第 26 卷第 2 期 电 子 与 信 息 学 报 Vol.26No.2
2004 年 2 月 Journal of Electronics & Information Technology Feb. 2004

一种基于公告牌的反拒认协议 [1]

张键红 王继林 王育民

(西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要: 反拒认协议是为参与电子交易的双方事后抵赖提供不可否认证据的一个重要安全协议。然而，交易的高效性、公平性也是人们所追求的目标。该文基于公告牌给出了一个高效的、公平的反拒认协议，有效地解决了由于可信的第 3 方负担过重造成的瓶颈。并实现了公平性，高效性，低计算量特点。

关键词: 反拒认，公平性，电子证据，高效性

中图分类号: TN919.1 **文献标识码**: A **文章编号**: 1009-5896(2004)02-0322-04

A Non-repudiation Protocol Based on Bulletin Board

Zhang Jian-hong Wang Ji-lin Wang Yu-min

(*National Key Lab of ISN, Xidian University, Xi'an* 710071, *China*)

Abstract Non-repudiation is a security protocol to provide non-repudiation evidences for two transaction parties against the other falsely denying a particular event in electronic commerce while efficiency and fairness are what people have expected during electronic commerce. In this paper, a fair non-repudiation protocol based on bulletin-board is proposed to resolve the problem that a trusted third party brings into bottle-neck of communication. This protocol can achieve non-repudiation service in an efficient and practical way.

Key words Non-repudiation, Fairness, Electronic evidence, Efficiency

1 引言

随着电子商务的迅速发展，越来越多的商业活动转移到 Internet 网上。计算机网络为进行各种电子服务提供了有效的手段，但对计算机的依赖性也使信息系统面临巨大的挑战，为此，对网络的安全提出了更高的要求。反拒认协议是计算机网络中一项重要安全服务，它主要防止某项事务的参与双方的任意一方在事后进行抵赖，拒绝对自己的行为负责。一般情况下，在电子事务中通信的双方不是面对面，并且双方相互不信任，消息的发送者希望在发送消息前得到接收方的电子收据，同时接收方也希望在发送电子收据前得到发送方的消息。为了解决此矛盾，公平的反拒认协议必须在协议的每一步中为双方提供不可否认的证据，使得在任何时候通信的一方并不比另一方占更大优势。当发生争议时，争议的解决依赖于交易双方所持有的不可否认证据。不可否认证据应满足 (1) 证据的产生者可被认证； (2) 证据的完整性能被认证；(3) 证据的有效性不可抵赖。

反拒认协议的设计可分为两类：一类是没有可信的第 3 方存在，基本思想是交易的双方逐步地把秘密泄露给对方 [1,2]，但这种方案太复杂、计算量和通信量大，不实际。另一类是基于可信的第 3 方。基于可信第 3 方的设计方法也是目前认为可行的一种方法。一个好的反拒认协议应使得可信第 3 方尽可能少地参与，消息数目尽可能的少，发送方和接收方尽可能的公平。本文基于一个消极的 (passive) 第 3 方即公告牌设计一个仅需 5 次交互的高效公平的反拒认协议，同时解决了由于主动的第 3 方负担过重引起的通讯和计算瓶颈问题。

[1] 2002-09-23 收到，2003-04-14 改回
国家自然科学基金项目 (No:19931010) 资助课题

2 符号表示

本文用以下符号表示：X, Y：表示两个消息 X 和 Y 的级连；$H(X)$ 表示对消息 X 的哈希值；$\mathrm{PK}_A(\cdot)$ 表示用 A 的公钥加密；PK_A 表示 A 的公钥；$\mathrm{Sign_A}(m)$ 表示 A 对消息 m 的签名；$\{m\}_K$ 表示用对称钥 K 对消息 m 加密；A→B, X 表示 A 给 B 发送消息 X。A←B, X：表示 B 主动从 A 上获取消息 X。

3 协议

对反拒认协议的研究越来越受到关注，国际标准化组织 (ISO) 先后于 1989 和 1996 年制定了两个相关的标准 [3,4]。近几年，关于公平反拒认协议的不同方案被提出，文献 [5] 中利用可信任的第 3 方提出了一个反拒认协议，有效地解决了拒认问题，但在公平性上却存在弱点；文献 [6] 给出了一个能够双向反拒认的协议，可以简单地解决可能发生的争端，但是通信量太大，一次协议要进行 11 次交互通信；文献 [7] 中的方法虽仅需要 5 次交互，但问题在于接收者发出反接收者拒认后可能无限等待，并且，如果消息发送方 A 具有恶意，它对时间的估计和网络通信的不可靠性的恶意的阻挠和干扰会使消息接收者 B 处于不利地位。尽管上述文献中的协议存在着不同的缺陷，但是他们的设计思想是值得我们借鉴的。一个好的反拒认协议应以通信的双方的公平性，交换信息少，信息短为目标。本文为了减少可信第 3 方的负担，基于消极的第 3 方公告牌提出了一个高效的反拒认公平协议，避免了由于第 3 方负担过重造成的系统瓶颈问题。

3.1 基于公告牌的一种反拒认协议

由于数字签名的不可否认性、不可伪造性、完整性，所以数字签名是实现反拒认协议一个有力的工具。在反拒认协议中，发送者和接收者的数字签名就成为不可否认的证据。但由于公钥私钥是有期限的，因而，证据具有有效期。在有效期内的证据才是有效的证据，为了防止通信一方在协议执行以后宣布私钥泄露，申请证书撤消，我们必须在签名中加入时戳，为了简单讨论，在下面的协议设计中忽略时戳。

在通常的反拒认协议中，可信的第 3 方都要主动地参与通信，当通信量太大时，由于负担太重就可能造成通信瓶颈，为了减少第 3 方的通信量和对第 3 方的依赖性，本文采用的第 3 方是一个消极的 (passive) 第 3 方公告牌 (Bulletin board)，我们的协议由发送方 A，接收方 B 和一个消极第 3 方公告牌即反拒认服务器 NRS(Non-Repudiation Server) 构成 (注：公告牌是一个可读、写但不能修改的公告牌)。消息 m 是由 A 发送到 B，在整个通信过程中不允许有第 3 方知道，A 需要在 B 知道消息 m 以前得到 B 对此消息的电子收据；同时，接收方 B 也希望得到此消息是由发送方 A 发出的电子证据。主要思想是：先用对称密钥 K 对消息 m 加密，把密文传给 B, B 签名以后把数据张贴到公告牌上，接着 A 用接收者 B 的公钥对 K 进行加密，把密文张贴到公告牌上，最后，B 取回密钥 K 解密就得到了消息 m。协议一共分为 5 步进行 (见图 1)：

(1) A→B: MSG1, 其中 MSG1=M, N, $c = \{m\}_k$。M=A,B, NRS, TID(Transaction IDentity 交易号)，T_b(B 张贴数据的最迟时间)，$h(c)$。$N = \mathrm{Sign_A}(M)$。

(2) B→NRS: MSG2, 其中 MSG2=U, V, M, N。U=A,B, NRS, TID, T_b, T_a (A 张贴密钥的最迟时间), $V = \mathrm{Sign_B}(U)$。

(3) NRS←A: MSG3, 其中 MSG3=MSG2。

(4) A→NRS: MSG4, 其中 MSG4=P, Q。P=A,B,NRS, $\mathrm{PK_B}(K)$, $h(m)$, TID, T_b, T_a, $Q = \mathrm{Sign_A}(P)$。

(5) NRS←B: MSG5, 其中 MSG5=MSG4。

下面我们对上述的协议进行分析：

第 1 步　A 随机选取一个对称密钥 K，用密钥 K 加密消息 m 传给 B，同时发送交易号 TID，密文的哈希值 $h(c)$, T_b, NRS 和签名给 B。其中 TID 作为整个协议交易过程中的标识

符，它将协议中交互的每条消息有机地联系在一起，同时，也使任何人在公告牌上很容易地找到与 TID 相关的信息。NRS 是 A 和 B 张贴数据的公告牌。如果这时 B 终止与 A 的交易，B 并不比 A 占更多的优势。因为 B 收到是消息 m 的密文，且没有对应的密钥，因此，B 不能解读密文。从而保证了 B 和 A 的公平性。

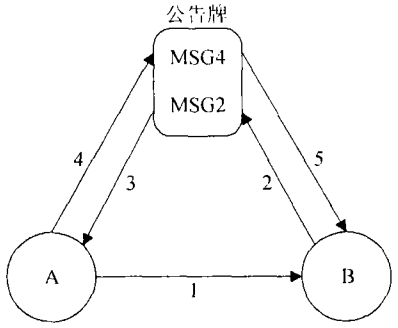

图 1 公平的反拒认协议

第 2 步 当 B 接收到消息 MSG1 后，首先验证签名的合法性以确认确实来自于发送者 A，签名验证通过后，如果 B 认为自己不可能在时间 T_b 以前把数据张贴到 NRS 上就终止协议，否则，就继续执行协议，目的是防止 A 无限制的等待。接着把 MGS2 张贴到公告牌上，因 MGS2 中有发送者 A 和 B 的签名，这条数据是 B 对从发送方 A 处得到了消息 m 密文的确认。

第 3 步 发送方 A 从公告牌 NRS 上得到 MSG2 。A 首先验证数据 MGS2 中 M, N 是否与自己第一次发给 B 相一致，如果一致就继续执行协议；否则，终止协议的执行，接着验证消息 MGS2 中的 B 的签名是否正确，如果正确就继续执行协议，最后还要检验能否在时间 T_a 以前提交密钥，如果不能就终止协议，因为有些消息对时间比较敏感，超过一定时间期限之后对于 B 来说就失去了价值。当所有的检验都通过后，执行第 4 步。

第 4 步 A 张贴用 B 的公钥加密的密钥 K 。

第 5 步 B 从公告牌 NRS 上取得消息 MGS4 ，首先验证 A 的签名，如果正确说明密钥来自发送者 A；接着用 B 的私钥解密得到密钥值 K，再用密钥 K 解密 $\{m\}_K$ 得到消息 m；最后验证 m 的哈希值是否与 MSG4 中的 m 的哈希值一致。

3.2 解决争端

争端 1 发送者拒认。即接收者 B 声称从 A 处得到消息 m ，发送者却拒绝承认，仲裁机构 (judge) 需让 B 出示证据。

第 1 步 B 向 judge 提交证据 TID, M, N, K, 公告牌， $\{m\}_K$ ， m 。

第 2 步 judge 验证如下操作：(1) 验证消息 MSG1 中的 N 是否为 A 对 M 的合法签名。(2) 用 B 的公钥加密 K 与公告牌上的消息 MSG4 中 $\mathrm{PK_B}(K)$ 比较是否相等。(3) 验证公告牌上的 A 对 $\mathrm{PK_B}(K)$ 签名。(4) 比较用 K 解密 $\{m\}_K$ 所得的消息与提交的 m 是否一致。

如果上述的验证通过，断定 A 在说谎。

争端 2 接收者拒认。即发送方 A 宣称发送了消息 m 给 B ，但 B 却拒绝承认，仲裁机构需 A 出示以下证据。

第 1 步 A 向 judge 提交证据 MSG3, TID, K, 公告牌， MSG4 。

第 2 步 judge 验证如下操作：(1) 验证公告牌上 MSG4 中 A 签名的合法性。(2) 比较用 B 的公钥加密 K 所得的密文与 MSG4 中的密文是否一致。(3) 验证 MSG3 是否与公告牌上的 MSG2 相一致。(4) 验证 MSG2 中 B 签名的合法性。

如果上述的验证通过，断定 B 在说谎。

争端 3　发送者实行欺骗，即消息发送者 A 用另一个密钥 K_1 加密消息 m，而发送给接收方 B 的密钥却是 K。

第 1 步　B 向 judge 提交证据 K, m, MGS1, $h(c)$, $\mathrm{PK_B}$, 公告牌。

第 2 步　judge 验证如下：(1) 验证 MSG1 中 A 的签名的正确性。(2) 验证用 K 加密 m 所得密文的哈希值是否与 MGS1 中的 $h(c)$ 相一致。(3) 比较用 B 的公钥加密 K 所得的密文是否与公告牌上的 MSG4 中用 B 的公钥加密对称钥相一致。

如果上述的验证不通过，断定 A 确实实行欺骗。

3.3 协议的分析

由以上的协议的执行可知，本协议具有以下性质：

公平性　由以上讨论可知，当消息 MSG1 传给 A 以后，如果终止协议，A 并不比 B 占更大优势，因任何人都可以看到公告牌上的内容，因而，公告牌上的信息为 A,B 提供了不可否认的证据。

高效性　在整个协议过程中，公告牌只是作为一个消极的第 3 方，不参与任何操作，从而，解决了由于第 3 方负担太重造成的通信瓶颈。

保密性　在整个过程中消息 m 的内容仅仅 A 和 B 知道，防止了信息的泄露，克服了文献 [4–6] 的缺点。

实用性　由于我们的可信的第 3 方是一个消极的第 3 方，不主动参与任何通信和计算，因而，造成通信和计算瓶颈的可能性很小。是一种很实用的协议。

4 结论

反拒认协议是当前电子商务发展中亟需解决的问题。如：挂号电子邮件，合同签字，安全公文传递等都离不开它，它主要是防止参加某项事务的双方事后任一方进行抵赖，拒绝对自己的行为负责。本文基于半可信的第 3 方模型，提出了一个公平的反拒认协议，解决了收发双方的拒认问题，具有公平性、高效性，计算量少、实用性等特点，采用公告牌作为一个消极的第 3 方有效地解决了第 3 方由于负担太重造成通信瓶颈的问题。同时采用公告牌也防止由于信道不可靠造成的信息丢失、重传与不诚实的接收者的说谎问题。是一种有实际意义的公平的反拒认协议。

参 考 文 献

[1] Even S, Goldreich O, Lempel A. A randomized protocol for signing contracts[J]. *Communication of the ACM*, 1985, 28(6): 634–647.

[2] Brickell E, Chaum D, Damgard I, Graaf J. Gradual and verifiable release of a secret[A]. Advances in Cryptology-Proceeding of CRYPT87[C] LNCS, Berlin, Springer-Verlag, 1988: 345–353.

[3] ISO/IEC13888-2, Information technology-security techniques-non-repudiation-Part 2 Mechanisms using symmetric techniques (1998).

[4] Zhou J, Gollmann D. Observations on non-repudiation[A]. Lecture Notes in Computer Science 1163, Advances in Cryptology: Proceedings of Asiacrypt'96[C], Kyongju, Korea, Springer-Verlag, November 1996: 133–144.

[5] 蒋晓宁，叶澄清. 电子证据与反拒认协议 [J]. 通信学报，2000, 21(7): 76–81.

[6] Zhou J, Gollmann D. A fair non-repudiation protocol[A]. Proceedings of 1996 IEEE Symposium on Security and Privacy [C], Oakland, California IEEE Computer Society Press, May, 1996: 55–61.

[7] Kim K, Park S, Baek J. Improving fairness and privacy of Zhou Gollmann's fair non-repudiation protocol[A]. Proc. of 1999 ICPP Workshops on Security [C], IEEE Computer Society Wakamatsu, Japan, Sep 21–22, 1999: 140–145.

张键红：　男，1975 年生，博士生，研究方向为网络安全、电子商务.

王继林：　男，1962 年生，博士生，研究方向为网络安全、电子商务.

王育民：　男，1936 年生，教授，博士生导师，研究方向为网络安全、信息论、编码、密码学.