公平的非否认密码协议及其形式分析与应用*

李先贤, 怀进鹏

(北京航空航天大学 计算机科学与工程系,北京 100083)

E-mail: lixx@cscw.buaa.edu.cn

http://www.buaa.edu.cn

摘要: 在安全数据通信中,数据发送和接收的非否认性是一个极为重要的问题.近年来,实现这种类型的密码协议主要是通过可信第三方参与数据的加密与传送,因而,可信第三方的可靠性和安全性是系统性能的瓶颈.提出了一个公平的双方不可否认的密码协议——NCP(non-repudiation cryptographic protocol).这个协议解决了可信第三方的性能瓶颈问题,是一个更为有效的、安全的密码协议.用信任逻辑对其进行了形式分析,最后探讨了它在电子邮件中的应用.

关键词: 数字签名;非否认密码协议;公钥体制;私钥体制;信任逻辑

中图法分类号: TP393 **文献标识码**: A

计算机和通信网的广泛应用,在为人们的生活和工作带来极大方便的同时,也带来了许多急需解决的安全问题,其中数据的认证是一个重要的问题.在端到端通信中,发送数据的不可否认性可通过数字签名技术来实现.随着应用环境安全要求的复杂化,例如在发送有价消息和重要消息时,接收者对所收到的消息必须承担一定的责任,这时,系统还需提供接收数据的不可否认性.我们称具有发送和接收双方不可否认性的密码协议为NCP(non-repudiation cryptographic protocol).

本文设计了一个双方不可否认的、安全实用的密码协议,并用信任逻辑对它进行了安全性分析.该协议基于公钥体制、私钥体制和Hash函数,引入第三方可信中心作为裁决者.这个协议具有如下特点:如果通信双方遵守协议,则无需通过可信中心即可完成数据交互,可信中心只在双方发生纠纷时,通过仲裁协议确定哪一方是欺骗者,以保证信息交易安全、公平地进行,不会因其中一方中止执行协议而致使另一方利益受到损失;且只须进行3次数据传送便可完成一次双方不可否认的通信;此外,协议的安全性基于所用密码算法的安全性,与通信双方的计算能力无关,也不依赖于可信中心的安全性.NCP协议特别适用于发送重要的消息和有价消息,接收者必须对所收到消息负担责任的应用环境.协议为这一类的应用环境提供了安全服务,具有很好的应用价值.

本文第2节描述了一个新的不可否认密码协议(NCP).第3节用信任逻辑对NCP协议做了形式化分析.第4节探讨了此协议在电子挂号邮件中的应用.

1 国内外相关研究工作

为了解决数据通信中敏感和重要的非否认性问题,前人已在此领域做了大量研究工作.1985年,Even[1]等人利用不经意的传输协议提出了一个数字挂号函件公平协议.这个协议的诱人之处在于:无需第三方介入便可自动防止对方欺骗,从而实现了公平性和双方不可否认性.遗憾的是,这个协议需要双方进行过多的信息交换(交换次数多于所用密钥长度位数,例如用128位密钥,则至少需要进行128次数据交互),在目前的Internet上是令人无法忍受的;其次,这个协议假设通信双方具有相同的计算能力,但这个假设在很多情况下是不真实的,

* 收稿日期: 2000-01-25; 修改日期: 2000-03-30

基金项目: 国家自然科学基金资助项目(69775015);国家863高科技项目基金资助项目(863-306-02-01)

作者简介: 李先贤(1969-),男,广西人,讲师,博士生,主要研究领域为信息安全;怀进鹏(1962),男,山东人,教授,博士生导师,主要研究领域为人工智能,协同工作,信息安全.

例如,一般认为公司比个人有更强的计算能力,因而这个协议不具有实用性.

1996年,Robert Deng和Li Gong等人[2]提出了认证电子邮件协议,为电子邮件的传输提供非否认服务.J.Zhou和D.Gollman[3]设计了签订电子合同协议,可提供双方不可否认性.在这两个协议中,通信主体须与可信中心共享密钥.基于电子商务的应用背景,IBM公司开发了一组安全电子支付协议——iKP(i-key-protocol,i=1,2,3,...),然而,这个协议无法解决公平性问题.1999年,卿斯汉等人[4]基于电子商务应用,对iKP协议进行了改进,设计了iKPI(i-key-protocol issuer)协议,这个协议引入了网关作为第三方可信中心,可实现公平的信息交易,保证交易双方的不可否认性.以上这3个协议均通过引入可信第三方参与数据加密与传送,以实现数据发送和接收的非否认性,因此也都存在两个缺陷:一个是大量消息经过可信中心传递,可信中心成为消息流通的瓶颈,且需5次以上数据交互才可完成一次数据通信,从而降低了系统的效率;另一个是过多地依赖于可信中心的安全性、可靠性,给可信中心的安全管理带来极大的困难.

2 NCP协议的描述

2.1 协议概述

协议包括3个参与方:发送者A(Alice),接收者B(Bob)和可信中心C(Center).A和B均拥有公开密钥对和相应的公开密钥证书,C是协议中公正的认证方(C不必拥有公开密钥),C拥有一个向外发布消息的网址,设立可供公众检索的公用信息数据库,只有C具有对该数据库的写权限,其余各方只有读取权.可信中心C充当"权威机构",当通信双方发生争议时,根据双方提出的证据按仲裁协议进行仲裁.

2.2 协议的描述

基本的密码假设与符号说明:

(1) 私钥体制算法假设:用$\{M\}_K$表示在密钥K控制下对M进行加密运算得到的密文,由$\{M\}_K$恢复M或由$\{M\}_K$,M求K在计算上是不可行的.

(2) 公钥体制算法假设:设A具有公钥a,而相应的私钥a^{-1}永远不会被A以外的任何主体知道,由密文$\{M\}_a$恢复M在计算上是不可行的.

(3) 公钥签字算法:用$\{M\}_{a^{-1}}$表示A用私钥对M作的一个签字,而任何一个主体均可验证A的签字,用$V_A(M,\{M\}_{a^{-1}})$表示用A的公钥a对签字验证,$V_A(M,\{M\}_{a^{-1}})$为真表示签字合法.

(4) 杂凑(hash)函数:是将任意长字串映射为一个较短的定长字串的函数,用H表示,一个强单向Hash函数是一个单向Hash函数,而且找一对$x_1,x_2,x_1\neq x_2$,使$H(x_1)=H(x_2)$在计算上是不可行的.

下面对NCP协议方案进行描述.

设a和b分别是A和B的公钥,H是公开的强单向Hash函数,符号"$A\rightarrow B:X$"表示主体A向主体B发送消息X;用"$A\rightarrow C(B):X$"表示主体A向主体C和主体B发送了消息X,并且C可收到消息X当且仅当B可收到消息X.此外,下面的描述还将沿用前面和文献[5]中的符号,详细说明见文献[5].

协议由通信协议和仲裁协议两个部分组成.

(一) 通信协议步骤的描述如下:

(1) $A\rightarrow B:\{M\}_K,\{H(\{M\}_K),T_A\}_{a^{-1}},T_A$,

(2) $B\rightarrow A:\{H(\{M\}_K),T_A+1,T_B\}_{b^{-1}},T_B$,

(3) $A\rightarrow C(B):\{K\}_b,\{H(K),T_B+1,T_C\}_{a^{-1}},T_C$.

说明:① K是A随机生成的会话密钥,T_A是时戳;

② T_B是B生成的时戳,B只有在验证A的签字$\{H(\{M\}_K),T_A\}_{a^{-1}}$合法后,才执行协议第(2)步,否则中止执行协议;

③ T_C是时戳,A只有在验证B的签字$\{H(\{M\}_K),T_A+1,T_B\}_{b^{-1}}$合法后,才会执行协议第(3)步.在协议第(3)步,A将消息发布在公开数据库中,任何主体均可随时访问(不能删除和更改),A同时将消息发送给B,可节省B访问公开数据库的开销.

④ B 获得$\{K\}_b$后,用 B 的私钥b^{-1}解密得到K,用K解密$\{M\}_K$即可得到消息M.

(二) 仲裁协议

当接收者否认收到消息时,A 请求 C 裁决,C 根据下面的规则裁决 B 是否收到消息M:

(1) C 首先检索公证数据库和审计日志,若 C 没有检索到 A 公开的$\{K\}_b$及其签字,则判定 B 没有收到M;

(2) 否则,设 C 检索到 A 公开$\{K\}_b$的时间为T',则 A 将下列数据提交给 C:

$$k', M', \{H(\{M\}_K), T_A+1, T_B\}_{b^{-1}}, T_A, T_B$$

(a) C 验证等式$\{K'\}_b=\{K\}_b$是否成立,并且用 A 的公钥检验签字$\{H(K), T_B+1, T_C\}_{a^{-1}}$是否合法;

(b) C 根据k', M'计算$\{M'\}_{K'}$和$H(\{M'\}_{K'})$,并用 B 的公钥b验证 B 的签字$V_B((H(\{M'\}_{K'}), T_A+1, T_B), S)$是否合法,其中$S=\{H(\{M\}_K), T_A+1, T_B\}_{b^{-1}}$.

如果(a)、(b)都成立,则判定 B 在时间$T'+\Delta T$内已收到消息M,否则判定 B 没有收到消息M. 这里的ΔT是根据具体应用环境规定的一个固定值.

说明:① 由加密算法的确定性可知,条件(a)成立当且仅当$K=K'$确实由 A 在通信协议发送,故而 B 已得到了K(因 B 已得到了$\{K\}_b$,而b是 B 的公钥);条件(b)说明了$\{M'\}_{K'}=\{M\}_K$,从而得到了$M'=M$,即证明 B 确实收到了 A 的原发消息M,所以,(a)和(b)成立,则 B 收到了消息M.

② 仲裁协议只是在发生纠纷时才执行,不是每次通信都执行. 这里,可信中心 C 存储$\{K\}_b$并做审计以确认数据存入的时间,同时,供 B 查询,将来作为仲裁的证据.

③ 在实际应用中,根据具体情况可以规定一个裁决的截止日期,过期后,数据库自动删除过期的$\{K\}_b$,以免造成公开数据库数据沉积,难以检索.

3 NCP 协议的形式分析

现在,我们用逻辑系统分析和说明 NCP 协议是正确、公平和安全的.

1989 年,Burrows 等人[5]提出一种基于信任逻辑的形式化方法,用于分析认证协议的安全性. 此后,研究人员对这种方法进行了大量的改进和扩充,形成了所谓的 BAN(即 Michael Burrows, Martin Abadi 和 Roger Needham)类逻辑. 然而,BAN 逻辑不适于分析协议的可追究性和公平性[6,7]. 为此,Kailar[6]提出了新的逻辑,用于分析电子商务协议的可追究性,然而,Kailar 逻辑用于分析协议公平性也具有一定缺陷[7]. 为了分析 NCP 协议的公平性,我们将扩充 BAN 逻辑的语义和逻辑公理,所引入的公理的意义是明确的. 然而,在这里我们不打算为分析一般协议的公平性而建立逻辑框架,这还是一个有待于解决的问题[7].

3.1 基本概念和符号

应用环境假设:由证书机构 CA(certification authority)所颁发的证书是新的. 我们主要考虑"过去"和"当前"这两个时间的区别,"当前"从协议的执行开始,而这一时间之前所有消息的发送都被看成是"过去"发生的事件. 这里沿用 BAN 逻辑系统的一些符号和语义,特定主体用符号 A,B,C 表示;P,Q,R代表主体变量标识符,X,Y代表任意表述,K代表任意的加密密钥(详细说明参见文献[5]).

$P\models X$:表示 P 信任 X;

$P\mid\sim X$:表示 P 曾经说过 X,即 P 在过去某时刻发送了一个包含表述 X 的消息;

$P\lhd X$:表示 P 看到了消息 X,即 P 曾经阅读并可以重复 X;

$\#(X)$:表示表述 X 是新鲜的,即在此协议之前,X 从没有被发送过. 对于一次性随机数和时戳来说,这通常是真实的;

$\overset{a}{\mapsto}P$: 表示 P 具有公钥 a,相应的私钥 a^{-1}永远不会被主体 P 之外的任何主体知道.

在 BAN 逻辑系统中,核心是"信任关系",而没有不可否认性的分析与描述. 为了更准确地描述 NCP 协议,我们增加一些语义:

P CanProve X:表示对于任何主体 Q,P 可通过执行一系列的操作,使 Q 相信公式 X(这条语义来源于文献[6]).

$VT_a(X,S)$:表示用公钥 a 验证 S 是 X 的一个合法签字,即 $S=\{X\}_{a^{-1}}$.

逻辑规则:

R1(公钥解密规则) $$\frac{P\models\stackrel{a}{\mapsto}P,P\lhd\{X\}_a}{P\lhd X};$$

R2(私钥解密规则) $$\frac{P\lhd K,P\lhd\{X\}_K}{P\lhd X};$$

R3(新鲜传播规则) $$\frac{P\models\#(X)}{P\models\#(X,Y)};$$

R4(说过投射规则) $$\frac{P\models(Q\mid\sim(X,Y))}{P\models(Q\mid\sim X),P\models(Q\mid\sim Y)}.$$

在BAN逻辑系统中,签字的意义规则没有对签字的不可伪造性进行准确的描述.为了分析NCP协议,我们增加下面的逻辑规则:

M1(签字不可伪造规则) $$\frac{P\models\stackrel{b}{\mapsto}P,P\models\#(X),VT_b(X,S)}{P\models P\mid\sim X}.$$

说明:条件 $P\models\#(X)$ 意味着在这之前主体 P 没有对消息 X 进行过签字,即可保证签字不是重发的.这个条件是必要的,否则不能保证不受重放攻击.

M2(杂凑函数不可求逆规则) $$\frac{P\models P\mid\sim H(X)}{P\lhd X}.$$

3.2 NCP协议的理想化描述

在本协议中,可信中心有公开数据库,即有假设:若可信中心C收到了消息 X,则任何一个主体 Q 均可得到消息 X.在实际应用中,应规定 Q 在公开消息后一段时间内查询这个公开消息,为了简单,本理想化描述省略了时间区别.因此,在具体协议中的表述"主体A公开某个消息 X"等价于描述"C收到了消息 X".沿用前面和文献[5]中的符号,给出具体协议的理想化描述:

(1) $A\rightarrow B:\{M\}_K,\{H(\{M\}_K),T_A\}_{a^{-1}}$,

(2) $B\rightarrow A:\{H(\{M\}_K),T_A+1,T_B\}_{b^{-1}}$,

(3) $A\rightarrow C:\{K\}_b,\{H(K),T_B+1,T_C\}_{a^{-1}}$.

下面几个命题是协议运行的前提条件.

命题1. $C\lhd\{K\}_b\Rightarrow VT_b((H(\{M\}_K),T_A+1,T_B),S),S=\{H(\{M\}_K),T_A+1,T_B\}_{b^{-1}}$.

命题2. $C\lhd\{K\}_b\Leftrightarrow B\lhd\{K\}_b$,见原通信协议说明③.

命题3. $B\lhd M\Leftrightarrow(B\lhd K,B\lhd\{M\}_K)$,由于 M 是发送者A用密文发出的,因此B必须得到加密密钥才能解密得到明文.

命题4. $B\lhd K\Rightarrow B\lhd\{K\}_b$,因为 K 是A随机生成的会话密钥.

仲裁协议可理想化地描述为

$$\text{A提交}:\{H(\{M\}_K,T_A+1,T_B)\}_{b^{-1}},K',M.$$

可信中心的仲裁规则可表述为

$$C\models(B\lhd M)\text{当且仅当}C\lhd E,\{K'\}_b=E\text{且}VT_b(H(\{M\}_{K'},T_A+1,T_B),S).$$

这里,E 是C由数据库检索到的A曾公开的 $\{K\}_b$.注意,$\{K\}_b$ 是密文形式,C无法看到 K,$S=\{H(\{M\}_K,T_A+1,T_B)\}_{b^{-1}}$.

说明:仲裁协议是通信协议之后执行的,可信中心C只能凭公开数据库的数据和A提交的数据按协议进行裁判.$C\models B\lhd M$ 表示C判断B收到消息 M,从而B不可否认.

协议的初始假设为

① $A\models\stackrel{a}{\mapsto}A$,② $A\models\stackrel{b}{\mapsto}B$,③ $B\models\stackrel{a}{\mapsto}A$,④ $B\models\stackrel{b}{\mapsto}B$,⑤ $C\models\stackrel{a}{\mapsto}A$,⑥ $C\models\stackrel{b}{\mapsto}B$,⑦ $A\models\#(T_A)$,⑧ $B\models\#(T_B)$,⑨ $A\models\#(K)$.

3.3 NCP协议的形式化分析

定理1. 如双方都遵守协议(可不必执行仲裁协议),可得:

(1) $B \lhd M$(B可获得消息M);

(2) B CanProve $(A \mid\sim M)$(发送消息的不可否认性).

由数字签字的不可否认规则,这个定理的正确性是明显的.利用Kailar逻辑系统(见文献[6]),它的形式证明也是容易的.限于篇幅,这里不作详细证明.

定理2(公平性和接收消息的不可否认性). 通过执行仲裁协议可得$B \lhd M \Leftrightarrow C \models (B < M)$.即C通过仲裁协议裁决B收到了消息$M$当且仅当接收者B收到了消息$M$.

证明:(1) 先证$B \lhd M \Rightarrow C \models (B \lhd M)$.

如果$B \lhd M$,由命题3的$B < M \Leftrightarrow (B \lhd K, B \lhd \{M\}_K)$和命题4的$B \lhd K \Rightarrow B \lhd \{K\}_b$得到$B \lhd \{K\}_b$,由命题2可得$C < \{K\}_b$.

据命题1得到$VT_b((H(\{M\}_K), T_A+1, T_B), S)$,$S=\{H(\{M\}_K), T_A+1, T_B\}_b^{-1}$.另外,因$K, M$是由A产生的,A可向C提交数据$K'$,$M$使$K'=K$,所以有$\{K'\}_b=\{K\}_b$,那么,综上所述,由仲裁规则得$C \models (B \lhd M)$.

(2) 证明$C \models (B < M) \Rightarrow B \lhd M$.

设$C \models (B \lhd M)$,由仲裁规则得

$$C < E, \{K'\}_b = E \text{ 且 } VT_B((H(\{M\}_{K'}), T_A+1, T_B), S),$$

即得$C \lhd \{K'\}_b$,由命题2,有$B \lhd \{K'\}_b$,初始条件$B \models \overset{b}{\mapsto} B$,由规则R1得$B < K'$.

另外,由初始假设$\models \#(T_B)$,根据规则R3得$B \models \#(H(\{M\}_{K'}), T_A+1, T_B)$.又因$B \models \overset{b}{\mapsto} B$和$VT_b((H(\{M\}_{K'}), T_A+1, T_B), S)$,根据签字不可伪造规则M1得:$B \models B \mid\sim (H(\{M\}_{K'}), T_A+1, T_B)$,由规则R4得$B \models B \mid\sim H(\{M\}_{K'})$,再由杂凑不可求逆规则M2得:$B < \{M\}_{K'}$,又根据前面所证$B \lhd K'$,根据规则R2即得$B < M$.

安全性:从以上分析过程可以看出,NCP协议实现了发送和接收消息的不可否认性.同时,协议是公平的,即如果B没有收到消息M,A不能伪造证据证明B收到了消息.由形式化分析可知,协议可抵抗重放攻击和中间人攻击.

为了抵抗选择密文攻击,在协议中传送签字时,用对方的公钥将签字加密后再传送,这样可以提高系统的安全性,但却不可避免地增加了加密运算的开销,这要根据具体的应用环境而定.此外,发送者应保证会话密钥生成的随机性.

4 NCP协议的应用

4.1 NCP协议在电子商务中的应用

在协议的实现过程中,协议的第(3)步A将$\{K\}_b$在C处公开的同时,应把$\{K\}_b$传送给B,这样可以避免B访问C,从而提高系统的效率.另外,还应规定A公开$\{K\}_b$的时间T'应在某个具体时间T_0之前,即$T' \leqslant T_0 = T_B + D$,$D$是视具体应用而定的一个固定值.这样,若接收者B没有收到A传送的$\{K\}_b$,可在时间T_0之前查询可信中心C,保护接收者的利益.事实上,在实际应用中,一般认为在A不能欺骗B的情况下,A不愿给B制造麻烦.A在第(3)步把$\{K\}_b$送给C公开,而不送给B,这样做只是让B不得不访问C,对A没有好处(因为A不能以此欺骗B).

从以上讨论可以看出,NCP协议是一个公平的协议.对通信双方的利益都做了保证,通信中不会因其中一方不遵守协议而损害另一方利益,特别适用于发送有价消息、重要的消息,可用于电子商务中的电子支付和订单发送、政府部门的重要通知以及收费通知等等.在这些应用环境中,接收消息者要对收到的消息负责,他有可能企图否认收到过消息.利用NCP协议可实现这种安全需求,限于篇幅,这里不作详细的介绍.

4.2 电子挂号邮件

目前Internet上通信增多,电子邮件的安全问题引起了人们的广泛关注,实现安全电子邮件已有很多安全系统,典型的如PGP(pretty good privacy)和PEM(privacy enhanced mail),都具有数据机密性、数据源验证、消息完整性和发送方不可否认性.这里,我们考虑利用NCP协议对PGP系统改进实现电子挂号邮件业务.

PGP是一种混合密码系统,用公钥体制(RSA)、私钥体制(IDEA)、单向杂凑函数(MD-5)和RSA签名算法

实现.这些算法经检验具有较好的安全性.这里,我们只讨论利用这些算法和本文的密码协议实现挂号邮件算法过程,关于PGP算法的详细内容参考文献[8].

用$E_k(M)$($D_k(M)$)表示私钥体制下相应的加密(解密)运算(IDEA算法),而用H表示Hash函数MD-5,设(n_1,a,a')是发送者A的RSA公钥系统,a是公钥,a'是A的私钥.相应地,B的公钥系统是(n_2,b,b'),b是公钥,b'是私钥.A将消息M挂号发送给B,按PGP对消息进行预处理(M,C),C是报文,其中包含双方公开信息.步骤如下:

(1) A随机选择会话密钥k,计算$E_k(M)$,$s_1=H(E_k(M))^{a'} \bmod n_1$,将$(E_k(M),s_1)$与报文C发送给B;

(2) B验证$H(E_k(M))\equiv s_1^a \bmod n_1$是否成立,若成立则计算$L=H(E_k(M),T_1,T_2)$,$s_2=L^{b'} \bmod n_2$,$T_1$是时戳,$T_2=T_1+\Delta T$,$\Delta T$是固定的,发送$(s_2,T_1,T_2)$给A;

(3) A计算$L=H(E_k(M),T_1,T_2)$,验证$L\equiv s_2^b \bmod n_2$是否成立,若成立则计算$k'=k^b \bmod n_2$,$s'=H(k)^{a'} \bmod n_1$,在时间T_2之前将(k',s')发送给C和B;

(4) B计算$k'^{b'} \bmod n_2=(k^b)^{b'} \bmod n_2=k$,用$k$解密计算$D_k(E_k(M))=M$.

可信中心C.与PGP不同,系统必须建立一个可信中心C.在C处建立一个数据库以支持用户公开消息的存储和查询,用户无权修改这些信息.C对用户公开的消息作审计记录以确认时间,一旦用户双方发生纠纷,以审计记录时间为准进行裁决,因此,系统应以C的时间为准,保证C的时钟的准确性.

对回执签字.挂号邮件加上标识符,使系统可以识别出挂号邮件,以作相应的处理.当收到挂号邮件时,先验证发送者的身份,再确定是否接收这封邮件(这时只收到密文,接收者不知道邮件内容),如果不想接收这封邮件,可拒绝对回执签字,这样可以避免挂号邮件的滥用.

保存与传递.发送用户应保存挂号邮件的原文、会话密钥和对方的签字,直到认为消息失去价值.这是为了防止对方否认.

5 与相关工作的比较

(1) 在NCP协议中,可信中心只是起监督和仲裁的作用,在通信中如果双方都遵守协议,则可信中心可以不参与数据交互,而在实际应用中,一般认为在大多数情况下双方是遵守协议的,这样就避免了可信第三方是系统性能的瓶颈问题,而这是目前协议存在的问题.此外,可信中心的数据秘密泄露不会导致用户保密数据的泄露,即比NCP协议的安全假设少.同时,NCP协议保证了通信双方的公平性,通信双方不能因欺骗另一方而使其利益受到损害.NCP协议还具有较好的安全性,经形式化分析表明:NCP协议安全性基于所用密码算法的安全性,可以抵抗常见的攻击,如假冒攻击和中间人攻击等.

(2) 虽然在Even[1]的方案中完全抛开了可信中心,可自动实现双方不可否认性,但需要进行的数据交互过多,而且要求通信双方有相同的计算能力,这是没有实用价值的.相对而言,NCP协议虽然引入了可信中心裁决,但只需3次数据交互便可完成一次数据通信且与双方的计算能力无关,是一个实用的协议.

(3) 灵活性.NCP协议可以采用任何已知的具有代表性的密码算法,包括公钥算法、私钥算法和杂凑算法,因此,协议的实现可不受密码算法产品出口的限制.

6 结 论

本文以公钥体制、私钥体制和数字签名技术为基础,分析设计了一个抗否认的密码协议方案,并用信任逻辑分析了它的安全性,讨论了它在电子邮件中的应用.从以上讨论可以看出,这个方案确实避免了可信中心的瓶颈问题和对它的安全性依赖,同时实现了发收双方的不可否认性.在没有第三方参与的双方不可否认协议的实现中,最难解决的问题是如何同时交换签字,事实上,它已被证明是不可完全实现的[1].本文引入可信中心作为裁决者,然而对它没有过多的依赖,提供了密码协议设计的一个新思路.

References:

[1] Even, S., Goldreich, O., Lempel, A. A randomizing protocol for signing contracts. Communications of the ACM,

1985,28(6):637～647.

[2] Deng R. H., Gong L. Practical protocols for certified electronic mail. Journal of Network and Systems Management, 1996,4(3):279～297.

[3] Zhou, J., Gollman, D. A fair non-repudiation protocol. In: Roscheisen, M., Serban, C. eds. Proceedings of the 1996 IEEE Symposium on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 1996. 55～61.

[4] Qing Si-han, Chang Xiao lin, Zhang Jiang. Design and implementation of secure electronic commerce protocol iKPI. In: Qing Si-han, Feng Deng-guo eds. Information and Communication Security——CCICS'99: Proceedings on the 1st Chinese Conference of Information and Communication Security. Beijing: Science Press, 2000. 230～239 (in Chinese).

[5] Burrows, M., Abadi, M., Needham, R. A logic of authentication. ACM Transactions on Computer Systems, 1990,8(1):18～36.

[6] Kailar, R. Accountability in electronic commerce protocols. IEEE Transactions on Software Engineering, 1996,22(5): 313～328.

[7] Zhou Dian-cui, Qing Si-han, Zhou Zhan-fei. Limitations of Kailar logic. Journal of Software, 1999,10(12):1238～1245 (in Chinese).

[8] Zimmermann, P. R. The official PGP user's guide. Boston: MIT Press, 1995.

附中文参考文献:

[4] 卿斯汉,常晓林,章江. 安全电子商务协议 iKPI 的设计和实现. 见:卿斯汉,冯登国,等编. 信息和通信安全——CCICS'99: 第1届中国信息和通信安全学术会议论文集. 北京:科学出版社,2000. 230～239.

[7] 周典萃,卿斯汉,周展飞. Kailar 逻辑的缺陷. 软件学报,1999,10(12):1238～1245.

A Fair Non-Repudiation Cryptographic Protocol and Its Formal Analysis and Applications

LI Xian-xian, HUAI Jin-peng

(Department of Computer Science and Engineering, Beijing University of Aeronautics and Astronautics, Beijing 100083, *China)*

E-mail: lixx@cscw.buaa.edu.cn

http://www.buaa.edu.cn

Received January 25, 2000; accepted March 30, 2000

Abstract: Non-Repudiation in data sending and receiving is essential in the secure communication. In recent years, this kind of cryptographic protocols has been mainly implemented by the intervention of the trusted third party in transmission and encryption of data, thus the dependability and security of the trusted third party become a bottleneck in these secure systems. In this paper, a fair non-repudiation cryptographic protocol (NCP) for both sender and receiver is proposed. It is a more efficient and secure protocol, which solves the bottleneck problem of trusted third party. And its formal analysis is presented using the belief logic. Finally its applications to E-mail communication are discussed.

Key words: digital signature; non-repudiation cryptographic protocol; public key cryptosystem; private key cryptosystem; belief logic