第11卷 第1期 电子科学学刊 Vol. 11, No. 1
1989 年 1 月 JOURNAL OF ELECTRONICS Jan., 1989

利用身份证进行密钥分配的新方案* **

杨 义 先
(北京邮电学院信息工程系,北京)

摘要 本文给出了两类利用身份证进行密钥分配的新方案，并将它们推广到会议密钥分配方案中去.

关键词 密码;密钥分配;保密通信;身份证;会议密钥.

1. 引言

利用身份证进行保密通信这一想法最初是由沙米尔[1]提出的，他给出了第一种利用身份证进行签字的方案. 最近日本学者[2]又给出了两类利用身份证进行密钥分配的方案. 在本文的第二节中我们将再给出另外两类利用身份证进行密钥分配的方案. 从某种意义上来说它们可看作是文献[2]的推广. 它们也是一般密钥分配研究的一部分[3-14].

对话型的通信是常见的一种通信方式. 但是随着信息社会的不断发展，会议型的通信将越来越普遍. 因此会议型通信方式保密方案就非常有意义了. 本文的第三节将研究利用身份证进行会议密钥分配的问题.

2. 利用身份证进行密钥分配的两种新方案

首先介绍一下常见的引理:

引理 $g(x)=g_1^{l_1}(x)\cdot g_2^{l_2}(x)\cdots g_k^{l_k}(x)$

其中 $g_j(x)$ 是 $GF(p)$ 上的 m_j 次不可约多项式 $(1\leqslant j\leqslant k)$. 记 m 为 $g(x)$ 的次数. 又设:

$$\varphi(p,g(x))=p^m\cdot\prod_{i=1}^{k}(1-1/p^{m_i})$$

那么对 $GF(p)$ 上的任意一个次数大于 0 的多项式 $u(x)$, 只要 $\gcd(u(x),g(x))=1$ 就必有:

$$[u(x)]^{\varphi(p,g(x))}\equiv 1(\mathrm{mod}\,(g(x)))$$

其中 $\gcd(\cdot,\cdot)$ 表示最大公因式, $\mathrm{mod}(\cdot)$ 表示模运算。

设每个用户由 $GF(p)$ 上的一个多项式 $u_i(x)$ 唯一地确定.

第一种方案 分配中心先秘密地选取 k 个不可约的多项式 $g_1(x),\cdots,g_k(x)$ 使得 $g_j(x),(1\leqslant j\leqslant k)$ 的次数 m_j 很大，并且 $\gcd(u_j(x),g_j(x))=1$. 计算 $g(x)=g_1^{l_1}(x)g_2^{l_2}(x)\cdots g_k^{l_k}(x)$, (其中 $l_1,\cdots,l_k$ 是任取的). 然后分配中心再秘密地选一个素数 e 并计算出 d 使得 $ed\equiv 1\ (\mathrm{mod}\,(\varphi(p,g(x))))$. 最后分配中心计算出 $s_i(x)=$

* 1987 年 4 月 27 日收到，1987 年 9 月 7 日修改定稿.
** 中国科学院科学基金资助课题.

$[u_i(x)]^d \bmod (g(x))$，选取 $GF(p)$ 上的一个本原多项式 $f(x)$ 并将 $(g(x), f(x), e, s_i(x))$ 秘密地送给用户 i. $(1 \leqslant i \leqslant n)$. 上述各项任务完成以后，如果不再增加新用户的话，密钥分配中心就可以永远关闭了。

现在如果用户 i 和 j 想同时获得对话密钥，他们可作如下操作：用户 i 任选正整数 r_i，计算 $y_i(x) = s_i(x)(f(x))^{r_i} \bmod (g(x))$，并将 $y_i(x)$ 通过公开信道传给用户 j. 同样地用户 j 任选正整数 r_j 并计算出 $y_j(x) = s_j(x)(f(x))^{r_j} \bmod (g(x))$，并将$y_j(x)$ 通过公开信道传给用户 i.

然后用户 i 计算出 $[(y_j(x))^e/u_i(x)]^{r_i} \bmod (g(x)) = K_1(x)$，用户 j 计算 $[(y_i(x))^e/u_j(x)]^{r_j} \bmod (g(x)) = K_2(x)$.

利用前面的引理可以证明：

$$K_1(x) = K_2(x) = (f(x))^{er_ir_j} \bmod (g(x))$$

于是用户 i 和 j 就获得了所需的对话密钥.

安全性分析简述：由于用户 i 与 j 通话的密钥是 $(f(x))^{er_ir_j} \bmod (g(x))$，它与用户 i 和 j 随机选取的 r_i 和 r_j 有关，而破译者所知道的信息中只有 $y_i(x)$ 和 $y_j(x)$ 才与 r_i 和 r_j 有关。所以破译者就只有充分利用等式：

$$y_i(x) = s_i(x)(f(x))^{r_i} \bmod (g(x))$$

和

$$y_j(x) = s_j(x)(f(x))^{r_j} \bmod (g(x))$$

将等式两边各取 e 次幂得到：

$$(y_i(x))^e \equiv (s_i(x))^e(f(x))^{er_i} \bmod (g(x))$$

即

$$(y_i(x))^e \equiv u_i(x)(f(x))^{er_i} \bmod (g(x))$$

由于 $\gcd(u_i(x), g(x)) = 1$ 所以此式等价于

$$(y_i(x))^e u_i^{-1}(x) \equiv (f(x))^{er_i} \bmod (g(x))$$

因此最后就将求 r_i 的问题化成了多项式环上求对数的问题，而后者已知是一个难题。综上所述我们有理由认为第一种方案比较安全。

第二种方案　　分配中心将 $(g(x), f(x), e, c, s_i(x))$ 秘密地传给用户 i. 其中 c 是一个素数。$g(x), f(x), e, s_i(x)$ 的含义与第一种方案相同。

用户 i 与 j 可按下述步骤获得对话密钥：

首先用户 i 任选一个正整数 r_i，并计算出

$$y_i(x) = (f(x))^{cr_i} \bmod (g(x))$$

和

$$h_i(x) = s_i(x)(f(x))^{cr_i} \bmod (g(x))$$

然后将 $(y_i(x), h_i(x))$ 通过公开信道传给用户 j. 用户 j 任选 r_j（正整数）并计算 $y_j(x) = (f(x))^{cr_j} \bmod (g(x))$ 和 $h_j(x) = s_j(x)(f(x))^{cr_j} \bmod (g(x))$然后将 $(y_j(x), h_j(x))$ 通过公开信道传给用户 i.

用户 i 验算等式：

$$(h_j(x))^e/(y_j(x))^c \equiv u_i(x) \bmod (g(x))$$

是否成立。若等式不成立就说明有人冒充用户 j。若等式成立他就再计算

$$(y_j(x))^{r_i} \bmod (g(x)) = K_1(x).$$

同样地用户 j 验算等式:

$$(h_i(x))^e / y_i(x))^c \equiv u_i(x) \bmod (g(x))$$

是否成立。若等式不成立就说明有人冒充用户 i。若等式成立他就再计算

$$(y_i(x))^{r_j} \bmod (g(x)) = K_2(x).$$

可以验证:

$$K_1(x) = K_2(x) = (f(x))^{cr_ir_j} \bmod (g(x))$$

于是用户 i 与 j 就达到了目的。

此方案的安全性讨论与前相似。

3. 利用身份证进行会议密钥分配的方案

本节将上节中的方案推广为会议密钥分配方案。限于篇幅只详述第一种方案的推广过程。

为了直观起见先叙述三人会议的会议密钥分配。下面的各符号与上节相同。

第一步　用户 0, 1, 2 各自随机独立地选取正整数 r_0, r_1, 和 r_2。然后:

用户 0 计算 ${}_1y_{01}(x) = s_0(x)(f(x))^{r_0} \bmod (g(x))$ 并将 ${}_1y_{01}(x)$ 通过公开信道传给用户 1。

用户 1 计算 ${}_1y_{12}(x) = s_1(x)(f(x))^{r_1} \bmod (g(x))$ 并将 ${}_1y_{12}(x)$ 通过公开信道传给用户 2。

用户 2 计算 ${}_1y_{20}(x) = s_2(x)(f(x))^{r_2} \bmod (g(x))$ 并将 ${}_1y_{20}(x)$ 通过公开信道传给用户 0。

第二步　用户 0 计算 $f_{20}(x) = \{[{}_1y_{20}(x)]^e / u_2(x)\}^{r_0} \bmod (g(x))$ 和 ${}_2y_{01}(x) = s_0(x)[f_{20}(x)]^{r_0} \bmod (g(x))$ 并将 ${}_2y_{01}(x)$ 通过公开信道传给用户 1。

用户 1 计算出 $f_{01}(x) = \{[{}_1y_{01}(x)]^e / u_0(x)\}^{r_1} \bmod (g(x))$ 和 ${}_2y_{12}(x) = s_1(x) \cdot (f_{01}(x))^{r_1} \bmod (g(x))$ 并将 ${}_2y_{12}(x)$ 通过公开信道传给用户 2。

用户 2 计算出 $f_{12}(x) = \{[{}_1y_{12}(x)]^e / u_1(x)\}^{r_2} \bmod (g(x))$ 和 ${}_2y_{20}(x) = s_2(x) \cdot (f_{12}(x))^{r_2} \bmod (g(x))$ 并将 ${}_2y_{20}(x)$ 通过公开信道传给用户 0。

第三步　用户 0 计算 $f_{1220}(x) = \{[{}_2y_{20}(x)]^e / u_2(x)\}^{r_0} \bmod (g(x))$ 和 ${}_3y_{01}(x) = s_0(x)(f_{1220}(x))^{r_0} \bmod (g(x))$ 并将 ${}_3y_{01}(x)$ 通过公开信道传给用户 1。

用户 1 计算出 $f_{2001}(x) = \{[{}_2y_{01}(x)]^e / u_0(x)\}^{r_1} \bmod (g(x))$ 和 ${}_3y_{12}(x) = s_1(x) \cdot (f_{2001}(x))^{r_1} \bmod (g(x))$ 并将 ${}_3y_{12}(x)$ 通过公开信道传给用户 2。

用户 2 计算出 $f_{0112}(x) = \{[{}_2y_{12}(x)]^e / u_1(x)\}^{r_2} \bmod (g(x))$ 和 ${}_3y_{20}(x) = s_2(x) \cdot (f_{0112}(x))^{r_2} \bmod (g(x))$ 并将 ${}_3y_{20}(x)$ 通过公开信道传给用户 0。

第四步(最后一步)

用户 0 算出 $K_0(x) = \{[{}_3y_{20}(x)]^e / u_2(x)\}^{r_0} \bmod (g(x))$

用户 1 算出 $K_1(x) = \{[{}_3y_{01}(x)]^e / u_0(x)\}^{r_1} \bmod (g(x))$

用户 2 算出 $K_2(x) = \{[{}_3y_{12}(x)]^e / u_1(x)\}^{r_2} \bmod (g(x))$

不难证明:

$$K_0(x)=K_1(x)=K_2(x)=(f(x))^{e^3(r_0r_1r_2)^2} \bmod (g(x))$$

于是用户 0，1，2 就获得了所需的会议密钥。

现在来考虑 n 人会议的情形。

第 1 步　用户 0，1，…，$n-1$ 各自随机独立地选取正整数 $r_0, r_1, \cdots, r_{n-1}$。

用户 i 计算 ${}_iy_{i+1}(x)=s_i(x)(f(x))^{r_i} \bmod (g(x))$ 并将 ${}_iy_{i+1}(x)$ 通过公开信道传给用户 $i+1$。（此处当 $i+1=n$ 时作为 0 处理）。

⋮

第 k 步 $(2\leqslant k\leqslant n)$　用户 i 在第 k 步中的工作是将第 $k-1$ 步中用户 $i-1$ 传给他的多项式 $a(x)$ 作如下处理：计算出 $b(x)=\{[a(x)]^e/u_{i-1}(x)\}^{r_i} \bmod (g(x))$ 和 $c(x)=s_i(x)(b(x))^{r_i} \bmod (g(x))$ 并将 $c(x)$ 通过公开信道传给用户 $i+1$。

⋮

第 $n+1$ 步(最后一步)　用户 i 在此步中的工作是将第 n 步中用户 $i-1$ 传给他的多项式 $d(x)$ 作如下处理：计算出 $K_i(x)=\{[d(x)]^e/u_{i-1}(x)\}^{r_i} \bmod (g(x))$

可以验证：

$$K_0(x)=K_1(x)=\cdots=K_{n-1}(x)=[f(x)]^{e^n(r_0r_1\cdots r_{n-1})^2} \bmod (g(x))$$

于是各用户就都获得了所需的会议密钥。

上述会议密钥分配的安全性讨论与第二节中的相似。在此略去。

参　考　文　献

[1] A. Shamir, Advance in Cryptograph-Proceedings of Crypto'84, Santa Barbara, August 1984, 44.
[2] E. Okamoto, *IEE. Electron. Lett*, 22(1986), 24, 1283.
[3] Ingemarsson, D. Tang, *IEEE Trans. on IT*, IT-28(1982), 714.
[4] W. Diffie, M. Hellamn, *IEEE Trans. on IT*, IT-22(1976), 644.
[5] Yang Yi Xian, *IEE Electron. Lett.*, 23(1987)11, 560.
[6] Yang Yi Xian, *IEE Electron. Lett.*, 23(1987)18, 934.
[7] Yang Yi Xian, *IEE Electron Lett.*, 23(1987)20, 1043.
[8] Yang Yi Xian, *IEE Electron. Lett.*, 23(1987)24, 1277.
[9] Yang Yi Xian, *IEE Electron. Lett.*, 23(1987)25, 1335.
[10] Yang Yi Xian, *IEE Electron. Lett.*, 24(1988)3, 154.
[11] Yang Yi Xian, *IEE Electron. Lett.*, 24(1988)15, 961.
[12] Yang Yi Xian, IEEE ICCS'88, Singapore, 1988.
[13] Yang Yi Xian, IWIT'88, Beijing, China, 1988.
[14] 杨义先，电子科学科刊 9(1987) 4，368—370.

NEW SCHEMES FOR IDENTITY-BASED KEY DISTRIBUTION

Yang Yixian

(Beijing University of Posts and Telecommunications, Beijing)

Abstract Two classes of identity-based key distribution schemes and the corresponding conference key distribution schemes are proposed in this paper.

Key words Cryptograph; Key distribution; Privacy communication; Conference key; Identity