析。尽管计算开销性能有所降低，但 CRTSS 方案克服了传统集中式平面型方案更新开销大的通病，大大降低了密钥更新开销，提升了整体性能，是一种可靠的、新型的集中式平面型组播密钥管理方案。

参 考 文 献

[1] 王　琳, 解冲锋, 杨明川. IP 组播的关键技术. 信息网络, 2003, 1: 28−33.

[2] 赵膺, 宋佳兴, 徐万鸿, 刘卫东. 安全组播综述. 小型微型计算机系统, 2003, 24(10): 1873−1877.

[3] Eskicioglu A M. Multimedia security in group communications: Recent progress in key management, authentication, and watermarking. *ACM Multimedia Systems*, Special Issue on Multimedia Security. September 2003: 239−248.

[4] Eskicioglu A M, Eskicioglu M R. Multicast security using key graphs and secret sharing. Proceedings of the Joint International Conference on Wireless LANs and Home Networks (ICWLHN 2002) and Networking (ICN 2002), Atlanta, GA, August 26-29, 2002: 228−241.

[5] Hardjono T, Cain B, Monga I. Intra-domain group key management protocol, work in progress, draft-harney-sparta-gsakmp-sec-00.txt, November 1998.

[6] Suvo M. Iolus: A framework for scalable secure multicasting. ACM SIGCOMM Computer Communication Review, New York: ACM Press, 1997, 27 (4): 277−288.

[7] 陈泽文, 张龙军, 王育民, 等. 一种基于中国剩余定理的群签名方案, 电子学报, 2004, 32 (7): 1062−1065.

席国宝：　男，1979 年生，硕士，研究方向为网络通信、网络安全.

陈惠芳：　女，1971 年生，副教授，博士，研究方向为网络通信、网络安全.

赵问道：　男，1966 年生，副教授，博士，研究方向为网络通信.