基于 Asmuth-Bloom 门限体制的密钥托管 [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。本文基于 Asmuth-Bloom 门限体制提出了一种密钥托管体制，并分析了体制的安全性。

关键词 密钥托管，门限方案，委托人

中图号 TN918

1 引 言

随着密码学的飞速发展，密码算法数量越来越多、强度越来越高，现代通讯系统和计算机系统将成为犯罪分子进行犯罪活动的安全港。密钥托管的主要目的就是在保密通信中为法律授权的政府机构留一“后门”，以截取“可疑分子”的通信信息，打击犯罪分子的非法活动。其次，密钥托管也可为用户在密钥丢失或损坏时提供恢复的手段 [1,2] 。

本文提出利用 Asmuth-Bloom 门限体制的密钥托管方案。用户按 Asmuth-Bloom 门限体制将其密钥分为一组密钥分量，并将每一个密钥分量交付一个委托人托管。每一委托人均验证自己收到的密钥分量是否有效。若每一密钥分量都有效，则在一定的条件下 (如法院命令)，一组委托人仅当他们的个数不少于方案的门限值时，他们联合起来可以恢复出用户的密钥。

2 Asmuth-Bloom 门限方案 [3]

首先选取一大素数 q, 正整数 s, 以及 n 个严格递增的数 $m_1, m_2, \cdots, m_n$; 满足：(a) $q > s$, (b) $(m_i, m_j) = 1(\forall i, j, i \neq j)$, (c) $(q, m_i) = 1(\forall i)$, (d) $N = \prod_{i=1}^{k} m_i > q \prod_{i=1}^{k-1} m_{n-i+1}$ 。

以 s 作为秘密数据，条件 (a) 指出，秘密数据小于 q, 条件 (d) 指出，N/q 大于任取的 $k-1$ 个不同的 m_i 之积。进而，随机选取 A，满足 $0 \leq A \leq [N/q] - 1$, 并公布 q 和 A。

求 $y = s + Aq$(由上知 $y < N$), 则由 $y_i = y(\mathrm{mod}\, m_i)(i = 1, \cdots, n)$ 给出的集合 $\{(m_i, y_i)\}_{i=1}^{n}$ 即构成了一个 (k, n) 门限方案。

这是因为, 当 k 个参与者提供出自己的 (m_i, y_i) 时, 由中国剩余定理可求得 $y' = y(\mathrm{mod}N')$, 式中 $N' = \prod_{j=1}^{k} m_{i_j} \geq N$ 。

因为 $y < N \leq N'$, 所以 $y' = y$; 另一方面, 若仅有 $k-1$ 个参与者提供出自己的 (m_i, y_i), 则只能求得 $y'' = y(\mathrm{mod}N'')$，式中 $N'' = \prod_{j=1}^{k-1} m_{i_j}$ 。

由条件 (d)， $N'' < N/q$, 即 $N/N'' > q$ 。

由于 $N/N'' > q$, $(N'', q) = 1$，故集合 $\{[x] | [x] = \{x : x \mathrm{mod} N'' = y''\}\}$ 将覆盖所有的模 q 同余类。或者更简单地说，至少以下整数 $y'' + \alpha N''(0 \leq \alpha < q)$ 都是 y 的可能取值。因此无法确定 y 。

[1] 1997-10-24 收到， 1999-01-09 定稿
军事电子预研资金资助课题

3 密钥托管方案

密钥管理中心在有限域 GF(q)(其中 q 是一大素数) 上选取一个随机数 p 和一个本原元 h，使得用户无法知道 $\log_p h$。并设 $E(x,y)=p^x h^y$。又设密钥管理中心为用户选取满足 Asmuth-Bloom 门限方案的 n 个公开的、严格递增的数 $m_1,m_2,\cdots,m_n$。

设用户的密钥为 s，用户选取满足 $0\le A\le [N/q]-1$ 的 A，并公布 A。求 $y=s+Aq$。用户按以下方式将 y 分为 n 个密钥分量，将每一密钥分量分别交付给一个委托人托管：

步骤 1　对秘密 y，随机选 $u\in \mathrm{GF}(p)$, 计算并公布 $E(y,u)$。

步骤 2　求 $y_i\equiv y(\mathrm{mod}\ m_i)(i=1,\cdots,n)$，将 y_i 提交给委托人 T_i，作为密钥分量。求 $u_i\equiv u(\mathrm{mod}\ m_i)$ 及 $E(y_i,u_i)$, 公开 $E(y_i,u_i)$。

步骤 3　每一委托人 $T_i(i=1,\cdots,n)$ 验证

$$\prod_{j=1}^{n} E(y_j,u_j)^{mx_j/m_j}=E(y,u)(\text{其中 } x_j \text{ 满足}\frac{m}{m_j}x_j\equiv 1(\mathrm{mod}\ m_j)) \tag{1}$$

是否成立，若成立，则认为所托管的内容是有效的。

4 安全性分析

首先证明 $E(x,y)$ 具有以下性质：

(1) $E(x,y)$ 不会泄露关于 x 的任何信息。这是因为，对固定的 x，$E(x,y)=p^x h^y$ 在 GF(q) 上是均匀分布的，所以接收者从 $E(x,y)$ 不能得到关于 x 的任何信息。(2) 用户不能用 $E(x,y)$ 提供假的 x 来欺骗委托人，即不能找出 $x'(x'\ne x)$ 及 y', 使得 $E(x',y')=E(x,y)$。

若 $p^{x'}h^{y'}=p^x h^y$, 即 $p^{x'-x}=h^{y-y'}$。因为 $y-y'\ne 0$(由 $x\ne x'$ 知)，所以 $y-y'$ 在 GF(q) 上有逆元 β。对 $p^{x'-x}=h^{y-y'}$ 两边取 β 次方得 $p^{\beta(x'-x)}=h$。所以 $\beta(x'-x)=\log_p h$。所以用户若不知道 $\log_p h$，他就不能找出上述的 x'。

由上面步骤 3 中的 $\prod_{j=1}^{n} E(y_j,u_j)^{mx_j/m_j}=E(y,u)$ 可知：

$$\begin{aligned}\prod_{j=1}^{n} E(y_j,u_j)^{\frac{m}{m_j}x_j}&=\prod_{j=1}^{n}(p^{y_j}h^{u_j})^{\frac{m}{m_j}x_j}=\prod_{j=1}^{n}(p^{\frac{m}{m_j}x_j y_j}h^{\frac{m}{m_j}x_j u_j})\\&=p^{\sum_{j=1}^{n}\frac{m}{m_j}x_j y_j}h^{\sum_{j=1}^{n}\frac{m}{m_j}x_j u_j}=E(y,u)=p^y h^y,\end{aligned}$$

所以

$$y\equiv\sum_{j=1}^{n}\frac{m}{m_j}x_j y_j(\mathrm{mod}\ m),\quad u\equiv\sum_{j=1}^{n}\frac{m}{m_j}x_j u_j(\mathrm{mod}\ m). \tag{2}$$

又由中国剩余定理知，一次同余方程组

$$\left.\begin{aligned}y_1&\equiv y(\mathrm{mod}\ m_1),\\y_2&\equiv y(\mathrm{mod}\ m_2),\\&\vdots\qquad\vdots\\y_n&\equiv y(\mathrm{mod}\ m_n).\end{aligned}\right\} \tag{3}$$

对模 $m=\prod_{j=1}^{n} m_j$ 的唯一解是：$y \equiv \sum_{j=1}^{n} \frac{m}{m_j} x_j y_j (\mathrm{mod}\, m)$。其中 x_j 满足 $\frac{m}{m_j} x_j \equiv 1 (\mathrm{mod}\, m_j)$ 所以满足 (1) 式的 y 即为满足 (2) 式的 y，也一定为满足 (3) 式的 y。根据 Asmuth-Bloom 门限方案知任意 k 个委托人由自己的 (m_i, y_i) 可恢复出 y，从而得到用户的密钥 s。

又由 $E(x,y)$ 的性质 (1) 可知，在上述的密钥托管方案中，用户不会泄露自己的秘密信息；所以本方案的门限值不会减小，因此少于 k 个委托人则无法恢复出用户的密钥。

5 结 论

本文基于 Asmuth-Bloom 门限体制，提出了一种密钥托管方案。方案中有多个委托人，这样可减少因个别委托人串通或被收买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，本方案可防止因个别委托人拒绝合作或无法合作 (如密钥分量的丢失或委托人的死亡等) 而造成的密钥的不可恢复性。本方案中委托人还需对用户密钥分量的有效性进行验证，从而可防止用户向委托人提交“垃圾”。

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] Asmuth C, Bloom J. A modular approach to key safeguarding. IEEE Trans. on Information Theory, 1983, IT-29: 208–210.

[4] Desmedt Y, Frakel Y. Threshold Cryptosystems. In G. Brassard, editor, Advances in Cryptology, Proc.of Crypto'89 (Lecture Notes in Computer Science 435), Heidelberg: Springer-Verlag, 1990, 307–315.

[5] Pedersen T. Non-interactive and Information Theoretic Secure Verifiable Secret Sharing. Advances in Cryptology-Crypto '91 (Lecture Notes in Computer Science 576), Berlin: Springer-Verlag, 1991, 129–140.

KEY ESCROW BASED ON ASMUTH-BLOOM THRESHOLD SYSTEM

Yang Bo Wang Yumin

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

Abstract A key escrow cryptosystem can not only provide protection for user's privacy, while at the same time, allows for the wiretapping when lawfully authorized. In this paper, a secret key escrow system based on Asmuth-Bloom threshold scheme is given and its security is analysed.

Key words Key escrow, Threshold scheme, Trustee

杨 波： 男，1963 年生，博士，副教授，目前研究领域：密码学，通讯网的安全.
王育民： 男，1936 年生，教授，博士生导师，目前研究领域：密码、编码，信息论.