改进的基于 RSA 签名的公平交换协议

Improvement of Fair Exchange Protocol Based on RSA Signature

马昌社　（华南师范大学计算机学院　广州市 510631）

摘要：公平性是安全电子商务的基石，分析了一个基于 RSA 签名的公平交换协议的缺陷：由于其交换的数据不具有可恢复性，因此协议的公平性不能得到保证。为此，提出了一个改进的公平交换协议，改进后的协议简单、高效并能保证真正公平性。

关键词：公平交换协议　RSA 签名　公平性

1　引言

近年来，B2C 和 C2C 的电子商务在我国发展迅猛，崛起了一批电子商务网站如：sohu 商城、当当、eBay 易趣、淘宝等。但是交易还是采用货到付款，送货上门的 B2C 的交易模式，C2C 模式中绝大部分局限于本地的面对面交易，实际上这些网站也就是一个信息发布平台，没有真正体现商务里面的交易环节。尽管这些网站有了相应的网上支付工具如：易安付、支付宝等，但是却忽略了一个对每一个顾客或商家来说最基本的安全性——公平性[1]。它能保证在交易结束后，要么交易的双方都得到对方的商品；要么任何一方都得不到对方商品的任何有用信息。在密码领域内，该问题一直受到了研究人员的高度重视，并提出了一系列的解决方案。初期对公平交换协议的研究主要集中于逐步交换协议[2]，但该类协议通信和计算开销巨大，因此该类协议没有实用价值。随后研究人员开始研究使用可信第三方（TTP）[3]的协议。其中之一叫在线 TTP 公平交换协议[3]，这类协议需要 TTP 直接参与每一个交易，并且在整个的交易过程中必须始终保持可用、可信。然而，维护这么一个高度可信、在线的 TTP 本身代价很高，同时 TTP 容易成为效率的瓶颈，并易于遭受拒绝服务（DoS）攻击。另一类使用可信第三方的协议叫作优化的公平交换协议[4-7]，与在线 TTP 协议不同的是：在没有异常问题出现的情况下，该类协议不需要 TTP 参与交易的任何一个环节。这类使用离线 TTP 协议克服了以前协议的所有缺陷，因此叫作优化的公平交换协议。这类协议后来成了公平交换协议的研究主流。

文[8]中提出了一个基于 RSA 签名的优化的公平交换协议，其采用的主要密码技术是可验证可恢复的加密数据这一密码构件。本文的分析表明：文[8]中协议采用的可验证可以恢复的加密数据只具有可验证性，但不具有可恢复性，因此文[8]中的协议不能保证真正的公平性。因此，本文设计了两种简单的攻击该协议的有效方法。同时为了弥补原协议的缺陷，本文提出一个改进的公平交换协议，改进后的协议简单、高效、实用并具有真正公平性。

本文组织如下：在第二节里简单回顾文[8]中的协议；第三节对文[8]中的协议进行了分析和攻击；第四节设计了一个改进的公平交换协议；第五节总结了全文。

2　基于 RSA 签名的公平交换协议

这节简单回顾文[8]的协议。先给出一些符号、记号和系统假设以便于简单的描述协议。

2.1　记号、符号和系统假设

- n_i 用户 i 的 RSA 模；
- pk_i, sk_i 用户 i 的 RSA 公钥和私钥；
- X,Y 消息 X 和消息 Y 的逐比特连接；
- $h(\cdot)$ 单向抗碰撞的杂凑函数，如 SHA256；
- $E_i(\cdot), D_i(\cdot)$ 对称加解密算法，其密钥是 k_i；
- $pk_i(\cdot)$ 采用用户 i 的公钥进行加密；
- $sk_i(\cdot)$ 用户 i 对消息进行数字签名；
- 假定参与协议交换的两方为 A 和 B，可信第三方为 T，每一参与者都有一对 RSA 公私钥对 (pk_i, sk_i)，这里 $i \in \{A,B,T\}$；

· 假定 A 和 B 参与交换的数据分别为 D_A 和 D_B，用户 A 从 T 那里为其商品数据申请一张证书 $Cert_A = (sn_A, h(D_A), h(E_a(D_A)), pk_A, sign_{TA}$，这里 k_a 是加密其数据的对称算法密钥，$sign_{TA} = sk_T(sn_A, h(D_A), h(E_a(D_A)), pk_A)$；同样 B 也拥有其商品数据的证书 $Cert_B$；

2.2 基于 RSA 签名的公平交换协议

文[8]中的协议由两个子协议组成，它们分别是交换子协议和恢复子协议。

交换子协议（由 A 发起协议运行，分四轮消息完成，具体交换如下表 1 所示）

表 1　文[8]中的交换子协议

T1. $A \rightarrow B: pk_B(E_a(D_A)), pk_T(k_a), pk_B(sn_A, sn_B), sign_{A1}$
T2. $B \rightarrow A: pk_A(E_b(D_B)), pk_T(k_b), pk_A(sn_B, sn_A), sign_{B1}$
T3. $A \rightarrow B: pk_B(k_a^1), pk_B(sn_A, sn_B), sign_{A2}$
T4. $B \rightarrow A: pk_A(k_b), pk_A(sn_B, sn_A), sign_{B2}$

这里 $sign_{A1} = sk_A(pk_B(E_a(D_A)), pk_T(k_a), pk_B(sn_A, sn_B))$ 是对一轮消息的完整性标识，同样在其他的三轮消息中都有相应的完整性标识。sn_A 和 sn_B 是交换数据编号，也可以看成是会话标识。在 B 收到 A 的第一轮消息后，先解密得到 $E_a(D_A)$，计算其散列值并与 A 的商品证书中的散列值加以比较，如果不相等就中止协议执行。同样在 T2 阶段，A 进行类似的检验。在 T4 阶段，如果 A 没有收到 B 的消息，或者发现 B 发给 A 的解密密钥不正确，就调用恢复子协议来保证公平性。

恢复子协议（只能由 A 发起，如下表 2 所示）

表 2　文[8]中的恢复子协议

E1. $A \rightarrow T: pk_T(pk_A(E_b(D_B)), pk_T(k_b), pk_A(sn_B, sn_A), sign_{B1}), sign_{AT}$
E2. $T \rightarrow A: pk_A(k_b), sign_{TA}$

在交换协议的 T4 阶段，如果 A 没有收到 B 的消息，或者发现 B 发给 A 的解密密钥不正确，就调用该子协议。首先 A 把它收到的 T2 阶段的消息用 T 的公钥加密并对其签名后就发送给 T，然后 T 解密该消息，并同时解密 $pk_T(k_b)$ 得到 k_b，用 A 的公钥加密之，最后把它发送给 A。

3　分析和攻击

这节对文[8]中的协议进行安全性分析，具体从以下两个个方面来分析。

3.1 攻击一该攻击由 B 发起。如果 A 是诚实的一方，那么不诚实的 B 可以对该协议发起以下攻击来赢得非公平性。具体攻击如下表 3 所示。

表 3　攻击一

T1. $A \rightarrow B: pk_B(E_A(D_A)), pk_T(k_a), pk_B(sn_A, sn_B), sign_{A1}$
T2. $B \rightarrow A: pk_A(E_b(D_B)), pk_T(r), pk_A(sn_B, sn_A), sign_{B1}$
T3. $A \rightarrow B: pk_B(k_a), pk_B(sn_A, sn_B), sign_{A2}$
T4. $B \rightarrow A$: nothing

B 在收到 A 的第一轮消息后，然后随机选择一个随机数 r 当作他的解密密钥 k_b 来构造第二轮的消息，并把它发送给 A。在第三步中，A 收到该消息后，不能检测出 r 的非法性，因此会发送其解密密钥 k_a 给 B，B 收到该解密密钥后，中止协议运行。之后，由于 A 没有收到第四轮中 B 的消息，他就调用恢复子协议，但此时 A 得到的解密密钥是 r，非 k_b。这样 B 得到了 A 的商品数据，而 A 却没有得到 B 的商品数据。可见协议的公平性没有得到保证。

3.2 攻击二

该攻击由 A 发起。假设 B 是诚实的一方，那么不诚实的 A 可以通过以下的方法来得到 B 的数据 D_B，而不让 B 拥有他的数据 D_A，具体攻击如下表 4 所示。

表 4　攻击二

T1. $A \rightarrow B: pk_B(E_a(D_A)), pk_T(k_a), pk_B(sn_A, sn_B), sign_{A1}$
T2. $B \rightarrow A: pk_A(E_b(D_B)), pk_T(k_b), pk_A(sn_B, sn_A), sign_{B1}$
T3. $A \rightarrow B$: nothing

A 在第二轮中收到 B 的消息后，就中止交换子协议的运行，然后他就执行恢复子协议，从恢复子协议中，显然他能得到 B 的解密密钥 k_b，而 B 却不能得到 A 的解密密钥 k_a，因此 A 能得到 B 的数据，但 B 却不能得到 A 的数据。协议的公平性再一次被打破。

存在以上两种攻击的主要原因是由于文[8]中协议

所采用的商品证书 $Cert_A(sn_A, h(D_A), h(E_a(D_A)), pk_A, sign_{TA})$ 并没有把加密商品数据的对称密码算法的密钥的相关信息包含进去，因此造成了该加密数据的不可恢复性。例如：A 可以传递给 B 一个随机数当作他的加密数据的密钥，此时 B 就不能判断这个随机数是不是他想要的解密密钥，因为协议中没有任何检测该数据的可靠性的机制。

3.3 效率分析

首先公钥加解密是非常耗时的操作，文[8]中的协议采用了大量的公钥加解密操作，可见效率相当低下，尤其是当用户的商品数据比较大时（比如为 mp3、电影等），该协议几乎是不行的。其次，在协议执行的过程中，需要传输 A、B 双方的加密的数据，这对于比较大的数据来说，占用太多的实时带宽，因此在通信上也是不可行的。

4 改进的基于 RSA 签名的公平交换协议

这一节提出一个改进的优化公平交换协议，并对其安全性和效率进行了分析和比较。

4.1 改进的公平交换协议

改进的优化公平交换协议由注册子协议、交换子协议、争端解决子协议组成，他们分别具体描述如下：

注册子协议：对于用户的每一个商品数据 D_i，这里 $i \in \{A, B\}$，用户 i 首先发送 D_i 及其描述值 $desc(D_i)$、商品编号 sn_i 和 pk_i 给 T，T 检验产品 D_i 符合它的描述值，接着它就选取一个随机数 $\overline{k_i} \in Z_{n_T}^*$，然后它计算出加密数 D_i 据的对称密钥 $k_i = h(\overline{k_i})$，计算 $ck_i = pk_T(\overline{k_i})$ 以及它的签名 $sign_{Ti} = sk_T(sn_i, ck_i, h(D_i), h(E_i(D_i)), pk_i)$，$D_i$ 的证书是

$Cert_i = (sn_i, ck_i, h(D_i), h(E_i(D_i)), pk_i, sign_{Ti})$。

最后，T 发送 $Cert_i$ 和 $pk_i(\overline{k_i})$ 给 i，而 i 把它的产品证书 $Cert_i$ 和加了密数据 $E_i(D_i)$ 放在其 Web 上以便消费者来购买。

交换子协议：在开始该子协议之前，假设 A 和 B 分别从 Web 上获得对方的加密数据和相应的商品证书。协议执行如下表 5 所示。

表 5　改进的交换子协议

T1. $A \rightarrow B: pk_B(sn_A, sn_B), sign_{A1}$
T2. $B \rightarrow A: pk_A(k_b), sign_{B1}$
T3. $A \rightarrow B: pk_B(k_a), sign_{A2}$

在 T1 阶段，A 加密 sn_A 和 sn_B，表明他想要用自己的商品 sn_A 来交换 B 的商品 sn_B，接着它对加密的结果签名 $sign_{A1}sk_A(sn_A, sn_B)$ 来保证完整性和不可否认性。

在 T2 阶段，B 首先解密得到 sn_A 和 sn_B，证实自己也希望用商品 sn_B 来交换 A 的商品 sn_A，然后验证签名 $sign_{A1}$ 的正确性，如果都成立，那么他就用 A 的公钥加密自己的商品解密密钥 k_b，并同时加密 sn_B 和 sn_A，然后计算签名 $sign_{B1} = sk_B(k_b, sn_b, sn_a)$，一并发送给 A。

在 T3 阶段，A 首先解密 $pk_A(k_b)$ 得到 k_b，然后解密 $E_b(D_B)$ 得到 D'_B，通过 B 的商品证书来验证 $h(D'_B) = h(D_B)$，以确信自己得到的是 A 的数据 D_B，如果得到确信，那么 A 就发送包含他的解密密钥的消息 $pk_B(k_a)$，$sign_{A2}$ 给 B。否则，A 就中止协议执行。

最后，当 B 收到 A 的消息 $pk_B(k_a)$，$sign_{A2}$ 后，首先解密得到 k_a，然后解密 A 的加密数据 $E_a(D_A)$ 得到 D'_A，通过 A 的商品证书来验证 $h(D'_A) = h(D_A)$，如果成立，那么交换协议以成功而结束。否则他调用争端解决子协议来保证自己的公平性。当然，当 A 在 T3 步中止了协议的执行，或者 A 发送给 B 的消息在一定的时限内没有到达 B 时，B 也调用争端解决子协议来保证自己的公平性。

争端解决子协议：当 B 在 T3 步接收到的数据没有通过验证或者在一定时限内没有接收到 A 的消息时，他就调用该子协议，具体执行如表 6 所示。

表 6　争端解决子协议

E1. $B \rightarrow T: cert_A, cert_B, sn_A, sn_B, sign_{A1}$
E2. $T \rightarrow B: pk_B(k_a), s_{TB}$
$T \rightarrow A: pk_A(k_b), s_{TA}$

首先，B 把 $cert_A, cert_B, sn_A, sn_B, sign_{A1}$ 发送给 T，收到这个消息，T 首先检查 $cert_A$ 中的商品编号和 sn_A 相等；同样检查 $cert_B$ 中的商品编号和 sn_B 相等；验证签名 $sign_{A1}$ 的正确性；如果至少有某一个不成立那么 T 就结束协议的执行。否则，T 就从 $cert_A$ 中解密 ck_a 得到 $\overline{k_a}$，然后计算 $k_a = h(\overline{k_a})$，按同样的方法计算出 k_b；然后分别发送 $pk_B(k_a), s_{TB}$ 和 $pk_A(k_b), s_{TA}$ 给 B 和 A。这里 s_{TA} 和 s_{TB} 分别是 T 对消息 $pk_A(k_b)$ 和 $pk_B(k_a)$ 的签名。

4.2 安全和效率分析

安全分析：从两方面来分析本文协议的安全性。首先如果 A 得到了 B 的数据，那么 B 也会得到了 A 的数据。这是因为：A 得到 B 的数据的途径只有两条，第一是通过交换协议，那么在 T1 阶段 A 发给 B 的消息一定通过了 B 的验证，那么 B 要么可以通过交换子协议得到了 A 的数据，要么可以通过调用争端解决子协议来得到 A 的数据；第二是通过争端解决子协议，此协议只有 B 才能调用，那么在 A 得到 B 的数据之前，B 就得到了 A 的数据。

其次，如果 B 得到了 A 的数据，那么 A 也会得到了 B 的数据。这是因为：B 得到 A 的数据的途径只有两条，第一是通过交换协议，那么在 T2 阶段 B 就把它的解密密钥发送给了 A，否则，B 不可能在 T3 阶段得到 A 的解密密钥，因此在 B 得到 A 的数据之前 A 就得到了 B 的数据。第二是通过争端解决子协议，此协议只有 B 才能调用，如果 B 调用该协议得到了 A 的解密密钥，那么 A 也会得到 B 的解密密钥。由此可见，无论在什么情况下，A，B 要么都得到自己想要得数据，要么都得不到任何有关对方数据的信息。因此改进的协议具有强公平性。

效率分析：从消息轮数上来说，改进的协议比文[8]中的协议少一轮；从每轮消息的长度来看，改进的协议要远远短于文[8]中的协议，而且在协议的执行过程中不需要实时传输加密的数据内容，因此节约了大部分带宽；从计算上来看，改进的协议不需要计算对加密数据的公钥加密操作，而且在很大程度上的节省了计算开销。具体比较如下表 7。从表 7 可以看出，改进的协议要简单、高效、安全、实用。

表 7　改进协议与文[8]中协议比较
（只比较交换子协议）

	改进的协议	文[8]中协议
消息轮数	3	4
公钥加解密操作次数	6	14
大块数据传输	N	Y
公平性	Y	N

5 结论

公平交换协议是电子商务中最重要的基础构件之一，它能保证参与交易的双方都能得到对方的商品，或者都得不到对方的商品的任何信息。由于网络本身所固有安全缺陷，这就使得设计安全、高效、实用的公平交换协议尤其重要。本文分析文[8]中公平交换协议的缺陷，同时设计了一个改进的公平交换协议，与文[8]中协议比较起来，改进的协议具有简单、高效、安全、实用等优点。

参考文献

1 N. Asokan, Matthias Schunter, and Michael Waidner. Optimistic protocols for fair exchange. 4th ACM Conference on Computer and Communications Security, pp. 6 – 17, 1997.

2 S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. Communications of the ACM, 28(6): pp. 637 – 647, 1985.

3 Colin Boyd and Ernest Foo. Off – line fair payment protocol using convertible signatures. ASIACRYPT98, LNCS 1514 , pp. 271 – 285, 1998.

4 . F. Bao, R. H. Deng and W. Mao. Efficient and practical fair exchange protocols with off – line TTP. Proceedings of 1998 IEEE Symposium on Security and Privacy, pp. 77 – 85, 1998.

5 M. K. Franklin and M. K. Reiter. Fair exchange with a semi – trusted third party. Proceedings of the 4th ACM Conferences on Computer and Communications Security, pp. 1 – 5, 1997.

6 Indrakshi Ray and Indrajit Ray, An optimistic fair exchange e – commerce protocol with automated dispute resolution, Proceedings of the First International Conference on Electronic Commerce and Web Technologies, pp. 84 – 93, 2000.

7 R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public – key cryptosystems. Communications of the ACM, 21 (2), pp. 120 – 126, 1978.

8 闫乐林、蔡平胜，一种基于 RSA 签名的公平交换协议的算法设计，计算机系统应用，vol. 5，2006，pp. 40 – 42.