ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.11, November 2007, pp.2871−2881
DOI: 10.1360/jos182871

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于证人不可区分的通用可复合安全并行可否认认证*

冯 涛+, 马建峰

(西安电子科技大学 计算机网络与信息安全教育部重点实验室,陕西 西安 710071)

Universally Composable Security Concurrent Deniable Authentication Based on Witness Indistinguishable

FENG Tao+, MA Jian-Feng

(Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an 710071, China)

+ Corresponding author: Phn: +86-29-88202352, Fax: +86-29-88202352, E-mail: fengt@lut.cn, http://www.xidian.edu.cn

Feng T, Ma JF. Universally composable security concurrent deniable authentication based on witness indistinguishable. *Journal of Software*, 2007,18(11):2871−2881. http://www.jos.org.cn/1000-9825/18/2871.htm

Abstract: A new approach and an idea for exploration are presented to the concurrent deniable authentication based on witness-indistinguishable (WI) within the framework of universally composable (UC) security. A definition of an ideal functionality for deniable authentication is formulated. A new deniable authentication protocol is proposed based on two primitives of the verifiably smooth projective Hashing (VSPH) and non-committing encryptions (NCE). This new approach is practically relevant to VSPH based on the Decisional Diffie-Hellman (DDH) assumption and NCE based on the decisional composite residuosity (DCR) assumption. Compared with a timing constraint and public directory model, simulation of the concurrent protocols is not needed to restrict an adversary capability in a common reference string (CRS) model. The protocols are forward deniable and UC security against adaptive adversaries. Unlike previous proposals with the CCA2 public-key cryptosystem or multi-trapdoor commitments paradigm, the new paradigm leads to more efficient protocols.

Key words: information security; concurrent deniable authentication; universally composable security; witness-indistinguishable; verifiably smooth projective Hashing

摘 要: 针对并行可否认认证问题,在UC(universally composable)安全框架中,基于WI(witness indistinguishable)提出了一种新的研究思路和解决方法.根据可否认认证的安全目标,形式化地建立了 UC 安全的并行可否认认证模型.利用可验证平滑投影哈希函数和非承诺加密体制,构造了一类新的并行可否认认证协议结构,基于确定性复合剩余假设和确定性Diffie-Hellman假设,实现了一个具体的协议方案.在公共参考串模型中,利用UC框架解决并行协议仿真问题,与定时假设和公共目录方案相比,不需要限定攻击者能力.新方案具备前向可否认性,是自适应攻击者UC安全的.不同于CCA2加密体制结构或多陷门承诺结构的并行可否认认证,协议效率得到了改善.

关键词: 信息安全;并行可否认认证;通用可复合安全;证人不可区分;可验证平滑投影哈希函数

中图法分类号: TP309 **文献标识码**: A

* Supported by the National Natural Science Foundation of China under Grant Nos.60573036, 60633020 (国家自然科学基金)
Received 2006-11-03; Accepted 2007-04-06

Dowork等人在研究并行零知识证明问题时,提出了并行可否认认证(concurrent deniable authentication,简称CDA)协议[1].可否认认证能够使接收者鉴别消息的来源,但是,接收者不能向第三方证明消息来源,接收者通过“仿真”发送者和接收者之间的消息实现可否认认证.签名认证机制不具有可否认性.许崇祥等人基于DH(Diffie-Hellman)假设提出了一个简单的可否认认证[2].Cao等人提出了利用对映射的基于身份的可否认认证[3].

协议并行运行存在消息交叉循环嵌套,无法直接使用基于仿真的方法进行协议的安全性分析.通过一些变通技术可以使用基于仿真的可证明安全方法.例如,在限定攻击者能力的情况下,基于时间假设模型,Dowork等人提出了CCA2 安全加密体制的可否认认证协议[1].基于公共目录假设模型,Aumann等人使用纠错码技术和CCA2 安全加密体制,提出了基于大整数分解问题的可否认认证协议[4].在Aumann方案基础上,Deng等人提出了两个计算复杂度较小的方案[5].但是,Zhu等人发现,Deng方案在使用哈希函数嵌套运算时,自适应的攻击者可以实现可伪造的认证[6].

一般意义上的可否认认证是指接收者不能向第三方证明发送者的认证消息,即发送者可否认.从应用实际出发,一旦攻击者攻陷了发送者,发送者的内部状态完全暴露,攻击者可以利用发送者的秘密信息向第三方证明发送者和接收者之间的认证消息,导致接收者不具有可否认性.Raimondo等人基于多陷门承诺(multi-trapdoor commitments,简称MTC)解决了接收者的可否认性[7],该性质称为“前向可否认性”.

上述这些方案研究了并行可否认认证问题,但是所选用的协议安全分析模型却是独立计算模型[8].由于分析模型的局限性,协议安全性令人质疑[9].针对协议的并行安全性需求,Canetti提出了更为实际的异步并行环境通用可复合(universally composable,简称UC)安全模型[10].

如何实现UC安全的并行可否认认证,目前未见相关文献.本文研究了UC安全的可否认认证协议.在UC框架模型中,基于公共参考串模型,利用UC状态关联复合解决嵌套仿真问题,与现有的时间假设模型和公共目录假设模型方法相比,不需要限定攻击者能力.协议安全模型是分析和设计安全协议的关键.Aumann等人定义了静态攻击者能力的可否认认证协议安全模型[4].本文提出了更强攻击者能力的可否认认证协议安全模型,即自适应攻击者能力的可否认认证理想函数$F_{UC\text{-}CDA}$.

为了实现可否认认证理想函数$F_{UC\text{-}CDA}$,本文提出了一个实现可否认认证协议的新结构.该结构基于可验证平滑投影哈希函数(verifiably smooth projective Hashing,简称VSPH)[11]和非承诺加密体制(non-committing encryptions,简称NCE)[12].利用NP困难子集成员问题,VSPH通过哈希函数描述成员采样(投影哈希)和非成员采样(平滑哈希),非成员采样是可验证的.本文的研究思路基于证人不可区分[13],利用VSPH的成员采样和非承诺加密体制实现发送者的可否认,即接收者提供共享秘密信息;同时,利用VSPH的投影密钥算法和接收者提供的投影密钥,实现发送者可仿真投影密钥的内部秘密信息,保证接收者的可否认性.

1 UC安全模型框架

UC框架[9,10]为密码学协议任务的安全定义提供了精确方法.符合UC框架安全定义的协议称为通用可复合安全的.在UC框架中,协议被描述为一个交互式的概率多项式时间图灵机系统.每个交互图灵机是一种算法,用参与方P_i表示第i种算法.输入与输出纸带被模型化为算法的输入和输出,通信纸带被模型化为协议消息的发送和接收.攻击者实体被模型化为一个交互图灵机.为了描述协议并行运行的安全,UC框架模型中有一个特殊的攻击者实体“环境机Z”,它代表着外部环境Z以任意方式与攻击者及参与方交互.“环境机Z”获得的输出视图信息是协议最终的输出.

现实模型.协议执行的现实模型表示为$REAL_{\pi,A,Z}$.攻击者A与运行协议π的参与方$P_1,\ldots,P_n$共存.假定所有参与方通过点对点通信信道连接,信道是公开的,每一个参与方最初都是诚实地遵守预定的协议规则.攻击者可以在协议开始或在协议执行的任意点攻陷参与方.一旦攻击者A攻陷参与方,攻击者A将获得参与方内部的状态数据(例如秘密信息和算法的随机信息).令$REAL_{\pi,A,Z}(k,z,r)$表示当Z与攻击者A、参与方在运行协议π时的交互信息视图,其中,随机信息$r=r_Z,r_A,r_1,r_2,\ldots,r_n$.当分布空间满足$X=\{REAL_{\pi,A,Z}(k,z)\}_{k\in N,Z\in\{0,1\}^*}$时,简记为$REAL_{\pi,A,Z}$.

理想过程.协议的理想过程表示为$IDEAL_{F,S,Z}$.理想过程包括理想函数F,理想过程攻击者S(也被称为仿真

器),虚构的参与方 $p_1', p_2', ..., p_n'$.理想函数描述了协议的安全属性.虚构的参与方之间只能借助理想函数 F 在安全信道中通信,攻击者S不能阅读安全信道的内容.虚构参与方一旦得到某些输入,就将该信息传递给理想函数F,同时,理想函数F通过输出信息作出响应,攻击者S的能力与现实模型中A的能力一样.令$IDEAL_{F,S,Z}(k,z,r)$表示当Z与攻击者S、理想函数F运行时的交互信息视图,其中,随机信息$r=r_Z,r_S,r_1,r_2,\ldots,r_n$.当分布空间满足$X=\{IDEAL_{F,S,Z}(k,z)\}_{k\in N,Z\in\{0,1\}^*}$时,简记为$IDEAL_{F,S,Z}$.

区分器.在理想过程和现实模型之间存在一个区分器"环境机 Z".Z 通过提供参与方的输入,阅读参与方的输出与参与方交互,Z 也可以单独与攻击者 A 或 S 通信.可复合安全协议即协议π安全实现理想函数 F.

定义 1. 令$n\in N$,F是理想函数,π是n方协议,称π通用可复合安全实现F,若对于任何攻击者A都存在一个理想过程攻击者S,使得外部环境Z对于分布空间$IDEAL_{F,S,Z}$和分布空间$REAL_{\pi,A,Z}$是多项式时间计算不可区分的,并表示为

$$REAL_{\pi,A,Z}\stackrel{c}{=}IDEAL_{F,S,Z} \tag{1}$$

2 可否认认证协议的安全模型

如果攻击者攻陷参与方,仅仅获得参与方输入的初始秘密信息,则称为erase攻陷模型;如果攻击者可以获得参与方在协议执行过程中的所有的随机比特信息和秘密信息,则称为non-erase攻陷模型.攻击者在协议执行开始之前就攻陷了参与方,该类攻击者称为静态攻击者.攻击者在协议交互的过程中,对协议参与方的攻陷是自适应的,该类攻击者称为自适应攻击者(目前最强的攻击者模型).基于公共参考串(common reference string,简称CRS)模型[8],许多基本的协议可以满足并行UC安全定义,例如承诺协议、零知识证明协议等.CRS模型假设仿真器S已知某些可信任的参与方建立的公开参考串.基于CRS模型,本文在non-erase攻陷模型和自适应攻击者模型假设下研究UC安全的可否认认证协议.

2.1 可否认认证协议的安全目标

在对可否认认证协议的安全目标进行定义之前,先对定义的描述符号进行说明.参与方:消息认证者T和消息接收者R;消息认证码随机密钥:k_{MAC};消息认证者T需要认证的消息:m;被认证消息的认证码:$MAC(m,k_{MAC})$;消息认证者T的密钥信息:SK_T;消息认证者T的公开信息:PK_T;自适应安全的保密消息传输函数:$SMT(k_{MAC})$.

可否认认证协议的安全目标应该满足[1,4,7]:

(1) 正确性.对任何消息 m,如果认证者 T 和接收者 R 执行的协议是为了认证消息 m,那么,接收者 R 接受.

(2) 抗中间人攻击.假定认证者T想要认证多项式数量的消息$m_1,m_2,\ldots$,在这些消息可能被自适应的攻击者A选择的情况下(例如,假冒接收者 $\hat{R}$,认证者T提供预言机服务),称攻击者A成功地攻击了协议方案,若存在一个伪造者C(被A控制,并且假冒成 $\hat{T}$)成功地向接收者R认证了消息$m\notin(m_1,m_2,\ldots,)$.抗中间人攻击保证所有的概率多项式时间的攻击者 A 最多以可忽略的概率成功.

(3) 可否认性.假定攻击者A能力如上,认证者T将认证消息m,那么对每一个攻击者A,都存在一个多项式时间的可否认仿真器S_{CDA},仿真器的输出 $Sim\text{-}Trans(m,MAC(m,k_{MAC}),SMT(k_{MAC}))$ 与协议实际执行的输出 $Trans(m,MAC(m,k_{MAC}),SMT(k_{MAC}))$是不可区分的.

(4) 前向可否认性.对于可否认认证协议,认证者内部状态信息表示为$Int(m,SK_T,SMT(k_{MAC}))$,根据消息源m的认证和密钥信息SK_T存在一个多项式时间的前向可否认仿真器$S_{F\text{-}CDA}$,如果输入SK_T和$Trans(m,MAC(m,k_{MAC}),SMT(k_{MAC}))$,仿真器$S_{F\text{-}CDA}$对消息源$m$的认证存在仿真$Sim\text{-}Int(m,SK_T,SMT(k_{MAC}))$与真实的$Int(m,SK_T,SMT(k_{MAC}))$是不可区分的.

2.2 可否认认证协议的理想函数

在UC安全框架中,本文通过"理想函数$F_{UC\text{-}CDA}$"定义可否认认证协议的安全模型.形式化的可否认认证协议的理想函数$F_{UC\text{-}CDA}$如图 1 所示.基于NP问题,证人不可区分与零知识证明等价,但是与零知识证明协议相比,证人不可区分可以更好地描述并行协议和协议的复合[13].本文将抗中间人攻击转化为证人不可区分问题,通过理

想函数$F_{UC\text{-}CDA}$的 4 个阶段实现可否认认证安全目标.

Functionality $F_{UC\text{-}CDA}$

$F_{UC\text{-}CDA}$ proceeds as follows, running with parties $P_1,\ldots,P_n$ and an adversary S, and is parameterized by a security value k and a relation R_w:

Message source registration:

Upon receiving a request (*Identification*,*Sid*,PK_T) from party T, and if this is not the first message from T, then ignore this request. If yes, then record $PK_T \leftarrow \varphi \cup PK_T$, φ is empty set. do:

1. Upon receiving a witness message (w_b) from party T, then record $list\text{-}w_T \leftarrow \varphi \cup \{w_b\}$, and send (*Receipt*,*Sid*) to R and to the adversary, $b \in \{0,1\}$.
2. Upon receiving an arbitrariness message (*Identification-prover*,*Sid*,x_b) from party T, then prove $R_w(x_b,list\text{-}w)$. If $R_w(x_b,list\text{-}w)=1$,then send (*Identification-proof*,*Sid*,x_b) to R and to the adversary. If is not, then ignore all subsequent requests.

Share information secret transfers:

1. Upon receiving a message (*Send*,*Sid*,T,R,x_b,x_{1-b},$\alpha=\alpha_b||\alpha_{1-b}$), $x_b \in R_w(x_b,list\text{-}w)$, $x_{1-b} \notin R_w(x_b,list\text{-}w)$ from party R, then send (*Sid*,α) to the adversary. (α) is an assistant message.
2. Upon receiving a message (*Send*,*Sid*,R,T,k_{MAC-0},k_{MAC-1}) from party R, then record (*Sid*,k_{MAC-0},k_{MAC-1}).
3. Upon receiving a message (*Send*,*Sid*,T,R,x_b,w_b,α) from party T, if $R_w(x_b,list\text{-}w)=1$, then send (*Sid*,k_{MAC-b}) to party T.

Authentication:

1. Upon receiving a message (*Authentication*,*Sid*,m,k_{MAC-b}) from party T, if $m \in \{0,1\}^*$, and existed record (*Sid*,k_{MAC-0}, k_{MAC-1}) then send (*Sid*,m,*MAC*) to the adversary, If is not, then ignore an authentication message.
2. Upon receiving a message (*Sid*,SK_T,α) from party T and a message (*Sid*,r_β) from party R, achieve emulational information(s) as interior status information of party R, then send (*Sid*,s,α) to the adversary.

Verify:

Upon receiving a message (*MAC-verify*,*Sid*,m,*MAC*,s) from party R, do: if (T,*MAC*,s,α) is successful, then output acc=1, if is failing, then output acc=0.

Fig.1 An ideal functionality for deniable authentication, $F_{UC\text{-}CDA}$

图 1 可否认认证理想函数$F_{UC\text{-}CDA}$

消息源注册.假定消息认证者需要认证消息,为了绑定认证消息,可以通过证人不可区分协议完成证明.接收者(攻击者)提交询问信息,认证者提供证明信息,接收者接受证明.即使接收者知道两个证人,通过询问信息也不能区分认证者使用哪一个证人.一旦证人不可区分执行结束,就进入其他阶段.

共享信息保密传输."消息认证码的随机密钥"是接收方和发送方共享的秘密信息,接收方提供秘密信息并安全传输秘密信息,对于自适应攻击者,安全传输秘密信息必须为仿真器提供仿真机制.一方面,接收方的认证密钥由接收方提供,协议具有了发送方可否认仿真性质;另一方面,消息源的证人不可区分,表明没有攻击者可以获得证人区分信息.假定理想函数仅仅通过证人信息向认证者提供共享信息,一旦发送方暴露,证人信息就会暴露.由于发送方获得的共享信息来自接收方,接收方不可否认协议消息.为了解决该问题,我们作如下考虑:接收方通过引入辅助信息α实现前向可否认,认证者必须同时拥有辅助信息和证人信息才能获得理想函数提供的共享秘密信息.辅助信息与接收方内部秘密信息相关,解决接收方可否认仿真问题.辅助信息由两部分组成,$\alpha=\alpha_b||\alpha_{1-b}$,其中,$b \in \{0,1\}$,||表示串接.认证者可选择辅助信息的一部分实现接收方可否认仿真问题证明.针对辅助信息由两部分组成,本文考虑接收者提供两个秘密信息k_{MAC-0},k_{MAC-1}.传输结束后,发送者因为拥有证人信息而获得其中的一个秘密信息.

认证阶段:T通过共享秘密信息提交认证消息.同时,根据T的秘密信息SK_T和接收者R发出的随机挑战信息r_β.消息认证者T计算s,s消息与部分辅助信息α相关,是认证者T的可仿真验证信息.

验证阶段:接收者 R 验证 s 消息的可仿真性.根据共享秘密信息验证并接受发送者的消息认证.

3 协议的安全原语

本文使用VSPH和NCE作为协议基本组件.VSPH通过成员采样预防恶意的发送者同时获得接收者提供的两个秘密信息k_{MAC-0},k_{MAC-1}.由于VSPH的投影密钥算法与文本后续的证明有关,因此本文以DDH(decisional diffie-hellman assumption)假设为例说明VSPH的构造.本文的NCE基于DCR(the decisional composite

residuosity)假设[14]构造.“非承诺加密体制”除了具有基本的加密性质之外,可以为“仿真器”提供“同一明文的可仿真密文”.在基于仿真器技术的安全协议分析证明中,使用非承诺加密的目的是预防攻击者对安全消息传输的自适应攻击.该机制不提供接收者或发送者的可否认性.

3.1 VSPH

Cramer-Shoup首次定义了投影哈希函数[15].投影哈希函数有两个密钥:一个是秘密的哈希密钥k,一个是公开的投影密钥α.投影哈希函数的多元组表示为$\boldsymbol{H}=(H,K,X,L,\Pi,\beta,\alpha)$.令$\{H_k:X\to\Pi\}_{k\in K}$是以$K(\xi)$为密钥的哈希函数集合,$X$是消息集合,$\Pi$是哈希函数值的集合,$K$是哈希函数密钥集合.定义投射密钥函数$\beta:k\to\alpha$,即$\alpha=\beta(k)$,$\alpha$是投影密钥.困难子集成员问题针对每一个实例$\xi$说明了两个有限非空集合$X,W\subseteq\{0,1\}^{ploy|k|}$和一个NP关系$R\subset X\times W$,即$\xi=(X,W,R)$使得对应的语言$L=\{x:\exists w.s.t(x,w)\in R\}$是非空的.VSPH整合了投影哈希函数和可验证困难子集成员问题,强调了困难子集成员问题中的成员采样和非成员采样的可验证性.

定义 2(可验证困难子集成员问题). 称困难子集成员问题M是可验证样本,若下列条件成立:

(1) 问题可采样.存在一个概率多项式算法$P(n)$,$n=1^k$,采样得到一个实例$\xi=(X,W,R)\leftarrow I_k$.

(2) 成员可采样.存在一个输入是实例$\xi=(X,W,R)\in M$的概率多项式算法,输出是$x_0\in L$和$w\in W$,使得x_0的分布是L统计可忽略的均匀分布.

(3) 非成员可采样.存在一个输入是实例$\xi=(X,W,R)\in M$和元素$x_0\in X$的概率多项式算法NO-M,输出$x_1=NO\text{-}M(\xi,x_0)$,使得:如果$x_0\in_R L$,那么x_1的分布是$Y\subseteq X-L$统计可忽略的均匀分布;如果$x_0\in_R X$,那么x_1的分布是X统计可忽略的均匀分布.

(4) 非成员可验证.存在一个输入是任意的三元组(ξ,x_0,x_1)的概率多项式算法YV,可验证存在比特$b\in(0,1)$使得$x_{1-b}\in Y\subseteq X-L$,即

(a) 如果$x_0\notin Y$且$x_1\notin Y$成立,那么$YV(\xi,x_0,x_1)=0$;

(b) 存在比特b,如果$x_b\in L,x_{1-b}\in NO\text{-}M(\xi,x_0)$,那么$YV(\xi,x_0,x_1)=1$.

定义 3(投影哈希函数). 称(H,K,Π,α,β)是困难子集成员问题M的投影哈希函数,若对每个实例$\xi\in M$存在一个函数f,使得每一个$x\in L(\xi)$和每一个$k\in K(\xi)$,$\alpha=\beta(k)$,有$f(x;\beta(k),w)=H_k(x)$.

定义 4(非成员平滑投影哈希函数). 称(H,K,Π,α,β)是困难子集成员问题M的非成员平滑投影哈希函数,若对每个实例$\xi=(X,W,R)$和$x_{1-b}\in Y$,其中当$Y\subseteq X-L$时,$(\beta(k_{1-b}),H_k(x_{1-b}))$和$(\beta(k_{1-b}),\Pi\leftarrow\{0,1\}^k)$是不可区分的.

基于DDH假设的VSPH(DDH-VSPH)[11]:

(1) 成员可采样.随机选择(u,v),令$U=g^u,V=g^v,x_0=g^{uv}\in L(\xi)$.这里,$w=u$是证人.

(2) 非成员可采样.随机选择$z\in_R Z_{qk},z\neq uv,x_1=g^z$,即$x_1\in X(\xi)-L(\xi)$.

(3) 非成员可验证.$(x_0/x_1)\neq 1$.

(4) 成员采样投影哈希的有效性.假定投影密钥$\alpha=\beta(k,r)=V^k g^r$,哈希函数$H_k(x_0)=x^k U^r$.

$$H_k(x_0)=x_0^k U^r=(g^{uv})^k U^r=(g^{uv})^k(g^u)^r=(g^{vk})^u(g^r)^u=(V^k g^r)^u=\beta(k,r)^u.$$

3.2 非承诺加密体制

非承诺加密(NCE)由 5 个概率多项式时间算法组成,简记为$(G;E;D;F;R)$.为了提高协议参与方的计算效率,文献[16]证明了 DCR 假设构造的 NCE 可以处理指数空间的消息(string),而 DDH 假设的 NCE 仅能处理多项式空间消息(bit),对带宽而言,协议效率更高.本文使用非承诺加密的密文将执行⊕(与或)运算,所以使用 DCR 假设构造安全原语(基于 DCR 假设的 NCE 的构造见文献[16]).

随机密钥生成算法$G:(pk;sk;z_D)\leftarrow G(1^k)$,$k$是安全参数,$z_D$是辅助信息,$(pk;sk)$是密钥对.

随机加密算法$E:c\leftarrow E(pk;m,r_E)$,$m$是明文,$c$是密文,$r_E$是随机数.

解密算法$D:m\leftarrow D(sk;E(pk;m,r_E))=D(sk;c)$.

虚拟加密算法$F:c'\leftarrow F(pk;sk;z_D;r_F)$,$c'$是虚拟密文.

虚拟密钥生成算法$R:sk'\leftarrow R(pk;sk;z_D;c';m;r_R)$,$sk'$是虚拟密钥.使用$sk'$可以解密$c'$得到明文$m$.

4 并行可否认认证协议

根据可验证平滑投影哈希函数的定义和性质,本文通过VSPH实现证人不可区分和秘密信息传输.基本思路是:发送者进行采样,接收者获得发送者提供的采样信息(x_0,x_1)之后,随机选择哈希函数的密钥信息,生成非成员哈希函数值和成员哈希函数值;然后,接收者随机选择信息(k_{MAC-0},k_{MAC-1}),通过非承诺加密生成密文(c_0,c_1),由于哈希函数的随机分布和单向性,将哈希值与密文通过⊕运算生成随机消息.

发送者拥有证人信息、投影密钥和成员采样信息,可以通过证人信息和接收者提供的投影密钥($F_{UC\text{-}CDA}$定义的辅助信息α)获得加密信息$E(pk_T;k_{MAC-b},r_E)$.另外,接收者随机选择哈希函数的密钥信息,利用投影密钥算法β计算投影密钥(α_b,α_{1-b}).如果投影密钥算法具有陷门承诺的性质,一旦接收者提交投影密钥,发送者就可以根据成员采样算法的秘密信息进行投影密钥的内部状态仿真.

非成员采样是可验证的.本协议方案不需要假定发送者是诚实的,如果是不诚实采样,那么接收者R可以通过验证算法拒绝协议执行.在协议的建立阶段,发送方采样算法中的保密信息为$SK(u,v,z)$,公开信息为$PK(U,V,g,x_0,x_1,m)$.另外,发送方使用NCE体制需要生成$(pk;sk;z_D)\leftarrow G(1^k)$,$k$是安全参数,$z_D$是辅助信息,$(pk;sk)$是密钥对.协议的实现方案如图 2 所示,其中,可验证平滑投影哈希函数基于DDH假设构造.

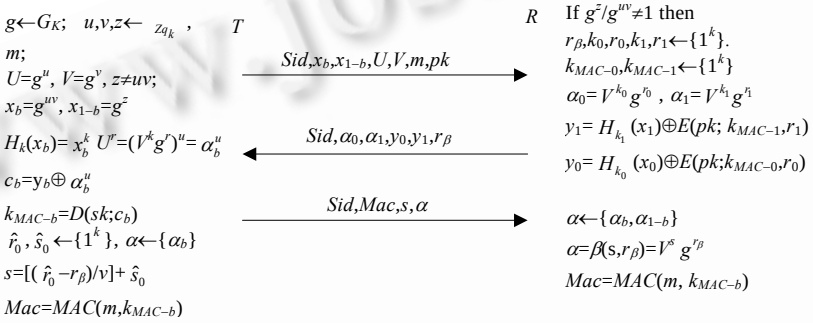

Fig.2 UC security deniable authentication protocols

图 2 UC 安全的可否认认证协议

UC-CDA 协议的说明:

1. $T\rightarrow R$:发送者T选择X,L,构成基于困难问题的采样.随机产生三元组(x_b,x_{1-b},w_b),其中

$$x_b\in_R L,(x_b,w_b)\in_R R,x_{1-b}\in_R X-L.$$

保留证人w_b.x_{1-b}由非子集成员算法$NO\text{-}M(\xi,x_b,z)$产生.使用NCE体制生成$(pk;sk;z_D)\leftarrow G(1^k)$,向$R$发送$(Sid,x_b,x_{1-b},U,V,m,pk)$,$Sid$是UC-CDA协议并行异步运行时一个协议实例的会话标识.

2. $R\rightarrow T$:根据接收到的消息(Sid,x_0,x_1,U,V,m,pk),接收者R执行非成员可验证算法$YV(\cdot)$.如果$YV(\cdot)=0$,则协议终止;如果$YV(\cdot)=1$,则选择两个不同的随机哈希函数密钥(k_0,k_1).计算$(H_{k_0}(x_b),H_{k_1}(x_{1-b}))$,执行投影密钥算法$\beta(k,r)$,获得投影密钥$(\alpha_0,\alpha_1)$.接收者$R$随机选择信息$(k_{MAC-0},k_{MAC-1})$,通过非承诺加密生成密文$(c_0,c_1)$,计算随机消息$y_0=H_{k_0}(x_b)\oplus c_0$, $y_1=H_{k_1}(x_{1-b})\oplus c_1$,向$T$发送$(Sid,\alpha_0,\alpha_1,y_0,y_1,r_\beta)$.这里,共享信息$k_{MAC-b}\leftarrow\{k_{MAC-0},k_{MAC-1}\}$为可否认认证协议的"消息认证码随机密钥",$r_\beta$为投影密钥的可否认挑战信息.

3. $T\rightarrow R$:已知证人w_b和投影密钥α_b,计算$H_{k_b}(x_b)=f(x_b,\alpha_b,w_b)$,$c_b=y_b\oplus f(x_b,\alpha_b,w_b)$.获得$k_{MAC-b}=D(sk;c_b)$.根据挑战信息$r_\beta$和具有陷门承诺性质的投影密钥算法$\beta(k,r)$,通过投影密钥$\alpha_b$,计算发送者内部可仿真状态信息$s$.最后计算认证消息的消息认证码$Mac=MAC(m,k_{MAC-b})$.向$R$发送$(Sid,s,\alpha_b,Mac)$.

4. R: 验证$\alpha\leftarrow\{\alpha_b,\alpha_{1-b}\}$,$\alpha=\beta(s,r_\beta)$是否成立,如果成立,由于$R$知道$k_{MAC-b}\leftarrow\{k_{MAC-0},k_{MAC-1}\}$,则验证$Mac=MAC(m,k_{MAC-b})$是否成立.

5 UC-CDA 的安全性分析

根据理想函数$F_{UC\text{-}CDA}$的定义,在进行UC-CDA协议的安全性分析之前,我们先证明两个引理.

引理 1. 可验证平滑投影哈希函数的投影密钥算法是陷门承诺安全的,对于自适应攻击者,UC-CDA协议安全实现了理想函数$F_{UC\text{-}CDA}$的前向可否认性.

证明:接收者利用保密信息$\{k_b,k_{1-b}\}$提交投影密钥之后,发送者根据投影密钥$\{\alpha_b,\alpha_{1-b}\}$和成员采样证人信息$w_b$可以获得投影哈希函数值$H_{k_b}(x_b)=f(x_b,\alpha_b,w_b)$并最终获得$k_{MAC-b}\leftarrow\{k_{MAC-0},k_{MAC-1}\}$.在协议执行结束后,接收者希望对投影密钥$\{\alpha_b,\alpha_{1-b}\}$的保密信息$\{k_b,k_{1-b}\}$可否认,即投影密钥算法$\beta(k,r)=V^k g^r$应该提供可仿真机制.由于发送者已知投影密钥算法中$V$的秘密信息$v$,不失一般性,假定随机选择$(k_b,r_b)$和任意一个$r_\beta$,$V^{k_b}g^{r_b}=V^s g^{r_\beta}$,根据陷门承诺的性质,有$vs+r_\beta=vk_b+r_b$,可以很容易地得到$s=[(r_b-r_\beta)/v]+k_b$.自适应攻击者攻陷发送者获得投影密钥$\{\alpha_b,\alpha_{1-b}\}$,由于投影密钥可由发送者提供的$(s,r_\beta)$验证,对接收者提供的$(k_b,r_b)$可以仿真,因此攻击者不能向第三方证明投影密钥与接收者相关,即前向可否认性成立. □

引理 2. 基于CRS模型,可验证平滑投影哈希函数是安全的,对于自适应攻击者,UC-CDA协议安全实现了理想函数$F_{UC\text{-}CDA}$的共享信息传输.

证明:首先建立各种仿真情景,其次证明 $REAL_{\pi,A,Z}\overset{c}{=}IDEAL_{F,S,Z}$.

令A是自适应攻击者,在现实模型中,与运行UC-CDA协议的参与方交互.现在构造一个理想过程中的攻击者S(称为仿真器S).在理想过程中,S可以与理想函数$F_{UC\text{-}CDA}$及环境机Z交互.S因A的副本 $\tilde{A}$ 调用而工作,副本 $\tilde{A}$ 与现实模型中的A交互.对于仿真器S,在理想过程中的交互称为仿真器S的外部交互,与A的副本 $\tilde{A}$ 之间的交互称为仿真器S的内部交互.基于CRS模型,仿真器S已知接收方的随机哈希函数密钥(k_0,k_1)和发送方NCE的私钥sk.

仿真器 S 的工作情况如下:

(1) 协议开始,仿真 R 被攻陷,T 被攻陷的情况

仿真器 S 获得 $\tilde{A}$ 提供的参与方真实协议消息,仿真器 S 使用真实协议消息仿真.

(2) 仿真 R 未被攻陷,T 未被攻陷的情况

在理想过程中,仿真器S获得(Sid),然后终止.对于现实模型中的发送者T和接收者R的仿真通过协议规程完成.仿真器S模拟虚拟的发送者T提供(b).模拟虚拟的接收方R接收数据(x_0,x_1),验证数据的非成员采样;基于CRS模型,仿真器S选择(k_0,k_1),计算 $H_{k_b}(x_b)$并利用投影密钥算法$\beta(\cdot)$生成投影密钥(α_0,α_1);基于CRS模型,仿真器S利用密钥生成算法G:$(pk;sk;z_D)\leftarrow G(1^k)$,获得辅助信息$z_D$,密钥对$(pk,sk)$,同时利用虚拟加密算法$F$:$c'\leftarrow F(pk;sk;z_D;r_F)$生成虚拟密文 c'_b. 另外,随机选择 $c'_{1-b}\leftarrow\{0,1\}^{|m|}$;计算$y_b\leftarrow c'_b\oplus H_{k_b}(x_b)$,随机选择$y_{1-b}\leftarrow\{0,1\}^{|m|}$,并发送$\{y_0,y_1,\beta(k_0),\beta(k_1)\}$.由于两个参与方都没有被攻陷,所以仿真器$S$仿真的消息$(x_0,x_1)$,$\{y_0,y_1,\beta(k_0),\beta(k_1))\}$,$(b)$都是随机分布的,同时被仿真的接收方$R$的内部数据,例如虚拟加密算法$F$使用的加密随机参数$(r_F)$是随机分布的.

(3) 仿真 R 未被攻陷,T 开始被攻陷的情况

仿真器S在内部交互的仿真过程中,通过 $\tilde{A}$ 获得真实T(A攻陷T)提供的消息(x_1,x_0).仿真器S在外部交互模仿T($\tilde{A}$ 将w_b提供给仿真器S)向理想函数$F_{UC\text{-}CDA}$提供(b)并获得从$F_{UC\text{-}CDA}$发向虚拟T的消息(k_{MAC-b})(见图 1, $F_{UC\text{-}CDA}$ 理想函数中共享信息秘密传输的第 3 条说明).这时,仿真器S在内部交互的仿真过程中模仿R,根据获得的真实的k_{MAC-b},基于CRS模型,利用加密算法E:$c_b\leftarrow E(pk;k_{MAC-b},r_E)$,生成$c_b$,随机选择$c_{1-b}\leftarrow\{0,1\}^{|m|}$;计算$y_b\leftarrow c_b\oplus H_{k_b}(x_b)$, 随机选择$y_{1-b}\leftarrow\{0,1\}^{|m|}$,并发送$\{y_0,y_1,\beta(k_0),\beta(k_1)\}$.被仿真的$R$的内部数据,例如随机加密算法$E$使用的加密随机参数$(r_E)$是随机分布的.

(4) 仿真R给理想函数发送秘密消息(k_{MAC-0},k_{MAC-1})之前,攻击者A攻陷R,T未被攻陷的情况

仿真器S在内部交互的仿真过程中, $\tilde{A}$ 将(k_{MAC-0},k_{MAC-1})提供给仿真器S.由于仿真器S获得了被攻陷R提供的(k_{MAC-0},k_{MAC-1})(见图 1,$F_{UC\text{-}CDA}$理想函数中共享信息传输的第 2 条说明).那么,仿真器S在内部交互仿真过程中模

仿R使用加密算法E:$c\leftarrow E(pk;m;r)$和真实的(k_{MAC-0},k_{MAC-1})产生消息(c_1,c_0)及(y_1,y_0).

(5) 仿真R发送消息(y_0,y_1)之后,T和R被攻陷的情况

攻击者A此时获得真实的(k_{MAC-0},k_{MAC-1})信息并通过已知证人w_b和投影密钥$\beta(k_b)$,函数$c_b=y_b\oplus f(x_b;\beta(k_b),b)$恢复$c_b$.同时,仿真器$S$在交互外部获得了被攻陷$R$提供的$(k_{MAC-0},k_{MAC-1})$和被攻陷$T$提供的$b$,利用虚拟密钥生成算法$R$:$sk'\leftarrow R(pk;sk;z_D;c';m;r_R)$生成虚拟密钥$sk'_b$.此时,在内部交互的仿真过程中假定攻击者$A$要求验证仿真器$S$仿真的消息$k_{MAC-b}$是否一致,仿真器$S$将虚拟密钥$sk'_b$提供给攻击者$A$,$A$使用虚拟密钥$sk'_b$解密仿真的虚拟密文$c'_b$,即$D$:$k_{MAC-b}\leftarrow D(sk'_b;c'_b)$.判定仿真器提供的$k_{MAC-b}$与真实的$k_{MAC-b}$信息是否一致.

仿真器S通过5个具体的实现策略仿真了协议共享信息传输和证人不可区分验证的全部状态.

$REAL_{\pi,A,Z}\stackrel{c}{=}IDEAL_{F,S,Z}$的证明.由于$Z$和$A$及协议参与方交互获得的信息视图与理想过程中$Z$和$S$及在内部交互中副本$\tilde{A}$的信息视图等价,$Z$的信息视图的不可区分性证明转化为仿真器$S$的内部交互仿真与外部交互仿真的不可区分.由于参与方在协议开始都被攻陷和都未被攻陷的计算不可区分是直接的,因此本文仅需证明单方被攻陷和共享信息传输结束后两方被攻陷的不可区分.仿真器S内部交互仿真与外部交互仿真的不可区分性最终归约为可验证平滑投影哈希函数的安全性.

R被攻陷的仿真是不可区分的.假定接收者R被攻陷,攻击者A控制接收者R,攻击者A获得发送者T的证人w_b是可忽略的.

反证法.假设存在一个不可忽略的概率多项式攻击算法B预知w'_b.攻击者B可以通过预知w'_b进而区分$x\in_R L$和$x\in_R X$,这将破坏困难子集成员问题M的定义.

假定一个实例$\xi_k(X,W,R)\leftarrow I_k$和一个元素$x\in X$.

(1) 随机选择b,令$x_b=x$.

(2) 利用算法$NO\text{-}M(\cdot)$产生x_{1-b}.

(3) 将(x_0,x_1)发给攻击者B,并获得攻击者B预知的w'_b.

(4) 如果$w'_b=w_b$,则表明攻击者B预知$x\in_R L$.如果$w'_b\neq w_b$,则表明攻击者B预知$x\in_R X$.一方面,如果预知$x_b\in_R L$,那么存在一个不可忽略的概率多项式攻击者B预知w_b,与本文定义2矛盾;另一方面,如果$x_b\in_R X$,则$x_{1-b}\in_R X$,对于这种情况,w_b是不可预知的(信息论已有理论).既然不存在不可忽略的概率多项式攻击者B,那么,也不可能存在同样能力的攻击者A和Z.

T被攻陷的仿真是不可区分的.假定发送者T被攻陷,攻击者A控制发送者T,非成员平滑投影哈希函数的性质保证发送者T只能获得(k_{MAC-0},k_{MAC-1})中的一个.攻击者A对随机分布的密文信息的可区分是可忽略的.

关于(y_0,y_1)的随机均匀分布.R产生的$y_b\leftarrow c_b\oplus H_{k_b}(x_b)$,$y_{1-b}\leftarrow\{0,1\}^{|m|}$)是不可区分的(由仿真器$S$仿真).根据非成员采样,必存在$x_0\in Y$或$x_1\in Y$,否则,协议终止.对于$b\in\{0,1\}$.不失一般性,假定$x_{1-b}\in Y$,那么根据非成员平滑投影哈希函数的性质(见定义4),$[\beta(k_b),H_{k_b}(x_b)]$和$(\beta(k_{1-b}),r\leftarrow\{0,1\}^{|m|})$是不可区分的,从而$[\beta(k_b),c_b\oplus H_{k_b}(x_b)]$与$[\beta(k_{b-1}),r\leftarrow\{0,1\}^{|m|}]$是均匀分布的.

关于(c_0,c_1)的随机均匀分布.在仿真场景(1)中,仿真器S提供的$c'_b\leftarrow F(pk;sk;z_D;r_F)$,$c'_{1-b}\leftarrow\{0,1\}^{|m|}$.在仿真场景(2)中,仿真器$S$提供的$c_b=E(pk;k_{MAC-b},r_E)$,$c_{1-b}\leftarrow\{0,1\}^{|m|}$.根据非承诺加密体制的性质:可以为“仿真器”提供“同一明文的可仿真密文”,因此,c_b和c'_b是不可区分的.

基于non-erase模型的仿真是不可区分的.仿真器S在仿真过程中需要仿真参与方的随机信息并写入随机纸带,随机信息是参与方的内部数据.例如,加密算法E的随机信息(r_E)、虚拟密钥生成算法R的随机信息(r_R)、虚拟加密算法F的随机信息(r_F).本协议的随机信息是由非承诺加密体制的安全性保证不可区分性.另外,在仿真场景(4)中,攻击者A获得了协议参与方的数据(k_{MAC-b}),仿真器S有能力通过提供虚拟密钥sk'_b,使得被仿真的现实模型中攻击者A具有与被攻陷的参与方一致的内部状态信息. □

定理. 基于CRS模型,VSPH和NCE是安全而有效的,对于自适应的攻击者,可否认认证协议UC-CDA安全实现理想函数$F_{UC\text{-}CDA}$.

证明:首先证明正确性、抗中间人攻击、协议可否认性,然后证明协议是UC安全的.

正确性:根据协议规则,协议实施了认证方对消息 m 的认证,正确性成立.

抗中间人攻击:

(1) 根据VSPH的构造,成员采样和非成员采样的证人信息是不可区分的.根据引理2,攻击者试图获得证人的消息是可忽略的,认证方获得共享秘密.如果存在攻击者区分证人消息,则破坏困难子集成员问题 M 的定义.

(2) 根据VSPH的投影密钥算法$\alpha=\beta(k,r)=V^k g^r$.如果存在攻击者获得$v$,则与引理 1 矛盾,同时,VSPH是不安全的.

(3) 接收方通过共享秘密验证消息认证.

可否认性:

(1) 根据引理 1,接收者R提供了投影密钥信息,发送方获得共享信息(k_{MAC-b}),同时,投影密钥通过发送者的秘密信息可仿真,接收者是可否认的(前向可否认性).

(2) 根据引理 2,接收者R向发送者T提供共享信息(k_{MAC-b}),发送者使用共享信息(k_{MAC-b})进行消息认证,发送者是可否认的.协议安全实现了完全的可否认性.

协议是自适应的攻击者 UC 安全的:仿真器 S 对协议作高层仿真,详细细节与引理 2 证明相似.

发送方被攻陷.仿真器获得发送方秘密信息和公开信息,根据引理 2,接收者的密文 c 可仿真.根据引理 1,接收者提供的投影密钥可仿真.其他随机信息是均匀分布的.

接收方被攻陷.仿真器获得接收方秘密信息,根据引理 2,发送者对共享信息(k_{MAC-b})可仿真.

仿真器 S 内部交互仿真与外部交互仿真的不可区分性由引理 1 和引理 2 可知成立. □

6 相关工作比较

并行可否认认证方案的研究主要关注了如下 4 点:

(1) 协议的可证明安全性.例如,可否认认证协议的形式化安全模型,协议的安全性分析是否为可证明的,协议的攻击者能力模型如何.

(2) 协议的结构和相关的基本安全原语.

(3) 协议的通信效率,例如协议执行一次的交互次数和协议的通信复杂度.

(4) 协议的计算效率.例如,协议参与方在执行过程中使用模指数运算的规模.表 1 为本文方案与其他代表性方案的比较.

Table 1 Comparison between the different schemes for concurrent deniable authentication

表 1 不同的并行可否认认证方案比较

	Dowork, *et al.*'s	Aumann and Rabin's	Deng, *et al.*'s	Raimondo, *et al.*'s	Our's
Setup assumptive	A timing constraint	Public directory	Public directory	A timing constraint	Common reference string
Constitution	CCA+ZK	CCA+ZK	CCA+ZK	MTC+ZK	VSPH+NCE+WI
Security model	Sequence concurrent	Stand-Alone	Stand-Alone	BCK security	UC security
Adversaries model	Static+erase	Static+erase	Static+erase	Static+non-erase	Adaptive+non-erase
Complexity of communication	$O(2m/3)$	$O(m)$	$O(t)$	$O(m/c)$	$O(1)$
Complexity of computation	$2m\|NIZK\|/3+E+D$	$4m$	$(3+E+D)/4s$	$(\|MTC\|+2\|ZK\|)/m$	$(6+2\|NCE\|+\|NCD\|)/m$
Interactive	4	3	3	4	3
Forward deniable	Yes, not prove	No	No	Yes, prove	Yes, prove

现有方案的安全建立假设分别为时间定时、公共目录.本文基于CSR模型,利用VSPH和NCE提出了WI-based的新结构,不同于CCA-based和MTC-based的结构.Raimondo方案的安全证明使用BCK(Bellare-Canetti-Krawzyk)分析模型[17],严格地说,BCK模型仍然是一个独立计算分析模型.从攻击者能力模型角度分析,本文假定的攻击者能力最强.对于前向可否认性,CCA-based方案无法实现可证明安全,Raimondo方案需要假定发送者是诚实的,本文根据VPSH的性质,不需要对此加以限制.

假定协议认证消息的长度为$|m|$,Aumann 和 Rabin 方案是按 1-bit 位可否认认证的,通信复杂度为 $O(m)$,Deng 方案是将认证消息分为 t 块,每块处理 s-bit 位,通信复杂度为 $O(t)$.Raimondo 方案可否认认证的消息 bit 位与多陷门承诺(MTC)的通信复杂度相关,假定 MTC 的处理空间为 c-bit 位,那么通信复杂度为 $O(m/c)$.Dowork 方案和本文方案都使用了接受者提供的共享秘密信息,但是,Dowork 方案为了实现并行的不可伪造性证明,执行了 $2m/3$ 次的非交互零知识证明(non-interactive zero-knowledge,简称 NIZK),通信复杂度为 $O(2m/3)$.本文方案为了实现高通信效率,利用 VSPH,NCE 实现了并行的不经意共享秘密信息传输,通信复杂度改善为 $O(1)$.

以 Aumann 和 Rabin 方案的 1-bit 位计算复杂性为基准,假定一次模指数计算为单位 1,那么,该协议处理 $|m|$-bit 的计算复杂性为 $4m$.令零知识证明的复杂性为$|ZK|$(例如 Deng 方案$|ZK|=3$);CCA2 公钥加密复杂性为$|E|$,解密复杂性为$|D|$(例如,文献[15]的$|E|=5$,$|D|=3$);多陷门承诺协议复杂性为$|MTC|$(由于实现构造 MTC 方案的安全原语不同,MPC 的复杂性存在差异,本文以变量方式表达).不同方案的比较的计算复杂性见表 1.本文的 UC 安全模型为协议并行运行的复杂性提供了协议参与方线性相关的功能,不同于其他方案并行运行的会话数线性相关复杂性,为协议实现提供了简单而有效的方法.

7 结 论

本文研究了UC安全的并行可否认认证协议,形式化地定义了并行可否认认证协议安全模型:UC框架的理想函数$F_{UC\text{-}CDA}$,同时,基于可验证平滑投影哈希函数和非承诺加密体制构造了一类新的并行可否认认证协议结构.在公共参考串模型中,新方案具备前向可否认性,是自适应攻击者通用可复合安全的.该协议能够防止中间人攻击,这在电子选举和网上谈判等系统中可以保证公平性和安全性.

References:

[1] Dwork C, Naor M, Sahai A. Concurrent zero-knowledge. In: Vitter J, ed. Proc. of the 13th Annual ACM Symp. on Theory of Computing. New York: ACM Press, 1998. 409−418.

[2] Xu CX, Fan L, Li JH. Deniable authentication protocol based on diffie-hellman algorithm. Computer Engineering, 2002,28(10): 145−146 (in Chinese with English abstract).

[3] Cao TJ, Lin DD, Xue R. An efficient ID-based deniable authentication protocol from pairings. In: Proc. of the 19th Int'l Conf. on Advanced Information Networking and Applications, Vol.1. IEEE Press, 2005. 388−391.

[4] Aumann Y, Authentication MR. Enhanced security and error correcting codes (extended abstract). In: Proc. of the 18th Annual Int'l Cryptology Conf. on Advances in Cryptology. London: Springer-Verlag, 1998. 299−303.

[5] Deng X, Lee CH, Zhu H. Deniable authentication protocols. IEE Proc.-Computers Digital Techniques, 2001,148(2):101−104.

[6] Zhu RW, Wong DS, Lee CH. Cryptanalysis of a suite of deniable authentication protocols. IEEE Communications Letters, 2006, 10(6): 504−506.

[7] Raimondo MD, Gennaro R. New approaches for deniable authentication. In: Proc. of the 12th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2005. 112−121.

[8] Goldreich O, Micali S, Wigderson A. How to play any mental game or a completeness theorem for protocols with honest majority. In: Proc. of the 19th Annual ACM Conf. on Theory of Computing. New York: ACM Press, 1987. 218−229.

[9] Canetti R, Lindell Y, Ostrovsky R, Sahai A. Universally composable two-party and multi-party secure computation. In: Proc. of the 34th ACM Symp. on the Theory of Computing. Quebec: ACM Press, 2002. 494−503.

[10] Canetti R. Universally composable security: A new paradigm for cryptographic protocols. In: Proc. of the 42nd IEEE Symp. on the FOCS. New York: IEEE Computer Society Press, 2001. 136−145.

[11] Kalai YT. Smooth projective hashing and two-message oblivious transfer. In: Advances in Cryptology, Eurocrypt 2005. LNCS 3494, Berlin: Springer-Verlag, 2005. 78−96.

[12] Damgard I, Nielsen JB. Improved non-committing encryption schemes based on general complexity assumptions. In: Proc. of the CRYPTO 2000. LNCS 1880, Berlin: Springer-Verlag, 2000. 432−450.

[13] Feige U, Shamir A. Witness indistinguishable and witness hiding protocols. In: Proc. of the 22nd ACM Symp. on the Theory of Computing. Baltimore: ACM Press, 1990. 416–426.

[14] Paillier P. Public-Key cryptosystems based on composite-degree residuosity classes. In: Advances in Cryptology, Eurocrypt'99. LNCS 1592, Berlin: Springer-Verlag, 1999. 223–238.

[15] Cramer R, Shoup V. Universal Hash proofs and a paradigm for adaptive chosen cipher text secure public-key encryption. In: Advances in Cryptology, Eurocrypt 2002. LNCS 2332, Berlin: Springer-Verlag, 2002. 45–64.

[16] Canetti R, Halevi S, Katz J. Adaptively-Secure, non-interactive public-key encryption. http://eprint.iacr.org/2004/317.pdf

[17] Bellare M, Canetti R, Krawzyk H. A modular approach to the design and analysis of authentication and key exchange protocols. In: Proc. of the 30th Symp. on Theory of Computing. Dallas: ACM Press, 1998. 419–428.

附中文参考文献:

[2] 许崇祥,范磊,李建华.基于 Diffie-Hellman 算法的可否认认证协议.计算机工程,2002,28(10):145–146.

冯涛(1970－),男,甘肃临洮人,博士生,研究员,主要研究领域为安全协议复合理论,无线传感器网络安全.

马建峰(1963－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为计算机安全,密码学,移动与无线网络安全.

* *

第 3 届中国可信计算与信息安全学术会议

征 文 通 知

为了加强我国可信计算和信息安全领域学术、技术交流，促进我国可信计算和信息安全领域的学术繁荣、技术进步和产业发展，由解放军密码管理局和中国计算机学会容错专业委员会主办，中国人民解放军信息工程大学电子技术学院承办的“第三届中国可信计算与信息安全学术会议”拟于 2008 年 10 月 25 日－28 日在河南郑州举行。会议将邀请本领域的专家作专题报告，将邀请研究人员、企业代表等，针对可信计算与信息安全领域的关键技术和热点问题进行交流和研讨。欢迎各位专家、研究开发及工程技术人员、及该领域的企事业人士踊跃投稿并参加会议。

一、征文范围

会议重点征集可信计算与信息安全理论和技术方面的研究论文。具体包括（但不限于）：可信计算体系结构：可信计算理论，信任理论，可信计算平台体系结构，可信计算软件体系结构，可信网格，容错计算；可信软件：高可信软件，操作系统安全，数据库安全，软件容错，软件测试；可信硬件：可信计算平台，可信计算平台模块，信息安全芯片，智能卡，硬件容错，硬件测试，电子设备的物理安全；（4）网络与通信安全：可信网络，网络安全技术，网络协议安全，网络容侵与容灾，通信安全，无线通信网络安全，计算机病毒技术；（5）密码学：密码学的理论与技术，新型密码，密码应用技术；（6）信息隐藏：信息隐藏，数字水印，数字版权管理；（7）信息安全应用：电子政务安全，电子商务安全，可信计算与信息安全的应用，信息安全管理。

二、征文要求

本次会议投稿一律通过会议网站 http://www.tc2008.org 的投稿系统进行。论文必须为未公开发表且未向学术刊物和其他学术会议投稿的最新研究成果，文稿使用中文或英文书写，字数一般不超过 6000。录用的英文稿件将在《武汉大学学报（英文版）》上发表，录用的中文稿件在核心期刊《武汉大学学报》（正刊）发表。

三、重要日期

征文截止：2008 年 4 月 30 日　录用通知：2008 年 6 月 1 日　返回修改稿：2008 年 6 月 20 日　定稿：2008 年 7 月 1 日

四、会议通讯方式

联系地址：河南郑州商城东路 12 号信息工程大学电子技术学院信息安全研究所

邮政编码：450004

联系人：李立新，周雁舟

E-mail：tc2008_zz@163.com
电话：0371-63538081，0371-66094401