一个多方公平电子合同协议

李志江, 李明柱, 杨义先, 胡正名
(北京邮电大学信息安全中心, 北京 100876)

摘 要: 电子合同协议的研究越来越受到人们的重视, 本文给出了一个多方公平电子合同协议. 这个多方公平电子合同协议需要可信第三方的参与, 但不会形成网络瓶颈. 通过对其公平性与效率的分析, 可知本协议在满足了公平性的同时具有较高的实用性.

关键词: 电子商务; 电子合同; 数字签名
中图分类号: TN911.22 文献标识码: A 文章编号: 0372-2112 (2002) 10-1435-03

A Multi-Part Fair Electronic Contract Protocol

LI Zhi-jiang, LI Ming-zhu, YANG Yi-xian, HU Zheng-ming
(*Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China*)

Abstract: Electronic contract protocol is receiving more and more attention. In this paper, a multi-part fair electronic contract protocol is proposed. This multi-part fair electronic contract protocol needs a trusted third part. But the trusted third part will not make a bottle-neck. Through the analysis to its fairness and efficiency, we know this protocol is fair and efficient.

Key words: electronic commerce; electronic contract; digital signature

1 引言

随着 Internet 的飞速发展, 作为电子商务重要组成部分的电子合同也逐渐受到人们的重视, 制定公平的电子合同协议是电子合同得以应用的关键. 目前有关公平电子合同协议的研究主要是针对合同当事人只有两方的情况[1-6]. 但在商务活动中, 合同当事人为三方或多方的情况并不少见, 因此有必要制定多方公平电子合同协议.

合同当事人甲乙通过 Internet 签订电子合同时, 如果甲将自己对合同的数字签名发送给乙之后, 而没有收到乙对合同的数字签名, 这时甲就处于不利地位. 因为, 一旦发生合同纠纷, 当合同内容对乙有利时, 乙可以拿出甲对合同的数字签名, 证明甲曾经与自己签订过这个合同. 而当合同内容对乙不利时, 甲拿不出乙对合同的数字签名, 乙会矢口否认曾经与甲签订过这个合同. 对于合同当事人为三方或更多方时, 也存在这样的欺诈问题. 为了保障合同当事人的利益需要制定公平的电子合同协议. 对于一个电子合同协议, 如果按照该协议签定电子合同, 任意一个合同当事人不会因为其他当事人的作弊或通信线路故障而使自己处于不利地位, 就称之为公平电子合同协议.

对于多方公平电子合同协议, 在考虑存在合同当事人一方作弊不按协议执行的同时, 还必须防止多个合同当事人联手共同作弊的情况, 必须保证诚实信用严格执行协议的当事人的利益不会由于其他当事人的作弊行为而受到损失.

2 多方公平电子合同协议

本文给出的这个多方电子合同协议, 很容易由合同当事人为三方推广到合同当事人为更多方的情况, 为了描述方便, 只给出合同当事人为三方的情况. 为了准确描述协议, 这里使用了如下的符号和约定:

TTP	可信第三方
A, B, C	合同当事人 A, B, C
R_s	S 生成的随机数
M	电子合同内容
$Sign_s(X)$	S 使用自己的签名私钥对消息 X 进行数字签名的签名结果
$H(X)$	消息 X 的哈希值
(X, Y)	消息 X 与消息 Y 的连接
$[t_n, t_{n+1}]$	协议执行的第 n 阶段, t_n, t_{n+1} 表示相邻的两个时刻 $(1 \leqslant n \leqslant 10)$

2.1 协议的具体描述

在协议执行的第一阶段 $[t_1, t_2]$ 内, 合同当事人 A, B, C 分别生成:

$$N_A = (A, B, C, H(R_A), H(M), Sign_A(H(M)), [t_{10}, t_{11}])$$

$$N_B = (B, A, C, H(R_B), H(M), Sign_B(H(M)), [t_{10}, t_{11}])$$

收稿日期: 2001-10-20; 修回日期: 2001-12-29
基金项目: 国家重点基础研究发展规划项目(No. G1999035805); 国家杰出青年基金(No. 69425001); 国家自然科学基金(No. 69882002, 60073049)

N_C= (C, A, B, $H(R_C)$, $H(M)$, $Sign_C(H(M))$, [t_{10}, t_{11}])

其中 R_A、R_B、R_C 由 A、B、C 各自秘密生成, 在没有得到 M_1= (N_A, N_B, N_C, $Sign_A(N_A, N_B, N_C)$) 的情况下不得泄漏给任何人.

在协议执行的第二阶段[t_2, t_3] 内, 合同当事人 B、C, 分别将 N_B, N_C 发送给当事人 A.

在协议执行的第三阶段[t_3, t_4] 内, 如果 A 在 t_3 时刻之前成功地收到了 N_B、N_C, 则计算 $Sign_A(N_A, N_B, N_C)$, 生成 M_1= (N_A, N_B, N_C, $Sign_A(N_A, N_B, N_C)$) 供 B、C 在协议执行的第四阶段下载. 如果没有成功收到 N_A、N_B, N_C 中的任意一个, 则生成 $Sign_A(NOsubmit, A, B, C, H(M))$.

在协议执行的第四阶段[t_4, t_5] 内, B、C 从 A 处下载 A 在第三阶段生成的信息 M_1 或 $Sign_A(NOsubmit, A, B, C, H(M))$.

在协议执行的第五阶段[t_5, t_6] 内, B、C 根据自己在第四阶段是否成功地下载了 M_1 而决定是否将 R_B, R_C 发送给 A. 如果成功下载了 M_1 则发送, 否则不发送.

在协议执行的第六阶段[t_6, t_7] 内, A 根据自己在第五阶段是否成功收到 R_B, R_C 而生成供 B、C, 在第七阶段下载的信息. 如果成功收到 R_B、R_C, 则生成 M_2 = (R_A, R_B, R_C, $Sign_A(R_A, R_B, R_C)$), 否则生成 $Sign_A(NOcommit, A, B, C, H(M))$.

在协议执行的第七阶段[t_7, t_8] 内, B、C 从 A 处下载 A 在第六阶段生成的信息 M_2 或 $Sign_A(NOcommit, A, B, C, H(M))$.

在协议执行的第八阶段[t_8, t_9] 内, A, B, C 根据自己是否已经拥有了 M_1 与 M_2 而采取不同的动作. 这里用二维向量 (x, y) 来表示 A, B, C 在第七阶段结束之后拥有 M_1 与 M_2 的情况. x = 1 表示拥有 M_1, x = 0 表示没有 M_1. y = 1 表示拥有 M_2, y = 0 表示没有 M_2. 在第七阶段结束后, 这个二维向量可能是 $(1, 1)$, $(1, 0)$, $(0, 0)$, $(0, 1)$. 对于 A, B, C 中任意一方, 如果其状态为 $(1, 1)$ 则终止执行; 如果其状态为 $(0, 0)$ 或 $(0, 1)$ 则一直等待到协议执行的第十阶段结束看是否有可信第三方 *TTP* 发送的合同有效裁决; 如果其状态为 $(1, 0)$ 则在协议执行的第九阶段向可信第三方 *TTP* 发送裁决合同有效请求. 当 A, B, C 中任意一方 X 需要向可信第三方 *TTP* 发送裁决合同有效请求时, 发送的请求消息为 $Sign_X(A, B, C, M_1)$.

在协议执行的第九阶段[t_9, t_{10}] 内, 如果可信第三方 *TTP* 收到了合同当事人发送的裁决合同有效请求, 则生成合同有效裁决 M_3= (M_1, $Sign_{TTP}(M_1)$), 并在协议执行的第 10 阶段结束即 t_{11} 之前将 M_3 发送给当事人 A, B, C.

2.2 合同有效的证据

当发生合同纠纷时, 证明 A, B, C 曾经成功签订过合同 M 的证据为 (M_1, M_2) 或 M_3. 只要 A, B, C 中有一方能够提供 (M_1, M_2) 或 M_3, 仲裁者就可以断定 A, B, C 曾经成功签订过合同 M.

2.3 协议的公平性分析

无论合同当事人是否严格按照协议执行, 在协议执行的第八阶段合同当事人的状态只可能有 $(1, 1)$, $(1, 0)$, $(0, 0)$, $(0, 1)$ 四种情况.

首先可知状态为 $(1, 1)$ 的合同当事人由于已经拥有了证明曾经成功签订过合同 M 的证据 (M_1, M_2), 所以其不会处于不利地位. 其次状态为 $(1, 0)$ 的合同当事人由于其可以向可信第三方 *TTP* 发送裁决合同有效请求, 从而可以在第十阶段收到可信第三方发送的证明曾经成功签订过合同 M 的证据 M_3, 所以只要状态为 $(1, 0)$ 的合同当事人严格按照协议执行就不会处于不利地位. 状态为 $(0, 1)$ 的当事人显然是没有严格按照协议执行, 本协议不保护不严格按照协议执行的当事人的利益. 以下是对状态为 $(0, 0)$ 的合同当事人的讨论.

定理 1 在协议执行的第八阶段, 如果既存在状态为 $(1, 1)$ 的当事人, 又存在状态为 $(0, 0)$ 的当事人, 则状态为 $(0, 0)$ 的当事人一定没有严格按照协议执行.

证明 设当事人 X 的状态为 $(0, 0)$, Y 的状态为 $(1, 1)$, $X, Y \in \{A, B, C\}$, $X \neq Y$. X 的状态为 $(0, 0)$ 意味着 X 既没有 M_1 又没有 M_2. Y 的状态为 $(1, 1)$ 意味着当事人 Y 已经拥有了 M_1 与 M_2. 由于 M_2= (R_A, R_B, R_C, $Sign_A(R_A, R_B, R_C)$), 因而当事人 Y 知道 R_A、R_B、R_C 所以该当事人 Y 知道 R_X. R_X 是由 X 私下秘密产生的, 一定是 X 没有严格按照协议规定在没有得到 M_1 的情况下泄漏了 R_X.

在协议执行的第八阶段存在状态为 $(0, 0)$ 的当事人的可能情况是:

(1) A, B, C 状态都为 $(0, 0)$.

(2) A, B, C 三者只具有 $(1, 0)$, $(0, 0)$ 两种状态.

(3) A, B, C 三者只具有 $(1, 1)$, $(0, 0)$ 两种状态.

(4) A, B, C 三者具有 $(1, 1)$, $(0, 1)$, $(0, 0)$ 三种状态.

(5) A, B, C 三者具有 $(1, 1)$, $(1, 0)$, $(0, 0)$ 三种状态.

对于第一种情况, A, B, C 状态都为 $(0, 0)$, 这时合同当事人都没有证明曾经成功签订过合同 M 的证据 (M_1, M_2), 同时也都没有用来生成可以请求可信第三方 *TTP* 裁决合同有效 M_3 的 M_1. 在协议执行的第十阶段之后, 都不能收到可信第三方 *TTP* 发送的合同有效裁决 M_3. 所以协议执行完之后合同当事人都不可能拥有曾经成功签订过合同 M 的证据. 因而, 这种情况下状态为 $(0, 0)$ 的当事人不会处于不利地位.

对于第二种情况, 如果状态为 $(1, 0)$ 的当事人利用 M_1 生成裁决合同有效请求, 并发送给可信第三方 *TTP*, 则在协议执行的第十阶段, 所有当事人都可以收到可信第三方 *TTP* 发送的证明曾经成功签订过合同 M 的证据 M_3, 状态为 $(0, 0)$ 的当事人不会处于不利地位. 如果状态为 $(1, 0)$ 的当事人都没有向可信第三方 *TTP* 发送裁决合同有效请求, 则在协议执行的第十阶段, 所有当事人都不能收到可信第三方 *TTP* 发送的证明曾经成功签订过合同 M 的证据 M_3, 状态为 $(0, 0)$ 的当事人同样不会处于不利地位.

对于第三、四种情况, 在协议执行的第七阶段之后状态为 $(1, 1)$ 的当事人已经拥有了证明曾经成功签订过合同 M 的证据 (M_1, M_2), 而状态为 $(0, 0)$ 的当事人没有用来生成可以请求可信第三方 *TTP* 裁决合同有效 M_3 的 M_1. 在协议执行的第十阶段之后, 不能收到可信第三方 *TTP* 发送的合同有效裁决 M_3, 这种情况下对状态为 $(0, 0)$ 的当事人不利. 根据定理 1 可

知, 这种不利是由状态为(0, 0)的当事人没有严格按照协议执行造成的.

对于第五种情况, 在协议执行的第七阶段之后状态为(1, 1)的当事人已经拥有了证明曾经成功签订过合同 M 的证据(M_1, M_2), 而状态为(0, 0)的当事人没有用来生成可以请求可信第三方 *TTP* 裁决合同有效M_3 的 M_1. 状态为(1, 0)的当事人与状态为(1, 1)的当事人串通不向可信第三方 *TTP* 发送裁决合同有效请求, 在协议执行的第十阶段之后, 状态为(0, 0)的当事人不能收到可信第三方 *TTP* 发送的合同有效裁决M_3. 这种情况下对状态为(0, 0)的当事人不利. 根据定理 1 同样可知, 这种不利是由状态为(0, 0)的当事人没有严格按照协议执行造成的.

通过对以上各种情况的分析, 可知状态为(0, 0)的合同当事人不会处于不利地位.

这里需要指出的是状态为(1, 0)的当事人如果不严格按照协议执行, 其结果不会使自己处于有利地位, 相反还可能使自己处于不利地位. 因为在协议执行的第八阶段可能出现合同当事人 A, B, C 三者只具有(1, 1), (1, 0)两种状态的情况. 这时状态为(1, 1)的当事人拥有证明曾经成功签订过合同 M 的证据(M_1, M_2). 状态为(1, 0)的当事人只有按照协议利用 M_1 生成裁决合同有效请求, 并发送给可信第三方 *TTP*, 才能在协议执行的第十阶段收到可信第三方 *TTP* 发送的证明曾经成功签订过合同M 的证据M_3. 如果状态为(1, 0)的当事人不按照协议规定向可信第三方 *TTP* 发送裁决合同有效请求, 在协议执行的第十阶段就可能收不到可信第三方 *TTP* 发送的证明曾经成功签订过合同M 的证据M_3. 这样会因为别人拥有证明曾经成功签订过合同 M 的证据而自己没有使自己处于不利地位.

根据以上的分析可知, 合同当事人不严格按照协议执行的结果不但没给自己带来任何好处, 反而会使自己处于不利地位. 合同当事人无论在第八阶段的状态如何, 只要严格按照协议执行都不会处于不利地位. 在协议执行完之后, 如果严格按照协议执行的合同当事人没有证明成功签订过电子合同 M 的证据, 则其他合同当事人也都不会拥有证明成功签订过电子合同 M 的证据, 因而本协议是公平的.

2.4 协议的效率分析

对于实际应用中, 大多数情况下合同当事人都是诚实信用的, 都会按照协议规定的去做. 特别是当合同当事人理解了协议的公平性, 知道自己的作弊行为不会给自己带来什么好处之后, 那些想作弊的人也不会作弊. 对于一个实用高效的公平电子合同协议, 必须保证当合同当事人都诚实地按照协议规定的去做时, 电子合同的签订会高效快捷. 本协议中当合同当事人都诚实信用按照规定的去做时, 不需要可信第三方参与, 当事人之间传输的信息也只有 8 条. 而当合同当事人增加到 n(n> 3)时, 当事人之间传输的信息也只有 4(n- 1)条, 在第八阶段完成后即可停止执行协议. 可信第三方只是在有人作弊或通信线路出现故障时才参与协议的执行, 这大大降低了可信第三方成为瓶颈的概率, 因而本协议是高效实用的.

3 总结

本文给出的协议需要可信第三方的参与, 在保证公平性的同时降低了可信第三方 TTP 成为瓶颈的概率. 本协议中, 合同当事人 B, C 的地位完全相同. 当有更多的合同当事人参与时, 三方之外的合同当事人只要同 B, C 的地位相同即可保证协议的公平性.

参考文献:

[1] Shimon Even, Oded Goldreich, Abraham Lempel。A randomized protocol for signing contracts [J]. Communications, 1985, ACM28(6): 637 - 647.

[2] M Ben-Or, O Goldreich, S Micali, R L Rivest. A fair protocol for signing contracts [J]. IEEE Transactions on Information Theory, 1990, 36(1): 40- 46.

[3] Shimon Even. A protocol for signing contracts [J]. ACM SIGACT News, 1983, 15(1): 34- 39.

[4] Oded Goldreich. A simple protocol for signing contracts [A]. Crypto'83 [C]. New York: Plenum Press, 1984. 133- 136.

[5] N Asokan, V Shoup, Michael Waidner. Asynchronous protocols for optimistic fair exchange [A]. 1998 IEEE Symposium on Research in Security and Privacy [C]. Los Alamitos: IEEE Computer Society Press, 1998.

[6] B Pfitzmann, M Schunter, M Waidner. Optimal efficiency of optimistic contract signing [DB/OL]. IBM Research Report RZ 2994 (#93040), IBM Zurich Research Laboratory, http://www.semper.org/direne/publ/PFSW-98PODC98.ps.gz. 03/02/1998.

作者简介:

李志江　男, 1971 年 10 月生于河北省赤城县, 密码学博士生, 主要从事密码学、网络安全、电子商务安全等方面的研究与开发工作.

李明柱　男, 1973 年 10 月生于山东省郓城县, 密码学博士生, 主要研究方向为网络信息安全, 电子商务安全等.