可转换认证加密的安全邮件协议

崔 军[1,2]，刘 琦[3]，张振涛[1,2]，李忠献[1,2]，杨义先[1,2]

(1. 北京邮电大学网络与交换技术国家重点实验室 北京 海淀区 100876;
2. 北京邮电大学网络与信息攻防技术教育部重点实验室 北京 海淀区 100876;
3. 天津城市建设学院电子与信息工程系 天津 西青区 300384)

【摘要】通过对电子商务中不可否认公平交换协议的运行流程进行了研究，论证了基于第三方的不可否认公平交换协议至少需要运行4步骤，进而指出现有一个协议实质上是需要运行4步骤的，而不仅仅是运行3步骤。依据安全协议与密码系统分开设计的原则，对比分析已有可转换认证加密方案，提出了一个可转换认证加密方案的系统模型。并基于该系统模型，设计了基于半可信第三方的不可否认的安全邮件协议。通过形式化方法分析表明，该协议具备邮件发送方和接收方均不可否认的特点。

关 键 词 可转换的认证加密； 电子商务； 公平交换； 形式化方法； 不可否认
中图分类号 TP309 **文献标识码** A doi:10.3969/j.issn.1001-0548.2010.04.027

A Sec-Email Protocol Based on the Convertible Authenticated Encryption Scheme

CUI Jun[1,2], LIU Qi[3], ZHANG Zhen-tao[1,2], LI Zhong-xian[1,2], and YANG Yi-xian[1,2]

(1. State Key Lab. of Networking and Switching Technology, Beijing University of Posts & Telecommunications Haidian Beijing 100876;
2. Key Lab. of Nnetwork and Information Attack & Defence Technology of MOE,
Beijing University of Posts & Telecommunications Haidian Beijing 100876;
3. Electronic and Information Engineering Department, Tianjin Institute of Urban Construction Xiqing Tianjin 300384)

Abstract On deep research on the workflow of non-repudiation and fair-exchange protocols in electronic commerce, it is proved that these protocols with trusted third party need to run in four steps at least. The analysis of an existing protocol shows that it needs to run in four steps, rather than just run in three steps it claims. On the principle that security protocol and cryptography system should be designed separately, a common model of convertible authenticated encryption schemes is proposed by analyzing some existing convertible authenticated encryption schemes. By using this model, a secure email protocol with semi-trusted third party is designed. Result shows that this protocol has non-repudiation features of both sender and receiver by formal analysis.

Key words convertible authenticated encryption; electronic commerce; fair-exchange; formal methods; non-repudiation

随着网络的普及，网上电子商务越来越流行，其交易的公平性也越来越受到重视。公平交换协议可以使交易双方以公平的方式交换消息，保证双方都可以得到对方的消息(或者都得不到对方的消息)，并且双方都不能对已发生的交易进行否认。

在实际生活中，要求具有公平交换特性的应用很多，如网上交易、电子邮件等。安全邮件协议是公平交换协议中的一类，是一个发送方将发送邮件m与接收方收到邮件m的证据进行交换的协议[1-4]。文献[1]提出了一种挂号电子邮件协议方案，称为CMP1。尽管对CMP1协议进行形式化分析表明，CMP1协议能达到可追究性目标(即发送者和接收者均不可否认)[5]，但是在信道不可靠的条件下，CMP1协议是非公平的。相当多的研究者基于该协议模型进行了大量基础性的研究，改进并提出了许多切实可行的邮件协议和其他公平交换协议。

文献[2]提出了一种面向邮件的不可否认邮件协议，并进行了形式化分析，指出所提出的协议只需要运行3个步骤即可。通过对发送者不可否认证据和接收者不可否认证据的定义和本文所论证的结论

收稿日期：2008 – 12 – 23；修回日期：2009 – 06 – 30
基金项目：国家973计划(2007CB310704)；国家863计划(2007AA01Z430)；国家自然科学基金(60821001).
作者简介：崔 军(1979 –)，男，博士生，主要从事网络安全、公平交换方面的研究.

(基于第三方的不可否认的公平交换协议至少运行4步骤)，以及形式化分析可知，文献[2]提出的协议实质需要运行4步骤，本文对文献[2]提出的协议作如下补充：

(1) $S\rightarrow R$: $L,S,\{M\}_K,\{\{M\}_R\}_T$，$\{L,H(\{M\}_K),H(\{\{M\}_R\}_T)\}_{S^{-1}}$；

(2) $R\rightarrow T$: $L,S,R,\{\{M\}_R\}_T$，$\{L,H(\{M\}_K),H(\{\{M\}_R\}_T)\}_{S^{-1}}$，$\{L,H(\{M\}_K)\}_{R^{-1}}$；

(3) $T\rightarrow R$: $L,\{M\}_R$；

(4) $T\rightarrow S$: $\{L,H(\{M\}_K)\}_{R^{-1}}$。

为了便于理解，对协议符号作说明如下。协议中包括发送者S、接收者R、可信中心T。M是主体S发给主体R的消息，也即需要真正传输的内容。用“$S\rightarrow R$: X”表示主体S向R发送数据X。S具有公钥S和相应的私钥S^{-1}；R具有公钥R和相应的私钥R^{-1}；T具有公钥T和相应的私钥T^{-1}。(x,y)表示x和y按$x\rightarrow y$的顺序串接。K是S随机生成的S与R之间的会话密钥。$\{M\}_K$是使用密钥K对M进行加密运算得到的密文。$H(x)$为对x使用单向散列(Hash函数)得到的值。$\{M\}_S{}^{-1}$为S用私钥对M做的签名，任何一个主体都可以验证S的签名。

CMP1和文献[1]所提邮件协议均属在线TTP邮件协议，在协议执行过程中，需要TTP参与。目前已有不少离线TTP或无TTP的邮件协议[3]，但协议的分析过程较为复杂。研究表明，没有可信第三方的参与，公平交换协议无法真正实现收发双方的公平交换[6-7]。

CMP1和文献[1]所提邮件协议中的算法运算实质上采用了加密和签名分开的传统方法。但是，文献[8-10]提出的认证加密(也称为签密)方案为邮件协议的设计提供了另一种途径。认证加密即将加密和签名结合在一起，为传送的数据同时提供不可伪造性、不可否认性和机密性，计算和通信的代价都明显小于加密和签名分开的方案。

本文基于一个半可信第三方(STTP)，借鉴可转换认证加密、多重加密传输思想，提出一个交互4步骤的不可否认安全邮件协议，实现了邮件收发双方均不可否认，并根据安全协议与密码系统分开设计的思想[11]，提出了该交互4步骤的不可否认安全邮件协议要求的可转换认证加密方案的系统模型。最后，利用文献[5]介绍的方法，对新提出的协议进行了形式化分析。

1　协议至少运行4步骤结论

本节首先论证“基于第三方的不可否认的公平交换协议至少运行4步骤”。设发送方为S，接收方为R，参与协议可信第三方为T，协议执行的步骤必须如下。

步骤 1　S通过T向R发送数据。S发送交互数据M(直接或间接)给R。交互数据M包含消息m和S的发送不可否认证据。为了获取R的接收不可否认证据，必须至少运行该步骤，将消息m和S的发送不可否认证据隐藏于M中。当T参与协议运行后，包含于M中的消息m和S的发送不可否认证据才能被R获取。

步骤 2　R向T请求S的发送数据。T参与交互数据M的处理，交互对象为R。R为了获取包含于M中的消息m和S的发送不可否认证据，T必须参与协议运算，并获取R的接收不可否认证据。

步骤 3　R从T获取S的发送数据。只有T参与协议运算，并确认R的接收不可否认证据，R才能获取包含于M中的消息m和S的发送不可否认证据。

步骤 4　S从T获取R的接收凭据。S从T获取R的接收不可否认证据，必须至少运行该步骤。当T参与交互数据M的处理后，S必须主动或被动地从T获取R的接收不可否认证据。

综合上面的分析，基于一个第三方的不可否认的公平交换协议，至少必须运行4个步骤。缺少任何一个步骤，协议就将无法正常执行，或是不公平的。

同样，基于第三方的不可否认的邮件协议也必须至少运行4个步骤。如果发送者不主动或被动地从TTP处获取接收者的接收不可否认证据，该邮件协议对发送者是不公平的。文献[2]中的邮件协议实质上缺少了S从T获取R的接收不可否认证据。

2　可转换认证加密系统模型

文献[11]指出，在设计安全协议时，可以将安全协议本身与安全协议所具体采用的密码系统分开，在假定密码系统是“完善”的基础上讨论安全协议本身的性质，即首先研究安全协议本身的安全性质，然后讨论实现层次的具体细节，包括所采用的具体密码算法等。因此，本文提出的安全邮件协议涉及的可转换认证加密方案不具体指定。但是，协议所采用的可转换认证加密方案必须满足：(1) 接收者可正常恢复消息和验证签名；(2) 当发送者否认签名时，接收者不需发送者的合作就可单独将发送者签名转换为一般签名。验证者在验证签名时，并不能获取消息明文内容。

通过对比分析已有的可转换认证加密方案[8-10]，本文提出可转换认证加密方案的系统模型。该系统模型由系统的初始化、消息的加密与签名、消息的恢复与验证、签名的转换与验证组成。

(1) 系统的初始化。系统选择或者交易双方协商选择具体的可转换认证加密方案，并公布相关参数，包含单向Hash函数。每个用户都拥有自己的公钥和私钥，如用户A的公钥为P_A、私钥为S_A。假定A为发送者，B为接收者，X为将被传递的消息。

(2) 消息的加密与签名。消息的加密与签名函数为Sig()。σ=Sig(S_A,P_B,X)表示发送者A用S_A和P_B对消息X进行的可转换加密签名，只有被指定的接收者B可恢复与验证该签名σ。

(3) 消息的恢复与验证。消息的恢复函数为De()。X=De(S_B,P_A,σ)表示接收者B用S_B和P_A解密恢复消息X，并计算$h(X)$。验证函数为Verify()，Verify(P_A,$h(X)$,σ)表示接收者B使用P_A、和$h(X)$验证A对消息X的签名σ。

(4) 签名的转换与验证。如果发送者A否认对消息X的签名，则接收者B公开$h(X)$、P_A、以及A对消息X的签名σ，任何人可由Verify(P_A,$h(X)$,σ)验证签名的有效性。

由此可见，可转换认证加密方案可以保障接收者B不必暴露消息明文且不需要签名者A参与，就可以让任何人验证原始签名σ的有效性。

基于本文提出的可转换认证加密方案的系统模型，选择满足系统模型要求的具体认证加密方案，如文献[8-10]中的认证加密方案，就能构造出本文安全邮件协议的具体实现。

3 安全邮件协议

协议基本符号说明如下：

A、B分别为邮件收、发双方，其中A为发送者，B为接收者，且邮件消息为m；

STTP为半可信的第三方；

$A\rightarrow B$: X表示A向B发送消息X；

$A\leftrightarrow B$: X表示B主动向A发送一次消息X，如果A未收到，A可以通过其他方式(如ftp)从B获得消息X；

(X,Y)表示消息X和Y进行级连；

L为标志协议的唯一标签，为一随机数；

f_1、f_2、f_3、f_4、f_5分别为协议每个运行步骤的标志；

T为由发送者A指定的接收者B能将交换消息提交到STTP的截止时间，也即STTP获得双方交换消息并承诺处理的最后时间期限；

R为交换消息子集的简称，R=L,A,B,STTP,T；

$h(X)$表示对消息X用Hash函数取摘要；

P_A、S_A分别为A的公开密钥和私有密钥；

Sig(S_A,P_B,m)为B可恢复与验证的A对消息m进行的可转换加密签名；

Sig(S_A,P_{STTP},(R,Sig(S_A,P_B,m)))为STTP可恢复与验证的A对消息(R,Sig(S_A,P_B,m))进行的可转换加密签名。

本文提出的安全邮件协议如下。

协议 1 $A\rightarrow B$: f_1,N

R=L,A,B,STTP,T;

M = R,$h(m)$,Sig(S_A,P_{STTP},(R,Sig(S_A,P_B,m)))；

N = Sig(S_A,P_B,M)。

协议 2 $B\rightarrow$STTP: f_2,P

O = M,Sig(S_B,P_A,(R,$h(m)$))；

P = Sig(S_B,P_{STTP},O)。

协议 3 $B\leftrightarrow$STTP: f_3,S

H = h(Sig(S_A,P_B,m),Sig(S_B,P_A,(R,$h(m)$)))；

S = Sig(S_{STTP},P_B,(R,Sig(S_A,P_B,m),H))。

协议 4 $A\leftrightarrow$STTP: f_4,U

U = Sig(S_{STTP},P_A,(R,Sig(S_B,P_A,(R,$h(m)$)),H))。

实际上，协议3和协议4不分先后，可以同时执行。邮件收发完成后，若收发双方A、B之间产生纠纷，则由事先共同商定的仲裁方裁定。相对其他邮件协议，本文协议具有以下3个特点。

(1) 本文协议采用可转换的认证加密方案，其计算和通信代价都明显小于加密和签名分开的方案。并且，协议实现了邮件收发双方均不可否认，具体分析见之后的“协议形式化证明”的“可追究性分析”部分。

(2) 基于可转换认证加密方案的特点，本文协议执行过程的数据也采用加密合并签名方式，保证邮件无关者无法获取相关消息，实现了邮件传递过程的保密要求，降低了对可信第三方的可信要求。因此，本文提出的邮件协议可称为安全邮件协议。

(3) 本文协议仅需运行4个步骤就可实现安全邮件协议过程，降低了通信量，提高了效率。本文协议减少运行步骤的基本思路是，发送者A通过接收者B间接向STTP发送交换消息，而不是直接向STTP发送交换消息，A和B分别直接从STTP接收交换信息。

4　协议形式化证明

4.1　基础知识

本节简要介绍文献[5]中的形式化方法。为了论述方便，本文将该形式化方法称为卿氏方法。

1) 形式化分析涉及卿氏方法基本符号。

(1) (m,n)表示消息m与消息n进行级连。

(2) K_A为主体A的公开密钥，用于验证A的数字签名；K_A^{-1}为与K_A对应的主体A的私有密钥。

(3) $h(m)$为应用于消息m的单向Hash函数。

(4) EOO(evidence-of-origin)为发送方不可否认证据，是协议向接收方提供的不可否认证据，用于证明发送方发送过某个消息。

(5) EOR(evidence-of-receipt)为收接方不可否认证据，是协议向发送方提供的不可否认证据，用于证明接收方收到发送方发送的某个消息。

2) 形式化分析涉及卿氏方法逻辑构件。

(1) A Can Prove x表示对于任何B，A可以通过执行一系列操作，使B相信公式x，且不向B泄漏任何秘密$y \neq x$。

(2) A Claims x表示A声明对公式x(以及所有x蕴涵的公式)负责，在分析过程中，蕴涵式A Claims $(x,y) \Rightarrow A$ Claims x成立，若A声明对(x,y)负责，则同时对公式x负责。

(3) A Controls x表示A对公式x具有管辖权，即参与协议的主体都相信A所声明的公式x是正确的。

(4) A Has m表示A拥有消息m。

(5) PK(A,K)表示K是A的公开密钥，用于验证A用K^{-1}签名的消息。

3) 形式化分析涉及卿氏方法公理。

公理 1　连接公理：

$$A \text{ CanProve } x \wedge A \text{ CanProve } y \Rightarrow A \text{ CanProve } (x \wedge y)$$

如果A既能够证明公式x，又能够证明公式y，则A能够证明公式$x \wedge y$。

公理 2　蕴涵公理：

$$A \text{ CanProve } x \wedge (x \Rightarrow y) \Rightarrow A \text{ CanProve } y$$

如果A能够证明公式x，且公式x蕴涵公式y，则A能够证明公式y。

公理 3　签名公理：

$$(A \text{ Has } \{m\}_{K^{-1}}) \wedge A \text{ CanProve PK}(B,K) \Rightarrow A \text{ CanProve } (B \text{ Claims } m)$$

如果A有消息m的K^{-1}签名$\{m\}_{K^{-1}}$，且A能证明K用于验证B的身份，则A能证明B对消息m负责。

公理 4　管辖公理：

$$A \text{ CanProve } (B \text{ Controls } x) \wedge A \text{ CanProve}(B \text{ Claims } x) \Rightarrow A \text{ CanProve } x$$

如果A能够证明B对公式x具有管辖权，且A能够证明B对公式x负责，则A能证明公式x成立。

因篇幅所限，卿氏方法的详尽描述可参阅文献[5]。

4.2　协议形式化证明

证明前，引入谓词Match，用于校验消息(X,Y)与其摘要$h(X,Y)$的一致性，亦即Match$((X,Y),h(X,Y))$= TRUE当且仅当对(X,Y)应用Hash函数$h()$时，其结果为$h(X,Y)$。证明如下：

令 $X = \text{Sig}(K_A^{-1},K_B,m)$，$Y = \text{Sig}(K_B^{-1},K_A,(R,h(m)))$，$H = h(X,Y)$，$R = L,A,B,\text{STTP},T$。

1) 协议分析准备

(1) 列出初始拥有集合$O_A^0 = \{K_A^{-1},K_A,K_B,K_{\text{STTP}}\}$，$O_B^0 = \{K_B^{-1},K_B,K_A,K_{\text{STTP}}\}$。

(2) 列出初始状态假设集合，其中基本假设为：

假设 1　A CanProve PK(B,K_B)；

假设 2　B CanProve PK(A,K_A)；

假设 3　A,B CanProve PK$(\text{STTP},K_{\text{STTP}})$。

可信假设为：

假设 4　A,B CanProve (STTP Controls(将(Y,H)发送A))；

假设 5　A,B CanProve (STTP Controls(将(X,H)发送B))；

假设 6　STTP Claims(将H发送A) $\Rightarrow$ STTP Claims Match($(X,Y),H$)

假设 7　STTP Claims(将H发送B) $\Rightarrow$ STTP Claims Match($(X,Y),H$)；

假设 8　STTP Claims Match($(X,Y),H$) $\Rightarrow$ STTP Claims (将Y发送A)；

假设 9　STTP Claims Match($(X,Y),H$) $\Rightarrow$ STTP Claims (将X发送B)；

假设 10　A,B CanProve(STTP Controls Match ($(X,Y),H$))。

协议理解假设为：

假设 11　(将(X,H)发送B) $\Rightarrow B$ Has(X,H)；

假设 12　(B Has X) $\wedge$ (B Has H) $\wedge$ Match ((X,Y), H) $\Rightarrow B$ Claims m；

假设 13　STTP Claims $(B,H) \Rightarrow$ STTP Claims (将H发送B)；

假设 14　B Has $\text{Sig}(K_{\text{STTP}}^{-1},K_B,(R,X,H)) \Rightarrow B$ Has X。

(3) 列举EOO= $\mathrm{Sig}(K_{\mathrm{STTP}}^{-1},K_B,(R,X,H))$ 和EOR= $\mathrm{Sig}(K_{\mathrm{STTP}}^{-1},K_A,(R,Y,H))$。

2) 可追究性分析

(1) 列举可追究性目标

目标 1 *B* CanProve (*A* Claims *m*)

目标 2 *A* CanProve (*B* Claims *m*)

(2) 分析EOO与EOR是否符合可追究性要求

假定 EOO $\in O_B$ 成立，即 $\mathrm{Sig}(K_{\mathrm{STTP}}^{-1},K_B,(R,X,H)) \in O_B$。

由*B* Has $\mathrm{Sig}(K_{\mathrm{STTP}}^{-1},K_B,(R,X,H))$、假设3和假设14可得*B* Has *X*，即*B* Has $\mathrm{Sig}(K_A^{-1},K_B,m)$。

由*B* Has $\mathrm{Sig}(K_A^{-1},K_B,m)$、假设2和公理3可得目标1，即*B* CanProve (*A* Claims *m*)。

假定 EOR $\in O_A$ 成立，即 $\mathrm{Sig}(K_{\mathrm{STTP}}^{-1},K_A,(R,Y,H)) \in O_A$，由*A* Has $\mathrm{Sig}(K_{\mathrm{STTP}}^{-1},K_A,(R,Y,H))$、假设3和公理3可得*A* CanProve (STTP Claims (*R*,*Y*,*H*))。

由*A* CanProve (STTP Claims (*R*,*Y*,*H*))、$(R \Rightarrow B)$、$((R,Y,H) \Rightarrow H)$和公理2可得*A* CanProve (STTP Claims (*B*,*H*))。

由*A* CanProve (STTP Claims (*B*,*H*))、假设13和公理2可得*A* CanProve (STTP Claims (将*H*发送*B*))。

由*A* CanProve (STTP Claims (将*H*发送*B*))、假设5、公理2和公理4可得*A* CanProve (将*H*发送*B*)。

由*A* CanProve (将*H*发送*B*)、假设11和公理2可得*A* CanProve (*B* Has *H*)。

由*A* CanProve (STTP Claims (将*H*发送*B*))、假设7和公理2可得*A* CanProve (STTP Claims Match((*X*,*Y*),*H*))。

由*A* CanProve (STTP Claims Match((*X*,*Y*),*H*))、假设10和公理4可得*A* CanProve (Match((*X*,*Y*),*H*))。

由*A* CanProve (STTP Claims Match((*X*,*Y*),*H*))、假设9和公理2可得*A* CanProve (STTP Claims (将*X*发送B))。

由*A* CanProve (STTP Claims (将*X*发送B))、假设5、公理2和公理4可得*A* CanProve (将*X*发送*B*)。

由*A* CanProve (将*X*发送*B*)、假设11和公理2可得*A* CanProve (*B* Has *X*)。

由*A* CanProve (*B* Has *H*)、*A* CanProve (Match((*X*,*Y*),*H*))、*A* CanProve (*B* Has *X*)和公理1可得*A* CanProve ((*B* Has *X*) Λ (*B* Has *H*) Λ Match((*X*,*Y*),*H*))

由*A* CanProve ((*B* Has *X*) Λ (*B* Has *H*) Λ Match((*X*,*Y*),*H*))、假设12和公理2可得目标2，即*A* CanProve (*B* Claims *m*)。

因此，协议EOO与EOR的设计满足可追究性要求。

(3) 分析协议是否达到可追究性目标

因为 $O_B^3=O_B^2 \cup$ EOO 和 $O_A^4=O_A^3 \cup$ EOR，所以有 $\mathrm{EOO} \in O_B^3 \subseteq \mathrm{O_B}$ 和 $\mathrm{EOR} \in O_A^4 \subseteq O_A$。因此，协议达到可追究性目标，即发送方*A*和接收方*B*均不可否认。

3) 公平性分析

协议达到公平性目标等价于下述命题成立，即 $\mathrm{EOO} \in O_B^{i-1}$ 当且仅当 $\mathrm{EOR} \in O_A^{i-1}$，其中*i*=1,2,3,4。

由于假设*A*、*B*与STTP之间的信道为可靠信道；协议满足 $\mathrm{EOO} \in O_B^3 \subseteq O_B$，$\mathrm{EOO} \notin O_B^2 \subseteq O_B$，$\mathrm{EOR} \in O_A^4 \subseteq O_A$，$\mathrm{EOR} \notin O_A^2 \subseteq O_A$；并且协议3和协议4不分先后，可以同时进行。因此本文协议满足公平性的要求。

5 结 束 语

本文首先论证了“基于第三方的不可否认的公平交换协议至少运行4步骤”的结论，然后提出了可转换认证加密方案的系统模型，并基于该系统模型，设计了一个安全邮件协议。该协议具有交互次数少、公平性高、收发双方均不可否认、传输安全等特点。结合本文的认证加密方案系统模型和具体的认证加密方案，就能构造出本文邮件协议的具体实现。因此，本文提出的安全邮件协议具有一定的实际应用价值。

参 考 文 献

[1] DENG R, GONG L. Practical protocols for certified electronic mail[J]. Journal of Network and Systems Management, 1996, 4(3): 279-297.

[2] 彭红艳, 李肖坚, 夏春和, 等. 一种面向电子邮件的不可否认协议及其形式化分析[J]. 计算机研究与发展, 2006, 43 (11): 1914-1919.
PENG Hong-yan, LI Xiao-jian, XIA Chun-he, et al. A non-repudiation protocol for E-Mail and its formal analysis [J]. Journal of Computer Research and Development, 2006, 43(11): 1914-1919.

[3] 张 青, 张 龙, 温巧燕, 等. 基于签密的认证邮件协议[J]. 电子科技大学学报, 2008, 37(2): 282-284.
ZHANG Qing, ZHANG Long, WEN Qiao-yan, et al. A new certified E-mail protocol based on signcrytion[J]. Journal of University of Electronic Science and Technology of China, 2008, 37(2): 282-284.

[4] SHAO Min-hua, WANG Gui-lin, ZHOU Jian-ying. Some common attacks against certified email protocols and the countermeasures[J]. Computer Communications (Special Issue on Internet Communications Security), 2006, 29(15): 2759-2769.

(下转第622页)

stability criteria for interval delayed neural networks via an LMI approach"[J]. IEEE Trans on Circuits and Systems II, 2008, 55(11): 1198-1202.
[18] SHAO J L, HUANG T Z, ZHOU S. An analysis on global robust exponential stability of neural networks with time-varying delays[J]. Neurocomputing, 2009, 72(7-9): 1993-1998.
[19] HORN R A, JOHNSON C R. Topics in Matrix Analysis[M]. Cambridge: Cambridge Univ Press, 1991.
[20] HADDOCK J R, TERJEKI J. Liapunov-Razumikhin functions and an invariance principle for functional differential equations[J]. Journal of Difference Equations, 1983, 48: 95-122.
[21] ZHANG Q, WEI X P, XU J. An analysis on the global asymptotic stability for neural networks with variable delays[J]. Physics Letters A, 2004, 328: 163-169.

编 辑 蒋 晓

(上接第584页)

[12] 朴承镐, 高文信, 蔡 立. 轨迹成型法精密磨削加工机床的精度分析[J]. 光学技术, 1999, 1(1), 54-57.
PIAO Cheng-hao, GAO Wen-xin, CAI Li. Precision analysis of precisely grinding machining machine for locus shaping method[J]. Optical Technology, 1999, 1(1), 54-57.
[13] 杜西亮, 戴景民. 基于神经网络的分振幅光偏振仪的数据处理[J]. 中国激光, 2007, 34(1): 89-93.
DU Xi-liang, DAI Jing-min. Data processing method for the division-of-amplitude photopolarimeter based on an artificial neural network[J]. Chinese Journal of Lasers, 2007, 34(1): 89-93.
[14] 於自岚, 高传玉, 曾丹勇, 等. 激光冲击区表面质量的人工神经网络研究[J]. 激光技术, 2001, 25(1): 1-6.
YU Zi-lan, GAO Chuan-yu, ZENG Dan-yong. Study of the surface qualities of laser shock-processing zones using an artificial neural network[J]. Laser Technology, 2001, 25(1): 1-6.
[15] 万来毅, 陈建勋, 王卫平, 等. 基于BP神经网络的图像识别研究. 武汉科技大学学报(自然科学版), 2006, 29(3): 277-279.
WAN Lai-yi, CHEN Jian-xun, WANG Wei-ping, et al. Image recognition based on BP neural network[J]. Journal of Wuhan University of Science and Technology (Natural Science Edition), 2006, 29(3): 277-279.

编 辑 漆 蓉

(上接第602页)

[5] 卿斯汉. 一种电子商务协议形式化分析方法[J]. 软件学报, 2005, 16(10): 1757-1765.
QING Si-han. A formal method for analyzing electronic commerce protocols[J]. Journal of Software, 2005, 16(10): 1757-1765.
[6] PAGNIA H, GATNER F C. On the impossibility of fair exchange without a trusted third party[R]. Darmstadt, Germany: Darmstadt University of Technology, 1999.
[7] ALPTEKIN K, ANNA L. Usable optimistic fair exchange [J/OL]. [2008-11-19]. Cryptology ePrint Archive, http://eprint.iacr.org/2008/431.pdf.
[8] ZHENG Y. Digital signcryption or how to achieve cost (signature and encryption) << cost(signature) + cost (encryption)[C]//Advance Cryptology-CRYPTO'97. Berlin: Springer-Verlag, 1997, 1294: 169-179.
[9] WU T, HSU C. Convertible authenticated encryption scheme[J]. The Journal of Systems and Software, 2002, 62: 205-209.
[10] WANG Gu-lin, BAO Feng, MA Chang-she. Efficient authenticated encryption schemes with publicly verifiability[C]//IEEE 60th Vehicular Technology Conference. Los Angeles: IEEE, 2004: 3258-3261.
[11] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.

编 辑 蒋 晓