第 16 卷第 4 期,增刊　　广西科学院学报　　Vol. 16, No. 4 & Supplement
2000 年 11 月　　Journal of Guangxi Academy of Sciences　　November 2000

一个基于 DSS/DSA 的群体数字签名—(t,n)共享认证方案

A Multisignature —(t,n) Shared Verification Scheme Based on DSS/DSA Signature Scheme

华 云　　钟 诚*　　苏德富
Hua Yun　　Zhong Cheng　　Su Defu

(广西大学计算机与信息工程学院　南宁　530004)
(College of Comp. & Info. Sci., Guangxi University, Nanning, 530004)

摘要　利用 DSS/DSA 数字签名标准,结合 Shamir 秘密共享方案,提出了多对多数字签名认证概念,并在此基础上建立、分析了一个新型数字签名方案。

关键词　数字签名　群体数字签名　共享认证　秘密共享
中图法分类号　TP 309.2

Abstract　Based on both DSS and DSA signature schemes, and combining Shamir's secret sharing scheme, a new multisignature-multiverification concept is proposed. In addition, a new signature scheme is presented and discussed.

Key words　digital signature, multisignature, shared verification, secret sharing

1991 年,美国国家安全局与国家标准局联合推出了美国数字签名体制 DSS 及其算法标准 DSA。随着计算机和网络通信技术的发展,应用需求的复杂化,数字签名技术也从最初意义上的单人签名,单人验证的模式扩展到更为广泛的领域。数字签名的(t,n)共享认证就是该要求的一种解决方案,它假定系统有n个认证者,需要其中的任意t个人方可对签名进行认证。文献[1]给出一种基于 DSA 的群体数字签名方案,文献[1～3]分别给出了(t,n)共享认证方案,但它们都存在一定缺陷,例如群体数字签名只能多人签名 1 人认证,(t,n)共享认证只能到了 1 人签名多人认证。文献[1]中所提出的基于 DSS/DSA 的(t,n)共享认证方案存在不合理性,即要求签名用户知晓认证中心系统秘密密钥。那么能不能找到一种办法,将多人签名与多人认证结合起来。本文即在上述方案的基础上,提出了一个基于 DSS/DSA 的群体数字签名—(t,n)共享认证方案。

1　方案描述

2000-09-20 收稿。

* 中国科技大学计算机系,安徽合肥,230027。

其中 m 为待签名信息，c 为签名信息，SGC 为签名中心，PGC 为验证中心。

PGC 上的约定：p_p 是素数（$2^{511}<p_p<2^{512}$），$w_p=(p_p-1)/2$ 是素数（$2^{510}<w_p<2^{511}$），q_p 为 w_p-1 的素因子（$2^{159}<q_p<2^{160}$），PGC 具有 n_p 个验认管理员，PGC 公开 p_p、w_p、q_p。

SGC 上的约定：p_s 是素数（$2^{511}<p_s<2^{512}$），q_s 是 p_s-1 的一个素因子（$2^{159}<q_s<2^{160}$），$g_s\equiv h_s^{(p_s-1)/q_s}\bmod p_s$，其中 h_s 为任一整数（$0<h_s<p_s$），且 $g_s>1$；Hs 是一个单向 hash 函数；SGC 公开 p_s、q_s、g_s、H_s；并假定其有 n_s 个用户参与签名。

方案分为 3 个阶段：SGC 向 PGC 注册阶段，SGC 签名阶段，PGC 验证阶段。

1.1　注册阶段

步骤 1：SGC 向 PGC 申请注册成为签名用户，PGC 产生随机数 $e(0<e<w_p)$，$x_s(0<x_s<q_s)$，计算 $\alpha_s\equiv e^{(\omega_p-1)/q_p}\bmod w_p>1$，则 α_s 为 $GF(w_p)$ 中阶为 q_p 的生成元，通过秘密通道将 α_s、x_s 发送给 SGC，其中 x_s 作为 SGC 对 PGC 签名的秘密密钥。

步骤 2：由 Shamir 秘密共享方案[4]，PGC 选取 Z_q 作为 x_s 可能的密钥集，构造一个具有固定参数 x_s 的 $t-1$ 阶多项式：

$$f(z)=x_s+a_1z+a_2z^2+\cdots+a_{t-1}z^{t-1}\bmod q_p,$$

其中 $a_i(i=1,2,\cdots,t-1)$ 是从 Z_q 中随机选取。PGC 向系统的 n_p 个管理员分发并于密钥 x_s 的部分信息 $x_i\equiv\alpha_s^{f(z_i)}\bmod w_p$，$(i=1,2,\cdots,n)$，作为个人密钥保管，$Z_i$ 是各管理员的公开信息，则这 n_s 个人至少 t 个在一起可恢复 $\alpha_s^{x_s}$（由 Lagrenge 插值法得到）：

$$\alpha_s^{x_s}=\alpha_s^{f(0)}\equiv\alpha_s^{(\sum_{i=1}^{t}f(z_i)\prod_{i\neq j,j=1}^{t}\frac{z_j}{z_j-z_i}\bmod q_p)}\bmod w_p\equiv\prod_{i=1}^{t}x_i^{(\prod_{i\neq j,j=1}^{t}\frac{z_j}{z_j-z_i}\bmod q_p)}\bmod w_p. \tag{1}$$

为安全起见，PGC 不保存 α_s、x_s，即注册过程结束后将 α_s、x_s 丢弃。

步骤 3：（可与步骤 2 并行地）SGC 计算　$y_s\equiv g_s^{x_s}\bmod p_s$ 为 x_s 对应的公钥（这里，可把 $\{x_S,y_S\}$ 看作是 SGC 中第 n_S+1 个参与签名的用户的秘钥、公钥对，仅由 SGC 掌握，且 y_s 同样处于保密状态）。通过方程：$y_s\equiv g_s^{x_s}\bmod p_s\equiv g_{sp}^{\alpha_s^{x_s}}$ 解出 g_{sp}。

1.2　签名阶段

步骤 1：每个用户 u_{is} 随机地选择 $k_{is}(0<is<n_s+1)$，计算 $r_{is}\equiv(g_s^{k_{is}}\bmod p_s)\bmod q_s$ 将 $\{r_{is},k_{is}\}$ 传送给签名中心 SGC。（其中第 n_s+1 个“用户”由 SGC 自身担任）

步骤 2：SGC 计算 $r\equiv(\prod_{is=1}^{n_s+1}r_{is}\bmod p_s)\bmod q_s$，　$k\equiv\sum_{is=1}^{n_s+1}k_{is}\bmod q_s$. 将 $\{r,k,T\}$ 广播至每个用户，T 为 SGC 自动生成的时间戳。

步骤 3：每个用户 u_{is} 计算 $s_{is}\equiv(k^{-1}(H_s(m,T)+x_{is}r))\bmod q_s$. 将 s_{is} 传播至 SGC。其中 x_{is} 为各用户的秘钥，其对应的公钥为 $y_{is}\equiv g_s^{x_{is}}\bmod p_s$。

步骤 4：SGC 接收 s_{is}，并检验此签名是否合法。它首先查看是否 $1\leqslant r_{is},s_{is}\leqslant q_s-1$，若是则继续计算 $w_{is}\equiv(s_{is})^{-1}\bmod q_s$，$u1_{is}\equiv(H_s(m,T)w_{is})\bmod q_s$，　$u2_{is}\equiv(rw_{is})\bmod q_s$，　$v_{is}\equiv((g_s^{u1_{is}}\cdot y_s^{u2_{is}})\bmod p_s)\bmod q_s$. 若 $v_{is}=r_{is}$ 则从用户 u_{is} 得到的个体签名被验证。

步骤 5：SGC 计算 $s\equiv\sum_{is=1}^{n_s+1}s_{is}\bmod q_s$，然后将 $C=\{r,s,g_{sp},T\}$ 送至 PGC。

1.3　验证过程

PGC 接收到 $\{r,\ s,\ g_{sp},\ T\}$ 后，执行下列步骤。

步骤 1：计算 $\triangle T=T'-T$，（T' 是接收签名时间），如果超过规定值，则拒绝认证，否则执

行步骤 2。

步骤 2：查看 $1 \leqslant r, s \leqslant q_s - 1$，如果不是，拒绝认证，否则继续。

步骤 3：计算 $y' \equiv \prod_{i=1}^{n_s} y_i \bmod p_s$，$y_i$ 为 n_s 个签名者的公开密钥；在 n_p 个验证者中任选 t 个，由 (1) 式计算出 $\alpha_s^{x_s}$，进而计算 $y'_s \equiv g_{sp}^{\alpha_s^{x_s}} \bmod p_s$，$y \equiv y' \cdot y'_s \bmod p_s$ 即由 t 个验证者，方可求得 SGC 对 PGC 的签名公开密钥 y_s。

步骤 4：计算 $w \equiv s^{-1} \bmod q_s$，　$u1 \equiv ((n_s + 1) H_s(m, T) w) \bmod q_s$，

$$u2 \equiv (rw) \bmod q_s, \quad v \equiv ((g_s^{u1} \cdot y^{u2}) \bmod p_s) \bmod q_s.$$

若 $v = r$，那么签名被验证（关于 $v = r$ 的证明参见文献[1]）。

2 安全性分析

该签名方案中，签名方 SGC 与验认方 PGC 进行了两次交互，体现在 SGC 首先向 PGC 申请注册，通过秘密通道得到 x_s 和 α_s；然后 SGC 将签名信息 C 传递给 PGC。由于注册后 PGC 不保存 x_s 和 α_s，即 x_s 和 α_s 仅由 SGC 掌握，故在不失安全性前提下，并非每一次 SGC 向 PGC 提交签名都要执行注册过程，x_s 和 α_s 可在一定时期内有效。下面讨论对本方案的一些攻击情况。

攻击 1：n_s 个用户之外的第三方用户或少于 n_s 个用户企图伪造 n_s 个用户签名攻击。第三方用户或少于 n_s 个用户无法推测出剩余用户的秘密密钥 x_{is}，故而此类攻击无法成功。（由于本方案构架在 DSA 上，其安全性依赖于 DSA）

攻击 2：重播攻击，攻击者通过改变 T 来达到攻击目的，但由于其无法改变 $H_s(m, T)$，故而此类攻击无法成功。

攻击 3：PGC 中 t 个验证者联合伪造 SGC 签名攻击。大于等于 t 个验证者可以通过 (1) 式求解出 $\alpha_s^{x_s}$，进而妄想伪造 $n_s = 0$ 情况下的 SGC 签名。但由于通过方程：$y \equiv g_{sp}^{\alpha_s^{x_s}} \bmod p_s \equiv g_s^{x_s} \bmod p_s$，求解 x_s 属离散对数求解问题，故而排除了多于 t 个验证者联合攻击的可能。

攻击 4：n_s 个 SGC 用户与 PGC 小于 t 个不诚实验证者联合伪造验证攻击。根据 Shamir 秘密共享机制，任何小于 t 个用户无法求解 $\alpha_s^{x_s}$，故而此类攻击无法成功。

3 结语

该数据签名方案利用再构造一个第 $n_s + 1$ 用户的方式，将群体数字签名与 (t, n) 共享认证紧密地结合起来，实现了真实意义上的多人签名、多人认证。方案中要求多个用户联合签名，任何第三方用户或小于规定数目用户无法完成签名过程，提高了签名的可信赖性；多个验证者共享认证，任何小于规定数目验证者无法完成认证过程，分散了各个认证管理者的安全责任。可以认为，该方案较之传统的 1 对 1、多对 1、1 对多数字签名认证方案更可靠，安全性更高。

参考文献

1 谭凯军等. 基于数字签名方案 DSS/DSA 的几种应用方案. 计算机研究与发展，1999，36 (5)：632～637.

2 祁 明，肖国镇. 基于 Harn 签名方案的远距离通行字认证方案. 通信学报，1996，17 (1)：114～119.

3 施荣华. 基于离散对数的 (t, n) 门陷共享验证签名方案. 计算机研究与发展，2000，37 (3)：319～323.

4 Shamir A. How to share a secret. Commun ACM，1979，22 (3)：612～613.

5 卢开澄. 计算机密码学—计算机网络中的数据保密与安全. 第 2 版. 北京：清华大学出版社，1998，7.

（责任编辑：黎贞崇）