基于 Authentication Test 方法的高效安全 IKE 形式化设计研究

蒋 睿[1)] 胡爱群[1)] 李建华[2)]

[1)](东南大学无线电工程系 南京 210096)

[2)](上海交通大学电子工程系 上海 200030)

摘 要 基于 Authentication Test 方法,围绕高效安全 Internet 密钥交换(ESIKE)协议的安全目标,提出一种具体地构建唯一满足两个通信实体变换边的形式化协议设计方法,设计出了高效安全的 IKE 协议;并且基于 Strand Space 模型和 Authentication Test 方法,形式化分析 ESIKE 协议,证明了其所具有的安全特性.该 ESIKE 协议克服了原有 Internet 密钥交换(IKE)协议存在的安全缺陷,提供了安全的会话密钥及安全关联(SA)协商,保护了通信端点的身份,并且保证了协议发起者和响应者间的双向认证.同时,ESIKE 仅需 3 条消息及更少的计算量,更加简单、高效.

关键词 协议设计;形式化方法;Authentication tests;密钥交换;Strand space 模型

中图法分类号 TP309

Research on Formal Design of ESIKE Based on Authentication Tests

JIANG Rui[1)] HU Ai-Qun[1)] LI Jian-Hua[2)]

[1)](*Department of Radio Engineering, Southeast University, Nanjing* 210096)

[2)](*Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai* 200030)

Abstract Based on the authentication tests, this paper presents a concrete formal protocol design approach, which constructs the only transforming edge between the two communication entities, to create an Efficient and Secure Internet Key Exchange (ESIKE) protocol according to the security goals of the ESIKE protocol. Then the secure properties of ESIKE are formally proved with the strand space model and the authentication tests. The ESIKE protocol overcomes the security shortages of the Internet Key Exchange (IKE), and can provide secure negotiation of session key and Security Association (SA), protection of endpoints' identities, and mutual authentication between the initiator and the responder. It needs only three messages and less computational load, and it is simple and efficient.

Keywords protocol design; formal method; authentication tests; key exchange; strand space model

1 引 言

Internet 密钥交换(Internet Key Exchange, IKE)协议是由 Internet 团体开发的一个密钥交换协议,其详细的描述可参见 RFC2409[1].其设计的主要目的是为 ISAKMP[2] 和 IPSec 的 AH, ESP 等安全服务建立安全关联(SA)及获得认证所需的会话密钥

收稿日期:2005-12-10;修改稿收到日期:2006-06-01.本课题得到国家"八六三"高技术研究发展计划项目基金(2003AA142160)资助和国家 115 科研基金(P2006014EA)资助.蒋 睿,男,1968 年生,博士,讲师,主要研究方向为计算机网络安全、下一代无线通信网安全.E-mail: R. Jiang@seu.edu.cn.胡爱群,男,1964 年生,博士,教授,博士生导师,主要研究领域为无线网络安全、信号处理、无线多媒体通信.李建华,男,1965 年生,博士,教授,博士生导师,主要研究领域为信息安全、宽带多媒体通信.

素材. 它的运行分成两个阶段. 阶段 1 建立一个 ISAKMP 的安全关联 SA，并导出用于保护第二阶段通信的共享会话密钥. 阶段 2 为 IPSec 协商安全关联并产生新鲜的密钥素材. 此外，Internet 密钥交换协议还定义了三种基本的交换模式：其中主模式(main mode)和野蛮攻击模式(aggressive mode)应用于阶段 1，快速模式(quick mode)应用于阶段 2.

然而，IKE 存在着许多安全缺陷. Meadows[3] 应用 NRL 协议分析器指出阶段 1 中，对于野蛮攻击模式中的数字签名方案，存在着身份认证的攻击；并且对于阶段 2 中的快速模式，存在着反射攻击. Zhou 在文献[4]中指出阶段 1 的主模式中存在着对 ISAKMP 安全关联认证的攻击；在文献[5]中指出主模式数字签名方案中身份保护的失效、主模式预共享密钥方案中无法支持漫游用户的缺陷以及主模式公钥加密方案中证书应用的缺陷. Perlman 和 Kaufman[6] 则指出 IKE 太复杂，其中的第二阶段应当除去；IKE 的规范太复杂、困难以至无法理解，并且对于某些模式仅能隐藏一个通信端点的身份. Aiello等人[7] 则提出了一个新的密钥交换协议，命名为 JFK(Just Fast Keying)，来克服 IKE 的诸如消息交换回合过多、协议和规范太过复杂的不足. 而至今 IKE 的升级版 IKEv2[8] 草案仍在设计修改之中.

在另一方面，对于密码协议设计的研究也已有了一定的发展. 然而，一系列的协议设计研究工作诸如 Abadi 和 Needham 的工作[9] 似乎仅依靠设计者的技巧和独创性，却没有提出一个基本的理论来指导密码协议的设计，并以此确保协议目标的正确实现. Woo 和 Lam[10] 则致力于从低效“全信息”协议中安全地除去信息. 他们的方法存在着两大局限性：其一对于如何构建一个能获得设计目标的全信息协议没有指导；其二所谓安全除去信息的准则似乎是无力的. Buttyan 等人[11] 描述了一个类 BAN 逻辑来推动密码协议的设计，但似乎很难从他们给出的示例中抽象出一种方法. 基于 Strand Space 模型[12] 及 Authentication Test 方法[13]，Guttman[14] 描述了一种抽象的协议设计架构，并给出了示例说明如何设计基于 Authentication test 的安全电子商务交易协议(ATSPECT)的思路. 而 Perrig 和 Song 采用他们自己的、与 Authentication Test 方法相关的自动协议发生器 APG[15]，生成了三方认证密钥交换协议的候选协议，然后调用 Athena[16] 应用 Strand Space 模型过滤这些协议，从而声称获得了符合规范要求的合适协议.

本文基于 Strand Space 模型及 Authentication Test 方法，提出一种具体的形式化协议设计方法，从而设计出高效安全 Internet 密钥交换协议(ES-IKE). 本文所提出的形式化协议设计方法是一种具体的方法，而不是文献[14]中所述的抽象架构；并且由于该方法简单、高效，从而避免了文献[15,16]中的无限状态搜索问题. 所设计的 ESIKE 协议可以安全地保护会话密钥和安全关联 SA 的协商，安全地保护通信端点的身份，可获得协议发起者和响应者间的双向认证，并且可以防止上述对于 IKE 的攻击. 此外，ESIKE 协议仅包含 3 条消息，舍弃了 IKE 中的第二阶段，并且仅需更少的计算量，因而比 IKE，JFK 和 IKEv2(草案)更高效.

本文第 2 节提出 ESIKE 协议的安全目标；第 3 节基于 Authentication Test 方法，提出密码协议设计的形式化方法，一步一步设计出 ESIKE 协议；第 4 节基于 Strand Space 模型及 Authentication Test 方法形式化分析 ESIKE 协议，证明其安全有效性；对 ESIKE 协议效率的讨论见第 5 节；最后总结全文.

2　ESIKE 协议设计目标

如引言所述，引起 IKE 安全缺陷的原因在于不安全的安全关联 SA 及会话密钥协商、通信端点身份的泄露以及缺乏协议发起者和响应者间的双向认证. 因此，ESIKE 协议设计的安全目标必须能够克服上述缺陷，提供协议发起者和响应者间的双向认证，提供安全的会话密钥及 SA 协商，同时保护通信双方的身份以确保通信双方交互中特定信息的机密性. 此外，ESIKE 协议必须使用尽量少的信息交互及更少的计算量.

2.1　协议的参与实体

协议的参与实体在协议中通常扮演两个不同的角色，典型的有客户机和服务器，或可称之为发起者和响应者. 本章中的两个协议参与实体分别称为 I 和 R. 协议中诸如实体的身份、安全关联 SA 及会话密钥等秘密数据，对于协议实体之外的第三方必须保证其机密性.

同样的实体在不同的协议运行过程中可能扮演不同的角色. 当不同的客户机相互提供服务的时候，它们变换着执行不同的角色 I 和 R.

2.2　协议的设计目标

对于协议的参与实体，其安全目标可分为以下 4 类：

(1) 机密性. 所有的重要数据,比如实体的身份、安全关联 SA 以及会话密钥信息,在协议交互传输过程中必须保证机密性,即这些仅由协议双方共享的数据不能泄露给任何的第三方.

(2) 认证特性 1. 每一实体 I 必须收到一个保证,保证每一个通信对方 R 已经收到了 I 发送的数据并且该数据已经得到 R 的认可.

(3) 认证特性 2. 每一个实体 R 必须收到一个保证,保证据称从通信实体 I 发送来的数据事实上起源于实体 R,以确保该数据在最近协议运行中的新鲜性.

(4) 效率. 协议必须在信息交换的数量、通信中所需的计算量以及所需消耗的带宽等方面具有较高的效率.

3 ESIKE 协议的设计

本节首先简要介绍基于 Strand Space 模型的 Authentication Test 方法[13]的基本思路,然后提出具体的密码协议形式化设计方法,一步一步地设计出满足 2.2 节安全目标的 ESIKE 协议. 有关 Strand Space 模型理论的基本概念参见文献[12].

3.1 Authentication Test 方法基本思路

固定一些 Strand Space Σ,可以识别对于测试有用的正常 Strands 片段,这些正常 Strands 片段的出现将保证其他正常 Strands 存在于同一 bundle 中,这就是 Authentication Test 的目的所在. 有三种测试,分别为出测试(outgoing test)、入测试(incoming test)和未经请求测试(unsolicited test). 其中入测试和出测试能保证崭新性,相比而言未经请求测试无法保证崭新性.

Authentication Test 方法中隐含了协议设计的思路. 在抽象的层次上,认证协议的设计可以看作一个选择 Authentication Test,并且构建一个唯一满足两个实体的变换边的过程. 本节的后续部分将围绕具体 ESIKE 协议的安全目标,选择 Authentication Test 来完成这一密码协议的设计. 关于 Authentication Test 的基本概念参见文献[13,14].

3.2 假设及符号表示

本节合理地假设每一通信实体至少具有一个公钥和私钥对. 公钥用来加密消息和验证签名,私钥用来解密信息和签名消息. 假设所有实体的公钥可通过公钥基础设施可靠地得以确定.

实体 I 具有公共加密密钥 K_I,用 $\{|t|\}_I$ 表示 $\{|t|\}_{K_I}$(由 K_I 加密的信息 t). 假设 K_I^{-1} 不泄露(即 $K_I^{-1}\in S$),则仅由 I 才能从加密的信息中恢复 t. 同样,实体 I 具有秘密签名密钥 S_I,用 $[\![t]\!]_I$ 表示 $\{|t|\}_{S_I}$(由 S_I 签名的信息 t),则仅由实体 I 才能由新的信息 t 构建 $[\![t]\!]_I$.

本节引入密码学原函数 $h(x)$,其为一单向 Hash 函数. $h(t)$ 表示对消息 t 的 Hash 函数值. 假设没有实体能找到一对值 t_1,t_2 使得 $h(t_1)=h(t_2)$ 成立,或对于给出的 v 能找到 t 使得 $h(t)=v$ 成立.

3.3 负载及机密性

ESIKE 协议设计的目的在于产生安全的会话密钥,保护通信双方的身份,完成 IPSec 通信所需的安全关联 SA 协商以及获得两通信实体间的双向认证. 因此,根据 2.2 节所述的安全目标,本节规定了用作负载的一系列信息元以确保 ESIKE 协议满足上述要求. 这些负载信息元描述如下.

SA_I:协议发起者 I 希望建立的安全关联 SA 及其密码学业务特性.

SA_R:协议响应者 R 回应发起者 I 的安全关联 SA 信息(即 IPSec 中的响应者的 SPI 信息等).

N_I:发起者的新鲜性参数,一个随机比特串.

N_R:响应者的新鲜性参数,一个随机比特串.

KE_I:发起者的当前 Diffie-Hellman(DH)指数.

KE_R:响应者的当前 Diffie-Hellman(DH)指数.

ID_I:发起者的证书或公钥标识信息.

ID_R:响应者的证书或公钥标识信息.

$h(M)$:消息 M 的 Hash 值. 其同时隐含 $h(x)$ 为一消息认证码(MAC)函数.

为了确保 ESIKE 协议的机密性目标要求,在通信过程中必须保证数据 $SA_I,SA_R,ID_I,ID_R,KE_I,KE_R$ 的安全性. 然后安全地导出会话密钥 $K_{IR}=H_{DH}(N_I,N_R)$,其中 $H_k(M)$ 为带密钥 k 的 Hash 函数值. 在 ESIKE 协议中,密钥 k 即为 DH 交换密钥,可由 KE_I 和 KE_R 导出.

3.4 ESIKE 协议的设计

本节将根据 ESIKE 的安全目标,基于 Authentication Test 方法,一步一步地设计出 ESIKE 协议.

(1) 协议机密性的获得

ESIKE 协议机密性的目标:所有在信息交换中传输的重要数据必须保证其机密性,并且由通信双方共享的数据不能泄露给任何第三方.

因此,数据 $SA_I,SA_R,ID_I,ID_R,KE_I,KE_R$ 在协议交互中传输时不能以明文的形式出现. 对于这些数据的传输必须以加密的形式出现,密钥可采用公

钥 K_I 或 K_R；或以单向 Hash 函数 $h(t)$ 的形式出现，其中 $h(x)$ 满足 3.2 节中的安全性假设.

(2) 认证特性 1 的获得

ESIKE 协议认证特性 1 的目标：每一个参与实体 I 应当收到一个保证，保证每一实体 R 已经收到 I 发送的数据并且该数据已经得到 R 的认可.

I 发送的数据即为数据 SA_I，ID_I 和 KE_I，必须以 $\{|SA_IKE_IID_I|\}_R$ 的形式在协议中传输. 由文献[13]中入测试可知，一个可以确保“认证特性 1”实现的方法为：发起者准备一新鲜性参数 N_I，并使之与 $\{|SA_IKE_IID_I|\}_R$ 一起传输；在收到和处理该单元后，响应者 R 返回一形式为 $[\![\cdots N_I\cdots]\!]_R$ 的认证消息，以证明 N_I 到达了 R 且作为一成功 strand 的一部分得到 R 的认可.

协议同时必须保证参数 N_I 伴随着负载 SA_I，ID_I 和 KE_I 一起得到处理. 因此，认证消息必须以 $[\![\cdots N_It]\!]_R$ 的形式出现，其中 t 包含了负载的某种形式. 特别地，为了保证负载的机密性，这些负载必须经加密运算或 Hash 运算. 本文在认证消息中采用 $h(SA_IKE_IID_I)$ 而不是加密元 $\{|SA_IKE_IID_I|\}_I$ 形式，以确保协议仅需更少的运算而更高效，因而可得认证消息的形式为 $[\![\cdots N_Ih(SA_IKE_IID_I)]\!]_R$. 整个处理过程可参见图 1. 显然，假设 R 的秘密签名密钥不泄露且 N_I 唯一产生，则对于发起者 I 的上述过程构成一个入测试.

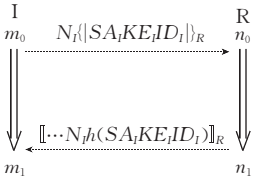


图 1　获得认证特性 1 的一组边

(3) 认证特性 2 的获得

ESIKE 协议认证特性 2 的目标：每一实体 R 必须收到一个保证，保证据称从通信实体 I 发送来的数据事实上起源于实体 R，以确保该数据在最近协议运行中的新鲜性.

为了获得这一认证目标，必须扩展图 1 的协议运行过程. 特别地，将产生 2 阶崭新性节点（文献[14]定义 2.2）. R 的数据即数据 SA_R，KE_R 和 ID_R，必须以 I 的公钥加密形式在协议交互过程中进行传输. 由入测试可知，一个可以保证对于 R 负载认证的方法为：由响应者 R 准备一新鲜性参数 N_R，并使之与 $\{|SA_RKE_RID_R|\}_I$ 一起传输. 合并对于 I 的认证消息和 R 本应发送的消息，因此，扩展图 1 中的协议交互在图 1 中认证消息的基础上增加由 R 发出的唯一新鲜性参数 N_R 及 R 的秘密数据 $\{|SA_RKE_RID_R|\}_I$. 因而消息具有 $[\![\{|SA_RKE_RID_R|\}_IN_RN_Ih(SA_IKE_IID_I)]\!]_R$ 的形式. 在收到并处理过该单元后，发起者 I 用新鲜的证书对于 N_I，N_R 及 Hash 负载进行签名，得到的消息形式为 $[\![N_IN_Rh(SA_IKE_IID_ISA_RKE_RID_R)]\!]_I$. 这样的变换边在假设 I 的私密签名密钥不泄露的情况下，完成了对于响应者 R 的一个入测试. 参见图 2 中下面的矩形部分（从右向左）.

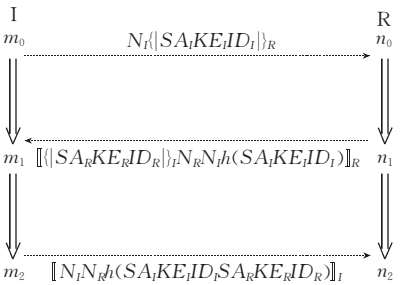


图 2　获得认证特性 2 的一组边

实体 R 知道签名消息 $[\![N_IN_Rh(SA_IKE_IID_ISA_RKE_RID_R)]\!]_I$ 是在 N_R 产生后才生成的. 并且，若实体 I 运行正常，则该签名消息一定发送于促发新鲜性参数 N_I 产生的通信回合. 这样，节点 m_2 对于节点 n_2 是崭新的，且节点 m_0 对于节点 m_2 是崭新的. 因此，节点 m_0 对于节点 n_2 是 2 阶崭新的.

经过上述步骤可得出基于 Strand Space 模型及 Authentication Test 方法设计的 ESIKE 协议，该协议的详细描述参见图 3. 其中 $\{M\}_{K_R}$ 和 $\{M\}_{K_I}$ 分别表示消息 M 由公钥 K_R 和 K_I 进行加密. $\{M\}_{S_I}$ 表示签名消息对 $(M,Sig_{S_I}(M))$，其中 $Sig_{S_I}(M)$ 表示消息 M 用私密密钥 S_I 生成的签名. $\{M\}_{S_R}$ 的含义与 $\{M\}_{S_I}$ 相同，只是其中的私密密钥为 S_R. 该 ESIKE 协议中，发起者和响应者之间仅由 3 条消息完成安全关联 SA 的协商，获得共同的会话密钥（由 KE_I，KE_R，N_I 和 N_R 导出），保证身份信息等重要数据的机密性，并且获得相互间的双向认证.

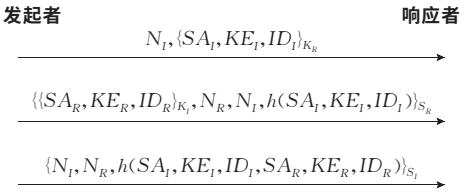


图 3　ESIKE 协议

4　ESIKE 协议的形式化证明

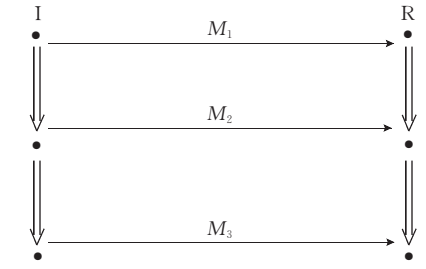
本节基于 Strand Space 模型理论及 Authenti-

cation Test 方法形式化分析 ESIKE 协议，证明其满足协议设计的安全目标.

根据 Strand Space 模型理论的要求，ESIKE 协议形式化为包含两类正常的 strands，详细的描述见图 4.

(1) 发起者的 strands，其迹为 $\langle +M_1, -M_2, +M_3 \rangle$. 其中 $ID_I, ID_R \in T_{name}$，$N_I, N_R, KE_I, KE_R, SA_I, SA_R \in T$，但是 $N_I, KE_I, SA_I \notin T_{name}$；$K_I, K_R \in K$ 为公钥用于加密，$S_I, S_R \in K$ 为私钥用于签名，$K_I^{-1}, K_R^{-1} \in K$ 为私钥用于解密. $Init[N_I, N_R, SA_I, SA_R, KE_I, KE_R, ID_I, ID_R]$ 表示具有上述迹的所有 strands 集.

(2) 响应者的 strands，其迹为 $\langle -M_1, +M_2, -M_3 \rangle$. 其中 $ID_I, ID_R \in T_{name}$，$N_I, N_R, KE_I, KE_R, SA_I, SA_R \in T$，但是 $N_R, KE_R, SA_R \notin T_{name}$；$K_I, K_R \in K$ 为公钥用于加密，$S_I, S_R \in K$ 为私钥用于签名，$K_I^{-1}, K_R^{-1} \in K$ 为私钥用于解密. $Resp[N_I, N_R, SA_I, SA_R, KE_I, KE_R, ID_I, ID_R]$ 表示具有上述迹的所有 strands 集.



这里 $M_1 = N_I\{|SA_IKE_IID_I|\}_{K_R}$

$M_2 = \{|\{|SA_RKE_RID_R|\}_{K_I} N_R N_I h(SA_IKE_IID_I)|\}_{S_R}$

$M_3 = \{|N_I N_R h(SA_IKE_IID_ISA_RKE_RID_R)|\}_{S_I}$

图 4 ESIKE 协议中的正常 bundle

以下命题针对 ESIKE 协议以命题的形式阐述协议的目标，证明协议发起者和响应者可以安全地共享会话密钥，安全地协商安全关联 SA，保护相互的身份不泄露，同时获得相互间的双向认证.

命题 1(实体 I 数据的机密性). 假设 $\mathcal{C}$ 为 $\sum$ 中的一个 bundle，$ID_I, ID_R \in T_{name}$；$K_R^{-1} \notin K_P$；同时 $\mathcal{C}$ 包含发起者 strand $s \in Init[N_I, N_R, SA_I, SA_R, KE_I, KE_R, ID_I, ID_R]$ 且其 $\mathcal{C}$-$height$ 为 3. 若 $S_1 = \{SA_I, KE_I, ID_I\}$ 唯一产生，则对于任何节点 $n \in \mathcal{C}$，可得 $term(n) \notin S_1$.

证明. 采用反证法. 设 k 为不安全密钥集的逆集，即 $k = (K \backslash S)^{-1}$，其中 S 为安全密钥集. 设 π 为 $S_1 \cup S$，即 $\pi = S_1 \cup S$.

由文献[12]诚实理想子环推论 6.12 可知，若存在节点 $m \in \mathcal{C}$ 且 $term(m) \in S_1$，因而 $term(m) \in I_k[\pi]$，则一定存在正常节点 $n \in \mathcal{C}$，且 n 为 $I_k[\pi]$ 的登入点. 然而，检查 $\sum$ 中 bundle 的正的正常节点(参见图 4)，没有发现任何 π 集中的元素在协议中被发送，被发送的数据要么是由 K_R 加密保护的数据(形式为 $\{|SA_IKE_IID_I|\}_{K_R}$)，其相应的解密私钥根据假设 $K_R^{-1} \notin K_P$ 是安全的；或者是由单向 Hash 函数保护的数据(形式为 $h(SA_IKE_IID_I)$ 和 $h(SA_IKE_IID_ISA_RKE_RID_R)$)，其中根据 3.2 节的假设，任何人无法从 $h(t) = v$ 中得到 t. 因此，与 $term(m) \in S_1$ 的假设相矛盾. 所以，对于任何节点 $n \in \mathcal{C}$，$term(n) \notin S_1$. 证毕.

命题 1 证明了 ESIKE 协议中由 I 发送的秘密数据 $S_1 = \{SA_I, KE_I, ID_I\}$ 不可能泄露给其他任何第三方，除非攻击者获得实体 R 的私钥，即 $K_R^{-1} \in K_P$.

命题 2(实体 R 数据的机密性). 假设 $\mathcal{C}$ 为 $\sum$ 中的一个 bundle，$ID_I, ID_R \in T_{name}$；$K_I^{-1} \notin K_P$；同时 $\mathcal{C}$ 包含响应者 strand $s \in Resp[N_I, N_R, SA_I, SA_R, KE_I, KE_R, ID_I, ID_R]$ 且其 $\mathcal{C}$-$height$ 为 3. 若 $S_1 = \{SA_R, KE_R, ID_R\}$ 唯一产生，则对于任何节点 $n \in \mathcal{C}$，可得 $term(n) \notin S_1$.

证明. 同样采用反证法. 设 k 为不安全密钥集的逆集，即 $k = (K \backslash S)^{-1}$，其中 S 为安全密钥集. 设 π 为 $S_1 \cup S$，即 $\pi = S_1 \cup S$.

根据文献[12]诚实理想子环推论 6.12 可知，若存在节点 $m \in \mathcal{C}$ 且 $term(m) \in S_1$，因而 $term(m) \in I_k[\pi]$，则存在正常节点 $n \in \mathcal{C}$，且 n 为 $I_k[\pi]$ 的登入点. 然而，检查 $\sum$ 中 bundle 的正的正常节点(参见图 4)没有发现任何 π 集中的元素在协议中被发送，被发送的数据要么是由 K_I 加密保护的数据(形式为 $\{|SA_RKE_RID_R|\}_{K_I}$)，其相应的解密私钥根据假设 $K_I^{-1} \notin K_P$ 是安全的；或者是由单向 Hash 函数保护的数据(形式为 $h(SA_IKE_IID_ISA_RKE_RID_R)$)，其中根据 3.2 节的假设，任何人无法从 $h(t) = v$ 中得到 t. 因此，与 $term(m) \in S_1$ 的假设相矛盾. 所以，对于任何节点 $n \in \mathcal{C}$，$term(n) \notin S_1$. 证毕.

命题 2 证明了 ESIKE 协议中由 R 发送的秘密数据 $S_1 = \{SA_R, KE_R, ID_R\}$ 不可能泄露给其他任何第三方，除非攻击者获得实体 I 的私钥，即 $K_I^{-1} \in K_P$.

命题 3(认证特性 1). 假设 $\mathcal{C}$ 为 $\sum$ 中的一个 bundle，$ID_I, ID_R \in T_{name}$；$S_R \notin K_P$；同时 $\mathcal{C}$ 包含发起者 strand $s \in Init[N_I, N_R, SA_I, SA_R, KE_I, KE_R,$

ID_I, ID_R]且其 $\mathcal{C}$-*height* 至少为 2. 若 N_I 唯一产生，则 $\mathcal{C}$ 一定拥有一匹配的响应者 strand $s' \in Resp[N_I, N_R, SA_I, SA_R, KE_I, KE_R, ID_I, ID_R]$ 且其 $\mathcal{C}$-*height* 至少为 2.

证明. 由图 4 首先可以确定 s 的第一和第二节点对于 N_I 构成一入认证测试. 由于 $\{|\{|SA_R KE_R ID_R|\}_{K_I} N_R N_I h(SA_I KE_I ID_I)|\}_{S_R}$ 为位于节点 $\langle s,2\rangle$ 的对于 N_I 的一个测试组元，因其包含 N_I 且无正常节点以该形式的项作为合适子项. 由假设条件 $S_R \notin K_P$，则根据文献[13]中定义 14 可得 $\langle s,1\rangle \Rightarrow^+ \langle s,2\rangle$ 对于 $\{|\{|SA_R KE_R ID_R|\}_{K_I} N_R N_I h(SA_I KE_I ID_I)|\}_{S_R}$ 中的 N_I 构成一入测试.

根据文献[13]中 Authentication Test 2(入测试)的要求，必定存在正常节点 $n_0, n_1 \in \mathcal{C}$，使得 $\{|\{|SA_R KE_R ID_R|\}_{K_I} N_R N_I h(SA_I KE_I ID_I)|\}_{S_R}$ 为节点 n_0 的一个组元且 $n_0 \Rightarrow^+ n_1$ 为对于 N_I 的一条变换边.

由于 n_1 为一正的正常节点且 $\{|\{|SA_R KE_R ID_R|\}_{K_I} N_R N_I h(SA_I KE_I ID_I)|\}_{S_R} = term(n_1)$，$N_I$ 在节点 $\langle s,1\rangle$ 处唯一产生，则一定存在一负节点 n_0 来接收 N_I. 由于 n_0 为一负节点，其一定位于某个响应者 strand $s' \in Resp[N_I, N_R, SA_I, SA'_R, KE_I, KE'_R, ID_I, ID'_R]$ 的节点 $\langle s',1\rangle$ 处. 由于 $\langle s',1\rangle \Rightarrow^+ \langle s',2\rangle$ 且 $term(\langle s',2\rangle) = \{|\{|SA_R KE_R ID_R|\}_{K_I} N_R N_I h(SA_I KE_I ID_I)|\}_{S_R}$，其中包含 $\{|SA_R KE_R ID_R|\}_{K_I}$，因此可知 $ID'_R = ID_R$，$SA'_R = SA_R$，$KE'_R = KE_R$. 所以 s' 的 $\mathcal{C}$-*height* 至少为 2. 证毕.

命题 3 证明了协议 ESIKE 中，当假设条件成立时，协议发起者能够获得对于响应者的安全认证. 此外，由于该方案包含对于 N_I 的入测试，因此根据文献[14]中的定义 2.1 可确保 N_I 的崭新性. 所以协议 ESIKE 的发起者可以防止恶意的重放攻击.

命题 4(认证特性 2). 假设 $\mathcal{C}$ 为 $\sum$ 中的一个 bundle，$ID_I, ID_R \in T_{name}$；$S_R, S_I \notin K_P$；同时 $\mathcal{C}$ 包含响应者 strand $s \in Resp[N_I, N_R, SA_I, SA_R, KE_I, KE_R, ID_I, ID_R]$ 且其 $\mathcal{C}$-*height* 为 3. 若 N_R 唯一产生，则 $\mathcal{C}$ 一定拥有一匹配的发起者 strand $s' \in Init[N_I, N_R, SA_I, SA_R, KE_I, KE_R, ID_I, ID_R]$ 且其 $\mathcal{C}$-*height* 为 3，同时 $\langle s,2\rangle \prec \langle s',2\rangle$.

证明. 由图 4 首先可以确定 s 的第二和第三节点对于 N_R 构成一入认证测试. 由于 $\{|N_I N_R h(ID_I ID_R SA_I SA_R KE_I KE_R)|\}_{S_I}$ 为位于节点 $\langle s,3\rangle$ 的对于 N_R 的一个测试组元，因其包含 N_R 且无正常节点以该形式的项作为合适子项. 由假设条件 $S_I \notin K_P$，则根据文献[13]中定义 14 可得 $\langle s,2\rangle \Rightarrow^+ \langle s,3\rangle$ 对于 $\{|N_I N_R h(ID_I ID_R SA_I SA_R KE_I KE_R)|\}_{S_I}$ 中的 N_R 构成一入测试.

根据文献[13]中 Authentication Test 2(入测试)的要求，必定存在正常节点 $n_0, n_1 \in \mathcal{C}$，使得 $\{|N_I N_R h(ID_I ID_R SA_I SA_R KE_I KE_R)|\}_{S_I}$ 为节点 n_0 的一个组元且 $n_0 \Rightarrow^+ n_1$ 为对于 N_R 的一条变换边.

由于 n_1 为一正的正常节点且 $term(n_1) = \{|N_I N_R h(ID_I ID_R SA_I SA_R KE_I KE_R)|\}_{S_I}$，$N_R$ 在节点 $\langle s,2\rangle$ 处唯一产生，则一定存在一负节点 n_0 来接收 N_R. 由于 n_0 为一负节点，其一定位于某个发起者 strand $s' \in Init[N_I, N_R, SA_I, SA'_R, KE_I, KE'_R, ID_I, ID'_R]$ 的节点 $\langle s',2\rangle$ 处，因而有 $\langle s,2\rangle \prec \langle s',2\rangle$. 由于 $\langle s',2\rangle \Rightarrow^+ \langle s',3\rangle$ 且 $term(\langle s',3\rangle) = \{|N_I N_R h(ID_I ID_R SA_I SA_R KE_I KE_R)|\}_{S_I}$，其中包含 ID_I, SA_I, KE_I 信息，因此可知 $ID'_R = ID_R$，$SA'_R = SA_R$，$KE'_R = KE_R$. 所以 s' 的 $\mathcal{C}$-*height* 为 3. 证毕.

命题 4 证明了协议 ESIKE 中响应者能够安全地认证发起者. 此外，由于 $\langle s,2\rangle \prec \langle s',2\rangle$，则节点 $\langle s',1\rangle$(其中信息 N_I, ID_I, SA_I 和 KE_I 在此产生)根据文献[14]中定义 2.2 对于节点 $\langle s,3\rangle$ 具有 2 阶崭新性. 具有 2 阶崭新性的协议同样能够确保协议响应者防止恶意的重放攻击.

至此，本文基于 Authentication Test 方法及 Strand Space 模型完成了 ESIKE 协议的设计，并基于上述理论形式化分析了所设计出的协议，证明了其所满足的安全目标. 以下将就 ESIKE 协议的效率进行进一步讨论说明.

5　ESIKE 协议的效率

在许多密码协议中，会话密钥在通信过程中需频繁地建立，因而往往成为影响通信效率的瓶颈. 因此密钥交换协议必须具有尽量少的信息交互，尽量少的计算量和尽量少地占用通信带宽. 尤其在不可靠的通信链路上，信息交换的数目往往是影响通信效率的最重要的一个因素. 采用 ESIKE 协议，仅需三条消息即可实现 IKE 的安全目标，这一点较现存的 IKE 协议、JFK 协议和 IKEv2 协议(草案)更为优越.

此外，ESIKE 协议舍弃了 IKE 协议运行两阶段的思路. 在 IKE 协议中，加入第二阶段的应用一般认为有着以下几个理由：首先是为安全关联 SA 产生现行的会话密钥素材，期望在一个连接中重复建立多个会话密钥过程中省去阶段 1 交互所需的开

销;第二个理由是允许周期性地更改会话密钥,期望仅需通信双方建立阶段 2 间的连接来实现会话密钥的更替,比之建立阶段 1 间的连接开销更少;第三个理由是允许同时建立多个具有不同安全业务要求的及不同会话密钥的通信连接. 然而,上述三条理由在实际的应用中都不易成立. 首先,对于第一个理由,通过 1 阶段协商产生会话密钥素材更有效;同时,采用两阶段协商来产生会话密钥素材并没有比执行两次 1 阶段交互的开销具有本质性地降低. 对于第二个理由,可采用更有效的底层加密算法如 AES 算法,就可避免频繁更换会话密钥这一情况. 只要 AES 算法的密钥长度足够,就能使得任何蛮力攻击失效. 同时,通过会话密钥的更替实现会话密钥的完美前向机密性,采用两阶段信息交换并没有比执行两次 1 阶段交换所需的开销本质性地降低. 对于第三个理由,首先该情况的出现仅是小概率事件,其次对于每一个应用建立不相关的安全关联 SA 比之采用两阶段方法更有效. 因此,本文在设计 ESIKE 协议时舍弃了 IKE 协议采用两阶段交互的做法,而直接采用一阶段的交互,这样就使得ESIKE协议更高效.

表 1 为 ESIKE,IKE,JFK 及 IKEv2(草案)计算量的比较,其中 C_{EXP},C_{HASH} 分别表示指数运算和 Hash 运算,I 和 R 分别表示协议的发起者和响应者.

表 1 ESIKE,IKE,JFK 及 IKEv2(草案)的计算量比较

Protocol	Computational Load	
	I	R
ESIKE	$2C_{EXP}+1C_{HASH}$	$2C_{EXP}+1C_{HASH}$
IKE*	$2C_{EXP}+5C_{HASH}$	$2C_{EXP}+5C_{HASH}$
JFK**	$3C_{EXP}$	$3C_{EXP}+1C_{HASH}$
IKEv2***	$2C_{EXP}+3C_{HASH}$	$2C_{EXP}+3C_{HASH}$

表 1 中,IKE* 为预共享密钥主模式协议,且仅包含协议阶段 1 的计算量;JFK** 为 JFK_r 协议;IKEv2***(草案)仅包含协议初始交换(相当于 IKE 阶段 1)的计算量. 可见,ESIKE 协议具有更少的计算量,因而更高效.

6 结束语

本文基于 Authentication Test 方法和 Strand Space 模型理论,提出了具体的密码协议形式化设计方法,并由此设计了高效安全的 Internet 密钥交换(ESIKE)协议. 首先基于 IKE 中存在的一些安全缺陷,确定了 ESIKE 协议的安全目标. 然后根据协议所需实现的安全目标,基于 Authentication Test 方法一步一步地完成了整个协议的设计. 最后基于 Strand Space 模型理论和 Authentication Test 方法形式化证明了 ESIKE 所需获得的安全设计目标. ESIKE 协议克服了 IKE 协议中存在的安全缺陷,同时提供对于会话密钥及安全关联 SA 的安全协商,提供了对于通信端点的身份保护,并且实现了协议发起者和响应者间的双向认证. 该协议仅需三条消息及更少的计算量,其实现更加简单高效.

参 考 文 献

1 Harkins D., Carrel D.. The Internet key exchange (IKE). RFC 2409. November 1998.

2 Maughan D., Schertler M., Schneider M., Turner J.. Internet security association and key management protocol (ISAKMP). RFC 2408, November 1998

3 Meadows C.. Analysis of the Internet key exchange protocol using the NRL protocol analyzer. In: Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, 1999, 216～231

4 Zhou J.. Fixing a security flaw in IKE protocols. Electronics Letters, 1999, 35(13): 1072～1073

5 Zhou J.. Further analysis of the Internet key exchange protocol. Computer Communications, 2000, 23: 1606～1612

6 Perlman R., Kaufman C.. Key exchange in IPSec: Analysis of IKE. IEEE Internet Computing, 2000, 4: 50～56

7 Aiello W., Bellovin S. M., Blaze M., Canetti R., Loannidis J., Keromytis A. D., Reingold O.. Efficient, DoS-resistant, secure key exchange for Internet protocols. In: Proceedings of the ACM CCS' 02, Washington, DC, USA, 2002, 27～39

8 Kaufman C.. Internet key exchange (IKEv2) protocol. Internet Draft, Internet Engineering Task Force, September 2005. Work in progress

9 Abadi M., Needham R.. Prudent engineering practice for cryptographic protocols. In: Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy, Oakland, CA, 1994, 122～136

10 Woo T. Y. C., Lam S. S.. A lesson on authentication protocol design. Operating Systems Review, 1994, 28: 24～37

11 Buttyan L., Staamann S., Wilhelm U.. A simple logic for authentication protocol design. In: Proceedings of the 11th IEEE Computer Security Foundations Workshop, Rockport, Massachusetts, 1998, 153～162

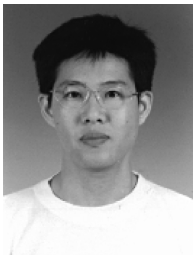
12 Fabrega F. J. T., Herzog J. C., Guttman J. D.. Strand spaces: Proving security protocols correct. Journal of Computer Security, 1999, 7(2/3): 191～230

13 Guttman J. D., Fabrega F. J. T.. Authentication tests and the structure of bundles. Theoretical Computer Science, 2002, 283(2): 333～380

14 Guttman J.. Security protocol design via authentication tests. In: Proceedings of the 15th IEEE Computer Security Foundation Workshop, Keltic Lodge, Canada, 2002, 92～103

15 Perrig A., Song D. X.. Looking for diamonds in the desert: Extending automatic protocol generation to three-party authentication and key agreement protocols. In: Proceedings of the 13th IEEE Computer Security Foundations Workshop, Cambridge, England, 2000, 64～76

16 Song D. X.. Athena: A new efficient automated checker for security protocol analysis. In: Proceedings of the 12th IEEE Computer Security Foundations Workshop, Mordano, Italy, 1999, 192～202



JIANG Rui, born in 1968, Ph. D.. His current research interests include computer network security and the next generation wireless network security.

HU Ai-Qun, born in 1964, Ph. D., professor, Ph. D. supervisor. His current research interests include wireless network security, signal processing and wireless multimedia communication.

LI Jian-Hua, born in 1965, Ph. D., professor, Ph. D. supervisor. His current research interests include information security and broadband multimedia communication.

Background

This work is supported by the National High Technology Research and Development Program (863 program) under grant No. 2003AA142160, and the National 115 Science Research Foundation under grant No. P2006014EA.

To design a security protocol is not easy. Many security protocols that seem correct have security shortages not easily discovered. Therefore, it is prone to be wrong for the design of security protocol. For example, some security protocols are designed by cryptographers with cryptography algorithm, and later, the fatal shortages are discovered in these protocols. By now, much work has been done on focusing to the analysis and validation of the security protocol. However, in the long-range development, it is of great importance to design a protocol which has no weakness and fits for the security requirements of the protocol at the beginning. For it can save the research cost, improve the research efficiency and avoid the afresh development.

Although the research on the security protocol design has the definite development, the theory and the method of the security protocol design have not been formed systemically and needed to improve further. Now, there are some quite succeed systems, such as Athena system and etc., which are based on the formal Strand Space model and the state searching technology, but they can not avoid the infinite states searching problem. Based on the BAN logic, some researches are done for the security protocol design, but it is difficult to gain a concrete method form the researches. Other informal protocol design methods only depend on the skill and creativity of the designers, and cannot propose a basic theory for security protocol design.

On the other hand, the Internet Key Exchange (IKE) has a lot of security weaknesses, too many rounds of information exchange, and the specifications are too complex to be understand. By now, the IKEv2 draft is still working in progress.

Under these circumstances, this paper does the research on the formal design of Efficient and Secure Internet Key Exchange (ESIKE) protocol based on the Strand Space model and the Authentication Test, and proposes a concrete formal protocol design approach, which constructs the only transforming edge between the two communication entities, to create the ESIKE protocol. The authors' method can avoid the infinite states searching problem, ensure the security properties of the designed protocol, improve the efficiency of IKE and give a heuristic way applied to the design of other security protocol.