一种新的多方不可否认协议*)

李艳平　司光东　王育民
(西安电子科技大学 ISN 国家重点实验室　西安 710071)

摘　要　首次指出不可否认协议运行结果可分为认证强公平和期望强公平，其中后者优于前者。利用 GPS 数字签名方案，提出一个新的带离线可信第三方的多方不可否认协议，该协议实现了期望强公平且允许发方给不同的接收方发送不同的消息，突破了先前协议只允许发方给不同的接收方发送同一消息的局限性。协议同时允许发方自由选择交易方，使得交易灵活而符合实际。最后给出协议的安全性分析。

关键词　可信第三方，不可否认协议，组播，可恢复信道

A New Multi-party Non-repudiation Protocol

LI Yan-Ping　SI Guang-Dong　WANG Yu-Min
(State Key Lab of Intergrated Service Network, Xidian University, Xi'an 710071)

Abstract　Expected strong fairness and certified strong fairness, two executie results of non-repudiation protocols, are firstly introduced, and the former is superior to the later. Based on the GPS digital signature scheme and a group encry ption scheme, a new multi-party non-repudiation protocol with an off-line trusted third party is presented. The presented protocol provides"expected strong fairness", and allows one sender to send different messages to multiple different recipients, eliminates the previous restriction on the exchange of the"same message". The sender can barter with any recipients at his will and it makes the protocol more practical. The security analysis are given finally.

Keywords　Trusted third party, The non-repudiation protocol, Multicast, Resilient channel

1　研究背景和相关工作

通过网络发送有价消息(如订货单、电子支票)时，往往易产生收发方否认的纠纷。目前较可取的解决方案是借助一离线可信第三方(Trusted Third Party，后称 TTP)，在意外情况下(如某方的错误行为或有意欺诈或网络传输的失败)介入协议，仲裁纠纷，生成签名证据来宣判协议的运行情况，保证参与方之间的公平性。

不可否认协议及其实现技术是多种多样的，但一个好的不可否认协议必须实现不可否认性、公平性和时效性，时效性又会影响协议的公平性，所以不可否认协议的公平性是一个关键性质。关于不可否认的公平性已有粗略划分[1]：弱公平性、强公平性。而在实现强公平的基础上可根据 TTP 签名证据的不同可对强公平性进行进一步的细化：一种是 TTP 签名证据不同于协议正常运行下收发双方生成的不可否认证据，但这种"宣判证据"可用来替代收发方的证据并具有相同的法律效力，即参与方在协议末获得自己意定的其他参与方的消息证据或 TTP 的签名证据来证明协议的运行情况，故称协议实现了认证强公平；另一种是 TTP 签名证据与参与方在正常情况下生成的证据一模一样，即不管 TTP 是否介入协议，诚实参与方在协议执行末一定能获得自己意定的消息和不可否认证据，故称协议实现了期望强公平。这时协议外的人从参与方持有的不可否认证据不能判定 TTP 是否介入了该协议，从而避免了在实际电子商务应用中人们对 TTP 介入协议原因的猜测以及对协议参与方名誉可能造成不良的影响。因为参与方执行协议的希望是得到协议初协商好的其他参与方的交换信息及不可否认证据，而非 TTP 的签名证据，所以在计算量和通信量等条件相同的情况下，实现期望强公平的协议优于实现认证强公平的协议。

现已公开发表的不可否认协议多数实现的是认证传递[1]，最近 Wang CF 等提出一个带离线半可信 TTP 的不可否认协议，其借助 CEMBS 密码技术[2,3]利用半可信 TTP 的公钥生成可验证密文，意外情况下 TTP 可协助收方恢复发方发送的消息，但发方却只能得到 TTP 的签名证据，即该协议对收方实现了期望强公平，对发方却仅实现了认证强公平。Markowitch 和 Kremer 利用透明 TTP 提出一个实现了收发方的期望强公平[4]的不可否认协议，但该协议仅适用于双方间进行。实际上现有的多方不可否认协议很少且都是发方对多个收方发送的同一消息。一旦发方想给不同的发方发送不同的消息，就得启用新一轮的协议，耗费量大且时间上不能达到同步执行(只能依次执行)。本文利用 GPS 数字签名方案，设计了一个实现期望强公平的多方不可否认协议。该协议允许发方对多个接收方同时发送不同的消息，突破了先前协议只允许发方给不同的接收方发送同一消息的局限，经分析知本方案满足不可否认协议的三条基本性质以及机密性。

2　预备知识：GPS 数字签名

该签名可通过两个阶段实现：签名者先产生一个承诺签名，然后由签名者本人或 TTP 将其转换为最终签名用作发送和接收消息的不可否认证据。在我们协议中，TTP 先选择两个大的强素数 p、q，其积为 n，再选一个阶为 $\phi(n)$ 的元 α 以及一个小整数 c 使得 $\gcd(\phi(n),c)=1$，然后 TTP 计算满足 $cd\equiv 1(\bmod \phi(n))$ 的 d 以及 $\beta=\alpha^c(\bmod n)$，最后 TTP 公开 α、n、β、c，保密 d 丢弃 p、q。签名者 U_i 任选一随机数 x_i 作为秘密密钥，计算其对应公钥 $y_i=\alpha^{x_i}(\bmod n)$ 并向某证书中心为 y_i 申请一公钥证书。A 要签消息 m，需选一随机数 r_A 并计算 $t_A=$

*)基金项目：国家"973"重大基础研究项目(G1999035804)资助，陕西省自然科学基础研究计划项目(2004A14)。李艳平　博士研究生，研究兴趣为安全协议的设计与分析。

$\beta'^{z_A} \pmod n$，$Z_A = c \cdot r_A + h(t_A, m) \cdot x_A \pmod{\psi(n)}$。我们称$(t_A, z_A)$为 A 的承诺签名，记作 $\mathrm{ComS}_A(m)$。接收者 B 检验 $\alpha^{Z_A} \pmod n \stackrel{?}{=} t_A \cdot y_A^{h(t_A,m)} \pmod n$。若相等则说明在意外情况下，TTP 有能力从承诺签名中恢复主体 A 的最终签名。然后由 A 自己计算 $t'_A = \alpha^{r_A} \pmod n$ 或由 TTP 计算，$t'_A = t_A^d \pmod n$，(t'_A, z_A)称为 A 的最终签名，记作 $\mathrm{FinalS}_A(m)$。验证最终签名只需比较。$t_A \stackrel{?}{=} t'_A \pmod n \Leftrightarrow \alpha^{z_A} \pmod n \stackrel{?}{=} t'^{c}_A \cdot y_A^{h(t'^{c}_A \bmod n, m)} \pmod n$。验证简单高效，安全性论证详见文[5, 6]。

3 本文协议

3.1 协议中的基本记号

R：其中 $R=(R_1, R_2, \cdots, R_n)$，为本协议中消息的接收者的全体集，其中 R_i 为成员的数字化身份符；

$A \Rightarrow R$：发方 A 利用组播技术向 R 中成员发送消息；$A \rightarrow B$：发方 A 向接收者 B 发送消息；

R'：返回给发方 A 有效的承诺签名的接收者的集合，其中成员用 $R'_i \in R'$ 表示；

$c_i = E_{k_i}(M)$：利用对称加密算法用密钥 k_i 对消息 M_i 进行加密得密文 c_i，加密密钥 $k_i = n_i \oplus k$；

$v_i = PE_{R_i}(n_i)$：n_i 为由发方 A 为收方 R_i 选取的与 k 同长的随机数，n_i 的汉明重量为 $|k|/2$(1 的个数)；

$l_i = H(M_i, n_i)$：消息 M_i 的标识，$H()$表示一强单向 Hash 函数，“,”表示链接；

T：收发方协商好的时间限，即只有过了该时间限后，TTP 才受理 $\mathrm{Recovery}_x$ ($x \in R \cup A$)协议；

$EOO_i = \mathrm{ComS}_A(TTP, T, PE_T(k), H(k) R_i, l_i, c_i)$：发方 A 发送消息 m 给 R_i 的承诺不可否认证据；

$EOR_{R_i} = \mathrm{ComS}_{R_i}(TTP, T, PE_T(k), H(k), R_i, l_i, c_i)$：收方 R_i 收到消息 m 的承诺不可否认证据；

$NRO_i = \mathrm{FinalS}_A(TTP, T, PE_T(k), H(k) Ri, l_i, c_i)$：发方 A 发送消息 m 给 R_i 的有效不可否认证据；

$NRR_{R'_i} = \mathrm{FinalS}_{R'_i}(TTP, T, PE_T(k), H(k), A, l_i, c_i)$：收方 $R'_i \in R'$ 收到消息 m 的有效不可否认证据；

S_x：表主体 X 普通签名，即用户 X 利用密钥对(x_i, y_i)根据 DSA 签名算法得到签名(r_i, s_i)；

$Early = S_T(Early, A, R, T)$：TTP 通告发起 $\mathrm{Recovery}_x$ 协议请求的时间过早；

$Abort = S_A(Abort, A, R'', L)$：发方放弃与主体 $R_j \in R'' \subseteq R' \subseteq R$ 进行交易的请求，$L = \{l_j\}$集合；

$Rec_x = S_x(\mathrm{Rec}_x, X, Y, l_i)$：主体 X 要求恢复协议的请求，若 $X \in R$，则 $Y = A$；若 $X = A$，则 $Y \in R$；

$Con_a = S_T(Con_a, A, R'', L)$：TTP 对放弃协议请求的确认；

$Con_e = S_T(Con_e, A, R, T)$：TTP 对协议运行错误的确认。

3.2 协议描述

假设本协议中用于加解密或签名验证的公钥均有证书中心颁发的数字证书。并设 TTP 与通信各方之间的信道是可恢复的，即送入该信道消息必在有限未知的时间内传给收方。在协议进行前，参与方已约定好 TTP、公用参数及 Hash 函数。只有在协议出现意外时，处于离线状态的 TTP 才介入协议保证参与方的公平性。协议包括三个子协议：Main 协议，$\mathrm{Recovery}_x$ 协议以及 Abort 协议。$\mathrm{Recovery}_x$ 表示主体 X 发起恢复协议的请求，其中 $X \in R \cup A$。

Main 协议如下：

(1) $A \Rightarrow R$: $A, \mathrm{TTP}, T, PE_T(k), H(k), \{R_i, l_i, c_i, EOO_i\}$, $i = 1, 2, \cdots, n$;

(2) $R_i \rightarrow A$: R_i TTP, A, l_i, EOR_{R_i}；时间超过 A 的某时间 T'[7]，A 发起放弃协议；

(3) $A \Rightarrow R'$: $R', k, \{R'_i, \mathrm{NRO}_i\}$；若超过时间 T，则 R'_i 发起恢复协议；

(4) $R'_i \rightarrow A$: $R'_i, l_i, NRR_{R'_i}$。若超过时间 T，则 A 发起恢复协议。

第一步执行以后，每个接收方 R_i 收到了 l_i, c_i，承诺不可否认证据 EOO_i 以及由 TTP 的公钥加密的 k 的密文 $PE_T(k)$，如果有某个接收方不同意发方 A 所规定的时间限 T，其不必回复 A 即可安全退出该协议。

第二步中，A 利用相关模型[7]估计一个时间限 $T' < T$，将所有 T' 时间以前给 A 回复了有效承诺签名的接收方记为 R'，过 T' 不再接收。

第三步中，A 将 k 群有向加密给 R' 中的成员，他们各自解密 v_i 得半密钥 n_i，由 $k_i = n_i \oplus k$ 就可解密密文 c_i，最后再拿 $l_i = H(M_i, n_i)$来验证明文 M_i 和半密钥的 n_i 的正确性。若某收方不进行第四步，A 拿该方的有效承诺签名请求 TTP 帮助恢复为最终有效签名。下面即为恢复协议($\mathrm{Recovery}_X$ 协议)，X 为请求人。

$\mathrm{Recovery}_X$ 协议如下：

$X \rightarrow \mathrm{TTP}$: $R, T, X, Y, l_i, PE_T(k), H(k) \mathrm{Rec}_X, EOR_X, EOO_i$；

若 $X \in R$，则 $Y = A$，若 $X = A$，则 $Y \in R$，TTP 收到该消息后做如下验证：

验证 1　看时间是否超过 T，若没超过，则 TTP $\Rightarrow R \cup A$: $A, R, \mathrm{T}, Early$；否则

验证 2　协议是否已被 A 放弃，则 TTP 终止协议；否则

验证 3　$H(k) \stackrel{?}{=} H(PD_T(PE_T(k)))$，若不一致，则 TTP 发起错误通知 TTP $\Rightarrow R \cup A$: A, R, T, Con_e；否则

验证 4　TTP 再检验 EOR_x 是否合法，以确保 TTP 能够将其转化为合法的 NRR_x，若 EOR_x 签名无效或已执行过 $\mathrm{Recovery}_X$ 协议，主体 X 的请求就被 TTP 掷弃。否则 TTP 同时进行以下两步操作：

TTP $\rightarrow A$: A, X, l_i, NRR_X；

TTP $\rightarrow X$: $A, X, l_i, PE_X(k, \mathrm{NRO}_i$(一个 X)。

验证 2 避免协议执行重复操作，节省计算量与通信量。验证 3 用于保证加密消息的密钥 k 与向 TTP 提交的密钥的一致性。有些协议要执行到协议末接收方解密后才发觉密钥有诈[8]，这样及时终止协议可避免不必要的通信与运算量。验证 4 用于防止收方进行欺骗。因为每个接收者 $R_i = X$ 收到 Main 协议中的一条消息后，他随时都可发起 $\mathrm{Recovery}_X$ 协议借助 TTP 恢复密钥 k 以及终签名，但验证 4 要求其必须提供必要的有效证据，所以验证 4 保证 $R_i = X$ 与发方 A 之间的公平性。若上述检验均通过，TTP 用 d 密钥将承诺签名转换为最终签名发送给相应的接收方。考虑到某些情况下 A 可能在发出第一条消息后又想放弃本次协议或想放弃与若干人 R'' 的交易，所以允许 A 向 TTP 发起 Abort 协议：

$A \rightarrow \mathrm{TTP}$: $A, R'', L, Abort$；若已执行过某个 $\mathrm{Recovery}_X$ 协议，

则 TTP $\rightarrow A$: A, X, l_i, NRR_X；

否则 TTP $\Rightarrow R'' \cup A$: A, R'', L, Con_a。

我们这里允许 A 根据自己的需求而灵活的选择交易方，

其中 $R''\subseteq R'$，这主要考虑到实际情况中 A 可能会由于意外原因想结束与某方 $R'_i\in R'$ 的交易，这使得协议更灵活而符合实际。

3.3 安全性分析

我们按 Markowitch 所列的不可否认协议应满足的三个主要性质[1,4]：收发方的不可否认性、公平性、时效性以及机密性来分析本协议。

① 发方不可否认性。若发方 A 否认她发过消息 M_i，则向某仲裁机构 ADJ(Adjudicator)提供：A，TTP，T，$PE_T(k)$，$H(k)$，R_i，l_i，v_i，c_i，NRO_i，M_i，n'_i，k'，其中 n'_i，k' 分别是 v_i 和 $E_{R'}(k)$(或 $PE_{R'_i}(k)$)解密得到的密文。ADJ 逐步验证：a. $l_i\stackrel{?}{=}H(M_i,n'_i)$，$H(k)\stackrel{?}{=}H(k')$，$PE_T(k)\stackrel{?}{=}PE_T(k')$，$PE_T(k')$，$PE_{R'_i}(n'_i)\stackrel{?}{=}v_i$；b. 若上述验证都通过，计算 $k_i=n'_i\oplus k'$，验证 $c_i\stackrel{?}{=}E_{k'_i}(M_i)$；c. 若第二步验证通过，再验证 NRO_i 是 A 对关于(TTP，T，$PE_T(k)$，$H(k)$，R_i，l_i，v_i，c_i)的最终签名。若三步验证都通过，则判断 A 的确发过 m。

② 收方不可否认性。若某收方 $R'_i\in R'$ 否认接收到消息 m，A 向 ADJ 提交证据：R'_i，TTP，T，$PE_T(k)$，$H(k)$，l_i，v_i，c_i，$NRR_{R'_i}$，m_i，n_i，k'。ADJ 逐步验证：a. $l_i\stackrel{?}{=}H(M_i,n'_i)$，$H(k)\stackrel{?}{=}H(k')$，$PE_T(k)\stackrel{?}{=}PE_T(k')$；$PE_{R'_i}(n'_i)\stackrel{?}{=}v_i$；b. 若上述验证都通过，计算 $k_i=n'_i\oplus k'$，验证 $c_i\stackrel{?}{=}E_{k'_i}(M_i)$；c. 若第二步验证通过，再验证 $NRO_{R'_i}$ 是 R'_i 对关于(TTP，T，$PE_T(k)$，$H(k)$，l_i，v_i，c_i)的最终签名。若三步验证都通过，则判断 A 的确收过 m。

③ 公平性。我们来看某方有意中止协议是否会导致该主体处于有利地位。在主协议执行过程中，若某接收方 X 在第一步中止，他获得的仅是 A 的消息密文以及承诺签名，得不到任何有价值的东西，A 可发起 Abort 协议防止 X 后来利用 Recovery_x 协议获得相关证据，双方均不持有对方完整的不可否认证据。若 X 已提前发起 Recovery_X 协议，那 TTP 分别发给与完整的对方不可否认证据，协议保持公平。若 A 在第二步中止且未发起 Abort 协议，过时间 T 后接收方 X 可发起 Recovery_X 协议，而该协议也能保证 A 与 X 之间的公平。而 A 发起 Abort 协议，则 TTP 亦能保证发收方之间的公平性。若 X 在第三步中止，即不发出主协议中第四条消息，A 可发起 Recovery_A 协议，获得 NRR_X。因 TTP 与协议各方间的信道为弹性信道，故收发方必将各获所需，达到协议的目的。因此，不管是信道原因还是通信方不诚实，任何时候中断协议，都不会使协议中某一方处于弱势而蒙受损失。又由于本协议采用的是 GPS 数字签名，若协议正常结束，收发各方得到自己所期望的消息和电子证据。即使在意外情况下离线 TTP 介入协议，TTP 恢复的最终不可否认证据与收发方自己生成的最终不可否认证据具有同一形式，参与方从 TTP 处获得自己意定的消息，故本协议实现了期望强公平。

④ 时效性指协议各诚实的参与方均能在有限时间内公平的结束协议。发方 A 可发起 Abort 协议或 Recovery_A 协议可结束协议，接收者 $X\in R$ 只要不回复 A 的第一条消息且不发起 Recovery_x 协议就可公平退出协议。而 $X\in R'$ 中成员均可通过 Recovery_X 协议来强迫协议继续进行，公平结束。由于 TTP 与收发方间的信道是可恢复的，所以任意参与协议的主体均可使交换在有限时间内公平结束，保持时效性。

⑤ 机密性。指任意的参与方(包括 TTP)都不能非法读解发方发给他人的消息。解读消息途径有二：一是直接从密文读解明文，这与我们假设所选公私钥算法是安全的相悖；二是获取加密密钥 k_i，由于 $k_i=k+n_i$，而 n_i 由指定接收方的公钥加密，故敌手至多能截获 k，无法得到另一密钥分量 n_i，设 $|k|=l$ bits(至少 56bits，如 DES)，而 n_i 的汉明重量为 $l/2$，敌手的解密 $C_l^{l/2}$ 次(至少得 $C_{56}^{28}\approx 9.2\times 10^{17}$ 次)，即使敌手 1 秒解密一次，也需大约 6×10^{11} 年，故无法读解消息。

3.4 性能比较

若通过文[4]中的协议发送 n 条不同的消息，则需要依次执行 n 次协议，繁琐且时间上不能同步。我们就发送 n 条不同的消息这一事件，比较文[1]中协议和本文协议所需的计算量和通信量：

	本文协议		文[4]中协议
计算量	发方：生成 n+1 个随机数 n_i，k	$\approx$	发方：生成 n 个随机数 k_i
	各 n 次对称机密，公钥加密，EOO 和 NRO 签名	$=$	各 n 次对称机密，公钥加密，EOO 和 NRO 签名
	n+1 次 Hash 运算	$<<$	2n 次 Hash 运算
	每位收方：各 1 次 EOR 和 NRR 签名	$=$	每位收方：各 1 次 EOR 和 NRR 签名
通信量	发方发送 2 次信息	$<<$	发方发送 2n 次消息，
	每位收方发送 2 次消息	$=$	每位收方发送 2 次消息
时间	时间上可以同步进行		时间上又先后，必须依次进行

结束语 本文协议实现了期望强公平且允许发方给不同的接收方发送不同的消息，突破了先前协议只允许发方给不同的接收方发送同一消息的局限性。协议同时允许发方自由选择交易方，使得交易灵活而符合实际。最后分析协议满足收发方的不可否认性，期望强公平性，时效性，机密性。现虽已有一个带离线 TTP 的多方不可否认协议，但其实现的只是认证强公平，即协议末交易方可能获得的是离线 TTP 的签名证据来证明协议的运行情况，且协议外的任何人只需看一下双方持有的证据，就知道 TTP 是否介入协议，从而对 TTP 介入原因进行猜测并可能对交易方产生坏的声誉影响。本文协议中离线 TTP 生成的证据与收发方在协议正常运行完毕的情况下生成的证据一模一样，任何协议外的人都无法判断离线 TTP 是否介入协议，避免了上述影响，因此本协议在电子商务中具有潜在的应用价值。

参 考 文 献

1 Markowitch O, Kremer S. A multi-party optimistic non-repudiation protocol. Information Security and Cryptography. LNCS 2015, Seoul, Korea, 2000. 109～122

2 王彩芬，葛建华. 带脱线半可信第三方的公平非否认协议. 电子学报，2002，30(2)：286～288

3 Bao F, Deng RH, Mao W. Efficient and practical fair exchange protocols with off-line semi-trusted third party. In: Proc. of the 1998 IEEE Symp. On Security and Privacy, Oakland: IEEE Computer Press, 1998. 77～85

4 Markowitch O, Kremer S. An optimistic non-repudiation protocol with transparent trusted third party. Information Security Conference(ISC'2001). LNCS 2200, Springer- Verlag, Berlin, 2001. 363～378

5 Girault M. Self-certified public keys. Advances in Cryptography-Proceedings of EUROCRYPT'91, Brighten, UK, LNCS 547, Springer-Verlag, 1991. 490～497

6 Poupard M, Stern J. Security analysis of a practical 'on the fly' authentication and signature generation. Advances in Cryptology - Eurocrypt'98, Lecture Notes in Computer Science 1403, Springer-Verlag, 1998. 422～436

7 Carbonell M, Onieva J A, Lopez J, Galpert D, Zhou J. Timeout estimation using a simulation model for non-repudiation protocols. ICCSA 2004, LNCS 3043, 2004. 903～914

8 Zhou J, Deng RH, Bao F. Some remarks on a fair exchange protocol. In: Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptography'2000, Australia., Springer- Verlag, 2000. 46～57