一种基于群签名的有效电子现金模型

王大星[1],滕济凯[2]
(1. 滁州学院 数学系 信息与计算科学研究所,安徽 滁州 239012;
2. 中国科学院 软件研究所,北京 100190)

摘 要:电子商务正在以爆炸性的速度发展,其最终目标是实现商务活动各环节的电子化。但是真正进行电子支付、开展电子交易的仍然比较少,电子商务的一个核心问题是支付问题,如何安全、公平并且保护用户隐私的电子交易是决定电子商务发展的关键问题。解决这些问题的关键技术就是电子现金技术,当前电子现金系统的运行效率一直是倍受关注的问题。利用一种基于RSA安全参数的群签名,构造了一个新的电子现金模型,该模型消除了一般方案中复杂的取款协议运算,并且为用户提供了匿名性和不可追踪性。经分析,本方案降低了软硬件实现的系统开销,特别适合当前电子商务安全、高效、便捷和实时交互反应的发展趋势。

关键词:群签名;电子现金;匿名性;合谋攻击
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2009)10-0174-03

An Efficient Electronic Cash Model Based on Group Signature

WANG Da-xing[1], TENG Ji-kai[2]
(1. Inst. of Info. and Computing Sci., Dept. of Mathematics, Chuzhou Univ., Chuzhou 239012, China;
2. Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

Abstract: E-commerce system is now developing at an enormous speed, whose final objective is to electrize every phase of commercial activity. But the real electronic transactions in which the payments are initiated online are very few. Electronic payment is the core of E-commerce. How to achieve safe and fair electronic transactions as well as not reveal the intimacy of customers is the key to the development of electronic-commerce. The operating effiency of electronic cash is closely watched currently. A new E-cash model is designed by a group signature based on RSA- variant which eliminates the withdrawal phase of general model and to provide users with anonymity and untracebility. Further analyses also justify the scheme reduced the hardware and software systems' cost, particularly for the current E-commerce security, with efficient and convenient and real-time interactive response to the trend.

Key words: group signature; electronic cash; anonymity; collusion-attack

0 引 言

电子商务就是通过Internet网所进行的商务活动,对电子商务一个关键的要求就是要有一个安全高效的电子支付系统。电子现金是一种非常重要的电子支付系统,它可以看作是现实纸币的数字模拟,但比前者更方便、经济。它的最简单的形式包括三个主体,四个协议过程:顾客、商家、银行,开户协议、取款协议、支付协议、存款协议。1982年D. Chaum提出了第一个电子现金系统[1],之后的电子现金系统经历了由完全匿名到条件匿名,由在线到离线,由不可分到可分的日趋完善。由于群签名自身具有匿名控制功能,因此利用群签名设计公平电子现金方案具有很大的优势。同时群签名又是设计多银行电子现金系统的重要工具,因此群签名在电子现金中有着广泛的应用。人们利用群签名设计了许多电子现金系统[2]。然而已有的利用群签名设计的电子现金系统效率大都较低,主要表现在:数字签名太长、计算量太大,或者取款协议中顾客和银行交互太多等等。因此利用群签名设计高效安全的电子现金系统仍是电子现金领域的热点问题。文中的主要工作是利用一个已有的可证安全的群签名方案设计了一个高效的电子现金模型。

近年来利用群签名设计了许多电子现金系统。但是这些基于群签名的现金系统存在以下问题:

1)所基于的群签名是不安全的[3];

2)不具有匿名控制功能[4];

收稿日期:2009-02-24;**修回日期**:2009-05-07
基金项目:滁州学院科研基金资助项目(2008kj011B)
作者简介:王大星(1980-),男,讲师,硕士,研究方向为密码学与信息安全;滕济凯,博士,研究方向为密码学与通信安全技术。

3)效率不高,例如取款协议太复杂[4,5]。

笔者利用群签名[6]构造了一个新的电子现金系统,更好地解决了以上三个问题。

新系统满足:

(1)可以实现匿名控制,具有现金追踪和现金所有者追踪的功能;

(2)消除了一般方案中复杂的取款协议运算,群成员用户可以自己产生电子现金,效率更高;

(3)证明了新系统满足匿名性和不可伪造性等。

1 群签名简介

群数字签名是由 D. Chaum 和 E. VanHeist 于 1991 年首先提出[7]。它是一种特殊类型数字签名。

群数字签名允许一个群组的任何一个成员,代表群组对消息作数字签名。任何拥有群组公钥的人,都可以验证群数字签名的有效性。群数字签名隐藏了签名者的身份(即匿名性),群组中有一个指定的群主管,在必要时,群主管可"打开"群数字签名,计算并证明出签名者的群成员身份。任何人,包括群主管,都不能诬陷某个群成员对某消息作过签名。除群主管外,任何人要想判定多个群数字签名是否是由同一个群成员所签,在计算上是不可行的(即不可联系性)。

1.1 群签名的定义

一个群数字签名方案是由以下五个过程组成的数字签名方案:

1)设置(Setup):输入安全参数 1^k,输出初始的群公钥(包括所有的系统参数)以及群主管的秘密钥的概率多项式时间的算法。

2)加入(Join):用户和群主管之间的交互协议,使得用户成为新的群成员用户输入其私钥和公钥,得到群成员证书。

3)签名(Sign):输入群公钥、群成员证书、群成员私钥以及消息 m,输出对 m 的群数字签名的概率多项式时间算法。

4)验证(Verify):输入群数字签名的消息签名对,根据群公钥判断该签名是否是对该消息的有效群签名,若有效,则输出真(True),否则输出假 (False)的概率多项式时间的算法。

5)打开(Open):输入有效的群数字签名的消息签名对、群公钥、群主管的秘密钥,输出群签名的群成员的身份,以及这个事实的证明的概率多项式时间的算法。

1.2 群签名的性质

群数字签名的效率群公钥的大小,群签名的长度以及 Sign, Verify, Setup, Open 和 Join 的效率有关,一个安全的群数字签名必须满足如下的性质:

1) 正确性(Correctness):由群成员使用 Sign 产生的群签名,必须为 Verify 所接受;

2) 不可伪造性(Unforgeability): 只有群成员才能够代表群组,产生群数字签名;

3) 匿名性(Anonymity):给定对某消息的有效群数字签名,除了群主管之外,任何人要识别出签名者的身份在计算上是困难的;

4) 不可关联性 (Unlinkability): 除群主管外,任何人要确定两个有效的群数字签名是否源自同一群成员所签,在计算上是困难的;

5) 可开脱性 (Exculpability):群主管和群成员都不能代表另一个群成员产生出有效的群数字签名。这就使得群成员不必为不是由他产生的群数字签名担负责任;

6) 可跟踪性(Traceability): 群主管总能打开有效的群数字签名,从而识别出签名者的真实身份;

7) 防合谋(Coalition - Resistance):群成员的合谋子集(甚至整个群组)不能产生一个这样的有效群签名,使得群主管不能将该群签名和其中一个群成 员的身份联系起来。

群数字签名的匿名性、可跟踪性、不可伪造性、不可联系性以及防合谋攻击性,使得群数字签名在电子商务中具有广泛的应用,譬如互联网中群组信息的匿名发布;电子货币的匿名发行(所有的电子货币发行银行构成群组);匿名的电子投票选举;网上投标等等。

2 基于群签名的电子现金模型

以下给出的方案基于群签名[5],其中涉及到的协议参与者有用户 U,银行 B,可信第三方 T。

2.1 参数的生成

银行 B 选择随机选择两个安全参数:大素数 p, q,使得 $p = 2p' + 1, q = 2q' + 1$,而 p', q' 也为素数;银行公开 $n = pq$,而秘密保存 p, q,然后定义一个子群 $< g >= G \subset Z_n^*$,选择 $z, h \in_R G$。

可信第三方 T 选择秘密密钥 x,计算公钥 $y = g^x$,并公开一个碰撞自由的哈希函数 H。

2.2 开户协议

用户 U 可以在任何一家有发行电子现金权利的银行 B 开户,存入一笔现金。随机选择两个素数 e, e_n,计算 $e_m = ee_n, z_m = z^{e_n}$。银行计算 $u = z_m^{1/e_m}$,并发送 u 给用户,用户检查 $z = u^e$。银行在顾客的数据库中存储 (u, e_m, z_m) 和用户 U 的身份,用户 U 保存 (u, e) 作为其成员密钥。

2.3 支付协议

当用户 U 与商家 S 在网上交易时，他将用自己的成员密钥为商家签发交易信息，包括商家的身份信息 ShopID，支付的金额，货币信息等。而商家则用银行发送给他的公钥进行验证，验证通过就表明本次支付信息有效，接受用户的电子现金。

具体的协议执行过程如下：

Step1. 商家首先生成一个交易信息 m 发送给用户：$m = H(\text{ShopID}, \text{Date}, \text{Time}, \text{Amount}, \text{Current})$

Step2. 用户选择一个整数 w，并计算：$a = g^w$，$b = uy^w$ 和 $d = g^e h^w$；

Step3. 用户选择 r_1, r_2, r_3，并计算：$t_1 = b^{r_1}(1/y)^{r_2}$，$t_2 = a^{r_1}(1/g)^{r_2}$，$t_3 = g^{r_3}$，$t_4 = g^{r_1}h^{r_3}$，然后计算：$c = H(g \| h \| y \| z \| a \| b \| d \| t_1 \| t_2 \| t_3 \| t_4 \| m)$，$s_1 = r_1 - c(e - 2^{l_1})$，$s_2 = r_2 - cew$，$s_3 = r_3 - cw$；

Step4. 交易信息 m 的签名就是：$(c, s_1, s_2, s_3, a, b, d)$，用户将该签名发送给商家，则该签名就是用户在此次交易中支付给商家的电子现金；

Step5. 商家收到电子现金后，验证下列等式是否成立，即可决定是否接受该电子现金：

$$c = H(g \| h \| y \| z \| a \| b \| d \| z^c b^{s_1 - c2^{l_1}} / y^{s_2} \| a^{s_1 - c2^{l_1}} / g^{s_2} \| a^c g^{s_3} \| d^c g^{s_1 - c2^{l_1}} h^{s_3} \| m);$$

命题 1. 如果用户 U 和商家 S 正确地执行上述支付协议，则 Step5 中的等式成立，也即此次用户支付的电子现金有效。

证明：比较支付协议中 Step3 和 Step5 中的哈希函数 H 的输入（比特串的连接），可以发现下面 4 个等式成立：

1) $z^c b^{s_1 - c2^{l_1}} / y^{s_2} = z^c b^{r_1 - \alpha e} y^{-s_2} = z^c b^{r_1 - \alpha e} y^{\alpha ew - r_2} = z^c b^{-\alpha e} y^{\alpha ew} b^{r_1} y^{-r_2} = u^{\alpha e}(uy^w)^{-\alpha e} y^{\alpha ew} b^{r_1} y^{-r_2} = b^{r_1} y^{-r_2} = t_1$；

2) $a^{s_1 - c2^{l_1}} / g^{s_2} = a^{r_1 - \alpha e} g^{\alpha ew - r_2} = g^{wr_1 - w\alpha e} g^{\alpha ew - r_2} = g^{wr_1 - r_2} = a^{r_1} g^{-r_2} = t_2$；

3) $a^c g^{s_3} = g^{wc} g^{r_3 - cw} = g^{r_3} = t_3$；

4) $d^c g^{s_1 - c2^{l_1}} h^{s_3} = g^{\alpha e} h^{wc} g^{r_1 - \alpha e} h^{r_3 - cw} = g^{r_1} h^{r_3} = t_4$。

因此，所证的命题成立。

2.4 存款协议

在任何合适的时间，商家 S 发送其收到的电子现金到可信第三方 T，T 验证签名的正确性，并计算用户的身份码 $u' = b/a^x$，接着定期将存款信息和 u' 发送给银行 B，银行知道用户 U 的真正身份信息和身份码 u' 之间的联系。这样就可以正确地从用户 U 的帐户中扣除相应的金额到商家 S 的帐户中。

3 安全性分析

3.1 匿名性和非法用户的身份识别

由支付协议的过程知，要确定一份电子现金的拥有者，即支付信息的签名者的真正身份，需要验证等式：$\log_g a = \log_y (b/b')$。但是在决定性 Diffi - Hellman(DDH) 假设下，如果没有可信第三方 T 的密钥，这在计算上是困难的。一旦用户有非法行为（如超额支付或重复花费），可信第三方 T 将和银行 B 追踪到用户的支付信息，因为这时用户的身份和支付信息是可以联系起来的。

3.2 不可伪造性

由开户协议和支付协议知，仅仅只有用户 U 才能用其成员密钥签发电子现金。

3.3 无关联性

要决定两份电子现金 $(c, s_1, s_2, s_3, a, b, d)$ 和 $(c', s'_1, s'_2, s'_3, a', b', d')$ 是否来自同一个用户 U，需要验证等式：$\log_y (a/a') = \log_y (b/b') = \log_y (d/d')$。但是在 DDH 假设下，这在计算上是无法达到的。

3.4 无欺诈性

由以上分析可知，因除了电子现金拥有者 U，任何人不能解决离散对数问题 $\log_u z$，因此，即使银行 B 和可信第三方 T 合谋，也不能假冒 U 签发电子现金。

4 结束语

利用一种群签名方案结合电子现金基本模型，构造了一个高效的电子现金方案。该方案简化了已有电子现金模型，使得用户避免了在取款协议中所要进行的交互运算，大大提高了取款效率，方便了用户的使用。然而，在该模型下如何避免可信第三方 T 的欺骗行为，以及电子现金的可转移性研究等，仍需进一步研究。

参考文献：

[1] Chaum D, Fiat A, Naor M. Untraceable Electronic Cash[C] //Advances in Cryptology - CRPTO' s 88 Proceedings. [s. l.]: Springer - verlag, 1988: 319 - 327.

[2] 徐 明，张祥德. 一个基于群签名的电子钱包的应用方案[J]. 计算机技术与发展，2008，18(4)：134 - 136.

[3] Chen X, Zhang F, Wang Y. A New Approach to Prevent Blackmailing in E - Cash[EB/OL]. 2003. Cryptology ePrint Archive, Report 2003/055, availing at http://eprint.iacr.org/2003/055/.

[4] Tseng Y M, Jan J K. Improved Group Signature Scheme Based on Discrete Logarithm Problem[J]. Electronics Letters, 1999, 35(16): 1324 - 1325.

（下转第 192 页）

模拟 2:在 Walker 星座卫星网仿真平台进行模拟,以 Courier 星座为网络模型,轨道高度 800 千米,8 个轨道平面,每个轨道平面有 9 颗卫星,倾斜角 84.7 度(如图 5 所示)。

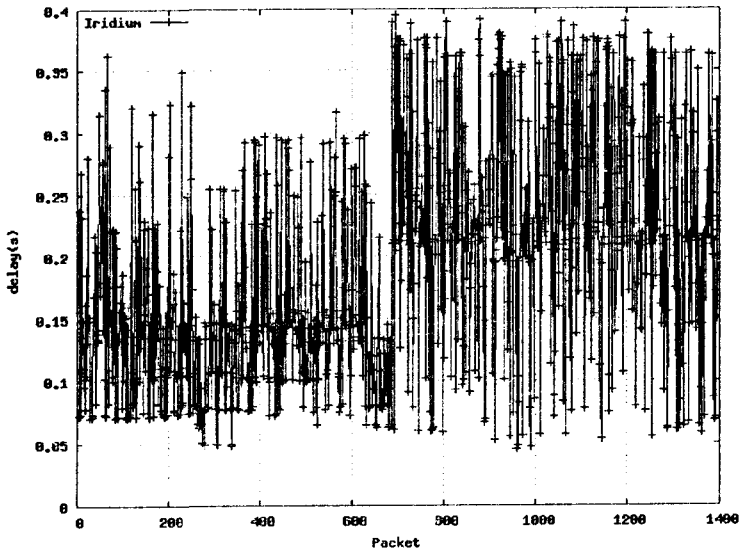

图 4 Iridium 星座

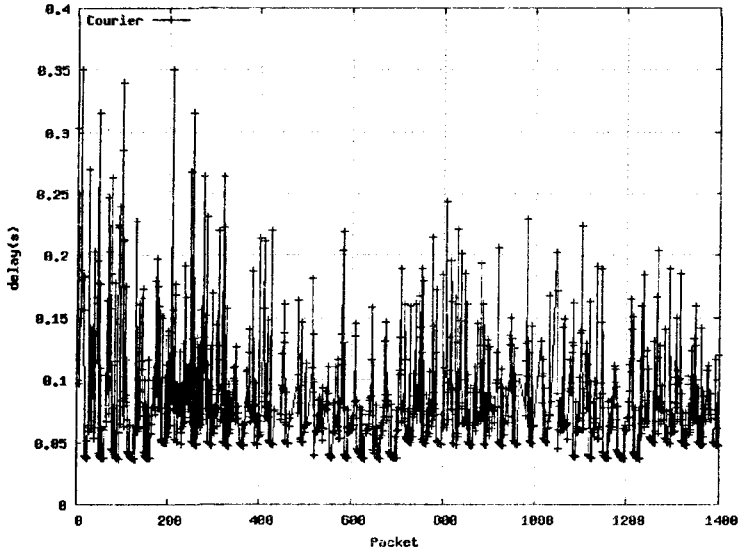

图 5 Courier 星座

实验结果分析:由上面实验可以看到,Walker 星座由于不存在星间切换,因此对于同一个算法来说,Walker 星座在分组时延的大小、时延的抖动方面明显优于极地星座。

4 结束语

NS2 源代码开放,实验结果分析方便,有较好的稳定性,而且能方便地扩展功能模块,适合很多卫星网路由协议的仿真。文中介绍了 Walker 星座卫星网络仿真平台的构造,并对其进行了一定的改进,同时分析了 NS2 中进行卫星网仿真的方法,对利用 NS2 进行测试和评价 Walker 星座卫星网络的性能有一定的帮助。

参考文献:

[1] Ekici E, Akyildiz I F, Bender M D. A Distributed Routing Algorithm for Datagram Traffic in LEO Satellite Networks[J]. IEEE/ACM Trans. Net.,2001,9(2):137-147.

[2] 刘兼唐,赵 敏.基于 ObjectAgent 的小卫星星务系统研究与仿真[J].计算机技术与发展,2007,17(4):140-143.

[3] 王 鹏,白建军,卢泽新.卫星网络协议的仿真与模拟技术研究[J].计算机工程与科学,2004,26(5):4-6.

[4] Walker J G. Continuous Whole Earth Coverage by Circular Orbit Satellite Patterns[R]. Royal Aircraft Establishment. Technical Report 77044 (UDC 629.195:527),1977.

[5] 黄筱俊,郑善贤.基于 NS 的移动网络仿真研究[J].微机发展(现更名:计算机技术与发展),2004,14(5):27-29.

[6] 徐雷鸣,庞 博,赵 耀.NS 与网络模拟[M].北京:人民邮电出版社,2003.

[7] 杨玉华,刘培宁,刘际炜,等. NS-2 的仿真模拟技术分析[J].计算机工程,2005,31(15):110-111.

[8] 李向丽,李 磊,陈 静.网络实验仿真与网络技术实践[J].计算机技术与发展,2006,16(3):74-76.

[9] Henderson T R, Katz R H. Network Simulation for LEO Satellite Networks[C]// In: Proceeding of 18th International Communication Satellite Systems Conference. Oakland, CA:[s.n.], 2000.

[10] Brunt P. IRIDIUM: Overview and Status[J]. Space Commun.,1996,14(2):61-68.

(上接第 176 页)

[5] Canard S, Gouget A, Traor J. Improvement of Efficiency in (Unconditional) Transferable E-Cash[C]// Mexico, In Financial Cryptography and Data Security'08, volume 4887 of LNCS. [s.l.]:Springer, 2008:571-589.

[6] Camenisch J, Michels M. A Group Signature Scheme with Improved Eifficiency[C] // Advances in Cryptology ASIACRYPT'98, Lecture Notes in Computer Science. [s.l.]: Springer-Verlag, 1998:160-174.

[7] Feige U, Lapidot D, Shamir A. Multiple non-interactive zero-knowledge proofs under general assumptions[J]. SIAM Journal on Computing,1999,29(1):1-28.