一个带签名者意向的结构化多重签名方案

吴克力[①②] 吴 斌[①] 韦相和[①] 刘凤玉[②]
[①](淮阴师范学院计算机科学系 淮安 223001)
[②](南京理工大学计算机科学与技术系 南京 210094)

摘 要 多重签名是一种由多个签名者同时协作完成对一个消息签名的群体签名形式。在多重签名技术的应用中，签名方之间的签名顺序有可能需要满足某一特定的要求，有时签名者还要对消息签署意见并供其后的签名者参考。考虑到这些应用需求，该文提出了一个基于双线性对的多重签名方案，该方案具有预先设定签名者之间的签名次序和在签名中加入签名者各自意向的特性。安全分析表明它能抵抗各种内部和外部攻击，是一种安全的多重签名方案。

关键词 数字签名，签名者意向，结构化多重签名，双线性对
中图分类号：TP309.2 **文献标识码**：A **文章编号**：1009-5896(2006)05-0823-04

A Structured Multi-signature Scheme with Signers' Intentions

Wu Ke-li[①②] Wu Bin[①] Wei Xiang-he[①] Liu Feng-yu[②]
[①](*Department of Computer Science, Huaiyin Teachers College, Huaian* 223001,*China*)
[②](*Dept. of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing* 210094, *China*)

Abstract A multi-signature scheme is a digital signature scheme that allow multiple signers to generate in a collaborative and simultaneous manner. In the application of multi-signature, the signing order among co-signers may satisfy a special sequence and sometimes the each signer can express his intention associating with the message to be signed and referring by others. Considering the need of application, a multi-signature from bilinear pairings is proposed in this paper. The proposed scheme has two properties that it can set up the order of signing in advance and add the intention of signer into the signature. The security analysis of the new scheme shows that it can resist all kind of outsider and insider attacks.

Key words Digital signature, Signers' intentions, Structured multi-signature, Bilinear pairings

1 引言

在现实生活中，一份文件需要几个单位或部门分别盖章是件十分常见的事，多重签名技术就是在Internet环境里解决这类问题的一种方法。在一些应用中，对一个文件的盖章需要考虑先后顺序，即只有当某一个或几个部门结束盖章后，才能执行该部门的盖章，据此文献[1,2]提出了结构化多重签名的概念。在对文件的内容进行签名的同时，有时会要求签名方注明同意与否等信息，也就是要签署意见，针对该问题文献[3]提出了一种带签名者意向的多重签名方案。

正是由于多重签名技术的应用范围较广，使得同时由多人参与的多重签名协议研究是数字签名领域中一个十分活跃的分支，已有诸多方案被提出。它们可分为两类：基于RSA的多重签名方案和基于离散对数问题的多重签名方案[4]。考虑到应用领域的特点，人们又先后提出了有序多重签名、代理多重签名[5]、带签名者意向的多重签名等概念和相应方案，满足了应用的多样性需求。在日常事务中，签名方往往需要依据所签文件和相关方签署的内容决定自己的意见，如：总经理常常根据部门经理签署的意见做出自己的决定。可见，多重签名方案中同时具有结构化和带有签名者意向双重特性在一些应用场合有用武之地。

将多重签名中结构化和签名者意向两概念结合，借鉴文献[2]的思想方法，本文提出了一种具有结构化和带签名方意向两个特性的多重签名方案。它以双线性对运算为基础，有高效和安全的特点。

2 双线性对基础

近年来，双线性对因其良好的特性在密码学的研究中找

2004-10-13收到，2005-06-03改回
国家自然科学基金(60273035)，国防科工委应用基础基金(J1300D004)和江苏省高校自然科学研究指导性项目(03KJD520055)资助课题

到了许多应用，下面对该内容做一简要介绍，详见文献[6,7]。

定义 1 设 G 是由 P 生成的循环加群，其阶为素数 q；V 是一个阶为 q 的循环乘群。双线性对是指具有下面性质的映射 $e:G\times G\to V$：

(1)双线性　对所有的 $P,Q\in G$ 和 $a,b\in Z_q^*$，

$e(aP,bQ)=e(abP,Q)=e(P,abQ)=e(P,Q)^{ab}$。

(2)非退化　存在一个 $P\in G$，满足 $e(P,P)\neq 1$。

(3)可计算　对 $P,Q\in G$，存在一个有效的算法计算 $e(P,Q)$。

注：超单椭圆曲线中的 Weil 对和 Tate 对具有上述双线性性质。

几个数学问题：

(1)离散对数问题(DLP)：给定 P 和 G，找整数 n，满足 $Q=nP$。

(2)判定 Diffie-Hellman 问题(DDHP)：对 $a,b,c\in Z_q^*$，给出 P,aP,bP,cP 判定 $c\equiv ab \bmod q$ 是否成立。

(3)计算 Diffie-Hellman 问题(CDHP)：对 $a,b\in Z_q^*$，给定 P,aP,bP 计算 abP。

(4)间隙 Diffie-Hellman 问题(GDHP)：指这样一类问题，其上 CDHP 是困难问题而 DDHP 不是。

这里假设 CDHP 和 DLP 是困难问题，即对该问题不存在有不可忽略概率值的多项式时间算法。在群 G 上，若 DDHP 不是困难问题而 CDHP 是困难问题，称群 G 为间隙 Diffie-Hellman 群。这类群存在于超单椭圆曲线或有限域上的超椭圆曲线。在 G 上，求双线性对的逆是困难问题，即给出 $P\in G$ 和 $e(P,Q)\in V$，找 $Q\in G$ 还不存在有效的算法。

3 多重签名的结构化与签名方意向

多重签名是由多个签名者对同一个文件进行分别签名的签名方式，在现实世界中普遍存在。多个签名者的地位通常是不平等的，因而签名也常有先后顺序的问题，有序多重签名就是该类问题的一种解决方案。将有序情况一般化，人们又提出了结构化多重签名的概念[1]。

假设 $Q=\{u_1,u_2,\cdots,u_n\}$ 表示由 n 个共同参与结构化多重签名的成员组成的集合，签名结构 Λ (如图 1)是一个有向图，其中 $u_i\in Q$ 为实心点，表示签名者，u_0 和 u_∞ 为空心点，分别表示起始点和终止点。从 u_a 指向 u_b 的有向边表示在 u_b 签名前应先完成 u_a 的签名。对于更一般的情况如图 1(c)，u_2 到 u_3 的有向边表示当 u_2 签名结束后才能让 u_3 签名，u_3 签名结束后应将所签结果传给 u_4 和 u_5。用 $\mathrm{prev}(u_i)$ 表示在签名结构 Λ 中 u_i 的直接前趋元素所构成的集合，如在图 1(c)中，$\mathrm{prev}(u_5)=\{u_1,u_3\}$。显然，串行和并行两种情况可认为是混合情况的特例。

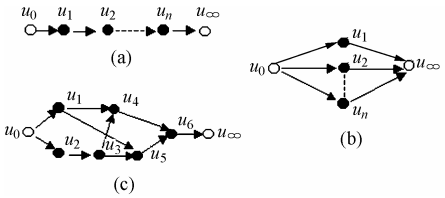

图 1 签名结构 (a)串行　(b)并行　(c)混合

Fig. 1 Signature structure, (a)Serial, (b)Parallel, (c)Mixed

根据消息的内容表明签名者的意见在现实生活中极为常见，将其与签名结果结合更能有效地防止签名方意见被恶意更换的情况发生。签名者针对文件或消息内容所欲表示的意见通常是可事先确定的几种形式，如：同意、不同意、暂缓等，可用集合 $I=\{I_1,I_2,\cdots,I_m\}$ 表示，所有签名者的意向取之于集合 I。

4 带签名方意向的结构化多重签名方案

在多重签名中，每个参与者均有自己的密钥以及相应的公钥。结构化多重签名中，需要根据签名结构 Λ 和签名成员 $Q=\{u_1,u_2,\cdots,u_n\}$ 的密钥产生签名的验证公钥。以下是我们基于双线性对运算所构造的带有签名方意向的结构化多重签名方案。

4.1 系统参数

G，V，P，q 和 e 参见第 2 节。$x_i\in Z_q^*$ 是签名者 u_i 的签名密钥，$y_i=x_iP$ 是相应的公钥。H_1 是一个单向 hash 函数，$H_1:\{0,1\}^*\to G$。H_2 也是一个单向 hash 函数，$H_2:\{0,1\}^*\to Z_q^*$。

4.2 验证公钥的生成

假设所有的签名者 $u_i\in Q$ 同意签名结构 Λ，起点 u_0 产生 $v_0=0$，$v_0\in G$。对于每一个 $u_i\in Q$ 依据 Λ 的次序生成 $v_i=x_i\left(P+\sum_{u_j\in \mathrm{prev}(u_i)}v_j\right)$，任何人均可通过验证式(1)得到 v_i 是否有效。

$$e(P,v_i)=e\left(P+\sum\nolimits_{u_j\in \mathrm{prev}(u_i)}v_j,y_i\right) \tag{1}$$

最后，多重签名的验证公钥为 $v=\sum_{u_j\in \mathrm{prev}(u_\infty)}v_j$。

4.3 多重签名的产生

设 m 为所签消息。集合 $\alpha=\{\alpha_1,\cdots,\alpha_l\}$ 为签名者意向集，这里 $\alpha_i\in I$。依据签名结构图 Λ，每个签名者 $u_i\in Q$ 顺次执行下列步骤。

步骤 1　首先验证其直接前趋的意向的有效性，根据所签消息 m 和其直接前趋 $\mathrm{prev}(u_i)$ 的签名意向确定自己的签名意向 α_i，计算 $c_i=H_2(m,\alpha_i)$ 和 $M=H_1(m)$。

步骤 2　对 $u_j\in\mathrm{prev}(u_i)$，验证 $e(P,\sigma_j)=e(M,v_j)$ 是否成立。为真，则继续。任取 $r_i\in_R Z_q^*$，计算 $k_i=r_iP$ 和 $d_i=c_ix_i+r_i \bmod q$。再计算 $\sigma_i=x_i(M+\sum_{u_j\in\mathrm{prev}(u_i)}\sigma_j)$，这

里 $\sigma_0=0$。将 α_i 并入 α，即 $\alpha=\alpha\cup\alpha_i$。将 (k_i,d_i,σ_i) 传给其后继结点。

终点 u_∞ 进行多重签名的最后阶段的工作，计算 $\sigma=\sum_{u_j\in\mathrm{prev}(u_\infty)}\sigma_j$，对每个 u_i 的签名意向利用 $e(d_iP,P)=e(c_iy_i,P)e(k_i,P)$ 进行验证，计算 $D=\sum_{i=1}^{n}d_i$ 和 $K=\sum_{i=1}^{n}k_i$。以 4 元组 (α,K,D,σ) 作为带签名者意向 α 的结构化签名的签名结果。

4.4 多重签名的验证

签名的验证方先根据 α，计算出 $c_i=H_2(m,\alpha_i)$ 其中 $i=1,\cdots,n$，再计算 $M=H_1(m)$。用式(2)验证结构化签名正确与否。

$$e(P,\sigma)=e(v,M) \tag{2}$$

用式(3)验证签名意向的有效性。

$$e(DP,P)=e\left(\sum_{i=1}^{n}c_iy_i,P\right)e(K,P) \tag{3}$$

若对消息 m 的多重签名使等式(2)，式(3)成立，则说明签名有效。

4.5 正确性推导

定理 1　满足校验方程式(2)和式(3)的签名是有效的带签名者意向的结构化多重签名。

证明　先证式(2)。

设 u_t 的直接前趋是 u_0，则有 $e(P,x_tM)=e(M,x_tP)$。若 u_l 是 u_t 的直接后继，于是，

$$\begin{aligned}e(P,\sigma_l)&=e(P,x_l(M+x_tM))=e(P,x_lM)e(P,x_lx_tM)\\&=e(x_lP,M)e(x_lx_tP,M)\\&=e(x_l(P+x_tP),M)=e(v_l,M)=e(M,v_l)\end{aligned}$$

同理，应用递推式可得对任一 u_j 有 $e(P,\sigma_j)=e(M,v_j)$，所以有

$$\begin{aligned}e(P,\sigma)&=e\left(P,\sum_{u_j\in\mathrm{prev}(u_i)}\sigma_j\right)=\prod_{u_j\in\mathrm{prev}(u_i)}e(P,\sigma_j)\\&=\prod_{u_j\in\mathrm{prev}(u_i)}e(M,v_j)=e\left(M,\sum_{u_j\in\mathrm{prev}(u_i)}v_j\right)\\&=e(M,v)\end{aligned}$$

再证式(3)。

$$\begin{aligned}e(DP,P)&=e\left(\sum_{i=1}^{n}d_iP,P\right)\\&=\prod_{i=1}^{n}e(d_iP,P)=\prod_{i=1}^{n}e(c_ix_iP,P)e(r_iP,P)\\&=\prod_{i=1}^{n}e(c_iy_i,P)e(k_i,P)=e\left(\sum_{i=1}^{n}c_iy_i,P\right)e\left(\sum_{i=1}^{n}k_i,P\right)\\&=e\left(\sum_{i=1}^{n}c_iy_i,P\right)e(K,P)\end{aligned}$$

证毕

所以，能通过方程式(2)和式(3)检验的签名是有效的带有签名者意向且结构化的多重签名。

5　安全性分析

对于由多人合作产生签名的方案，它的安全性一般应从签名集体内部和外部两个方面进行考虑。以下是我们对方案的安全性所进行的分析。

定理 2　恶意的外部攻击者无法根据 v 和 α 伪造出对消息 m 的多重签名。

证明　攻击者能很容易得到 P，M 和 v，则 $e(M,v)$ 易求出，但解 $e(P,\sigma)=e(M,v)$ 中的 σ 将面临困境。攻击者若用另一消息 m' 的签名 σ' 充当 m 的签名，此时必须能给出合适的 M，与前相同这是十分困难的。攻击者欲篡改签名者的意向，他能算出 $e\left(\sum_{i=1}^{n}c_iy_i,P\right)$，但给出 D，K 中任一个根据式(3)求出另一个将面临解困难问题。

因此，外部攻击者成功地伪造签名和篡改签名者意向的可能性极低。

定理 3　部分签名者合谋伪造多重签名将面临解困难问题。

证明　这里考虑某一个签名者 u' 没有参与签名，另外 $n-1$ 签名人合谋伪造有效签名的情况。v 是由 n 个签名者事先联合产生的验证公钥，含有 u' 的私钥。事实上，若在 σ 和 $\sum_{i=1}^{n}c_iy_i$ 中绕过 u' 或编造一个值，将使验证方程式(2)和式(3)不能成立，即不能通过验证，是无效签名。要根据 $y_i=x_iP$ 求出 x_i，则遇到解 DLP 难题。因而缺少任一签名者参与的签名均不能顺利通过式(2)和式(3)的验证。

定理 4　不按预定的结构次序所做的多重签名不能被验证为真。

证明　从运算公式 $\sigma_i=x_i\left(M+\sum_{u_j\in prev(u_i)}\sigma_j\right)$ 不难看出整个计算值与 x_i 的位置有关，所以，调整签名者的次序将使签名结果 σ 与 v 不匹配。不过签名意向的验证与次序无关。

定理 5　签名者不能抵赖自己所选的意向。

证明　签名方的意向已通过 $c_i=H_2(m,\alpha_i)$ 使其与 m 和 c_i 相关，在不知道 r_i 和 x_i 的情况下，能计算出通过 $e(d_iP,P)=e(c_iy_i,P)e(k_i,P)$ 验证的 d_i 和 k_i 的概率可忽略不计，因而能通过验证的 α_i 必为其本人所选。

定理 6　签名意向与消息不可分离。

证明　攻击者想用对其有利的消息 m' 的意向 α' 来代替消息 m 的意向，必将导致验证时计算出的 c_i 不能使式(3)成立，这样用 hash 单向函数确保了意向与消息之间的联系。

综上分析，本文提出的多重签名方案是安全的。

6　结束语

随着 Internet 上的电子商务、电子政务的广泛应用，多重签名技术必将以其独有的特性为这些领域提供其它技术

所不能替代的服务。本文提出的方案融入了在实际应用中普遍存在的两个需求，是一种更加实用的多重签名方案。

利用双线性对的运算性质，本文构造了一个含有签名者意向和必须按照预定好的次序签名的多重签名协议。正如文献[6]所述，基于双线性对的签名长度在相同的安全等级下与 DSA 签名相比较短，本方案也有这个特点。安全分析表明该方案是安全的，此外，签名者意向和结构化多重签名在本方案中是相对独立的两个部分，完全可以单独使用结构化多重签名部分。

参 考 文 献

[1] Burmester M, Doi H, Mambo M, Okamoto E, Tada M, Yoshifuji Y. A structured ElGamal-type multisignature scheme. Proceedings of International Workshop on Practice and Theory in Public Key Cryptography, LNCS, Springer-Verlag, 2000, Vol.1751: 466 – 483.

[2] Lin CY, Wu TC, Zhang F. A structured multisignature scheme from the gap Diffie-Hellman group. http://citeseer. ist. psu. edu /576710.html

[3] Kawauch K, Minato H, Miyaji A, Tada M. A multi-signature scheme with signers' intentions secure against active attacks. ICISC 2001, Seoul, South Korea: 328 – 340.

[4] Mitomi S, Miyaji A. A general model of multisignature schemes with message flexibility, order flexibility, and order verifiability. *IEICE Trans. Fundamentals*, 2001, E84-A(10): 2488 – 2499.

[5] 伊丽江，白国强，肖国镇. 代理多重签名：一类新的代理签名方案. 电子学报，2001，29 (4)：569 – 570.

[6] Boneh D, Shacham H, Lynn B. Short signatures from the Weil pairing. In proceedings of Asiacrypt '01, LNCS, Springer-Verlag 2001, Vol. 2139: 514 – 532.

[7] Chen X, Zhang F, Kim K. A new ID-based group signature scheme from bilinear pairings. Proceedings of WISA'2003, Jeju Island(KR), August 2003: 585 – 592.

吴克力： 男，1963 年生，副教授，博士，主要研究方向为信息安全、数字签名.

吴 斌： 男，1963 年生，讲师，主要研究方向为计算机网络.

韦相和： 男，1965 年生，讲师，硕士生，研究方向为网络安全.

刘凤玉： 女，1943 年生，教授，博士生导师，主要研究领域为人工智能、信息安全技术等.