第 26 卷第 8 期 电子与信息学报 Vol.26No.8
2004 年 8 月 Journal of Electronics & Information Technology Aug. 2004

一种新型的多方公平交换协议 [1]

李艳平 张建中

(陕西师范大学数学与信息科学学院 西安 710062)

摘 要: 对现有的各种公平交换协议进行了分类. 利用公开可验证秘密共享原理、群加密方案, 提出一个新的基于离线半可信第三方的多方公平交换协议, 离线第三方只在意外情况下才介入协议且其只能解密半个密钥分量, 既保证了交换数据的机密性又实现了交易的真正公平, 且交换的拓扑关系也对外 (包括第三方) 保密.

关键词: 不可否认, 公开可验证秘密共享 (PVSS), 群加密, 组播

中图分类号: TN918 **文献标识码**: A **文章编号**: 1009-5896(2004)08-1340-05

A New Fair Multi-party Exchange Protocol

Li Yan-ping Zhang Jian-zhong

(*College of Mathematics and Info. Sci., Shaanxi Normal Univ., Xi'an* 710062, *China*)

Abstract The fair exchange protocols are classified. Based on publicly verifiable secret sharing scheme and group encryption scheme, a new multi-party fair exchange protocol with an off-line Semi-Trusted Third Party(off-STTP) is presented. The off-STTP intervenes into the exchange in case of problems. That the off-STTP can decipher a sub-secret key makes sure the confidentiality of exchange data and the true fairness of the barter. The participants can barter with others at their will and the exchange topology is unknown to others including the off-STTP.

Key words Non-repudiation, Publicly Verifiable Secret Sharing(PVSS), Group encryption, Group broadcasting

1 引言

随着 Internet 的迅猛发展, 电子商务、网上交易成为一种发展趋势. 针对电子商品的公平交换, 人们作了大量工作且提出不少有价值的公平交换协议 [1](包括其特例不可否认协议 [2,3]), 较为可行的公平交换协议都利用了一个可信任第三方 TTP(Trusted Third Party), 而且这些协议多数是双方公平交换协议, 对于多方 (两方以上) 公平交换协议国内外研究的文献为数不多. 根据交换拓扑的不同, 可将多方公平交换协议分为两类: 一类是单对多交换协议 [3], 即一个主体同时与多个主体进行公平交易, 包括多对单交换协议; 另一类是多对多交换协议, 即多个主体间以一种公平的方式进行交易. 多对多交换协议又可分为环型交易和网 (阵) 型交易. 环型协议往往存在效率和公平性方面的缺陷 [4]. 网型交易要求每个参与主体至少发出和收到一个电子商品 [5], 每个主体可把自己要交换的电子商品同时发给其他交易参与方, 有效节省计算量和通信开销. 这里的电子商品均指有价消息 (较短) 或加密有价消息 (较长) 的对称密钥.

本文在前人的研究基础上, 利用公开可验证秘密共享原理和群加密技术, 提出一个基于离线半可信第三方 (off-line Semi-Trusted Third Party, off-STTP) 的多方网型公平交换协议. 此协

[1] 2003-04-16 收到, 2003-09-14 改回

国家自然科学基金 (No.10271069)、陕西省自然科学基础研究计划项目 (2002A03)、陕西师大重点科研项目资助课题

议实现了网上交易的最优化，即第三方只有在意外情况下才被涉及到，这使得第三方成为瓶颈的可能性大大降低．第三方不必一直在线参与每一次交易且不必完全可信，对第三方的依赖性大大减少．保证了交易的公平性和交易数据的机密性，即使信道不可靠或某些方要赖， off-STTP 的存在也能保证交易的公平性且 off-STTP 始终不知道交易的具体内容和交易的交换拓扑．本协议不要求第三方必须可信 (如文献 [3])，且半可信第三方甚至可以是网络中一个随机成员，这使第三方的可获得性大大提高，故本协议在现实的网络中具有很大的实用价值．

2 预备知识

2.1 群加密方案

文献 [6] 给出一个基于中国剩余定理 (CRT) 与公钥加密方案的组加密技术．即对于某个发送者 S 来说，共有 n 个数据接收者，每个接收者 P_i 都有一个大整数 N_i ，且 N_j 与 N_i 互素， $\forall i \neq j$ ． S 要把某加密密钥 k 群加密，他先用每个 P_i 的公钥加密得 $\mathrm{PE}_{P_i}(k)$(要求 $N_i > \mathrm{PE}_{P_i}(k), i = 1, \cdots n)$ ．由于各个 N_i 两两互素，根据 CRT ，对于 n 个同余方程组 $X \equiv \mathrm{PE}_{P_i}(k)(\mathrm{mod}N_i)(i = 1, 2, \cdots, n)$ 必存在惟一解．为保证上式中解的惟一性， X 取值为方程组成立的最小的自然数．然后 S 组播 X 给每个接收者 P_i, P_i 计算 $X \mathrm{mod} N_i \equiv \mathrm{PE}_{P_i}(k)$ ，然后用私钥解密即可获得密钥 k ．详见文献 [6] ．

2.2 公开可验证秘密共享 (PVSS)

文献 [7] 中给出一个加解密特别简单、计算量较低的 PVSS 方案．设每个分享者 P_i 都有一公开的加密函数和一秘密的解密函数，用一公开密码体制的公私钥对即可．秘密 k 的分发者 (Dealer) 将每一子密 k_i 用分享者的公开加密函数加密并公布于众： $K_i = E_i(k_i), i = 1, 2, \cdots, n$ ．本文中 $i = 1, 2$ ．任一分享者 P_i 可以通过 PubVerify() 验证每一分享值的真伪，且满足 $\exists u, \forall X \in A$(访问结构)， $(\forall i \in X, \mathrm{PubVerify}(K_i) = 1) \Rightarrow (\mathrm{Recover}(\{D_i(K_i) | i \in X\}) = u)$ ．若 Dealer 诚实，则 $u = k$ ．这里， Dealer 虽能欺骗，但能识别． PubVerify() 可以是秘密分享者与秘密拥有者之间的交互协议，也可以是非交互的．为了节省通信开销，需采用非交互的，分发者在公布 K_i 时，同时提供相应的证据 (Proof_i), Proof_i 生成的具体形式和采用的具体算法及实现方法有关．详见文献 [7] ．

3 本文协议

3.1 基本符号与含义

P_i 为参与本次公平交易的主体，共有 n 位，即 $i = 1, 2, \cdots, n$ ，其身份标识号为 ID_{P_i} ； R_i 为本协议起始阶段主体 P_i 议定的消息接收者的全体， $|R_i| = n - 1$, 其身份识别符的全体集记为 ID_{R_i} ； R_i' 为最终收到主体 P_i 发出的消息并在有效时间内回应 P_i 的接收者的全体，$|R_i'| \leq n - 1$ ； $E_R(X)$ 为对消息 X 进行群加密，加密后的密文只能由 R 内的主体能进行解密，$E_k(X)$ 为用对称密钥算法及其密钥 k 对消息 X 进行加密； $\mathrm{PE}_{P_i}(X)(\mathrm{PD}_{P_i}(X))$ 为用某个主体 P_i 的公 (私) 钥 X 进行加 (解) 密， Sig_i 表示 P_i 的签名； $\mathrm{PE}_T(X)(\mathrm{PD}_T(X))$ 为表示 off-STTP 的公 (私) 钥对消息 X 加 (解) 密函数， Sig_T 表 off-STTP 的签名； $\mathrm{Share}(k_i) = (k_{i1}, k_{i2})$ 为用 PVSS 技术对加密密钥 k_i 生成公开可验证子密 k_{i1}, k_{i2} ； $\mathrm{Recover}(k_{i1}, k_{i2}) = k_i$ 为利用子密恢复共享秘密的算法； Abort_j 为表示主体 P_j 要放弃本次协议． $\mathrm{Abort}_{j \leftrightarrow i}$ 表示 P_j 放弃与主体 P_i 的交易．

3.2 协议描述

假设本次交易的每个参与者 (包括 off-STTP) 都有两对公私钥对，一对用于加解密，一对用于签名验证．并设文中出现的签名均是不可伪造的，且惟一地代表着签名主体的身份．本协议的思想是： n 个主体 $P_i(i = 1, \cdots, n)$ 已达成协议准备交换各自的等价消息 M_i ，意外情况下

off-STTP 可协助保证协议的公平性. 每个主体 P_i 生成随机加密密钥 k_i , 用对称密钥算法加密 M_i 得 $E_{k_i}(M_i)$ 并将五元组 $<\mathrm{ID}_i, \mathrm{Dec}_i, E_{k_i}(M_i), H(k_i), \mathrm{Sig}_{Ai}>(i=1,\cdots,n)$ 在交易进行前公布在权威机构的公共目录. 其中 Dec_i 是对交换消息 M_i 的内容简介, $H(k_i)$ 是对加密密钥 k_i 的 Hash 值, 这里 $H(\cdot)$ 表强单向无碰撞 Hash 函数. Sig_{Ai} 是权威机构对前四元组的签名. 假设交易各方都从该目录中心取回其它方的五元组. 这些措施都是为了确保用 k_i 解密 $E_{k_i}(M_i)$ 能得到 Dec_i 描述的消息, 从而保证交易的进一步安全性. 然后每位主体应用 $\mathrm{Share}(k_i)=(k_{i1},k_{i2})$ 将 k_{i1} 群加密给 R_i , 把 k_{i2} 用 PE_T 加密发给其他每个接收者. 显然在意外情况下, off-STTP 直接解密半个密钥, 恢复 k_{i2} 来保证协议的安全性, 避免了文献 [3] 中的二次加密, 降低了运算量和对第三方可靠信要求.

(1) 每位主体 $P_i(i=1,\cdots,n)$ 运行 $\mathrm{Share}(k_{i1})=(k_{i1},k_{i2})$. 先用 $P_j(j\neq i)$ 的公钥加密 k_{i1} , 再利用群加密技术得 $E_{R_i}(k_{i1})$, 用 PE_T 加密 k_{i2} 得 $\mathrm{PE}_T(k_{i2})$, 并生成相应 Proof_{iR_i}, Proof_{iT} . 然后, 每位主体将 $m_{i1}=\{\mathrm{ID}_{P_i},\mathrm{ID}_{R_i},T_{i1},E_{R_i},\mathrm{PE}_T(k_{i2}),\mathrm{Proof}_{iR_i},\mathrm{Proof}_{iT}\}$ 及签名 $\mathrm{Sig}_{i1}(m_{i1})$ 组播给 R_i 的每位接收者. 其中 T_{i1} 是主体 P_i 明确规定的时间期限, 来确定 R_i' , 其他参与方 P_j 应将 m_{j1} 在 T_{i1} 之前发给 P_i .

(2) 每位接收者 $P_j(j\neq i)$ 接到其他主体发来的消息后 (以 T_{j1} 为界) , 先验证 $\mathrm{Sig}_{i1}(m_{i1})$ 的有效性, 再通过 Proof_{iR_i}, Proof_{iT} 运行 PubVerify() 验证 $E_{R_i}(k_{i1})$, $\mathrm{PE}_T(k_{i2})$ 的正确性. P_j 保留通过两步验证有效的 m_{i1}, $\mathrm{Sig}_{i1}(m_{i1})$, 无效的则丢弃. 若 P_j 因意外原因要放弃, 则发 Abort_j 或 $\mathrm{Abort}_{j\leftrightarrow i}$ 给 off-STTP .

(3) 截止时间 T_{i1}, P_i 收到有效的消息的响应者的全体记为 R_i' . 显然, 集合 R_i' 与 $R_j'(i\neq j)$ 的大小及成员可能不同. P_i 继续生成 $m_{i2}=\{\mathrm{ID}_{P_i},\mathrm{ID}_{R_i'},T_{i2},E_{R_i'}(k_{i2}),\mathrm{Proof}_{iR_i'}\}$ 及签名 $\mathrm{Sig}_{i2}(m_{i2})$ 组播给 R_i' 的每位接收者. 而任意 $P_j\in R_i-R_i'$ 均无法利用 $E_{R_i'}(k_{i2})$ 求得 k_{i2} , 也就无法通过 $\mathrm{Recover}(k_{i1},k_{i2})=k_i$ 恢复加密密钥 [8] , 其中时间期限 T_{i2} 用以控制协议的时间跨度, 因为有些消息在一定时间期限后对某些主体来说将变得毫无价值. 超过此时间, 则 R_i' 中的每一个主体均可向 off-STTP 求助获得 k_{i2} , 从而保证了协议的公平性.

(4) 对于每个 $P_j\in R_j'$ 均可由 $E_{R_i}(k_{i1})$, $E_{R_i'}(k_{i2})$ 求得 k_{i1}, k_{i2} , 再用 $\mathrm{Recover}(k_{i1},k_{i2})=k_i$ 恢复加密密钥 k_i , 若 P_j 对密钥 k_i 怀疑, 则对 k_i 取 Hash 值与公布的 $H(k_i)$ 比较来验证 k_i 的正确性. 通过此步验证即可用 k_i 读解主体 P_j 的加密消息 M_i .

3.3 纠纷解决

在协议末或超过时间 T_{j2} , 某方 P_i 向 P_j 分发了 $E_{R_i}(k_{i1})$, $E_{R_i'}(k_{i2})$ 而仅收到 $E_{R_j}(k_{j1})$. 此时, P_i 向 off-STTP 提供: m_{i1}, $\mathrm{Sig}_{i1}(m_{i1})$, m_{i2}, $\mathrm{Sig}_{i2}(m_{i2})$, m_{j1}, $\mathrm{Sig}_{j1}(m_{j1})$, TS_i . TS_i 为 P_i 发出该消息的时戳. 事实上, 参与协议的每个主体都可能向 off-STTP 求助, off-STTP 分情况处理各种求助信息.

(1) off-STTP 查看 TS_i 是否的确超过 T_{j2} , 若还没有超过, 则发签名消息 “时间还早” 给 P_i .

(2) 若已超过时间 T_{j2} , 则 off-STTP 查看是否收到来自 P_j 的 Abort_j 或 $\mathrm{Abort}_{j\leftrightarrow i}$ 消息。若收到 Abort_j , 则广播一签名消息 “ P_j 已放弃本次协议”; 若收到 $\mathrm{Abort}_{j\leftrightarrow i}$, 则发签名消息 “ P_j 已放弃” 给 P_i .

(3) 若已超过时间 T_{j2} 且没有收到来自 P_j 的 Abort_j 或 $\mathrm{Abort}_{j\leftrightarrow i}$ 消息, 则 off-STTP 验证 P_i 是否为合法者. 显然, 如果不对 P_j 的第一个消息响应的主体不可能获得 m_{j2}, $\mathrm{Sig}_{j2}(m_{j2})$. 即

使他在信道上截获 m_{j2}, $\mathrm{Sig}_{j2}(m_{j2})$，但 m_{j2} 中 $\mathrm{ID}_{R_i'}$ 可以证明 P_i 为非法接收者，故 off-STTP 对其不作回应.

(4) 若已超过时间 T_{j2}，且 $\mathrm{ID}_{R_i'}$ 中有 P_i 的身份标识符 ID_{P_i}，即表明 P_i 的确给 P_j 的第一个消息发出正确的响应. 不管是 P_i 自己生成 m_{i2}, $\mathrm{Sig}_{i2}(m_{i2})$ 来欺骗，还是曾广播过 m_{i2}, $\mathrm{Sig}_{i2}(m_{i2})$, 只要 off-STTP 没有收到来自 P_j 的 Abort_j 或 $\mathrm{Abort}_{j\leftrightarrow i}$ 消息，且验证 P_i 提供的消息均合法，则 off-STTP 解密 $\mathrm{PE}_T(k_{j2})$ 得 k_{j2}，用 P_i 的公钥加密得 $\mathrm{PE}_{P_i}(k_{j2})$ 并随签名发给 P_i, P_i 接到 $\mathrm{PE}_{P_j}(k_{j2})$ 后解密得 k_{j2}，然后用 $\mathrm{Recover}(k_{j1}, k_{j2}) = k_j$ 恢复加密密钥 k_j，最后读解主体 P_j 的由 k_j 加密的消息 M_j. 若 P_j 在时间 T_{i2} 内得不到 m_{i2}, $\mathrm{Sig}_{i2}(m_{i2})$，他也可求助 off-STTP 获得 k_{i2}.

(5) Abort_j 和 $\mathrm{Abort}_{j\leftrightarrow i}$ 的引入是为了使交易变得更加灵活，即某主体虽然进行了第一轮交互，但由于意外情况决定放弃本次协议，于是他给 off-STTP 发 Abort_j，表示不要为任何主体解密 $\mathrm{PE}_{R_j}(k_{j2})$；有时主体 P_j 决定放弃与 P_i 之间的交易，所以他给 off-STTP 发 $\mathrm{Abort}_{j\leftrightarrow i}$，要求 off-STTP 不给主体 P_i 恢复 k_{j2}.

3.4 安全性分析

(1) 完备性　由上分析知，只要交易各方遵守协议且不放弃交易，则交易顺利完成且能达到交易的目的. PVSS 能检验各参与方的不诚实行为，并保证每个主体的密钥子密的可验证性及其被分发过程的正确性，公开的 $H(k_i)$ 能验证恢复的加密密钥的真伪，Dec_i 保证了加密的数据文件不被替换.

(2) 公平性　由 3.3 节的分析知，若协议某方只发出密钥的一半，其他处于受害地位的交易方均可借助 off-STTP 来获得密钥的另一半，而无论哪方中止协议并进行欺骗都得不到 off-STTP 的支持，从而保证了交易的公平性.

(3) 高效性　在正常情况下，协议并不涉及 off-STTP 且仅需 3.2 节中的 (1)–(4) 步即可完成某交易组或团体内主体间随意的交换，避免了文献 [3] 中二次加密运算 (其中群加密结果长短不定，又用 off-STTP 的公钥加密，导致了很大的运算量).

(4) 可行性　本协议中 off-STTP 可获得性强，即使 off-STTP 被破坏，也不会出现文献 [3] 中某主体的秘密被全体接收者读解的情况；不像有些协议只要某方中止交易就导致整个交易的失败 [5]，本协议允许某些主体因意外原因放弃交易，使得交易更加灵活，符合实际；文献 [5] 中协议没有时间限制，可能导致协议无限制拖延，于是本文加了明确的时间限，有利于交易的公平进行，且有效控制协议的始终.

(5) 交换拓扑保密性　这是文献 [9] 提出的一个公开问题. 在现实交易中，交易方往往不想向外界透露他们的交换关系，因此交换关系的拓扑保密，可视为多方交换的一条独特性质. 该协议交换拓扑统而言之为网型，但具体的交换关系却对外 (包括 off-STTP) 保密.

4 结束语

多方公平交换协议是实现电子商务的一个重要基础，本文基于一个离线半可信第三方，利用 PVSS 与群加密技术，提出一个公平高效的网型多方交换协议，实现了多方网上电子数据交易的最优化，并保证数据的机密性和交易的公平性. 故本协议具有较强的实用价值，有利于电子商务的进一步开展.

参　考　文　献

[1]　蒋晓宁，叶澄清，潘雪增. 基于半可信离线第三方的公平交易协议. 计算机研究与发展，2001, 38(4): 502–508.

[2] Zhou J, Gollman D. A fair non-repudiation protocol. In: M Rroscheisen, C Serban, eds. Proc. of 1996 IEEE Symposium on Security and Privacy. Oakland, IEEE Computer Society Press, 1996: 55–61.

[3] 邓所云, 隋爱芬, 胡正名, 杨义先. 一个优化的公平的多方不可否认协议. 电子与信息学报, 2002, 24(12): 1985–1989.

[4] Franklin M, Tsudik G. Secure group barter: Multi-party fair exchange with semi-trusted neutral parties. In: Financial Cryptography'98, 1998, LNCS 1465: 90–102.

[5] 伊丽江, 肖鸿. 一个高效带有离线半可信第三方的多方公平协议. 西安电子科技大学学报, 2000, 27(6): 745–748.

[6] G Chiou, W Chen. Secure broadcasting using the secure lock. *IEEE Trans. on Software Engineering*, 1989, 15(8): 929–934.

[7] B Schoenmakers. A simple pubilcly verifiable secret sharing scheme and its application to electronic voting. In: Advance in Cryptology-Proc. of CRYPT'99, Berlin, Springer-Verlag, 1999, LNCS 1666: 148–164.

[8] T Hwang. Cryptosystem for group oriented cryptography. In: I B Damgard, editor. Advances in Cryptology-EUROCRYPT'90, Denmark, Springer-Verlag, 1991, LNCS 473: 352–360.

[9] Zheng Dong, Chen Kefei. Multi-item fair exchange scheme. *Journal of Electronics*(China), 2002, 19(4): 363–368.

李艳平: 女, 1978 年生, 硕士生, 主要研究兴趣: 公平协议与电子商务.

张建中: 男, 1960 年生, 教授, 硕士生导师, 主要研究兴趣为: 秘密共享.