

文章编号: 1673-1522 (2010) 04-0472-03

# 一种新的在线/离线门限签名方案

张津铭<sup>1</sup>, 李树栋<sup>2</sup>, 陆洪文<sup>3,4</sup>

(1. 烟台职业学院 信息工程系; 2. 山东工商学院 数学学院, 山东 烟台 264005;  
3. 同济大学 应用数学系, 上海 100092; 4. 华东师范大学 网络信息安全研究所, 上海 200062)

**摘要:** 基于门限签名算法和变色龙哈希函数, 提出了一种新的在线/离线门限签名方案, 其安全性完全基于离散对数假设。该方案能容忍  $t < n/3$  个恶意会员, 并在标准模型中证明该方案是安全的。

**关键词:** 门限签名; 在线/离线; 离散对数

**中图分类号:** TP393.08

**文献标志码:** A

## 0 引言

一个  $(t, n)$  门限签名<sup>[1]</sup>将签名密钥分发给  $n$  个成员, 任何大于或等于  $t$  个成员可联合重构出签名密钥, 从而产生合法的有效签名。门限签名在大规模的分布式数据存储等系统中有广泛的应用, 但在这些系统中, 计算门限签名需要大量的时间。在线/离线门限签名可有效解决该问题, 它将大量的签名运算集中在离线签名阶段, 在线签名阶段只需少量的计算即可生成消息的签名。变色龙哈希函数<sup>[2]</sup>是一个具有门限密钥的哈希函数, 一旦门限密钥已知可找到任意有效的碰撞, 是构造在线/离线签名的一个重要密码学工具。很多密码学者认为, 在随机预言模型下证明安全的签名方案, 在实际应用中有时是不安全的, 建立标准模型下的签名方案具有更强的安全性。文献[3]提出了一种标准模型下的门限签名方案, 本文基于该门限签名方案和变色龙哈希函数, 构造一种新的在线/离线门限签名方案。在不需要可信中心的条件下, 能保证签名方案的安全性和高效性。同时, 新方案也是强壮的, 即使最多有  $t$  个成员被敌手攻陷, 也能产生合法的门限签名。

## 1 准备知识

### 1.1 双线性映射

设  $G_1$  和  $G_2$  是两个阶为素数  $p$  的循环群,  $g$  是  $G_1$

的生成元, 则双线性映射  $e: G_1 \times G_1 \rightarrow G_2$  具有如下性质:

双线性: 若对任意的  $P, Q \in G_1$ ,  $a, b \in Z_p$ , 有  $e(P^a, Q^b) = e(P, Q)^{ab}$ ;

交换性:  $e(P, Q) = e(Q, P)^{-1}$ ;

非退化性: 存在  $P, Q \in G_1$ , 使得  $e(P, Q)$  不等于  $G_2$  的单位元;

可计算性: 存在一个高效的算法<sup>[1]</sup>计算  $e(P, Q)$ , 其中  $P, Q \in G_1$ 。

### 1.2 离散对数假设

设  $G_1$  是阶为素数  $p$  的循环群,  $g$  是  $G_1$  的生成元, 离散对数困难问题描述为: 设点  $P \in G_1$ , 求整数  $x$ , 使得  $P = g^x$ 。

### 1.3 门限签名方案

一个  $(t, n)$  门限签名方案一般由 3 个算法构成。门限密钥生成算法生成群公钥  $VK$  以及每个成员的私钥份额  $sk_i$ , 即  $(sk_i)$  构成群私钥  $SK$  的门限秘密分享。门限签名生成算法对于给定的签名消息  $m$ ,  $t$  个以上的成员联合生成消息  $m$  的门限签名。门限签名验证算法检验给定消息签名的有效性。

### 1.4 门限签名的安全性

一个  $(t, n)$  门限签名是安全的, 必须满足以下两个条件:

健壮性: 敌手最多可攻陷  $t$  个成员, 算法仍能

收稿日期: 2009-11-25; 修回日期: 2010-04-30

基金项目: 国家自然科学基金资助项目 (10471104); 上海市科委基金资助项目 (03JC14027)

作者简介: 张津铭 (1980-), 男, 硕士。

成功地运行，生成有效的合法签名。

不可伪造性：敌手进行有效次的选择消息询问后，伪造一个合法签名的概率是可忽略的。

### 1.5 在线/离线门限签名

与门限签名方案基本相同，但在线/离线门限签名将签名算法分成两个阶段。离线签名阶段生成一个签名标签和每个成员的部分签名；在线签名阶段根据签名消息、签名标签和部分签名生成消息的门限签名。

## 2 在线/离线门限签名方案

设  $n$  个群签名成员  $(P_1, \dots, P_n)$ ， $t < n/3$  是门限值。选择散列函数  $H_1: \{0,1\}^* \rightarrow \{0,1\}^{nm}$  将签名消息的长度映射为固定长度  $nm$ 。

令  $G_1$  和  $G_2$  是两个阶为素数  $p$  的有限循环群， $g$  是  $G_1$  的一个生成元。

构造双线性配对  $e: G_1 \times G_1 \rightarrow G_2$ ，随机选取  $h, u \in G_1$ ， $n_m$  维向量  $U = (u_i)$ ，其中， $u_i \in G_1$ 。所有签名成员共享公共参数  $(G_1, G_2, e, p, g, H_1, nm, h, u, U)$ 。

用 T-Key 表示文献[3]中门限签名方案的密钥生成算法，T-Sign 表示门限签名的生成算法，T-Vry 表示签名验证算法。

### 2.1 密钥生成算法

1) 所有成员运行一次门限密钥生成算法 T-Key，生成群公钥  $VK = e(h, g)^{SK}$ ，每个成员  $P_i$  得到群私钥  $SK$  的秘密份额  $sk_i$ 。

2) 所有成员运行两次分布式密钥生成协议 DKG<sup>[4]</sup>，生成两个公开值  $h_1 = g^y$  和  $h_2 = g^z$ ，其中  $y, z \in Z_p$ ；每个成员  $P_i$  获得  $y$  和  $z$  的秘密份额  $y_i$  和  $z_i$ 。

3) 所有成员运行一次求逆元算法 INV<sup>[5]</sup>，每个成员  $P_i$  获得  $y$  的逆元  $Y$  的秘密份额  $Y_i$ 。

4) 所有成员运行一次乘法算法 MUL<sup>[6]</sup>，每个成员  $P_i$  获得  $K = Y \times z$  的秘密份额  $K_i$ 。

公开参数  $PK = (VK, h_1, h_2, g^{K_i}, g^{Y_i})$ ，每个成员  $P_i$  的私钥  $SK_i = (sk_i, y_i, z_i, Y_i, K_i)$ 。

### 2.2 离线签名算法

1) 所有成员运行 3 次可验证的秘密分享协议 VSS<sup>[7]</sup>，生成 3 个随机数  $c, r, s$ ，其中  $c, r, s \in Z_p$ ；每个成员  $P_i$  获得  $c, r, s$  的秘密份额  $c_i, r_i, s_i$ 。

2) 所有成员输入  $c_i, r_i, s_i$  运行一次幂指数运算算法 EXP<sup>[8]</sup>，生成  $comm = g^c h_1^r h_2^s$ ，令

$$com = H_1(comm) \in \{0,1\}^{nm} \text{ 和 } \omega = u \prod_{i=1}^{nm} u_i^{com_i}。$$

3) 所有成员运行一次门限签名生成算法 T-Sign，生成  $com$  的门限签名  $\delta = (\delta_1, \delta_2)$ ，其中  $\delta_1 = h^{SK} \omega^r$ ， $\delta_2 = g^r$ ， $r \in Z_p$ 。

4) 所有成员运行 2 次乘法算法 MUL，计算  $r \times y$  和  $s \times z$ ，同时计算  $\mu = c + r \times y + s \times z$ 。再运行一次乘法算法 MUL，计算  $D = \mu \times Y$ ，每个成员  $P_i$  获得  $D$  的秘密份额  $D_i$ 。

5) 所有成员运行一次可验证的秘密分享协议 VSS，生成一个  $2t$  次多项式  $f_0(x)$ ，使得  $f_0(0) = 0$ ，每个成员  $P_i$  得到一个秘密份额  $f_i$ 。

6) 所有成员运行一次可验证的秘密分享协议 VSS，生成一个随机数  $s'$ ，每个成员  $P_i$  获得  $s'$  的秘密份额  $s'_i$ 。

7) 输出签名标签  $(com, \delta)$ ，每个成员  $P_i$  的部分签名是  $(D_i, f_i, s'_i)$ ，公开  $(g^{f_i}, g^{D_i})$ 。

### 2.3 在线签名算法

1) 假定签名的消息为  $m'$ ，每个成员广播  $s'_i$ ，则成员  $P_i$  利用插值公式可重构出  $s'$ 。

2) 每个成员  $P_i$  计算

$$r'_i = D_i - m' \times Y_i - s' \times K_i + f_i \text{ mod } p。$$

3) 每个成员  $P_i$  广播  $r'_i$ ，利用插值公式可重构出  $r'$ 。

4) 消息  $m'$  的门限签名是  $(com, \delta, r', s')$ 。

### 2.4 签名验证算法

1) 计算  $comm = g^{m'} h_1^{r'} h_2^{s'}$ 。

2) 利用门限签名验证算法 T-Vry 检验等式  $e(\delta_1, g) \times e(\delta_2, \omega)^{-1} = VK$  是否成立。

### 2.5 部分签名验证算法

当生成的门限签名是无效时，可利用下式检验部分签名的合法性：

$$e(g^{r'_i}, g) = e(g^{D_i}, g) e(g^{Y_i}, g)^{-m'} e(g^{K_i}, g)^{-s'} e(g^{f_i}, g)。$$

每次生成部分签名后不进行签名验证，只有最终的门限签名非法时，才运行部分签名验证算法。找出提供非法部分签名的成员并在群中删除，重新加入新成员生成合法有效的签名。

### 3 安全性和有效性分析

#### 3.1 正确性

$$\begin{aligned} e(g^{r_i}, g) &= e(g^{D_i - m' \times Y_i - s' \times K_i + f_i}, g) = \\ &= e(g^{D_i}, g) e(g^{Y_i}, g)^{-m'} e(g^{K_i}, g)^{-s'} e(g^{f_i}, g), \\ e(\delta_1, g) \times e(\delta_2, \omega)^{-1} &= e(h^{SK} \omega^r, g) \times e(g^r, \omega)^{-1} = \\ &= e(h^{SK}, g) \times e(\omega^r, g) \times e(g^r, \omega)^{-1} = e(h, g)^{SK} = VK。 \end{aligned}$$

#### 3.2 有效性

本文构造的门限签名算法，其计算量大部分在离线签名阶段，在线签名阶段只需两次模的乘法运算和加法运算，而不需要任何配对或幂指数运算，因此与文献[3]的门限签名方案相比，本文的签名方案签名速度更快、更高效。

#### 3.3 安全性分析

**定理 1：**本文的门限签名方案是强壮的， $t < n/3$ 。

证明：因为本文的方案所采用的标准协议和算法都是强壮的；且文献[3]的签名方案也具有强壮性，能容忍  $t < n/2$  个恶意成员的攻击，所以本文的门限签名方案也是强壮的。新方案的在线签名阶段重构  $r_i'$  时需要一个  $2t$  次多项式，但重构协议只允许最多有  $t$  个恶意成员，所以为了保证整个方案的强壮性，则  $t < n/3$ 。即最多有  $n/3$  个成员被敌手攻陷，本文的签名算法依然能正确运行，生成合法有效的门限签名。

**定理 2：**在标准模型下，本文的门限签名方案是不可伪造的。

证明：在标准模型下，文献[3]中基于 CDH 困难假设的门限签名方案是不可伪造的。本文采用了文献[2]的双门限密钥变色龙函数，文献[2]已证明该函数构造的分布式门限协议在标准模型下也是不可伪造的。于是利用类似文献[2-3]的方法构造门限密钥模拟器和门限签名模拟器，不仅能模拟攻击者在门限密钥生成算法中输出验证公钥的试图，也能模拟攻击者在门限签名算法中输出消息及签名的试图，所以本文的门限签名方案也是可模拟的，即在标准模型下本文的方案对适应性选择消息攻击也是不可伪造的。

综合定理 1 和 2，很容易得到如下定理：

**定理 3：**在离散对数困难问题假设下，即使任

意  $t < n/3$  个成员被敌手攻陷，我们的签名方案在标准模型下是安全的。

### 4 结论

基于传统的离散对数困难问题假设，提出了一种在标准模型下安全的在线/离线门限签名方案。签名的验证不需要成员的交互协商，且签名的计算量集中在离线签名阶段，在线签名阶段只需少量的计算，大大提高了门限签名的效率，使得门限签名具有更广的应用前景。

### 参考文献：

- [1] SHOUP GENNARO V. Securing threshold cryptosystems against chosen ciphertext attack[J]. Journal of Cryptology, 2002,15(1):75-96.
- [2] EMMANUEL BRESSON, DARIO CATALANO, ROSARIO GENNARO. Improved on-line/off-line threshold signatures[G]//LNCS. Berlin: Springer, 2007: 217-232.
- [3] 徐静. 标准模型下可证安全的门限签名方案[J]. 计算机学报, 2006,29(9):1636-1640.
- [4] GENNARO R, JARECKI S, KRAWCZYK H, et al. Secure distributed key generation for discrete-log public-key cryptosystems[J]. Journal of Cryptology, 2007,20(1):51-83.
- [5] BAR-ILAN J, BEAVER D. Non cryptographic fault tolerant computing in a constant number of rounds of interaction[C]//Proceedings of the ACM Symposium on Principles of Distributed Computation. 1980:201-209.
- [6] BEN-OR M, GOLDWASSER S, WIDGERSON A. Completeness theorems for non-cryptographic fault tolerant distributed computation[C]//Proceedings of 20<sup>th</sup> Annual Symposium on Theory of Computing. 1988:114-124.
- [7] Pedersen T. Non-interactive and information-theoretic secure verifiable secret sharing. Crypto'91[C]// Proceedings of the 11<sup>th</sup> Annual International Cryptology Conference on Advances in Cryptology. 1992:129-140
- [8] DIRAIMONDO M, GENNARO R. Provably secure threshold password-authenticated key exchange[C]// Proceedings of Eurocrypt'03. 2003:507-523.

(下转第 480 页)