普适安全的基于身份的签名机制

王 竹[1],戴一奇[1],叶顶锋[2]
(1.清华大学计算机科学与技术系,北京 100084;2.中国科学院研究生院信息安全国家重点实验室,北京 100049)

摘 要: 理想功能是 UC 安全协议的基本单元和核心内容.在 UC 安全框架下协议设计的首要步骤就是要将协议所希望完成的功能抽象为一个"理想功能","理想功能"的合理定义不仅要从定义上保证安全,更重要的是要兼顾其可实现性.本文定义了基于身份的签名机制(IBS)在 UC 安全框架下对应的理想功能 F_{IBS},证明了其可实现性以及 UC 安全的 IBS 与经典 IBS 安全定义 EUF-CMIA 安全之间的等价关系,保证了在构造复杂环境下 UC 安全协议的时候,EUF-CMIA 安全的 IBS 可以作为一个模块被安全调用.

关键词: 普适安全;理想功能;基于身份的签名机制;抗选择性消息和身份攻击
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2011) 07-1613-05

Universally Composable Identity-Based Signature

WANG Zhu[1], DAI Yi-qi[1], YE Ding-feng[2]
(1. *Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*;
2. *Graduate University of the Chinese Academy of Sciences, State Key Laboratory of Information Security, Beijing* 100049, *China*)

Abstract: Idea Functionality is the core and basic unit of Universally Composable (UC) security protocols. The first step of designing the protocols, within the UCsecurity framework, is to extract an ideal functionality from the expected functionalities of the protocols. To appropriately define an ideal functionality we should not only protect the security of the definition, but also consider the realizability. This study investigates the security of identity-based signature (IBS) within the UCframework, defines a realizable identity-based signature functionality F_{IBS}, proves that UC-secure IBS is equivalent to conventionally-secure (EUF-CMIA -secure) IBS. As a result, we are able to make sure that the EUF-CMIA scheme can be a module in designing a complex protocol that satisfies the UCrequirement.

Key words: universally composable (UC) security; ideal functionality; identity-based signature (IBS); existential unforgery for adaptive chose-message and identity attack (EUF-CMIA)

1 引言

安全性是密码协议研究的重要问题.从最初的经验性(无定义)到形式化方法,对协议安全的考虑也从协议单独运行的情形扩展到在复杂环境中运行的情形[1].解决复杂环境中问题的方法之一就是针对具体的环境定义具体的安全.这样的结果就是使得定义更加复杂也局限了使用范围(因其只是针对某一环境而定义).另外一种方法就是独立定义而保证其具有普遍适应性,使得它在任意环境下都可以确保安全.显然,后一种方式更具优越性,是目前协议安全性研究的主流.

普适安全(Universally Composable Security,以下简称 UC 安全)是 2001 年由 Canetti 提出的安全协议概念[2].它最大的特点就是满足协议模块化设计的要求,可以单独设计协议,只要协议满足 UC 安全,那么在普适性定理的保障下就可以在任何环境下保持其安全特性.设计 UC 安全协议的首要步骤和核心内容就是要将协议所希望完成的功能抽象为一个理想功能(Ideal Functionality).理想功能是一个协议各方可以以规定的接口访问的 Oracle,相当于现实世界中一个不可攻陷的可信第三方.可以想象的是,对现实中的参与者而言,要"安全地"合作完成某项分布式计算任务,如果有"理想功能"的帮助,事情是就会变得简单,而这样的理想功能如何定义也是容易的.问题是如果任意定义这样的理想功能,虽然能完成协议规定的任务,却不能保证该"理想功能"能被现实协议实现.一般来说,能被现实协议实现的理想功能都需要对"理想敌手"做恰当的让步:把一些在现实世界中无法避免的安全"隐患"明确规定为"理想敌手"的破坏能力.这是通过在"理想功能"与"理想敌手"之间定义适当的接口来实现的.正因为如此,"理想功能"

收稿日期:2010-05-07;修回日期:2010-09-20
基金项目:国家 863 高技术研究发展计划(No.2006AA01Z420)

的定义一般都不是平凡的任务.

目前常用的一些密码功能,已在 UC 框架下被理想化,并给出了一定假设下的实现方案.如认证消息传输 F_{AUTH}[4]、安全消息传输 F_{SMT}[2]、密钥交换 F_{KE}[5]、公钥加密 F_{PKE}[2]、签名 F_{SIG}[2]、承诺 F_{COM}[6]、不经意传输 F_{OT}[2]等.与其它模型相比,UC 模型的抽象层次更高[3],具有更强的安全要求.因此,不是所有的理想功能 F 都可以由现实的协议实现.例如在文献[2]中提出 F_{SIG}被文献[7]证实不能被任何签名机制实现.而作为构建密码协议的基本原件之一的基于身份的签名理想功能,除了在文献[8]中在基于身份的加密机制下作为 $F_{SIG_{id}}$来研究,它的 UC 安全性到目前并没有给出足够的研究结果.本文针对上述问题,通过对 UC 安全框架分析和已有基于身份签名机制及其安全性研究:

(1)给出了 UC 安全框架下可实现的基于身份的签名机制的理想功能 F_{IBS}的定义.

(2)给出了基于身份的签名机制的 UC 安全性与 EUF-CMIA 安全性之间的等价关系.

2 基本概念

2.1 UC 安全框架

UC 安全框架是用于定义密码协议安全性的一般模型,它的核心由三个部分构成:环境,协议(参与协议各方),敌手.其定义一个协议的安全性主要思路如下:把协议实际运行中可能出现的所有景象抽象为环境、用户和敌手之间的交互,其中"环境"的视角包括所有通信和敌手的外部行为(包括"腐败(corrupt)用户的动作");敌手控制用户之间的通讯,并可以"腐败用户".一个协议是 UC 安全的,意思是对任一敌手,任何"环境"所看到的一切都可以在"理想世界"看到,而"理想世界"中用户是不需要交互的,现实协议所希望完成的任务可以通过访问一个 oracle(理想功能)来完成.以下我们将简要介绍该框架下一些关键定义和术语.

协议:协议即是一个交互式图灵机(ITM).通常,一个协议是几个参与者交互的规定,每个参与者都是一个 ITM.在 UC 框架下,代表各参与者的 ITM 被合并到一起形成一个总的 ITM.参与者之间不能直接传送消息,而是由先发给敌手、再从敌手处得到应答的方式来实现消息传递.就是说,敌手完全控制网络.一个运行中的协议有一个唯一的标示符 sid,并期待着与环境或敌手交互(收发消息);一般原则是功能接口(各参与者的输入输出)与环境相连,网络接口与敌手相连;消息格式一般是(receiver, sender, sid, actioncode, parameters),其中,如果接收者或发起者是环境或敌手时,相应项可省略.理想功能也是协议,但它不需要在参与者之间传送消息,且它期待的敌手是理想敌手(Simulator).按功能划分,常见协议可分为分布式计算或反应式服务两类.

环境和敌手:环境和敌手也是 ITM,它们都期待按各自的接口与协议交互,并可以相互通信.一般的原则是敌手对协议发出腐败指令必须由环境发出.只是在协议和环境之间忠实地传递消息的敌手被称为哑敌手,此时我们可以让环境直接对协议发出一切指令并得到回复.

根据敌手腐败参与者的时间点,敌手可以分为静态敌手和适应性敌手.如果敌手在协议的一开始就确定腐败任意的一组参与者(数量是有一定限制的)作为恶意参与者,在协议执行以后就不改变了,则称这种敌手是静态敌手.如果敌手不是在执行协议之前就确定他要腐败的参与者,而是在协议执行中根据协议的执行的情况来决定腐败哪个参与者,这种敌手就称为适应性敌手.

协议运行:在 UC 框架下,协议运行总是在环境的主导下进行.一次运行 $Excu(Z,\Pi,A)$一般是如下进行的:环境 Z 首先启动,然后发送指令激活协议 Π 或敌手 A;协议 Π 或敌手 A 在处理好当前指令后可发出下一指令并休息;收到指令者被激活;依次下去,直到如下情况:协议 Π 或敌手 A 在处理完当前指令后无消息发出;此时,环境 Z 被激活,并发出新的指令…;直到 Z 停止.

UC 安全性:在 UC 安全性的定义中,不妨规定环境总是输出 0,1.我们将一次运行 $Excu(Z,\Pi,A)$后 Z 的输出记做 $Z^{(\Pi,A)}$.我们说协议 πUC 仿真协议 Σ,意思是对任何 Π 的敌手 A 存在 Σ 的敌手 S,使得对任何环境 Z,$|Pr(Z^{(\Pi,A)}\rightarrow 1)-Pr(Z^{(\Sigma,S)}\rightarrow 1)|$可忽略.我们说一个现实的协议 π 安全地实现了一个理想功能 F(简称 UC 安全),意思是 πUC 仿真 F.形象地说就是,任何环境在现实世界看到的在理想世界也能看到,如图 1 所示.

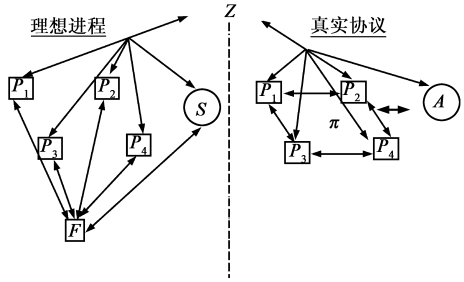

图1 UC安全模型

定义 1 UC 安全等价定义 设 π,F 分别为协议和理想功能;如果对协议 π 的哑敌手 A,存在理想敌手 S,使得对任何环境 Z,$|\Pr(Z^{(\pi,A)}\rightarrow 1)-\Pr(Z^{(F,S)}\rightarrow 1)|$可忽略,则 πUC 实现 F.

2.2 基于身份的签名机制

定义 2[9]　**基于身份的数字签名体制**　基于身份的数字签名体制 Σ 是由四个概率多项式算法(参数生成(Setup)算法、密钥生成(Extract)算法、签名(Sign)算法和验证(Verify)算法)组成的算法组:

①参数生成(Setup)算法:由可信中心 KGC 完成,输入安全参数 $1^\lambda(\lambda\in N)$,输出系统参数 *para* 和主密钥 s,KGC 公开发布 *para*,保密主密钥 s;

②密钥生成(Extract)算法:输入用户身份 $ID\in(0,1)^*$,KGC 利用掌握的主密钥 s 和系统参数 *para*,生成用户私钥 S_{ID}.

③签名(Sign)算法:输入系统参数 *para*、用户私钥 S_{ID}和消息 $m\in(0,1)^*$,输出相应的签名(m,σ);

④签名验证(Verify)算法:输入系统参数 *para*、用户身份和签名(m,σ),输出为 1 或 0,1 表示该签名是身份为 ID 用户的合法签名,而 0 表示签名无效.

这组算法满足起码的完备性和相容性要求,即以绝对优势概率保证正常产生的签名总是能通过验证并且验证算法对相同的输入有相同的输出.

2.3 EUF-CMIA 安全[9]

适应性选择消息和 ID 下抵抗存在性伪造攻击(EUF-CMIA)是针对 IBS 机制的普通安全定义.(existential unforgery for adaptive chose-message-and-identity attack)

设 $IBS=\{Setup, Extract, Sign, Verify\}$为基于身份数字签名体制,对任意的攻击者 A,安全参数 λ,定义 EUF-CMIA Game $Exp_A^{IBS}(\lambda)$为基于挑战者 C 和敌手 A 之间的游戏.

(1)C 运行 $Setup(1^\lambda)$,把生成系统参数 *para* 发送给 A, C 保存主密钥 s.

(2)A 可发起如下查询:

①密钥生成查询:给定身份 ID,C 运行密钥生成算法 Extract,将私钥 S_{ID}返回给 A.

②签名查询:给定身份 ID 和消息 m,C 运行签名算法 Sign,将对应签名 σ 返回给 A.

(3)A 输出(ID', m', σ'),若满足 ID' 和 ID', m' 不是之前进行的密钥生成查询和签名查询的输入,而 *Verify* $(ID', m', \delta')=1$,我们称 A 赢得该游戏,$Exp_A^{IBS}(\lambda)$返回 1,否则 A 失败,返回 0.

A 的成功优势定义为 $Adv_A^{IBS}(\lambda)=\Pr(Exp_A^{IBS}(\lambda)=1)$.

如果没有概率多项式敌手 A 以不可忽略的优势赢得上述游戏,则称 IBS 机制是 EUF-CMIA 安全的.

2.4 UC 框架下对应基于身份的数字签名体制 Σ 的协议 π_Σ

这里"基于身份的数字签名体制"并不是一个完整的基于身份的数字签名系统,而只是这样的系统中起核心作用的一组密码算法.对一个实际应用系统而言,通常由一个可信第三方 KGC 控制 Setup 和 Extact 算法,并负责制订和维护关于用户私钥的申请、发放和更新等安全策略.也就是说,上述"基于身份的数字签名体制 Σ"并不是在 UC 框架下的协议:它没有定义好恰当的功能接口.而我们的首要任务是给出在 UC 框架下"基于身份的数字签名体制 Σ"的功能接口.

对一个基于身份的数字签名体制 Σ,我们定义其在 UC 框架下对应的协议 π_Σ 如下:

π_Σ 具有主私钥变量 *sk*、标示变量 *Sid*,并维持一个签名者登记表.

—在收到请求$(KGC, setup, sid)$后,检验 $sid=(KGC, sid')$,运行 $Setup(1^\lambda)\rightarrow(s, para)$, $sk=s$, $Sid=(sid, para)$,并返回 *Sid*.此后忽略与 *Sid* 不匹配的所有请求(以下假定所有消息的 *sid* 都匹配,故以下消息中都省掉 *sid* 项).

—在收到请求$(U, setupsigner, ID)$后,运行 *Extract* $(para, sk, ID)\rightarrow s_{ID}$,将$(U, ID, s_{ID})$添加到签名者登记表中.

—在收到请求$(U, sign, m, ID)$后,如(U, ID)不在签名者登记表中,返回错误;否则运行 $sign(para, s_{ID}, m, ID)\rightarrow\delta$,并返回 δ.

—在收到请求$(V, Verify, m, \delta, ID)$后,运行 *Verify* $(para, m, \delta, ID)\rightarrow f$,并返回 f.

—在收到请求$(P, corrupt)$后,如果 $P=KGC$,返回主私钥,并停止;如 P 是已登记的签名者,返回对应的 S_{ID};否则,不动作.

注:在具体实现时,KGC 控制主私钥和 Extract 算法;setupsigner 可由 KGC 将用户私钥秘密传送给用户的方式实现;用户控制自己的签名功能;无须任何参与者维持签名者登记表.

3 理想功能 F_{IBS}

如何定义理想功能 F_{IBS}是需要一些思考的.首先,F_{IBS}应该与 π_Σ 有完全一样的接口.其次,我们希望在保证 F_{IBS}的"从定义上安全"的前提下兼顾其可实现性;具体地说,我们希望 F_{IBS}能被满足一定条件的"基于身份的数字签名体制 Σ"实现.这里我们借鉴 Canetti 对理想签名功能 F_{sig}的定义,定义 F_{IBS}如表 1.不同于传统公钥密码的数字签名体制,基于身份的签名的机制使用用户身份(或者可由身份信息通过公开算法导出)作为用户公钥的算法.理想的 F_{IBS}应该遵循如果没有参与方被腐败,参数生成(Setup)算法、密钥生成(Extract)算法、签名(Sign)算法和验证(Verify)算法可以安全实现.也就是

说，F_{IBS}扮演了一个可信第三方的角色.

表 1 理想功能 F_{IBS}

F_{IBS}具有标示变量 *Sid*，并维持一个签名者登记表、腐败签名者名单和一个签名表，均初始化为空.

—在收到请求(*KGC*, *setup*, *sid*)后，检验 *sid* = (*KGC*, *sid'*)，将此消息转发给理想敌手，在得到理想敌手回复(*setup*, *verify*(), *para*)后，记录下算法 *verify*()，令 *Sid* = (*sid*, *para*)，并返回 *Sid*. 此后忽略与 *Sid* 不匹配的所有请求(以下假定所有消息的 *sid* 都匹配，故以下消息中都省掉 *sid* 项).

—在收到请求(*U*, *setupsigner*, *ID*)后，将此消息转发给理想敌手，并将(*U*, *ID*)添加到签名者登记表中.

—在收到请求(*U*, *sign*, *m*, *ID*)后，

(**1**)如(*U*, *ID*)不在签名者登记表中，返回错误；

(**2**)否则，将此消息转发理想敌手，在得到理想敌手回复(*signed*, *m*, *ID*, δ)后：

①如 *U* 已被腐败，将(*m*, *ID*, δ, *verify*(*m*, *ID*, δ))添加到签名表中；

②如(*m*, *ID*, δ, **0**)不在签名表中将(*m*, *ID*, δ, **1**)添加到签名表中；返回 δ.

③否则，返回错误.

—在收到请求(*V*, *Verify*, *m*, δ, *ID*)后，如果(*m*, *ID*, δ, *f*)不在签名表中，运行 *Verify*(*para*, *m*, δ, *ID*)→*f*，将(*m*, *ID*, δ, *f*)添加到签名表中，并返回 *f*.

—在收到理想敌手的(*KGC*, *corrupt*)消息时，停止服务；在收到(*signer*, *corrupt*)时，将 *signer* 添加到腐败者名单中.

注：F_{IBS}无须回复腐败(corrupt)指令，因为理想敌手可独立完成对该指令的回复. 我们的理想功能 F_{IBS}并没有对同一 *ID* 限制唯一的参与者，如果需要，这样的限制可以由具体实现来解决.

在收到 *KGC* 请求(*KGC*, *setup*, *sid*)后，F_{IBS}检验 *sid* = (*KGC*, *sid'*)，将此消息转发给理想敌手，要求理想敌手提供 PPT 算法，在得到理想敌手回复(*setup*, *verify*(), *para*)后，记录下算法 *verify*()，令 *Sid* = (*sid*, *para*)，并返回 *Sid*. 此后忽略与 *Sid* 不匹配的所有请求(以下假定所有消息的 *sid* 都匹配，故以下消息中都省掉 *sid* 项).

在收到请求(*U*, *setupsigner*, *ID*)后，F_{IBS}将此消息转发给理想敌手，并将(*U*, *ID*)添加到签名者登记表中.

根据收到参与方 *m* 的请求(*U*, *sign*, *m*, *ID*)后，F_{IBS}将按如下方式执行：首先检查(*U*, *ID*)是否在签名者登记表中，如(*U*, *ID*)不在签名者登记表中，返回错误；否则 F_{IBS}将此消息转发理想敌手，在得到理想敌手回复(*signed*, *m*, *ID*, δ)后，检查腐败签名者名单：如果 *U* 在名单中，将(*m*, *ID*, δ, *verify*(*m*, *ID*, δ))添加到签名表中；如(*m*, *ID*, δ, 0)不在签名表中，将(*m*, *ID*, δ, 1)添加到签名表中；返回 δ. 如果上述情况均不是就返回错误信息.

在收到请求(*V*, *Verify*, *m*, δ, *ID*)后，F_{IBS}检查(*m*, *ID*, δ, *f*)是不是在签名中，如果不在，运行 *Verify*(*para*, *m*, δ, *ID*)→*f*，将(*m*, *ID*, δ, *f*)添加到签名表中，并返回 *f*.

在收到理想敌手的(*KGC*, *corrupt*)消息时，F_{IBS}停止服务；在收到(*signer*, *corrupt*)时，F_{IBS}将 *signer* 添加到腐败者名单中.

4 主要定理

定理 在适应性腐败敌手模型下，协议 π_Σ 安全实现了 F_{IBS}当且仅当签名机制 Σ 为 EUF-CMIA 安全.

证明：

(1)必要性：假如存在敌手 *A* 以不可忽略优势赢得 EUF-CMIA Game，我们将构造一个环境 Z_A，使得对任何理想敌手 *S*，Z_A 能以不可忽略概率区分它是与(π_Σ，哑敌手)还是与(F_{IBS}, *S*)交互. Z_A 首先对协议发送 *setup* 请求，在收到回复 *Sid* 后，将其中的 *para* 作为输入启动 *A*；对于 *A* 的请求(*Extract*, *ID*)，Z_A 可以先对协议发送(*U*, *setupsigner*, *ID*)请求，再发送相应的(*U*, *corrupt*)请求，以后者的返回值回应 *A*. 对于 *A* 的请求(*sign*, *m*, *ID*)，Z_A 可以先对协议发送(*U*, *setupsigner*, *ID*)请求，再发送相应的(*U*, *sign*, *m*, *ID*)请求，以后者的返回值回应 *A*. 当 *A* 输出(m^*, δ^*, ID^*)时，检验如果 ID^* 没运行过密钥生成算法，且 *A* 没发过(*sign*, m^*, ID^*)请求(否则 Z_A 返回失败)，对协议发送(*V*, *verify*, m^*, δ^*, ID^*)请求，输出返回值. 可以看出，在现实世界，Z_A 输出 1 的概率正是 *A* 赢得 EUF-CMIA Game 的概率，而在理想世界，Z_A 总是输出 0.

(2)充分性：首先我们构造如下的理想敌手 *S*：*S* 维持一个签名者注册表，运行过程如下：

—在收到 F_{IBS}的消息(*KGC*, *setup*, *sid*)后，运行 *Setup*(1^λ)→(*s*, *para*)，并返回(*setup*, *verify*(), *para*).

—在收到 F_{IBS}的消息(*U*, *setupsigner*, *ID*)时，运行 *Extract*(*s*, *ID*, *para*)→s_{ID}；将(*U*, s_{ID}, *ID*)添加到注册表中.

—在收到 F_{IBS}的消息(*U*, *sign*, *m*, *ID*)时，如果(*U*, s_{ID}, *ID*)在注册表中，返回 *sign*(*para*, s_{ID}, *m*, *ID*)；否则返回随机的签名字符串.

—在收到环境的(*P*, *corrupt*)指令后，首先转发给 F_{IBS}；如果 *P* = *KGC*，返回主私钥 *s*；如 *P* 是已登记的签名者，返回对应的 S_{ID}；否则，不动作.

我们下面来证明，*S* 模拟了哑敌手：即如果 Σ 为 EUF-CMIA 安全，则任何环境不可区分它是与(π_Σ，哑敌手)还是与(F_{IBS}, *S*)交互. 如不然，假如 *Z* 是例外，我们如下构造 EUF-CMIA Game 中的敌手 A_Z：

A_Z 维持一个签名者登记表、一个签名表和一个污染 ID 表，均初始化为空；运行过程如下：

—在得到挑战者的 *para* 后，启动 *Z*；

—当收到 *Z* 的请求(*KGC*, *setup*, *sid*)时，以 *Sid* =

(sid, $para$)做应答;

—在收到 Z 的请求(U, $setupsigner$, ID)后,向挑战者发出($Extract$, ID)请求;在得到应答 s_{ID} 后,将(U, ID, s_{ID})添加到签名者登记表中;

—在收到 Z 的请求(U, $sign$, m, ID)后,如(U, ID)不在签名者登记表中,返回错误;否则运行 $sign(para, s_{ID}, m, ID)\rightarrow\delta$,将($m$, ID, δ)添加到签名表并返回 δ;

—在收到 Z 的请求(V, $Verify$, m, δ, ID)后,运行 $Verify(para, m, \delta, ID)\rightarrow f$;(1)如果 $f=1$, ID 不在污染 ID 表,且(m, ID, δ)不在签名表中,输出(m, ID, δ)并停止.(2)否则,返回 f.

—在收到 Z 的请求(P, $corrupt$)后,(1)如果 $P=KGC$,输出失败并停止;(2)如 P 是已登记的签名者,将 ID 添加到污染 ID 表,返回对应的 s_{ID};(3)否则,不动作.

—当 Z 停止时,输出失败并停止.

可以验证,在 A_Z 输出失败的情形下,Z 看到的景象在与(π_Σ,哑敌手)交互时和与(F_{IBS}, S)交互时完全一样.所以这种情形发生的概率不超过 $1-|\Pr(Z^{\pi_\Sigma}\rightarrow 1)-\Pr(Z^{(F_{IBS},S)}\rightarrow 1)|$.而这种情形不发生时即是 A_Z 赢得 EUF-CMIA Game.也就是说,A_Z 赢得 EUF-CMIA Game 的概率不小于 $|\Pr(Z^{\pi_\Sigma}\rightarrow 1)-\Pr(Z^{(F_{IBS},S)}\rightarrow 1)|$.

另外对于在静态腐败敌手模型下,协议 π_Σ 安全实现 F_{IBS} 对签名机制 Σ 的要求又如何呢?从以上定理的证明中不难看出此时协议 π_Σ 安全实现 F_{IBS} 当且仅当签名机制 Σ 满足如下的安全性:在 EUF-CMIA Game 中,敌手不可以访问密钥生成 oracle,只能先由签名者生成参数,再访问相应的签名 oracle.

5　结论

普适安全是基于仿真的安全定义模型,可用于描述和分析并发环境下的协议安全问题.相对其它安全模型而言,普适安全具有更苛刻的安全定义.在 UC 安全框架下,"理想功能"的定义一般都不是平凡的任务.目前国际密码学界对 UC 安全的理论已经做了大量研究,大多数密码功能的 UC 安全性已得到清晰刻画,但是还没有提出与基于身份的签名机制相关的理想功能.本文给出了基于身份签名机制的理想功能 F_{IBS},并说明了在静态敌手和自适应敌手模型下基于身份签名机制是 UC-安全的充分必要条件.

参考文献

[1] 卿斯汉.安全协议 20 年研究进展[J].软件学报,2003,14(10):1740 – 1752.
Qing Sihan. Twenty years development of security protocols research[J]. Journal of Software, 2003, 14(10): 1740 – 1752. (in Chinese)

[2] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols[A]. Proceedings of 42nd IEEE Symposium on Foundations of Computer Science(FOCS)[C]. Oakland: IEEE, 2001. 136 – 145.

[3] 季庆光,冯登国.对几类重要网络安全协议形式模型的分析[J].计算机学报,2005,28(7):128 – 141.
J Ji Qingguang, Feng Dengguo. Towards analyzing some kinds of critically formal models for network security protocols[J]. Chinese Journal of Computers, 2005, 28(7): 128 – 141. (in Chinese)

[4] Ran Canetti. Universally composable signature, certification, and authentication[A]. Proceedings of CSFW 2004[C]. Chicago: IEEE Press, 2004. 219 – 235.

[5] Ran Canetti. Universally composable key exchange and secure channels[A]. Proceedings of Eutocrypt' 02[C]. New York: Springer, 2002. 337 – 351.

[6] Ran Canetti, M. Fischlin. Universally composable commitments[A]. Proceedings of Crypto 01[C]. London: Springer-Verlag, 2001. 19 – 23.

[7] Michael Backes, Dennis Hofheinz. How to break and repair a universally composable signature functionality[A]. Proceedings of Information Security Conference-ISC LNCS[C]. Berlin: Springer-Verlag, 2004. 61 – 74.

[8] Ryo Nishimaki, Yoshifumi Manabe, Tatsuaki Okamoto. Universally composable identity-based encryption[A]. Proceedings of Vietcrypt 2006. LNCS 4341[C]. Vietnam: Springer, 2006. 337 – 353.

[9] Adi Shamir. Identity-based cryptosystems and signature schemes[A]. Proceedings of Advances in Cryptology[C]. Santa Barbara: Springer, 1984. 19 – 22.

[10] 冯涛,马建峰,李凤华.UC 安全的高效不经意传输协议[J].电子学报,2008,36(1):17 – 23.
Feng Tao, Ma Jianfeng, Li Fenghua. Efficient and universally composable security oblivious transfer[J]. Acta Electronica Sinica, 2008, 36(1): 17 – 23. (in Chinese)

作者简介

王　竹　女,1972 年生于山西,清华大学计算机科学与技术系博士后.研究方向为安全协议.
E-mail: wzjsj@mail.tsinghua.edu.cn

戴一奇　男,1946 年生于浙江,清华大学计算机科学与技术系教授.研究方向:网络信息安全,算法设计与分析.

叶顶锋　男,1969 年生于四川,信息安全国家重点验室、中国科学院研究生院教授.研究方向为密码理论与技术.