第 35 卷 第 4 期 计 算 机 工 程 2009 年 2 月
Vol.35 No.4 Computer Engineering February 2009
·安全技术· 文章编号：1000—3428(2009)04—0157—02 文献标识码：A 中图分类号：TP309.7

新的随机化广播加密方案

赖 霞，陈利娅，何明星
(西华大学数学与计算机学院，成都 610039)

摘 要：提出一种新的随机化广播加密方案，通过构建随机函数族为用户分配密钥，可以使合法用户以概率 1 获取解密密钥，而用户的密钥存储仅为 $(l+1)$ 个，与其他基于二叉树结构的方案相比，该方案在密钥存储量上具有显著优势，在一定条件下可使传输成本最小化。
关键词：广播加密；随机函数族；多方退出

New Randomized Broadcast Encryption Scheme

LAI Xia, CHEN Li-ya, HE Ming-xing
(School of Mathematics & Computer, Xihua University, Chengdu 610039)

【Abstract】Broadcast encryption scheme is a wildly used scheme in group security communication, which has good application foreground in such fields as pay-TV, video-conferencing, and Wireless Sensor Network(WSN). This paper presents a new randomized broadcast encryption scheme, which distributes keys for users by constructing family of random functions. It makes legal users gain decryption keys with probability as one, and the key storage number of users is (l+1). Compared with other schemes based on binary tree structure, this scheme has advantages in quantity of key storage, and it reduces transmission cost to minimum under some conditions.
【Key words】broadcast encryption; family of random functions; multiple revocation

1 概述

在每次会话中，会话中心(GC)都必须加密会话密钥，并将加密后的秘密信息在不安全的信道上分发给动态用户群，只有拥有特权的合法用户才能解密秘密信息，文献[1]提出了广播加密方案。本文提出一种新的随机化广播加密(Randomized Broadcast Encryption, RBE)方案。该方案通过随机函数族[2-3]构建 l 个相互独立(辅助)的密钥池。在系统开始运行前，每个用户从每个密钥池获得一个密钥。在加密阶段，会话中心只需用退出用户不拥有的其他(辅助)密钥加密会话密钥即可。在解密阶段，对于未退出用户，在一定程度上总能找到一个密钥与会话中心在加密会话密钥时所使用的密钥相匹配，当然，对于退出用户，即使他们全部联合起来也不可能得到解密密钥。该方案在多方退出[3]操作上简捷有效，在用户密钥存储和传输成本等方面较文献[4-5]中的方案具有一定优势。

2 新的随机化广播加密方案

下面先定义几个参数，注册用户集合用 N 来表示，设 $N=\{U_1,U_2,\cdots,U_n\}$，R 是退出用户集合，假定其元素个数 $|R|=r$，$r\in[0,n]$，用户 U_i 对应其解密密钥(辅助密钥) K_i，K 为此次会话密钥，M 为此次会话的明文消息。

(1)初始化

1)随机函数族的构造：假定 N，M，S 是 3 个有限集合，元素个数分别为 n,m,l。现构造一个随机函数族：$\{f_s\,|\,f_s:N\to M,s\in S\}$，要求 $f_s:N\to M$ 是满射，简记为 $(f_s)_{s\in S}$。

2)密钥生成：会话中心用 $(f_s)_{s\in S}$ 给每个用户生成 l 个辅助密钥，如用户 u_i 获得对应的辅助密钥是 $K(u_i)=\{k_{s,f_s(i)}\,|\,s\in S\}$，因此，会话中心共生成 lm 个辅助密钥，记为 $\kappa=\{k_{s,v}\,|\,s\in S,v\in M\}$。另外，会话中心再随机选取一个与用户单独共享的密钥，如与用户 u_i 共享密钥 K_{Gi}，$i=1,2,\cdots,n$，该共享密钥用于当用户的 l 个辅助密钥都无法解密中心广播的消息时，可供与中心保持通信。中心将 l 个辅助密钥和共享密钥一并秘密分发给每个对应用户。

(2)广播加密

1)加密密钥生成：假设有 $r(r\le n)$个用户退出，用集合 R 表示。为使每个合法用户都能得到解密密钥，同时排除 R，GC 必须选用不被 R 所拥有的每个辅助密钥加密会话密钥 K。另外，部分用户(事实上很少)的所有辅助密钥可能全部被退出用户的辅助密钥所覆盖而成为受害者需要启用与 GC 共享的共享密钥，因此，加密密钥为 K_i 和，其中，$K_i,K_j\in\kappa,K_i,K_j\notin K(R),1\le i\ne j\le n-r$。

2)广播消息：GC 给每个用户广播消息 $<[E_{K_i}(K),E_{K_{Gj}}(K)],E'_K(M)>$，方括号内的部分称为头部(Hdr)，$E'_K(M)$ 称为主体，其中，E 和 E'是 2 个对称加密算法。

(3)解密

每个不属于 R 的用户 u_i 用其辅助密钥 $k\in K(u_i)$ 解密 $E_k(K)$，从而获得会话密钥 K，并用 K 解密 $E'_K(M)$ 得到明文 M。即使找不到辅助密钥也可以用共享密钥 K_{Gi} 以解密 $E_{k_{Gi}}(K)$，得到明文 M。

随机函数的构造如图 1 所示。

作者简介：赖 霞(1972－)，男，硕士，主研方向：密码学与信息安全；陈利娅，硕士；何明星，教授、博士
收稿日期：2008-09-05 **E-mail：**laixia811@yahoo.com.cn

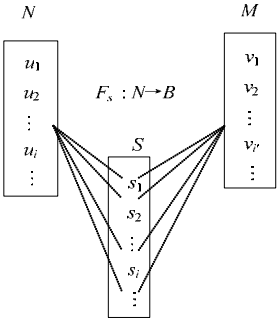

图 1　随机函数族的构造

3　新方案的效能

3.1　新方案有效性分析

(1)确保剩余的合法用户以概率为 1 成功解密。首先，即便 l 很小，对于剩余的任何合法用户 u_i 都能以较大概率找到一个属于他的辅助密钥成功解密。其次，即便当用户的 l 个辅助密钥都无法解密中心广播的消息时，也可用共享密钥与中心保持通信。下面对合法用户 u_i 能以较大概率找到一个属于他的辅助密钥进行论证。

当且仅当 $K(u_i) \not\subset K(R)$ 时，用户 u_i 能够成功解密。现假定对于某一固定 s，计算 $P(k_{s,f_s(i)} \notin \{k_{s,f_s(j)} \mid j \in R\})$。显然，$P(k_{s,f_s(i)} \notin \{k_{s,f_s(j)} \mid j \in R\}) = P(k_{s,f_s(i)} \neq k_{s,f_s(j)} \forall j \in R) = (\frac{m-1}{m})^r = [(1-\frac{1}{m})^{-m}]^{-\frac{r}{m}} \approx \mathrm{e}^{-\frac{r}{m}}$，所以，$P(k_{s,f_s(i)} \in \{k_{s,f_s(j)} \mid j \in R\}) \approx 1\text{-}\mathrm{e}^{-\frac{r}{m}}$，又因为 $|S| = l$，所以 $P(u_i$ 不能解密$) \approx (1-\mathrm{e}^{-\frac{r}{m}})^l$，即 $P(u_i$ 能解密$) \approx 1-(1-\mathrm{e}^{-\frac{r}{m}})^l$

模拟举例，假如 $n=10^5, m=10^4, l=100$

1) $r<m$，即 $r=\frac{1}{2}\times 10^4$, $P \approx 1-0.3^{100}$

2) $r=m$，即 $r=10^4$, $P \approx 1-0.63^{100}$

3) $r>m$，即 $r=2m=2\times 10^4$, $P \approx 1-0.86^{100}$

可以看出，l 取得越大就几乎可以不用共享密钥，但另一方面，l 越大用户和中心的存储成本会越大，下面来讨论 l 的合理取值以使传输成本最低。

(2)传输成本。传输成本与中心广播的消息头部长度相关，即与中心广播的消息头部加密次数成正相关。

由 $P(u_i$ 能解密$) \approx 1-(1-\mathrm{e}^{-\frac{r}{m}})^l$ 可知，能从辅助密钥成功解密的人数为 $P(u_i$ 能解密$)(n-r)$，不能从辅助密钥成功解密的人数为 $(n-r)$ - $P(u_i$ 能解密$)(n-r)$。

使用辅助密钥加密次数为 $lm\cdot \mathrm{e}^{-\frac{r}{m}}$，用共享密钥加密的次数即为不能从辅助密钥成功解密的人数为 $(1-\mathrm{e}^{-\frac{r}{m}})^l(n-r)$，所以，GC 总共加密次数为 $(1-\mathrm{e}^{-\frac{r}{m}})^l(n-r) + lm\cdot \mathrm{e}^{-\frac{r}{m}}$，记为 $f(l,m,r)$。当把 r,m,n 看作常数时，就能将 $f(l,m,r)$ 看作是 l 的函数 $f(l)$，通过 $f(l)$ 对 l 求导可得

$$f'(l)= (1-\mathrm{e}^{-\frac{r}{m}})^l(n-r)\ln(1-\mathrm{e}^{-\frac{r}{m}}) + m\mathrm{e}^{-\frac{r}{m}}$$

令 $f'(l)=0$ 就可得到

$$l_0= \log_{(1-\mathrm{e}^{-\frac{r}{m}})} \frac{m\mathrm{e}^{-\frac{r}{m}}}{(r-n)\ln(1-\mathrm{e}^{-\frac{r}{m}})}$$

取 $l_{\min}=[l_0]+1$。因此，可以根据该网络的具体情况选取适当的密钥池个数 $l_{\min}$ 将使传输成本最低，如假定 $n=10^5, m=10^4$, $r=4\times 10^4$，可得 l_0 =97.427 34，进而得到 $l_{\min}=98$。也可以将 l,n,r 看作常数，将 $f(l,m,r)$ 看作是 m 的函数 $f(m)$，对 m 求导计算得出 m_0，从而得到 $m_{\min}=[m_0]+1$，假定 $n=10^5$, $r=4\times 10^4$, l =98，可计算出 $m_{\min}$ =9 728。同样，将 l, n, m 看作常数，将 $f(l,m,r)$ 看作是 r 的函数 $f(r)$，对 r 求导计算得出 r_0，从而得到 $r=[r_0]+1$，假定 $n=10^5$，$m=9\ 728$, l =98，可计算出 $r_{\min}$ =39 214。

通过以上计算和分析可以看出，当 $n=10^5$，$r \in [39\ 214, n]$ 时，可建立 98 个密钥池，每个密钥池仅存储 9 728 个密钥，这就可以确保未退出用户以概率为 1 获得解密。新 RBE 方案与 *SD* 方案传输成本的比较如图 2 所示。

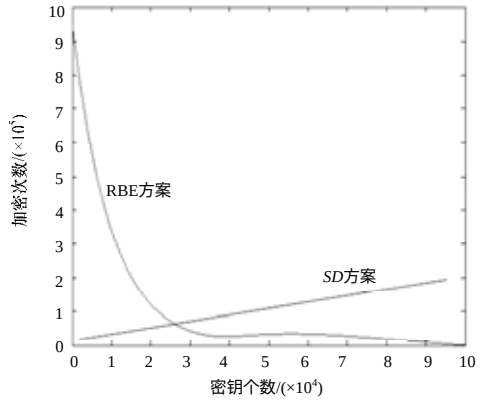

图 2　RBE 方案与 *SD* 方案传输成本比较

(3)存储需求

在本方案中，每个用户只需(l +1)个辅助密钥，GC 需要 lm 个密钥，而在 *SD* 方案中，用户密钥存储量为 $\frac{1}{2}\log_x^2 n+\frac{1}{2}\log_x n+1$，中心密钥控制量为 $O(n)$，显然本方案较 *SD* 方案具有一定优势。

3.2　安全性分析

(1)会话密钥安全：在本方案中，GC 生成的会话密钥是随机的，所有通信都在群内，且由用户的辅助密钥加密，攻击对手不可能用可行的方式发现或计算会话密钥，因此，会话密钥安全可以得到保证。

(2)前向安全：一旦某用户退出，所有属于他的密钥不再使用，即攻击者不可能利用他的信息解密出当前会话密钥，也就不能解密当前秘密信息，前向安全可以得到保证，这也是广播加密方案必须满足的条件。

(3 后向安全：没有新的用户加入，后向安全也就不在考虑的范围之内。

4　结束语

本文利用随机算法思想构造一个随机函数族，由该函数族构造 l 个密钥池，以安全有效地为用户分配密钥。该方案能使剩余的合法用户以较大概率从 l 个辅助密钥中成功找到一个解密密钥，即使某些用户拥有的辅助密钥被退出用户所用的辅助密钥，也可启用与中心单独共享的共享密钥来解密，即合法用户可以以全概率获得解密，同时用户的密钥存储仅为 $(l+1)$ 个，较许多基于二叉树结构的方案(如 *SD* 方案)在密钥存储量上具有一定优势。另外，该方案在一定条件下可使传输成本最小化。 (下转第 164 页)