云南大学学报（自然科学版），2011，33（6）：658～661　　CN 53－1045/N　ISSN 0258－7971
Journal of Yunnan University　　http://www.yndxxb.ynu.edu.cn

公平的基于身份的有向签名方案*

王大星[1]，朱鹤鸣[1]，滕济凯[2]
（1.滁州学院 数学科学学院，安徽 滁州　239000；2.中国科学院 软件研究所，北京　100190）

摘要：为了保护签名接收者的隐私，有向签名方案要求签名的验证必须得到接收者或签名者的合作.利用椭圆曲线上双线性映射的基于身份的密码体制，提出了一个公平的基于身份的有向签名方案.当签名者与验证者发生争议时，在二者的协助下，可信第三方能够进行公开验证签名.结果的分析表明，所提方案与同类方案相比签名长度更短并且通信代价更小.

关键词：基于身份的密码体制；有向签名；双线性映射；公平性
中图分类号：TP 309　　**文献标识码**：A　　**文章编号**：0258－7971(2011)06－0658－04

在现代网络通信系统中，数字签名技术在数据完整性检验、身份鉴别、身份证明、防否认等方面独特的功能和实际用途，尤其是在一些特殊行业，比如金融、商业、军事等有着广泛的应用.普通的数字签名中，任何人只要获得签名者的公钥，就可以验证被签发的文件有效性[1].然而，对于一些私人或公司的保密文件的签名，如果也可以肆意传播和验证，定会造成不良后果甚至灾难.从另一个角度看，有些签名文件也许包含有汇款单、工资单、遗传病史等，这些对签名接收者是很敏感的.也就是说，这些签名最好只允许由接收者本人直接验证.

为了解决上述问题，有向签名方案[2]被提出.这种签名的特点是签名者以自己的私钥及指定接收者的公钥产生对消息的签名，接收者以自己的私钥及签名者的公钥来验证.近几年来，基于身份的公钥密码体系[3－5]引起了许多研究者的兴趣.基于身份的密码系统的主要优点是减少证书管理开销.使用基于身份的密码系统，不需要保存每个用户的公钥证书.系统中每个用户都有1个身份，用户的公钥可以由任何人根据其身份信息计算出来，而私钥则由可信中心统一生成.

作者提出了一个公平的基于身份的有向签名算法，该算法建立在Hess的签名方案[4]基础之上.当签名者与验证者发生争议时，可以由可信第三方出面调停，以达到公平性的效果.由于利用了双线性映射及基于身份的密码体系，本文所提方案与同类方案[6－7]相比签名长度更短并且通信成本更小.

1　准备工作

本节我们简要介绍一些背景知识和模型说明，以满足后文新方案的建立.

1.1　双线性对和密码学困难问题　设G_1，G_2为两个阶均为大素数q的群.其中G_1是一个加法循环群，G_2是一个乘法循环群.设p是G_1的任意一个生成元.假设离散对数问题(DLP)在G_1和G_2中都是困难的.映射$e:G_1 \times G_1 \to G_2$是密码学中的双线性对.

定义1　椭圆曲线离散对数问题(ECDLP)：给定1条定义于有限域F_q上的椭圆曲线E和E上的2点$P,Q \in E(F_q)$寻找一整数x，使在E中有$xP = Q$；

定义2　计算性Diffie－Hellman问题(CDHP)：已知P,aP,bP,cP，其中$a,b \in Z_q^*$，计算abP.到目前

* 收稿日期：2011－04－19
基金项目：国家自然科学基金重点项目资助(90604036)；安徽省高校省级自然科学研究项目资助(KJ2011Z277)；滁州学院科研基金资助项目资助(2010kj009B).
作者简介：王大星(1980－)，男，安徽人，硕士，讲师，主要从事密码学与信息安全方面的研究.

为止,上述 2 个问题都没有多项式时间的有效算法可以解决;

定义 3　可判别 Diffie – Hellman 问题(DDHP):给定(P,aP,bP,cP),$a,b,c \in Z_q^*$,如果有 $c = ab$ 成立,则称(P,aP,bP,cP) 为有效 Diffie – Hellman 元组.

1.2　Hess 签名方案简介　下面我们来简单介绍 Hess 签名过程.

系统的建立:密钥生成中心(PKG)随机选取 $s \in_R Z_q^*$ 作为它的主密钥,并计算它的全局公钥 $P_{\text{Pub}} = sP$. PKG 同时选择两个密码学上的哈希函数 $H_1:\{0,1\}^* \to G_1^*$,$h:\{0,1\}^* \times G_2 \to Z_q^*$. 然后,PKG 将主密钥 s 秘密保存,公布系统参数 params$\langle G_1,G_2,e,P,P_{\text{Pub}},H_1,h\rangle$.

密钥提取:假定签名者的身份信息是 ID,PKG 为签名者计算私钥 $d_{ID} = sQ_{ID}$,其中 $Q_{ID} = H_1(ID)$ 为签名者的公钥.

签名:要签发一条消息 $M \in \{0,1\}^*$,签名者任选 $P_1 \in G_1^*$,$k \in Z_q^*$ 然后计算 $R = e(P_1,P)^k$,$V = h(M,R)$,$U = Vd_{ID} + kP_1$. 消息 M 的签名是 $\sigma = (U,V) \in G_1 \times Z_q^*$.

验证:验证者计算 $R = e(U,P)e(Q_{ID}, -P_{Pub})^v$. 当且仅当 $V = h(M,R)$ 时接受签名.

1.3　新签名方案的模型说明　一个公平的基于身份的有向签名模型由算法集〈Setup,Extract,Sign,DVerify,TVerify〉组成,下面我们给出它们的定义.

系统初始化(Setup):密钥生成中心(PKG)生成系统参数 Params 和主密钥 x. 主密钥是秘密保存的,而系统参数 Params 是公开的,并且将会输入到以下所有的算法.

密钥提取(Extract):给定一个用户的身份信息 ID 和主密钥 x,PKG 为用户计算私钥 d_{ID},并通过安全的信道发送给该用户.

签名的生成(Sign):输入签名者的身份信息 IDs,验证者的身份信息 IDv,消息 M 和私钥 d_{ID},为指定验证者 IDv 生成关于消息 M 的签名 σ.

有向验证(DVerify):输入 IDs,IDv,私钥 d_{ID},消息 M 和签名 σ,该算法验证 σ 的有效性. 如果输出 1 表示签名有效,输出 0 表示签名无效.

可信方验证(TVerify):输入 IDs,IDv,消息 M 和签名 σ. 可信第三方(TTP)在 IDs 和 IDv 的协助下验证 σ 的有效性. 如果输出 1 表示签名有效,输出 0 表示签名无效.

2　基于身份的数字签名的安全模型

2.1　随机预言机模型　密码学上的 Hash 函数能保障数据的完整性. Hash 函数通常用来构造数据的短"指纹";一旦数据改变,指纹就不再正确. 即使数据被存储在不安全的地方,通过重新计算数据的指纹并验证是否改变,就能够检测数据的完整性[8].

1993 年,Bellare 和 Rogaway 引入随机预言机模型(Random Oracle Model)[9-10],提供了一个理想的 Hash 函数数学模型. 记 X 表示所有消息的集合,Y 表示所有的消息摘要组成的有限集,令 $F^{(x,y)}$ 为所有从 X 到 Y 的函数集合. 在这个模型中,随机从 $F^{(x,y)}$ 中选出一个 Hash 函数 $h:X \to Y$,我们仅允许预言器访问函数 h. 这意味着不会给出一个公式或者算法来计算函数 h 的值. 因此,计算 $h(x)$ 的惟一方法是询问预言器. 这可以想象为在一本巨大的关于随机数的书中查询 $h(x)$ 的值,对于每一个,有一个完全随机的值 $h(x)$ 与之对应. 作为在随机预言模型假定下的结果,下面的独立性质是显然的:

定理 1　假定 $h \in F^{(x,y)}$ 是随机选择的,令 $X_0 \subseteq X$,假定当且仅当 $x \in X_0$ 时,$h(x)$(通过 h 的随机预言器)被确定. 那么,对所有的 $x \in X \backslash X_0$ 和 $y \in Y$,有 $P_r[h(x) = y] = 1/M$.

在定理 1 中,概率 $P_r[h(x) = y]$ 实际上是对任意的 $x \in X_0$ 计算所有的函数 h,得出指定值的条件概率. 该定理是随机预言模型中关于问题复杂性证明中所要用到的关键性质[11-12].

2.2　基于身份的数字签名安全性定义

定义 4　(基于身份的数字签名的安全性定义)如果不存在这样的敌手,在概率多项式时间以一个不容忽略的优势在以下游戏中获胜,那么这样一个基于身份的数字签名在适应性选择消息和身份的攻击下是存在性不可伪造的.

(1) 挑战者 C 首先执行 setup 算法,生成系统参数 params 和系统私钥 s,然后将 params 发给敌手 A.

(2) 敌手 A 进行下面的预言机查询:

① Hash 询问:对 A 的每条 Hash 值的查询,算法 C 都返回相应的值给 A;

② 私钥解析询问:A 可以根据自己的需要向挑战者 C 询问用户 ID 的私钥,C 运行 Key Extract 算法产生私钥 d_{ID},并将 d_{ID} 发送给 A;

③ 签名询问:A 根据自己的需要向挑战者 C 询问身份 ID 关于任意消息 m 的签名,挑战者 C 运行 sign 算法生成相应的签名 σ 并返还给 A.

(3) A 生成1个身份 ID^* (ID^* 的私钥没有泄露) 的消息/签名对 M^*,σ^*,如果满足下面的条件,就表明 A 在该游戏中获胜.

① Verify(params,ID^*,M^*,σ^*) = 1;

② ID^* 从未提交给私钥解析预言机;

③ (ID^*,M^*) 从未提交给签名预言机.

3 公平的基于身份的有向签名方案

下面我们以 Hess 签名方案为基础,利用双线性对构造一种公平的基于身份的有向签名方案. 具体描述如下:

3.1 系统初始化(Setup) 密钥生成中心 PKG 随机选择 $x \in_R Z_q^*$ 作为其主密钥,并计算全局公钥 $P_{Pub} = xP$. 然后,PKG 选择安全的哈希函数 H_1,H_2,h. 其中,$H_1,H_2:\{0,1\}^* \to G_1^*$,$h:\{0,1\}^* \times G_2 \to Z_q^*$. 双线性映射 $e:G_1 \times G_1 \to G_2$,其中 G_1,G_2 分别为阶为素数 q 的加法群和乘法群,P 是 G_1 的一个生成元. 系统参数集为 params$\langle G_1,G_2,e,P,P_{Pub},H_1,h\rangle$.

3.2 密钥提取(Key Extract) 给定一个用户的身份 $ID \in \{0,1\}^*$. PKG 计算 $Q_{ID} = H_1(ID) \in G_1$,然后计算用户的私钥 $d_{ID} = xQ_{ID} \in G_1$.

3.3 签名的生成(Sign) 为了给一个指定的验证者 IDv 生成关于身份 IDs 的有向签名,我们按如下步骤进行:

Step1:签名者随机选择 $P_1 \in_R G_1^*, r_1, k \in Z_q^*$.

Step2:计算 $U = e(P_1P)^k, L = r_1Q_{IDs}$.

Step3:计算 $V = h(H,U)$,这里 $H = H_2(IDs,IDv,M,U,e(d_{IDs},r_1Q_{IDv}))$.

Step4:计算 $W = Vd_{IDs} + kP_1$.

最后得到消息 M 的签名即为 $\sigma = (V,W,L)$.

3.4 有向验证(DVerify) 对于一个声称是消息 M 的关于身份 IDs 的签名 $\sigma = (V,M,L)$,验证者 IDv 用他的私钥验证. 方法如下:

Step1:计算 $U' = e(W,P) \cdot e(Q_{IDs}, -P_{Pub})^v$.

Step2:计算 $H = H_2(IDs,IDv,M,U',e(d_{IDv},L))$.

如果 $V = h(H,U')$,则接受签名;否则就断定签名无效,拒绝接受.

3.5 可信方验证(TVerify) 当签名者与验证者发生争议时,对于上述一个有向签名方案,可信第三方(TTP) 可以解决争议. TTP 在 IDs 和 IDv 的协助下获得辅助信息 $A = e(d_{IDv},L) = e(d_{IDs}r_1Q_{IDv})$,TTP 计算 $U' = e(W,P) \cdot e(Q_{IDs}, -P_{Pub})^v$ 和 $H = H_2(IDs,IDv,M,U',A)$. 当 $V = h(H,U')$ 时接受签名,否则拒绝.

4 新方案的分析

下面我们对方案的正确性、安全性和效率方面作一些分析.

4.1 正确性分析 下面我们证明有向验证(DVerify) 算法的正确性,而可信方验证(TVerify) 正确性的证明类似. 从上述签名的过程和验证的过程知,我们只需证明 $U' = U$ 即可.

$$U' = e(W,P) \cdot e(Q_{IDs}, -P_{\mathrm{Pub}})^v = e(Vd_{IDs} + kP_1,P) \cdot e(Q_{IDs}, -P_{\mathrm{Pub}})^v =$$

$$e(Vd_{IDs},P)\cdot e(kP_1,P)\cdot e(Q_{IDs},-P_{Pub})^v = e(d_{IDs},P)^v\cdot e(P_1,P)^k\cdot e(Q_{IDs},-P_{Pub})^v =$$
$$e(Q_{IDs},-P_{Pub})^v\cdot e(P_1,P)^k\cdot e(Q_{IDs},-P_{Pub})^v = U.$$

4.2　安全性分析　从签名算法的过程知道,任何一个攻击者包括指定的接收者 *IDv* 都不能假冒签名者 *IDs* 伪造签名,因为 *IDv* 不能够从 U' 恢复出签名 σ. 另一方面,只有指定的接收者 *IDv* 利用自己的私钥 d_{IDv} 才能计算出 $e(d_{IDv},L)$,从而计算出 H. 因此,其他用户要验证该签名是不可行的. 也即伪造签名相当于计算 G_1 或 G_2 上的离散对数问题. 由于本方案基于 Hess 签名方案的,所以在随机预言模型下,其安全性等价于双线性 Diffe – Hellman 问题. 更详细的证明过程可以参考文献[6],这里不再赘述.

4.3　效率分析　下面我们来分析我们提出的签名方案的效率,并将其与目前较好的方案,即文献[6 – 7] 作比较. 我们只考虑双线性对的计算,而其它的计算(如点加点乘运算) 相对于双线性对的计算量很小,这里不作考虑. 记 Pa(即 Pairing) 表示需要计算双线性对的次数. 文献[6] 中的签名长度为 $3|G_1|$,签名阶段只需作 1 次双线性对运算,而有向验证和公开验证的计算量分别为为 4 次和 3 次双线性对运算. 文献[7] 的签名长度为 $4|G_1|$,有向验证和公开验证的计算量都比文献[6] 大. 通过比较发现,我们的方案在验证阶段计算量较小,并且签名的长度也较短. 具体如下表 1 所示.

表 1　几种同类方案的效率对比

Tab. 1 Efficiency compaison of several similar programs

方案	签名长度	签名计算量	有向验证计算量	公开验证计算量
文献[6]	$3\|G_1\|$	1Pa	4Pa	3Pa
文献[7]	$4\|G_1\|$	1Pa	5Pa	5Pa
本文方案	$2\|G_1\|+\|Z_q^*\|$	2Pa	3Pa	2Pa

5　结束语

因为有向签名具有不可否认性和有向验证性,所以,当被签发的消息或文件含有个人或商业的敏感信息时,有向签名可以解决此类问题. 本文中,我们提出了一种公平的基于身份的有向签名,这种签名只有指定的接收者才能验证,而且不需要验证签名的公钥证书. 另外,在签名者与验证者发生争议时,可以由可信第三方出面调停和公开验证. 通过与同类方案相比较,我们的签名的计算量较小且签名长度较短,在随机预言模型下,其安全性等价于双线性 Diffe – Hellman 问题. 因此,从接收者权利的保护及通信效率等方面来看,该方案具有广阔的应用空间.

参考文献:

[1]　孙超亮. 代理重签名研究[D]. 上海:上海交通大学,2008.

[2]　张彰,王培春. 基于离散对数的有向签名方案及其应用[J]. 西安电子科技大学学报,2002,29(4):510-512.

[3]　杜红珍. 数字签名技术的若干问题研究[D]. 北京:北京邮电大学,2009.

[4]　王永兴. 基于身份的有向签名[J]. 榆林学院学报,2005,5(5):1-3.

[5]　HESS F. Efficient identity based signature schemes based on pairings,Selected Areas in cryptography[C]. SAC 2002,Springer – Verlag,2003:310-324.

[6]　SUN X,LI Jian-hua,CHEN Gong-liang,et al. Identity – Based Directed Signature Scheme from Bilinear Pairings[EB/OL][2011 – 04 – 17]. http://eprint. iacr. org/2008/305.

[7]　ZHANG J,YANG Y,NIU Xin-xin. Efficient provable secure ID – Based directed signature scheme without random oracle[C]. Proceedings of the 6th International Symposium on Neural Networks:Advances in Neural Networks,LNCS,Vol. 5553,Springer – Verlag,2009:318-327.

(下转第 666 页)