文章编号: 1001-2486 (2000) 02 -0074-04

一种安全的组签字方案*

施荣华, 胡湘陵

(长沙铁道学院, 湖南 长沙 410075)

摘 要: 基于离散对数给出了一种组签字方案。该方案保留了已有方案的主要优点, 并且解决了 "匿名"性问题。在该方案中, 既使组权威公布了一些附加信息以供验证者确认签字者的身份, 但可确保签字者其它的组签字的 "匿名"性, 组权威也不必更新签字者的任何密钥。因为组权威公布的信息只是为了识别指定的组签字。

关键词: 组签字; 组权威; 匿名性; 离散对数

中图分类号: TP30 文献标识码: A

A Secure Group Signature Scheme

SHI Rong-hua, HU Xiang-ling

(Changsha Railway University, Changsha 410075, China)

Abstract: Based on the discrete logarithm, this paper proposes a group signature schemes. The scheme preserves the main merits inherent in previously proposed schemes, and solves the anonymity problem. In the scheme, even though the group authority announces some additional information to provide the verifier with confirmation of the identity of the signer, the anonymity of this signer will be maintained in the other group signatures, and the group authority need not renew any of the keys of this signer. The reason is that announced information is only provided in order to identify the specific group signature.

Key words: Group signature; Group authority; Anonymity; The discrete logarithm

20世纪90年代初, Chaum 和 Heyst 提出了一种称为组签字的新型签字方案[1]。组签字允许组内的单个成员代表组进行签字。组签字方案有以下特性:

㈠ 只有组中的成员能够对信息进行签字;

㈡ 接收者能够认证签字的确是该组的有效签字, 但不能发现是组中哪个成员的签字;

㈢ 在发生争议的情况下, 能够 "打开"签字以获取签字者的身份。

Chaum-Heyst 方案给出了四种组签字方式。然而, 这四种方式有两个不足: 若组发生变化, 则每个成员得重新选择一个新密钥, 动态特性不好; 另外, 组权威不能识别签字者的身份, 在发生争议的情况下, 要组中所有成员联合才能识别签字者的身份, 效率低。为克服以上不足, Chen 和 Pedersen 于1994年给出了一种新的组签字方案[2]。然而, Chen-Pedersen 方案是交互式的, 它用签字者与验证者之间的交互式协议来验证组签字, 缺乏有效性。

1998年, Lee 和 Chang 基于离散对数问题[3,4]给出了一种非交互式组签字方案[5], 克服了 Chen-Pedersen 方案的有效性问题。然而, Lee-Chang 的方案有以下缺点: 在组签字发生争议的情况下, 得公布一些额外的信息以使验证者确认签字者的身份。由于针对不同的信息, 签字者的各种组签字均含标识信息。于是, 该签字者身份只要被标识一次, 则他以前所签的组签名也同时被标识, 损坏了该签名者以前组签名的 "匿名"性。另外, Lee-Chang 方案组权威处理完一次争议情况之后, 得更新被标识签字者的好几个密钥, 以保证该签字者以后签名的 "匿名"性。

为克服已有方案[1,2,5]的不足, 本文给出了一种安全的组签字方案。

* 收稿日期: 1999-09-23
基金项目: 铁道部科技专项项目及长院科研重点项目资助
作者简介: 施荣华 (1964-), 男, 副教授, 从事计算机网络与计算机通信保密的研究和教学。

1 方案描述

1.1 初始化阶段

设 p、q 是两个大素数且 $q \mid (p-1)$，g 是 GF(P) 上的 q 阶生成元。每个组员 u_i，选择一个保密密钥 x_i 并计算其公开密钥:

$$y_i = g^{x_i} \bmod p \tag{1}$$

设 T 是一个组权威成员，其保密密钥为 x_T，公开密钥:

$$y_T = g^{x_T} \bmod p \tag{2}$$

针对每一个组成员 u_i，T 利用 Nyberg—Rueppel 方法[6]计算:

$$\begin{cases} r_i = g^{-k_i} \cdot y_i^{k_i} \bmod q & (3) \\ S_i = k_i - r_i \cdot X_T \bmod q & (4) \end{cases}$$

这里: k_i 是一个 Z_q^* 中的随机数。然后 T 把 (r_i, s_i) 安全的送给组成员 u_i。

u_i 接收到 (r_i, s_i) 之后，借助于检查等式:

$$g^{s_i} \cdot y_T^{r_i} \cdot r_i \equiv (g^{s_i} \cdot y_T^{r_i})^{x_i} \bmod p \tag{5}$$

来验证其签字。若上式成立，则针对 u_i 的签字 (u_i, s_i) 是有效的。

下面证明 (5) 式的正确性:

$$\begin{aligned} g^{s_i} \cdot y_i^{r_i} \cdot r_i &\equiv g^{s_i} \cdot g^{x_T r_i} \cdot g^{-k_i} \cdot g^{x_i k_i} \quad (\text{由}(1)(2)(3)\text{式}) \\ &\equiv g^{(x_i k_i)} \quad (\text{由}(4)\text{式}) \\ &\equiv (g^{k_i})^{x_i} \\ &\equiv (g^{(s_i + x_T r_i)})^{x_i} \quad (\text{由}(4)\text{式}) \\ &\equiv (g^{s_i} \cdot g^{x_T r_i})^{x_i} \\ &\equiv (g^{s_i} \cdot y_T^{r_i})^{x_i} \bmod p \quad (\text{由}(2)\text{式}) \quad (\text{证毕}) \end{aligned}$$

1.2 签字验证阶段

假定组成员 u_i 要对信息 m 进行签字。u_i 先在 Z_q^* 中随机选择三个整数 a、b、t，并利用 (r_i, s_i) 计算:

$$\begin{cases} A = r_i^a \bmod p & (6) \\ B = r_i a \bmod q & (7) \\ C = (s_i - b) \bmod q & (8) \\ D = g^{ab} \bmod p & (9) \\ E = g^a \bmod p & (10) \end{cases}$$

u_i 再计算:

$$\begin{cases} \alpha_i = E^C \cdot y_T^B \cdot D \bmod p = g^{a k_i} \bmod p & (11) \\ R = \alpha_i^t \bmod p & (12) \end{cases}$$

于是，u_i 解以下关系等式就可获得参数 s:

$$h(m) = R \cdot x_i + t \cdot s \bmod p \tag{13}$$

于是，获得信息 m 的组签字为 {R, S, h (m), A, B, C, D, E}。收到该组签字的任何验证者按以下步骤都能确定组签字的有效性:

$$\begin{aligned} \alpha &= E^C \cdot y_T^B \cdot D \bmod p \\ H_i &= \alpha \cdot A \bmod p \end{aligned} \tag{14}$$

检查关系等式:

$$\alpha^{h(m)} \equiv H_i^R \cdot R^s \bmod p \tag{15}$$

若 (15) 式成立，则 u_i 针对 m 的组签字 {R, S, h (m), A, B, C, D, E} 有效。

下面证明 (15) 式的正确性:

$$\begin{aligned}
\alpha_i^{h(m)} &\equiv \alpha^{(R\,x_i + t\,s)} \quad (\text{由}(13)\ \text{式})\\
&\equiv (\alpha_i^{x_i})^{R} \quad (\alpha_i^{l})^{s}\\
&\equiv (g^{a\,k_i\,x_i})^{R} \quad R^{s} \quad (\text{由}(11)(12)\ \text{式})\\
&\equiv (y_i^{a\,k_i}))^{R} \quad R^{s} \quad (\text{由}(1)\ \text{式})\\
&\equiv (g^{a\,k_i} \quad r_i^{a})^{R} \quad R^{s} \quad (\text{由}(3)\ \text{式})\\
&\equiv (\alpha_i \quad A)^{R} \quad R^{s} \quad (\text{由}(11)(6)\ \text{式})\\
&\equiv H_i^{R} \quad R^{s} \bmod p \quad (\text{由}(14)\ \text{式}) \qquad (\text{证毕})
\end{aligned}$$

1.3 组成员识别阶段

因为组权威已经存有每一个成员 u_i 的 $(r_i,\ s_i,\ k_i)$，所以他可以查询 u_i 的 $(r_i,\ s_i,\ k_i)$ 是否满足关系式:

$$E_C \quad y_T^{B} \quad D = E^{k_i} \bmod p \quad (\text{由}(10)(11)\ \text{式}) \tag{16}$$

这里: $i = 1,\ \cdots,\ n,$; n 是组成员数。于是，组权威能够确定签字者 u_i 是谁。

要使验证者相信 u_i 的确是签字者，组权威由 (7) 式计算:

$$a = B \quad r_i^{-1} \bmod p \tag{17}$$

然后，再在 Z_q^* 中随机选择一个整数 d 并计算:

$$\begin{cases} r_T = (g \quad y_i)^{d} \bmod p & (18)\\ s_T = (d - r_T \quad a \quad k_i) \bmod p & (19) \end{cases}$$

最后，组权威公布识别信息 $(r_T,\ s_T,\ y_i)$。

一旦收到该信息，验证者就可以按以下步骤识别签字者 u_i:

$$\beta_i = g \quad y_i \bmod p \tag{20}$$

$$\partial = \alpha \quad H_i \bmod p \tag{21}$$

检查关系式:

$$\beta_i^{r_T} \quad \partial^{r_T} \equiv r_T \bmod p \tag{22}$$

若 (22) 式成立，则验证者就可识别出 u_i 是组签字者。

下面证明 (22) 式的正确性:

$$\begin{aligned}
r_T &\equiv \beta_i^{d} \quad (\text{由}(18)(20)\ \text{式})\\
&\equiv \beta_i^{s_T + r_T\,a\,k_i} \quad (\text{由}(19)\ \text{式})\\
&\equiv \beta_i^{s_T} \quad (g \quad g_i^{x_i})^{r_T\,a\,k_i} \quad (\text{由}(20)(1)\ \text{式})\\
&\equiv \beta_i^{s_T} \quad [g^{a\,k_i} \quad g^{a\,k_i\,x_i}]^{r_T}\\
&\equiv \beta_i^{s_T} \quad (\alpha_i \quad H_i)^{r_T}\\
&\equiv \beta_i^{s_T} \quad [\alpha_i \quad \alpha \quad A]^{r_T} \quad (\text{由}(11)(6)(14)\ \text{式})\\
&\equiv \beta_i^{s_T} \quad \partial^{r_T} \bmod p \quad (\text{由}(12)\ \text{式}) \qquad (\text{证毕})
\end{aligned}$$

2 方案的安全特性分析

攻击 1: 组权威企图获取组成员 u_i 的保密密钥 x_i。虽然组权威知道 $(r_i,\ s_i,\ k_i)$ 并可由 (3) 式求得 y_i。但要从 (1) 式求解 x_i，得求解离散对数问题[3, 4]。

攻击 2: 组权威企图伪装成组签字者。由 (1) 式，因为生成器 α_i 与 g 均为 q 阶，所以组权威用 $(r_i,\ s_i,\ k_i)$ 由 (12) (13) 式伪造 $(R,\ S)$ 的难度与攻破 ELGmal 方案[6]的难度一样[3]，得求解离散对数。既然组权威不能进行伪造攻击，那么其他入侵者进行伪装攻击就更难了。

攻击 3: 入侵者从所接收的签字 $\{R,\ S,\ h\ (m),\ A,\ B,\ C,\ D,\ E\}$ 中企图获得 y_i，进而可以识别签字者。但入侵者不知道签字者的 $(r_i,\ s_i,\ k_i)$，于是，他不能检查 (17) 式。要从 $\{A,\ B,\ C,\ D,\ E\}$ 中获取 $(r_i,\ s_i,\ k_i)$ 再获取 y_i，其难度比求解离散对数还难[8]。由此可见，在这种情况下，组签字者的 "匿名" 性是可以得到保证的。

攻击 4：入侵者接到组权威公布给验证者的信息 (r_T, S_T, y_i) 之后，企图标识出 u_i 以前的所有组签名，破坏“匿名”性。组权威公布信息 m 的信息 (r_T, S_T, y_i) 使验证者能够检查 u_i 的身份，这不会损坏 u_i 以前组签名的匿名性。因为 (r_T, S_T, y_i) 提供的只是针对指定信息 m 的一次组签名 $\{R, S, h(m), A, B, C, D, E\}$。对于不同的信息，$u_i$ 将去选择不同的随机整数 a、b、t 来生成组签名。若入侵者要从可获取的 $\{A, B, C, D, E\}$ 中获取 a、b、t 及 (r_i, s_i)，其难度比求解离散对数还难[7, 8, 9]。

3 结论

基于离散对数，本文给出了一种非交互式的组签字方案。该方案保留了已有方案的优点，并从根本上解决了组签字的“匿名”性问题。但在通信时间及组签字长度方面增加了一些开销。当然，签字者 u_i 可以使用 (r_i, s_i) 预先计算不同的 $\{\alpha, A, B, C, D\}$ 来改善方案的实时特性。

参考文献:

[1] CHAUM D. and HEYST, E. Group signature [A]. Proc. EUROCRYPT'91, 1992: 257-265.

[2] CHEN L. and PEDRSEN T. P. New group signature schemes [A]. Proc. EUROCRYPT'94, 1995, PP. 171～181.

[3] 施荣华. 一种基于单向函数的双重认证存取控制方案 [J]. 电子科学学刊, 1992, 19 (2): 278～281.

[4] Harn L. New digital signature scheme based on discrete logarithm [J]. Electron Lett. 1994; 30 (5): 396-398.

[5] LEE W. B. and CHANG C. C. Efficient group signature scheme based on the discrete logarithms [J]. IEE Proc. Comput. Digit. Tech., 1998, 145 (1): 15～18

[6] ELGamal. T. A public key Crypto-system and a signature scheme based on discrete logarithms [J]. IEEE Trans. IT, 1985, 31 (4): 469～472.

[7] Harn L. Group-oriented (t, n) threshold digital signature and digital multisignature [J]. IEE Proc. Comp. Digit. Teeh., 1994, 141 (5): 307～313.

[8] 祁明, 肖国镇. 基于 Harn 签字方案的远距离通行字认证方案 [J]. 通信学报, 1996, 17 (1).

[9] 施荣华. 一种能抵御重试攻击的远程用户认证方案 [J]. 铁道学报, 1997, 19 (6): 82～85.