基于 RSA 签名的优化公平交换协议*

周永彬[1,2+], 张振峰[1,2], 卿斯汉[1,3], 季庆光[1,3]

[1](中国科学院 软件研究所,北京 100080)

[2](中国科学院 软件研究所 信息安全国家重点实验室,北京 100080)

[3](中国科学院 信息安全技术工程研究中心,北京 100080)

A Fair Exchange Protocol Based on RSA Signature Scheme

ZHOU Yong-Bin[1,2+], ZHANG Zhen-Feng[1,2], QING Si-Han[1,3], JI Qing-Guang[1,3]

[1](Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)

[2](State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)

[3](Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijing 100080, China)

+ Corresponding author: Phn: +86-10-82612797, E-mail: zhouyongbin@sina.com, http://www.is.iscas.ac.cn

Received 2003-08-01; Accepted 2003-10-31

Zhou YB, Zhang ZF, Qing SH, Ji QG. A fair exchange protocol based on RSA signature scheme. *Journal of Software*, 2004,15(7):1049~1055.

http://www.jos.org.cn/1000-9825/15/1049.htm

Abstract: Fairness is the basic requirement of E-Commerce protocols. RSA is one of the most widely used cryptosystems. A fair-exchange protocol allows two parties to exchange items in a fair way so that either each party gets the other's item, or neither party does. In this paper construction and architecture of the existing fair exchange protocols are analyzed. Both practicality and efficiency problems of these protocols are also presented. Based on this analysis, an optimistic fair exchange protocol totally based on RSA signature scheme is proposed. The novel scheme employs verifiably encrypted RSA signatures in the extended integer ring that is elaborately constructed. The security and efficiency of the newly devised scheme are also proved and examined. It is showed that the proposed scheme is secure and efficient.

Key words: fair exchange protocol; RSA cryptosystem; verifiably encrypted signature; information security

摘 要: 公平性是电子商务协议的基本安全要求.RSA 是应用最为广泛的公钥密码体制之一.公平交换协议可以使得参与交换的双方以公平的方式交换信息,这样,要么任何一方都可以得到对方的信息,要么双方都得不到对方的信息.分析了现有的公平交换协议构造方法、体系结构及其在实用性和效率方面存在的问题.在此基础上,利用精心构造的扩环中可公开验证的、加密的 RSA 签名,提出了一种完全基于 RSA 签名方案的优化公平交

* Supported by the National Natural Science Foundation of China under Grant Nos.60373039, 60083007 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973))

作者简介: 周永彬(1973－),男,山东阳信人,博士,主要研究领域为应用密码学,网络与信息安全理论与技术;张振峰(1972－),男,博士,副研究员,主要研究领域为密码学,信息安全理论与技术;卿斯汉(1939－),男,研究员,博士生导师,主要研究领域为信息安全理论与技术;季庆光(1968－),男,博士,主要研究领域为安全系统形式化分析.

换协议,并对其安全性和效率进行了证明和分析.分析表明,提出的方案是简洁、高效、安全的.

关键词: 公平交换协议;RSA 密码体制;可验证的、加密的签名;信息安全

中图法分类号: TP309 **文献标识码**: A

电子商务、移动商务已成为基于 Internet 的现代经济活动的主要形式之一.尽管对信息安全系统的研究已有近 70 多年的历史,但是新的经济活动形式对安全的特殊需求也不断提升,诸如公平性、原子性、可追踪性等新的安全特性就是除了传统的保密性、完整性、非否认性等安全要求之外的新需求.基于信息技术的商务活动的主要问题之一就是在任意两个互不信任的主体之间以一种高效、公平的方式来交换电子数据.公平性和高效性成为这类电子商务协议的基本要求.公平交换协议可以使得参与交换的双方以公平的方式交换信息,这样,要么任何一方都可以得到对方的信息,要么双方都得不到对方的信息.

由于公平交换协议在密码理论和应用领域的重要性,该问题一直得到研究人员相当的重视,也提出了各种各样的方案.但是,大多数已有方案在交换过程中都使用了零知识证明系统[1~4],而零知识系统本身计算量大的特点就注定会使得这类公平交换协议的效率很低.第一个基于 RSA 密码体制的公平交换协议是 J.M. Park 等人在 PODC 2003 上基于 RSA 多签名技术提出的公平交换协议[5].但遗憾的是,该方案旋即被攻破[6],攻击者已经证明了该方案完全不安全.此外,再没有一个已经公开的、安全、高效且完全基于 RSA 密码体制[7]的公平交换协议.RSA 密码体制是应用最为广泛的密码体制之一,因此,研究基于 RSA 密码体制的高效、安全的公平交换协议具有重要的理论和应用价值.基于此,本文给出了一种新颖的基于 RSA 密码体制的安全、高效的优化公平交换协议.

本文第 1 节简要介绍构造公平交换协议方面已有的工作和成果.第 2 节给出文中使用的一些记号和符号.第 3 节详细说明在精心构造的扩环中的 RSA 加密和解密操作原理.第 4 节给出基于 RSA 密码体制构造的优化公平交换协议的细节.第 5 节对新构造出的公平交换协议进行安全性分析,并给出相关证明.第 6 节总结全文.

1 已有的工作和成果

现有的公平交换协议大致可以分为如下 4 种类型[8]:① 逐步秘密交换:这种方式反映了网络异步交换的特点,但是它总存在“一比特的不公平性”[9].② 使用在线可信第三方(即 TTP)的公平交换协议[10]:由于协议中使用了一个在线的 TTP 作为公平交换的基础,所以无论从计算上还是在通信上讲,TTP 都会成为一个瓶颈,这就注定这类协议的效率不会很高.③ 使用在线的半可信第三方(即 STTP)的公平交换协议[11].④ 使用离线 TTP 的优化(optimistic)公平交换协议[9,12],这类协议是目前公平交换协议研究的重点和热点.

现有的效率较高的公平交换协议大多数采用基于离线 TTP 的优化公平交换方式.其基本结构可以分为注册过程(可选)、交换过程、争端解决过程.这种机制基于这样一种合理的假设:在大多数情况下,参与交换的双方都是诚实的.本文也将采用这种基本框架来设计公平交换协议.

就实现技术而言,现有的公平交换协议多数采用交互式系统,如基于可验证的、加密的签名[13]等.这类协议在交换过程中都使用了零知识证明系统,而零知识系统本身计算量大的特点就使得这类公平交换协议的效率很低.此外,大多数公平交换协议中使用的签名方案多是基于离散对数或者椭圆曲线离散对数的签名方案.最近,J.M. Park 等人提出了第一个基于 RSA 签名方案的非交互式公平交换协议[4],但是它很快就被证明是完全不安全的[6].

据我们所知,目前尚没有一个安全、实用、高效且完全基于 RSA 签名体制的公平交换协议.这在很大程度上与安全工程实践的发展和应用水平不相称.因为在诸如 PKI、电子商务、移动商务等密码工程中,需要大量使用 RSA 密码体制.

2 记号和符号

本节将给出文中所使用的一些符号和记号.

与公钥密码系统有关的记号如下:

- P: 公钥密码系统;
- P_{encr}: P 的加密算法;
- P_{decr}: P 的解密算法;
- PK: P 中的公钥;
- SK: P 中与 PK 相对应的私钥;
- $P_{encr}(PK,M)$: 使用 PK 加密明文 M 的加密输出(密文);
- $P_{decr}(SK,C)$: 使用 SK 解密密文 C 的解密输出(明文).

与数字签名方案有关的记号如下:

- S: 数字签名方案;
- S_{sign}: S 的签名算法;
- S_{veri}: S 的验证算法;
- sk: S 中的私钥(签名密钥);
- pk: S 中与 sk 相对应的公钥(验证密钥);
- $S_{sign}(sk,M)$: 用私钥 sk 对消息 M 的签名;
- $S_{veri}(pk,s,M)$:使用公钥 pk 对消息 M 的签名 s 进行验证;如果签名 s 有效,它输出 Yes;否则,输出 No.

协议中涉及的主体如下:

- Alice: 公平交换协议中的一个主体,它有一对用于签名算法 S 的密钥对 (pk_A,sk_A);
- Bob: 公平交换协议中的另一个主体,它有一对用于签名算法 S 的密钥对 (pk_B,sk_B);
- TTP: 一个离线的可信第三方,它有一对用于加密算法 P 的密钥对 (PK_{TTP},SK_{TTP}).

其他记号如下:

- $X\|Y$: 消息 X 和消息 Y 的逐比特连接;
- $|x|$: 串 x 的比特长度.

3 扩环中的RSA加、解密操作

文献[9]中提出的一种重要的密码构造部件 CEMBS,其基本思想是让消息 M 的接收方确信:某个加密的消息 C 确实是发送方对消息 M 的签名(设签名为 s),接收方却无法获得这个真实的签名 s ;但是,借助于一个可信第三方(TTP),接收方可以获得该真实的签名 s.

本文利用这一思想(仅仅是借鉴这一思想,但并不试图构造这样的 CEMBS),并借助于对常规的 RSA 加、解密操作基于的整数环进行扩展来实现这一目的.

记 C 为某个签名 s (对于验证者而言是未知的)的一个(在扩环中)密文,则存在一个公开的验证算法:

$$Veri(C,M,PK,pk)=\text{Yes 或者 No.}$$

如果 $Veri(C,M,PK,pk)=$Yes,则必有

$$C=P_{encr}(PK,s) \text{ 并且 } S_{veri}(pk,s,M)=\text{Yes.}$$

下面来说明本文中所采用的基本思想.

TTP 生成自己的加密用 RSA 密钥对 PK_{TTP} 和 SK_{TTP} ,其中:

$$PK_{TTP}=(e_{TTP},n_{TTP}),\ SK_{TTP}=(d_{TTP},n_{TTP}).$$

特别值得说明的是,为了能使系统正常工作,必须要求 TTP 的 RSA 模 n_{TTP} 比系统中所有的其他任何用户的 RSA 模 n_i 都要大(即 $n_{TTP}\succ n_i$, i 为系统中的任一用户),这是保证在扩环中的 RSA 操作得以正确进行的最重要的前提之一.这个前提条件很容易满足.例如,假定系统中的用户所使用的 RSA 模长度为 k 比特,那么最简单的方法就是可以使 TTP 的 RSA 模 n_{TTP} 为 $k+2$ 比特.事实上,考虑到加密填充等因素的影响[14,15],实际所需要的 n_{TTP} 可能会更大一些,但是这对于说明问题并不重要.同时需要满足的一个条件是,系统中除 TTP 之外的任何用户的 RSA 模必须为两个强素数的积.也就是说,对于任意的用户 i ,有 $n_i=pq$;这里, $p=2p'+1$ 且 $q=2q'+1$, p,q,p',q' 均为素数.故 $\varphi(n_i)=4p'q'$,其中 $\varphi(n)$ 为欧拉函数.这一条件将在后面的证明中用到.

Alice 生成自己的签名用密钥对 pk_A 和 sk_A,其中 $pk_A=(e_A,n_A)$, $sk_A=(d_A,n_A)$.

Bob 生成自己的签名用密钥对 pk_B 和 sk_B,其中 $pk_B=(e_B,n_B)$, $sk_B=(d_B,n_B)$.

为了表示上的方便,我们记 $N_{TTP,i}=n_{TTP}*n_i$,则有 $N_{TTP,A}=n_{TTP}*n_A$, $N_{TTP,B}=n_{TTP}*n_B$.

3.1 签 名

设待签名的消息为 M,Alice 对该消息的签名为 s,签名过程如下:

$$s=Sign_A(M,sk_A)=H(M)^{d_A} \bmod n_A.$$

这里, H 是一个公开的、高强度的单向杂凑函数 $H_l:\{0,1\}^*\to\{0,1\}^l$, H 的输出长度 l 至少为 128 比特(例如,可以是 MD5,SHA1 等).在本文下面的叙述中, H 的含义相同,不再说明.

3.2 加 密

设 Alice 使用 TTP 的公钥 PK_{TTP} 对 s 加密后的密文为 C_A.Alice 进行如下计算:

$$C_A=P_{encr}(PK_{TTP},s)=s^{e_{TTP}} \bmod N_{TTP,A}.$$

这里需要特别说明的是,上式中的 RSA 加密运算不是在传统的环 $Z_{n_{TTP}}$ 中进行的,而是在 $Z_{N_{TTP,A}}$ 中进行的.从上式中可以看出, s 实质上是 C_A 在 $Z_{N_{TTP,A}}$ 中的一个 e_{TTP} 次根.

为了使得 TTP 在发生争端时能够正确地从 C_A 中恢复出 Alice 的签名 s,Bob 需要相信 Alice 的确知道 C_A 的 e_{TTP} 次根.Alice 可以通过零知识的技巧来向 Bob 证明这一事实.具体来说,Alice 随机选取长度为 k 的随机数 r,计算

$$\omega=H(C_A\|e_{TTP}\|r^{e_{TTP}} \bmod N_{TTP,A}),\quad z=r\cdot s^{\omega}.$$

Alice 把 (ω,z) 随同 C_A 一起发送给 Bob.

3.3 验 证

Bob 接收到 C_A 和 (ω,z) 之后进行如下检查:

$$C_A^{e_A}=(H(M))^{e_{TTP}} \bmod n_A,\quad \omega=H(C_A\|e_{TTP}\|z^{e_{TTP}}C_A^{-\omega} \bmod N_{TTP,A}),\quad |z|\le(\omega+1)k.$$

如果 Alice 正确地执行协议,则上式总是成立的.

证明: $C_A^{e_A} \bmod n_A=(s^{e_{TTP}} \bmod N_{TTP,A})^{e_A} \bmod n_A=((H(M)^{d_A} \bmod n_A)^{e_{TTP}} \bmod N_{TTP,A})^{e_A} \bmod n_A$

$$=((H(M)^{(d_Ae_{TTP})} \bmod N_{TTP,A})^{e_A} \bmod n_A,$$

注意到 $n_A\prec N_{TTP,A}$ 且 $n_A\mid N_{TTP,A}$,

所以上式 $=((H(M))^{(d_Ae_{TTP})e_A} \bmod n_A=((H(M))^{(d_Ae_A)e_{TTP}} \bmod n_A=(H(M))^{e_{TTP}} \bmod n_A$.

因为 $r^{e_{TTP}}=(zs^{-\omega})^{e_{TTP}}=z^{e_{TTP}}C_A^{-\omega} \bmod N_{TTP,A}$,所以有 $\omega=H(C_A\|e_{TTP}\|z^{e_{TTP}}C_A^{-\omega} \bmod N_{TTP,A})$ 成立. □

3.4 解 密

TTP 应该能够使用自己的解密私钥 sk_{TTP} 恢复出 Alice 的签名 s.注意:由于加密运算是在 $Z_{N_{TTP,A}}$ 中进行的,它毕竟和在环 $Z_{n_{TTP}}$ 中进行的运算不同,那么,TTP 能否正确恢复出这个 e_{TTP} 次根 s 呢?下面将给出相关证明.

证明:TTP 首先计算 $C_A^{d_{TTP}} \bmod n_{TTP}=(s^{e_{TTP}} \bmod N_{TTP,A})^{d_{TTP}} \bmod n_{TTP}$.注意到 $n_{TTP}\mid N_{TTP,A}$,上述计算结果为 $s^{e_{TTP}d_{TTP}} \bmod n_{TTP}=s-t'n_{TTP}$,其中 t' 为一非负整数.

由于 $|z|\le(\omega+1)k$,我们有 $k-1+\omega|s|-\omega\le|z|\le(\omega+1)k$,即 $|s|\le k+1+\frac{1}{\omega}<|N_{TTP}|$.因此 $t'=0$,所以上式 $=s \bmod n_A$.

因此,TTP 可以正确恢复出 Alice 对 M 的签名 s. □

4 安全性分析

由上面的描述可以看出,在协议的构造过程中,Alice 使用了 TTP 的公钥 $PK_{TTP}=(e_{TTP},n_{TTP})$ 加密了 s (在

$Z_{N_{TTP,A}}$ 中进行).因为只有 TTP 拥有 $PK_{TTP}=(e_{TTP},n_{TTP})$ 所对应的私钥 $SK_{TTP}=(d_{TTP},n_{TTP})$,所以也只有 TTP 可以恢复出这个 e_{TTP} 次根.上面我们已经证明了 TTP 能够正确恢复出这个 e_{TTP} 次根 s.

但是,由于对 s 的加密运算都是在 $Z_{N_{TTP,A}}$ 中,而不是在传统的环 $Z_{n_{TTP}}$ 中进行的,那么 Alice可否伪造出一个密文 C'_A 以及相应的证据(ω',z')通过相应的检验,但是 TTP 却无法从 C'_A 中恢复出 Alice 对于该消息的正确签名呢?下面证明 Alice 无法进行这样的伪造.

假设 Alice 能够伪造这样的(C'_A,ω',z'),则根据零知识证明的证据(ω',z')的合法性,Alice 必然知道 s'使得 $C'_A=(s')^{e_{TTP}} \bmod N_{TTP,A}$.

所以我们有 $C'^{e_A}_A=((s')^{e_{TTP}})^{e_A}=((s')^{e_A})^{e_{TTP}} \bmod n_A$;另一方面,对于一个有效的密文 C'_A,必然满足 $C'^{e_A}_A=(H(M))^{e_{TTP}} \bmod n_A$.这样就有 $((s')^{e_A})^{e_{TTP}}=(H(M))^{e_{TTP}} \bmod n_A$.也就是说,$(s')^{e_A}$ 必然为 $\varpi H(M)$ 的形式,其中 ϖ 是环 Z_{n_A} 中的 1 的一个 e_{TTP} 次单位根,即 $\varpi^{e_{TTP}}=1 \bmod n_A$.

如果 $\varpi=1$,也就是说 ϖ 是一个平凡 e_{TTP} 次单位根,则必有 $(s')^{e_A}=H(M)$.此时 $s'=((s')^{e_A})^{d_A}=(H(M))^{d_A}=s \bmod n_A$,可知$s$=$s'$;这就与$s'$和$s$不同相矛盾.所以,$\varpi$ 一定是环 Z_{n_A} 的一个非平凡 e_{TTP} 次单位根.注意到条件 $e_{TTP}<\varphi(n_A)=4p'q'$,所以必有 $e_{TTP}\mid\varphi(n_A)$;又由于 2 不是 e_{TTP} 的因子,故 e_{TTP} 必为 $p',q',p'q'$三者之一.也就是说,由此可以成功地分解大整数 n_A.根据 RSA 假设可知,在现有的计算能力范围内,不可能在多项式时间内以不可忽略的概率来分解一个 RSA 大整数.因此,ϖ 不可能是环 Z_{n_A} 的一个非平凡 e_{TTP} 次单位根.

也就是说,必然有 $s'=s \bmod n_A$ 成立.又注意到$|s'|<|n_{TTP}|$,所以 TTP 一定可以正确地恢复出签名 $s'=s \bmod n_A$.

5 一种新颖的公平交换协议

下面利用上面所描述的思想来构造一类重要的公平交换协议.该类公平交换协议的双方完成对某一个共同拥有文件 M 的签名的交换[11~13].例如,协议双方交换一份电子合同.

5.1 注 册

该过程是用户向 TTP 提交其 RSA 签名公钥的过程.在这个过程中,TTP 需要确保用户的 RSA 签名公钥的模 n_i 比 TTP 的 RSA 加密密钥的模 n_{TTP} 小;此外,TTP 还必须确信用户确实拥有其声称的 RSA 公钥所对应的私钥,以及用户的 RSA 模为两个强素数的积.这些证明可用零知识证明协议来完成,具体的细节在此不再赘述.

此外,在协议过程中所用到的 RSA 公钥的真实性和完整性既可以使用 PKI 中的公钥证书来保证[15],也可以使用其他物理分发技术来保证,这里也不再赘述.同时,本文也忽略了 RSA 密钥对的生成过程,其细节和安全性要求可以参见文献[7].

5.2 交 换

设交换的双方分别为 Alice 和 Bob.Alice 执行交换协议,发起与 Bob 之间的公平交换.我们假定在进行公平的签名交换之前,Alice 和 Bob 进行了一个协商过程,二者同意交换各自对信息 M 的签名.同时,也假定整个签名交换过程都使用了安全的通信协议(例如 SSL/TLS 协议等),以满足签名保密性要求.签名的交换过程如下:

1. $Alice \rightarrow Bob: C_A,(\omega,z)$

Alice 计算他对文件 M 的签名 $s_A=S_{sign}(sk_A,H(M))$,使用 TTP 的加密公开钥 PK_{TTP} 加密(在扩环中进行)签名 s_A 得到密文 $C_A=P_{encr}(PK_{TTP},s_A)$;同时,Alice 生成一个第 4.2 节中描述的 (ω,z).Alice 将 C_A 和 (ω,z) 传送给 Bob.

2. $Bob \rightarrow Alice: s_B$

Bob 接收到 C_A 和 (ω,z) 之后,使用 TTP 的加密用公开钥 PK_{TTP} 和 Alice 的签名用公开钥 pk_A 来验证 C_A 和 (ω,z) 的正确性.如果该验证过程返回 No,则交换协议中止;如果它返回 Yes,Bob 计算他对文件 M 的签名 $s_B=S_{sign}(sk_B,H(M))$,并把签名 s_B 发送给 Alice.

3. $Alice \rightarrow Bob: s_A$

Alice 接收到 s_B 后,使用 Bob 的签名用公钥 pk_B 执行 $S_{veri}(pk_B,s_B,M)$ 来验证 Bob 的签名.如果它返回 No,则

交换协议中止;如果它返回 Yes,则 Alice 将他的签名 s_A 发送给 Bob.

总之,当参与交换的双方 Alice 和 Bob 都非常诚实时,二者之间的消息交换过程如图 1 所示.

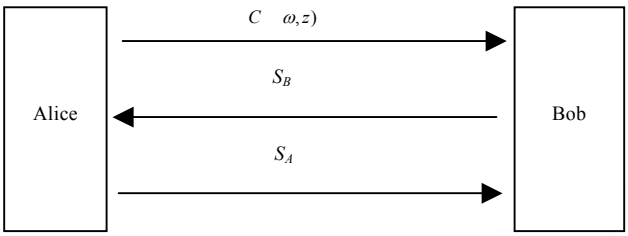

Fig.1 Exchange process

图 1 交换过程

由图 1 可以看出,上述签名交换过程十分简介、高效.需要说明的是,在用户注册阶段,TTP 需要使用零知识系统来对用户的所注册公钥进行验证,该过程仅仅是一次性开销,由于该过程不参与整个签名交换过程,因此它对交换过程的效率并无任何影响.

5.3 争端解决

当 Bob 没有接收到 Alice 的签名 s_A,或者接收到的签名 s_A 无效时,Bob 与 TTP 联系,执行如下争端解决过程.

1. $Bob \rightarrow TTP$: $\{M, C_A, (\omega, z), S_B\}$

TTP 使用 Bob 的签名用公钥 pk_B 来验证 s_B 是否为 Bob 对 M 的签名;如果 s_B 正确,TTP 用它自己的私钥 SK_{TTP} 解密出 Alice 对 M 的签名 s_A,并检查 s_A 的有效性.如果 s_A 或者 s_B 无效,则协议终止.

2. $TTP \rightarrow Bob$: s_A

TTP 将 s_A 发送给 Bob.

3. $TTP \rightarrow Alice$: s_B

TTP 将 s_B 发送给 Alice.

6 结 论

公平性是电子商务协议的基本安全要求之一.公平交换协议可以使得参与交换的双方以公平的方式交换信息,这样要么任何一方都可以得到对方的信息,要么双方都得不到对方的信息.因此,构造安全、高效的公平交换协议在安全的电子商务协议中具有重要的理论和应用价值.

本文分析了现有的公平交换协议构造方法与体系结构及其在实用性和效率方面存在的问题.利用精心构造的扩环中的可验证的、加密的 RSA 签名,首次提出了一种完全基于 RSA 签名体制的简洁、高效、安全的优化公平交换协议,并对其安全性和效率进行了证明和分析.

本文所使用的签名方案是标准的 RSA 签名方案,这一特点也使得可以很容易地使用本文构造公平交换协议的思想将公平交换特性集成到现有的电子商务系统中.

致谢 在此,我们向本文的匿名审稿专家表示感谢,感谢他们给本文提出的宝贵意见.

References:

[1] Diffie W, Hellman M. New directions in cryptography. IEEE Trans. on Information Theory, 1976,22(6):644~654.

[2] Menezes AJ, Oorschot PC, Vanstone SA. Handbook of Applied Cryptography. New York: CRC Press, 1996. 385~420.

[3] Verheul ER, Tilborg ER. Binding ElGamal: A fraud-detectable alternative to key escrow proposals. In: Fumy W, ed. Proc. of the Eurocrypt'97. Berlin: Springer-Verlag, 1997. 119~133.

[4] Guillou LC, Quisquater JJ. A paradoxical identity-based signature scheme resulting zero-knowledge. In: Goldwasser S, ed. Advances in Cryptolgy-Crypto'88. Taiwan: Springer-Verlag, 1988. 216~231.

[5] Park JM, Chong E, Siegel H, Ray I. Constructing fair exchange protocols for E-commerce via distributed computation of RSA signatures. In: Proc. of the 22th Annual ACM Symp. on Principles of Distributed Computing. Boston: Massachusetts Press, 2003. 172~181.

[6] Dodis Y, Reyzin L. Breaking and reparing optimistic fair exchange from PODC 2003. In: Yung M, ed. Proc. of the 2003 ACM Workshop on Digital Rights Management. New York: ACM Press, 2003. 47~54.

[7] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978,21(2):120~126.

[8] Ray I, Ray I. Fair exchange in E-commerce. ACM SIGecom Exchanges, 2002,3(2):9~17.

[9] Bao F, Deng RH, Mao W. Efficient and practical fair exchange protocols with off-line TTP. In: Proc. of the 1998 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Press, 1998. 77~85.

[10] Zhou J, Gollmann D. A fair non-repudiation protocol. In: Proc. of the 1996 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Press, 1996. 55~61.

[11] Franklin MK, Reiter MK. Fair exchange with a semi-trusted third party. In: Proc. of the 4th ACM Conf. on Computer and Communications Security. Switzerland: ACM Press, 1997. 1~5.

[12] Boyd C, Foo E. Off-Line fair payment protocols using convertible signatures. In: Ohta K, Pei DY, eds. Advances in Cryptology (ASIACRYPT'98). Beijing: Springer-Verlag, 1998. 271~285.

[13] Asokan N, Shoup V, Waidner M. Optimistic fair exchange of digital signatures. In: Nyberg K, ed. Advances in Cryptology-EUROCRYPT'98. Helsinki: Springer-Verlag, 1998. 591~606.

[14] Zhou YB, Feng DG, Xu Z, Li DQ. IPsec: Securing VPNs. Beijing: Tsinghua University Press, 2002. 80~100 (in Chinese).

[15] Feng DG, Zhou YB, Zhang ZF, Li DQ. RSA Security's Official Guide to Cryptography. Beijing: Tsinghua University Press, 2001. 85~121 (in Chinese).

附中文参考文献:

[14] 周永彬,冯登国,徐震,李德全.IPSec:VPN 的安全实施.北京:清华大学出版社,2002.80~100.

[15] 冯登国,周永彬,张振峰,李德全.密码工程实践指南.北京:清华大学出版社,2001.85~121.