利用门限密码实现乐观的步进式公平交换

蓝 天，秦志光，赵 洋

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】提出一个在不存在单一可信第3方的分布式环境中的乐观公平交换协议。该协议的整个交换过程分为秘密分块密文交换阶段和密钥步进式交换阶段。双方都能以高概率在交换过程中检测到欺骗行为，从而停止揭示剩余的秘密分块，只有在最后阶段出现异常情况才会求助一个门限解密组。该协议不基于双方相等计算能力的假设，也不依赖于可信第3方来确保公平性，计算复杂度与已有的小步进交换协议相当，而通信复杂度更低。

关 键 词 电子商务； 信息安全； 乐观公平交换； 门限密码； 可信第3方

中图分类号 TP393.08 **文献标识码** A doi:10.3969/j.issn.1001-0548.2011.01.019

Optimistic Gradual Fair Exchange by Using Threshold Cryptography

LAN Tian, QIN Zhi-guang, and ZHAO Yang

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract An optimistic fair exchange protocol in distributed settings without a single trusted third party is proposed. In this protocol, the exchange process consists of secret share ciphertext exchange phase and key gradual exchange phase. Each party is able to stop releasing the rest secret shares in case of cheat, which can be detected with high probability during the process. A threshold decryption group is involved only when unfair behavior occurs in the last exchange round. The proposed protocol does not rely on equal computing power assumption or a trusted third party to guarantee fairness. It also has equivalent computation complexity and smaller communication complexity compared with previous gradual release schemes.

Key words electronic commerce; information security; optimistic fair exchange; threshold cryptography; trusted third party

电子商务中的商业交易通常可归结为用一个商品交换另一个商品，不同种类的商业活动存在不同场景的交换，比如购买、签约、挂号邮件、物物交换等[1]。公平交换问题就是研究如何在任意两个互不信任的主体之间以一种高效、公平的方式交换电子数据。

公平性有强弱之分，强公平性是指当交换过程结束后，要么交换双方都收到期望的交换品，要么双方都未收到；弱公平性是指当交换过程结束后，要么满足强公平性，要么未收到期望交换品的一方能得到对方已收到期望交换品的证据，以便未收到一方能向仲裁人出示该证据，证明自己的利益受损。

本文考虑如何在分布式系统中不依赖一个可信第3方保证公平性的问题，提出了一个基于门限密码的乐观公平交换协议，公平性不依赖于交换双方拥有相等的计算能力，欺骗行为能在交换过程中以高概率被检测出来，在出现异常时可以求助一个门限团体进一步保证公平性。

1 相关工作

一般将已有的公平交换协议分为在线第3方协议、离线第3方协议(乐观交换协议)和小步进交换协议3类。在线第3方协议的优点是可以保证强公平性，缺点主要是安全性来自对可信第3方的依赖，并且在有多个交换实例的场景里第3方成为影响效率的瓶颈，但是完全脱离第3方的两方公平交换是不能保证强公平性的[2]，因此近年很多研究集中于乐观交换[3-6]方案。

文献[3]提出了一个用4条消息进行同步签约的乐观协议，并在文献[4]中做了改进，继而提出了4

收稿日期：2009 – 07 – 27； 修回日期：2010 – 11 – 22
基金项目：教育部高等学校博士学科点专项科研基金(20050614018)；四川省科技攻关计划(05GG007-011-01)
作者简介：蓝 天(1977 –)，男，博士生，主要从事安全多方计算及其应用方面的研究.

条消息的异步签约协议，用可验证加密实现了签名的公平交换。文献[5]也提出使用可验证加密做公平签名交换，该类协议在正常情况下不需要求助第3方，只有某方出现异常行为时才会让第3方介入仲裁，所以效率高，并对交换双方都是不可抵赖的，但本质上还是要依靠一个可信第3方保证公平性。

没有第3方的小步进交换协议可进一步分为两类。一类小步进交换协议以文献[7]提出的协议为代表，它们以茫然传输为基础，秘密被分为n份，先用茫然传输发送一半的秘密给对方，然后双方逐位交换每份秘密，已经收到的一半秘密用于检测欺骗。这样的协议叫做PSE(局部秘密交换)协议，缺点之一是公平性依赖于双方的计算能力相等，即假设双方具有同样程度的能力计算剩余的秘密；缺点之二是通信复杂度大，茫然传输和逐位交换使通信轮数倍增。提出一种小步进交换协议，该协议基于特权的逐渐提升，但只能应用于公平签约问题。

本文提出的协议旨在降低对单一可信第3方的依赖，正常情况下像小步进协议一样交换秘密，去除对相等计算能力的依赖，并降低通信复杂度。

2　预备知识

2.1　门限密码系统

门限密码系统[9-14]通过将信息分散到多个载体达到保护信息安全的目的，分布式解密是其一种应用。门限密码系统TCS包含4个组成部分，可表示为TCS = (KG,EN,SD,CB)，其中KG是密钥产生算法，EN是加密算法，SD是分享解密算法，CB是组合算法。

1) 密钥产生算法表示为：

$$(\mathrm{PK},\mathrm{SK}_1,\mathrm{SK}_2,\cdots,\mathrm{SK}_l,\mathrm{VK},\mathrm{VK}_1,\cdots,\mathrm{VK}_2,\mathrm{VK}_l)=G(k,l,t,\omega)$$

该算法以安全参数k、解密成员数量l、门限值t和随机串ω作为输入，产生公钥PK、成员私钥列表SK_1、SK_2、⋯、SK_l 和验证项VK、VK_1、VK_2、⋯、VK_l。

2) 加密算法表示为：

$$c=\mathrm{EN}_\omega(\mathrm{PK},M)$$

该算法以随机串ω、公钥PK和明文M作为输入，产生密文。

3) 分享解密算法表示为：

$$(c_i\mathrm{pf}_i)=\mathrm{SD}(\mathrm{PK},i,\mathrm{SK}_i,c)$$

该算法用于第i名解密成员，以公钥PK、序号i、私钥SK_i和密文c作为输入，产生解密分片c_i和有效性证明pf_i。

4) 组合算法表示为：

$$M=\mathrm{CB}(\mathrm{PK},c,c_1,\cdots,c_l,\mathrm{VK},\mathrm{VK}_1,\mathrm{VK}_2,\cdots,\mathrm{VK}_l,\mathrm{pf}_1,\mathrm{pf}_2,\cdots,\mathrm{pf}_l)$$

该算法以公钥PK、解密分片$c_1,c_2,\cdots,c_l$验证项VK、VK_1、VK_2、⋯、VK_l和有效性证明pf_1、pf_2、⋯、pf_l为输入，如果有多于门限t的有效解密分片，就可以输出明文M。

2.2　模型和假设

假设交换双方A与B都位于一个分布式系统中，且该系统包含足够多的对等实体，双方协商选定一个对等实体组G，建立相应的门限密码系统TCS_G。关于G的选取本文不作重点讨论，可以采取所有成员由双方临时选定的方式，也可以采取由系统预先划分好多个组，然后双方随机选组的方法。

TCS_G的公开信息即k、t、ω、PK_G、VK、VK_1、VK_2、⋯、$\mathrm{VK}_{|G|}$等由A和B共享。A和B都可以对消息进行门限加密，也能组合解密分片恢复明文。假设G中总有超过t的成员能提供有效的解密分片，为描述方便，简化TCS_G验证部分的内容，对于明文M和密文c，$c=\mathrm{EN}_\omega(\mathrm{PK}_G,M)$、$c_G=\mathrm{SD}(\mathrm{PK}_G,\mathrm{SK}_G,c)$、$M=\mathrm{CB}(\mathrm{PK}_G,c,c_G)$，其中$\mathrm{SKG}=\mathrm{SK}_1,\mathrm{SK}_2,\cdots,\mathrm{SK}_{|G|}$是$G$中各成员的解密私钥，$c_G=c_1,c_2,\cdots,c_{|G|}$是所有有效的解密分片。

交换的一方A要将自己的秘密a与另一方B的秘密b相交换。A将自己的秘密a分成n份a_1、a_2、⋯、a_n，每份都是能被B识别的；同样地，B也将自己的秘密b分成可以被A识别的n份b_1、b_2、⋯、b_n。只有拿到全部n份子秘密，才能得到一份完整的秘密，双方都只掌握对方部分子秘密的情况，被认为是公平状态。

$H(\cdot)$是一个无碰撞的单向HASH函数，$c=F(M,K)$是一个对称加密算法，K为密钥，相应的解密算法用$M=F^{-1}(c,K)$表示。A和B有各自用于数字签名和加解密的公私钥对。对于输入x，$E_P(x)$代表P对x的加密。对于协议中的每条消息m，发送方应该附加自己和对方的ID、时间戳，防止重放攻击，并对整条消息做认证签名$\mathrm{SIG}_P(H(m))$。出于保密性考虑还应以对方的公钥加密，但为了描述方便，所有的消息都简化表示为m。系统中采用超时重传等手段使消息传递可靠，协议中不考虑超时问题。

3　协议描述

协议的主要思想是：双方将n份子秘密分别用随机生成的不同密钥进行对称加密，互换密文后按份逐渐交换这些密钥。交换过程中，双方随机选取对

方下一步要发送的密钥，使得一方用假密钥欺骗对方的可能性减小。为防止一方得到对方最后一份密钥后恶意离开协议，双方还要先将所有的对称密钥用G的公钥加密交给对方，遇到上述情况时，可以由G帮助解密。下面对协议进行详细描述。

3.1 交换主协议

正常情况下需要n+1轮交换，即1轮密文交换和n轮密钥交换，每轮交换包含两条消息，如图1所示。步骤如下：

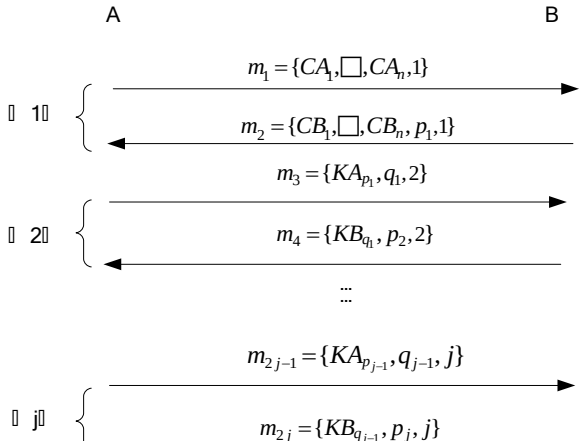


图1 交换主协议

交换步骤如下：

1) 第1轮 密文交换为：

$$m_1=\{\mathrm{CA}_1,\mathrm{CA}_2,\cdots,\mathrm{CA}_n,1\}:A\to B$$

A将每份子秘密$a_i(1\leqslant i\leqslant n)$分别用独立的随机密钥$\mathrm{KA}_i$加密，得到$\alpha_i=F(a_i,\mathrm{KA}_i)$。然后用$G$的公钥加密这些随机密钥，得到$\mathrm{VA}_i=\mathrm{EN}_\omega(\mathrm{PK}_G,\mathrm{KA}_i)$。最后计算$\mathrm{CA}_i=\alpha_i\|\mathrm{VA}_i$，将第1轮附在$m_1$末尾，有：

$$m_2=\{\mathrm{CB}_1,\mathrm{CB}_2,\cdots,\mathrm{CB}_n,p_1,1\}:B\to A$$

在收到m_1后，B先将所有的α_i和VA_i从CA_i中提取出来保存，类似地，将每份子秘密$b_i(1\leqslant i\leqslant n)$分别用独立的随机密钥$\mathrm{KB}_i$加密，得到$\beta_i=F(b_i,\mathrm{KB}_i)$。然后用$G$的公钥加密这些随机密钥，得到$\mathrm{VB}_i=\mathrm{EN}_\omega(\mathrm{PK}_G,\mathrm{KB}_i)$，由$\beta_i$和$\mathrm{VB}_i$得到$\mathrm{CB}_i=\beta_i\|\mathrm{VB}_i$。$m_2$与$m_1$的不同是，$B$要随机指定一个序号$p_1(1\leqslant p_1\leqslant n)$，让$A$发送对应的密钥$\mathrm{KA}_{p_1}$。最后附上第1轮。

2) 第2轮 密钥交换为：

$$m_3=\{\mathrm{KA}_{p_1},q_1,2\}:A\to B$$

A先将所有的β_i和VB_i从CB_i中提取出来保存，然后根据B在m_2中指定的序号p_1找到KA_{p_1}，并随机指定$q_1(1\leqslant q_1\leqslant n)$，声明下一步$B$应该发送的密钥为$\mathrm{KB}_{q_1}$，最后附上第2轮，有：

$$m_4=\{\mathrm{KB}_{q_1},p_2,2\}:B\to A$$

B先用KA_{p_1}解密α_{p_1}，得$\alpha_{p_1}=F^{-1}(\alpha_{p_1},\mathrm{KA}_{p_1})$，识别$\alpha_{p_1}$是否为一份有效的子秘密，并验证$\mathrm{VA}_{p_1}$是否为$\mathrm{KA}_{p_1}$的正确门限加密$\mathrm{EN}_\omega(\mathrm{PK}_G,\mathrm{KA}_{p_1})$。识别和验证都通过后，就将$A$要求的$\mathrm{KB}_{q_1}$和下一步要交换的密钥随机序号$p_2$回送，附上第2轮；若任一检验没有通过，那么$B$直接终止协议。

3) 第$j(3\leqslant j\leqslant n+1)$轮 密钥交换为：

$$m_{2j-1}=\{\mathrm{KA}_{p_{j-1}},q_{j-1},j\}:A\to B$$

A先用$\mathrm{KB}_{q_{j-2}}$解密$\beta_{q_{j-1}}:b_{q_{j-2}}=F^{-1}(\beta_{q_{j-2}},\mathrm{KB}_{q_{j-2}})$，识别子秘密$b_{q_{j-2}}$的有效性，验证$\mathrm{VB}_{q_{j-2}}$的值是否为$\mathrm{EN}_\omega(\mathrm{PK}_G,\mathrm{KB}_{q_{j-2}})$。都通过后，就将$B$要求的$\mathrm{KA}_{q_{j-1}}$和下一步交换的密钥随机序号$q_{j-1}$回送，附上轮数$j$。若任一检验没有通过，那么$A$直接终止协议，有：

$$m_{2j}=\{\mathrm{KB}_{q_{j-1}},p_j,j\}:B\to A$$

B用$\mathrm{KA}_{p_{j-1}}$解密$\alpha_{p_{j-1}}$，得到$\alpha_{p_{j-1}}=F^{-1}(\alpha_{p_{j-1}},\mathrm{KA}_{p_{j-1}})$，识别子秘密$\alpha_{p_{j-1}}$的有效性，验证$\mathrm{VA}_{p_{j-1}}$的值是否为$\mathrm{KA}_{p_{j-1}}$的正确加密。都通过后，就将$A$要求的$\mathrm{KB}_{p_{j-1}}$和下一步交换的密钥随机序号$p_j$ $(p_{n+1}=0)$回送，附上轮数j。若任一检验没有通过，那么B直接终止协议。正常情况下，交换将以A收到B发送的最后一条消息$\{\mathrm{KB}_{q_n},0,n+1\}$作为结束，$A$得到全部$b_1$、$b_2$、…、$b_n$，$B$也得到全部$a_1$、$a_2$、…、$a_n$。

然而，如果A没有收到B的最后一条消息或者对KB_{q_n}的检验没有通过，那么协议异常结束，A可以向G申请协助恢复密钥，进入恢复子协议。但A又可能在还没有给B发送正确的KA_{q_n}之前，利用恢复子协议获取KB_{q_n}，因此在恢复子协议中要对A的申请作检验。

3.2 恢复子协议

由于假设G中总存在多于门限t的诚实成员，因此恢复子协议中将G的成员作为整体讨论。实际上，每个成员都要单独运行恢复子协议，步骤如下：

1) A的申请需要包含两条消息m_{2n}、m_{2n+1}和需要解密的VB_{q_n}。因为消息包含双方的签名，可以证明是进行到了最后一轮。

2) G将联系B，证实m_{2n+1}的真实性，如果B向G证明没有收到m_{2n+1}或者m_{2n+1}中的密钥检测错误，G就认为A是恶意申请，终止恢复子协议。

3) 如果G无法联系到B或者B无法证明A发送了错误的m_{2n+1}，G的成员共同解密VB_{q_n}，令$c=\mathrm{VB}_{q_n}$，有$c_G=\mathrm{SD}(\mathrm{PK}_G,\mathrm{SK}_G,c)$，将$c_G$返回$A$。

4) A运行组合算法解得$\mathrm{KB}_{q_n}=\mathrm{CB}(\mathrm{PK}_G,c,c_G)$，

于是可进一步解密 $b_{q_n}=F^{-1}(\beta_{q_n},\mathrm{KB}_{q_n})$。

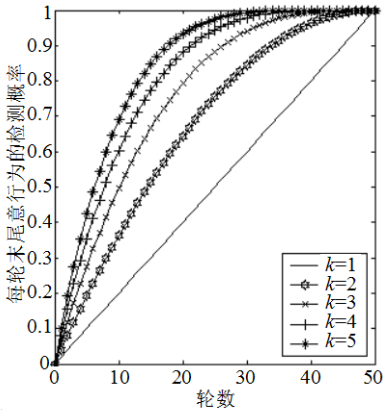
4　协议分析

4.1　安全性分析

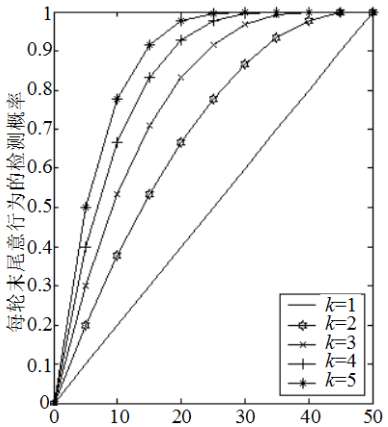
协议的安全性主要针对公平性进行分析，消息本身的安全性本文不作考虑(可以使用安全信道或者公钥加密实现消息的保密)。在主协议的密文交换阶段，双方只是交换子秘密的密文以及用G公钥加密的密钥密文，显然这是一个公平状态。在后续的密钥交换的每个步骤中，接收方收到自己随机指定的密钥后，都对其正确性进行验证，检查对应的子秘密明文是否正确和对应密钥密文是否正确加密，在交换过程中发现恶意行为。

恶意行为有两种：1) 用假的子秘密进行密文交换；2) 用假的密钥密文使得恢复出的密钥也没有用。假设恶意方的n个子秘密中有k个存在上述恶意行为之一，可以计算在前j轮交换中其恶意企图不被检测出来的概率为：

$$\mathrm{Pr}_j=1-\frac{C_{n-j}^{k}}{C_n^k}=1-\prod_{i=0}^{k-1}\frac{n-i-j}{n-i}$$



a. n=50 时的检测曲线



b. n=10 时的检测曲线

图2　恶意行为检测的概率曲线

图2以$n=50$和$n=10$为例绘制了当k=1、2、3、4、5时的恶意行为检测概率曲线。k>2时，当协议进行到一半时，恶意行为被检测出的概率都高于0.9。概率曲线随轮数递增快速趋近于1；反过来，恶意行为不被检测出来的可能性也就快速趋近于0。由此可见，j越大，交换的轮数越大，检测出的概率Pr_j越高；k越大，恶意方的无效数据越多，恶意企图也越容易被检测出来。

本文协议不用假设交换双方具有相等计算能力，因为n个子秘密是独立加密的，每个子秘密的明文空间不像PSE协议会随交换过程逐渐缩小，计算能力强，不会占有很大优势。由于在交换过程中恶意行为随轮数增长被检测出来的概率越来越大，最后一份子秘密有恶意行为的可能性也很小，所以可以通过恢复子协议保证最后一步的公平性。

值得注意的是，交换子协议中接收方在还没有发送完自己的所有密钥之前，对收到对方密钥检测出错的处理都是直接终止协议。这样做是基于前述假设，即双方各自掌握对方部分子秘密不影响公平性，只有在一方掌握了全部子秘密而另一方只得到部分子秘密才视作对公平性的破坏。

4.2　复杂度分析

在密文交换阶段，双方共需执行对称加密操作2n次(子秘密加密)、非对称加密操作2n次(密钥加密)；在密钥交换阶段共需对称解密操作2n次(子秘密解密)、非对称加密操作2n次(验证密钥密文)。恢复子协议的计算复杂度与n无关，并且不属于交换双方的必要开销，故主协议的计算复杂度为$O(n)$。

协议的通信复杂度主要是以通信轮数复杂度作为衡量标准，正常结束的情况下，需要双方交换$n+1$轮，故总体通信复杂度为$O(n)$。而PSE协议的通信复杂度为$O(n+l)$，其中l为子秘密的长度。

与小步进交换协议相比，本文协议的计算复杂度相当于茫然传输部分的计算复杂度，而通信复杂度更小。

5　结 束 语

本文提出一个基于门限密码的乐观公平交换协议。该协议的运行在多数情况下只涉及交换双方，以步进交换的方式进行，在交换过程中能以高概率检测恶意行为，只有在最后一轮交换出现异常时，才求助一个门限团体进一步保证公平性。该协议不依赖于双方具有相等计算能力的假设，并且降低了

通信复杂度，适用于没有可信第3方的分布式环境中的公平交换。

参 考 文 献

[1] ASOKAN N. Fairness in electronic commerce[D]. Ontario, Canada: Department of Computer Science, University of Waterloo, 1998.

[2] MICALI S. Simple and fast optimistic protocols for fair electronic exchange[C]//PODC 2003: Proceedings of the Twenty-second Annual Symposium on Principles of Distributed Computing. Boston: ACM Press, 2003.

[3] ASOKAN N, SCHUNTER M, WAIDNER M. Optimistic protocols for fair exchange[C]//Proceedings of the 4th ACM Conference on Computer and Communications Security. Zurich: ACM Press, 1997.

[4] ASOKAN N, SHOUP V, WAIDNER M. Optimistic fair exchange of digital signatures[J]. IEEE Journal on Selected Areas in Communications, 1999, 18(4): 593-610.

[5] BAO F, DENG R H, MAO W. Efficient and practical fair exchange protocols with off-line TTP[C]//Proceedings of the 19th IEEE Computer Society Symposium on Research in Security and Privacy. Oakland: IEEE Computer Press, 1998.

[6] 张青, 温巧燕. 一种新的公平交换协议[J]. 北京邮电大学学报, 2006, 29(5): 63-65.
ZHANG Qing, WEN Qiao-yan. A new fair-exchange protocol[J]. Journal of Beijing University of Posts and Telecommunications, 2006, 29(5): 63-65.

[7] EVEN S, GOLDREICH O, LEMPEL A. A randomized protocol for signing contracts[J]. Communications of the ACM, 1985, 28(6): 637-647.

[8] BEN-OR M, GOLDREICH O, MICALI S, et al. A fair protocol for signing contracts[J]. IEEE Transactions on Information Theory IT, 1990, 36(1): 40-46.

[9] DESMEDT Y. Some recent research aspects of threshold cryptography[C]//ISW 1997. Okamoto: Springer, 1997.

[10] DESMEDT Y, FRANKEL Y. Threshold cryptosystems[C]//CRYPTO 1989. Brassard: Springer, 1989.

[11] DESMEDT Y, FRANKEL Y. Shared generation of authenticators and signatures[C]//CRYPTO 1991. Feigenbaum: Springer, 1991.

[12] DESMEDT Y, FRANKEL Y. Homomorphic zero-knowledge threshold schemes over any finite abelian group[J]. SIAM Journal on Discrete Mathematics, 1994, 7(4): 667-679.

[13] SHOUP V. Practical threshold signatures[C]//Eurocrypt 2000. Preneel: Springer, 2000.

[14] ZHANG Xian-feng, ZHANG Feng, QIN Zhi-guang, et al. ECC based threshold decryption scheme and its application in web security[J]. Journal of Electronic Science and Technology of China, 2004, 2(4): 41-46.

编 辑 黄 莘