无强迫的最优合同签署方案

陈晓峰[1], 王继林[2], 王育民[1]
(1. 西安电子科技大学 ISN 国家重点实验室, 陕西西安 710071; 2. 浙江财经学院信息学院, 浙江杭州 310012)

摘 要: 合同签署是一项重要而频繁的商务活动. 现有的合同签署方案都没有解决"强迫签署"的问题: B 强迫 A 签署一项 A 不愿签署的合同. 本文首次引入了"强迫签署"的概念, 然后利用 XTR 公钥密码体制中共轭元素的性质, 提出了一种无强迫的最优合同签署方案. 在可信赖第三方的帮助下, A 可以提供相应的证据来废除所签署的合同, 从而最大程度地保证了系统的公平性.

关键词: XTR 公钥体制; 最优合同签署; 公平交换
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2004) 03-0404-04

Optimistic Contract Signing Scheme Without Coercion

CHEN Xiao-feng[1], WANG Ji-lin[2], WANG Yu-min[1]
(1. National Key Laboratory of ISN, Xidian University, Xi'an, Shaanxi 710071, China;
2. Zhejiang University of Finance & Economics, Hangzhou, Zhejiang 310012, China)

Abstract: Contract signing is a fundamental and frequent service in electronic commerce. All present contract-signing schemes cannot solve the crime of "coercive signing": B forces A to sign a contract that he would not like to sign. The concept of "coercive signing" is firstly introduced in this paper and an optimistic contract-signing scheme without coercion is proposed by using the properties of conjugate elements in XTR system. With the help of the trusted third party, A can offer some evidence to abort the contract, so it ensures the fairness of the system furthest.

Key words: XTR public key system; optimistic contract signing; fair exchange

1 引言

合同签署是一项重要而频繁的商务活动, 它可以看作是双方对合同的签名的公平交换的一种推广. 虽然合同签署问题可以通过交换双方的签名而完成, 但是签名的公平交换和公平的合同签署是两个不同的问题, 这是因为并不是所有的合同签署都需要交换对方的签名. 合同签署只需双方保证对合同协商的不可否认即可. 所以, 合同签署可定义为签署双方(或多方)对某一特定文本的不可否认的协商及交换.

在目前的研究中, 都假定主体愿意签署合同. 然而, 如同现实生活中一样, 在某些情况下存在"强迫签署"的问题, 即 B 强迫 A 签署一项 A 不愿签署的合同, 此时由于 A 对合同的期望与 B 的描述不符, 所以即使执行所谓的"公平交换协议", 也不能保证系统的公平性.

本文我们利用 XTR 公钥密码体制中共轭元素的性质, 给出了一种无强迫的最优合同签署方案. 受害者可以在协议中嵌入相应的证据来证明自己受到了威胁, 而罪犯无法察觉. 协议完成后, 在可信赖第三方的帮助下就可废除所签署的合同, 从而最大程度地保证了系统的公平性.

2 公平交换

2.1 基本符号

公平交换方案一般包括一个发送方(originator), 接收方(recipient), 可信赖第三方(the trusted third party). 所要交换的物品(item)可分为: 机密数据, 公开数据, 支付.

i_A: Alice 想发送的物品(item).

$desc_A$: 对物品 i_A 详尽的描述, 包含了物品所有重要的特性, 使得其它主体能够确认.

$expect_A(desc_A, desc_B)$: Alice 对用物品 i_A 交换得到物品 i_B 的期望值. 如果 Alice 对收到的 i_B(用 $desc_B$ 描述)表示满意, 则 $expect_A(desc_A, desc_B) = "true"$.

$fits(desc, i)$: 如果描述和物品相符合, 则 $fits(desc, i) = "true"$.

图 1 给出了一个成功的公平交换的模型.

2.2 公平交换的基本要求

p 有效性(effectiveness): 如果 Alice 诚实地执行协议, 而且她和 Bob 都没有中止协议, 那么在协议结束后, Bob 就可以得到他所期待的物品.

收稿日期: 2002-12-04; 修回日期: 2003-11-20
基金项目: 973 国家重大项目(No. G1999035804)

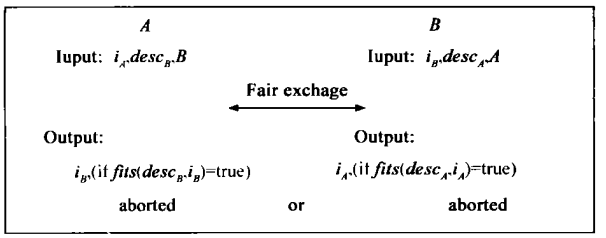

图 1　公平交换模型

p 秘密性(privacy): 交换必须保护用户的秘密隐私信息.

p 不可否认性(non2repudiation): 在进行有效的交换后, 交换的任何一方都不能对他所传递和收到的信息进行否认.

p 高效实用性(efficiency): 协议的效率要高, 以保证实用.

p 公平性(fairness): 如果在交换结束后, 要么每一方都得到了他所期待的物品(或服务), 要么每一方都没有得到任何有意义的东西. 公平性又可分为强公平性和弱公平性:

p 强公平性: 在协议结束后, 要么 Alice 得到了 i_B 满足 desc(i_B)= expect(i_B); 要么 Bob 没有得到任何有关 i_A 的附加信息.

p 弱公平性: 在协议结束后, 要么 Alice 得到了 i_B 满足 desc(i_B)= expect(i_B); 要么 Bob 没有得到任何有关 i_A 的附加信息, 或者 Alice 能向仲裁者证明: Bob 收到了(或能收到) i_A 满足 desc(i_A)= expect(i_A).

p 时限性(timeless): 协议必须保证在某一时刻中止. 协议结束时, 无论交换处于何种状态, 都不能影响协议的公平性.

p 第三方可验证性(verifiability): 发生纠纷时第三方可进行仲裁, 对不诚实的一方可进行制裁. 同时, 如果第三方不诚实使得该协议对 Alice 不公平, 则 Alice 可向仲裁者(arbiter)证明第三方的不公正行为.

p 无滥用性(abuse2free): 在合同签署中, 参与交换的任一子集在协议的任何时刻, 都无法向第三者证明他们有能力中止(或完成)协议.

3　XTR 公钥体制

XTR 公钥体制, 即有效的紧致的子群迹表示, 由 Lenstra 等人[1]提出, 它是一种传统的基于子群离散对数问题的密码体制. 由于它使用 $GF(p^2)$ 的算术来达到 $GF(p^6)$ 上的安全性, 这样 XTR2DL 问题就比分解 6l 1$\log_2 p$ 比特 RSA 模更为困难, 而且数据量降低到原来的 1/3. 如果 p, q 取 1702比特的素数, 则 XTR 就比 10202比特 RSA 更为安全. 与目前实用的 ECC 公钥密码体制相比较, 同等安全程度的 XTR 体制的实现在计算、密钥存储和通信方面的要求和 ECC 基本相同, 而 XTR 的密钥和参数选取要比 ECC 简单, 其指数计算比 ECC 标量乘计算快. 所以, 在同等的安全程度下, XTR 就大大减少了数据的存储量, 计算量和通讯量. XTR 已成为一种非常有吸引力的新的公钥密码体制. 当然, 如何进一步改进 XTR 的算法, 优化参数选取, 使 XTR 走上实用需要进一步的工作[2]. 近来, S Lim[3]等人将 XTR 体制推广到 $GF(p^{6^m})$, 我们称之为广义的 XTR 体制. 由于现有的微处理器都是以 word 为单位对数据进行处理的, 对特别大的整数必须用多个 word 表示, 计算也非常复杂. 广义的 XTR 体制可以选择与 word 相当的 p(如选择 p 为一个大约 64bit 的素数), 从而避免了多精度运算的一些缺陷, 如模规约运算、进位运算等.

311　系统参数

令 p= 2mod3 是一个素数, 6 次分圆多项式在 p 的值 $\Phi_6(p)= p^2- p+ 1$ 有一个素因子 q. g I $GF(p^6)^*$ 的阶为 q, Tr(g) I $GF(p^2)$ 是 g 的迹. 给定 Tr(g), 由 g 生成的 q 阶子群就称为 XTR 群.

令 c= Tr(g), 多项式 $F(c, X)= X^3- cX^2+ c^pX- 1$ I $GF(p^2)[X]$. 对整数 n I Z, 我们定义 c_n 为 F(c, X)的根的 n^{th} 方幂之和, 即如果 $F(c, h_j)= 0$, j= 0, 1, 2, 则 $c_n= h_0^n+ h_1^n+ h_2^n= Tr(g^n)$, 显见 $c_1= c$.

给定 c 和任意整数 n, Lenstra 等给出了一个快速算法计算 $S_n(c)= (c_{n-1}, c_n, c_{n+1}$. 这样, XTR 的参数就为 p, q, c. 用户选择秘密密钥 n 并通过计算 $S_n(c)$ 得到对应的公钥. 而且, Lenstra[2]指出 c_{n-1}(或 c_{n+1}) 可以通过 c, c_n 和 c_{n+1}(或 c_{n-1}) 表示出来, 这样 c_{n-1}, c_{n+1} 就不必包括在 XTR 公钥信息中.

312　XTR2Schnorr 签名方案

XTR 系统参数如上, H(,) 是一个安全的 Hash 函数. A 的签名私钥为 x, 所对应的公钥为 $y= Tr(g^x)$. 所要签名的消息为 m.

步骤 1　A 随机选择 k I z_q, 计算 $S_k(Tr(g))$ 并发送 r= Tr(g^k) I $GF(p^2)$ 给 B.

步骤 2　设 r= (a, b), A 计算 e= H(m, ap+ b)modq.

步骤 3　A 计算 s= k- exmodq, 然后 A 给 B 发送对消息 m 的签名(s, e).

验证: B 利用算法 21418[5]计算 S= Tr($g^s g^{xe}$) I $GF(p^2)$. 设 S= (ac, bc). 如果 H(m, acp+ bc)= e, 则签名正确. 这是因为:

$$S= Tr(g^{s+xe})= Tr(g^{k-xe+ex})= Tr(g^k)= r$$

定理 1　在步骤 3 中, 如果 A 发送 $s_c= kp^2- ex \bmod q$ 或 $s_d= kp^4- ex \bmod q$, 上述的签名方案仍然成立.

证明: 如果 A 发送 s_c 给 B, B 计算 S= Tr(g^{s_c+xe})= Tr($g^{kp^2-xe+ex}$)= Tr(g^{kp^2}). 由于对 P k I z_q, 都有 Tr(g^k)= Tr($g^{kp^2 \bmod q}$)= Tr($g^{kp^4 \bmod q}$), 所以 S= r.

4　无强迫的最优合同签署方案

现有的最优合同签署方案一般包括三个子协议: 交换, 异常中断, 仲裁. 在通常的情况下, 只有交换协议发生. 在发生纠纷时, 就要执行其它两个协议. 现有的合同签署协议为了达到安全性的目的, 都非常的复杂. 最近, 文献[4]给出了一个非常简单的协议, 我们将在此协议的基础上给出我们的无强迫的合同签署方案.

411　符号

我们用 A, B 分别表示合同签署的双方, TTP 表示可信赖的第三方. TTP 首先选择 XTR 体制的系统参数. 假设 A, B, TTP 分别选择自己的私钥 x_A, x_B, x_T I z_q, 并公布自己的公钥 Tr(g^{x_A}), Tr(g^{x_B}), Tr(g^{x_T}). 我们假定系统提供时戳服务, 消息

按照所发送的时间顺序对应一个时刻 t, 而且任何人都可以公开验证. $S_x(m)$表示用 XTR2Schnorr 签名方案对消息 m 的签名, 私钥为 x.

设双方所要签署的合同为 m, H(,)是一个安全的 Hash 函数.

4.2.2 无强迫的合同签署方案

我们的方案包括一下几个子协议:

4.2.2.1 通知协议

假设 B 强迫 A 签署一项他不愿签署的合同 m. 在进行签署协议前, A 首先通过一个安全信道发送下面的消息通知 TTP 自己受到了威胁, 不妨设此消息对应的时戳为 t_0:

$\{ID_A, m, cancel, k, H(m,k), Tr(g^l), S_{x_A}(H(m,k))\}$

其中随机数 $k, l \in z_q$. 如果令 $Tr(g^l)=(A,B)$, 那么 $S_{x_A}(H(m,k))=(E,S)$, 其中 $E=H(H(m,k), Ap+B) \bmod q$, $S=l-ex_A \bmod q$. TTP 可验证此签名的正确性.

4.2.2.2 交换协议

Step1 A 发送消息 $Tr(g^k)=(a,b)$, m, S_{x_A}, $S_{x_A}(H(m))=(e,s)$给 B, 其中 $e=H(H(m), ap+b)$, $s=kp^{2t}-ex \bmod q$. 当发生强迫签署时, $t=1$ 或 2; 否则 $t=0$. 设此消息对应的时戳为 t_1.

Step2 由定理 1, B 可验证(e, s)是 A 对 H(m)的签名. 然后, B 发送$S_{x_B}(H(m))$给 A.

Step3 A 验证$S_{x_B}(H(m))$的正确性, 然后发送 $S_{x_A}(H(S_{x_B}(H(m))))$给 B.

4.2.2.3 作废协议

A 在某个适当的时候(如他的孩子被释放后), 向 TTP 提出废除合同的请求. TTP 要求 B 提供 A 对合同的签名 m, $S_{x_A}(H(m))=(e,s)$. TTP 首先验证 $t_0<t_1$, 然后再验证合同及 A 的签名是否正确. 如果正确, 他 A 要求提供自己的私钥 x_A, 然后计算 $ec=H(H(m), ap+b)$, $sc=k-ex_A \bmod q$, 并验证 $Tr(g^{sc}g^{xec})=Tr(g^k)$. 如果 $e \neq ec$, TTP 拒绝 A 的要求; 如果 $e=ec$, 且 $s=sc$, TTP 拒绝 A 的要求; 否则断定 B 强迫 A 签署合同, 并宣布合同作废.

4.2.2.4 仲裁协议

在没有发生强迫签署时, A, B 之间也有可能发生纠纷. 此时就要执行仲裁协议, 即废除合同(如果 B 确实欺骗 A)或强迫执行合同(如果 A 确实欺骗 B). 仲裁协议类似于文献[5], 这里就不再给出.

所以当发生 B 强迫 A 签署合同时, 执行通知协议, 交换协议, 作废协议; 如果没有强迫行为发生, 而且 A, B 诚实地签署合同, 则只需执行交换协议; 如果虽然没有强迫行为发生, 但是 A, B 中有一方没有诚实地签署合同或交换协议异常中止, 则执行交换协议后, 还需要执行仲裁协议. 这样就保证了系统的公平性, 最大程度的保护了诚实用户的利益.

当然, 我们的方案也可以推广到多方合同签署中[7,8], 这里我们不再讨论.

5 方案的分析

这一节我们将给出方案的安全性及效率性分析:

5.1.1 安全性分析

5.1.1.1 我们的方案满足无强迫性、有效性、秘密性、实用性、不可否认性、公平性、时限性、第三方可验证性以及无滥用性.

证明 这里我们只证明无强迫性, 其它性质的证明可参阅文献[4]. 发生强迫签署后, A 提交自己的私钥 x_A, 于是 TTP 计算: $ec=H(H(m), ap+b)$, $sc=k-ex_A \bmod q$, 并验证 $Tr(g^{sc}g^{xec})=Tr(g^k)$, 而且 $sc=k-ex_A \bmod q \neq kp^{2t}-ex_A \bmod q=s$, $t=1$ 或 2. 于是 TTP 就得到了 A 受到强迫的证据, 而 B 不能抵赖. 当然在执行协议的过程中 B 无法判断 A 是否欺骗自己, 这是因为. $Tr(g^k)=Tr(g^{kp^2})=Tr(g^{kp^4})$.

5.1.1.2 如果罪犯 B 强迫 A 使用他选定的随机数 k, 那么这种攻击就相当于 B 强迫 A 泄漏自己的密钥.

证明 如果 B 强迫 A 泄漏自己的私钥, 那么 B 就可以代替 A 自己签名完成所谓的"公平交换协议", 这种攻击是最危险的. 一旦发生, A 在协议前必须向 TTP 提出吊销私钥的请求或声明私钥作废.

此外, 如果罪犯 B 强迫 A 使用他选定的随机数 k, 那么这种攻击就相当于 B 强迫 A 泄漏自己的密钥. 因为 B 可以由 s 计算 $x=e^{-1}(k-s) \bmod q$. 然后 B 首先验证 $Tr(g^x)=Tr(g^{x_A})$ 是否成立. 若成立, 再分别计算 $Tr(g^{x+1})$, $Tr(g^{(xp^2+1) \bmod q})$, $Tr(g^{(xp^4+1) \bmod q})$. 如果 $Tr(g^{x+1})$ 是这三个数中"最小的", 那么他相信 A 没有欺骗自己, 从而得到 A 的私钥 $x_A=x$; 否则认为 A 欺骗自己, 拒绝接受 s.

注记: B 由 s 计算出 $x=e^{-1}(k-s) \bmod q$, 不能直接验证 $Tr(g^s g^{xe})=Tr(g^k)$ 成立就断定 A 没有欺骗自己. 这是因为 $Tr(g^{xp^2})=Tr(g^x)$, A 可以发送 $s=k-e(xp^2) \bmod q$ 来欺骗 B.

5.1.1.3 受害者 A 必须在执行公平交换协议前告知 TTP 他受到了罪犯 B 的强迫.

证明 首先, A 不能在执行公平交换协议的任何时刻告知 TTP 他受到威胁. 否则, A 一旦想中止协议, 他就可以随时告知 TTP 自己受到威胁, 这样他就可以向别人证明他有能力中止协议, 这就与协议的无滥用性相矛盾. 其次, A 也不能在公平交换协议结束后告知 TTP 他受到威胁. 否则 B 可以声称 A 诬陷自己, 而 TTP 无法仲裁(因为确实存在 A 诬陷 B 的可能).

所以, 受害者 A 必须在执行公平交换协议前告知 TTP 他受到了罪犯 B 的强迫. 而且, 他必须在协议中嵌入相关的证据.

5.1.1.4 如果 B 是诚实的, 那么 A 诬陷 B 就会有一定的商业风险.

证明 A 没有必要诬陷诚实的 B, 因为如果 A 对合同不满意, 他一开始就可以拒签; 否则, 他就面临着损失这个合同的风险(A 愿意与 B 签署这个合同), 除非他能预测有更好的合同(如引言中所讨论的). 此外, A 还要承担自己信用度受损的风险.

5.1.2 效率性分析

在目前所有合同签署协议中, 文[4]的协议使用的步骤最少, 而且易于理解. 我们的方案基于该协议, 而且我们使用了

XTR2Schnorr 签名方案. 所以通信量、计算量与存储量大约是使用其它签名方案的 1/3, 效率较高, 有实用价值.

6 结论

/ 强迫签署0 是合同签署中的一种犯罪行为. 由于受害者对合同的期望与罪犯 B 对合同的描述不符, 所以即使执行所谓的/ 公平交换协议0, 也不能保证系统的公平性. 本文首次引入/ 强迫签署0 的概念, 然后利用 XTR 公钥密码体制中共轭元素的性质, 给出一种无强迫的最优合同签署方案. 在可信赖第三方的帮助下, 受害者可以提供相应的证据来废除所签署的合同, 于是可以最大程度地保证系统的公平性. 该方案不仅满足公平交换的基本要求, 而且由于使用了 XTR2Schnorr 签名方案, 所以具有通信量、计算量与存储量小的优点, 效率较高.

参考文献:

[1] A K Lenstra, E R Verheul. The XTR public key system [A]. LNCS 1880, Crypto. 2000[C]. Berlin: Springer2Verlag, 2000. 1- 19.

[2] A K Lenstra, E R Verheul. Key improvements to XTR [A]. LNCS 1880, Asiacrypt. 2000[C]. Berlin: Springer2Verlag, 2000. 1- 19.

[3] S Lim, S Kim, I Yie, J Kim, H Lee. XTR extended to GF(p6m) [A]. LNCS 2259, SAC 2001[C]. Berlin: Springer2Verlag, 2001, 301- 312.

[4] J L Ferrer2Gomila, et al. Efficient optimistic n2party contract signing protocol[A]. LNCS 2200, ISC 2001 [C]. Berlin: Springer2Verlag, 2001. 394- 407.

[5] J A Garay, P MacKenzie. Abuse2free multi2party contract signing[A]. LNCS 1693, DISC 99[C]. Berlin: Springer2Verlag, 1999. 151- 165.

作者简介:

陈晓峰　男, 1976 年生于陕西宝鸡, 西安电子科技大学 ISN 国家重点实验室博士研究生, 感兴趣的研究方向为椭圆曲线密码与电子商务.

王继林　男, 1965 年生于河南柘城, 西安电子科技大学 ISN 国家重点实验室博士研究生, 副教授, 研究方向为电子商务的安全技术.