基于身份的 Elgamal 盲签名方案及其应用

顾兆军[1,2]，刘东楠[1,2+]

（1. 中国民航大学 信息安全测评中心，天津 300300；
2. 中国民航大学 计算机科学与技术学院，天津 300300）

摘 要：为解决基于身份的盲签名中使用双线性对带来的计算复杂度问题，结合 Elgamal 算法提出一种基于身份的盲签名方案，并将盲签名方案应用于民航数据传输中。签名者对原始信息是不可见的，无法在签名中建立数学关系试图恢复。使用哈希函数处理私钥及身份信息，在随机预言模型下提了签名的安全强度，基于经典 Elgamal 算法，在数学难题中属于离散对数难题。实验结果表明，该方法能够有效抵抗密钥恢复攻击和签名伪造攻击，具备较高的安全性和运算效率，相比其它方案需要较少的模运算及指数运算。在民航数据传输领域，该方案优于其它方案。

关键词：数字签名；盲签名；Elgamal 签名；随机预言模型；民航信息系统

中图法分类号：TP393.08 **文献标识号**：A **文章编号**：1000-7024（2019）05-1201-04

doi：10.16208/j.issn1000-7024.2019.05.001

Identity based Elgamal blind signature scheme and its application

GU Zhao-jun[1,2], LIU Dong-nan[1,2+]

(1. Information Security Evaluation Center, Civil Aviation University of China, Tianjin 300300, China;
2. College of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China)

Abstract: To solve the problem of computational complexity brought by bilinear pairing in identity based blind signature, an ID-based blind signature scheme was proposed, and the blind signature scheme was applied to the field of civil aviation data transmission. The signer was not visible to the original message and the original message could not be restored through the signed message. The use of hash function to deal with both private key and the identity information was secure under the random oracle model. Based on the classical Elgamal algorithm, the problem belonged to the discrete logarithm problem. The scheme was applied in the field of civil aviation data transmission. Experimental results show that it can effectively resist key recovery attacks and signature forgery attacks. The scheme has high resistance ability to attack and it also operates efficiently. Compared with other schemes, it needs less module operation and exponential operation. The proposed scheme is better than other schemes in the civil aviation's field.

Key words: digital signature; blind signature; Elgamal signature; random oracle model; information system of civil aviation

0 引 言

在信息安全领域，人们通常使用数字签名对信息进行标识或加密，数字签名是该领域最重要的环节之一。常见的数字签名有：盲签名、群签名、环签名、属性签名、代理签名等。由于信息对签署者是可见的，会给信息传递带来一定的安全威胁，故近年来越来越多的学者致力于对盲签名的研究。

由于 Elgamal 密码体制[1]使用较少的模逆运算，具有较高的安全强度，越来越多地被人们应用在数字签名中[2,3]；Chen H 等提出一种属于离散对数难题基于身份的无证书数字签名方案[4]，但该算法较为简单；Ribarski P 等

收稿日期：2018-03-07；**修订日期**：2019-02-25

基金项目：国家自然科学基金项目（61601467、U1533104）；中央高校基本科研业务费中国民航大学专项基金项目（3122013Z008、3122013C004、3122015D025）；民航科技创新引导资金基金项目（MHRD20140205、MHRD20150233）；民航安全能力建设资金基金项目（PDSA008、AADSA0018）

作者简介：顾兆军（1966-），男，山东烟台人，博士，教授，研究方向为网络与信息安全、民航信息系统；+通讯作者：刘东楠（1991-），男，辽宁沈阳人，硕士研究生，研究方向为网络与信息安全、民航信息系统。E-mail：ne_ldn@sina.com

将盲签名与双线性技术结合提出一种签名方案[5]，该方案需要大量的模运算和指数运算；Sha 等提出一种盲签名方案[6]，并将其应用到电子支付领域中，通过实验发现，该签名并不适用于民航领域；宋敏结合双线性对技术将身份属性应用到盲签名方案中[7]；Tian M 等采取两类攻击对数字签名进行安全性验证[8]；文献 [9] 提出一种身份认证方案，并将其应用到飞机与航空公司数据传输的情景中去。

本文结合近年来基于身份数字签名的研究方案，在文献 [9] 的背景中，提出一种基于身份的 Elgamal 盲签名方案，对其安全性和运算效率进行实验分析，探究其在该领域的适用程度。

1 基础知识

1.1 数学基础

(1) 离散对数问题

定义 1 离散对数 (discrete logarithm, DL)。设 G 为由 α 生成的 q 阶循环群，$x \in Z_q^*$，$y \in G$。则满足 $g^x = y$ 的最小整数 x，为 y 基于 g 的离散对数[1]。

定义 2 离散对数问题 (discrete logarithm problem, DLP)。给定 $P, Q \in G$，找出 $n \in Z_q^*$，使得 $P = nQ$[1]。

目前，人们还没有找到求解离散对数问题的多项式时间算法，在数字签名领域中，如 Elgamal 签名和 Schnorr 签名，都是基于 DLP 数学难题的数字签名算法。

(2) 随机预言模型

定义 3 随机预言模型 (random oracle model, ROM)。随机预言模型是一种安全假设，它为信息安全的安全性证明提供了通用的框架，在 ROM 中，哈希函数为完全随机函数，即假设哈希函数能够提供完全的随机预言，该模型可以被认为理想模型与实例化模型之间的过度模型。

人们通常使用哈希函数处理信息传递的过程，如：MD4、MD5、SHA-1、SHA-2、SHA-3 等。随着研究的深入，国内学者已成功攻破 MD4、MD5 等散列算法。目前 SHA-2 及 SHA-3 尚未被攻破，故方案在实现中选取的哈希函数为 SHA-2。

1.2 经典 Elgamal 签名方案

Elgamal 数字签名方案的安全性基于有限域上的离散对数问题，签名生成过程如下：

步骤 1 系统初始化 (Setup)，p 是一个大素数，α 是 Z_p^* 的一个生成元。

步骤 2 密钥生成 (KGen)，$x \in Z_{p-1}^*$ 作为私钥，计算：$y \equiv \alpha^x \bmod p$，则公钥为：$(y, \alpha, p)$。

步骤 3 签名 (Sign)，待签名信息为 m，选择随机数 k，$k \in [0, p-1]$，$\gcd(k, p-1) = 1$。

计算：$r \equiv \alpha^k \bmod p$，根据 Fermat 定理及 Euler 定理可得，$m \equiv xr + ks \bmod (p-1)$，解出 s，(r, s) 即为信息 m 的签名。

步骤 4 验证 (Verify)，计算 $\alpha^m \equiv y^r r^s \bmod p$，若等式成立，则签名有效，若等式不成立，则签名无效。

1.3 盲签名

盲签名是一种特殊的数字签名，其形式化描述如下：信息源 (Information Source) 希望信息签署者 (Information Signer) 在不知道信息内容的前提下，对信息进行签名，而签名者恰好对信息内容不关心，只保证在将来的某个时刻证明其真实性。

在盲签名中，通常包括如下几个步骤：

步骤 1 盲化 (blind transformation)：Information Source 对信息 m 进行数学变换，变为 m'，发送给 Information Signer。

步骤 2 签名 (sign)：Information Signer 对收到的信息 m' 签名，得到 Sig(m')，发送给 Information Source。

步骤 3 脱盲 (blind reduction)：Information Source 对 Sig(m') 进行处理，还原为 Sig(m)。

步骤 4 验证 (verify)：根据签名所满足的数学特性对该签名进行验证，并以此判断签名和信息的准确性。

盲签名的一般过程如图 1 所示。

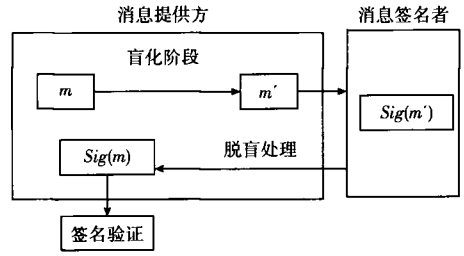

图 1 盲签名的一般过程

盲签名除具备一般数字签名所具备的性质外，还具备以下两个特性：

定义 4 盲性，即信息签署者无法掌握信息 m 的明文内容。

定义 5 不可追踪性，即信息签署者无法通过息 Sig(m') 还原 Sig(m)。

2 基于身份的 Elgamal 盲签名方案

本文基于 El-Gamal T[1] 提出的密码体制，提出一种基于身份的盲签名方案，其中，信息源对信息 m 被签名进行盲处理，签名者对盲化后的信息进行签名，签名后由信息源对已签名的信息 m' 进行脱盲处理。在签名中引入身份值 ID，通过身份值 ID 与私钥 x 的散列结合，将新散列值带入签名算法中计算，至此签名结束。使用 Elgamal 型盲签名，可有效避免双线性对运算中 Weil 对或 Tate 对的复杂运算，提升算法效率。

2.1 参数说明

在本方案中所出现的参数见表 1。

表 1　参数说明

参数	说明
p	大素数
α,β,k	随机数
x	私钥
ID	用户信息
$H_0()$	哈希函数
(y,α,p)	公钥
m	原始信息
m'	盲化后信息
(r,s)	盲化签名
(r',s')	脱盲后签名

2.2　签名方案

步骤 1　系统初始化（Setup），p 是一个大素数，α 是 Z_p^* 的一个生成元。

步骤 2　密钥生成（KGen），选取 $x \in Z_{p-1}^*$ 作为私钥，ID 为用户身份，选取哈希函数 $H_0(\ )$，计算 $d = H_0(x,ID)$，将身份信息与私钥结合，计算：$y \equiv \alpha^{H_0(x,ID)} \bmod p$，则公钥为：$(y,\alpha,p)$。

步骤 3　签名（Sign）

（1）Information Signer 选取随机数 $k \in Z_{p-1}$，计算 $r \equiv \alpha^k \bmod p$，将 r 发给 Information Source。

（2）（blind transformation）Information Source 随机选择 $\beta \in Z_{p-1}$，计算 $m' \equiv r^\beta m \bmod(p-1)$，将其发给 Information Signer。

（3）（sign）Information Signer 通过 $m' \equiv H_0(x,ID)r + ks \bmod(p-1)$ 计算得到 s，将签名 $(m',(r,s))$ 发送给 Information Source。

（4）（blind reduction）Information Source 计算：$r' \equiv r^{1-\beta} \bmod(p-1)$，$s' \equiv (1-\beta)^{-1} r^{-\beta} s \bmod(p-1)$，得到签名 $(m,(r',s'))$。

步骤 4　验证（verify）：计算 $\alpha^m \equiv y^{r'} r'^{s'} \bmod p$，若等式成立，则签名有效，若等式不成立，则签名无效。

2.3　该签名的性质

（1）盲性。Information Signer 对盲化后的信息 m' 签名后得到 (r,s)，不能还原信息 m，解决该问题等同于解决离散对数问题。

（2）不可追踪性。Information Signer 不能通过计算获得 (r,s) 以及 (r',s') 之间的联系，解决该问题同样等同于解决离散对数问题。

3　方案在民航数据传输中的应用

长期以来，盲签名技术被应用于电子投票系统和电子商务中，本文将提出的盲签名方案应用于机载天线与廊桥接入点进行业务数据传输中，下面对该签名的应用进行描述：

定义 6　ATB（Antenna to Bridge）传输过程，即飞机利用机载天线和廊桥接入点间建立的 802.11 无线网络传输关键数据的过程，该关键数据包括电子飞行包等飞行业务数据。

目前大量航空公司采用 GateLink 和人工拷贝的方式传输业务数据，详见文献 [9]，为了提高数据传输的效率和业务数据在传输过程中的安全性，国内部分航空公司已经通过 ATB 进行业务数据传输，对该过程的研究正处于起步阶段。

在本文的方案中，信息签署者为飞行员或航电工程师等航务工作者，信息源为航空公司。航务工作者对待传输数据（电子飞行包等关键数据）签名后通过 ATB 将数据传回至航空公司，在签名过程中，航务工作者对数据的内容是“不可见的”，该过程网络拓扑结构以及应用流程如图 2、图 3 所示。

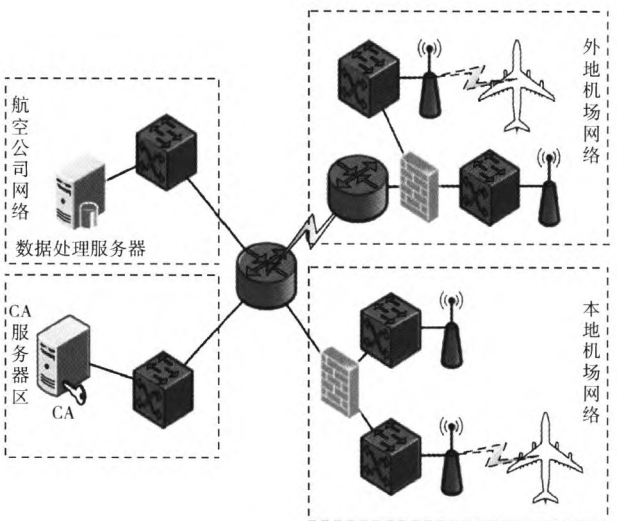

图 2　ATB 数据传输网络拓扑

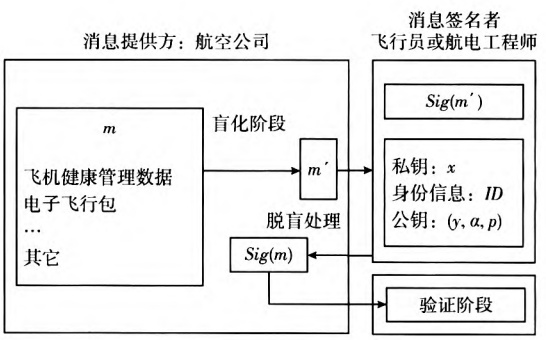

图 3　盲签名应用流程

4 实验仿真及安全性分析

4.1 常见攻击

文献［8］和文献［10］提出了对于 Elgamal 签名的常见攻击，经典 Elgamal 签名可以有效抵抗密钥恢复攻击和签名伪造攻击，本文依据文献［8］和文献［10］所提出的攻击方案对提出的盲签名方案进行模拟攻击，经仿真实验及数学证明，本文提出的方案可有效抵抗下述 4 类攻击。

攻击 1：攻击者使用 i 个信息 $m_1,m_2,\cdots,m_l$，及其相应的签名 $\{(r_i,s_i);i=1,2,\cdots l\}$，欲使用 $m'\equiv H_0(x,ID)r+ks \bmod(p-1)$ 构建 l 个等式建立数学关系计算 x 和 k。在本方案中，攻击者没有足够的条件恢复 x，因为即使存在 l 个方程，未知数个数为 $l+1$，且未知数存在于哈希函数中，所以该攻击在随机预言模型下是无效的。

攻击 2：攻击者尝试通过 $\alpha^m\equiv y^{r'}r'^{s'} \bmod p$ 解出 x。

$\because r'\equiv r^{1-\beta} \bmod(p-1)$，

$s'\equiv(1-\beta)^{-1}r^{-\beta}s \bmod(p-1)$，

$y\equiv\alpha^{H_0(x,ID)} \bmod p$

$\therefore \alpha^m\equiv\alpha^{H_0(x,ID)r'}\alpha^{s(1-\beta)} \bmod p$

由上式可知，x 与 β 均出现在等式中的指数位置，解决此问题等同于解决 $GF(P)$ 上的离散对数问题，故攻击无效。

攻击 3：攻击者尝试在未知数 $\{k_i,i=1,2,\cdots,l\}$ 之间建立线性依赖关系。

若 $k_i\equiv ck_j \bmod(p-1)$，则 $r_i\equiv r_j^c \bmod p$，若 c 可计算，则求解 k 是简单的，由于 c 也出现在等式中的指数位置，解决该问题仍等同于解决 $GF(P)$ 上的离散对数问题，故此攻击无效。

攻击 4：伪造者想找出满足方程 $\alpha^m\equiv y^{r'}r'^{s'} \bmod p$ 的数字签名 (r',s')。

$\because r'\equiv r^{1-\beta} \bmod(p-1)$，$r\equiv\alpha^k \bmod p$

$\therefore r'\equiv\alpha^{j(1-\beta)} \bmod(p-1)$

同理可得，$s'\equiv(1-\beta)\alpha^{-j\beta} \bmod(p-1)$。

该问题首先等同于解决等式中 r' 和 s'。若伪造者确定 r'，j 是随机值，计算 s' 等同于解决 $GF(P)$ 上的离散对数问题；若伪造者首先确定 s'，理论上 r' 可由 $y^{r'}r'^{s'}\equiv A \bmod p$ 计算出，经计算可知该方程在多项式时间内无解，故攻击无效。

4.2 实验及方案对比

本文将提出的盲签名方案应用到图 2 所示的面向 ATB 数据传输的原型系统中，对其进行安全性分析，即模拟上节所讨论的 4 类攻击，在安全性即效率两个维度与近年来同类研究进行比较分析，实验结果见表 2。其中，E_m 为模运算次数、E_e 为指数运算次数、E_H 为哈希函数运算次数、E_p 为协议交互次数，分析结果见表 3。

表 2 盲签名安全性分析

	文献[11]	文献[12]	文献[13]	本文方案
*attack*1	*No*	*Yes*	*No*	*Yes*
*attack*2	*Yes*	*No*	*Yes*	*Yes*
*attack*3	*Yes*	*Yes*	*Yes*	*Yes*
*attack*4	*Yes*	*Yes*	*Yes*	*Yes*

表 3 盲签名效率分析

方案	算法效率
文献[11]	$8E_m+6E_e+1E_H+5E_p$
文献[12]	$10E_m+9E_e+2E_H+7E_p$
文献[13]	$8E_m+7E_e+0E_H+4E_p$
本文方案	$7E_m+6E_e+1E_H+3E_p$

实验分析表明：

（1）提出的签名能够有效抵御密钥恢复攻击和签名伪造攻击，安全性明显高于文献［11-13］的方案；

（2）本文提出的方案的运算效率方面，相比其它方案占据较少的系统资源，需要较少的模运算、指数运算以及较少的两方交互。与此同时，哈希函数的使用还能提高安全性。

综上所述，本文提出的方案更优于其它方案应用于民航领域中，即 ATB 传输过程。

5 结束语

本文结合经典 Elgamal 签名以及盲签名思想，提出一种基于身份的 Elgamal 盲签名技术，使用经典 Elgamal 算法解决了传统基于身份的数字签名中双线性对运算的复杂性，减少了签名计算过程中的模运算和指数运算，在签名中引入哈希函数，在随机预言模型下提高了签名的抗攻击能力。将该方案应用到 ATB 模拟系统中进行仿真，突破了盲签名应用于电子投票系统的瓶颈，实验结果表明，该方案能够有效抵抗密钥恢复攻击和签名伪造攻击，相比其它算法占用较少的系统资源，更适用于民航领域。

参考文献：

[1] El-Gamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms [J]. IEEE Transactions on Information Theory, 1985, 31 (4): 469-472.

[2] Khadir O. Insecure primitive elements in an ElGamal signature protocol [J]. Journal of Discrete Mathematical Sciences & Cryptography, 2015, 18 (3): 237-245.

[3] Mohit P, Biswas GP. Design of ElGamal PKC for encryption of large messages [C] //International Conference on Computing for Sustainable Global Development. IEEE, 2015: 699-703.

（下转第 1209 页）

[2] ZHANG Yuqing, WANG Xiaofei, LIU Xuefeng, et al. Overview of cloud computing environment security [J]. Journal of Software, 2016, 27 (6): 1328-1348 (in Chinese). [张玉清, 王晓菲, 刘雪峰, 等. 云计算环境安全综述 [J]. 软件学报, 2016, 27 (6): 1328-1348.]

[3] LIU Mingjie, WANG An. Research on the dynamic and application of fully homomorphic encryption [J]. Journal of Computer Research and Development, 2014, 51 (12): 2593-2603 (in Chinese). [刘明洁, 王安. 全同态加密研究动态及其应用概述 [J]. 计算机研究与发展, 2014, 51 (12): 2593-2603.]

[4] Peikert C, Shiehian S. Multi-key FHE from LWE [R]. Berlin Heidelberg: Springer, 2016: 217-238.

[5] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) Fully homomorphic encryption without bootstrapping [R]. New York: ACM Press, 2012: 309-325.

[6] Biasse J, Ruiz L. FHEW with efficient multibit bootstrapping [R]. Guadalajara: Springer, 2015: 119-135.

[7] Brakerski Z, Perlman R. Lattice-based fully dynamic multi-key FHE with short ciphertexts [R]. Santa Barbara: Springer, 2016: 190-213.

[8] Genry C, Sahai A, Water B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based [R]. Berlin: Springer, 2013: 75-92.

[9] Ducas L. FHEW: Bootstrapping homomorphic encryption in less than a second [R]. Berlin: Springer, 2015: 617-640.

[10] Chillotti I, Gama N. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds [R]. Berlin Heidelberg: Springer, 2016: 3-33.

[11] Cheon J, Han K, Kim D. Faster bootstrapping of FHE over the integers [DB/OL]. https://eprint.iacr.org/2017/079.pdf, 2017.

[12] Douglas R Stnson. Cryptography theory and practice [M]. FENG Dengguo, transl. Beijing: Electronic Industry Press, 2008: 184-215 (in Chinese). [Douglas R Stnson. 密码学原理与实践 [M]. 冯登国, 译. 北京: 电子工业出版社, 2008: 184-215.]

(上接第 1204 页)

[4] Chen H, Zhang L, Xie J, et al. New efficient certificateless blind signature scheme [C] // Trustcom/Bigdatase/Ispa. IEEE, 2017: 349-353.

[5] Ribarski P, Antovski L. Comparison of ID-based blind signatures from pairings for e-voting protocols [C] //International Convention on Information and Communication Technology, Electronics and Microelectronics. IEEE, 2014: 1394-1399.

[6] Sha LM, Yang SZ. An online e-payment system applying to auto insurance based on proxy blind signature [J]. Applied Mechanics & Materials, 2014, 644-650: 2776-2783.

[7] SONG Min. Research on theory and application of blind signature [D]. Jinan: Shandong University, 2013 (in Chinese). [宋敏. 盲签名技术理论及应用研究 [D]. 济南: 山东大学, 2013.]

[8] Tian M, Zhu Y, Chen Z. Two simple attacks on a blind signature scheme [J]. International Journal of Network Security, 2014, 16 (6): 498-500.

[9] GU Zhaojun, LIU Dongnan. ECC identity authentication scheme between aircraft and passenger boarding bridges [J]. Journal of Chinese Computer Systems, 2019, 40 (1): 98-103 (in Chinese). [顾兆军, 刘东楠. 一种面向廊桥 AP 的 ECC 身份认证方案 [J]. 小型微型计算机系统, 2019, 40 (1): 98-103.]

[10] Vahini K, Prasad V, Chandra Sekhar UV. Defend data using ELGAMAL digital signature data decryption algorithm [J]. International Journal of Computer Science & Information Technology, 2014, 5 (4): 5062-5067.

[11] Ali M. An organizational signature schemes based on ElGamal signature [J]. International Journal of Information Systems, 2016, 10: 6-9.

[12] CAO Ye. Security analysis and improvement of ElGamal digital signature scheme [J]. Journal of Shenyang Ligong University, 2015, 34 (3): 32-36 (in Chinese). [曹烨. ElGamal 数字签名方案的安全性分析及改进 [J]. 沈阳理工大学学报, 2015, 34 (3): 32-36.]

[13] Chen CL, Chen YY, Jan JK, et al. A secure anonymous e-voting system based on discrete logarithm problem [J]. Applied Mathematics & Information Sciences, 2014, 8 (5): 2571-2578.