带脱线半可信第三方的公平非否认交换协议

王彩芬, 葛建华
(西安电子科技大学通信工程学院 ISN 国家重点实验室, 陕西西安 710071)

摘 要: 不可否认性和公平性是电子商务交换协议中的两个重要性质. 本文以带盲密文的可验证加密方案为基础, 提出了一种新的带有脱线半可信第三方公平的非否认协议, 使协议中的任何一方可以单方面终止协议的执行但又不破坏公平性.

关键词: 电子商务; 非否认性; 公平性; 半可信第三方; 带盲密文的可验证加密
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2002) 02-0286-03

A New Fair Non-Repudiation Protocol with Off-Line Semi-Trusted Third Party

WANG Cai-fen, GE Jiang-hua
(National Key Lab. on ISN, Xidian University Xi'an, Shaanxi 710071, China)

Abstract: Non-repudiation and fairness turn out to be two important security properties of electronic commerce protocols. In this paper, based on a verifiable encryption with blind decryption, we present a new fair non-repudiation protocol with off-line semi-trusted third party, so either transaction party can unilaterally bring a transaction to completion without losing fairness. This is the first non-repudiation protocol with off-line semi-trusted third party.

Key words: electronic commerce; non-repudiation; fairness; semi-trusted third party; verifiable encryption with blind decryption

1 引言

随着电子商务在计算机网络上的日益盛行, 关于交易的争论成为一个普遍的问题. 为了解决这种争论需要使用不可否认性. 当然, 协议的公平性更是必不可少的. 所以, 交易中两个重要的性质应该是交换的公平性和非否认性.

所谓公平性是指在协议执行的任何阶段, 参与协议的任何一方都不占优势. 并有强公平性与弱公平性的定义之分[3]. 对公平性形式化的分析也被广泛研究[7]. 而非否认性用来避免参与协议的各方否认曾经发生的行为, 在非否认协议中将产生、收集和维护证据以便解决协议结束后出现的争端.

定义[1]: 一个非否认协议是公平的是指当协议结束时为收方和发方提供有效的不可否认的证据, 而在协议执行的任何情况下没有使一方比另一方有利.

为了保证协议满足公平性要求, 通常使用一个第三方. 使用完全可信的第三方的非否认协议在许多文献[1~3]中已被讨论, 使用半可信的第三方(STTP)的非否认协议被讨论的较少[4]. 本文主要提出了带有脱线半可信第三方的非否认交换协议.

2 可验证的加密

将基于文献[6]带盲密文的可验证加密[4]与文献[5]中的技术结合起来对文献[4]的方案修改. 修改后的的方案作为协议设计的基础, 修改后方案描述如下: 初始化: 系统参数 n, g, v, H (公开), 其中 $n = PQ$ 而 $P = 2p + 1$, $Q = 2q + 1$, p, q 都是大素数. $g \in Z_n^*$ 是一个 pq 阶元, v 是素数, H 是 hash 函数, P, Q, p, q 是保密的.

STTP 的私钥和公钥对为 SK/PK, $PK = g^{SK} \bmod n$

对消息 m (保密) 的加密为: 加密者随机选择 ω, 令 $W = g^{\omega} \bmod n$, $V_T = m(PK)^{\omega} \bmod n$ 则 (W, V_T) 就是 m 的密文.

可验证加密的生成: 令 $V = (V_T)^v \bmod n$, $M = m^v \bmod n$, 加密者随机选择 u, 计算 $\alpha = g^u \bmod n$ 和 $A = ((PK)^v)^u \bmod n$ 令 $c = H(g \| W \| (PK)^v \| V/M \| \alpha \| A)$ 和 $r = u - c\omega$, 则 (r, c, M) 就是可验证加密.

可验证加密的验证: 收到 (W, V_T) 和 (r, c, M) 计算出盲密文 (W, V), 其中 $V = (V_T)^v \bmod n$, 然后, 验证等式 $c = H(g \| W \| (PK)^v \| V/M \| g^r W^c \| ((PK)^v)^r (V/M)^c)$, 用以说明 (W, V_T) 是对 $M = m^v \bmod n$ 的根的加密.

STTP 盲解密: 若 STTP 收到 (W, V) 和 (r, c, M) 首先验证等式 $c = H(g \| W \| (PK)^v \| V/M \| g^r W^c \| ((PK)^v)^r (V/M)^c)$ 是否成立, 若成立, 则计算 $W^{SK} \bmod n$, 只要得到 $W^{SK} \bmod n$ 就可获得消息 $m = V_T / W^{SK}$. 其中 v 的选取应该保证由 $M = m_v \bmod n$ 是难计算出 m 的.

3 使用半可信第三方的协议

协议中使用的记号: m 表示消息, $X \xrightarrow{} Y$: U 表示由 X 向 Y 发送消息 U. $X \leftrightarrow Y$: U 表示 X 利用 FTP 从 Y 公布的路径下取

收稿日期: 2001-03-01; 修回日期: 2001-06-21
基金项目: 国家教育部高校骨干教师资助项目

得 $U.EO-C=S_O(R,M,W,V_T,r,c)$ 是 O 的签名,表示发送密文的证据;$ER-C=S_R(O,M,W,V_T,r,c,EO-C)$ 是 R 的签名,表示收到密文的证据;$EO-B=S_O(R,M,W,V,r,c)$ 表示 O 向 STTP 提交盲密文的证据,其中 $V=(V_T)^v \bmod n$;$ER-B=S_R(O,M,W,V,r,c)$,表示 R 向 STTP 提交盲密文的证据;$EO-m=S_O(R,m)$,表示 O 向 R 发送消息 m 的证据;$ER-m=S_R(O,m)$ 表示 R 收到消息 m 的证据,$ES-W=S_{STTP}(O,R,W^{SK} \bmod n)$ 表示 STTP 公布 $W^{SK} \bmod n$ 的证据. 在协议设计中假定双方已就传送的消息进行了承诺. 协议中有三个子协议组成,Exchange、abore 和 resolve 子协议.

Exchange 子协议

①$O \xrightarrow{} R$: $R, M, (W, V_T), (r, c), EO-C$

如果 R 放弃则停止协议,否则

②$R \xrightarrow{} O$: $O, ER-C$

如果 O 放弃则执行 abort 子协议,否则

③$O \xrightarrow{} R$: $R, EO-m, m$

如果 R 放弃则执行 resolve 子协议,否则

④$R \xrightarrow{} O$: $O, ER-m$

如果 O 放弃则执行 resolve 子协议

Abort 子协议

$O \xrightarrow{}$ STTP: $R, EO-$ ABORT

如果 resolved 则 STTP $\xrightarrow{} O$: $ER-B, W^{SK} \bmod n, ES-W$ 否则

$O \xleftarrow{}$ STTP: $O, R,$ ABORTED$=S_{STTP}(O, R, EO-$ ABORT$)$

Resolve 子协议

$P \xrightarrow{}$ STTP: $M, (W, V), (r, c), EP-B$

若协议已经 abort 则

STTP $\xrightarrow{} P$: $O, R,$ ABORTED$=S_{STTP}(O, R, EO-$ ABORT$)$ 否则

$O \xleftarrow{}$ STTP: $O, R, W^{SK} \bmod n, ES-W, EP-B$

$R \xleftarrow{}$ STTP: $O, R, W^{SK} \bmod n, ES-W, EP-B$

其中 P 可以是 O 或 R,$EP-B$ 表示:当 $P=O$ 时,$EP-B$ 为 $EO-B$;当 $P=R$ 时,$EP-B$ 为 $ER-B$. 在协议中无论是 O 还是 R 都可以产生盲密文,当需要时可以将其发送给 STTP.

4　协议的分析

协议中参与的双方都是诚实时,协议正常结束. 若有异常情况时使用子协议,由 O 激活的 Abort 子协议向 STTP 提出终止请求;由 O 或 R 执行的 Resolve 子协议向 STTP 发送盲密文,验证后 STTP 盲解密并公布. 协议不要求参与双方时钟的同步,每个参与方都可以单方面终止协议而不破坏公平性.

公平交换协议应该满足如下 5 个性质[3]

(1)有效性:指若两个参与者行为正确,在不涉及第三方的情况下,仍然能获得各自所需的东西.

(2)公平性:指协议完成后,或者每个参加者得到自己需要的或者谁什么也得不到.

(3)终止性:在协议执行的任何时间,每个参加者可单方面终止协议而不破坏公平性.

(4)不可否认性:若消息已经从 O 送给 R,O 不能否认是消息发方,R 也不能否认收到了消息.

(5)第三方的可验证性:指若由于第三方的行为不正确导致某一方失去公平,在争论中可以证明第三方的欺骗.

我们的协议同样应该满足这些性质. 在我们的协议中假定通信信道是可恢复的[2].

结论 **1**　若 O 和 R 之间的通信信道是可恢复的,则协议满足有效性要求.

证明　由有效性定义及 exchange 子协议知,结论显然成立.

结论 **2**　若 STTP 与每个参与者之间的通信信道是可恢复的,则协议满足公平性要求.

证明　若协议中的双方都是诚实的,协议完成后,O 和 R 得到自己想要的,公平性被保持.

若 O 在①发送完消息后从 R 没有获得任何消息,则 O 可以激活 abort 子协议,如果 R 已经执行 resolve 子协议,O 可以获得 STTP 公布 $W^{SK} \bmod n$ 的证据 $ES-W$ 以及 R 提交盲密文的证据 $ER-B$,这两个值可以说明 R 收到消息 m,此时 O 和 R 得到自己想要的,公平性被保持.

若 O 发送了消息 $EO-m$ 后,没有从 R 获得任何消息,则 O 激活 resolve 子协议以获得 $W^{SK} \bmod n, ES-W$,它们可以用来代替 $ER-m$,证明 R 收到了消息 m.

若 R 在执行完①后直接终止协议,则 O 和 R 谁也没有获得有用的信息,公平性成立.

若 R 在执行完②后没有从 O 得到任何消息,则 R 可以激活 resolve 子协议以获得 $ES-W$ 和 $W^{SK} \bmod n$ 从而得到消息 m.

因此,协议中没有哪一方比另一方处于有利地位,所以协议满足公平性要求.

结论 **3**　若 STTP 与每个参与者之间的通信信道是可恢复的,则协议满足终止性要求.

证明　首先 O 可以通过以下几个途径终止协议:

——在 exchange 子协议中 O 收到 $ER-m$ 后,协议正常结束. 此时 O 拥有 $(ER-C, ER-m)$,R 拥有 $(EO-C, EO-M)$,O 和 R 分别得到自己想得到的,所以协议不仅能终止而且保持公平性;

——在执行③之前通过激活 abort 子协议,终止协议的执行,此时 O 拥有 ABORTED,R 拥有 $EO-C$ 和密文,R 没有解秘密钥不能得到有用信息,这时 O 和 R 什么也没得到,协议保持公平性;

——通过激活 resolve 子协议,由协议知,若执行 resolve 之前已经由 O 调用了 abort 子协议,则协议能够终止且终止时的公平性如上分析不会被破坏;否则执行

$O \xleftarrow{}$ STTP: $O, R, W^{SK} \bmod n, ES-W, EP-B$

$R \xleftarrow{}$ STTP: $O, R, W^{SK} \bmod n, ES-W, EP-B$

然后协议终止,此时 O 拥有 $(W^{SK} \bmod n, ES-W, EO-B, ER-C)$,$R$ 拥有 $(W^{SK} \bmod n, ES-W, EO-B, EO-C)$,显然在这种情况下 O 和 R 分别得到自己想要的,所以协议不仅能终止而且保持公平性.

由假设 STTP 与每个参与者之间的通信信道是可恢复的, 因此, 由 O 激活的 abort 和 resolve 子协议可以在有限的时间内完成. 这就使得 O 总可以终止协议, 并且 O 单方面终止协议时没有破坏公平性.

另一方面, 同上述分析 R 也可以单方面终止协议的执行但仍然保持协议的公平性. 所以, 我们的协议满足及时的终止性.

结论 **4** 若 STTP 与每个参与者之间的通信信道是可恢复的, 则协议满足不可否认的要求.

证明 协议结束时 O 有 $(ER-C, ER-m)$ 或 $(ER-C, ES-W, ER-B)$ 或 $(ER-C, ES-W, EO-B)$ 或 ABORTED. D, R 有 $(EO-C, EO-m)$ 或 $(EO-C, ES-W, EO-B)$ 或 $(EO-C, EO-m)$ 或 ABORTED. 若 O 否认发送了消息 m, R 可以向仲裁者出示证据 $EO-C, EO-m$ 或 $EO-C, ES-W$ 和 $EO-B$, 仲裁者将检查: O 对密文的签名 $EO-C$; O 发送 m 的证据 $EO-m$; 或 O 向 STTP 提供盲密文的签名 $EO-B$; 以及 STTP 公布数据的签名 $ES-W$; m 是否等于 $V_T/W^{SK} \bmod n$. 如果检查都成立则仲裁者可以确定 O 的否认是无效的.

若 R 否认收到了消息 m, O 有 $ER-C, ER-m$, 或 $ER-C, ES-W$ 作为证据, 分别表示 R 收到密文 (W, V_T) 和消息 m 的不可否认证据, 及 STTP 发送 $W^{SK} \bmod n$ 的证据. 其中假定若 STTP 在公共路径中公布了 $O, R, W^{SK} \bmod n, ES-W, EP-B$, 就认为 R 已经获得消息 m.

结论 **5** 若 STTP 与每个参与者之间的通信信道是可恢复的, 并且 STTP 对任何传送到的请求最终被迫发送有效的响应, 则 STTP 是可验证的.

证明 每个参与者有 STTP 盲解密的证据 $ES-W$, 所以一旦出现不公平可以出示 $ES-W$ 说明 STTP 的欺骗.

协议的其它性质与文献[4]相同.

5 结语

在一些文献中给出了双方和多方的使用半可信第三方的公平交换协议, 但并没有讨论协议的非否认性. 在本文中首次提出了基于半可信脱线第三方的公平非否认协议. 基于半可信中立方的非否认协议还有许多工作要做.

参考文献:

[1] J Zhou, D Gollmann. A fair Non-repudiation protocol [A]. In Proceeding of 1996 IEEE Symposium on Security and Privacy [C], Okland, California, May 1996: 55-61.

[2] N Asokan. Optimistic fair exchange of digital signatures [J]. In IEEE Journal on Selected Areas in Communications, 2000, 18(4): 593-610.

[3] N Asokan, V Shoup, M Waidner. Asynchronous protocols for optimistic fair exchange [A]. 1998 IEEE Symposium on Security and Privacy [C], 1998: 6-17.

[4] Feng Bao, Robert H Deng. An efficient fair exchange protocol with off-line semi-trusted third party [A]. Cryptec' 99 [C], Hong Kong, 1999: 37-47.

[5] Markus Stadler. Publicly verifiable secret sharing [A]. In Eurocrypt' 96 [C], LNCS1070, Springer-verlag Berlin Heidelberg, 1996: 190-199.

[6] Feng Bao, R H Deng, WenboMao. Efficient and practical fair exchange protocols with off-line TTP [A]. 1998 IEEE Symposium on Security and Privacy [C], 1998: 77-85.

[7] 周展飞, 周典萃, 王贵林, 卿斯汉. 电子商务协议的公平性 [J]. 电子学报, 2000(9): 13-15.

作者简介:

王彩芬 女. 1963 年出生于河北省安国市. 1983 年获兰州大学数学力学系理学学士学位, 1998 年获兰州大学计算机科学系理学硕士学位. 现为西北师范大学数学与信息科学学院副教授, 西安电子科技大学通信工程学院密码学专业博士生, 主要从事密钥托管和电子商务中协议的设计与分析方面的研究.

葛建华 男. 1961 年出生于江苏南通. 西安电子科技大学通信工程学院教授, 博士, 博士生导师, 主要从事网络安全和 HDTV 方面的研究. 承担国家级项目若干项, 发表论文多篇.