第 33 卷 第 1 期 计 算 机 工 程 2007 年 1 月
Vol.33 No.1 Computer Engineering January 2007
·博士论文· 文章编号：1000—3428(2007)01—0038—02 文献标识码：A 中图分类号：TN918.1

基于 Schnorr 数字签名和秘密分享的交换协议

辛向军[1,2]，李发根[3]，肖国镇[1]
(1. 西安电子科技大学综合业务网国家重点实验室，西安 710071；2. 郑州轻工业学院信息与计算科学系，郑州 450002；
3. 西安电子科技大学网络与信息安全重点实验室，西安 710071)

摘 要：通过在 Schnlorr 签名方案中利用秘密分享技术，给出了一种新的公平交易方案。该方案的公平性和安全性依赖于多个可信任第三方(TTP)。由协议的公平性和安全性分析可知，它比那些单纯地依赖于一个可信任第三方的公平交易方案具有更好的安全性和可靠性。
关键词：数字签名；公平交换协议；Schnorr 签名；电子商务

Exchange Protocol Based on Schnorr Signature Scheme and Secret Sharing

XIN Xiangjun[1,2], LI Fagen[3], XIAO Guozhen[1]
(1. State Key Lab of Integrated Service Networks, Xidian University, Xi'an 710071; 2. Dept. of Information and Computing Science, Zhengzhou University of Light Industry, Zhengzhou 450002; 3. Key Lab of Computer Network and Information Security, Xidian University, Xi'an 710071)

【Abstract】 By using the secret sharing technique in the Schnorr signature scheme, a new scheme of fair exchange protocol is proposed, whose fairness and security depend on two or more trusted third authorities. According to the security and fairness analysis of this protocol, compared with the fair exchange protocols that fully depend on only one TTP, the proposed protocol is more secure and reliable.
【Key words】 Digital signature; Fair exchange protocol; Schnorr signature; E-commerce

公平高效是电子商务的一个基本要求。公平交换协议使得交易双方以一种公平的方式交换物品，其结果是双方都得到或未得到对方的物品。目前，多数公平交换协议的公平性基于一个离线可信第三方(TTP)[1,2]。然而，在虚拟的网络世界中，没有任何一个计算机主体是可以完全可信和依赖的。例如，在文献[2]中，若交换双方(记为A和B)都未得到对方的签名，但B方具有包含A方签名的密文，则B可能通过一些特殊的方式(比如贿赂或威胁等)使得“可信第三方”与B“合谋”，即可信第三方在一些意外的情况下解密包含A方签名的密文，由此得出A的签名，并将A的签名发送给B，这样B便能得到A的签名而导致协议的不公平。然而，通过增加可信第三方的个数，可使交易双方不必单纯地依赖于某个可信第三方，从而使得协议具有更好的安全性和可依赖性。然而，据作者所知，还未发现依赖于多个可信第三方的公平交换协议方案。本文利用Schnorr签名方案[3]，给出了一个多个可信第三方公平交换协议方案。显然，此方案比单纯依赖于一个可信第三方的方案具备更好的安全性。

1 Schnorr 签名方案简要回顾

设p 和q为两个大素数，且$q|p-1$。令$g\in Z_p\backslash\{0\}$，且$g^q\equiv1 \bmod p$，并且在Z_p中计算离散对数是困难的。Alice随机选取整数$1<x<q-1$，并计算 $y=g^x \bmod p$。(g, x)与(g, y)分别为Alice的私钥和公钥。假定M为要签名的消息，H是公开的单向hash函数。Alice随机在Z_q选取k并计算$r=g^k \bmod p$和$s=k+xH(r||M) \bmod q$，则(r, s)便为Alice对消息M的签名。而签名(r, s)为M的有效签名，当且仅当$g^s\equiv ry^{H(r||M)} \bmod p$成立。

2 注册

在以后的叙述中总是假定 TA1、TA2 和客户(CU)之间通过一个安全的信道进行通信。

假定有两个可信任权威机构TA1 和TA2，而向TA1 和TA2 申请获得交易证书(TC)的客户称为CU。假定i=1 或 2，用$\mathrm{Sign}_{\mathrm{TA}i}(d_i,.)$表示TA$i$的签名算法，其中$d_i$为TA$i$的私钥；$\mathrm{Ver}_{\mathrm{TA}i}(e_i,.)$表示TA$i$签名的验证算法，其中$e_i$为TA$i$的公钥；$\mathrm{E}_{\mathrm{TA}i}(.)$表示TA$i$的安全的对称加密算法(e.g. DES)，$\mathrm{D}_{\mathrm{TA}i}(.)$表示其相应的解密算法 (e.g. DES)。假定CU的公钥和私钥和其他参数如同第 1 节的参数，下面给出CU向TA1 和TA2 注册的步骤：

(1)CU随机在Z_q中选取x_1并计算x_2使得$x_1+x_2\equiv x \bmod q$，于是CU将(p, q, g, y, x_1)和(p, q, g, y, x_2)分别秘密地发送给TA1 和TA2。

(2a)TA1 在自己的数据库中查询是否已经存在(p, q, g, y)。如已存在，则TA1 要求CU重新执行步骤 (1)；否则TA1 计算$y_1=g^{x_1} \bmod p$并广播(p, q, g, y, y_1)。

(2b)TA2 执行类似(2a)的数据库查询步骤，计算$y_2=g^{x_2} \bmod p$，并广播 (p, q, g, y, y_2)。

(3a)TA1 检查等式$y_1y_2\equiv y \bmod p$是否成立。如不成立，则TA1 广播一个注册错误并停止执行以下步骤；否则TA1 计算TC1＝$\mathrm{Sign}_{\mathrm{TA1}}(d_1, p||q||g||y||c_1)$，其中$c_1=\mathrm{E}_{\mathrm{TA1}}(x_1)$，并将TC1 和 c_1 秘密地发送给CU，将TA1 (p, q, g, y)存入自己的数据库中。

(3b)TA2 执行类似(3a)检查等式的步骤，并计算TC2＝$\mathrm{Sign}_{\mathrm{TA1}}(d_2, p||q||g||y||c_2)$，其中$c_2=\mathrm{E}_{\mathrm{TA1}}(x_2)$，并将TC2 和$c_2$秘密

基金项目：国家自然科学基金资助项目(60473028，90104005)；郑州轻工业学院基金资助项目（2006XXJ17）
作者简介：辛向军(1974－)，男，博士生，主研方向：数字签名；李发根，博士生；肖国镇，教授
收稿日期：2006-01-23 **E-mail：**xin_xiang_jun@tom.com

地发送给CU，同时TA2 将(p, q, g, y)存入自己的数据库。

在上述注册过程中，(2a)和(2b)可同时发生，(3a)和(3b)可同时发生。CU 通过上述的注册过程得到 TC=(TC1, TC2)，并将 TC 用作自己的交易证书。

3 注册的安全性分析

(1)由求解离散对数的困难性假设可知，TA1 推出x_2 和x是困难的，TA2 推出x_1 和 x是困难的，并且不可能出现多个用户共用一个(p, q, g, y)的情况。

(2)尽管CU掌握c_1和c_2及其相应的明文x_1和x_2，但CU很难由c_1和c_2及其相应的明文x_1和x_2推出TA1 和TA2 在对称加密算法中使用的密钥。由于不知道TA1(TA2)在对称加密算法中使用的密钥，任何人(TA1(TA2)和CU除外)不能由$c_1(c_2)$得到$x_1(x_2)$。同时，只有TA1 和TA2“合谋”时才能重构CU的秘密。然而，本文假定TA1 和TA2 都是可信的，且TA1 和TA2 同时“合谋”的概率很小。另外，注册过程中只有两个可信机构。事实上，可使用k个可信机构，而此时只有此k个可信机构同时“合谋”时才可能获得用户的秘密，这无疑增加了注册系统的安全和可靠性。

4 公平交换协议

假设Alice和Bob为协议中参与交换的双方，他们都产生类似于第 1 节的参数，并打算公平地交换对方对合同m的签名，且Alice和Bob都已经向TA1 和TA2 注册获得各自的交易证书。令(g, y_A)为Alice的公钥，其相应的私钥为(g, x_A)。TC_A为 Alice 的交易证书，其中$TC_A=(TC1_A,TC2_A)$，$TC1_A=\mathrm{Sign}_{TA1}(d_1,p||q||g||y_A||c_{A1})$，$TC2_A=\mathrm{Sign}_{TA2}(d_2, p||q||g||y_A||c_{A2})$。由第 2 节可知，$D_{TA1}(c_{A1})+D_{TA2}(c_{A2})\equiv x_A \bmod q$。令$(g, y_B)$为Bob的公钥，其相应的私钥为$(g, x_B)$。$TC_B$为Bob交易证书，其中$TC_B=(TC1_B,TC2_B)$，$TC1_B=\mathrm{Sign}_{TA1}(d_1, p||q||g||y_B||c_{B1})$，$TC2_B=\mathrm{Sign}_{TA2}(d_2,p||q||g||y_B||c_{B2})$。由第 2 节可知，$D_{TA1}(c_{B1})+D_{TA2}(c_{B2})\equiv x_B \bmod q$。用Encr(g, y_A, .)表示Alice的公开的非对称加密算法，其中(g, y_A)为Alice的公钥，其相应的解密算法为Decr(g, x_A, .)，其中(g, x_A)为Alice的私钥；而Encr(g, y_B, .)和Decr(g, x_B, .)的含义类似于Encr(g, y_A, .)和Decr(g, x_A, .)。假定Alice为协议中的开始执行者，下面给出协议的步骤：

(1)Alice 在Z_q 中随机选取k并计算$r=g^k \bmod p$和 $s=k+x_A H(r||u) \bmod q$，其中$u=$ Encr(g, y_B, m)，并将 $(g, y_A, TC_A, c_{A1}, c_{A2}, u, r, s)$发送给Bob。

(2)Bob验证$\mathrm{Ver}_{TA1}(e_1, p||q||g||y_A||c_{A1}, TC1_A)=true$，$\mathrm{Ver}_{TA2}(e_2, p||q||g||y_A||c_{A2}, TC2_A)=true$和$g^s\equiv r(y_A)^{H(r||u)} \bmod p$是否同时成立。如果满足，则Bob停止执行以下步骤；否则他解密计算$m=$Decr(g, x_B, u)，若Bob不同意交换对消息m的签名，则Bob停止执行以下步骤，否则Bob在Z_q 中随机选取k_B，并计算$r_B=g^{k_B} \bmod p$和$s_B=k_B+x_B H(r_B||m) \bmod q$，于是他将 $(g, y_B, TC_B, c_{B1}, c_{B2})$和$(r_B, s_B)$发送给Alice。

(3)Alice利用y_B、c_{B1}、c_{B2}、$TC1_B$和$TC2_B$执行类似步骤(2)的验证步骤(不同的是验证 $g^{s_B} \equiv r_B y_B^{H(r_B||m)} \bmod p$)，并在$Z_q$ 中随机选取k_A并计算 $r_A = g^{k_A} \bmod p$ 和 $s_A=k_A+x_A H(r_A||m) \bmod q$，并将$(r_A, s_A)$发送给Bob。

5 协议中纠纷的解决

若Alice在交换协议的步骤(3)得到Bob对消息m的签名，但她没有将自己对消息m的签名(r_A, s_A)发送给Bob，则Bob可以通过以下步骤得到Alice的关于消息m的数字签名：

(1)Bob将$(m, g, y_A, TC_A, c_{A1}, c_{A2}, y_B, TC_B, c_{B1}, c_{B2}, u, r, s, r_B, s_B)$和$u=$Encr$(g, y_B, m)$的证据Proof(证据产生办法见本节末尾注释)发送给TA1 和TA2。

(2a)TA1 验证$\mathrm{Ver}_{TA1}(e_1, p||q||g||y_i||c_{i1}, TC1_i)=true$，$\mathrm{Ver}_{TA2}(e_2, p||q||g||y_i||c_{i2}, TC2_i)=true$，其中的$i$=A或B，$g^s\equiv r(y_A)^{H(r||u)} \bmod p$，$g^{s_B} \equiv r_B y_B^{H(r_B||m)} \bmod p$ 以及$u=$Encr(g, y_B, m)的证据Proof是否同时成立(证据产生办法见本节末尾注释)。若不同时成立，则停止执行以下步骤；否则TA1 在 Z_q中随机选择k_1并计算$r_1=g^{k_1} \bmod p$，然后向TA2 广播r_1。

(2b)TA2 执行类似(2a)的验证步骤。若验证通过，TA2 在Z_q中随机选择k_2并计算$r_2=g^{k_2} \bmod p$，然后向TA1 广播r_2。

(3)TA1 计算$t=r_1 r_2 \bmod p$，$x_{A1}=D_{TA1}(c_{A1})$和$s_1=k_1+x_{A1}H(t||m) \bmod q$，并将$(t, s_1, r_B, s_B)$发送给Bob 和 Alice。同时，TA2 计算$t=r_1 r_2 \bmod p$，$x_{A2}=D_{TA2}(c_{A2})$和$s_2=k_2+x_{A2}H(t||m) \bmod q$，并将$(t, s_2, r_B, s_B)$发送给Bob和Alice。

这里(2a)和(2b)可同时发生。这样Bob可以得到Alice对m的签名(t,w)，其中$w=s_1+s_2 \bmod q$。容易验证$g^w\equiv t(y_A)^{H(t||m)} \bmod p$。

注释：假定利用Bob的公钥(g, y_B)对m的加密结果为$u=$Encr(g, y_B, m)。而加密算法采用的是ElGamal加密算法，即$u=(R, C)$。其中$R=g^t \bmod p$，$C=m(y_B)^t \bmod p$。Bob为了证明$u=$Encr(g,y_B,m)，他只需证明离散对数等式$x_B=\log_g(y_B)=\log_R(Cm^{-1})$成立即可。为此，Bob利用文献[4]中的密码工具签名等式(Signature of Equality)产生$x_B=\log_g(y_B)=\log_R(Cm^{-1})$证据$SEQDL(g, R, y_B, Cm^{-1}, m)$并将$SEQDL(g, R, y_B, Cm^{-1}, m)$发送给验证人即可。而$SEQDL(g, R, y_B, Cm^{-1}, m)$的具体产生和非交互式验证过程可参考文献[4]，此处不再赘述。

6 交换协议的安全性、公平性和效率分析

(1)在交换协议中，交换方通过出示自己合法的交换证书使得对方相信在出现纠纷时能够通过第 5 节中的方案解决纠纷。交换协议中若 Alice 获得了 Bob 的有效签名，但 Bob 未获得 Alice 的有效签名，则 Bob 可以通过第 5 节的方案得到 Alice 的签名。

(2)在第 5 节中 Bob 出示的(r, s)保证了 TA1 和 TA2 能对正确的消息 m 产生签名。只有 TA1 和 TA2“合谋”才能成功构造出 Alice 的对消息 m 的签名。然而，我们假定 TA1 和 TA2 都是可信的机构，且 TA1 和 TA2 同时遭到胁迫或接受贿赂的概率很小。因此，本文的方案具备更好的安全性和可依赖性。

(3)事实上，为增加方案的安全度，在第 2 节中可类似地设置 2 个以上的可信第三方。随着第三方的增加，协议中所有第三方“合谋”的概率就越小，系统的安全性和可靠性就会大大增加。但是，随着第三方的增加会对网络开销有一定的影响：用户在注册和解决纠纷过程中就需要与多个第三方通信，这无疑增加了通信量；同时，用户交易证书的比特长度以及协议中证书验证所需的计算量也会随着可信第三方的线性增加而成比例增加。因此，在应用中可根据实际安全需要和网络计算能力适当地选取第三方的个数。

7 结论

通过公平交换协议的参与方注册，首次引入多个可信任第三方的公平交换协议。协议纠纷的公平解决依赖于多个可信任机构的同时合作，这使得在虚幻的网络世界中能更为可靠地保证交换协议的公平性。

（下转第 46 页）