基于公开可验证秘密分享的公平合同签署协议

刘文远 张 爽 张江霄
(燕山大学信息科学与工程学院 秦皇岛 066004)

摘 要 通过引入 n 个离线半可信第三方提出一种新的公平合同签署协议。该协议利用公开可验证秘密分享(PVSS)原理,不仅实现了签名者隐私的保护,还有效地降低了签名者中的一方与离线半可信第三方合谋来获取另一方签名的概率,从而使得合同签署协议具有更好的公平性。另外,本协议还通过利用多重签名技术,使签名者最终获得同时包含双方签名的合同,这是传统纸质合同的显著特点,因此提出的协议具有一定的实用性。

关键词 Schnorr 签名,公开可验证秘密分享(PVSS),(t,n)门限,合谋

Fair Contract Signing Protocol Based on Publicly Verifiable Secret Sharing

LIU Wen-yuan ZHANG Shuang ZHANG Jiang-xiao
(Information Science and Engineering Institute, Yanshan University, Qinhuangdao 066004, China)

Abstract Through introducing n off-line semi-trusted third parties, a new fair contract signing protocol was proposed. This protocol uses publicly verifiable secret sharing(PVSS) principle not only to realize the signers' privacy protection, but also reduce probability that one party conspires with off-line semi-trusted third parties to gain another party's signature, thus causes the contract signing protocol to have a better fairness. Moreover, the protocol also through the use of multiple signature technology, causes the signers to obtain finally the contract which contains both party's signatures. Of course, that is the outstanding feature of traditional paper contract. Therefore, the protocol proposed in this article has certain usability.

Keywords Schnorr-signature, Publicly verifiable secret sharing, (t,n) threshold, Conspiracy

1 引言

随着计算机网络的飞速发展,如何进行网上公平交易成为研究的热点。公平合同签署是公平交易的一种,公平合同签署协议实质上就是双方公平的交换对合同的签名。为了实现公平交换,引入了离线的可信第三方(off-line TTP)[1]。不幸的是,这种交换协议具有两个严重的缺点:第一,当离线可信第三方解决纠纷时,可以获得交换双方所交换的秘密,这样就存在着安全隐患,使得交换双方处于不利的地位。第二,把第三方看成是完全可信的,并认为他不会和交易双方中的任一方合谋。而事实上,可信第三方有可能与一方合谋揭示交换秘密,使另一方处于不公平的状态。

1997年,Franklin 和 Reiter[2] 首次提出了半可信第三方(STTP)的概念,其特点在于除非交易双方主动把秘密告诉第三方,否则 STTP 不可能知道双方交换的秘密。但是 STTP 是在线的,因此容易成为系统性能的瓶颈。2001年,蒋晓宁等人在文献[3]中,基于公开可验证秘密分享原理(PVSS)[4]提出了具有离线半可信第三方的公平交易协议,该协议是对文献[2]的改进,不仅半可信第三方离线工作,大大降低了通信量,而且保护了交换的秘密。但该协议没有考虑参与交易的一方和半可信第三方的合谋问题。2006年,WANG Chih-Hung 和 YIN Chih-Heng[5] 提出的公平合同签署协议除了具有文献[3]的性质外,还具有许多新的性质,但该协议仍然没有解决合谋问题。

本文针对这种交换协议的两个缺点,利用变形的 Schnorr 签名方案[6]、公开可验证秘密分享原理[4]和离线的(t,n)门限半可信第三方方案提出了一个新的公平合同签署协议。该协议不仅保护了交换的秘密,而且降低了合谋的可能性,并具有传统纸质合同的特点,因此更具实用性。

2 预备知识

2.1 Schnorr 签名方案

假设 $G=Z_P^*$,其中 p 是大素数,$p-1$ 有一大素数因子 q,g 是 Z_P^* 的阶为 q 的子群 G_q 的生成员。任选 $x\in_R Z_q$,计算 $y=g^x \bmod p$。在 Schnorr 签名方案中,x 为私钥,p,q,g,y 构成公钥。签名时,签名者任选 $r\in_R Z_q$,计算 $z=cx+r$,其中 $c=H(g^r,m)\in Z_q$,H 为 Hash 函数,签名为(c,z)。验证时,验证者检查等式 $c=H(g^z h^{-c},m)$是否成立。

2.2 公开可验证秘密分享(PVSS)

秘密的持有者随机选择 $c_j\in Z_q$,$j=1,\cdots,t-1$,公布 $V=$

到稿日期:2008-04-01 本文受国家科技部高新技术计划项目(2005EJ000017),国家电子信息发展基金及河北省信息产业发展计划项目(2005035025),河北省自然科学基金(F2005000368)资助。

刘文远(1968—),男,博士生导师,研究方向为电子商务、信息安全、智能计算;张 爽(1982—),女,硕士研究生,研究方向为电子商务、信息安全、密码学;张江霄 男,硕士研究生,研究方向为电子商务、信息安全。

$g^s \bmod p$ 和所有的 $L_j=g^{c_j} \bmod p$，其中 $s\in Z_q$ 是要分享的秘密。秘密持有者给每个分享秘密的参与者 U_i 安全地发送一份秘密的分享值 $s_i=s+\sum_{j=1}^{t-1}c_j d_i^j \pmod q$。对每个 U_i 来说，$d_i\in Z_q, d_i\neq 0$ 是个公开值。为了公开验证，秘密持有者对每份秘密分享值进行加密 $E_{PK_i}(s_i), i=1,\cdots,n$，其中 PK_i 为与 U_i 相对应的加密公钥。并公布 $E_{PK_i}(s_i), i=1,\cdots,n$。$v_i(=g^{s_i} \bmod p)$和 VEDL 的证明 $\text{Proof}_{VEDL}(E_{PK_I}(s_i), PK_i, v_i)$情况见本文 2.4 节。对每份秘密分享值的验证就是检验 $v_i=V\prod_{j=1}^{t-1}L_j^{(d_i^j)} \pmod p, i=1,\cdots,n$ 是否成立，以及 VEDL 的证据是否被正确地创建(详细情况见文献[4])。

2.3 具有可验证性质的单向函数

单向函数 f 的定义如下：$f: Z_q^* \to Z_p^*$，$f(a)=g^a \bmod p$。f 的可验证性和一个可计算的函数 F 有关。F 的定义如下：$F: Z_q^* \times Z_p^* \to Z_p^*$，$F(a,b)=b^a$，因此有 $F(a,f(b))=f(a.b)=f(b.a)=F(b,f(a))$(详细情况见文献[2])。

2.4 离散对数的可验证加密(VEDL)

设 U_P 是一证明者，U_V 是一验证者。U_P 可以向 U_V 证明密文 C 是对消息 m 的加密，而又不泄露消息 m。U_P 向 U_V 出示证据 $\text{Proof}_{VEDL}(C, PK, f(m))$，此证据可以证明 C 确实是对消息 m 的加密。其中 PK 表示加密公钥，如 $C=E_{PK}(m)$，$f()$表示一个认证的单向函数(详细情况见文献[4])。

2.5 两个离散对数相等的证明(PEDL)

令 p,q 的定义如上，$g_1\in Z_p, g_2\in Z_p$ 是阶为 q 的群 G_q 的两个元素。拥有秘密 $x\in Z_q^*$ 的证明者可以创建一个 PEDL，证明 y_1, y_2 具有相同的离散对数，而又不泄露秘密 x 的值。如 $\log_{g1}^{y1}=\log_{g2}^{y2}=x \pmod p$，PEDL 可以表示为 $\text{Proof}_{PEDL}(g_1, g_2, y_1, y_2)$(详细情况见文献[7])。

3 新协议

假设公平电子合同签署协议的用户为 U_A 和 U_B。$\text{STTP}_i (i=1,\cdots,n)$为解决协议纠纷的 n 个半可信第三方。协议中用到的(y_A, x_A)，(y_B, x_B)分别为 U_A 和 U_B 进行签名和验证的公私钥对，其中 $y_i=g^{x_i} \bmod p, i=A,B$。$(PK_A, SK_A)$，$(PK_B, SK_B)$，$(PK_{Ti}, SK_{Ti})$分别为 $U_A, U_B, \text{STTP}_i (i=1,\cdots,n)$加密解密的公私钥对。

协议的基本思想：由 PVSS 原理知，只要 t 个以上的 STTP 合作就可以恢复被分享的秘密。为了防止交换签名的泄露，本协议要求 U_A 先对要交换的签名进行划分，然后再对部分签名应用 PVSS。这样一来，只要不与 U_A 或 U_B 合谋，即使有 t 个以上的 STTP 合作也只能恢复出部分签名，从而保护了签名者的隐私。另外由于 U_B 只有 U_A 的部分签名，如果他想通过合谋来获得另一部分签名，由 PVSS 可知，只有 t 个以上的 STTP 同时愿意和他合谋才能成功，而这种可能性是很小的。

3.1 正常子协议

Step1 U_A 和 U_B 分别随机地选择 $r_A\in Z_q^*$，$r_B\in Z_q^*$。U_A 发送 $R_A=g^{r_A} \pmod p$给 U_B，同时 U_B 发送 $R_B=g^{r_B} \pmod p$给 U_A。

Step2 U_A 计算对合同 m 的签名 (c, z_A)，其中 $c=H(R_A.R_B, h(m))$，$z_A=c.x_A+r_A \pmod q$，H 和 h 是两个单向抵抗碰撞的哈希函数，x_A 是 U_A 的私钥。

Step3 U_A 随机地选择 $a_i\in Z_q^*$，并计算 $a_2=z_A a_1^{-1} \bmod q$。U_A 再根据 PVSS 原理把 a_1 划分成 n 份(每份用 a_{1i}表示)，$a_{1i}=a_1+\sum_{j=1}^{t-1}c_{Aj}d_{Ai}^j \bmod q, i=1,\cdots,n$。公布 $L_{Aj}=g^{c_{Aj}} \bmod p$，$j=1,\cdots,t-1$，$f(a_1)=g^{a_1} \bmod p$，$v_{Ai}=g^{a_{1i}} \bmod p$，$E_{PK_{T_i}}(a_{1i})$和 $\text{Proof}_{VEDL}(E_{PK_{T_i}}(a_{1i}), PK_{T_i}, v_{Ai}), i=1,\cdots,n$。最后 U_A 向 U_B 发送信息 $f(z_A)$，$Sig_{x_A}(c||f(z_A))$和 a_2。

Step4 U_B 计算 $c=H(R_A.R_B, h(m))$，验证等式 $R_A=f(z_A)y_A^{-c} \pmod p$，$F(a_2, f(a_1))=f(z_A)$是否成立。若都成立，$U_B$ 再验证 $v_{Ai}=f(a_1)\prod_{j=1}^{t-1}L_{Aj}^{(d_{Ai}^j)} \pmod p, i=1,\cdots,n$ 是否成立，$\text{Proof}_{VEDL}(E_{PK_{T_i}}(a_{1i}), PK_{T_i}, v_{Ai}), i=1,\cdots,n$ 是否被正确地创建，以及 $Sig_{x_A}(c||f(z_A))$的有效性。如果上述验证都通过，U_B 就把他对合同 m 的签名 z_B 发送给 U_A，否则 U_B 拒绝继续执行协议。

Step5 U_A 验证 $R_B=f(z_B)y_B^{-c} \pmod p$是否成立。如果成立，$U_A$ 向 U_B 发送自己的签名 z_A。

3.2 解决纠纷子协议

在 Step5 可能会产生争议。U_B 在 Step4 把自己对合同的签名 z_B 发送给 U_A，但并没有收到来自 U_A 的有效签名 z_A。这时 U_B 就会求助于 $\text{STTP}_i (i=1,\cdots,n)$，以获得有效的 z_A。

Step6 U_B 随机选择 $b_1\in Z_q *$，并计算 $b_2=z_B b_1^{-1} \bmod q$，同样根据 PVSS 原理把 b_1 分成 n 份，计算 $b_{1i}=b_1+\sum_{j=1}^{t-1}c_{Bj}d_{Bi}^j \bmod q, i=1,\cdots,n$，然后计算并公布下列信息：$E_{PK_A}(b_2)$，$f(b_2)=g^{b_2} \bmod p$，$\text{Proof}_{VEDL}(E_{PK_A}(b_2), PK_A, f(b_2))$，$f(b_1)=g^{b_1} \bmod p$，$L_{Bj}=g^{c_{Bj}} \bmod p, j=1,\cdots,t-1$，$v_{Bi}=g^{b_{1i}} \bmod p, i=1,\cdots,n$，$E_{PK_{Ti}}(b_{1i}), i=1,\cdots,n$，$\text{Proof}_{VEDL}(E_{PK_{To}}(b_{1i}), PK_{Ti}, v_{Bi}), i=1,\cdots,n$。

Step7 U_B 把从 U_A 接收到的 $E_{PK_{T_i}}(a_{1i})$和他的部分签名的秘密分享值 b_{1i}发送给 STTP_i。为了进一步验证还要把 $f(z_A), f(z_B), f(a_2), c, h(m), \text{Proof}_{PEDL}(g, f(a_1), f(a_2), f(s_A))$，$\text{Proof}_{PEDL}(g, f(b_1), f(b_2), f(z_B))$ and $Sig_{x_A}(c||f(z_A))$发送给 STTP_i。

Step8 STTP_i 计算 $R_A'=f(z_A)y_A^{-c} \pmod p$，$R_B'=f(z_B)y_B^{-c} \pmod p$，验证 $Sig_{x_A}(H(R_A'.R_B', h(m))||f(z_A))$是否有效。如果是有效签名则 STTP_i 解密 $E_{PK_{T_i}}(a_{1i})$，并验证下列消息是否被正确地创建：$g^{a_{1i}}=v_{Ai} \bmod p$，$g^{b_{1i}}=v_{Bi} \bmod p$，$\text{Proof}_{PEDL}(g, f(a_1), f(a_2), f(z_A))$，$\text{Proof}_{PEDL}(g, f(b_1), f(b_2), f(z_B))$，$v_{Ai}=f(a_1)\prod_{j=1}^{t-1}L_{Aj}^{(d_{Ai}^j)} \pmod p, i=1,\cdots,n$，$v_{Bi}=f(b_1)\prod_{j=1}^{t-1}L_{Bj}^{(d_{Bi}^j)} \pmod p, i=1,\cdots,n$，$\text{Proof}_{VEDL}(E_{PK_{Ti}}(a_{1i}), PK_{Ti}, v_{Ai}), i=1,\cdots,n$，$\text{Proof}_{VEDL}(E_{PK_{T_i}}(b_{1i}), PK_{Ti}, v_{Bi}), i=1,\cdots,n$，$\text{Proof}_{VEDL}(E_{PK_A}(b_2), PK_A, f(b_2))$。如果上述验证都成立，则 STTP_i 把 a_{1i}发送给 U_B，同时也把 b_{1i}发送给 U_A。由 PVSS 原理知，纠纷子协议结束后双方都能获得对方的签名。

4 新协议的分析

4.1 公平性

公平性分析可以分为如下 3 种情形(未考虑合谋)：

(1)U_A 和 U_B 都诚实地执行该新协议，最终双方都获得了对方对合同的签名，实现了公平性。

(2)U_B 诚实，而 U_A 是不诚实的，没有遵守新协议。如果 U_A 想通过发送不正确的证明来欺骗 U_B，由于 VEDL[4] 的安全性，U_B 可以检测出这种欺骗。如果 U_A 在 Step3 发送了有效的消息，但在 Step5 拒绝把他的有效签名发送给 U_B，这时 U_B 可以要求所有的 STTP 去解决这次纠纷。若至少 t 个 STTP 返回了有效的 a_{1i}，根据 PVSS 的安全性，就可以恢复出真正的秘密 a_1，从而得到 U_A 的签名。这种情况也保证了协议的公平性。

(3)U_A 诚实，而 U_B 没有诚实的遵守协议。当在 Step4 中发送无效的签名 z_B' 给 U_A 时，U_A 可以检测出来并拒绝向 U_B 发送签名 z_A，以达到公平。另外，若 U_B 在 Step3 中收到 U_A 的消息后直接执行解决纠纷子协议，此时要求 U_B 向每个 $STTP_i$ 发送 b_{1i} 和 $E_{PK_{T_i}}(a_{1i})$，如果至少有 t 个 $STTP_i$ 诚实地验证了 b_{1i} 和 a_{1i}，并按照协议把它们分别发送给 U_A 和 U_B，则新协议仍能实现公平性。

分析表明：协议结束时，要么 U_A 和 U_B 都得到了对方对合同的签名，要么 U_A 和 U_B 都没有得到对方的签名，协议保证了双方的公平性。

4.2 保密性

在解决纠纷子协议中，由于每个 STTP 解密得到的只是部分签名的分享值，因此即使有 t 个以上的 STTP 是不诚实的，他们相互合作恢复出来的也只是对合同的部分签名，并不能由此而得出对合同的完整签名。因此在整个交易过程中，双方交换的签名对 STTP 始终是保密的。

4.3 抗合谋性

如果 U_B 想获得 U_A 的签名 z_A，但又不想向 U_A 泄露自己的签名，他可以通过与 STTP 合谋来实现这个目的。由 PVSS 可知，U_B 必须和至少 t 个 STTP 合谋才能得到 a_1 进而求出 z_A，但是 t 个以上的 STTP 与 U_B 同时合谋的概率是很小的。PVSS 增加了用户和 STTP 合谋的难度，因此该新协议从一定程度上来说是抗合谋的。为了保证新协议在可能发生合谋的情况下仍然具有公平性，要求 $\left\lfloor \frac{n}{2} \right\rfloor + 1 \leqslant t \leqslant$ 诚实 STTP 的个数。

4.4 签名的完全性

在协议结束的时候，U_A 收到 U_B 对合同的签名 (c, z_B)，U_B 也收到 U_A 的签名 (c, z_A)。如果两个签名都是有效的签名，U_A 和 U_B 可以分别计算对合同的一个完全签名 $(c, z = z_A + z_B \pmod p)$。最终 U_A 和 U_B 都得到了包含双方签名的合同，使得新协议具有传统纸质合同的特点，因此具有一定的实用性。

4.5 安全性

该协议所具有的各种性质基于 VEDL 的安全性、PVSS 的安全性和离散对数难解问题。VEDL 和 PVSS 的安全性阻止了 U_A 的各种恶意行为，而离散对数难解问题也阻止了 U_B 想对该协议进行的各种攻击。另外，本文方案的安全性还取决于 Schnorr 签名的安全性和 Hash 函数的安全性。离线的 (t,n) 门限半可信第三方的引入使得该协议具有更好的安全性和可依赖性。

结束语 该协议通过引入 n 个半可信第三方，实现了签名者隐私的保密，大大降低了合谋的可能性，还具有传统纸质合同的特点，因此具有一定的实用性。但同时也增加了协议的复杂性和通信量，应该根据实际情况来确定协议中 t 和 n 的个数。多方公平合同签署协议是今后将要进一步研究的问题。

参 考 文 献

[1] Asokan N, Shoup V, Wander M. Optimistic Fair Exchange of Digital Signatures // Advances in Cryptology. Proceedings of EUROCRYPT 98. LNCS1403. Berlin: Springer-Verlag, 1998: 591-606

[2] Franklin M K, Reiter M K. Fair Exchange with a Semi-trusted Third Party[C] // Proc. of 4th ACM Conf. on Computer and Communication Security. Zurich, ACM Press, 1997: 1-5

[3] 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[J]. 计算机研究与发展，2001，38(4)：502-508

[4] Stadler M. Publicly Verifiable Secret Sharing[C]// Advances in Cryptology, EUROCRYPT'96. Berlin: Springer-Verlag, 1996: 190-199

[5] Wang C H, Yin C H. Practical Implementations of a Non-disclosure Fair Contract Signing Protocol. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2006, E89-A(1): 297-309

[6] Schnorr C P. Efficient Signature Generation for Smart Cards [J]. Journal of Cryptology, 1991, 4(3): 161-174

[7] Chaum D. Zero-knowledge Undeniable Signatures // Advances in Cryptology. Proc of EUROCRYPT'90. Lecture Notes in Computer Science(LNCS), 473. Springer-Verlag, 1998: 458-464

(上接第 106 页)

[12] Yuan W, Guan D, Lee S, et al. A dynamic trust model based on naive bayes classifier for ubiquitous environments // Proceedings of the 2006 International Conference on High Performance Computing and Communications (HPCC-06). Munich, Germany, September 2006: 562-571

[13] Giang P D, Hung L X, Lee S, et al. A flexible trust-based access control mechanism for security and privacy enhancement in ubiquitous systems // Proceedings of the International Conference on Multimedia and Ubiquitous. Seoul, Korea, April 2007: 698-703

[14] Yuan W, Guan D, Lee S, et al. Using reputation system in ubiquitous healthcare // Proceedings of the 9th IEEE International Conference on e-Health Networking, Application & Services (Healthcom 2007). Taipei, China, June 2007: 182-186

[15] Jameel H, Hung L X, Kalim U, et al. A trust model for ubiquitous systems based on vectors of trust values // Proceedings of the Seventh IEEE International Symposium on Multimedia (ISM'05). Irvine, California, USA, December 2005: 674-679

[16] Sharmin M, Ahamed S I, Ahmed S, et al. SSRD+: A privacy-aware trust and security model for resource discovery in pervasive computing environment // Proceedings of the 30th Annual International Computer Software and Applications Conference (COMPSAC 2006). Chicago, USA, September 2006: 67-70