网络环境中基于 RSA 算法的密钥托管 [1]

杨 波 王育民

(西安电子科技大学 ISN 国家重点实验室 西安 710071)

摘 要 密钥托管密码体制不仅能保护用户的隐私权，同时允许法律授权下的监听. 本文提出了在网络环境中基于 RSA 算法的一种密钥托管体制. 系统中有一可信中心，为每一用户指定 n 个委托人，每一委托人为网络中一服务器. 可信中心按 (t,n) 门限方案为 n 个委托人分配恢复用户密钥的部分能力. 用户在系统中广播自己经过加密的密钥时，仅当至少有 t 个委托人联合起来才能实施对用户的监听.

关键词 密钥托管， RSA 算法，网络环境，可信中心，委托人，监听

中图号 TN918

1 引 言

保密通信中，常有两种互相矛盾的要求. 一方面，用户要求他们的通信应该保密. 另一方面，为了保护国家利益，打击犯罪分子的非法活动，政府部门要求截取“可疑分子”的通信信息. 密钥托管的目的就是在这两种互相矛盾的要求中寻找出一种折衷.

1993 年 4 月，美国政府公布的托管加密标准 (EES)，是最早的托管方案 [1]. 该方案是通过防窜扰的芯片 (称 Clipper 芯片) 来实现的，它有两个特性: (1) 一个保密的加密算法——Skipjack 算法，它是一个对称的分组密码，密钥长度为 80bit，用于加 (解) 密用户间通信的消息. (2) 为法律实施提供“后门”的部分——法律实施访问域 (LEAF)，通过这个域，法律实施部门可在法律授权下，取得用户间通信的会话密钥.

自从 EES 公布以后，密钥托管技术受到了密码学界的普遍关注，提出了很多密钥托管方案 [2]. 本文基于 RSA 算法提出了适用于网络环境的一种密钥托管体制. 系统中以网络中的服务器作为委托人，且有一可信中心，为每一用户指定 n 个委托人，并为用户和每一委托人产生一主密钥，使得每一委托人由自己的主密钥可得用户的主密钥. 且可信中心为自己产生 RSA 密钥，并将 RSA 密钥按 (t,n) 门限方案分为 n 个子密钥，分别分配给 n 个委托人. 用户在系统中广播经过自己的主密钥和可信中心的 RSA 公钥加密的密钥时，则仅当至少有 t 个委托人联合起来才能恢复用户的密钥. 所以可信中心分配给委托人的是恢复用户密钥的部分能力.

用户在用任一标准加密算法通信时，常常是先加密会话密钥，加密会话密钥的密钥由托管方案广播给 n 个委托人. 本文第 4 节所提出的用户间的通信协议中，监听机构由法律实施访问域，可监听到用户间通信的消息，并验证消息是否满足签名方案. 以防止用户不遵守密钥托管协议，即通信时所用的密钥和广播给委托人的密钥不一致.

2 RSA 加密算法

设 p 、 q 是随机选取的两个保密的大素数， $N = p \times q$, N 的欧拉函数为 $\varphi(N) = (p-1) \times (q-1)$. 又设 e 是随机选取的整数，使得 $(e, \varphi(N)) = 1$. 以一对数 (e,N) 作为公开密钥，密钥 d 取为 $d = e^{-1}(\mathrm{mod}\varphi(N))$.

[1] 1998-06-29 收到， 1999-04-12 定稿
军事电子预研基金资助课题

对消息 M 的加密为： $C = M^e(\mathrm{mod}N)$,

解密为： $M = C^d(\mathrm{mod}N)$

文献 [3] 中给出了 RSA 的一种修改. 设 $p = 2p' + 1, q = 2q' + 1$ ，其中 p', q' 是两个保密的大素数，称满足以上关系的 p, q 为安全素数. 又设 $N = p \times q$, $\lambda(N) = 2p'q'$, $\lambda(N)$ 称为 Carmichael 函数，即 $\lambda(N)$ 是满足 $m^{\lambda(N)} = 1(\mathrm{mod}N)$(对 $\forall m \in Z_N^*$) 的最小正整数. 公钥 e 、密钥 d 满足 $e \times d = 1(\mathrm{mod}\lambda(N))$.

3 密钥托管方案

为了为某一用户托管密钥，可信中心选取 RSA 公钥 (e, N) ，密钥 d . 并为用户秘密指定 n 个委托人 $T_1, T_2, \cdots, T_n$. 以下协议中可信中心按文献 [3, 4] 中的 (t, n) 门限签字方案把 d 分成 n 个子密钥，秘密地分配给 n 个委托人. 同时可信中心还为用户和委托人产生秘密的主密钥，使得每一合法的委托人能得到用户的主密钥. 用户用自己的主密钥及 RSA 加密方式广播自己的密钥 K ， t 个合法的委托人联合起来才能恢复出用户的密钥 K . 所以本协议的中心思想是可信中心为每一委托人分配恢复用户密钥的部分能力.

协议如下：

Step1　可信中心执行以下操作：

(1) 秘密选取 n 个互不相同的素数 $t_1 = p_1, t_2 = p_2, \cdots, t_n = p_n$ ，把 $t = t_1 \times t_2 \times \cdots \times t_n$ 秘密发送给用户 U .

(2) 为委托人 T_i 计算公钥 $g(t_i) = t_i^d(\mathrm{mod}N)(i = 1, 2, \cdots, n)$ ；为用户 U 计算公钥 $g(t) = t^d(\mathrm{mod}N)$ ；

(3) 随机选取一个秘密值 K_0 ；为委托人 T_i 计算并秘密发送主密钥 $K_i = K_0^{t_i}(\mathrm{mod}N)$ ；为用户 U 计算并秘密发送主密钥 $K_U = K_0^t(\mathrm{mod}N)$.

Step2　可信中心执行以下操作：在 $Z_{\lambda(N)}$ 上随机选一次数为 $t-1$ 次的多项式 $f(x)$, 满足 $f(0) = d$. 又设 R 是 n 个委托人 $T_1, T_2, \cdots, T_n$ 构成的集合， $x_i \in Z_{\lambda(N)} \setminus \{0\}$ 是关于 T_i 的信息 (若 $i \neq j$, 则 $x_i \neq x_j$), x_i 仅为 n 个委托人及可信中心所知.

给 T_i 秘密发送 $L_i = \frac{f(x_i)/2}{\prod_{\substack{j \in R^{(x_i - x_j)/2} \\ j \neq i}}}(\mathrm{mod}p'q')$.

Step3　设 K 是 U 的密钥， U 广播 $C = K^e \times K_U(\mathrm{mod}N)$.

本协议所述密钥托管方案是一次性的，仅用于一个用户一次密钥的托管. 对不同用户或同一用户不同密钥的托管，应重复执行本协议. 否则，一旦某一用户的密钥被恢复后，这一用户以后就再也无秘密可言了.

4 正确性及安全性分析

命题 1　在以上托管协议的 Step1 中， $\frac{t}{t_i}(\mathrm{mod}\lambda(N)) = \left[\frac{g(t)}{g(t_i)}\right]^e(\mathrm{mod}\lambda(N))(i = 1, 2, \cdots, n)$ ，因此每一 T_i 可按下式获取 U 的主密钥： $K_U = K_i^{[g(t)/g(t_i)]^e}(\mathrm{mod}N)$.

证明　因为 t_i 能整除 t ，设 $t = r \times t_i$, 其中 r 为一整数，那么 $g(t) = (r \times t_i)^d$, 所以

$$\left[\frac{g(t)}{g(t_i)}\right]^e(\mathrm{mod}\lambda(N)) = \left[\frac{(r \times t_i)^d}{t_i^d}\right]^e(\mathrm{mod}\lambda(N)) = r^{d \times e}(\mathrm{mod}\lambda(N))$$

$$= r^{d \times e(\mathrm{mod}\lambda(N))}(\mathrm{mod}\lambda(N)) = r(\mathrm{mod}\lambda(N)) = \frac{t}{t_i}(\mathrm{mod}\lambda(N)).$$

因此

$$K_U = K_0^t(\mathrm{mod}N) = K_0^{t_i \times t/t_i}(\mathrm{mod}N) = (K_0^{t_i})^{(t/t_i)(\mathrm{mod}\lambda(N))}(\mathrm{mod}N)$$
$$= K_i^{\left[\frac{g(t)}{g(t_i)}\right]^e(\mathrm{mod}\lambda(N))}(\mathrm{mod}N) = K_i^{\left[\frac{g(t)}{g(t_i)}\right]^e}(\mathrm{mod}N).$$

证毕

命题 2 任意 t 个 $(t \le n)$ 委托人联合起来可恢复 d，从而可获取用户 U 的密钥 $K = \left[\frac{C}{K_U}\right]^d(\mathrm{mod}N)$，少于 t 个委托人则无法恢复用户 U 的密钥。

证明 设 R 是 n 个委托人 $T_1, T_2, \cdots, T_n$ 构成的集合，S 是 R 的任一子集，满足 $|S| = t$, S 中每一 T_i 计算 $a_{i,S} = L_i \times \left[\prod_{j\in R, j\notin S}(x_i - x_j) \times \prod_{j\in S, j\neq i}(0 - x_j)\right]$。由 Lagrange 插值公式可得 $f(x) = \sum_{i\in S} L_i \times \left[\prod_{j\in R, j\notin S}(x_i - x_j) \times \prod_{j\in S, j\neq i}(x - x_j)\right](\mathrm{mod}\lambda(N))$, 所以 $\sum_{i\in S} a_{i,s} = f(0)(\mathrm{mod}\lambda(N)) = d$。又由命题 1 知每一委托人可获取 U 的主密钥 K_u，所以 S 集合可得

$$\left[\frac{C}{K_U}\right]^d(\mathrm{mod}N) = \left[\frac{K^e \times K_U}{K_U}\right]^d(\mathrm{mod}N) = (K^e)^d(\mathrm{mod}N) = K.$$

又因 $f(x)$ 是 $t-1$ 次的多项式，系数和常数项共有 t 个，所以若委托人少于 t 个，则无法确定出系数和常数项，所以不能恢复出 $f(x)$ 及 d，从而无法恢复用户 U 的密钥。 证毕

5 用户间的通信及监听 [5]

设用户 U_1 欲向用户 U_2 发送消息 M， sk 是会话密钥 (由用户事先协商)。K 是用户 U_1 加密会话密钥的密钥，由上述托管方案广播给委托人。又设 H 是一公开的 Hash 函数。

U_1 向 U_2 发送 $\{E_1(M, sk), \mathrm{LEAF}\}$

其中 $\mathrm{LEAF} = \{E_2(sk, K), S(H(M))\}$。$E_1$ 和 E_2 是任意两个标准加密算法 (比如 DES 或 IDEA), $S(\cdot)$ 是签名算法 (相应的验证算法设为 $V(\cdot)$)。

U_2 可由 sk 及算法 E_1 解出消息 M。

监听过程

监听机构首先获取法院许可监听用户 U_1, U_2 间通信的证书，并将证书分别出示给任意 t 个委托人 $T_{i_j}(1 \le i_1 < i_2 < \cdots < i_t \le n)$, 委托人 T_{i_j} 验证了法院的证书后，将其所托管的内容 L_{i_j} 交给监听机构，监听机构由命题 2 可求出 U_1 用于加密会话密钥的密钥 K，由 K 及算法 E_2 解出 sk，由 sk 及算法 E_1 解出消息 M，然后求 $H(M)$ 及 $V(S(H(M)))$，即验证 $H(M)$ 是否满足签名方案，若不满足，则可确认 U_1 在密钥的托管过程中是不诚实的，即用户没有遵守密钥托管规则。

6 结 论

本文基于 RSA 算法提出了适用于网络环境中的一种密钥托管体制，它有如下特点：(1) 参加密钥托管的委托人为网络中的服务器。(2) 用户的委托人由可信中心指定，用户在托管自己的密钥时，并不知道自己的委托人。所以本方案可防止用户对委托人的收买。但存在这样一个缺点，当用户的密钥损坏或丢失时，若要恢复则必须求助于可信中心。(3) 在 EES

中仅有两个委托人．此方案推广为有多个委托人，这样可防止因个别委托人串通而造成的对用户密钥泄漏的危险性．再者，考虑到密钥的可恢复性，本体制利用门限方案可防止因个别委托人拒绝合作或无法合作 (如子密钥的丢失或服务器的故障等) 而造成的密钥的不可恢复性．(4) 利用广播机制，每一委托人得到的是经过加密的用户的密钥，这样可进一步防止用户密钥的泄漏．(5) 本方案仅用于一个用户一次密钥的托管，因此每一委托人每次仅得到恢复一个用户一次密钥的部分能力．对不同用户或同一用户不同密钥的托管，本协议将重复执行．

参　考　文　献

[1] Denning D E, Smid M. Key escrowing today. IEEE Communications Magazine. 1994, 32(9): 54–68.

[2] Denning D E, Branstad D A. A taxonomy for key-escrow encryption systems. Commun. ACM 1996, 39(3): 34–40.

[3] Desmedt Y, Frakel Y. Shared generation of authentications and signatures. In J. feigenbaum ed., Advances in Cryptology, Proc. of Crypto'91 (Lecture Notes in Computer Science 576), Springer-Verlag, 1991, 457–469.

[4] Liaw H T. A dynamic cryptographic key generation and information broadcasting scheme in information systems. Computer & Security, 1994, (13): 601–610.

[5] 杨波，马文平，王育民．一种新的密钥分割门限方案及密钥托管体制．电子学报，1998, 26(10): 1–3.

A KEY ESCROW SYSTEM FOR NETWORK ENVIRONMENT BASED ON RSA ALGORITHM

Yang Bo　　Wang Yumin

(*National Key Laboratory on ISN, Xidian University, Xi'an* 710071)

Abstract　A key escrow cryptosystem can provide protection for user's privacy, while at the same time, allows for the wiretapping when lawfully authorized. In this paper, a key escrow system based on RSA algorithm for network environment is given. A trusted center in this system specifies n trustees for every user, and distributes the part recovery ability of the user's secret key to n trustees by (t, n) threshold scheme. When the user broadcasts his encrypted key, only if at least t cooperated trustees can enforce the wiretapping to this user.

Key words　Key escrow, RSA algorithm, Network environment, Trusted center, Trustee, Wiretapping

杨　波：　男，1963 年生，博士，副教授，主要从事密钥托管及 E-cash 方面的研究．

王育民：　男，1936 年生，教授，博士生导师，主要从事信息论、密码、编码方面的研究．