DOI:10.16515/j.cnki.32-1722/n.2018.04.002

组密钥的分发与全愈

柳亚男[1,2],夏雨欣[1,2],邱 硕[1,2],张 正[1,2]

(1.金陵科技学院网络安全学院,江苏 南京 211169;2.金陵科技学院软件工程学院,江苏 南京 211169)

摘 要:在实时聊天系统等互联网应用中,新加入成员可能希望自动获得历史聊天内容,这一需求称为"历史会话恢复"。针对这一应用需求,提出组密钥"全愈"的概念,支持新加入组成员对历史会话密钥的自动恢复。基于哈希链与Shamir秘密共享,提出具体的组密钥分发与全愈方案。方案能够抵抗合法用户的共谋攻击,哈希函数的单向性保证了方案的后向安全性。方案在不产生额外传输开销的前提下自动、高效地恢复历史密钥。

关键词:全愈;组密钥;哈希函数;拉格朗日多项式

中图分类号:TP309 **文献标识码**:A **文章编号**:1672-755X(2018)04-0005-05

Group Key Distribution and Full-healing

LIU Ya-nan, XIA Yu-xin, QIU Shuo, ZHANG Zheng

(Jinling Institute of Technology, Nanjing 211169, China)

Abstract: In real-time chat systems and other Internet applications, new members may want to automatically get historical chat content, a requirement called "historical session recovery". In view of this application requirement, this paper proposes the concept of "full recovery" of group keys, which supports the automatic recovery of historical session keys by new group members. Based on the secret sharing between hash chain and Shamir, this paper proposes a specific group key distribution and full healing scheme. The scheme can resist the collusion attack of the legitimate users, resist the internal and external attacks of the attackers, and the one-way of the hash function guarantees the background security of the scheme. The scheme automatically and efficiently recovers the historical key without incurring additional transmission.

Key words: full-healing; group key distribution; one-way hash; Lagrange polynomial

安全组通信使用组密钥管理来提供机密性和认证性[1]。传统组密钥管理方案中,同时满足"前向安全"和"后向安全"是重要的安全性特征[2-3]。其中"前向安全"要求,从当前的会话内容中无法获得之前的会话密钥或会话内容。但是,在一些实际的(但不是机密和关键的)应用程序中,如即时通讯系统、大规模多人在线游戏等,"前向安全"并不是必须的。例如,在老同学之间建立的聊天组中,所有组成员可能不会被同时添加,其中一些成员被添加得非常早,而有些成员添加得比较晚。对于新加入的人来说,他们想知道在他们加入之前大家都讨论了些什么。假设此聊天组的授权成员对于聊天内容都具有相同的访问权

收稿日期:2018-07-06

基金项目:江苏省高等学校自然科学研究面上项目(17KJD520003);金陵科技学院高层次人才科研启动基金(jit-b-201639,jit-b-201726);网络安全专项项目(2017YFB0802800)

作者简介:柳亚男(1984—),女,江苏连云港人,讲师,博士,主要从事轻量级密码协议、传感器网络密钥管理、组密钥管理等研究。

限。新加入成员要求获得历史会话密钥,并解密以前的聊天记录。本文将这种需求命名为“历史会话密钥恢复”。

“历史会话密钥恢复”的一个简单的解决方案是向密钥生成中心(KGC)请求历史密钥,但是这会增加额外的通信开销。自2002年起Staddon等[4]提出了一类“自愈”式组密钥分配方案[5-6],使动态组成员即使丢失了一个或多个最新的消息,也能从最近的“密钥分发广播消息”中恢复丢失的会话密钥。“自愈”式的缺点是无法恢复最后一次会话密钥,也就是说,错过当前密钥分发消息的成员必须等到下一次会话分片时才能恢复最后一次会话丢失的密钥。“互愈”式组密钥分发的思想在2005年由Bohio等提出[7],并在2011年由Tian等改进[8]。然而,在“自愈”式和“互愈”式方案中,组成员只能在注册会话期间(依靠自己或邻居)恢复密钥。也就是说,与其他成员相比,新来的人加入聊天小组的时间较晚,不能通过自愈或互愈获得全部的历史记录。

本文基于Shamir秘密共享[9]提出一种新的组密钥分发方式,称为“全愈”式组密钥分发,它可以帮助新加入的组成员完全自主地恢复出历史会话密钥,能够满足要求“历史会话恢复”应用程序的需求,并通过哈希函数的单向性使得方案后向安全得到保证。

1 模型与定义

1.1 通信模型

方案应用于基于密钥生成中心(KGC)的组通信模型中。

通信实体包括一个组管理员与若干组成员。组管理员负责组管理、组员管理与密钥管理。方案目的是在组管理员与组成员之间建立公共的组会话密钥以加密组通信内容,支持新加入成员在不产生额外通信开销前提下对历史会话密钥的自动恢复。

通信组的生命周期被划分为 m 个独立的会话分片,每个会话分片开始时,组管理员选择组密钥,并根据当前组成员信息构造“密钥分发广播消息”在组内广播,组成员可以计算出组密钥,而非组成员即使收到“密钥分发广播消息”也无法计算出组密钥。会话更新在成员变更或会话到期时被触发,新的会话分片开始时,组密钥也要被更新,由此保证方案的后向安全性。

1.2 定义

定义1 组密钥的分配与自愈方案。

令 $U=\{U_1,\cdots,U_n\}$ 表示网络中全体用户的集合,其中一部分用户经过注册组成通信组 G,G 是 U 的动态子集。组管理员负责组的初始化、组成员加入与离开、组密钥分发与撤销及其他维护任务。组成员 U_i 注册时被预分配个人秘密 S_i。通信组 G 的生命周期被划分成 m 个独立的会话分片,$m>0$。在第 j 个会话分片时($j=1,\cdots,m$),令 G_j 表示该组成员集合,即 $G_j\subseteq U$;令 SK_j 表示组密钥,该密钥由组管理员生成并发送给组成员;令 B_j 表示组管理员发送的“密钥分发广播消息”;令 $Z_{i,j}$ 表示组成员 U_i 根据 B_j 和 S_i 计算出的信息;令 R_j 表示从会话分片 j 中退出的成员集合。组管理员GM负责组的初始化、组成员加入与离开、组密钥分发与撤销及其他维护任务。

某一方案 D 如果是组密钥分发与全愈方案,则必须满足以下性质:

1)方案 D 是一个安全的组会话密钥分配方案(由Staddon等提出[4])。a.通信组 G 在第 j 个会话分片 G_j 中的任一组成员 U_i,根据 B_j 和 S_i 计算出密钥信息 $Z_{i,j}$,并能够容易地计算出组密钥 SK_j。b.组退出成员无法共谋计算出任一组成员 U_i 的个人秘密 S_i。c.单独凭借密钥广播信息 $\{B_1,\cdots,B_m\}$ 或用户个人秘密集合 $\{S_1,\cdots,S_n\}$,无法计算出任一组密钥 SK_j。

2)方案 D 具有密钥全愈合性,当且仅当在会话分片 j 中任一新加入的组成员 U_i 能够根据 $Z_{i,j}$ 容易地计算出历史组密钥 $\{SK_l\}_{0<l<j}$。

3)方案 D 具有后向安全性,在会话分片 j 退出的成员集合 R_j 中的任何成员 U_c,无法计算出组密钥 $\{SK_{j+1},\cdots,SK_m\}$。

2　全愈式组密钥分发

2.1　组密钥的分发

2.1.1　**组的初始化**　由组管理员担任密钥生成中心 KGC。KGC 随机选择两个安全素数 p 和 q（即 $p'=(p-1)/2, q'=(q-1)/2$ 也是素数）并计算 $n=pq$（p, q 都是保密的；n 是公开的）。用户空间表示为 $U=\{U_1,\cdots,U_n\}$。KGC 在域 Z_n^* 上构造一个“密钥链”，步骤如下：

1）KGC 从域 Z_n^* 上选择根密钥，记为 K。

2）KGC 计算根密钥 K 的单向哈希链作为“密钥链”。令 H 表示单向哈希函数，令 $H(x)$ 表示关于 x 的哈希值，令 $H^{(m)}(x)=H(H^{(m-1)}(x))=H(H(\cdots H(x)\cdots))$ 表示 x 的 m 阶哈希链。根密钥 K 的单向哈希链表示为：

$$H(K)\rightarrow H^{(2)}(K)\cdots H^{(m-1)}(K)\rightarrow H^{(m)}(K) \tag{1}$$

也可记为：

$$K^{(1)}\rightarrow K^{(2)}\rightarrow\cdots\rightarrow K^{(m-1)}\rightarrow K^{(m)} \tag{2}$$

通信组 G 的生命周期将被划分成 m 个独立的会话分片，KGC 从“密钥链”中为每个会话分片分配会话密钥：

$$Session\text{-}key_1=K^{(m)}$$
$$Session\text{-}key_2=K^{(m-1)}$$
$$\cdots$$
$$Session\text{-}key_m=K^{(1)}$$

2.1.2　**新用户注册**　新加入用户向组管理员 GM 注册的过程如下：

1）网络中某一用户 U_i 向组管理员申请加入通信组，组管理员同意后向该用户发出注册成功通知。

2）KGC 为 U_i 选择个人秘密 $S_i=(x_{U_i}, y_{U_i})$ 并且秘密地把它发送给 U_i，其中 $x_{U_i}\in Z_n^*$，$y_{U_i}\in Z_n^*$，U_i 称为授权用户。

2.1.3　**组密钥分发**　令 $G_j=\{M_1,\cdots,M_t\}$ 表示在第 j 个会话分片时通信组的成员集合，即 $G_j\subseteq U$ 且 $|G_j|=t$。

1）KGC 广播组成员的标识列表 $\{ID_{M_1},\cdots,ID_{M_t}\}$；

2）每个授权成员 M_i 选择一个随机数 R_{M_i} 发送给 GM；

3）KGC 在域 Z_n^* 上构造 t 阶拉格朗日插值多项式：

$$F_j x = \sum_{s=0}^{t} c_s x \tag{3}$$

其中 $F_j(x)$ 经过 $t+1$ 个点：$(x_{M_i}, y_{M_i}\oplus R_{M_i})_{i=1,\cdots,t}$ 和 $(1, Session\text{-}key_j)$。多项式 $F_j(x)$ 的系数计算如下：

$$\begin{bmatrix} c_0 \\ c_1 \\ \cdots \\ c_t \end{bmatrix} = \begin{bmatrix} (x_{M_1})^0 & (x_{M_1})^1 & \cdots & (x_{M_1})^t \\ \cdots & \cdots & \cdots & \cdots \\ (x_{M_t})^0 & (x_{M_t})^1 & \cdots & (x_{M_t})^t \\ 1 & \cdots & \cdots & 1 \end{bmatrix}^{\mathrm{T}} \times \begin{bmatrix} y_{M_1}\oplus R_{M_1} \\ \cdots \\ y_{M_t}\oplus R_{M_t} \\ Session\text{-}key_j \end{bmatrix} \tag{4}$$

4）KGC 选择 $F_j(x)$ 曲线上的另外 t 个点 $Point_s=(x_s, F_j(x_s))_{s=1,\cdots,t}$，计算出消息验证码 MAC_j：

$$MAC_j=H_2(Session\text{-}key_j, ID_{M_1},\cdots,ID_{M_t}, Point_1,\cdots,Point_t) \tag{5}$$

H_2 表示单向哈希函数。KGC 发送“密钥分发广播消息”B_j 给组成员：

$$B_j=\{MAC_j, Point_1,\cdots,Point_t\} \tag{6}$$

5）授权组成员 M_i 根据自己的个人秘密 S_i 和收到的 B_j 计算出多项式 $F_j(x)$ 的系数如下：

$$\begin{bmatrix} c_0 \\ c_1 \\ \cdots \\ c_t \end{bmatrix} = \begin{bmatrix} (x_1)^0 & (x_1)^1 & \cdots & (x_1)^t \\ \cdots & \cdots & \cdots & \cdots \\ (x_t)^0 & (x_t)^1 & \cdots & (x_t)^t \\ (x_{M_i})^0 & \cdots & \cdots & (x_{M_i})^t \end{bmatrix}^{\mathrm{T}} \times \begin{bmatrix} F_j(x_1) \\ \cdots \\ F_j(x_t) \\ y_{M_i}\oplus R_{M_i} \end{bmatrix} \tag{7}$$

进而计算出当前会话分片的组密钥

$$Session\text{-}key_j = F_j(1) \tag{8}$$

2.2 历史会话密钥恢复

通信组在第 j 个会话分片时的任一授权成员 M_i 都能够根据“密钥分发广播消息”B_j 和个人秘密 S_i 计算出当前会话分片的组密钥 $Session\text{-}key_j$。此外，M_i 还可以容易地计算出 $1\sim(j-1)$ 分片的会话组密钥，即“历史会话密钥恢复”：

$$Session\text{-}key_{j-1} = H(Session\text{-}key_j)$$
$$Session\text{-}key_{j-2} = H^{(2)}(Session\text{-}key_j)$$
$$\cdots$$
$$Session\text{-}key_1 = H^{(j-1)}(Session\text{-}key_j) = K^{(m)}$$

3 性能分析

3.1 安全性

本节证明所提出的组密钥分发与全愈方案满足 1.2 节所提出的定义。

定理 1 本文提出的方案是一种安全的组会话密钥分配方案。

证明：本文提出的方案满足定义 1 中的所有要求。

1）在第 j 个会话分片开始，KGC 在域 Z_n^* 上构造一个 t 多项式 $F_j(x)$，它经过 $t+1$ 个点：$(x_{M_i}, y_{M_i}\oplus R_{M_i})_{i=1,\cdots,t}$ 和 $(1, Session\text{-}key_j)$。KGC 在曲线 $F_j(x)$ 上选择另外 t 个点 $Point_s=(x_s, F_j(x_s))_{s=1,\cdots,t}$ 来计算“密钥分发广播消息”B_j 并发送给组成员。通信组 G_j 中任一授权用户 M_i 根据 B_j 与自己的个人秘密 S_i 一起计算出多项式 $F_j(x)$ 的系数，进而得到会话密钥 $Session\text{-}key_j = F_j(1)$。未被授权的网络用户或通信组 G_j 以外的用户，即使通过 B_j 获得了 t 个公共点 $Point_{s=1,\cdots,t}$，也不能构造出多项式 $F_j(x)$。

2）对于授权组成员 $M_i\in G_j$，其个人秘密 $S_i=(x_{M_i}, y_{M_i})$ 是由 KGC 随机生成并在注册阶段秘密分发给 M_i 的。不同成员的个人秘密各不相同，同一用户加入不同通信组被分发的个人秘密也不相同。因此，任何攻击者除非通过物理攻击非法读取，否则无法获得其他成员的个人秘密。

3）KGC 通过结合两部分内容来定义一个多项式 $F_j(x)$：一个会话密钥 $Session\text{-}key_j$ 和 t 个授权成员的个人秘密；授权的组成员也通过两部分内容来重构多项式：自己的个人秘密和 t 个公共点。如果没有公共点信息，各成员的个人秘密只是二维平面上的 t 个离散点，从信息论角度上来看攻击者即使集合这 t 个点也无法共谋出 t 阶多项式 $F_j(x)$。另一方面，一个没有个人秘密的外部攻击者，即使能够通过监听获得“密钥分发广播消息”B_j 中的 t 个点信息 $Point_{s=1,\cdots,t}$，信息论角度上也无法重构出 $F_j(x)$。所以广播消息 $\{B_1,\cdots,B_m\}$ 本身并不提供任何有关会话密钥的信息。

定理 2 本文提出的方案具有“全愈”式属性。

证明：根据 1.2 节内容，会话分片 j 中的任一授权成员 M_i，无论他是新加入的或重新加入的成员，只要他能够正确地计算当前会话密钥 $Session\text{-}key_j$，就可以通过单向函数计算出历史会话密钥。因此，方案具有“全愈”式属性。

定理 3 本文提出的方案抵抗 r 共谋攻击。

证明：令 $R_j=\{RM_1,\cdots,RM_r\}$ 表示在第 j 个会话分片之前从通信组退出的成员集合，即 $R_j\subseteq U$ 且 $|R_j|=r$。R_j 中任意前组成员都无法共谋出当前会话分片的会话密钥。不同用户的秘密具有离散性和随机性，而任何在当前会话分片中未授权的网络用户，即使能获得公共点信息，也无法重构出会话密钥。

定理 4 本文提出的方案具备后向安全性。

证明：令 $R_j=\{RM_1,\cdots,RM_r\}$ 表示在第 j 个会话分片之前从通信组退出的成员集合，即 $R_j\subseteq U$ 且 $|R_j|=r$。因为每个会话分片的密钥是基于单向哈希链的，因此从第 j 个会话分片开始，集合 R_j 中的网络用户都无法计算出退出后会话分片对应的会话密钥 $\{SK_{j+1},\cdots,SK_m\}$。这称为方案具有后向安全性。

3.2 性能与开销

存储开销。本文提出的“全愈”式组密钥分发方案，在节省密钥存储开销方面具有优势。与其他组密钥分发方案[1-3]不同，本方案中组成员不存储历史会话密钥的完整映射，而只存储当前会话分片的单个密钥，历史密钥集可以通过“全愈合”属性导出。这能够降低密钥的存储开销。

计算开销。本方案采用 Shamir 秘密共享来实现组密钥分配，其计算开销主要发生在拉格朗日插值计算和哈希函数计算过程中，这种轻量级的计算特别适用于计算资源受限的设备，如手机、平板电脑等。

通信开销。本方案网络中的通信开销主要发生在密钥分发阶段，其中 KGC 通过一个广播消息分发组会话密钥。当新成员加入时，只有新加入的成员才产生通信和计算开销，而其他组成员不产生任何的通信或计算开销。而且，新加入的成员在恢复历史会话密钥过程中，也不需要依赖 KGC 或其他组成员的帮助，因此也不会产生额外的传输开销。与其他组密钥分发方案[10-11]相比，“全愈”式的属性节省了大量的通信开销，而且还避免了成员之间因身份验证等互操作带来的计算或通信代价。

4 结论与展望

本文提出一种“全愈式”的组密钥分发方案，支持组成员自主进行“历史会话密钥恢复”。“全愈”式的属性使得新加入成员在不依赖于组管理员或其他成员产生额外传输开销的前提下，自动地计算出历史会话密钥，进而恢复历史会话内容。文中给出了“全愈式”组密钥分发方案的定义，提出具体的解决方案，并给出安全性证明和性能分析。未来的工作是寻找除哈希链以外的有效工具，既有良好的单向性与安全性，又不限制会话周期。

参考文献：

[1] Rafaeli S, Hutchison D. A survey of key management for secure group communication[J]. ACM Computer Survey, 2003, 35(3): 309－329

[2] Klaoudatou E, Konstantinou E, Kambourakis G, et al. A survey on cluster-based group key agreement protocols for WSNs[J]. IEEE Communication Survey Tutorials, 2011, 13(3): 429－442

[3] Cho J, Swami A, Chen I. A survey on trust management for mobile Ad Hoc networks[J]. IEEE Communication Survey Tutorials, 2011, 13(4): 562－583

[4] Staddon J, Balfanz D, Miner S, et al. Self-healing key distribution with revocation[J]. Proceedings of the IEEE symposium on Security and Privacy, 2002: 241－257

[5] Rams T, Pacyna P. A survey of group key distribution schemes with self-healing property[J]. IEEE Communication Survey Tutorials, 2013, 15(2): 820－842

[6] Tian B, Han S, Parvin S, et al. Self-healing key distribution schemes for wireless networks: a survey[J]. Computer Journal, 2011, 54(4): 549－569

[7] Bohio M J, Miri A. Self-healing group key distribution[J]. International Journal of Network Security, 2005, 1(2): 110－117

[8] Tian B, Han S, Hu J, et al. A mutual-healing key distribution scheme in wireless sensor networks[J]. Journal of Network & Computer Applications, 2011, 34(1): 80－88

[9] Shamir A. How to share a secret[J]. Communication of the ACM, 1979, 22(11): 612－613

[10] Harn L, Lin C. Authenticated group key transfer protocol based on secret sharing[J]. IEEE Transactions on Computers, 2010, 59(6): 842－846

[11] Liu Y, Cheng C, Cao J, et al. Animproved authenticated group key transfer protocol based on secret sharing[J]. IEEE Transactions on Computers, 2013, 62(11): 2335－2336

（责任编辑：湛　江）