一种基于短签名和离线半可信第三方的公平交换协议

辛向军[1,2]，李发根[3]，肖国镇[1]

(1. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；2. 郑州轻工业学院 信息与计算科学系，河南 郑州 450002；3. 西安电子科技大学 教育部网络与信息安全重点实验室，陕西 西安 710071)

摘要：基于一个短签名方案和离散对数问题，给出了一种新的具有离线半可信第三方的公平交换协议. 协议中离线第三方只有在意外的情况下才介入协议，从而实现了公平交换的最优化. 离线第三方不必完全可信，因其在解决纠纷的同时并不能获得交换双方的签名. 由于基于短签名，所需存储和通讯的数据量小，故该协议适用于低带宽通信以及需要较小的数据存储量的环境.

关键词：短签名；数字签名；公平交换协议；电子商务

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1001-2400(2007)01-0092-04

A fair exchange protocol based on short signature with the off-line semi-trusted third party

XIN Xiang-jun[1,2], *LI Fa-gen*[3], *XIAO Guo-zhen*[1]

(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China; 2. Dept. of Information and Computing Science, Zhengzhou Univ. of Light Industry, Zhengzhou 450002, China; 3. Ministry of Edu. Key Lab. of Computer Networks and Information Security, Xidian Univ., Xi'an 710071, China)

Abstract: Based on a short signature scheme and discrete logarithm problem, a new fair exchange protocol with the off-line semi-Trusted Third Party (TTP) is proposed. The off-line semi-TTP intervenes into the protocol in case of trouble, which makes the fair exchange optimistic. The off-line TTP need not be completely trusted, since it can get neither signature exchanged when disputation is solved. Because this protocol is based on short signature, which needs low storage and little communication, it can be used in low-bandwidth communication and low-storage environments.

Key Words: short signature; digital signature; fair exchange protocol; E-commerce

电子商务是一种很重要的经济活动，而公平高效是它的基本要求. 公平交换协议使得交易双方以一种公平的方式交换双方的物品，交易的最终结果是要么交换双方都得到对方的物品，要么双方都未得到对方的物品. 许多公平交换协议的公平性(的保障)是基于一个离线可信第三方(TTP)[1~3]. 在公平交换协议中，若交换方中一方得到了对方的物品，而另外一个交换方未得到对方的物品，则出现了不公平的结果. 在此情况下，TTP 可解决纠纷使得交换双方都得到对方的物品. 然而，在解决纠纷的同时，TTP 也得到了交换双方中至少一方的物品，如在文[3]中 TTP 可得到交换双方的签名. 然而，这在实际生活中可能对交换双方带来不便. 比如，交换双方交换的是私人物品或者是电子商品. 因此，交换双方希望只有对方能够得到交换的物品，而并不希望 TTP 也能得到交换的物品.

短签名适用于低带宽通信以及需要较小的数据存储量的环境. 迄今为止，人们已经提出了许多短签名方案[4~7]. 笔者基于一个短签名方案[7]，给出了一种具有离线半可信第三方的、优化的公平交换协议. 该协议所需存储和通讯的数据量小，故其可用于低带宽通信以及需要较小的数据存储量的环境.

收稿日期：2006-03-23

基金项目：国家自然科学基金资助(60473028)；郑州轻工业学院基金资助(2006XJJ17)；国家信息安全重点实验室开放课题

作者简介：辛向军(1974-)，男，西安电子科技大学博士研究生.

1　预备知识

1.1　双线性对

令 G_1 和 G_2 分别为阶为 p(p 为一个大素数)加法循环群和乘法循环群. $e:G_1\times G_1\to G_2$ 为一个具有以下性质的双线性映射:

(1) **双线性**　对任意 $a,b\in Z_p$ 和 $R,S,T\in G_1$,成立 $e(aR,bS)=e(R,S)^{ab}$, $e(R+S,T)=e(R,T)\,e(S,T)$, $e(R,S+T)=e(R,S)\,e(R,T)$.

(2) **非退化性**　存在 $(R,S)\in G_1\times G_1$ 使得 $e(R,S)\neq I$,其中 I 表示 G_2 中的单位元.

(3) **可计算性**　对任意的 $(R,S)\in G_1\times G_1$,存在有效的多项式算法计算 $e(R,S)$.

1.2　一些基础问题

令 G_1 和 G_2 为 1.1 节所描述的群,P 为 G_1 的生成元,而 $a,b,c\in Z_p^*$.

定义 1　离散对数问题(DLP)　给定 (P,Q),其中 $Q\in G_1^*$,计算 a 使得 $aP=Q$.

定义 2　计算 Diffie-Hellman 问题(CDHP)　给定 P,aP,bP,计算 abP.

定义 3　判定 Diffie-Hellman 问题(DDHP)　给定 P,aP,bP,cP,判定 $c\stackrel{?}{\equiv}ab \bmod p$.

定义 4　k-合谋攻击问题(k-CAAP)　对于整数 $k,x\in Z_p$ 和 $P\in G_1$,给定$(P,Q=xP,h_1,\cdots,h_k\in Z_p, P/(h_1+x),\cdots,P/(h_k+x))$,计算$P/(h+x)$,其中$h\notin\{h_1,\cdots,h_k\}$[8].

1.3　公平交换协议所基于的短签名

这里简要回顾文献[7]的短签名方案(简称 ZSS 签名方案). 令参数 (G_1,G_2,P) 如同 1.2 节所述,m 为待签名的消息,$H:\{0,1\}^*\to Z_p^*$ 为一个公开的、抗碰撞的 hash 函数.

密钥生成:随机选取 $x\in Z_p^*$,计算 $P_{\text{pub}}=xP\in G_1$. 私钥为 x,其相应的公钥为 P_{pub}.

签名:计算 $s=(x+H(m))^{-1}P$. 这里$(x+H(m))^{-1}$ 是在有限域 Z_p 中计算的. s 即为消息 m 的签名.

验证:s 为消息 m 的有效签名当且仅当等式 $e(s,H(m)P+P_{\text{pub}})=e(P,P)$ 成立.

2　公平交换协议

假定系统公开参数 $\{G_1,G_2,P,p,H\}$ 及 m 如第 1 节所述. 始终假定在 G_1 中求解 CDHP、DLP 和 k-CAAP 是困难的,而求解 DDHP 问题是容易的. 令 A 和 B 分别为参与公平交换协议的交换双方;C 为半可信第三方(Semi-TTP),它在协议中作为仲裁保证协议的公平性;$x_L\in Z_p^*$ 和 $y_L=x_LP$ 分别为 L 的私钥和公钥,而 L 可以为 A,B,C. 假设 A 和 B 打算公平地交换对方对合同 m 的 ZSS 签名,A 为交换协议的发起方. 交换协议的步骤如下:

(1) B 计算 $y_{B,C}=x_By_C$,并将 $y_{B,C}$ 发送给 A.

(2) A 根据公钥 y_B 和 y_C 判定 $y_{B,C}$ 是否正确(即验证 $e(y_B,y_C)=e(y_{B,C},P)$ 是否成立). 若 $y_{B,C}$ 正确,则 A 计算$t_A=(x_A+H(m))^{-1}y_{B,C}$,并将 t_A 发送给 B;否则中止协议.

(3) B 验证 $e(t_A,y_A+H(m)P)=e(y_{B,C},P)$ 是否成立. 如果成立,B 计算 $s_B=(x_B+H(m))^{-1}P$,并将自己的 ZSS 签名 s_B 发送给 A;否则中止协议.

(4) A 验证 $e(s_B,y_B+H(m)P)=e(P,P)$ 是否成立. 若成立,A 计算 $s_A=(x_A+H(m))^{-1}P$ 并将自己的 ZSS 签名 s_A 发送给 B.

在交换协议的步骤(3)和(4)中,为保证 t_A,s_A 和 s_B 不被敌手截获,可采用加密措施发送 t_A,s_A 和 s_B. 交换协议中至多交换的数据量为 $4|P|$ 比特,而协议成功完成后 A 和 B 分别需要存贮的数据量仅为 $|P|$ 比特(即 A 和 B 只需存贮对方的 ZSS 签名即可),其中 $|P|$ 表示 P 的二进制长度.

3　协议的安全性分析

由双线性对的性质、s_L 及 ZSS 签名的产生过程易证下面定理 1 与定理 2 成立.

定理 1 协议中若 $t_A = (x_A + H(m))^{-1} y_{B,C}$，则下式总是成立：

$$e(t_A, y_A + H(m)P) = e(y_{B,C}, P) \quad . \tag{1}$$

定理 2 协议中 s_L 为 L 的关于消息 m 的 ZSS 签名，其中 $L = A$ 或 B.

定理 3 在不知道密钥 x_A 的情况下伪造 A 的关于消息 m^* 的 t_A^* 使得

$$e(t_A^*, y_A + H(m^*)P) = e(y_{B,C}, P) \tag{2}$$

式成立是困难的，其中 $y_{B,C} = x_B y_C = x_C y_B$.

证明 考虑 4 种敌手：(1) 第 1 种敌手仅获得公开参数(即 $G_1, G_2, P, p, H, y_A, y_B, y_C$)；(2) 第 2 种敌手不仅获得了公开参数，而且获得了 $y_{B,C}$ 和 B 的私钥 x_B；(3) 第 3 种敌手不仅获得了公开参数，而且获得了 $y_{B,C}$ 和 C 的私钥 x_C；(4) 第 4 种敌手不仅获得了公开参数，而且获得了 $y_{B,C}$，B 的私钥 x_B 和 C 的私钥 x_C. 显然，在这 4 种敌手中第 4 种敌手攻击力最强. 故只需证明 t_A^* 在第 4 种敌手攻击下是安全的(即不可伪造 t_A^*，使得 t_A^* 满足式(2)) 即可. 称第 4 种敌手为 A_d. 若敌手 A_d 可在多项式时间内以不可忽略的概率伪造一个 t_A^* 使得式(2) 成立，则 A_d 可计算 ZSS 签名 $s_A^* = (x_B x_C)^{-1} t_A^*$. 即 A_d 可在多项式时间内以一个不可忽略的概率伪造 A 的一个 ZSS 签名. 然而，由文[7]知，在 k-CAAP 困难假设下 ZSS 签名在预言机下是安全的，故在不知密钥 x_A 的情况下伪造 t_A^* 使得式(2)成立是困难的.

定理 4 只有 C 和 B(而且 C 和 B 必须合作) 才可以从第 2 节的协议中由合法的 t_A(即 t_A 满足式(1)) 有效地得到 A 的关于消息 m 的 ZSS 签名 s_A.

证明 假定敌手 A_{d1} 仅知道公开参数(即 $G_1, G_2, P, p, H, y_A, y_B, y_C$) 和 $y_{B,C}$；敌手 A_{d2} 不仅知道公开参数和 $y_{B,C}$，而且知道 B 的私钥；敌手 A_{d3} 不仅知道公开参数和 $y_{B,C}$，而且知道 C 的私钥. 所有敌手的最终目的是获得 s_A. 然而，由文[7] 可知，在 k-CAAP 困难假设下所有敌手(他们都不知道 A 的私钥) 直接伪造 s_A 是困难的，因此，所有的敌手试图由 t_A 推出 s_A. 事实上，由式(1) 及双线性对的性质和 ZSS 签名 s_A 的验证过程可知 $s_A = (x_C x_B)^{-1} t_A$. 因此，为了由 t_A 得到 s_A，敌手须知道 $(x_C x_B)^{-1}$. 然而，由 DLP 假设可知，A_{d1} 由 $y_{B,C}$ 计算出 $x_C x_B$ 是困难的，A_{d2} 由 y_C 计算出 x_C 是困难的，A_{d3} 由 y_B 计算出 x_B 是困难的. 由以上论述可知任何人都不能有效地由 t_A 得到 s_A，并且单独的 C 或 B 也不能有效地由 t_A 推出 s_A. 但是，若 C 和 B 合作，则很容易由 t_A 推出 s_A. C 和 B 可合作如下：(1) B 将合法的 t_A(即 t_A 满足式(1)) 发送给 C；(2) C 计算出 $y_{B,C} = x_C y_B$，并验证 t_A 是否满足式(1)，若满足，则 C 计算 $D_1 = x_C^{-1} t_A$ 并将 D_1 发送给 B；(2) B 计算 $D_2 = x_B^{-1} D_1$. 由以上的步骤(1) 和 (2) 以及 ZSS 签名的验证过程可知 $D_2 = s_A$.

交换协议的最终结果只可能有 3 种情况：(1) A 和 B 都未得到对方的 ZSS 签名；(2) A 得到了 B 的 ZSS 签名，B 未得到 A 的 ZSS 签名，但 B 得到了 A 的合法的 t_A(即 t_A 满足式(1))；(3) A 和 B 都得到对方的 ZSS 签名. 对于第 2 种情况，可执行下节的解决方案，保证协议的公平性.

4 协议中纠纷的解决

4.1 纠纷解决方案

假定 C，A 和 B 通过一个安全的信道通信 (例如通过公钥和对称密码系统保证数据的保密性和数据完整性)，他们通过以下步骤解决纠纷：

(1) B 计算 $e_B = (x_B + H(m))^{-1} y_A$，然后将 e_B 和 t_A 发送给 C.

(2) C 接到 e_B 和 t_A 后验证式(1)和下式是否同时成立：

$$e(e_B, y_B + H(m)P) = e(y_A, P) \quad , \tag{3}$$

若同时成立，则执行以下步骤；否则中止.

(3) C 计算 $D_1 = x_C^{-1} t_A$ 并将 D_1 发送给 B；同时，C 将 e_B 发送给 A.

由定理 4 可知 B 和 A 可分别计算 $D_2 = x_B^{-1} D_1$ 和 $D_3 = x_A^{-1} e_B$ 得到对方的 ZSS 签名，从而保证了协议的公平性，同时 C 并未获得 A 和 B 的 ZSS 签名. 另外，在纠纷解决方案中至多交换的数据量为 $4|P|$ 比特，其中 $|P|$ 表示 P 的二进制长度. 纠纷解决方案执行完毕后 A 和 B 需要存储的数据量皆为 $|P|$ 比特.

4.2 纠纷解决方案的公平性和安全性分析

利用类似于定理 1、定理 3、定理 4 的证明，易证下面的定理 5～7 及推论 1 成立.

定理 5　纠纷解决方案中若 $e_B = (x_B + H(m))^{-1} y_A$, 则式(3)总是成立.

定理 6　在 4.1 节中 D_2 和 D_3 分别为由 A 和 B 签署的关于消息 m 的 ZSS 签名.

推论 1　在纠纷解决方案中 B 伪造 A 的关于消息 m^* 的 t_A^* 使得式(2)成立是困难的.

定理 7　在纠纷解决方案中,伪造 B 的关于消息 m^* 的 e_B^* 使得 $e(e_B^*, y_B + H(m^*)P) = e(y_A, P)$ 成立是困难的.

定理 8　在纠纷解决方案中,第三方 C 由合法的数据 e_B(即 e_B 满足式(3))和合法的数据 t_A(即 t_A 满足式(1))得到 A 和 B 的关于消息 m 的 ZSS 签名是困难的.

证明　若 k-CAAP 困难,则由文[7]可知 C 直接伪造 A 或 B 的 ZSS 签名是困难的. 由定理 4 的证明可知单独的 C 由 t_A 得到 A 的关于消息 m 的 ZSS 签名是困难的,但 B 却可通过解密由 C 提供数据 $D_1 (= x_C^{-1} t_A)$(即计算 $D_2 = x_B^{-1} D_1$)得到 A 的关于消息 m 的 ZSS 签名. 现在证明在 k-CAAP 困难假设下,第三方 C 由 e_B 得到 B 的关于消息 m 的 ZSS 签名是困难的. 事实上,由式(3)可知 $e(e_B, y_B + H(m)P) = e(P, P)^{x_A}$,由双线性、非退化性、$s_B$ 的验证过程以及上式可知 $s_B = (x_A)^{-1} e_B$. 因此,为了由 e_B 得到 s_B,第三方 C 须知道 $(x_A)^{-1}$,即敌手须知道 x_A. 然而,由 DLP 假设可知 C 由 y_A 计算出 x_A 是困难的. 因此,在 DLP 和 k-CAAP 困难假设下,C 由合法的数据 e_B 和 t_A 得到 A 和 B 的关于消息 m 的 ZSS 签名是困难的.

5　结 束 语

通过利用 ZSS 短签名方案,给出了一个基于短签名的公平交换协议. 在 DLP 问题和 k-CAAP 假设下半可信第三方可有效地解决纠纷以保证协议的公平性,且半可信第三方在解决纠纷的同时并不能获得交换双方的签名. 由于基于短签名,交换协议所需的数据通信量和存储量小,故该协议适用于低带宽通信以及需要较小的数据存储量的环境.

参考文献:

[1] Bao F, Deng R H, Mao W. Efficient and Practical Fair Exchange Protocols with Off-line TTP [C]//Proc of the 1998 IEEE Symp on Security and Privacy. Oakland: IEEE Computer Press, 1998: 77-85.

[2] Boyd C, Foo E. Off-Line Fair Payment Protocols Using Convertible Signatures [C]//Advances in Cryptology (ASIACRYPT'98). Beijing: Springer-Verlag, 1998: 271-285.

[3] 周永彬, 张振峰, 卿斯汉, 等. 基于 RSA 签名的优化公平交换协议[J]. 软件学报, 2004, 15(7): 1049-1055.

[4] Granboulan L. Short Signatures in the Random Oracle Model [C]//ASIACRYPT 2002. Berlin: Springer-Verlag, 2002: 364-378.

[5] Boneh D, Lynn B, Shacham H. Short Signature from the Weil Pairing [C]//Proceeding of Asiacrypt'01. Berlin: Springer-Verlag, 2001: 514-532.

[6] Huang Xinyi, Mu Yi, Susilo W, et al. A Short Proxy Signature Scheme: Efficient Authentication in the Ubiquitous World [C]// EUC Workshops 2005. Berlin: Springer-Verlag, 2005: 480-489.

[7] Zhang Fangguo, Safavi-Naini R, Susilo W. An Efficient Signature Scheme from Bilinear Pairings and Its Applications [C]//PKC 2004. Berlin: Springer-Verlag, 2004: 277-290.

[8] Mitsunari S, Sakai R, Kasahara M. A New Traitor Tracing [J]. IEICE Trans, 2002, E85-A (2): 481-484.

(编辑: 郭　华)