独立群密钥更新模型研究

周 健[1,2] 孙丽艳[1]

(安徽财经大学管理科学与工程学院 蚌埠 233041)[1] (北京邮电大学电子工程学院 北京 100083)[2]

摘 要 针对群组密钥更新中非更新成员参与共享密钥计算增加交互延时的问题,提出了一种独立密钥更新模型,通过门限密钥共享秘密乘积机制和双线性对设计一种独立群组密钥管理方案,群组成员具有满足密钥独立性的解密密钥。公开加密密钥更新不会破坏非更新成员解密密钥的有效性,使得非更新成员不参与密钥加入/退出操作,减少密钥更新延时和计算开销,符合独立密钥更新模型,适用于计算和延时受限的无线网络场景。

关键词 群组密钥管理,密钥更新,密钥独立性,更新延时

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.8.040

Research on Independence Rekey Model for Group Key Management

ZHOU Jian[1,2] SUN Li-yan[1]

(Department of Management Science and Engineering, Anhui University of Finance and Economics, Bengbu 233041, China)[1]

(School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100083, China)[2]

Abstract In group key management, much time is expended in rekeying due to non update members taking part in rekeying to distribute key material. To solve the problem, a novel independence rekeying model was presented, and then an independence group key management was designed based on bilinear pairing and shared production of threshold cryptography, which meets key independence and all non update members don't participate in rekeying for key joining/leaving operation. The fresh public encryption key cannot break the validity of secret decryption keys belonging to non update members. Therefore, the rekeying delay time and computation cost of proposed scheme are reduced efficiently. It also meets the independence rekeying model logically, moreover the scheme is suitable to wireless networks whose time delay and computation are limited strictly.

Keywords Group key management, Rekeying, Key independence, Rekeying time delay

1 引言

群组密钥管理是无线网络安全的基础技术之一,密钥更新是群组密钥管理的重要内容[1,2]。当有成员加入或离开网络时,网络通过密钥更新保证前向/后向安全性[3,4]。目前的密钥管理方案基于单加密密钥单解密密钥协议(One-Decryption-Key One-Encryption-Key Key Protocol, OOKP),一旦加密密钥发生更新,解密密钥也需要更新[5],如 GDH[6]、BD[7]、STR[8]、TGDH[9-11]、DH-LKH[12]等等。随着高性能处理器和能量水平的不断提高[20,21],减少密钥更新延时具有比减少计算开销更为重要的意义,如深空网络、DTN 网络和机会网络等[22,23]。苛刻的延时和非可靠的端到端链接需要延时性能更优的密钥管理方案[13]。

与 OOKP 不同,单加密密钥多解密密钥密钥协议(One-Decryption-Key Multi-Encryption-Key Key Protocol, OMKP)中加密密钥对应多个解密密钥,一个加密密钥加密的密文可被多个不同的解密密钥成功解密,如 SLP[14]、OMDEP[15,16]、PKM[17]、AGKM[18,19]。但是 SLP、OMDEP、AGKM 协议的密钥更新方式需要重新执行协议,更新后的公钥破坏非更新成员解密密钥的有效性,PKM 不满足前向和后向安全性。因此这些方案也存在密钥更新中非更新成员参与共享加密密钥更新的问题,增加了延时和计算开销,该问题成为研究基于单加密密钥多解密密钥密钥协议的密钥更新的一个挑战。本文建立独立密钥更新机制,使得 OMKP 加密密钥更新不会破坏非更新成员解密密钥的合法性和有效性,减少成员交互和计算开销,提高群组密钥更新效率。

2 独立密钥更新模型

2.1 单加密密钥多解密密钥基本模型

在单加密密钥多解密密钥基本模型中,一个加密密钥对应多个解密密钥,解密密钥组成合法解密密钥集合,公钥加密的密文可以被解密密钥集合中的任意解密密钥成功解密。解密密钥具有密钥独立性,即通过一个加密/解密密钥计算得到另一个加密/解密密钥是困难的,如图 1 所示。目前具有该性

到稿日期:2014-08-21 返修日期:2014-12-08 本文受国家自然科学基金项目(61402001),安徽省高等学校自然基金资助项目(KJ2013B001)资助。

周 健(1979—),男,博士后,副教授,CCF 会员,主要研究方向为密钥管理、无线网络安全、深空网络,E-mail:ac_zj_course@163.com;孙丽艳女,硕士,副教授,主要研究方向为网络安全、密钥协议、认知无线电网络。

质的加密解密算法有 SLP、OMEDP 和 AGKA 协议。

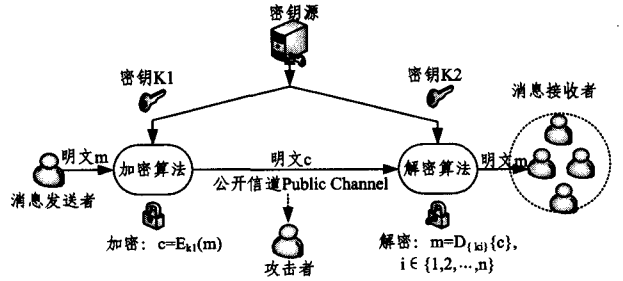

图 1　单加密密钥多解密密钥基本模型

定义 1　单加密密钥多解密密钥加密解密模型(One-Encryption-Key Multi-Decryption-Key Encryption Model, OMEM)，即存在一个加密密钥 $eKey$ 和解密密钥集合 $\{sKey_i\}$，使用相同加密密钥加密的信息能够被多个不同的解密密钥解密。满足如下的条件：

$$\begin{cases} eKey_i \neq eKey_j, eKey_i \in \{eKey_i\}, eKey_j \in \{eKey_i\} \\ R(eKey_i) \neq eKey_j \\ D_{sKey_i}(E_{eKey}(m)) = m \\ D_{sKey_i}(E_{eKey}(m)) = D_{sKey_j}(E_{eKey}(m)) \\ D_{sKey_k}(E_{eKey}(m)) \neq m, sKey_k \notin \{eKey_i\} \end{cases} \tag{1}$$

式(1)的第一行和第二行说明，两个不同的解密密钥属于集合$\{sKey_i\}$，且不存在一个函数能够根据 $sKey_i$ 求出 $sKey_j$，满足密钥独立性。第三行和第四行说明 $sKey_i$ 和 $sKey_j$ 都能对 $eKey$ 加密的秘密正确解密。最后一行说明非$\{sKey_i\}$中的解密密钥不能对 $eKey$ 加密秘密正确解密。

2.2　单加密密钥多解密密钥更新模型

单加密密钥多解密密钥密钥更新模型(One-Encryption-Key Multi-Decryption-Key Rekeying Model, OMRM)的密钥更新有两种形式(见图 2)：①全部密钥更新，成员私有的解密密钥即使不泄露，也会因为公开加密密钥更新，需要所有成员重新计算、更新私有解密密钥；②部分密钥更新，仅有部分成员的密钥需要更新，当有成员加入或者退出时，仅仅加入/退出成员的私有解密密钥和公开加密密钥需要被更新，而其他成员的密钥无需更新。在后一种方式中非更新成员的解密密钥仍具有合法性和有效性。在效率上，因为成员间的交互减少，非更新成员计算开销降低，进而提高了密钥更新效率。

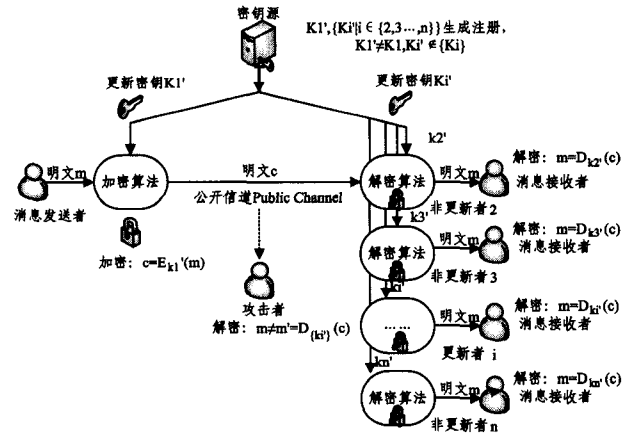

图 2　单加密密钥多解密密钥密钥更新模型

目前基于 OMRM 的密钥管理有 SLP、OMEDP、AGKA。由于密钥之间的关联性，或者解密密钥和加密密钥通过门限密钥机制生成，密钥资料的变化会引发其他密钥资料的变化，因此在成员加入/退出时为保证前向安全性和后向安全性，密钥管理者需要重新为每个成员计算秘密私钥和公开的加密密钥。密钥更新规模与网络的规模相关，更新效率因网络规模增加而降低。

2.3　独立更新模型

在独立单加密密钥多解密密钥密钥更新模型(Independence One-Encryption-Key Multi-Decryption-Key Rekeying Model, IOMRM)(见图 3)中，解密密钥之间具有密钥独立性，在密钥更新中非更新成员的秘密解密密钥不会因更新者的密钥变化而发生变化，因此保留非更新成员的秘密解密密钥不会产生前向和后向安全性问题。密钥源具有在保证非更新成员私有解密密钥的合法性的前提下对加密密钥和更新成员解密密钥更新的能力。在 IOMRM 中，非更新成员不参与更新过程，减少了交互过程，缩小了密钥更新规模，提高了密钥更新效率。目前，AGKA 协议在节点退出时的密钥更新具有该性质，而在节点加入过程中，尽管能保证成员私有解密密钥的合法性，但仍旧需要全部节点重新计算公开加密密钥资料。

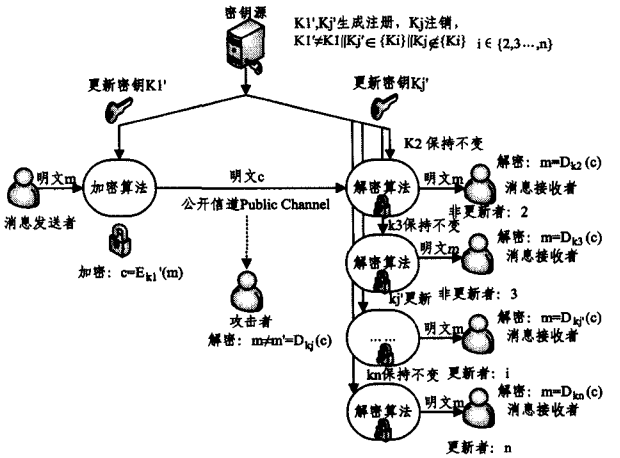

图 3　独立密钥更新模型

定义 2(独立密钥更新模型)　该模型中私有解密密钥 $sKey_i$ 更新不会引发其他成员的私有解密密钥 $sKey_j, i \neq j$ 更新，$sKey_i$ 更新后 $sKey_j$ 仍旧可以对更新的加密密钥 $eKey'$ 加密的信息解密，满足如下的条件：

$$\begin{cases} D_{sKey_i'}(E_{eKey'}(m)) = m \\ D_{sKey_j}(E_{eKey'}(m)) = m \\ R(sKey_i) \neq sKey_i' \\ R'(sKey_i') \neq sKey_j \end{cases} \tag{2}$$

相对于 OORM，IOMRM 不会破坏非更新节点解密密钥的合法性和有效性，更新规模限定在单个节点内。无论在 OMRM 还是 IOMRM 中，对于加密密钥的更新都是依赖密钥源执行，密钥管理成员(秘密解密密钥拥有者)不具有对加密密钥更新的能力，OMEDP 依赖 KMC 执行密钥更新过程，成员退出时，新鲜公钥引发 KMC 必须为剩余成员计算新解密密钥，AGKM 中非更新成员需要重新计算更新成员秘密解密密钥加工的公开密钥资料才能得到公开解密密钥。

3　独立密钥管理方案

在独立密钥管理方案(Independence Key Management Scheme, IKMS)中有一个密钥管理中心 KMC 和 n 个空间实

体消息接收方。设 $E_k(\cdot)$为对称密钥加密算法，$D_k(\cdot)$为对称密钥解密算法，$H(\cdot)$为哈希函数。

3.1 IKMS-DSDTN 协议初始化

步骤 1　KMC 从整数域 Z_p 内随机选择 $\alpha+\beta$ 个随机数 $\{a_1,a_2,\cdots,a_{\alpha-1},b_1,b_2,\cdots,b_{\beta-1},S_{k1},S_{k2}\}$并秘密保存，构造两个方程式，其中 $g_1(x)$为一元 $\alpha-1$ 次多项式，$g_2(x)$为一元 $\beta-1$ 次多项式，它们的形式表达如下：

$$\begin{cases} g_1(x)=\sum_{i=1}^{i=\alpha-1} a_i x^i+S_{k1} \\ g_2(x)=\sum_{i=1}^{i=\beta-1} b_i x^i+S_{k2} \end{cases} \tag{3}$$

令一元 $\alpha+\beta-2$ 次方程 $f(x)$为

$$f(x)=g_1(x)g_2(x)=(\sum_{i=1}^{i=\alpha-1} a_i x^i+S_{k1})(\sum_{i=1}^{i=\beta-1} b_i x^i+S_{k2}) \tag{4}$$

步骤 2　KMC 随机选择 $x+yn(x+y>\alpha+\beta-2, y<\beta-1, x>\alpha-1)$个不同的元素，组成如下的集合形式：

$V=\{v_{0,1},v_{0,2},\cdots,v_{0,i},\cdots,v_{0,x}\}$

$R_j=\{r_{j,1},r_{j,2},\cdots,r_{j,i},\cdots,r_{j,y}\}, j\in\{1,2,\cdots,n\}$

步骤 3　KMC 将 $S_{k1}S_{k2}$ 作为主加密密钥，计算 $Q_S=S_{k1}S_{k2}P\in G_1$；

步骤 4　KMC 选择两个元素 $Q_1,Q_2\in G_1$，计算如下的值：

$$\begin{aligned} V^*&=f(V)P=g_1(V)g_2(V)P \\ &=\{g_1(v_{0,1})g_2(v_{0,1})P,g_1(v_{0,2})g_2(v_{0,2})P,\cdots, \\ &\quad g_1(v_{0,x})g_2(v_{0,x})P\} \\ R_{1j}^*&=g_1(R_j)(Q_1+Q_2) \\ &=\{g_1(r_{j,1})(Q_1+Q_2),g_1(r_{j,2})(Q_1+Q_2),\cdots, \\ &\quad g_1(r_{j,y})(Q_1+Q_2)\} \\ R_{2j}^*&=g_2(R_j)P \\ &=\{g_2(r_{j,1})P,g_2(r_{j,2})P,\cdots,g_2(r_{j,y})P\}, j\in\{1,2,\cdots,n\} \end{aligned}$$

该阶段结束后，加密者具有的参数有：

$\langle p,G_1,G_2,e,P,Q_1,Q_2,Q_s,V^*,\{R_{1j}^*\},\{R_{2j}^*\}\rangle$

其中，Q_s 为消息发送者的加密主密钥，R_{1j}^* $(j\in\{1,2,\cdots,n\})$为接收方 $user_j$ 的解密密钥。

3.2 IKMS 加密阶段

KMC 向实体发送秘密消息 m 时，计算过程如下：

步骤 1　随机选择一个秘密数 r，计算 $Q_1^*=rQ_1$；

步骤 2　KMC 计算加密密钥 $k=(k_1,k_2)=H(id\|P^*\|Q_s\|r)$，计算 $c=E_{k_1}(m)$，$mac=H(m,k_2)$和 $\lambda=e(Q_S,Q_2)^r k$；

步骤 3　KMC 计算 $S^{**}=rS^*=\{rg_1(v_{0,1})g_2(v_{0,1})P,rg_1(v_{0,2})g_2(v_{0,2})P,\cdots,rg_1(v_{0,x})g_2(v_{0,x})P\}$和 $R_{2j}^*=rg_2(R_j)P=\{rg_2(r_{j,1})P,rg_2(r_{j,2})P,\cdots,rg_2(r_{j,y})P\}$；

步骤 4　KMC 公布加密信息 $c^*=\langle c,mac,\lambda,Q_1^*,S^{**},R_{2j}^*\rangle$。

3.3 IKMS 密钥更新阶段

当有实体加入和退出时，网络需要更新密钥，该方案只需要 KMC 更新自己的加密资料，而实体无需更新自己的秘密解密密钥。如果是新节点加入，不失一般性，设新加入的节点为 $user_{n+1}$，更新步骤如下：

步骤 1　KMC 为 $user_{n+1}$ 选择 y 个随机数 $R_{n+1}=\{v_{n+1,1},v_{n+1,2},\cdots,v_{n+1,y}\}$，得到新集合$\{R_j\,|\,j\in\{1,2,\cdots,n+1\}\}$；

步骤 2　KMC 注销方程 $g_2(x)$，随机选择系数$\{b_1',b_2',\cdots,b_{\beta-1}',S_{k_2}'\}$，得到方程 $g_2'(x)=\sum_{i=1}^{\beta-1} b_i' x^i+S_{k_2}'$；则令一元 $\alpha+\beta-2$ 次方程 $f'(x)$为

$$\begin{aligned} f'(x)&=g_1(x)g_2'(x) \\ &=(\sum_{i=1}^{i=\alpha-1} a_i x^i+S_{k1})(\sum_{i=1}^{i=\beta-1} b_i' x^i+S_{k2}') \end{aligned} \tag{5}$$

步骤 3　KMC 重新计算 V^* 和 R_{2j}^*：

$$\begin{aligned} V^*&=f'(V)P=g_1(V)g_2'(V)P \\ &=\{g_1(v_{0,1})g_2'(v_{0,1})P,g_1(v_{0,2})g_2'(v_{0,2})P,\cdots, \\ &\quad g_1(v_{0,x})g_2'(v_{0,x})P\} \end{aligned} \tag{6}$$

$$\begin{aligned} R_{2j}^*&=g_2'(R_j)P \\ &=\{g_2'(r_{j,1})P,g_2'(r_{j,2})P,\cdots,g_2'(r_{j,y})P\}, j\in\{1,2, \\ &\quad \cdots,n+1\} \end{aligned} \tag{7}$$

如果是节点退出网络，不失一般性，设退出节点为 $user_n$，更新步骤如下：

步骤 1　KMC 注销方程 $g_2(x)$，将 $user_n$ 对应的值 $R_n=\{v_{n,1},v_{n,2},\cdots,v_{n,\beta}\}$从集合$\{R_j\,|\,j\in\{1,2,\cdots,n\}\}$中删除；

步骤 2　KMC 随机选择系数$\{b_1',b_2',\cdots,b_{\beta-1}',S_{k2}'\}$，得到方程 $g_2'(x)=\sum_{i=1}^{\beta-1} b_i' x^i+S_{k2}'$；则令一元 $\alpha+\beta-2$ 次方程 $f'(x)$为

$$\begin{aligned} f'(x)&=g_1(x)g_2'(x) \\ &=(\sum_{i=1}^{i=\alpha-1} a_i x^i+S_{k1})(\sum_{i=1}^{i=\beta-1} b_i' x^i+S_{k2}') \end{aligned} \tag{8}$$

步骤 3　KMC 重新计算 V^* 和 R_{2j}^*：

$$\begin{aligned} V^*&=f'(V)P=g_1(V)g_2'(V)P \\ &=\{g_1(v_{0,1})g_2'(v_{0,1})P,g_1(v_{0,2})g_2'(v_{0,2})P,\cdots, \\ &\quad g_1(v_{0,x})g_2'(v_{0,x})P\} \end{aligned} \tag{9}$$

$$\begin{aligned} R_{2j}^*&=g_2'(R_j)P \\ &=\{g_2'(r_{j,1})P,g_2'(r_{j,2})P,\cdots,g_2'(r_{j,y})P\}, j\in\{1,2, \\ &\quad \cdots,n-1\} \end{aligned} \tag{10}$$

4　性能分析

4.1　正确性分析

空间实体只有正确地获取解密从而密钥 k 才能对密文 c 解密从而得到明文 m，因此对明文的正确解密依赖于加密密钥获取的正确性。如果解密者具有合法的解密密钥集合$\{R_j^*,j\in\{1,2,\cdots,n\}\}$，且已知 $\pi''=\{v_{0,1},v_{0,2},\cdots,v_{0,x},r_{i,1},r_{i,2},\cdots,r_{i,y}\}$，则对 k 的正确获取可以表示为：

$$\begin{aligned} &\frac{e(Q_1^*,Q_s)\lambda}{e(Q_1+Q_2,\sum_{i=1}^{i=x}\omega_{v_{0,i},\pi''}(0)\times rf(v_{0,i})p)\prod_{j=1}^{y}e(\omega_{r_{i,j},\pi''}(0)g_1(r_{i,j})(Q_1+Q_2),g_2(r_{i,j})rP)} \\ =&\frac{e(Q_1^*,Q_s)e(Q_S,Q_2)^r k}{e(Q_1+Q_2,\sum_{i=1}^{i=x}\omega_{v_{0,i},\pi''}(0)\times rf(v_{0,i})p)\prod_{j=1}^{y}e(\omega_{r_{i,j},\pi''}(0)g_1(r_{i,j})g_2(r_{i,j})(Q_1+Q_2),rP)} \\ =&\frac{e(rQ_1,Q_s)e(rQ_S,Q_2)k}{e(Q_1+Q_2,\sum_{i=1}^{i=x}\omega_{v_{0,i},\pi''}(0)\times rf(v_{0,i})p)e(\sum_{j=1}^{y}\omega_{r_{i,j},\pi''}(0)g_1(r_{i,j})g_2(r_{i,j})(Q_1+Q_2),rP)} \end{aligned}$$

$$=\frac{e(Q_1+Q_2,rQ_s)}{e(Q_1+Q_2,\sum_{i=1}^{i=x}\omega_{v_{0,i},\pi''}(0)\times rf(v_{0,i})p)e(\sum_{j=1}^{y}\omega_{r_{i,j},\pi''}(0)g_1(r_{i,j})g_2(r_{i,j})rP,(Q_1+Q_2))}$$

$$=\frac{e(Q_1+Q_2,rQ_s)}{e(Q_1+Q_2,(\sum_{i=1}^{i=x}\omega_{v_{0,i},\pi''}(0)\times f(v_{0,i})+\sum_{j=1}^{y}\omega_{r_{i,j},\pi''}(0)g_1(r_{i,j})g_2(r_{i,j}))rP)}$$

$$=\frac{e(Q_1+Q_2,rQ_s)}{e(f(0)rP,(Q_1+Q_2))}=\frac{e(Q_1+Q_2,rS_{k1}S_{k2}P)}{e(S_{k1}S_{k2}rP,(Q_1+Q_2))}=k \tag{10}$$

4.2 前向后向安全性

由于OMEDP方案不能抵御合谋攻击，因此OMEDP方案也不能保证前向和后向安全性，当有超过门限值数量的节点加入或退出时，它们可以合谋得到加入前或加入后的密文。在IKMS加密方案中，密文的安全性取决于加密密钥，而加密密钥不仅由主密钥 Q_s 控制，而且也受到加密者随机选择的随机数 r 控制，因此即使主密钥 Q_s 泄漏，单个攻击者也不能恢复出加密密钥。方程 $f(x)$，$g_1(x)$，$g_2(x)$ 的系数对新加入者和退出者都是未知的，因此新加入者和退出者不能根据方程计算密钥碎片，当节点加入网络中时，KMC更新方程 $g_2(x)$，并更新对应的 $\{R_{2j}^*\}$ 值，使得新加入者在解密中使用 $R_{2n+1}^*=g_2'(R_{n+1})P=\{g_2'(r_{n+!,1})P,g_2'(r_{n+!,2})P,\cdots,g_2'(r_{n+!,y})P\}$ 只能恢复出更新后的主密钥 $Q_s'=S_{k1}S_{k2}'P$，而由于新加入者没有 $R_{2n+1}^*=g_2(R_{n+1})P=\{g_2(r_{n+!,1})P,g_2(r_{n+!,2})P,\cdots,g_2(r_{n+!,y})P\}$ 不能恢复更新前的主密钥 $Q_s=S_{k1}S_{k2}P$，从而保证了密钥更新的后向安全性；当节点退出网络时，同理KMC更新方程 $g_2(x)$，并更新对应的 $\{R_{2j}^*\}$ 值，使得退出者在解密中只能恢复出更新前的主密钥 $Q_s=S_{k1}S_{k2}P$，而由于没有 $R_{2n+1}^*=g_2'(R_n)P=\{g_2'(r_{n,1})P,g_2'(r_{n,2})P,\cdots,g_2'(r_{n,y})P\}$ 不能恢复出更新后的主密钥 $Q_s'=S_{k1}S_{k2}'P$，因此保证了前向安全性。

加密阶段，密文形式为 $c^*=\langle c,mac,\lambda,Q_i^*,S^{**},R_{2j}^*\rangle$，设 G_1 和 G_2 的长度为 N_1，$E_k(\cdot)$ 的输出长度为 N_2，$H(\cdot)$ 的输出长度为 N_3，则通信复杂度为 $(x+yn+2)N_1+N_2+N_3$，与网络规模呈线性关系。

协议中双线性对运算具有较高的计算复杂度，包括倍加、模乘和指数运算。在密钥初始化中，执行2次倍加运算计算主密钥 Q_S，执行 x 次倍加运算计算 V^*，执行 ny 次倍加运算计算 $\{R_{1j}^*\}$，执行 ny 次倍加运算计算 $\{R_{2j}^*\}$，共执行 $x+2ny+2$ 次双线性对倍加运算。在加密过程中，执行1次倍加运算计算 Q_i^*，执行 x 次倍加运算计算 S^{**}，执行 ny 次倍加运算计算 R_{2j}^*，执行1次指数运算计算 λ，因此执行 $x+yn+1$ 次倍加运算和1次指数运算。在解密过程中，分母部分，执行 x 次倍加运算计算 $\sum_{i=1}^{i=x}\omega_{v_{0,i},\pi''}(0)\times rf(v_{0,i})p$，执行 y 次倍加运算和 y 次模乘运算计算 $\prod_{j=1}^{y}e(\omega_{r_{i,j},\pi''}(0)g_1(r_{i,j})(Q_1+Q_2),g_2(r_{i,j})rP)$，在分子执行1次模乘运算，所以总共执行 $x+y$ 次倍加运算和 $y+2$ 模乘运算。

在IKMS方案中，非加入或退出节点无需更新自己的秘密值，因此消息开销和网络负载为零；KMC为重新计算主密钥，需要重新对 V^* 和 R_{2j}^* 的值进行更新，新节点加入时计算量为 $\alpha+(n+1)(\beta-1)$ 次倍加运算，节点退出时，计算量为 $\alpha+(n-1)(\beta-1)$ 次倍加运算。在OMEDP方案中，当有节点加入或退出时，为了前向和后向安全性，需要重新执行协议1次，为每个成员发送新的秘密主密钥碎片，设门限密钥方程的次数也为 $\alpha+\beta-2$，且加密者拥有 x 份碎片，解密者拥有 y 份碎片，因此一旦成员加入，重新选择方程计算主密钥碎片，执行 $x+(n+1)(y-1)$ 次倍加运算。同理，节点退出时，执行 $x+(n-1)(y-1)$ 次倍加运算，为网络成员重新分配秘密主密钥碎片，需要为剩余的节点通过安全信道发送 $n+1$ 次消息和 $n-1$ 次消息。每个接收者接收的密钥碎片数量为 β，因此网络负载分别为 $(n+1)\beta N_1$ 和 $(n-1)\beta N_1$。两种方案的更新性能比较如表1所列。从以上更新性能对比可以看出，两种方案在计算开销上等同，但IKMS在消息开销和网络负载方面具有更好的性能，且无需保证全网络成员在密钥管理中的同步性。

表1 IKMS与OMEDP更新性能比较

方案	计算开销		消息开销		网络负载	
	加入	退出	加入	退出	加入	退出
IKMS	x+(n+1)y	x+(n−1)y	0	0	0	0
OMEDP	x+(n+1)y	x+(n−1)y	n+1	n−1	(n+1)*yN1	(n−1)yN1

4.3 密钥独立性

尽管每个成员的解密密钥都由方程 $f(x)=(\sum_{i=1}^{i=g-1}a_ix^i+S_{k1})(\sum_{i=1}^{i=g-1}b_ix^i+S_{k2})$ 生成，参数 $\{a_i\}$ 和 $\{b_i\}$ 对于成员是未知的，因此根据自身的解密密钥求解其他成员的秘密解密密钥是一个困难问题。同时，IKMS中，在加入/退出事件中，非加入/退出成员无需参与密钥更新过程，即加入或退出中公开加密密钥的更新不会破坏其他非更新成员解密密钥的合法性和有效性。如式(11)所示，IKMS方案的密钥更新过程满足式(2)，更新后的公开加密没有破坏非更新成员的解密密钥，解决了密钥更新过程中更新加密密钥破坏非更新成员秘密解密密钥有效性的问题，符合独立密钥更新模型，降低了密钥更新中的交互延时和计算开销。

$$\begin{cases} sKey_i'=R_{1i}^*=\{g_1(r_{i,1})p,g_1(r_{i,2})p,\cdots,g_1(r_{i,y})p\} \\ eKey'=\langle\{g_1(v_{0,1})g_2'(v_{0,1})P,g_1(v_{0,2})g_2'(v_{0,2})P,\cdots, \\ \qquad g_1(v_{0,x})g_2'(v_{0,x})P\},\{g_2'(r_{j,1})P,g_2'(r_{j,2})P, \\ \qquad \cdots,g_2'(r_{j,y})P\},Q_S=S_{k1}S_{k2}'P\rangle \\ sKey_j=R_{1j}^*,j\in\{1,2,\cdots,i,\cdots,n\},j\neq i \\ D_{sKey_i'}(E_{eKey'}(m))=m \\ D_{sKey_j}(E_{eKey'}(m))=m \\ R(sKey_i)\neq sKey_i' \\ R'(sKey'_i)\neq sKey_j \end{cases} \tag{11}$$

结束语 针对基于OOKP的密钥管理方案在密钥更新中引发较多的交互，导致延时较长的问题，基于OMKP通过门限密钥的共享秘密乘积机制和双线性对提出一种安全性更高的单加密密钥多解密密钥的组播密钥管理方案IKMS。该方案保持了单加密密钥多解密密钥的性质，不同解密密钥具有对同一加密密钥解密的能力。在密钥更新上，该方案利用共享秘密乘积机制将密钥碎片分为两个因子，组成员秘密保

（下转第214页）

[30] 彭云辉. 基于 AUTOSAR 的汽车电子操作系统及其应用的建模与分析[D]. 上海:华东师范大学,2014
Peng Yun-hui. Modeling and analysis of AUTOSAR OS and application [D]. Shanghai: East China Normal University, 2014

[31] Alkassar E, Böhme S, Mehlhorn K, et al. Verification of certifying computations[M]// Gopalakrishnan G, Qadeer S, eds. Computer Aided Verification. Springer Berlin Heidelberg, 2011: 67-82

[32] Alkassar E, Hillebrand M A, Paul W J, et al. Automated verification of a small hypervisor[M]// Leavens G, O'Hearn P, Rajamani S, eds. Verified Software: Theories, Tools, Experiments. Springer Berlin Heidelberg, 2010: 40-54

[33] Shadrin A. Mixed low-and high level programming language semantics and automated verification of a small hypervisor[D]. Saarbrucken: Saarland University, 2012

[34] The OSEK/VDX Group. OSEK/VDX Operating System specification Version 2. 2. 3[S/OL]. http://www. osek-vdx. org/: The OSEK/VDX Group, 2005

[35] AUTOSAR GbR. Technical Safety Concept Status Report V1. 0. 0 R4. 0 Rev 1[S/OL]. http://www. autosar. org/: AUTOSAR GbR, 2009

[36] 陈丽蓉,燕立明,罗蕾. 汽车电子嵌入式操作系统的隔离保护机制[J]. 电子科技大学学报,2014,43(3):450-456
Chen Li-rong, Yan Li-ming, Luo Lei. An isolation and protection mechanism of automotive electronic embedded operating system [J]. Journal of University of Electronic Science and Technology of China, 2014, 43(3): 450-456

[37] Alkassar E, Böhme S, Mehlhorn K, et al. A Framework for the Verification of Certifying Computations[J]. Journal of Automated Reasoning, 2014, 52(3): 241-273

(上接第 193 页)

存其中一个因子,KMC 保留另一个因子,主密钥的更新依赖 KMC 保留因子的更新,使得当有节点加入或退出时,合法成员的秘密解密密钥保持不变,减少了密钥更新时延。在安全性上,IKMS 方案支持前向/后向安全性,且无需安全信道的支持,具有比 OMEDP 更高的安全性。综合上述,IKMS 方案适合对密钥更新延时要求严格的动态网络。

参 考 文 献

[1] Akyildiz I F, Xudong W. A survey on wireless mesh networks [J]. IEEE Communications Magazine, 2005, 43(9): 23-30

[2] Yihchun H, Perrig A. A survey of secure wireless ad hoc routing [J]. IEEE Security and Privacy, 2004, 2(3): 28-39

[3] 李先贤,怀进鹏,刘旭东. 群密钥分配的动态安全性及其方案[J]. 计算机学报,2002,25(4):337-336
Li Xian-xian, Huai Jin-peng, Liu Xu-dong. Dynamic Security of group key Distribution and its Solutions[J]. Chinese Journal of Computers, 2002, 25(4): 337-345

[4] Johann M, Dawoud D, Stephen M. A survey on peer-to-peer key management for mobile ad hoc networks [J]. ACM Computing Surveys, 2007, 39(1): 1-46

[5] Yacine C, Hamida S. Group Key Management Protocols: A Novel Taxonomy [J]. International Journal of Information Technology, 2005, 2(2): 105-119

[6] Steiner M, Tsudik G, Waidner M. Diffie-Hellman Key Agreement Protocol with Key Confirmation [C]// Proceedings of Indocrypt 2000. LNCS 1977, Springer-Verlag, 2000: 237-249

[7] Burmester M, Desmedt Y. A Secure and Efficient Conference Key Distribution System [C]// Proceedings of Eurocrypt 1994. LNCS 950, Spring-Verlag, 1995: 275-286

[8] Steer D, Strawczynski L L, Diffie W, et al. A Secure Audio Teleconference System[C]// CRYPTO'88. 1988: 520-528

[9] Kim Y, Perrig A, Tsudik G. Communication-Efficient group Key Agreement [C]// IFIP SEC. June 2001

[10] Kim Y, Perrig A, Tsudik G. Tree-based group key agreement [J]. ACM Transactions on Information System Security, 2004, 7(1): 60-96

[11] L Li-jun, Manulis M. Tree-based group key agreement framework for mobile Ad-Hoc networks [J]. Future Generation Computer Systems, 2007, 23(16): 787-803

[12] Kim Y, Perrig A, Tsudik G. Simple and fault-tolerant Key Agreement for Dynamic Collaborative Groups [C]// 7th ACM Conference on Computer and Communications Security. 2000: 235-244

[13] Abdullatif S, Melek Ö, Refik M. Local key management in opportunistic networks[J]. International Journal of Communication Networks and Distributed Systems, 2012, 9(1/2): 97-116

[14] Chiou G H, Chen W T. Secure Broadcast using Secure Lock [J]. IEEE Transactions on Software Engineering, 1989, 15(8): 929-934

[15] Kurosawa K. Multi-recipient public-key encryption with shortened ciphetext[C]// Proceedings of 5th International Workshop on Practice and Theory in Public Key Cryptosystem. Paris, France, 2002: 48-63

[16] Liao P, Hui X L, P Qing-qi, et al. A Public Key Encryption Scheme with One-Encryption and Multi-Decryption[J]. Chinese Journal of Computers, 2012, 35(5): 1059-1067

[17] Abdel A K. Cryptanalysis of a Polynomial-based Key Management Scheme for Secure Group Communication[J]. International Journal of Network Security, 2013, 15(1): 68-70

[18] W Qian-hong, Yi M, Willy S, et al. Asymmetric Group Key Agreement[C]// Proceedings of the 28th Annual International Conference on Advances in Cryptology: the Theory and Applications of Cryptographic Techniques (EUROCRYPT'09). 2009: 153-170

[19] Lei Z, W Qian-hong, Bo Q, et al. Asymmetric group key agreement protocol for open networks and its application to broadcast encryption[J]. Computer Networks, 2011, 65(15): 3246-3255

[20] Alkalai L. An overview of flight computer technologies for future NASA space exploration missions[J]. Acta Astronautica, 2003, 52(9-12): 857-867

[21] Cassady R J, Frisbee R H, Gilland J H, et al. Recent advances in nuclear powered electric propulsion for space exploration[J]. Energy Conversion and Management, 2008, 49(3): 412-435

[22] Davarian F, Popken L. Technical advances in deep space communications and tracking[J]. Proceedings of the IEEE, 2007, 95 (11): 2108-2110

[23] 熊永平,孙利民,牛建伟,等. 机会网络[J]. 软件学报,2009,20(1):124-137
Xiong Yong-ping, Sun Li-min, Niu Jian-wei, et al. Opportunistic Networks[J]. Journal of Software, 2009, 20(1): 124-137