# 基于代理的多方公平交换签名方案

任双廷,王 箭
(南京航空航天大学 计算机科学与技术学院,江苏 南京 210016)

**摘 要**:在公平交换方案中,允许两个或者多个参与者以一种公平的方式进行信息交换。所谓公平是指:所有参与者都能得到所要交换的信息,或者所有参与者都无法得到所要交换的信息。提出一种基于代理的多方公平交换签名方案。在该方案中,参与者首先以一种公平的方式进行授权交换,一旦授权交换成功,则每个参与者可以代表其他参与者对指定的文件进行代理多签名,从而公平地实现了多方公平交换签名中每个参与者对其他参与者的约束,以及实现了多方公平交换签名。相对于其他的多方公平交换方案,该方案的原理既可应用于一对多类型的多方公平交换签名方案,也可应用于多对多类型的多方公平交换签名方案。此外,该多签名的公平交换并不依赖于可信或半可信的第三方,从而消除了公平交换签名的应用瓶颈。

**关键词**:代理;多方公平;公平交换;授权
**中图分类号**:TP301 **文献标识码**:A **文章编号**:1673-629X(2017)01-0080-04
doi:10.3969/j.issn.1673-629X.2017.01.

# Proxy-based Multi-party Fair Exchange Signature Scheme

REN Shuang-ting, WANG Jian
(College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

**Abstract**: A multi-party fair exchange protocol allows parties to exchange items in a fair way, which means that all of the parties obtain the other's items or neither party does. A novel protocol for multi-party fair exchanging signature without a Trusted Third Party (TTP) is proposed. In this protocol, participants exchange their warrants firstly. Then, each participant is able to sign a proxy multi-signature on behalf of its opponents. Owing to the proxy multi-signature's characteristics, the scheme achieves the desired effect of multi-party fair exchange of digital signatures. Besides, the principle of it can be used at both 1-to-n and n-to-n multi-party fair exchange signature protocols. Differing from existing fair exchange schemes, the scheme can be realized without the use of a TTP, which makes it more practical.

**Key words**: proxy; fair multi-party; fair exchange; warrant

## 1 概 述

1996 年,N. Asokan 等首先对多方公平交换协议进行了研究[1],此后,多方公平交换协议的研究受到了国内外学者的广泛关注。针对应用场景的不同,多方公平交换协议又可以分为两类,即一对多的公平交换协议[2-6]和多对多的公平交换协议[7-13]。此外,多方公平交换协议和两方公平交换协议比较类似,又可根据是否使用第三方分为三类,即不带可信第三方的多方公平交换协议、在线可信第三方的公平交换协议以及离线可信第三方的公平交换协议。1996 年,N. Asokan 在原有两方公平交换方案的基础上再次给出了多方公平交换的概念[14],方案允许多个参与者公平地交换电子信息。与两方公平交换协议类似:不带可信第三方的多方公平交换协议难以实现真正的公平,而在使用第三方的多方公平交换协议中,协议的安全性又过于依赖可信第三方的安全性。一旦可信第三方出现安全问题,整个协议都将失去其应有的价值,也就是说,可信第三方的使用成为制约多方公平交换协议应用的瓶颈[15-17]。针对这一问题,又有一些学者提出了半可信第三方的概念[10-12],但仍然未能很好地解决可信第三

**收稿日期**:2014-12-03 **修回日期**:2015-06-18 **网络出版时间**:2017-01-04
**基金项目**:江苏省普通高校研究生科研创新计划资助项目(CXZZ12_0161);中央高校基本科研业务费专项资金;江苏省高校优势学科建设工程资助项目
**作者简介**:任双廷(1988-),男,硕士生,研究方向为信息安全等;王 箭,教授,研究方向为信息安全等。
**网络出版地址**:http://www.cnki.net/kcms/detail/61.1450.TP.20170104.1017.002.html

方的问题。

代理签名最早由 Mambo 等在 1996 年提出[18],是指:在一个签名方案中,原始签名人通过代理权限的授予,使得代理签名人具有代表原始签名人进行签名的权力,即,允许原始签名人将自身的签名权力委托给代理签名人。有时人们需要一个代理人同时代表若干个原始签名人进行签名,这就是代理多签名体制[19-25]。

文中提出一种基于代理的多方公平交换签名协议。在该协议中,每个参与者首先与其他参与者交换他们的授权,一旦授权交换成功,参与者就可以依据所获得的授权进行代理签名,从而代替其他参与者对某一指定文件进行代理多签名。最终,每个参与者能得到对其他参与者具有约束效力的签名。相对于已提出的公平交换签名协议,所提方案不需要用到可信第三方,而且可以实现签名的多方公平交换。

## 2　前提知识

### 2.1　符号介绍

$i$:序号为 $i$ 的参与者。

PB:一个用于展示消息的公共平台,可以被看作如同网络般的一个公共环境而不是可信第三方。

$W_{ij}$:由 $i$ 制作的将要发送给 $j$ 的授权。

$V_{ij}$:参与者 $i$ 的一般签名,$j$ 为 $i$ 所发送授权的接收方。在这里,文中并没有指定特殊的签名方案,在实践中,要求所选择的签名方案都能被参与者双方所接受。

$E_{\mathrm{PK\_abolish}}$:用公钥 PK 对某一数据进行加密后得到的密文。在实践中,所选择的加密方案必须是参与者双方都能够接受的。

$\mathrm{PMV}_i$:由 $i$ 所制作的代理多签名。文中并没有给出确切的代理签名方案,在实践中,应该由参与者共同协商决定。

$V_{i\_\mathrm{abolish}}$:$i$ 所制作的一般签名。

### 2.2　假　设

公平:在 $n$ 个参与者中,要么所有参与者都能制作出对其他 $n-1$ 个参与者具有约束力的代理多签名;要么所有参与者都不能得到对其他参与者具有约束力的代理多签名。

## 3　基于授权的多方公平交换签名方案

### 3.1　简　述

所提方案原理为:首先,每个参与者都制作 $n-1$ 个授权,并将它们发送给相应的其他参与者,以期实现授权的多方公平交换。交换成功则执行下一步,即,所有参与者使用来自其他参与者的授权代表其他参与者制作具有约束力的代理签名;交换不成功,则所有参与者所得到的授权将在生效前被撤销,任何人都无法据此得到对其他参与者具有约束力的代理多签名,从而实现了签名的多方公平交换。



### 3.2　对授权的多方公平交换的分类

由于所提方案是以授权的公平交换为基础的,所以对授权的交换公平性及应对方略进行如下分类。

(1)所有参与者都是诚实的,则他们能够实现对授权的公平交换;

(2)参与者中的某一个是不诚实的,则所有参与者所得到的授权都将在生效前被撤销;

(3)多个参与者是不诚实的,此种情况可以归类到 2 当中。

从以上分类可知:如果所有参与者都能实现授权的公平交换,他们就可以使用得到的授权代表其他参与者制作具有约束效力的代理多签名,否则,所有授权都将在生效前被撤销,任何人都无法从中得到对其他人具有约束力的代理多签名,从而达到公平交换签名的效果。

### 3.3　定　义

该方案中具有两类实体参与者 $i$ 和公告牌 PB 。

定义:该方案是一个元组(Init, Authorization, Authorization Verifying, Proxy Multi-Signature, Recovery)。

(1) Init(初始化):算法输入安全参数 $1^k$ ($k \in N$),产生系统公共参数 params 。

(2) Authorization(授权发送):参与者制作 $n-1$ 个授权 $(W_{i1}, V_{i1}), \cdots, (W_{i(n-1)}, V_{i(n-1)})$,并分发给其他相应的参与者。

(3) Authorization Verifying(授权验证):参与者对所有接收到的授权进行验证,一旦出现验证不成立的情况,则分以下两种情况进行处理:还未发送自己制作的授权,则终止协议;已发送自己制作的授权,则启动恢复协议。

(4) Recovery(恢复):算法发送警报消息到 PB ,撤销所有已交换授权的有效性。

(5) Proxy Multi-Signature(代理多签名):每个参与者使用已得到的合法授权代表其他参与者行使签名权,产生对其他参与者具有约束效力的代理多签名。

### 3.4　签名方案

(1) Init(初始化):所有参与者协商确定时间参数 $T_0$ , $T_{\mathrm{abolish}}$ , $T_E$ , $T_{\mathrm{abolish}} < T_E$ ,并确定授权发送顺序。确定一个公共公私钥对 (sk, PK) 为所有参与者所共有。

(2) Authorization(授权发送):序号为 1 的参与者制定 $n-1$ 个授权 $(W_{12}, V_{12}), \cdots, (W_{1n}, V_{1n})$ 并分发给相应的参与者, $W_{1j} = (\mathrm{ID}_1, \mathrm{ID}_j, \mathrm{scope}_1, T_0, T_E, E_{\mathrm{PK\_abolish}}, \mathrm{etc})$。其中, $E_{\mathrm{PK\_abolish}}$ 为用 PK 对 $T_{\mathrm{abolish}}$ 进行加密后得到的密文。然后序号为 1 的参与者将所有制作的授权以及签名分别发送给相应的其他参与者。

for( $i=2, i<=n, i++$)

$1 \rightarrow i: W_{1i}, V_{1i}$

此后,序号为 2 的参与者重复序号为 1 的参与者的操作,依此类推。

(3) Authorization Verifying(授权验证)。每个接受者对已得到的授权进行验证:在时间 $T_0$ 前,所有参与者都得到了来自其他参与者的合法授权,则授权的公平交换过程结束。在时间 $T_E$ 后,每个参与者启用代理多签名算法:使用得到的授权代表其他 $n-1$ 个参与者行使代理多签名,从而每个参与者都得到了对其他 $n-1$ 个参与者都具有约束效力的签名(代理多签名);一旦在时间 $T_0$ 后,有参与者没能得到其本应得到的所有合法授权,则该参与者可启动恢复算法。

(4) Recovery(恢复):在时间 $T_E$ 前对 $E_{PK\_abolish}$ 进行解密,得到 $T_{abolish}$,并将其和自己的签名一起发送给 PB,从而在交换过程中产生的所有授权都被撤销。任何人都不能再使用签名所得到的授权行使代理签名权,也即任何人都无法得到对其他参与者具有约束效力的签名(代理签名)。

(5) Proxy Multi-Signature(代理多签名):超过时间 $T_E$ 后,每个参与者使用已得到的合法授权代表其他参与者行使签名权,产生对其他参与者具有约束效力的代理多签名。

for( $j=1, j<=n, j++$)

do $PMV_j$

时间 $T_E$ 之后, PB 不再接受任何来自该次代理多签名活动的警报信息。

## 4 方案分析

针对多方公平交换签名的攻击方式多种多样,然而,不管攻击者的攻击方式多么变化多端,他们的目的却是一致的,即在不付出代价的前提下,获得来自对方的有效证据。

文中假定 PB 和发起者之间可以在指定时间内完成交互,并且 PB 和参与者之间是同步的。这个条件并不难达到,可以把实现这一条件作为发起多方公平交换签名方案的必要条件。需要指出的是,在所提方案中,对于接收者不同步、系统错误或者系统延迟等问题都可以当作一种欺骗手段来处理。

插入攻击:这种攻击方式是指攻击者在指定步骤内退出系统。

攻击者接收到一个或者某几个或者全部其他参与者的授权后即刻退出,拒不分发自己的授权,从而导致了其他参与者在时间 $T_0$ 前无法获得来自该参与者的任何证据。根据系统规则,其他参与者可以通过恢复算法在时间 $T_E$ 前撤销他们所发给攻击者的授权。这些授权将在生效前被撤销。

攻击者在接收完其他参与者的授权,并分发自己对其他参与者的授权后,即刻推出系统。在这种情况下,攻击者与所有其他参与者完成了授权的多方公平交换。

延迟攻击:攻击者在接收到其他参与者的授权后并没有在 $T_0$ 前分发授权给其他参与者,此类攻击方式可归类到插入攻击方式中。最终,攻击者无法获得来自其他参与者的有效授权。

错误授权:攻击者发送错误的授权给其他参与者,其他参与者可以在下一步前对接收到的授权进行检查,如果不是自己需要的就终止协议,或启动恢复算法。这种情况下,任何一方参与者都无法得到来自其他参与者的有效授权。

虚假警报:如果所有参与者在完成了授权的交换后,攻击者仍然发送了警报消息,则所有参与者的授权都将被同时取消,从而所有参与者(包括攻击者)都不能得到来自其他参与者的有效授权(在时间 $T_E$ 之前)。

钓鱼攻击:在钓鱼攻击中,攻击者将自己伪装成某个原厂商的网站以期获得敏感信息(如信用卡信息)。特别地,攻击者可以伪装成可信的接收者,从而在电子交易中获得原厂商的某些敏感信息。为此,攻击者会建立一个与接收者的网站类似的虚假在线网站,并邀请用户在其网站上进行网络购物,从而获得敏感信息。攻击者可以利用这些敏感信息做一些有利于自身的活动,而不需经过持有者的授权(这里指信用卡信息)。

然而,文中所提方案是通过授权的多方公平交换来达到多方公平交换签名的效果。在授权生效前,授权以及相应的签名会被验证,从而避免了上述攻击情况的发生。

纠纷解决可以被分为两个方面:

(1)某个或某些参与者声称接收到了某个消息,而其他参与者否认发送了消息;

(2)某个或某些参与者声称发送了某个消息,而其他参与者并不承认接收到了该消息。

在该方案中,如果无法得到有效的授权,任何参与者都无法从该欺骗行为中得到利益。

从以上讨论可知,在交换结束后,要么参与者都能得到来自其他参与者的有效授权,从而代表其他参与者制作一个对他们具有约束力的代理多签名,要么参与者都无法得到来自其他参与者的有效授权,都无法制作相应的对其他参与者具有约束力的代理多签名,从而达到了公平交换签名的效果。

## 5 比 较

文中所提方案与当前几类多方公平交换签名方案

的比较见表 1。

表 1　所提方案与几类多方公平交换签名方案的比较

| 分　类 | 无可信第三方 | 在线可信第三方 | 离线可信第三方 | 文中方案 |
|---|---|---|---|---|
| 现象 | 公平\不公平 | 公平\不公平 | 公平\不公平 | 公平\不公平 |
| 是否需要可信第三方 | 不需要\不需要 | 需要\需要 | 不需要\需要 | 不需要\不需要 |

从以上对比可以看出:在线可信第三方的公平交换方案中,无论交易双方是诚实的还是不诚实的,在公平交换过程中都需要可信第三方的参与;在离线可信第三方公平交换方案中,一旦交换过程中出现不公平现象,就必须要有可信第三方的参与。即,第三方的参与成为该种方案的一个应用瓶颈。而所提方案,无论在交换过程中是否有不公平现象出现,都无需可信第三方的参与,参与方本身即可实现交换的最终公平性。因此,相对于前面的方案,所提方案消除了可信第三方必须参与的瓶颈,具有更广阔的应用前景。

需要指出的是,虽然无可信第三方的多方公平交换签名方案不需要可信第三方,但该类方案并不能实现真正的公平,实施时要求交换的参与者具有相同的计算能力。因此计算量大,不易于实践,目前已经不再是受关注对象。

## 6　结束语

通过对代理多签名和授权技术的使用,提出了一种多方公平交换授权协议,并在此基础上达到了多方公平交换签名的效果。在该协议中,恶意行为不能给攻击者带来任何利益,而诚实的参与者也不会遭受损失。协议允许参与者以一种公平的方式实现授权的相互交换,在此基础上,通过制作基于所得授权的代理签名,每个参与者都可以得到一个对其他参与者具有约束力的代理多签名;否则,所有参与者都无法得到来自其他参与者的有效授权,也就无法制作出对其他参与者具有约束力的有效代理多签名。文中实现了签名的多方公平交换,而无需用到可信第三方。然而,如何找到一个更有效的方式来实现授权的撤销(当出现不公平时)是未来工作的一个方面。

**参考文献:**


[1] Asokan N, Schuter M, Waidner M. Optimistic protocols for multi-party fair exchange[R]. Zurich: IBM Research Division, 1996.

[2] Onieva J, Zhou Jianying, Lopez J. Non-repudiation protocols for multiple entities[J]. Computer Communications, 2004, 27(16): 1608-1616.

[3] Kremer S, Markowitch O. Amulti-party non-repudiation protocol[C]//Proceedings of the IFIP TC11 fifteenth annual working conference on information security for global information infrastructures. Netherlands: Kluwer, 2000: 271-280.

[4] 韩志耕,罗军舟. 一个公平的多方不可否认协议[J]. 计算机学报,2008,31(10):1705-1715.

[5] 刘义春. P2P 组合交易的公平支付协议[J]. 计算机工程,2008,34(18):171-173.

[6] Wang Y, Au M H, Susilo W. Attribute-based optimistic fair exchange: How to restrict brokers with policies[J]. Theoretical Computer Science, 2014, 527(3): 83-96.

[7] Khill I, Kim J, Han J, et al. Multi-party fair exchange protocol using ring architecture model[J]. Computers & Security, 2001, 20(5): 422-439.

[8] Franklin M, Tsudik G. Secure group barter: multi-party fair exchange with semi-trusted neutral parties[C]//Second international conference on financial cryptography. [s. l.]: [s. n.], 1998: 90-102.

[9] Bao Feng, Deng R, Nguyen K Q, et al. Multi-party fair exchange with an off-line trusted neutral party[C]//Proceedings of the 10th international workshop on database & expert systems applications. Washington, DC: IEEE Computer Society Press, 1999: 858-862.

[10] 杜红珍,张建中. 一个新的带离线半可信第三方的多方公平交换协议[J]. 计算机应用研究,2006,23(8):248-250.

[11] 李艳平,张建中. 带离线半可信第三方的多方交换协议[J]. 西安电子科技大学学报,2004,31(5):811-814.

[12] Zhang Minqing, Xiao Haiyan, Yang Xiaoyuan. ID-based fair multi-party exchange protocol[C]//International conference on measuring technology and mechatronics automation. [s. l.]: IEEE, 2010: 402-405.

[13] Liu Y, Hu H. An improved protocol for optimistic multi-party fair exchange[C]//International conference on electronic and mechanical engineering and information technology. [s. l.]: IEEE, 2011: 4864-4867.

[14] Asokan N, Schunter M, Waidner M. Optimistic protocols for multi-party fair exchange[J]. Biotechniques, 1996, 37(1): 72-88.

[15] 伊丽江,肖　鸿. 一个高效的带有脱线半可信第三方的多方公平交换协议[J]. 西安电子科技大学学报,2000,27(6):745-748.

[16] González-Deleito N, Markowitch O. An optimistic multi-party fair exchange protocol with reduced trust requirements[C]//Proceedings of the 4th international conference on information security and cryptology. [s. l.]: [s. n.], 2001: 258-267.

[17] González-Deleito N, Markowitch O. Exclusion-freeness in multi-party exchange protocols[J]. Lecture Notes in Computer Science, 2002, 2433: 200-209.

[18] Mambo M, Usuda K, Okamoto E. Proxy signatures: delegation of the power to sign messages[J]. IEICE Transactions on Fun-




(下转第 88 页)

支付的特点提出了一种基于格的 ECC-NTRU 加密模型。分析表明该方案具有抗量子计算、效率高、安全等优点,但也增大了系统开销。未来的研究方向是:改进现有的 NTRU 签名算法,提高其效率和安全性;把 NTRU 加密算法融入 WAB 技术或者 XML 加密技术。

**参考文献:**


[1] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[EB/OL]. (1995 - 08 - 27). http://lanl. arxiv. org/pdf/quant - ph/9508027.

[2] Hoffstein J, Pipher J, Silverman J. NTRU: a ring-based public key cryptosystem[C]//Algorithmic number theory symposium. Portland: Springer, 1998: 267-288.

[3] Schoof R. Elliptic curves over finite fields and the computation of square roots mod p[J]. Mathematics of Computation, 1985, 44(170): 483.

[4] 何毅俊. WAP 中 WTLS 安全性研究[D]. 长沙:中南大学, 2007.

[5] 刘辉洲. WTLS 分析与设计[D]. 济南:山东大学, 2010.

[6] 车 葵, 牛晓太, 邢书涛. XML 加密方法的研究与实现[J]. 计算机工程与设计, 2008, 29(20): 5180-5183.

[7] 张若岩. 基于 SET 协议的移动支付系统的研究与实现[D]. 西安:西北大学, 2008.

[8] Ajtai M. Generating hard instances of lattice problems[C]// Proceedings of the 28th annual ACM symposium on theory of computing. New York: ACM, 1996: 99-108.

[9] Goldreich O, Goldwasscr S, Halevi S. Public-kcryptosystcms from lattice reduction problems[C]//Crypto'97. Santce Barbara: Springer, 1997: 112-131.

[10] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings[J]. Journal of ACM, 2013, 60(6): 1-23.

[11] Wei Ping, Wu Liqiang, Yang Xiaoyuan, et al. A public cryptosystem from R-LWE[C]//IEEE 3rd international conference on communication software and networks. [s. l.]: IEEE, 2011: 508-513.

[12] Jaulmes É, Joux A. A chosen-ciphertext attack against NTRU[C]//Advances in cryptology. Berlin: Springer, 2000: 20-35.

[13] Hoffstein J, Pipher J, Silverman J H. NSS: an NT-RU lattice-based signature scheme[C]//Advanced in cryptology-Eurocrypt'01. Berlin: Springer-Verlag, 2001: 123-127.

[14] Hoffstein J, Pipher J, Silverman J H, et al. NTRUSign: digital signatures using the NTRU lattice[C]//Proceedings of CTR-SA'03. San Francisco: [s. n.], 2003: 122-140.

[15] Gentry C, Szydlo M. Cryptanalysis of the revised NTRU signature scheme[C]//Advances in cryptology - Eurocrypt'02. Berlin: Springer-Verlag, 2002: 299-320.

[16] Nguyen P Q, Regev O. Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures[M]//Advances in cryptology-Eurocrypt'06. Berlin: Springer-Verlag, 2006: 271-288.

[17] Lenstra A K, Lenstra H W, Lovasz L. Factoring polynomials with rational coefficients[J]. Mathematische Analen, 1982, 261(4): 515-534.

[18] Silverman J H. Estimated breaking times for NTRU lattices[EB/OL]. 1999-03-09. http://www. ntru. com.

[19] 施荣华, 翁丽萍, 王国才. 基于单向哈希链的 Ad Hoc 网络密钥协商协议[J]. 湖南大学学报:自然科学版, 2011, 38(3): 77-81.


(上接第 83 页)


damentals of Electronics Communications and Computer Sciences, 1996, E79-A(9): 1338-1354.

[19] Yi L, Xiao G, Bai G. Proxy multi-signature scheme: a new type of proxy signature scheme[J]. Electronics Letters, 2000, 36(6): 527-528.

[20] Li X, Chen K. ID-based multi-proxy signature, proxy multi-signature and multi-proxy multi-signature schemes from bilinear pairings[J]. Applied Mathematics & Computation, 2005, 169(1): 437-450.

[21] Cao Feng, Cao Zhenfu. A secure identity-based proxy multi-signature scheme[J]. Information Sciences, 2009, 179(3): 292-302.

[22] Sun Y, Xu C, Yang Y B. Improvement of a proxy multi-signature scheme without random oracles[J]. Computer Communications, 2011, 34(3): 257-263.

[23] Cao H J, Wang H S, Li P F. Quantum proxy multi-signature scheme using genuinely entangled six qubits state[J]. International Journal of Theoretical Physics, 2013, 52(4): 1188-1193.

[24] He Du, Jian Wang. An anonymous but accountable proxy multi-signature scheme[J]. Journal of Software, 2013, 8(8): 1867-1874.

[25] Tang Pengzhi, Deng Junlei, Li Xiaoxiong. Based on bilinear bairing of proxy multi-signature scheme[J]. Journal of Hebei Normal University: Natural Science Edition, 2013, 37(2): 134-137.