一种基于 RSA 签名的公平交换协议的算法设计

A fair data exchange protocol based on RSA signature

闫乐林 蔡平胜 （山东省教育学院 计算机科学与技术系 济南 250013）

摘要：公平性是电子商务协议的基本安全要求。在电子商务活动中，进行实时公平的文件交换具有非常重要的意义。本文利用证书机制、应用公钥密码体制 RSA 的加密算法和数字签名技术，设计了一种新的公平交换协议。这种算法简单、高效、易于实现。

关键词：RSA 密码体制 公平交换 算法

1 引言

随着 Internet 的迅猛发展，电子商务、网上交易成为一种发展趋势。基于信息技术的商务活动的主要问题之一是在任意两个互不信任的主体之间以一种高效、公平的方式交换数据[1]。针对电子商品的公平交换，国内外许多学者做了大量研究，并提出不少有价值的公平交换协议。现有的公平数据交换协议，一般采用引入可信任第三方（TTP）的办法，将第三方作为数据交换的“中间站”，参与数据交换的全过程[2,3]；另一类为 TTP 不参与数据的交换，仅在交换失败的情况下参与数据的恢复，以保证数据交换的公平性[4]。

在公平交换协议的设计上，从早期单字节交错方式进行数据交换，演变为基于验证数据项交换方式，应用成熟的 RSA 算法进行数据项的生成与验证[5]。在设计具体的文件交换协议上，文献[6]在此基础上结合应用数论中的 CROSS－VALIDATION 定理，使交换中验证都建立在 RSA 算法的安全强度之上，提高了协议的可靠性。然而文献[6]在算法的构造中定义了多种证书以及协议假定的条件过强，如必须事先假定交易活动中的两方（交易方和 TTP）共享交换用的私钥等，都一定程度上限制了协议应用前景。本文对[6]的协议算法进行了优化改进，实现多类证书的统一，将较大一部分的数据验证脱离于实时的数据交换，取消了共享交换用私钥的条件限制，在不影响安全性的前提下，提高了协议的实用性。

2 公平协议算法设计

本文设计的协议包括两个子协议：交换子协议和恢复子协议。其中，交换子协议完成正常情况下（即双方互不欺骗、并排除网络故障等异常因素）交易双方的数据交换，同时交换双方在交易的每一步都可以选择退出，而不会影响到交换的公平性；恢复子协议引入离线的可信任的第三方（TTP），处理异常情况下数据的公平交换。

协议的设计思想是交易的双方产生可验证可恢复的加密数据。数据的可验证性说明接收方在没有得到数据明文的情况下仍然能够对其真实性进行验证，而可恢复性则意味着在对方失信或其它网络故障情况下，接收方仍然可以在离线第三方协助之下得到需要的数据。这样，数据的交换必然分两步进行：首先，双方先交换用对称密钥加密的文件及相关一些用于确认和恢复的数据项，然后是密钥的交换。这样，对那些数据项的要求有两个：

（1）确信密文是交换报文加密生成、且是对方传送给己方的。

（2）可恢复的，即交易的任一方可据此在 TTP 的帮助下，解开密钥恢复数据。

协议算法仍然基于 RSA 安全机制，即数据验证的可靠性、唯一性及不可抵赖性等都建立在 RSA 算法（还包括 Hash 运算等公认的权威算法）所提供的安全强度之上。

3 公平交换协议

3.1 协议的假定

在公平数据交换活动中，交易的双方希望要么都

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

能得到对方的交换信息，要么双方什么都得不到。为保证交换的公平性，交换的数据及处理必须满足一定的验证条件。同时为表述的方便，我们对交换的数据及处理提出如下的约定：

(1) 假定数据交换的双方为 A、B，可信任第三方为 T，A、B 参与交换的数据分别记为 D_A、D_B，双方交换数据前经协商选择 T 为可信第三方，并与 T 方达成一致。

(2) A 拥有一组基于 RSA 的公私密钥对 (sk_A, pk_A)，sk_A 是用做解密和签名的私钥。另外，A 作为交换发起方还拥有一个对称的密钥 K_a 用以对 D_A 加密；类似的，B 拥有一组基于 RSA 公私密钥对 (sk_B, pk_B)，T 拥有 (sk_T, pk_T)。

(3) D_A、D_B 均有一张表明其身份的商品证书，分别记为 $cert_A$、$cert_B$。商品证书 $cert_A$ 的格式为：$[sn_A, h(D_A), h(E_a(D_A)), pk_A, sign_{TA}]$，$cert_B$ 与 $cert_A$ 的格式相同。

其中：sn_A 为交换数据 D_A 的编号信息；

$h(D_A)$ 是哈希函数对 D_A 计算得到的哈希值；

$h(E_a(D_A))$ 是 D_A 用 K_a 加密的密文的哈希值；

pk_A 是 A 方的公开密钥；

$sign_{TA}$ 是 T 对 A 提交信息的签名，$sign_{TA} = sk_T(h(sn_A, h(D_A), h(E_a(D_A)), pk_A))$。

(4) A、B 能够在线(例如通过下载方式)获得证书 $cert_A$、$cert_B$。

3.2 交换子协议

不妨设 A、B 双方数据交换由 A 方发起，用 T1、T2、T3、T4 四个阶段完成数据交换，流程描述如下：

T1：Packet1(A—>B)

Packet1(A—>B)的数据内容为：$[pk_B(E_a(D_A)), pk_T(K_a), pk_B(sn_A, sn_B), sign_{A1}]$

其中：$sign_{A1} = sk_A(h(pk_B(E_a(D_A)), pk_T(K_a), pk_B(sn_A, sn_B)))$

T2：Packet2(B—> A)

Packet2(B—> A)的数据内容为：$[pk_A(E_b(D_B)), pk_T(K_b), pk_A(sn_B, sn_A), sign_{B1}]$

其中：$sign_{B1} = sk_B(h(pk_A(E_b(D_B)), pk_T(K_b), pk_A(sn_B, sn_A)))$

T3：Packet3(A—>B)

Packet3(A—>B)的数据内容为：$[pk_B(K_a), pk_B(sn_A, sn_B), sign_{A2}]$

其中：$sign_{A2} = sk_A(h(pk_B(K_a), pk_B(sn_A, sn_B)))$

T4：Packet4(B—> A)

Packet4(B—> A)的数据内容为：$[pk_A(K_b), pk_A(sn_B, sn_A), sign_{B2}]$

其中：$sign_{B2} = sk_B(h(pk_A(K_b), pk_A(sn_B, sn_A)))$

(1) T1 阶段。A 向 B 发送数据包 Packet1，数据包中使用了 B 的公钥、T 的公钥、A 自己的私钥，是保证数据传送的安全性和交换的公平性。Packet1 传送过程中，任何非法第三方都很难从中获得有用信息，B 这个阶段也不能获得解密后的 D_A，但在发生异常情况时，B 可以借助 T 的帮助恢复 D_A 内容，因此保证交换的公平性。

B 收到 Packet1，用私钥 sk_B 取出 $E_a(D_A)$，对其做哈希运算得 $h'((E_a(D_A))$。检验 $h'((E_a(D_A))$ 与 $cert_A$ 中的 $h((E_a(D_A))$ 是否相等，即 $h'((E_a(D_A)) = h((E_a(D_A))$。验证 Packet1 传送过程中的完整性，检验 $h'(pk_B(E_a(D_A)), pk_T(K_a), pk_B(sn_A, sn_B)) = pk_A(sign_{A1})$ 是否成立。

(2) T2 阶段。(sn_A, sn_B) 是 A 方数据包中交换数据的编号及要交换 B 方数据的编号，B 依此发送对应的交换报文 Packet2。A 收到数据包后，类似的对 Packet2 做 T1 阶段中的验证。

(3) T3 阶段。A 收到 Packet2 后，向 B 发送 Packet3。B 收到 Packet3，用私钥 sk_B 取出 K_a，用对 Packet1 中的 $E_a(D_A)$ 解密得到 D'_A，验证 $h'(D'_A) = h(D_A)$ 是否成立。若成立，B 得到希望的交换数据。验证数据完整性，即检验 $h(pk_B(K_a), pk_B(sn_A, sn_B)) = pk_A(sign_{A2})$ 是否成立。

(4) T4 阶段：B 向 A 发送 Packet4，A 采用与上述相同的办法及验证，得到 K_b 和 D_B。

3.3 恢复子协议

在交易出现异常情况时，交易的一方已发送完自己的敏感数据，而没有得到对方的交换数据，则转入恢复子协议进行处理。

假设 1：A 向 B 发送了 Packet1 数据，一段时间内未收到 B 的 Packet2 数据，则停止 Packet3 的发送，双方数据交换失败。即便 B 接受到 Packet1，因为没有 K_a，所以也得不到有用信息(除非 T 方与 B 方协同作弊)。

假定 2：A 向 B 发送了 Packet1 、Packet3，收到了 B

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

的 Packet2，但是未接收到 Packet4。这种情况下，A 发送了所有敏感数据，B 可以得到交换数据 D_A，而 A 得不到密钥 K_b，因此无法得到 D_B。因此为保证数据交换的公平性，A 要借助 T 的帮助，恢复出交换数据 D_B。

A 与 T 的数据交换流程描述如下：

E1：$Packet_{AT}$（A—>T）

$Packet_{AT}$的数据内容为：[pk_T（Packet2），$sign_{AT}$]

其中，$sign_{AT}=sk_A(h(pk_T(Packet2)))$

E2：$Packet_{TA}$（T—>A）

$Packet_{TA}$的数据内容为：[$pk_A(K_b)$，$sign_{TA}$]

其中，$sign_{TA}=sk_T(h(pk_A(K_b)))$

（1）E1 阶段。A 把接收到 B 的 Packet2 用 T 的公开密钥 pk_T 加密，并对此数据签名后发送给 T，其中，$sign_{AT}=sk_A(h(pk_A(E_b(D_B))，pk_T(K_b)，pk_A(sn_B，sn_A)，sign_{B1}))$。T 检验 A 传来的 Packet2 中 B 的签名是否真实，即验证 $h'(pk_A(E_b(D_B)))，pk_T(K_b)，pk_A(sn_B，sn_A))=pk_B(sign_{B1})$是否成立。

（2）E2 阶段。若 T 对 B 的签名验证通过，则相信 A 发来的消息是合法的。T 从 Packet2 中取出 K_b（$K_b=sk_T(pk_T(K_b))$），用 pk_A 加密并签名发送给 A。A 收到 $Packet_{TA}$，检验数据完整性，即检验 $h'(pk_A(K_b))=pk_T(sign_{TA})$是否成立。若成立，从 $Packet_{TA}$中取出 K_b，再用 K_b 得到 Packet2 中的 D_B；若不成立，与 T 重新交换数据。

在恢复子协议处理阶段，通过 A、T 的两次数据交换，A 可以获得 B 的交换数据 D_B，同理 B 亦然。

3.4 协议的安全性分析

由于交易双方互不信任，数据的交换必然分两步进行。首先是密文，然后是密钥。由于无法保证交易的严格同步，必然有一定的先后顺序，则以下几点尤为重要：

（1）双方接收到对方的密文后，要对密文的真实性进行验证；

（2）最先得到完整数据（机包括得到密文和密钥）的一方必须提供对方可以借助可信任第三方 TTP 恢复数据的证据；

（3）相关数据要进行数据完整性和真实性的验证。

正常情况下（指 A、B 交易双方都是诚实可信的），可信第三方 T 不参与数据的交换，T 没有 A（或 B）的协助也不会得到他们交易的内容，这使得协议有更强的适用性；其次，即便 T 参与数据恢复，但是它也不可能由此得到更多的信息，比如交换的文件的内容、签名数据等。因此，保证的交换的公平性，又保证了交换的封闭性。另外，为近一步加强数据交换的公平性和安全性，防止可信任第三方与其中一方协同作弊骗取另一方的信息资源，可以采用多 TTP 的机制。

4 结论

公平交换协议是实现电子商务的一个重要基础，笔者在前人的研究基础上，利用 RSA 加密和数字签名技术，设计了一种高效、简单、实用性强的公平交换协议。该协议降低了对可信第三方的依赖程度，并保证数据的机密性和交易的公平性。因此，本协议具有较强的实用价值，有利于电子商务的进一步开展。

参考文献

1 Asokan N, Victor Shoup, Michael Waider, Optimistic Fair Exchange of Digital Signatures[J]. IEEE JOURNAL ON Selected Areas In Communications, 2000, 18(4) 593－610.

2 Bao F, Deng RH, Mao WB. Eficient And Practical Fair Exchange Protocols With Off－Line TTP[A]. Proceeding Of The 1998 IEEE symposium on security and privacy [C], Oakland: IEEE Computer Socity Press. 1998. 77－85.

3 Colin Boyd, Ernest Foo, Off－Line Fair Payment Protocols Using Convertible Signatures [A], Proceedings of ASIACRYPT98 [C]. Berlin: Springer—Verlag, 1998, 271－285.

4 邓所云、隋爱芬、胡正名、杨义先，一个优化的公平的多方不可否认协议，电子与信息学报，2002，24（12），1985－1989。

5 Franklin M, Tsudik G. Secure group barter: Multi—party fair exchange with semi—trusted neutral parties. In: Financial Cryptography'98, 1998, LNCS 1465: 90－102.

6 NENADIC A, ZHANG N. On the Design of the Fair Intergrated Data Exchange System (FIDES) [A]. IADIS International Conference Lisbon Portugal[C]. 2003.

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn