

基于身份数字签名方案的通用可组合安全性

王泽成

(安徽财经大学 信息工程学院, 安徽 蚌埠 233041)

(w52051201006@hotmail.com)

摘要:在通用可组合安全性框架下定义了基于身份的数字签名方案的通用可组合安全性。证明了基于身份数字签名方案的通用可组合安全性与传统的——在选择消息和选择身份攻击下的不可存在性伪造——之间的等价性。这一结果表明基于身份的数字签名方案可以作为安全的密码原语用于构建更复杂的密码协议。

关键词:基于身份的数字签名;理想功能;通用可组合安全性

中图分类号: TP309.2 **文献标志码:** A

Universally composable security of identity-based signature schemes

WANG Ze-cheng

(School of Information Engineering, Anhui University of Finance and Economics, Bengbu Anhui 233041, China)

Abstract: A definition of universally composable security of identity-based signature schemes was proposed in the universally composable security framework. The equivalence of the universally composable security and the traditional security of identity-based signature schemes was proved. This result shows that an identity-based signature scheme can be used as a primitive block to design more complicated cryptographic protocols.

Key words: identity-based signature; ideal functionality; universally composable security

0 引言

基于身份的数字签名由 Shamir 于 1984 年提出^[1],目的是简化基于证书的公钥密码基础设施中的密钥管理问题。在一个基于身份的数字签名方案中,一个实体的公钥就是其公开的身份,而其对应的私钥则由一个私钥生成中心生成:私钥生成中心利用自己的主秘密密钥生成该实体的私钥并秘密地发送该实体。这样就消除了传统的公钥密码系统对公钥密码基础设施与公钥证书的需求。

关于基于身份的数字签名方案的安全性,Cha 等人提出了在选择消息和选择身份攻击下的不可存在性伪造(EU-CMIA)的定义^[2],这个定义是对传统的数字签名方案在选择消息攻击下不可存在性伪造安全性定义^[3]的一个自然扩展。此后,EU-CMIA 成为广泛接受的基于身份的数字签名方案安全性定义^[4-5]。

为了描述密码协议以及分析密码协议的安全性,密码学家 Ran Canetti 于 2001 年提出了通用可组合安全性框架(Universally Composable Security Framework)^[6]。该框架允许以一种统一的、系统的方式定义任意密码任务的安全性需求。更重要的是,在该框架下定义的安全协议,当它与任意其他的协议并发运行时其安全性仍然不受影响;并且它可以作为部件安全地组合到更复杂的密码协议中而保持安全性。这种组合操作称为通用组合,相应地在该框架下定义的协议安全性,称为通用可组合安全性(UC 安全性)。因此通用可组合安全框架提供了一种以模块化的方法设计和分析协议的机制。通过利用一些具有通用可组合安全性的密码原语和密码协议,可以很方便地得到安全的、更复杂的密码协议。

自从通用可组合安全性框架提出以来,许多密码原语和

密码协议的安全性在该框架下被重新定义,在该框架下给出的安全性定义和传统的安全性定义之间的关系也被深入地研究。结果表明,一方面,由于通用可组合蕴含了更强的安全性要求,因而一些密码原语和协议的传统安全性定义并不能满足通用可组合安全性需求。例如,在没有初始假设的情况下,不可能设计出具有 UC 安全性的两方密码协议^[6-10]。另一方面,也有一些密码原语和协议的传统安全性和通用可组合安全性是等价的。例如,公钥加密方案的 UC 安全性等价于传统安全性^[11],即适应性选择密文攻击下的不可区分性;基于身份的公钥加密方案的 UC 安全性等价于传统安全性^[12],即适应性选择消息和身份攻击下的不可区分性;数字签名方案的 UC 安全性等价于传统安全性^[6,13],即选择消息攻击下的不可存在性伪造。

由于数字签名方案和基于身份的数字签名方案经常被作为更大密码协议的构造模块(例如,密钥交换协议^[14-15]、IPSec 协议^[16]和用于 Ad Hoc 网络的协议^[17]等),因此定义数字签名方案和基于身份的数字签名方案的 UC 安全性并澄清其与传统安全性之间的关系就显得非常重要。为此,密码学家 Ran Canetti 经过多次尝试,最后在文献[13]中给出了数字签名方案的 UC 安全性定义,并证明了其与传统安全性定义之间的等价性。但是对于基于身份的数字签名方案至今还没有人给出其 UC 安全性定义并研究其与传统安全性定义之间的关系。

本文讨论了基于身份的数字签名方案的 UC 安全性定义并证明其与传统安全性定义之间的等价性。这对于应用基于身份的数字签名方案作为基本构造模块来设计更复杂的密码协议具有重要的意义,即满足传统安全性定义的基于身份的数字签名方案由于同时满足 UC 安全性,因而可以被安全地

组合到更复杂的密码协议中。本文首先采用 UC 安全性框架下统一的定义安全性的方法来定义基于身份的数字签名方案的 UC 安全性,即定义出基于身份的数字签名方案的理想功能 F_{IBS} ; 然后根据一个基于身份的数字签名方案构造了一个实现 F_{IBS} 的协议;最后证明,一方面,如果基于身份的数字签名方案是 EU-CMIA 安全的,那么该协议安全实现了 F_{IBS} , 另一方面,如果该协议安全实现了 F_{IBS} , 那么所使用的基于身份的数字签名方案一定是 EU-CMIA 安全的,即基于身份数字签名方案的 UC 安全性和传统的 EU-CMIA 安全性是等价的。

1 基本概念

1.1 基于身份的数字签名方案

一个基于身份的数字签名方案 Σ 由 4 个算法 (set, ext, sig, ver) 组成,描述如下。

set(1^k) 是一个概率多项式时间算法,输入系统安全参数 k , 输出系统公共参数 SP 和一个系统主密钥 MK 。运行该算法的私钥生成中心公布公共参数 SP , 保密系统主密钥 MK 。

ext(SP, MK, ID) 是一个概率多项式时间算法,输入系统公共参数 SP 、系统主密钥 MK 和一个身份字符串 ID , 输出与 ID 对应的一个私钥 d_{id} 。其中 ID 作为数字签名的验证公钥, d_{id} 作为数字签名的签名密钥。私钥生成中心运行该算法,并将所得到的私钥通过安全信道发送给身份 ID 对应的实体。

sig(SP, d_{id}, m) 是一个概率多项式时间算法,输入系统公共参数 SP 、身份 ID 对应的私钥 d_{id} 和消息 m , 输出身份为 ID 的实体对消息 m 的签名 σ 。该算法由身份为 ID 的签名实体运行。

ver(SP, ID, m, σ) 是一个确定性算法,输入系统公共参数 SP 、身份 ID 、消息 m 和签名 σ , 如果该签名是身份为 ID 的实体对消息 m 的合法签名,则输出 1; 否则输出 0。该算法可由任意实体运行。

定义 1 称一个基于身份的数字签名方案 $\Sigma = (\text{set}, \text{ext}, \text{sig}, \text{ver})$ 对选择消息和身份攻击是不可存在性伪造的 (EU-CMIA), 如果对任意可忽略的函数 $\nu(\cdot)$ 以及所有足够大的安全参数 k , 以下性质均能满足。

完备性 对任意的消息 m , 有:

$$\text{prob} \left[\begin{array}{l} (SP, MK) \leftarrow \text{set}(1^k); \\ d_{\text{id}} \leftarrow \text{ext}(SP, MK, ID); \\ \sigma \leftarrow \text{sig}(SP, d_{\text{id}}, m); \\ 0 \leftarrow \text{ver}(SP, m, \sigma, ID) \end{array} \right] < \nu(k)$$

一致性 (不可否认性) 对任意的消息 m , 执行算法 (SP, MK) \leftarrow set(1^k); $d_{\text{id}} \leftarrow$ ext(SP, MK, ID); $\sigma \leftarrow$ sig(SP, d_{id}, m) 后, 两次独立执行算法 ver(SP, ID, m, σ) 所得的输出是不一致的概率小于 $\nu(k)$ 。

不可伪造性 对任意的概率多项式时间伪造者 G , 有:

$$\text{prob} \left[\begin{array}{l} (SP, MK) \leftarrow \text{set}(1^k); \\ (ID, m, \sigma) \leftarrow G^{O_{\text{ext}}, O_{\text{sig}}}(k, SP); \\ 1 \leftarrow \text{ver}(SP, m, \sigma, ID) \text{ 且 } G \text{ 从未询问 } O_{\text{ext}} \\ \text{以提取 } ID \text{ 的私钥, 也未询问 } O_{\text{sig}} \text{ 以得} \\ \text{到身份为 } ID \text{ 的实体对消息 } m \text{ 的签名} \end{array} \right] < \nu(k)$$

其中 $O_{\text{ext}}, O_{\text{sig}}$ 分别为私钥提取预言机和签名预言机。输入身份 ID, O_{ext} 输出一个对应的私钥; 输入身份 ID 和消息 m, O_{sig} 输出身份为 ID 的实体对消息 m 的一个签名。

1.2 UC 安全性

UC 安全性是基于仿真的方法来定义的, 涉及到计算模

型、现实模型、理想模型等概念。本文只作简要介绍, 更多细节可参阅文献[11]。

计算模型 在 UC 框架中用概率多项式时间 (Probabilistic Polynomial Time, PPT) 交互式图灵机 (Interactive Turing Machine, ITM) 系统来描述一个协议的运行, 其中包括 3 个 PPT ITM, 即被执行的协议、环境以及敌手。协议的各个参与实体以特定的输入分别运行协议图灵机的一个实例, 环境和敌手分别运行各自图灵机的一个实例。

现实模型 描述实际的协议运行情况。由现实协议 π 、环境 Z 以及现实世界的敌手 A 的交互构成。协议 π 是实现指定任务的一个程序, 它由 n 个参与实体 P_1, P_2, \dots, P_n 共同执行。这些参与实体从环境 Z 接收输入并向 Z 输出结果, 它们之间通过敌手 A 进行通信。环境 Z 是协议运行的初始 ITM 并起控制的作用。它向敌手 A 发送信息 (可视为“指令”或“问题”), 并向执行 π 的各个参与实体提供输入以及接收各个参与实体的输出和由 A 报告的信息。敌手 A 可以传递消息、向 Z 报告信息以及入侵参与实体。环境 Z 的输出就是整个协议运行的结果, 不失一般性, 可以假设仅由一位的消息组成。

理想模型 描述协议执行的理想情况, 协议在此模型下可得到无条件的安全性。理想模型也是由三个 PPT ITM 的交互构成: 理想协议由 n 个哑元参与实体和一个理想功能 F 共同执行, 环境 Z 以及理想世界中的敌手 S 。在理想协议中, 哑元参与实体扮演只在 Z 和 F 之间传递消息的角色, 理想功能 F 则扮演一个不可破的可信第三方的角色以完成协议所执行的功能。环境 Z 与现实模型中的相同。敌手 S 也可以传递消息、向 Z 报告信息以及入侵参与实体。环境 Z 的输出也就是整个理想协议运行的结果, 由一位消息组成。

UC 安全性定义 令 $REAL_{\pi, A, Z}(k, z, r)$ 表示现实模型中环境 Z 的输出, 其中 k 是安全参数, z 是环境 Z 的辅助输入, $r = (r_Z, r_A, r_1, \dots, r_n)$ 是环境 Z 、敌手 A 以及协议的 n 个参与实体 P_1, P_2, \dots, P_n 的随机输入。令 $REAL_{\pi, A, Z}(k, z)$ 表示当 r 均匀取值时 $REAL_{\pi, A, Z}(k, z, r)$ 对应的随机变量, $REAL_{\pi, A, Z}$ 表示随机变量 $REAL_{\pi, A, Z}(k, z)$ 的总体 $\{REAL_{\pi, A, Z}(k, z)\}_{k \in \mathbb{N}, z \in \{0, 1\}^*}$ 。类似地, 令 $IDEAL_{F, S, Z}(k, z, r)$ 表示理想模型中环境 Z 的输出, 其中 k 是安全参数, z 是环境 Z 的辅助输入, $r = (r_Z, r_S, r_F)$ 是环境 Z 、敌手 S 以及理想功能 F 的随机输入。令 $IDEAL_{F, S, Z}(k, z)$ 表示当 r 均匀取值时 $IDEAL_{F, S, Z}(k, z, r)$ 对应的随机变量, $IDEAL_{F, S, Z}$ 表示随机变量 $IDEAL_{F, S, Z}(k, z)$ 的总体 $\{IDEAL_{F, S, Z}(k, z)\}_{k \in \mathbb{N}, z \in \{0, 1\}^*}$ 。

定义 2 UC 安全性。令 F 是一个理想功能, π 是一个 PPT 协议。如果对任意 PPT 敌手 A , 存在 PPT 敌手 S , 满足对任意的环境 Z 有: $IDEAL_{F, S, Z} \approx REAL_{\pi, A, Z}$ 成立, 其中“ \approx ”表示计算不可区分, 则称 π UC 实现了 F , 称协议 π 具有 UC 安全性。

由 UC 安全性的定义可以看出, 在 UC 安全框架下定义实现某个密码任务的密码协议的形式化安全模型, 关键是定义出该密码任务的理想功能。

2 基于身份的数字签名方案的理想功能

基于身份的数字签名方案的理想功能 F_{IBS} 的定义如下。

1) Setup. 当收到来自某个实体 T 的一个消息 (Setup, sid, T), 验证其形式是否为 $sid = (T, sid')$ 。如果不是, 则忽略

该消息。否则,将 $(Setup, sid, T)$ 交给敌手 S 。当收到来自于 S 的 $(Algorithms, sid, x, s, v)$, 其中 x, s 是两个概率多项式时间图灵机的描述, v 是一个确定多项式时间图灵机的描述。记录元组 (T, x, s, v) , 输出 $(VerAlgorithm, sid, v)$ 给 T 。忽略以后的 $Setup$ 消息。

2) Extract。当收到某个实体 I 发来的消息 $(Extract, sid, ID, I, v')$, 按下述方式进行操作:

①如果 T 已被入侵,则把 $(Extract, sid, ID, I, v')$ 交给敌手 S 。当收到来自 S 的 $(Extracted, sid, ID, I, d_{ID})$, 记录元组 (ID, I, d_{ID}) 到 ID-Reg 列表,输出 $(Extracted, sid, ID, I)$ 给 I 。

②否则,如果 $v' \neq v$ 或者在列表中已存在 (ID, \cdot, \cdot) 元组,则输出一个出错消息给 I 。

③否则,计算 $d_{ID} = x(ID)$, 记录 (ID, I, d_{ID}) 到 ID-Reg 列表,输出 $(Extracted, sid, ID, I)$ 给 I 。

3) Sign。当收到来自实体 I 的消息 $(Sign, sid, ID, m)$, 按下述方式进行操作:

①如果 I 已被入侵,则将 $(Sign, sid, ID, m)$ 交给敌手 S 。当收到来自 S 的 $(Signature, sid, ID, m, \sigma)$, 将其输出给 I 。

②否则,如果在 ID-Reg 列表中存在 (ID, I, d_{ID}) , 则计算 $\sigma = s(d_{ID}, m)$ 。如果 $v(ID, m, \sigma) = 1$, 则将 (ID, m, σ) 记录到列表 Meg-Sig 中,输出 $(Signature, sid, ID, m, \sigma)$ 给 I 。

③否则,输出一个出错消息给 I 。

4) Verify。当收到某个实体 V 的消息 $(Verify, sid, ID, m, \sigma, v')$, 如果 $v' = v$ 、 T 和 I 未被入侵、 $v(ID, m, \sigma) = 1$ 且列表 Meg-Sig 中没有记录 (ID, m, σ') , 其中 σ' 为任意一个值,则输出一个出错消息给 V 。否则,输出 $(Verified, sid, ID, m, v'(ID, m, \sigma))$ 给 V 。

该定义的基本思想是让 F_{IBS} 提供一个注册服务,签名人 I 可以注册一个(身份,消息,签名)元组。这通过两步来完成:首先,通过提取与身份对应的一个私钥来实现注册身份;然后,通过对消息进行签名实现任意的(消息,签名)对与相应身份一起注册。任意实体只要提供了正确的验证密钥(算法)就可以检查一个指定的元组是否已注册。

虽然在基于身份的数字签名系统中除私钥生成中心之外可以有多达 k 的多项式个参与实体,但按其所做的操作可视为签名者和验证者两种角色。因此本文用 I 表示执行提取私钥或签名操作的实体,用 V 表示执行验证操作的实体。

在 F_{IBS} 中首先执行 Setup 操作一次,然后可以执行 Extract 操作、Sign 操作以及 Verify 操作多达 k 的多项式次。这些操作分别由下面四种类型的输入激活。

当收到创建系统的实体(即私钥生成中心) T 的建立基于身份的数字签名系统的请求后, F_{IBS} 首先检查会话标识号 sid 构造是否正确,即该会话标识号是由 T 的身份加 1 个随机串构成。这个检查保证了每个 F_{IBS} 实例的唯一性。注意在其他的三个操作中也要做同样的检查,限于篇幅,在上面的定义中省略了。如果 sid 没有正确地构造,则该请求被忽略。否则, F_{IBS} 询问敌手提供三个算法描述:一个概率多项式时间私钥提取算法 x , 一个概率多项式时间签名算法 s 以及一个确定多项式时间验证算法 v 。然后把 v 输出给 T 。之后 T 可以公开 v 作为系统的公共参数。但算法 x 和 s 并不输出给 T 。 F_{IBS} 使用数据结构 ID-Reg 和 Meg-Sig 记录相关信息。

当收到身份为 ID 的某个实体 I 提取其私钥的请求(该请求中包含身份 ID 和作为系统公共参数的信息 v')后, F_{IBS} 按下述方式操作。如果 T 已经被入侵,则让敌手决定该身份所

对应的私钥并输出。这用于刻画恶意敌手的适应性入侵行为。如果 T 没有被入侵, $v' = v$ 且该身份的私钥没有被提取过,则 F_{IBS} 计算私钥 $d_{ID} = x(ID)$ 并将 (ID, I, d_{ID}) 记录到列表 ID-Reg 中。通过输出消息 $(Extracted, sid, ID, I)$ 给 I, F_{IBS} 告知 I 其身份 ID 已成功注册了。否则,如果 T 未被入侵,但是 $v' \neq v$ 或者该身份的私钥已被提取过, F_{IBS} 输出一个出错消息给 I 。这里 F_{IBS} 并不将计算出的私钥输出给 I 。

当收到身份为 ID 的某个实体 I 对消息 m 进行签名的请求, F_{IBS} 按下述方式操作。如果 I 已被入侵,则让敌手决定签名并输出。这用于刻画恶意敌手的适应性入侵行为。如果 I 未被入侵,且以前正确地提取过私钥,那么 F_{IBS} 用算法 s 为 I 计算签名。如果所计算的签名是正确的,那么记录该签名并输出 $(Signature, sid, ID, m, \sigma)$ 给 I 。否则,输出一个出错消息给 I 。

当收到某个实体 V 要求用验证算法 v' 验证 σ 是否为身份是 ID 的实体对消息 m 的合法签名的请求时, F_{IBS} 按下述方式操作。如果 T 和 I 均未被入侵,且 I 没有对消息 m 进行过签名,但是该签名又能使正确的验证算法的输出为 1,那么这个签名必定是一个伪造的签名。因此, F_{IBS} 输出一个出错的消息给 V 。否则,取验证算法 v' 的执行结果作为验证的结果。

F_{IBS} 按标准的方法处理敌手入侵。当一个实体被入侵了, F_{IBS} 记录下这个事实,并将该实体的所有输入和输出报告给敌手。对于签名者来说,这些信息包括所有的提取私钥请求、签名请求以及 F_{IBS} 针对这些请求的输出。对验证者来说,这些信息包括所有的验证请求和 F_{IBS} 针对这些请求的输出。对于私钥生成中心 T , 这些信息包括系统建立请求和 F_{IBS} 针对该请求的输出。另外,如果敌手入侵了一个签名者, F_{IBS} 同时报告签名算法(包括签名者的私钥)及其当前的状态;如果敌手入侵了私钥生成中心 T , F_{IBS} 同时报告私钥提取算法及其当前的状态。

下面从直观上说明 F_{IBS} 的定义是如何满足基于身份数字签名方案的一致性、完备性及不可伪造性的安全性要求的,下一节将正式证明由 F_{IBS} 给出的基于身份数字签名方案的 UC 安全性与传统的 EU-CMIA 安全性是等价的。首先,验证算法 v 是确定性的,这保证了“一致性”,即所有对于同一个元组 (ID, m, σ, v') 的验证请求,其输出都是一样的。其次,在签名生成时验证 $v(ID, m, \sigma) = 1$ 保证了“完备性”,即如果一个签名是诚实地生成的(即由 F_{IBS} 生成的),那么它一定能被正确地验证。最后,“不可伪造性”则是由验证时对伪造签名的检查来保证。

3 UC 安全性与 EU-CMIA 安全性之间的关系

下面我们证明上述通过理想功能 F_{IBS} 定义的基于身份数字签名方案的 UC 安全性和传统的 EU-CMIA 安全性是等价的。为此假设存在一个基于身份的数字签名方案 $\Sigma = (set, ext, sig, ver)$, 首先将其转化为一个协议 π_{Σ} , 然后证明当且仅当 Σ 是 EU-CMIA 安全的,协议 π_{Σ} 实现了理想功能 F_{IBS} , 即具有 UC 安全性。协议 π_{Σ} 在描述如下。

1) Setup。当输入 $(Setup, sid, T)$ 到私钥生成中心 T , T 通过运行算法 $set(1^k)$ 得到系统参数 SP 和主密钥 MK , 并令算法 $x = ext(SP, MK, \cdot)$, $s = sig(SP, \cdot, \cdot)$, $v = ver(SP, \cdot, \cdot)$ 。然后输出 $(VerAlgorithm, sid, v)$ 。此外, T 初始化一个列表 ID-Reg。

2) Extract。当输入 $(Extract, sid, ID, I, v')$ 到私钥生成中心 T , 如果 $v' \neq v$ 或者在列表 ID-Reg 中已存在 (ID, I, d_{ID}) 元组, 则输出一个出错消息给 I 。否则, 计算 $d_{ID} = x(ID)$, 记录 (ID, I, d_{ID}) 到 ID-Reg 列表, 输出 $(Extracted, sid, ID, I)$ 并通过 F_{SMT} 把 (ID, d_{ID}) 传送给 I 。

3) Sign。当输入 $(Sign, sid, ID, m)$ 到实体 I , 如果 I 还没有提取到正确的私钥 d_{ID} , 则 I 输出一个出错信息; 否则计算 $\sigma = s(d_{ID}, m)$ 。如果 $v(ID, m, \sigma) = 1$, 则输出 $(Signature, sid, ID, m, \sigma)$ 给 I ; 否则输出一个出错信息。

4) Verify。当输入 $(Verify, sid, ID, m, \sigma, v')$ 到某个实体 V , V 输出 $(Verified, sid, ID, m, v'(ID, m, \sigma))$ 。

协议 π_{Σ} 中算法 ext, sig, ver 中的“ \cdot ”代表相应的参数。为了实现私钥生成中心向签名实体安全地传输私钥, 协议 π_{Σ} 使用了文献[11]中定义的安全消息传输协议理想功能 F_{SMT} 。使用 F_{SMT} 刻画了基于身份的数字签名方案中一个隐含的假设, 即私钥生成中心可以安全地传输私钥给私钥提取者。理想功能 F_{SMT} 定义如下。

1) 当收到来自于某个实体 S 的输入消息 $(Send, sid, m)$, 如果 $sid = (S, R, sid')$ 则把 $(Send, sid)$ 发给敌手, 生成一个保密的延迟输出 $(Sent, sid, m)$ 给 R 之后停机; 否则忽略该输入。

2) 当收到来自于敌手的信息 $(Corrupt, sid, P)$, 其中 $P \in \{S, R\}$, 将消息 m 暴露给敌手。之后, 如果敌手提供了另外一个值 m' , 并且 $P = S$ 而消息 m 还没有传给 R , 则输出 $(Sent, sid, m')$ 给 R 之后停机。

在协议 π_{Σ} 的运行过程中, 如果一个参与实体被敌手入侵了, 那么敌手将获得其所有内部状态。对于签名者来说, 敌手也同时获得其签名私钥 d_{ID} ; 对于私钥生成中心来说, 敌手也同时获得其主密钥。即敌手完全控制了该参与实体。

定理 1 设 $\Sigma = (set, ext, sig, ver)$ 是一个基于身份的数字签名方案, 那么当且仅当 Σ 是 EU-CMIA 安全的, 上述协议 π_{Σ} UC 实现了理想功能 F_{IBS} 。

证明 首先证明必要性。采用反证法证明如果 Σ 不是 EU-CMIA 安全的, 那么 π_{Σ} 不可能 UC 实现理想功能 F_{IBS} 。通过构造出一个环境 Z 和一个现实协议 π_{Σ} 执行中的敌手 A , 使其满足对实现 F_{IBS} 的理想协议中的任意敌手 S, Z 均能区分出它是在和 π_{Σ} 与 A 交互, 还是在和 F_{IBS} 与 S 交互, 因而 π_{Σ} 不满足 UC 安全性定义, 与 π_{Σ} UC 实现了理想功能 F_{IBS} 矛盾。具体构造细节如下所述。

1) 假设 Σ 不满足完备性, 即存在消息 m 满足:

$$\text{prob} \left[\begin{array}{l} (SP, MK) \leftarrow \text{set}(1^k); \\ d_{ID} \leftarrow \text{ext}(SP, MK, ID); \\ \sigma \leftarrow \text{sig}(SP, d_{ID}, m); \\ 0 \leftarrow \text{ver}(SP, m, \sigma, ID) \end{array} \right] < 1 - \nu(k)$$

对无限多的 k 的都成立。那么下面的环境 Z 能区分出它是在和 π_{Σ} 与 A 交互, 还是在和 F_{IBS} 与 S 交互。首先, Z 置 $sid = (T, 0)$ 并以消息 $(Setup, sid, T)$ 为输入激活私钥生成中心 T , 得到验证算法 v 。其次, Z 以消息 $(Extract, sid, ID, I, v)$ 为输入激活某个签名者 I , 得到 $(Extracted, sid, ID, I)$ 。然后, Z 以消息 $(Sign, sid, ID, m)$ 为输入激活签名者 I , 得到 $(Signature, sid, ID, m, \sigma)$ 。最后, Z 以消息 $(Verify, sid, ID, m, \sigma, v)$ 为输入激活某个验证者 V , 并输出返回的验证值。显然, Z 在和 F_{IBS} 交互后总是输出 1, 但在和 π_{Σ} 交互后会以不可忽略的概率输出

0。

2) 假设 Σ 不满足一致性, 那么对 1) 中的环境 Z 作如下的修改: 它激活验证者 V 两次, 如果两次激活 V 所得的验证值相同, 则输出 1; 否则输出 0。同样地, Z 在和 F_{IBS} 交互后总是输出 1, 但在和 F_{IBS} 交互后会以不可忽略的概率输出 0。

3) 假设 Σ 不满足不可伪造性, 即存在一个成功的伪造者 G 。那么对 1) 中的环境 Z 做如下的修改。在 Z 的内部运行 G 的一个副本; 把从私钥生成中心 T 获得的验证算法 v 交给该副本。此后当 G 的副本询问提取私钥的预言机以提取身份 ID 所对应的私钥, Z 以消息 $(Extract, sid, ID, I, v)$ 为输入激活某个签名者 I , 当 Z 收到 $(Extracted, sid, ID, I)$ 后即指使敌手 (在现实协议中为 A , 在理想协议中为 S) 入侵签名者 I , 得到私钥 d_{ID} 后返回给 G 的副本。当 G 的副本询问签名预言机以获取身份为 ID 的实体对消息 m 的签名, Z 检查身份 ID 的私钥是否已提取过, 如未提取, 则以消息 $(Extract, sid, ID, I, v)$ 为输入激活某个签名者 I , 得到 $(Extracted, sid, ID, I)$, 之后以消息 $(Sign, sid, ID, m)$ 为输入激活签名者 I , 并将得到的签名返回给 G 的副本。当 G 的副本输出一个元组 (ID, m, σ) 后, Z 检查 G 的副本以前是否曾询问过身份 ID 的私钥或询问过身份为 ID 的实体对消息 m 的签名, 如是, 则输出 0 并停机。否则, Z 以消息 $(Verify, sid, ID, m, \sigma, v)$ 为输入激活某个验证者 V 并输出验证的结果。显见, 当 Z 在和 π_{Σ} 交互时, Z 内部运行的 G 的副本的视图与 G 在对 Σ 进行选择消息和选择身份攻击时的视图是相同的, 因此 Z 会以不可忽略的概率输出 1。然而, Z 在和理想协议交互时, 由于 G 的副本输出的元组 (ID, m, σ) 在 F_{IBS} 中没有注册过, 当 $v(ID, m, \sigma) = 1$ 时不会输出 1, 而是输出一个出错信息。

综上所述, 在所有情况下, 所构造出的 Z 都能区分它是在和 π_{Σ} 与 A 交互, 还是在和 F_{IBS} 与 S 交互。这与 π_{Σ} UC 实现了 F_{IBS} 矛盾。

接下来仍然采用反证法证明充分性。假设 π_{Σ} 没有 UC 实现 F_{IBS} , 即在 π_{Σ} 的执行中存在一个敌手 A 使得对 F_{IBS} 的理想协议执行中的任意敌手 S , 总存在一个环境 Z 能够区分它是在和 π_{Σ} 与 A 交互, 还是在和 F_{IBS} 与 S 交互, 我们证明 Σ 不可能是 EU-CMIA 安全的, 与条件矛盾。详细描述如下。

既然 Z 的区分能力对任意的理想敌手 S 都成立, 那么对下面所构造的 S 也是成立的。

S 在内部运行 A 的一个副本并为其模拟私钥生成中心 T 、签名者 I 以及验证者 V , S 同时为其模拟安全消息传输理想功能 F_{SMT} 。 S 按如下方式操作。

1) 对于来自于 Z 的输入均传递给 A , A 的输出则复制到 S 的输出带 (将被 Z 读取)。

2) 如果 S 在收到来自于 F_{IBS} 的 $(Setup, sid, T)$ 消息之前收到来自于 Z 的入侵 T 的消息 $(Corrupt, sid, T)$, 则将该入侵消息送给 F_{IBS} 以及其内部运行的 A 的副本。当收到 F_{IBS} 返回的信息后, 将这些信息作为被入侵的 T 的状态送给 A 的副本。此后, A 控制了模拟的实体 T , S 控制了理想协议执行中的哑元实体 T 。之后, 当 S 收到来自于 Z 的 $(Setup, sid, T)$ 消息 (实际上是 Z 传送给 T 的), 将其送给 F_{IBS} 。

3) 当 S 收到来自于 F_{IBS} 的 $(Setup, sid, T)$ 消息, 如果 T 已被入侵, 则将 $(Setup, sid, T)$ 交给 A 的副本, 然后将 A 的副本回复的信息返回给 F_{IBS} 。如果 T 未被入侵, S 运行 $(SP, MK) \leftarrow \text{set}(1^k)$, 令 $x = \text{ext}(SP, MK, \cdot)$, $s = \text{sig}(SP, \cdot, \cdot)$,

$v = \text{ver}(SP, \cdot, \cdot, \cdot)$ 并返回 $(\text{Algorithms}, \text{sid}, x, s, v)$ 给 F_{IBS} 。

4) 当 S 收到来自于 F_{IBS} 的 $(\text{Extract}, \text{sid}, ID, I, v')$ 消息 (由 F_{IBS} 的定义知, 此时 T 已被入侵), S 扮演签名者 I 将该消息送给 A 的副本 (因为它已控制了模拟的实体 T)。当收到 A 的副本返回的私钥 d_{ID} , S 返回消息 $(\text{Extracted}, \text{sid}, ID, I, d_{\text{ID}})$ 给 F_{IBS} 。

5) 当 S 收到来自于 F_{IBS} 的 $(\text{Sign}, \text{sid}, ID, m)$ 消息 (由 F_{IBS} 的定义知, 此时 I 已被入侵), S 将该消息送给 A 的副本 (因为它已控制了模拟的实体 I)。当收到 A 的副本返回的 $(\text{Signature}, \text{sid}, ID, m, \sigma)$, S 将其返回给 F_{IBS} 。

6) 当 Z 指示入侵一个参与实体, S 将入侵指令送给 F_{IBS} 并将 F_{IBS} 返回的信息作为 A 要入侵的模拟的参与实体的状态信息送给 A 的副本。此后, A 控制了模拟的参与实体, S 控制了理想协议执行中的哑元实体。

下面, 假设基于身份的数字签名方案 Σ 的完备性和一致性是满足的 (否则, 根据必要性的证明, 定理得证), 我们证明 Σ 的不可伪造性不满足。

令 B 表示在 π_{Σ} 和在 Z 以及 A 一起执行的过程中发生的事件: 某个参与实体 V 被消息 $(\text{Verify}, \text{sid}, ID, m, \sigma, v)$ 激活, $v(ID, m, \sigma) = 1$, T 和 I 均未被入侵, 而身份为 ID 的实体 I 从未对消息 m 进行过签名操作。那么对于上面构造的理想敌手 S , 我们可以看到只要事件 B 不发生, 那么 Z 的关于其和 π_{Σ} 与 A 交互的视图和关于其和 F_{IBS} 与 S 交互的视图是统计不可区分的。然而, 由我们的反证假设, Z 能够以不可忽略的概率区分它是在和 π_{Σ} 与 A 交互, 还是在和 F_{IBS} 与 S 交互。因此, 当 Z 在和 π_{Σ} 以及 A 一起执行时, 事件 B 总是会以不可忽略的概率发生。

基于上面的结果, 我们可以构造一个伪造者 G 以不可忽略的概率成功伪造签名, 即 Σ 不满足不可伪造性。

G 的输入是由 EU-CMIA 实验所产生的验证算法 $\text{ver}(SP, \cdot, \cdot, \cdot)$, 另外 G 还可以访问私钥提取预言机和签名预言机。 G 运行上述环境 Z , 并为 Z 模拟与 A 和 π_{Σ} 的交互, 其中 G 扮演 T, I, V 和 F_{SMT} 的角色。

1) G 运行 A 的一个副本。

2) 当 Z 发送消息 $(\text{Setup}, \text{sid}, T)$ 给 T, G 扮演 T 返回 $(\text{VerAlgorithm}, \text{sid}, v)$, 其中 $v = \text{ver}(SP, \cdot, \cdot, \cdot)$ 。

3) 当 Z 发送消息 $(\text{Extract}, \text{sid}, ID, I, v')$ 给某个签名实体 I, G 询问其私钥提取预言机以获得身份 ID 对应的私钥。得到私钥 d_{ID} 后, 将 (ID, I, d_{ID}) 记录到列表 ID-Reg 中。 G 扮演签名实体 I 返回 $(\text{Extracted}, \text{sid}, ID, I)$ 。

4) 当 Z 发送消息 $(\text{Sign}, \text{sid}, ID, m)$ 给签名实体 I , 如果在列表 ID-Reg 中不存在 (ID, I, d_{ID}) , 则 G 扮演签名实体 I 返回一个出错信息。否则 G 询问其签名预言机以获得身份 ID 对消息 m 的签名 σ , 然后扮演 I 返回 $(\text{Signature}, \text{sid}, ID, m, \sigma)$ 。

5) 当 Z 指示入侵除 T 外的某个参与实体, G 返回那个实体的所有信息。如果 Z 指示入侵 T , 则 G 停机, 输出一个失败信息。

6) 当 Z 发送消息 $(\text{Verify}, \text{sid}, ID, m, \sigma, v')$ 给某个实体 V , G 检查 (ID, m, σ) 是否是一个伪造的签名 (即是否 ID 对应的私钥从未被提取过并且 ID 对 m 的签名从未被查询过并且 $\text{ver}(SP, ID, m, \sigma) = 1$)。如果 (ID, m, σ) 是一个伪造的签名, 那么 G 输出这个元组作为它伪造出来的签名并停机。否则, 它返回 $(\text{Verified}, \text{sid}, ID, m, v'(ID, m, \sigma))$ 并继续运行。

下面分析 G 成功的概率。从 A 和 Z 的角度看, 与 G 的交互与在现实模型中与协议 π_{Σ} 的交互是相同的, 除非 T 被入侵。注意到事件 B 只可能在 T 被入侵之前发生, B 发生的概率是不可忽略的, 所以 G 会以不可忽略的概率成功伪造签名。这与 Σ 是 EU-CMIA 安全的相矛盾。

综合上述充分性和必要性的证明, 我们得出结论: 基于身份数字签名方案的 UC 安全性定义和传统的 EU-CMIA 安全性定义是等价的。

4 结语

本文研究了基于身份数字签名方案的通用可组合安全性, 定义了基于身份数字签名方案的理想功能。通过将一个基于身份的数字签名方案转化为一个签名协议, 证明了基于身份数字签名方案的 UC 安全性定义和传统的 EU-CMIA 安全性定义之间的等价性。结果表明, 满足 EU-CMIA 安全性定义的基于身份的数字签名方案可以安全地应用于更复杂的密码协议的构造。

参考文献:

- [1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// CRYPTO'84: Proceedings of the Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, 1984: 47-53.
- [2] CHA J C, CHEON J H. An identity-based signature from gap Diffie-Hellman groups [C]// PKC 2003: Proceedings of Public Key Cryptography. Berlin, Heidelberg: Springer-Verlag, 2003: 18-30.
- [3] GOLDWASSER S, MICALI S, RIVEST R L. A digital signature scheme secure against adaptive chosen-message attacks [J]. SIAM Journal on Computing, 1988, 17(2): 281-308.
- [4] BELLARE M, NAMPREMPRE C, NEVEN G. Security proofs for identity-based identification and signature schemes [C]// Eurocrypt 2004: Proceedings of the Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, 2004: 268-286.
- [5] PATERSON K G, SCHULDT J C N. Efficient identity-based signatures secure in the standard model [C]// Proceedings of ACISP 2006. Berlin, Heidelberg: Springer-Verlag, 2006: 207-222.
- [6] CANETTI R. Universally composable security: A new paradigm for cryptographic protocols [C]// Proceedings of the 42nd IEEE Annual Symposium on Foundations of Computer Science. Washington, DC: IEEE Computer Society, 2001: 136-145.
- [7] CANETTI R, DODIS Y, PASS R, et al. Universally composable security with global setup [C]// Proceedings of the Theory of Cryptography Conference. Berlin, Heidelberg: Springer-Verlag, 2007: 61-85.
- [8] CANETTI R, KUSHILEVITZ E, LINDELL Y. On the limitations of universally composable two-party computation without set-up assumptions [J]. Journal of Cryptology, 2006, 19(2): 135-167.
- [9] DATTA A, DEREK A, MITCHELL J C, et al. Games and the impossibility of realizable ideal functionality [C]// Proceedings of the Theory of Cryptography Conference. Berlin, Heidelberg: Springer-Verlag, 2006: 360-379.
- [10] HORVITZ O, KATZ J. Universally composable two-party computation in two rounds [C]// CRYPTO 2007: Proceedings of the Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, 2007: 111-129.
- [11] CANETTI R. Universally composable security: A new paradigm for cryptographic protocols [EB/OL]. [2010-02-20]. <http://eprint.iacr.org/2000/067.pdf>.

(下转第 126 页)

$MTTSF$ 表达式是一个关于 w_0 的减函数,这个结论是非常重要的。它表明:一个入侵容忍系统搭建好之后,它的安全性量化结果应该是动态变化的而不是固定不变的,这里参数 w_0 正反映这样的变化,动态地反映在 $MTTSF$ 的计算结果当中,同时可以通过调整 w_0 来控制一个系统的容侵能力。在量化过程中, w_0 反映的只是数值上的变化,实际上它代表着系统所处环境的变化过程:提供在线服务的时间越长,系统漏洞暴露的就越多,攻击者的攻击能力就越强,攻击工具可用性也越来越高等,所以这个参数体现出系统所处环境的变化。虽然这个参数目前还无法准确地量化这些因素的影响,但是它的确反映出一个人入侵容忍系统的安全性是动态变化的。

3 模拟实验分析

现在假定对一个典型的 SITAR 系统进行模拟实验分析,并通过分别改变各个参数,考查系统安全性量化结果在不同攻击速度下的变化。假定该 SITAR 系统配备了代理服务器、选举服务器和接受测试服务器各 4 个,以及 1 个审计单元和 1 个自适应重构单元,其中所有组件都实现了多样性,即攻击者每入侵一个服务器所需要的时间代价都是相同的。该 SITAR 系统维持正常运行需要的最少代理服务器数为 3,自我修复一个被入侵的服务器平均时间为 2 个单位时间。假设各个参数为: $p_u = 0.1, h_i = 1/4$ 。图 6 表示的就是系统在 $\lambda = 1, \lambda = 2$ 下 SITAR 系统的 $MTTSF$ 下限值随 w_0 变化情况。

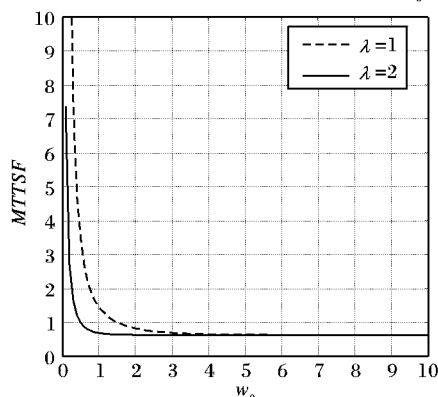


图 6 $MTTSF$ 下限值随 w_0 变化情况

从图 6 可以看出,随着 w_0 增大, $MTTSF$ 的值也在不断下降,最后趋于一个理论最小值。同时随着入侵速度 λ 的不断增大, $MTTSF$ 下限值的下降速度越来越快。当入侵的速度小于系统修复速度时,系统的 $MTTSF$ 值趋近于无穷大。

4 结语

本文主要对入侵容忍能力进行了量化分析,分析了系统

暴露窗口对安全性的影响。并以经典的入侵容忍系统 SITAR 为对象,进行了模拟实验和比较分析,验证了所提出的量化方法,并且重点探讨了暴露窗口对安全性量化结果的影响。最后的结论一方面反映了入侵容忍系统的安全性是随暴露窗口变化的,另一方面它对增强入侵系统的安全性提供了理论依据:如果系统能够通过各种技术手段恰当地设置服务器的暴露窗口,那么就能获取较大的 $MTTSF$,从而提高系统的安全性。当然在量化过程中,也存在不完善的地方,如:简化了攻击者的攻击能力^[8]和系统修复速度,所以最终的量化结果并不十分精确。这也是未来研究的主要方向,希望以后能建立更加准确的模型来实现更加精确的入侵容忍系统的安全性量化计算。

参考文献:

- [1] MADAN B M, GOŠEVA-POPSTOJANOVA K, VAIDYANATHAN K, *et al.* A method for modeling and quantifying the security attributes of intrusion tolerant systems[J]. *Performance Evaluation*, 2004, 56(1/4): 167–186.
- [2] JONSSON E, OLOVSSON T. A quantitative model of the security intrusion process based on attacker behavior[J]. *IEEE Transactions on Software Engineering*, 1997, 23(4): 235–245.
- [3] NGUYEN Q, SOOD A. Quantitative approach to tuning of a time-based intrusion-tolerant system architecture[C]// WRAITS 2009: The 3rd Workshop on Recent Advances on Intrusion-Tolerant Systems. Lisbon, Portugal: Dependable Systems & Networks, 2009: 7–13.
- [4] GONG FANGMING, POPSTOJANOVA K G, WANG FEIYING, *et al.* Characterizing intrusion tolerant systems using a state transition model[C]// Proceedings of the DARPA Information Survivability Conference and Exposition. Washington, DC: IEEE, 2001: 38–45.
- [5] 周华, 孟相如, 张立, 等. 分布式入侵容忍系统的主动恢复算法研究[J]. *西安电子科技大学学报: 自然科学版*, 2009, 36(2): 378–384.
- [6] UEMURA T, DOHI T. Quantitative evaluation of intrusiontolerant systems subject to DoS attacks via semi-Markov cost model[C]// Proceedings of the 2007 Conference on Emerging Direction in Embedded and Ubiquitous Computing, LNCS 4809. Taipei, Taiwan: Springer-Verlag, 2007: 31–42.
- [7] Huang Jian-hua, Yang Tian-yang. A method for quantifying the security of intrusion tolerant systems[C]// CNMT 2009: International Symposium on Computer Network and Multimedia Technology. Washington, DC: IEEE, 2009: 1–4.
- [8] 黄建华, 杨天扬. 入侵容忍系统的安全性量化方法分析[J]. *信息网络安全*, 2009(7): 7–9.

(上接第 122 页)

- [12] NISHIMAKI R, MANABE Y, OKAMOTO T. Universally composable identity-based encryption [C]// Proceedings of Progress in Cryptology. Berlin, Heidelberg: Springer-Verlag, 2006: 337–353.
- [13] CANETTI R. Universally composable signature, certification, and authentication [C]// Proceedings of the Computer Security Foundations Workshop. Washington, DC: IEEE Computer Society, 2004: 219–245.
- [14] HARKINS D, CARREL D. The Internet key exchange[EB/OL]. [2010-02-10]. <http://tools.ietf.org/html/rfc2409>.
- [15] ZHU R W, YANG GUOMIN, WONG D S. An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices [J]. *Theoretical Computer Science*, 2007, 378(2): 198–207.
- [16] DORASWAMY N, HARKINS D. IPSec: the new security standard for the Internet, Intranets and Virtual Private Networks [M]. 2nd Edition. London: Prentice Hall PTR, 2003.
- [17] LEEA J S, CHANG C C. Secure communications for cluster-based Ad Hoc networks using node identities[J]. *Journal of Network and Computer Applications*, 2007, 30(4): 1377–1396.