IKE2 协议的安全性分析

沈海峰[1] 薛 锐[2] 黄河燕[1,3]
(中国科学技术大学计算机科学系 合肥 230026)[1] (中科院软件所信息安全国家重点实验室 北京 100080)[2]
(中科院计算机语言信息工程研究中心 北京 100083)[3]

摘 要 本文首先扩展了串空间的理想理论,然后应用此扩展理论分析 IKE2 协议的核心安全:秘密性和认证性。通过分析,证明了 IKE2 协议的密钥交换和认证安全性,但同时发现它不能在主动攻击模式下保护发起者身份,对此我们提出了一个修改意见。对 IKE2 的分析也为扩展串空间理论在复杂协议分析中的应用提供了一个实践基础。

关键词 安全协议,扩展串空间,理想,IKE2

Security Analysis of IKE2

SHENG Hai-Feng[1] XUE Rui[2] HUANG He-Yan[1,3]
(Dept. of Computer Science, USTC, Hefei 230026)[1] (The State Key Laboratory of Information Security, ISCAS, Beijing 100080)[2]
(Engineering Research Center of Computer Language Information, CAS, Beijing 100083)[3]

Abstract In this paper, we first extend the ideal theory of Strand Spaces, and then apply this extended theory to analyzing a complex Internet key exchange protocol, IKE2. We focus on this protocol's core security: keys' secrecy and authentication correctness. Through our analysis we prove that IKE2 can achieve its security goals in keys' secrecy and entity authentication. But IKE2 can't protect initiator's identity against active attack. We propose a modified main exchange of IKE2 for this bug. This analysis also gives a practical base for further application of extended Strand Spaces in analyzing complicated protocols which include plenty cryptographic primitives.

Keywords Security protocols, Extended strand spaces, Ideal, IKE2

1 引言

IKE2[5]是 IETF 新发布的 IKE 版本,其目的是取代先前发布的互联网解释域 (DOI, RFC 2407)[6]、ISAKMP (RFC 2408)[7]、IKE (RFC 2409)[8]标准,将三者统一为一个高效、简洁、安全的协议。尽管 IKE 还是当前的 IPsec 密钥交换标准,但众所周知,该协议存在着若干安全漏洞[10~12]。除了一些核心缺陷外,普遍认为 IKE 的三个主要缺陷是:①消息交换回合数多,易受拒绝服务攻击;②协议描述复杂;③可选项冗余,有些是毫无用处的。这使得 IKE 至今还没有形成可互操作的商业应用[9]。为了解决这些安全及应用问题,IETF 提出了 IKE2 协议(IKE2 还没有形成最终的标准文档,本文分析的是第 11 次修订版)。原始串空间理论[2~4]、包括文[1]在分析 IKE2 协议时都存在着缺点,主要表现在不能表达丰富的密码原语,例如签名和散列函数。因此,我们首先扩展串空间理论,然后运用该扩展串空间理论分析 IKE2 主交换协议的核心安全:秘密性和认证性。我们不讨论 IKE2 的辅助安全特性(如抵抗 DOS 攻击能力),文[5]已经在这方面给出了详细的阐述。

2 扩展串空间理论

2.1 入侵模型扩展

本节将对串空间的理想理论作必要的扩展以分析 IKE2。新增加的三个入侵串如下,记$(h)_K$表示用密钥 K 对 h 签名,$H_K(h)$表示密钥 k 控制下对 h 求散列值:

S_i 签名:$\langle -K,-h,+(h)_k\rangle, K\in \boldsymbol{K}, h\in \boldsymbol{A}$

V_e 验证:$\langle -K^{-1},-(h)_K,+h\rangle, K\in \boldsymbol{K}, h\in \boldsymbol{A}$

H_K HMAC 散列:$\langle -K,-h,+H_K(h)\rangle, K\in \boldsymbol{K}, h\in \boldsymbol{A}$

定义 2.1 A 中新定义两种运算:签名 $sign: \boldsymbol{K}\times \boldsymbol{A}\rightarrow \boldsymbol{A}$,HMAC 函数 $hmac: K\times \boldsymbol{A}\rightarrow \boldsymbol{A}$。$sign$ 的值域是 $\boldsymbol{S}$,$hmac$ 的值域是 $\boldsymbol{H}$。

公理 2.2 $\boldsymbol{K}\cap \boldsymbol{T}=\emptyset, \boldsymbol{B}\cap \boldsymbol{S}=\emptyset, \boldsymbol{B}\cap \boldsymbol{H}=\emptyset, \boldsymbol{B}\cap \boldsymbol{C}=\emptyset, \boldsymbol{B}\cap \boldsymbol{E}=\emptyset$($B$ 的定义见文[1])。

公理 2.3(自由加密假设) $\{m\}_K=\{m'\}_{K'}\Leftrightarrow m=m'\wedge K=K'$。

公理 2.4(自由签名假设) $(m)_K=(m')_{K'}\Leftrightarrow m=m'\wedge K=K'$。

公理 2.5(自由散列假设) $H_K(m)=H_{K'}(m')\Leftrightarrow m=m'\wedge K=K'$。

公理 2.6 对 $m_0, m'_0, m_1, m'_1\in \boldsymbol{A}, K, K'\in \boldsymbol{K}$。1) $m_0m_1=m'_0m'_1\Rightarrow m_0=m'_0\wedge m_1=m'_1$;2) $m_0m_1\neq\{m'_0\}_K, m_0m_1\neq(m'_0)_K, m_0m_1\neq H_K(m'_0)$;3) $m_0m_1\notin \boldsymbol{K}\cup \boldsymbol{T}\cup \boldsymbol{B}$;4) $\{m_0\}\notin \boldsymbol{K}\cup \boldsymbol{T}\cup \boldsymbol{B}, (m_0)_k\notin \boldsymbol{K}\cup \boldsymbol{T}\cup \boldsymbol{B}, H_K(m_0)\notin \boldsymbol{K}\cup \boldsymbol{T}\cup \boldsymbol{B}$。

2.2 理想概念

我们将文[2]中理想(ideal)的定义调整如下。

定义 2.7 设 $\kappa\subseteq \boldsymbol{K}, \kappa=\boldsymbol{ek}\cup \boldsymbol{sk}\cup \boldsymbol{hk}$,$\boldsymbol{ek}$ 为加密密钥,$\boldsymbol{sk}$ 为签名密钥,$\boldsymbol{hk}$ 为 HMAC 函数密钥。子集 $I\subseteq \boldsymbol{A}$ 称为 $\boldsymbol{A}$ 的 κ 理想(k-ide al),如果对所有的 $h\in I, g\in \boldsymbol{A}$,$I$ 满足下列条件:

沈海峰 博士生,研究方向为密码学和网络安全。薛 锐 研究员,主要研究领域为:理论密码学,密码协议分析,形式化方法在密码学中的应用。黄河燕 教授,博士生导师,主要从事人工智能、形式化方法和计算语言学的研究工作。

1)$hg, gh \in I$;2)$\{h\}_K \in I, K \in \boldsymbol{ek}$;3)$(h)_K \in I, K \in \boldsymbol{sk}$;4)$H_K(h) \in I, K \in \boldsymbol{hk}$。包含 h 的最小 κ 理想记为 $I_\kappa[h]$。

定义 2.8 如果 $g \in I_\kappa[h]$,则 h 是 g 的子项,记为 $h \sqsubset g$。

命题 2.9 $\sqsubset$ 是自反的、可传递的二元关系。而且如果 $h, g \in \boldsymbol{A}, K \in \boldsymbol{K}$,则:1)$h \sqsubset hg, g \sqsubset hg$;2)$h \sqsubset \{h\}_K, h \sqsubset (h)_K, h \sqsubset H_K(h)$。

证明:(1)自反性显然;传递性:设 $g \sqsubset g', g' \sqsubset h$,则 $g' \in I_K[g], h \in I_K[g']$,由于 $h \in I_K[g'] \subseteq I_K[g]$,所以 $g \sqsubset h$。(2)两个结论可由定义 2.7、2.8 直接得到。 □

公理 2.10 如果 t 是简单项且 $gh \in I_\emptyset[t]$,则 $g \in I_\emptyset[t]$ 或 $h \in I_\emptyset[t]$,$\emptyset$ 表示 κ 为空集。

公理 2.11 $\boldsymbol{K}$、$\boldsymbol{T}$、$\boldsymbol{E}$、$\boldsymbol{C}$、$\boldsymbol{S}$、$\boldsymbol{H}$ 两两互不相交。

定义 2.12 设 $\kappa \subseteq \boldsymbol{K}$,当且仅当 $g \in I_\kappa[h]$ 时,$h \in \boldsymbol{A}$ 称为 $g \in \boldsymbol{A}$ 的 k 子项,记为 $h \sqsubset_\kappa g$。

命题 2.13 $\sqsubset_\kappa$ 是自反的、可传递的二元关系,且 $h \sqsubset_\kappa g$ 蕴涵 $h \sqsubset g$。

定义 2.14 $I_\kappa[S]$ 是包含 S 的最小 κ 理想,其中 $S \subseteq \boldsymbol{A}$。

命题 2.15 如果 $S \subseteq \boldsymbol{A}$,则 $I_\kappa[S] = \bigcup_{x \in S} I_\kappa[x]$。

引理 2.16 若 $S_{i+1} = \{\{g\}_{sK}, (g)_{sK}, H_{hK}(g) \mid g \in I_\emptyset[S_i], eK \in \boldsymbol{ek}, sK \in \boldsymbol{sk}, hK \in \boldsymbol{hk}\}, \kappa = \boldsymbol{ek} \cup \boldsymbol{sk} \cup \boldsymbol{hk}, S_0 = S$,则 $I_\kappa[S] = \bigcup_i I_\emptyset[S_i]$。

命题 2.17 设 $S \subseteq \boldsymbol{A}, S$ 是简单项集合,如果 $gh \in I_\kappa[S]$,则 $g \in I_\kappa[S]$ 或 $h \in I_\kappa[S]$。

证明:根据引理 2.16,$\exists i.\ gh \in I_\emptyset[S_i]$,由命题 2.15 得 $\exists x.\ x \in S_i \wedge gh \in I_\emptyset[x]$。若 $i=0$,则 $S_i = S_0 = S, x$ 是简单项;若 $i>0$,则 $x \in S_i$ 有形式 $\{h\}_{sK}$ 或 $(h)_{sK}$ 或 $H_{hK}(h)$,也是简单项。所以按公理 2.10 有 $g \in I_\emptyset[x] \subseteq I_\kappa[S]$ 或 $h \in I_\emptyset[x] \subseteq I_\kappa[S]$。 □

命题 2.18 设某个 $K \in \boldsymbol{K}, \kappa \in \boldsymbol{K}, S \subseteq \boldsymbol{A}, \forall s \in S$ 是简单项且不具有形式 $\{h\}_K$、$(h)_K$ 和 $H_K(h)$,如果 $\{h\}_K \in I_\kappa[S]$ 或 $(h)_K \in I_\kappa[S]$ 或 $H_K(h) \in I_\kappa[S]$,则 $h \in I_\kappa[S]$。

证明:假设 $h \notin I_\kappa[S]$。①设 I' 是差集 $I_\kappa[S] \backslash \{\{h\}_K\}$。由于 $S \subseteq I'$,$\{h\}_K$ 非 ab 形式,所以 I' 满足理想条件 1;同时 $\forall h_1 \in I', K_1 \in \kappa \cdot \{h_1\}_{K_1} \neq \{h\}_K$,否则按公理 2.3 有 $h = h_1 \in I'$,与 $h \notin I_\kappa[S]$ 矛盾,故 I' 满足理想条件 2、3、4,I' 是包含 S 的理想。但 $I' \subset I_K[S]$ 与最小的理想 $I_\kappa[S]$ 矛盾,所以 $h \in I_\kappa[S]$。

②设 I' 是差集 $I_\kappa[S] \backslash \{(h)_K\}$。由于 $S \subseteq I', (h)_K$ 非 ab 形式,所以 I' 满足理想条件 1;同时 $\forall h_1 \in I', K_1 \in \kappa \cdot (h_1)_{K_1} \neq (h)_K$,否则按公理 2.3 有 $h = h_1 \in I'$,与 $h \notin I_\kappa[S]$ 矛盾,故 I' 满足理想条件 2、3、4,I' 是包含 S 的理想。但 $I' \subset I_K[S]$ 与最小的理想 $I_\kappa[S]$ 矛盾,所以 $h \in I_\kappa[S]$。

③设 I' 是差集 $I_\kappa[S] \backslash \{H_K(h)\}$。由于 $S \subseteq I', H_K(h)$ 非 ab 形式,所以 I' 满足理想条件 1;同时 $\forall h_1 \in I', K_1 \in \kappa \cdot H_{K_1}(h_1) \neq H_K(h)$,否则按公理 2.5 有 $h = h_1 \in I'$,与 $h \notin I_\kappa[S]$ 矛盾,故 I' 满足理想条件 2、3、4,I' 是包含 S 的理想。但 $I' \subset I_\kappa[S]$ 与最小的理想 $I_\kappa[S]$ 矛盾,所以 $h \in I_\kappa[S]$。 □

推论 2.19 设 $K \neq K'$,则①$\{h'\}_{K'} \sqsubset \{h\}_K \Rightarrow \{h'\}_{K'} \sqsubset h$,$\{h'\}_{K'} \sqsubset (h)_K \Rightarrow \{h'\}_{K'} \sqsubset h$,$\{h'\}_{K'} \sqsubset H_K(h) \Rightarrow \{h'\}_{K'} \sqsubset h$;②$(h')_{K'} \sqsubset (h)_K \Rightarrow (h')_{K'} \sqsubset h$,$(h')_{K'} \sqsubset \{h\}_K \Rightarrow (h')_{K'} \sqsubset h$,$(h')_{K'} \sqsubset H_K(h) \Rightarrow (h')_{K'} \sqsubset h$;③$H_{K'}(h') \sqsubset H_K(h) \Rightarrow H_{K'}(h') \sqsubset h$,$H_{K'}(h') \sqsubset \{h\}_K \Rightarrow H_{K'}(h') \sqsubset h$,$H_{K'}(h') \sqsubset (h)_K \Rightarrow H_{K'}(h') \sqsubset h$。

证明:①按定义 2.8 有 $\{h\}_K \in I_K[\{h'\}_{K'}]$,$(h)_K \in I_K[\{h'\}_{K'}]$,$H_K(h) \in I_K[\{h'\}_{K'}]$。由于 $K \neq K'$,按命题 2.15 有 $h \in I_K[\{h'\}_{K'}]$,所以 $\{h'\}_{K'} \sqsubset h$。②、③同理可证。 □

命题 2.20 设某个 $K \in \boldsymbol{K}, \kappa \subseteq \boldsymbol{K}, S \subseteq \boldsymbol{A}, \forall s \in S$ 是简单项且不具有形式 $\{h\}_K$、$(h)_K$ 和 $H_K(h)$,如果 $\{h\}_K \in I_\kappa[S]$ 或 $(h)_K \in I_\kappa[S]$ 或 $H_K(h) \in I_\kappa[S]$,则 $K \in \kappa$。

证明:由于 $\{h\}_K \notin S$、$(h) \notin S$、$H_k(h) \notin S$,故 $\{h\}_K \in I_\kappa[S] \backslash S, (h)_K \in I_\kappa[S] \backslash S, H_K(h) \in I_\kappa[S] \backslash S$。按公理 2.11,$\{h\}_K$、$(h)_K$、$H_K(h)$ 只能由加密、签名和散列函数得到,所以有 $\exists K_1 \in \kappa, h_1 \in I_\kappa[S] \cdot \{h_1\}_{K_1} = \{h\}_K$,$\exists K_1 \in \kappa, h_1 \in I_\kappa[S] \cdot (h_1)_{K_1} = (h)_K$,$\exists K_1 \in \kappa, h_1 \in I_\kappa[S] \cdot H_{K_1}(h_1) = H_K(h)$,按公理 2.3、2.4、2.5 得 $K_1 = K \in \kappa$。 □

2.3 诚实性理论

针对入侵者的 B_f 串 $\langle -x_1, \cdots, -x_n, +y = f(x_1, \cdots, x_n)\rangle$ 中的函数 f 有下面定义[1]。

定义 2.21 如果当函数 f 起源于丛 C 的入侵结点,原象 $(x_1, \cdots, x_n)$ 都是 B 类型入侵串,则 f 关于 $(x_1, \cdots, x_n)$ 是诚实函数。

定义 2.22 结点 n 是数据集 $I \subseteq \boldsymbol{A}$ 的入点,当且仅当 term(n) 是正号,term$(n) \in I$,而且对同一个串上 n 的任何前继 n' 有 term$(n') \notin I$。

定义 2.23 项集合 $I \subseteq \boldsymbol{A}$ 关于丛 C 是诚实的,当且仅当一个入侵结点 p 是 I 的入点时,p 是 M 结点,K 结点或 B 结点。

根据前面扩展的理想概念,我们能证明下面几个重要的定理和推论。

定理 2.24 设 C 是 $\boldsymbol{A}$ 上的丛,$S \subseteq \boldsymbol{T} \cup \boldsymbol{K} \cup \boldsymbol{B}, \kappa \subseteq \boldsymbol{K}, \boldsymbol{K} \subseteq S \cup \kappa^{-1}$。$f$ 是诚实函数,且当 $y = f(x_1, \cdots, x_n)$ 起源于入侵结点时,$y \in I_\kappa[S] \Rightarrow x_1, \cdots, x_n \in I_\kappa[S]$。则理想 $I_\kappa[S]$ 是诚实的。

证明:只证 S_i、V_e 和 HMAC 不是 $I_\kappa[S]$ 的入点,F、T、C、S、E、D、B_f 型入侵串不含 $I_\kappa[S]$ 的入点已在文[2,1]中证明。

S_i:$\langle -K, -h, +(h)_k\rangle$,$I_\kappa[S]$ 可能的入点是 $+(h)_K$。如果 $(h)_K \in I_\kappa[S]$,则根据命题 2.18,$h \in I_\kappa[S]$,这与入点定义矛盾。

V_e:$\langle -K^{-1}, -(h)_K, +h\rangle$,若 $+h$ 是 $I_\kappa[S]$ 的入点,则必须 $K^{-1} \notin I_\kappa[S]$,从而 $K^{-1} \notin S$,由于 $K^{-1} \in K \subseteq S \cup \kappa^{-1}$,所以 $K^{-1} \in \kappa^{-1} \Rightarrow K \in \kappa$,既 $(h)_K \in I_\kappa[S]$,这与入点定义矛盾。

H_K:$\langle -K, -h, +H_K(h)\rangle$,若 $+H_K(h)$ 是 $I_\kappa[S]$ 的入点,则必须 $K \notin I_\kappa[S]$,根据命题 2.18,$H_K(h) \in I_\kappa[S] \Rightarrow h \in I_\kappa[S]$,这也与入点定义矛盾。

综上所证,可得 $I_\kappa[S]$ 是诚实的。 □

与原始串空间理论[2]相比,这里 $I_\kappa[S]$ 是诚实的不仅表示该理想的秘密性,还可能表示它的不可伪造性。

推论 2.25 设 C 是 $\boldsymbol{A}$ 上的丛,$\boldsymbol{B} \cap \boldsymbol{K} = \boldsymbol{B} \cap \boldsymbol{T} = \emptyset, \boldsymbol{K} = (S \backslash \boldsymbol{B}) \cup \kappa^{-1}, S \cap \boldsymbol{K}_P = S \cap \boldsymbol{B}_P = \emptyset$。如果 term$(m) \in I_\kappa[S], m \in C$,则 C 上存在一个常规结点 n 是 $I_\kappa[S]$ 的入点。

推论 2.26 设 C 是 $\boldsymbol{A}$ 上的丛,$\boldsymbol{B} \cap \boldsymbol{K} = \boldsymbol{B} \cap \boldsymbol{T} = \emptyset, \boldsymbol{K} = (S \backslash \boldsymbol{B}) \cup \kappa^{-1}, S \cap \boldsymbol{K}_P = S \cap \boldsymbol{B}_P = \emptyset$,且没有常规结点 $n \in C$ 是 $I_\kappa[S]$ 的入点,则对 $K \in S$ 任何形如 $\{g\}_K$、$(g)_K$ 和 $H_K(g)$ 的项不起源于入侵结点。

证明:由定理 2.24 得 $I_\kappa[S]$ 是诚实的。根据推论 2.25 的逆否结论知:如果没有常规结点 $n \in C$ 是 $I_\kappa[S]$ 的入点,则 $\forall m \in C.$ term$(m) \notin I_\kappa[S]$。

① 假设 $t_1 = \{g\}_K$ 起源于一个入侵结点,t_1 不可能发生在 F、T、C、K、M、E、D、B、B_f 型入侵串上。考虑可能的 E、D、S_i、V_e 和 H_K 入侵串:

E:t_1 发生在$\langle -K_0, -h, +\{h\}_{K_0}\rangle$串上。由于 $K_0 \notin I_r[S]$,$K_0 \neq K$,按推论 2.19,$\{g\}_K \sqsubset \{h\}_{K_0} \Rightarrow \{g\}_K \sqsubset h$,这与起源定义矛盾。

D:t_1 发生在$\langle -K_0^{-1}, -\{h\}_{K_0}, +h\rangle$串上。由于$\{g\}_K \sqsubset h \Rightarrow \{g\}_K \sqsubset \{h\}_{K_0}$,与起源定义矛盾。

S_t:t_1 发生在$\langle -K_0, -h, +(h)_{K_0}\rangle$串上。由于 $K_0 \notin I_r[S]$,$K_0 \neq K$,按推论 2.19,$\{g\}_K \sqsubset (h)_{K_0} \Rightarrow \{g\}_K \sqsubset h$,这与起源定义矛盾。

V_e:t_1 发生在$\langle -K_0^{-1}, -(h)_{K_0}, +h\rangle$串上。由于$\{g\}_K \sqsubset h \Rightarrow \{g\}_K \sqsubset (h)_{K_0}$,与起源定义矛盾。

H_K:t_1 发生在$\langle -K_0^{-1}, -h, +H_{K_0}(h)\rangle$串上。由于 $K_0 \notin I_r[S]$,$K_0 \neq K$,按推论 2.19,$\{g\}_K \sqsubset H_K(h) \Rightarrow \{g\}_K \sqsubset h$,这与起源定义矛盾。

②$(g)_K$ 和 $H_K(g)$的项不起源于入侵结点,同理可证。

□

3 IKE2 协议

3.1 协议简介

重新设计的 IKE2 与 IKE1 不兼容,其设计目标除了要提供 IPsec 应有的服务外,还包括:简化消息回合,修订 IKE1 的缺陷,为通信双方提供身份保护,能抵抗 DOS 攻击。

IKE2 的消息交换包括四种:①IKE_SA_INIT(主交换的前两个消息,建立 IKE 安全联合——IKE-SA);②IKE_AUTH(主交换的后两个消息,认证 IKE_SA_INIT 消息,并建立第一个子安全联合);③CREATE_CHILD_SA(建立子安全联合、重分配 IKE-SA 密钥、删除、建立新的);④INFORMATIONAL(传递控制信息)。

主交换(IKE_SA_INIT 和 IKE_AUTH)的四条消息是:

I→R:HDR, SAi1, KEi, Ni

R→I:HDR, SAr1, KEr, Nr,[CERTREQ]

I→R:HDR, SK {IDi,[CERT,][CERTREQ,][IDr,] AUTH, SAi2, TSi, TSr}

R→I:HDR, SK {IDr,[CERT,] AUTH, SAr2, TSi, TSr}

前两个消息(IKE_SA_INIT)建立 IKE 安全联合、完成 Diffie-Hellman 密钥交换。后两个消息一方面认证 IKE_SA_INIT 交换,另一方面建立第一个子安全联合。[CERTREQ]表示可选的证书请求项。SK{ }表示对内容加密,然后对整个消息实行数据完整性保护,既 $SK\{h\}=\{h\}_{SK\text{-}e}$, $H_{SK\text{-}a}(HDR, \{h\}_{SK\text{-}e})$。

IKE_SA_INIT 交换后,双方计算的密钥是:

SKEYSEED=prf(g^ir, Ni | Nr),

{SK-d | SK-ai | SK-ar | SK-ei | SK-er} = prf+(SKEYSEED, Ni | Nr | SPIi | SPIr)。

其中 prf+ (K,S)= T1 | T2 | T3 | T4 |…(prf 为伪随机函数),即进行密钥扩展。T1 = prf (K, S | 0x01);T2 = prf (K, T1 | S | 0x02);T3 = prf (K, T2 | S | 0x03);T4 = prf (K, T3 | S | 0x04)。

SK-ai、SK-ar、SK-ei、SK-er 用于 IKE 安全联合内双方的加密和认证。SK-d 用于抽取子安全联合的密钥。

AUTH 载荷认证各自的 IKE_SA_INIT 交换消息(在后面的分析中,我们将发现这个域对安全至关重要)。如果双方使用预共享秘密认证,$AUTH = prf(prf(shared\ secret,$ "*key pad for IKE2*"), ⟨*message octets*⟩),如果使用数字签名认证,$AUTH = sign(\langle message\ octets\rangle)$。记第三、四条消息中的 AUTH 分别为 AUTH1 和 AUTH2,则 AUTH1 中⟨*message octets*⟩=⟨*HDR*, *SAi1*, *KEi*, *Ni*, *Nr*, *prf*(*SK-ai*, *IDi*)⟩,*AUTH2* 中⟨*message octets*⟩=⟨ *HDR*, *SAr1*, *KEr*, *Nr*,[*CERTREQ*], *Ni*, *prf*(*SK-ar*, *IDr*)⟩。

后两个消息中捎带建立的子安全联合密钥从 SK-d 抽取:$KEYMAT = prf+(SK\text{-}d, Ni \mid Nr)$。在 CREATE_CHILD_SA 交换中抽取的密钥是:$KEYMAT = prf+(SK\text{-}d, g^{\wedge}ir\ (new) \mid Ni \mid Nr)$,$g^{\wedge}ir\ (new)$表示新的 Diffie-Hellman 交换。

关于 IKE2 的详细载荷细节请参阅文[5]。

3.2 协议抽象

HDR 中含有两个重要的信息:SPI(安全参数索引,用于识别 IKE-SA)和 Message ID(消息标识)。我们省略 SPI,假设双方都工作在正确的 IKE-SA 内(如果 SPI 被篡改,只能造成无法通信,或数据完整性检查失败,不会影响安全性)保留 Message ID,记为 M(IKE2 规定请求和响应是一一对应的,它们有相同的 Message ID)。第一条消息中 I 提供多个安全联合供 R 选择,我们统一 SAi1、SAr1 为一个记号 SA1,即假设双方事先约定了一个安全联合,这样证明 I 和 R 的 SA1 的一致性也就证明了 SAr1∈SAi1。入侵者可以篡改 SAi1,但是不能认证 SAi1。同理 SAi2 和 SAr2 也统一为 SA2。

对预共享秘密认证,秘密通常是口令 p。IKE2 要求将 p 扩展成强密钥,若用 HMAC 函数实现 prf,则 $K_{IR}=Hp$(密钥填充)。我们省略 K_{IR}的计算过程,就假设 K_{IR}是双方预共享的密钥。因此 AUTH1 和 AUTH2 的内容分别是:

$AUTH1=H_{KIR}(M, SA1, g^{\wedge}i, N_I, N_R, H_{SK\text{-}aI}(I))$

$AUTH2=H_{KIR}(M, SA1, g^{\wedge}r, N_R, N_I, H_{SK\text{-}aR}(R))$

我们先忽略可选载荷和数据完整性保护,得到如下的主交换密钥分配和认证协议:

1. I→R:M, SA_1, $g^{\wedge}i$, N_I
2. R→I:M, SA_1, $g^{\wedge}r$, N_R
3. I→R:M+1,{I, $H_{KIR}(M, SA_1, g^{\wedge}i, N_I, N_R, H_{SK\text{-}aI}(I))$, SA_2, TS_I, $TS_R\}_{SK\text{-}eI}$
4. R→I:M+1, {R, $H_{KIR}(M, SA_1, g^{\wedge}r, N_R, N_I, H_{SK\text{-}aR}(R))$, SA_2, TS_I, $TS_R\}_{SK\text{-}eR}$

4 IKE2 协议分析

4.1 协议的秘密性

定义 4.1 在 IKE2 协议里,设 B_f 型入侵串轨迹是⟨$-x$, $+g^x$⟩;$\boldsymbol{K}_P \cap \boldsymbol{B}_P = \emptyset$。

定义 4.2 设(Σ, P)是 IKE2 协议里包含入侵串的串空间,P 是全体入侵串,$Init[M, SA_1, i, r, N_I, N_R, I, R, SA_2, TS_I, TS_R]=\{s\in\Sigma \mid tr(s)=\langle +(M, SA_1, g^{\wedge}i, N_I), -(M, SA_1, g^{\wedge}r, N_R), +(M+1,\{I, H_{KIR}(M, SA_1, g^{\wedge}i, N_I, N_R, H_{SK\text{-}aI}(I)), SA_2, TS_I, TS_R\}_{SK\text{-}eI}), -(M+1,\{R, H_{KIR}(M, SA_1, g^{\wedge}r, N_R, N_I, H_{SK\text{-}aR}(R)), SA_2, TS_I, TS_R\}_{SK\text{-}eR})\rangle\}$;

$Resp[M, SA_1, i, r, N_I, N_R, I, R, SA_2, TS_I, TS_R]=\{s\in\Sigma \mid tr(s)=\langle -(M, SA_1, g^{\wedge}i, N_I), +(M, SA_1, g^{\wedge}r, N_R), -(M+1, \{I, H_{KIR}(M, SA_1, g^{\wedge}i, N_I, N_R, H_{SK\text{-}aI}(I)), SA_2, TS_I, TS_R\}_{SK\text{-}eI}), +(M+1, \{R, H_{KIR}(M, SA_1, g^{\wedge}r, N_R, N_I, H_{SK\text{-}aR}(R)), SA_2, TS_I, TS_R\}_{SK\text{-}eR})\rangle\}$;

定义$\sum init$是全体发起者串集合，$\sum resp$是全体响应者串集合。

所有生成的密钥的安全性都取决于Diffie-Hellman交换的安全性。我们不妨定义密钥抽取是函数：

$K(i,r)=SK-d|SK-aI|SK-aR|SK-eI|SK-eR$

命题4.3 协议双方共享一致的$SK-d|SK-aI|SK-aR|SK-eI|SK-eR$等价于它们共享一致的$i,r$。

证明：由Diffie-Hellman交换的特性可得此结论。 □

引理4.4 g^x是诚实函数。

证明：根据离散对数的计算困难性特点知g^x起源于入侵结点，则x起源于B型入侵结点。 □

命题4.5 设C是$(\sum, P)$上的丛，$I,R\in \boldsymbol{T}, i,r\notin \boldsymbol{B}_P, s_{init}\in \mathrm{Init}[M,SA_1,i,r,N_I,N_R,I,R,SA_2,TS_1,TS_R]$，在$C$上的丛高是4，$s_{resp}\in \mathrm{Resp}[M,SA_1,i,r,N_I,N_R,I,R,SA_2,TS_1,TS_R]$在$C$上的丛高是4，$S=\{i,r\}$，$\kappa=\boldsymbol{K}\backslash S$。则$I_\kappa[S]$是诚实的。

证明：由于发起者和响应者都完成了协议的执行，所以他们共享一致的K_*K_*，从而共享一致的i,r；g^x是诚实函数且$i,r\in \boldsymbol{B}_P$，得g^i,g^r不起源于入侵结点，所以没有B_f型入侵结点是$I_\kappa[S]$的入点。同时$\kappa\subseteq \boldsymbol{K}, \kappa=\kappa^{-1}, \boldsymbol{K}\subseteq S\cup\kappa^{-1}$，根据定理2.24$I_\kappa[S]$是诚实的。 □

证明了i、r的安全性，则I、R内部计算的所有密钥都是安全的。

命题4.6 设C是$(\sum, P)$上的丛，$SK-eI, SK-eR\notin \boldsymbol{K}_P, s_{init}\in \sum_{init}$在$C$上的丛高是4，$s_{resp}\in \sum_{resp}$在$C$上的丛高是4，设$S=\{SK-eI, SK-eR, I, R\}$，$\kappa=\boldsymbol{K}\backslash\{SK-eI, SK-eR\}$。则$I_\kappa[S]$是诚实的。

证明：同命题4.5证明。 □

4.2 协议的认证性

命题4.7 设C是$(\sum, P)$上的丛，$K_{XY}, SK-eX\notin \boldsymbol{K}_P$，则形如$H_{K_{XY}}(g)$、$\{g\}_{SK-eX}$的项不起源于$C$中入侵结点。

证明：设$S=\{K_{XY}, SK-eX\}$，则$S\cap \boldsymbol{K}_P=S\cap \boldsymbol{B}_P=\emptyset, \boldsymbol{K}=S\cup\kappa^{-1}, \kappa=\boldsymbol{K}$。按$Init[\ ]$、$Resp[\ ]$的定义，知$\sim\exists m\cdot m\in C\wedge(t=\mathrm{term}(m)\in I_\kappa[S]\wedge(K_{XY}\sqsubset t\vee SK-eX\sqsubset t\vee SK-eY\sqsubset t)$，所以没有常规结点是$I_\kappa[S]$的入点。根据推论2.26$H_{K_{XY}}(g)$、$\{g\}_{SK-eX}$只起源于常规结点。 □

命题4.8 设$H_{K_{XY}}(g)$起源于常规串s，如果$s\in \sum init$，则$g=M,SA_1,g^{\wedge}i,N_X,NY,H_{SK-aX}(X)$；如果$s\in \sum resp$，则$g=M,SA_1,g^{\wedge}r,N_Y,N_X,H_{SK-aY}(Y)$，其中$X,Y\in \boldsymbol{T}_{name}$。

证明：由定义4.2可知结论成立。 □

命题4.9 设s是常规串，如果$H_{KIR}(M,SA_1,g^{\wedge}i,N_I,N_R,H_{SK-aI}(I))$起源于$s$，$I\neq R$，则$s\in Init[M,SA_1,i,r,N_I,N_R,I,R,SA_2,TS_I,TS_R]$，$N_I$起源于$s$，该项起源于$\langle s,3\rangle$。；如果$H_{KIR}(M,SA_1,g^{\wedge}r,N_R,N_I,H_{SK-aR}(R))$起源于$s$，$I\neq R$，则$s\in Resp[M,SA_1,i,r,N_I,N_R,I,R,SA_2,TS_I,TS_R]$，$N_R$起源于$s$，该项起源于$\langle s,4\rangle$。

证明：由定义4.2和命题4.8可知结论成立。 □

命题4.10 设C是$(\sum, P)$上的丛，$I\neq R, K_{IR}, SK-eI\notin \boldsymbol{K}_P, N_I$唯一起源于$C$中结点。如果$s\in Init[M,SA_1,i,r,N_I,N_R,I,R,SA_2,TS_I,TS_R]$在$C$上丛高是4。则存在常规串$s_{resp}\in Resp[M,SA_1,i,r,N_I,N_R,I,R,SA_2,TS_I,TS_R]$，它在$C$上丛高是4。

证明：$s\in Init[M,SA_1,i,r,N_I,N_R,I,R,SA_2,TS_I,TS_R]$的$C$上串轨迹是$\langle+(M,SA_1,g^{\wedge}i,N_I),-(M,SA_1,g^{\wedge}r,N_R),+(M+1,\{I,H_{KIR}(M,SA_1,g^{\wedge}i,N_I,N_R,H_{SK-aI}(I)),SA_2,TS_I,TS_R\}_{SK-eI}),-(M+1,\{R,H_{KIR}(M,SA_1,g^{\wedge}r,N_R,N_I,H_{SK-aR}(R)),SA_2,TS_I,TS_R\}_{SK-eR})\rangle$。

由于$K_{IR}\notin \boldsymbol{K}_P$，按命题4.9，$H_{K_{IR}}(M,SA_1,g^r,N_R,N_I,H_{SK-aI}(R))\sqsubset term(\langle s,4\rangle)$起源于响应者串：$s_{resp}\in Resp[M,SA_1,i',r,N_I,N_R,I,R,SA_2',TS_I',TS_R']$。该项是$\langle s_{resp},4\rangle$的子项，所以$s_{resp}$在$C$上丛高是4。如果$s$正确解析了第四条消息，则$s$与$s_{resp}$共享相同的函数$K(i,r)$，所以$i'=i$。（*）

由于$SK-eI\notin \boldsymbol{K}_P$，可得$\{I,H_{K_{IR}}(M,SA_1,g^i,N_I,N_R,H_{SK-aI}(I)),SA'_2,TS'_1,TS'_R\}_{SK-eI}\sqsubset term(\langle s_{resp},3\rangle)$起源于$s_1\in \sum_{init}$，由于$N_I\sqsubset term(\langle s,1\rangle)$唯一起源于$C$中结点，所以$s_1=s$，得$SA'_2=SA_2, TS'_1=TS_1, TS'_R=TS_R$。故可得响应者串：$s_{resp}\in Resp[M,SA_1,i,r,N_I,N_R,I,R,SA_2,TS_I,TS_R]$。 □

在上面这个命题中，我们假设$SK-eI\notin \boldsymbol{K}_P$，但是$SK-eI$并非双方的预共享秘密密钥，而是临时生成的，其安全性取决于Diffie-Hellman交换的安全性。（*）号之前的证明结论是：$i\leftrightarrow I, r\leftrightarrow R$，因此发起者能够确定他是与一个身份明确的主体进行唯一的Diffie-Hellman交换。除非发起者不想完成协议，否则这里的Diffie-Hellman交换及其衍生的密钥都是安全的。因此命题的结论仍然成立。

命题4.11 设C是$(\sum, P)$上的丛，$I\neq R, K_{IR}, SK-eI\notin \boldsymbol{K}_P, N_I$唯一起源于$C$中结点。如果$s\in Resp[M,SA_1,i,r,N_I,N_R,I,R,SA_2,TS_I,TS_R]$在$C$上丛高是4。则存在常规串$s_{init}\in Init[M,SA_1,i,r,N_I,N_R,I,R,SA_2,TS_I,TS_R]$，它在$C$上丛高至少是3。

证明：$s\in Resp[M,SA_1,i,r,N_I,N_R,I,R,SA_2,TS_I,TS_R]$的$C$上串轨迹是$\langle-(M,SA_1,g^{\wedge}i,N_I),+(M,SA_1,g^{\wedge}r,N_R),-(M+1,\{I,H_{KIR}(M,SA_1,g^{\wedge}i,N_I,N_R,H_{SK-aI}(I)),SA_2,TS_I,TS_R\}_{SK-eI}),+(M+1,\{R,H_{KIR}(M,SA_1,g^{\wedge}r,N_R,N_I,H_{SK-aR}(R)),SA_2,TS_I,TS_R\}_{SK-eR})\rangle$。

由于$K_{IR}\notin \boldsymbol{K}_P$，按命题4.9 $H_{K_{IR}}(M,SA_1,g^i,N_I,N_R,H_{SK-aI}(I))\sqsubset term(\langle s,3\rangle)$起源于发起者串：$s_{init}\in Init[M,SA_1,i,r',N_I,N_R,I,R,SA'_2,TS_I',TS'_R]$。该项是$\langle s_{init},3\rangle$的子项，所以$s_{init}$在$C$上丛高至少是3。由于$s$正确解析并接受了第三条消息，因此$s$与$s_{init}$共享相同的函数$K(i,r)$，所以$r'=r$（如果不共享相同的$K(i,r)$，则响应者不能正确解密，协议失败）。（*）

由于$SK-eI\notin \boldsymbol{K}_P$，所以$\{I,H_{K_{IR}}(M,SA_1,g^i,N_I,N_R,H_{SK-aI}(I)),SA_2,TS_1,TS_R\}_{SK-eI}\sqsubset term(\langle s,3\rangle)$，起源于$s_1\in \sum_{init}$，因$N_I$唯一起源，所以$s_1=s_{init}$，得$SA'_2=SA_2, TS'_1=TS_1, TS'_R=TS_R$。故可得发起者串：$s_{init}\in Init[M,SA_1,i,r,N_I,N_R,I,R,SA_2,TS_I,TS_R]$。 □

4.3 秘密性解释和身份保密

在秘密性证明中，我们在发起者和响应者成功执行协议的前提下，证明i、r是安全的。同时只有假设双方完成协议的执行，证明密钥的安全性才有意义，如果某一方不能完成协议，则意味着协议失败，此时不会建立任何安全联合。协议的认证性结论也表明如果一方建立了安全联合，那么他知道该安全联合另一方的身份。

发起者是在第三条消息中发送自己的身份，根据命题4.10，如果I在C上的丛高是3，则可得响应者串$s_{resp}\in Resp[M,SA_1,i,r,N_I,N_R,I,*,SA_2,TS_I,TS_R]$，即发起者不能确定响应者的身份。这就存在下面的一个攻击：

1. I→P(R):M, SA_1, $g^{\wedge}i$, N_I

2. P(R)→I:M, SA_1, $g^{\wedge}r$, N_P

3. I→P(R):M+1,{I, $H_{KIR}(M, SA_1, g^{\wedge}i, N_I, N_R, H_{SK\text{-}aI}(I)), SA_2, TS_I, TS_R\}_{SK\text{-}eI}$

…

P 获得 I 的身份后就消失了。IKE2 为发起者提供被动攻击下的身份保护,但在这种主动攻击下却不能保护发起者的身份。

造成这个缺陷的原因是 IKE2 的身份认证发生在密钥交换之后,也就是把秘密交给了尚未认证的主体。一般来说,身份保密应该遵守的原则是:"如果协议主体 A 只想对 B 公开身份,那么他应该先认证 B,然后再公开自己的身份"。由于 IKE2 的响应者身份认证发生在发起者身份认证之后,因此这个原则不适用。

要解决 IKE2 的发起者身份保密问题,可以采用策略:"响应者认证可以滞后,但只有意定的响应者才能获取发起者身份"。因此我们将第三条消息改为 $M+1,\{\{I\}_{PKR}, H_{KIR}(M, SA_1, g^{\wedge}i, N_I, N_R, H_{SK\text{-}aI}(I)), SA_2, TS_I, TS_R\}_{SK\text{-}eI}, PK_R$ 是 R 的加密公钥。

IKE2 并不保证 I 拥有 R 的公钥,但提供了证书请求的可选载荷。这样发起者 I 可以在第一条消息中增加加密公钥证书请求载荷[CERTREQ],响应者 R 在第二条消息中回应加密公钥证书[CERTE]。修改后的协议如下:

1. I→R:HDR,SAi1,KEi,Ni,[CERTREQ]

2. R→I:HDR,SAr1,KEr,Nr,[CERTE,][CERTREQS]

3. I→R: HDR,SK{IDi}$_{PKR}$,[CERTS,][CERTREQ,][IDr,]AUTH,SAi2,TSi,TSr}

4. R→I: HDR,SK{IDr,[CERTS,]AUTH,SAr2,TSi,TSr}

即如果发起者需要在主动攻击下保护自己的身份,建议在第一条消息中增加加密公钥证书请求。

4.4 采用数字签名认证的安全性

采用数字签名认证方法的协议按 4.1 节简化如下:

1. I→R:M,SA_1,$g^{\wedge}i$,N_I

2. R→I:M,SA_1,$g^{\wedge}r$,N_R,CR_I

3. I→R:M+1,{I,C_I,CR_R,(M,SA_1,$g^{\wedge}i$,N_I,N_R,$H_{SK\text{-}aI}(I))_{SKI}$,$SA_2$,$TS_I$,$TS_R\}_{SK\text{-}eI}$

4. R→I:M+1,{R,C_R,(M,SA_1,$g^{\wedge}r$,N_R,CR_I,N_I,$H_{SK\text{-}aR}(R))_{SKR}$,$SA_2$,$TS_I$,$TS_R\}_{SK\text{-}eR}$

CR_I、CR_R 分别表示请求 I 和 R 的证书,C_I、C_R 分别表示 I 和 R 的证书。SK_I、SK_R 分别是 I 和 R 的签名密钥。

命题 4.12 设 C 是(Σ,P)上的丛,$Z\in \boldsymbol{T}_{name}$,$SK_Z\notin \boldsymbol{K}_P$,则形如$(g)_{SK_Z}$的项不起源于 C 中的入侵结点。

证明:设 $S=\{SK_Z\}$,$\kappa=\boldsymbol{K}$,$\boldsymbol{K}=S\cup\kappa^{-1}$。按 $Init[\ ]$、$Resp[\ ]$的定义,知$\sim\exists m\cdot m\in C\wedge(t=\text{term}(m)\in I_\kappa[S]\wedge SK_Z\sqsubset t$,所以没有常规结点是 $I_\kappa[S]$的入点。根据推论 2.26$(g)_{SK_Z}$只起源于常规结点。 □

命题 4.13 设$(g)_{SK_Z}$起源于常规串 s,如果 $s\in\sum init$,则 $g=M,SA_1,g^{\wedge}i,N_X,N_Y,H_{SK\text{-}aX}(X),X=Z$;如果 $s\in\sum resp$,则 $g=M,SA_1,g^{\wedge}r,N_Y,N_X,H_{SK\text{-}aY}(Y),Y=Z$。其中 $X,Y\in \boldsymbol{T}_{name}$。

命题 4.14 设 s 是常规串,如果$(M,SA_1,g^{\wedge}i,N_I,N_R,H_{SK\text{-}aI}(I))_{SKI}$起源于 s,$I\neq R$,则 $s\in Init[M,SA_1,i,r,CR_I,CR_R,C_I,C_R,N_I,N_R,I,R,SA_2,TS_I,TS_R]$,$N_I$ 起源于 s,该项起源于$\langle s,3\rangle$;如果$(M,SA_1,g^{\wedge}r,N_R,CR_I,N_I,H_{SK\text{-}aR}(R))_{SKR}$起源于 s,则 $s\in Resp[M,SA_1,i,r,CR_I,CR_R,C_I,C_R,N_I,N_R,I,R,SA_2,TS_I,TS_R]$,$N_R$ 起源于 s,该项起源于$\langle s,4\rangle$。

以上两个命题的证明类似命题 4.8 和 4.9 的证明。

命题 4.15 设 C 是$(\sum,P)$上的丛,$I\neq R$,SK_R,$SK-eI\notin \boldsymbol{K}_P$,$N_I$ 唯一起源于 C 中结点。如果 $s\in Init[M,SA_1,i,r,CR_I,CR_R,C_I,C_R,N_I,N_R,I,R,SA_2,TS_I,TS_R]$在 C 上丛高是 4。则存在常规串 $s_{resp}\in Resp[M,SA_1,i,r,CR_I,CR_R,C_I,C_R,N_I,N_R,I,R,SA_2,TS_I,TS_R]$,它在 C 上丛高是 4。

证明:$s\in Init[M,SA_1,i,r,CR_I,CR_R,C_I,C_R,N_I,N_R,I,R,SA_2,TS_I,TS_R]$的在 C 上的串轨迹是$\langle+(M,SA_1,g^{\wedge}i,N_I),-(M,SA_1,g^{\wedge}r,N_R,CR_I),+(M+1,\{I,C_I,CR_R,(M,SA_1,g^{\wedge}i,N_I,N_R,H_{SK\text{-}aI}(I))_{SKI},SA_2,TS_I,TS_R\}_{SK\text{-}eI}),-(M+1,\{R,C_R,(M,SA_1,g^{\wedge}r,N_R,CR_I,N_I,H_{SK\text{-}aR}(R))_{SKR},SA_2,TS_I,TS_R\}_{SK\text{-}eR})\rangle$。

根据命题 4.14,$(M,SA_1,g^{i},N_R,CR_1,N_I,H_{SK-aR}(R))_{SK_R}\sqsubset$ term$(\langle s,4\rangle)$起源于下面的响应者串:$s_{resp}\in Resp[M,SA_1,i',r,CR_I,CR'_R,C_{I'},C_R,N_I,N_R,I',R,SA'_2,TS'_I,TS'_R]$,所以$\langle s_{resp},4\rangle\in C$,故 s_{resp}在 C 上丛高是 4。如果 s 正确解析了第四条消息,则 s 与 s_{resp} 共享相同的函数 $K(i,r)$,所以 $i'=i$。(*)

由于 $SK-eI\notin \boldsymbol{K}_P$,所以$\{I,C_{I'},CR'_R,(M,SA_1,g^{i},N_I,N_R,H_{SK-aI}(I')_{SK_{I'}},SA_2',TS'_I,TS'_R\}_{SK-aI}\sqsubset term(\langle s_{resp},3\rangle$起源于某个 $s_1\in\sum_{init}$,因 N_I 唯一起源于 C,所以 $s_1=s$,得 $I'=I,CR'_R=CR_R,SA'_2=SA_2,TS'_I=TS_I,TS'_R=TS_R$。 □

(*)号之前的证明说明发起者能够确定他是与一个身份明确的主体进行唯一的 Diffie-Hellman 交换,并且双方共享一致的 i 和 r 值。根据命题 4.3 它们将获得相同的密钥集,从而保证了 $SK-eI\notin \boldsymbol{K}_P$ 的合理性。

命题 4.16 设 C 是$(\sum,P)$上的丛,$I\neq R$,SK_I,$SK-eI\notin \boldsymbol{K}_P$,$N_I$ 唯一起源于 C 中结点。如果 $s\in Resp[M,SA_1,i,r,CR_I,CR_R,C_I,C_R,N_I,N_R,I,R,SA_2,TS_I,TS_R]$在 C 上丛高是 4。则存在常规串 $s_{init}\in Init[M,SA_1,i,r,CR_I,CR_R,C_I,C_R',N_I,N_R,I,R',SA_2,TS_I,TS_R]$,它在 C 上丛高至少是 3。

证明:$s\in Resp[M,SA_1,i,r,CR_I,CR_R,C_I,C_R,N_I,N_R,I,R,SA_2,TS_1,TS_R]$的 C 上串轨迹是$\langle-(M,SA_1,g^{\wedge}i,N_I),+(M,SA_1,g^{\wedge}r,N_R,CR_I),-(M+1,\{I,C_I,CR_R,(M,SA_1,g^{\wedge}i,N_I,N_R,H_{SK\text{-}aI}(I))_{SKI},SA_2,TS_I,TS_R\}_{SK\text{-}eI}),+(M+1,\{R,C_R,(M,SA_1,g^{\wedge}r,N_R,CR_I,N_I,H_{SK\text{-}aR}(R))_{SKR},SA_2,TS_I,TS_R\}_{SK\text{-}eR})\rangle$。

根据命题 4.14,$(M,SA_1,g^{i},N_I,N_R,H_{SK-aI}(I))_{SK_I}\sqsubset$ term$(\langle s,3\rangle)$起源于某个发起者串:$s_{init}\in Init[M,SA_1,i,r',CR'_I,CR'_R,C_I,C_{R'},N_I,N_R,I,R',SA'_2,TS'_I,TS'_R]$,由于$\langle s_{init},3\rangle\in C$,故 s_{init}在 C 上丛高至少是 3。由于 s 正确解析并接受了第三条消息,因此 s 与 s_{init} 共享相同的函数 $K(i,r)$,所以 $r'=r,CR'_I=CR_I$。

由于 $SK-eI\notin \boldsymbol{K}_P$,所以$\{I,C_I,CR_R,(M,SA_1,g^{i},N_I,N_R,H_{SK-aI}(I))_{SK_I},SA_2,TS_1,TS_R\}_{SK-eI}\sqsubset$ term$(\langle s,3\rangle)$起源于 $s_1\in\sum_{init}$,因 N_I 唯一起源于 C 中结点,所以 $s_1=s_{init}$,得 $CR'_R=CR_R,SA'_2=SA_2,TS'_I=TS_I,TS'_R=TS_R$。故可得发起者串:$s_{init}\in Init[M,SA_1,i,r,CR_I,CR_R,C_I,C_{R'},N_I,N_R,I,R',SA_2,TS_1,TS_R]$。 □

对响应者来说,如果他完成了一次协议执行,那么他确信只与发起者 I 建立安全联合并共享一致的、安全的密钥集。

(下转第 123 页)

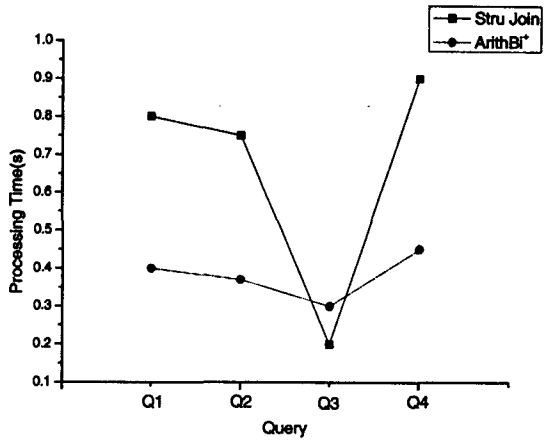

图 5 ArithBi+查询执行时间

图 5 中，我们利用基于 RDBMS 的 Structure Join 方法与 ArithBi+方法进行对比，可以看到，ArithBi+方法在各个查询语句(除 Q3)的表现都比前者要好很多。这是因为 Structure Join 方法的基本操作是 Join 操作，这种操作的代价是比较高的，并随着查询路径的增长所需要的 Join 次数越多。Q3 的情形比较特殊，这是由于 RDBMS 中是将同名的(如 AuthorName)存放在一张表中的，所以只需要一次选择操作就可以得到所有的结果。

5 相关工作

针对 XML 进行索引的工作有很多，但都不能直接用于经算术压缩的 XML 数据，参考文献中只列举了有代表性的几个[9~11]。XQzip[12]提出了一种有压缩功能的索引结构，但对基于算术压缩的 XML 数据不能进行处理；文[13]则提出了一种可根据压缩比率及查询能力选择有效 XML 压缩算法的查询处理系统，并没有讨论如何充分利用索引提高查询处理能力。

结论及展望 提出了一种压缩 XML 数据的索引结构 ArithBi+，应用该索引结构可以直接基于压缩 XML 文件进行查询，并可以较高效率实现对类似//element$_1$/element$_2$/…/elment$_m$ 语句的查询处理。后续的工作将在如何基于 ArithBi+进行复杂查询处理等方面开展进一步研究。

参 考 文 献

1 Liefke H, Suciu Dan. XMill: An efficient Compressor for XML data. In: Proc. of the 2000 ACM SIGMOD Int'l Conf. on Management of Data 2000, New York: ACM Press, 2000. 153～164
2 Tolani P M, et al. XGRIND: A Query-friendly XML Compressor. In: Proc. of the 18th Int'l Conf. on Data Engineering (ICDE' 02). Washington: IEEE Computer Society, 2002. 225～225
3 Min J-K, et al. XPRESS: A Queriable Compression for XML data. In: Proc. of the 2003 ACM SIGMOD Int'l Conf. on Management of Data, New York: ACM Press, 2003. 122～133
4 Papakonstantinou Y, Garcia-Molina H, Widom J. Object Exchange Across Heterogeneous Information Sources. In: Proc. of the 11th Int'l Conf on Data Engineering (ICDE' 95). Washington: IEEE Computer Society, 1995. 251～260
5 Lelewer D A, Hirschberg D S. Data Compression. ACM Computing Surveys, New York: ACM Press, 1987, 19(3): 261～296
6 Manolopoalos Y, Theodoridis Y, Tsotras V J. Advanced database indexing. Boston: Kluwer Academic Publishers, 1999. 61～81
7 Cormen T H, Leiserson C E, Rivest R L. Introduction to algorithms. Cambridge, MA: MIT Press, 1990
8 DBLP, XML Data. At http://dblp.uni-trier.de/xml/
9 Wang Haixun, Park Sanghyun, Fan Wei, Yu P S. ViST: Adynamic index method for querying XML data by tree structures. In: Proc. of the 2003 ACM SIGMOD Int'l Conf. on Management of Data, New York: ACM Press, 2003. 110～121
10 Chung C, Min J, Shim K. APEX: An adaptive path index for XML data. In: Proc. of the 2002 ACM SIGMOD Int'l Conf. on Management of Data, New York: ACM Press, 2002. 121～132
11 Goldman R, Widom J. DataGuides: Enabling Query Formulation and Optimization in Semistructured Databases. In: Proc. of the 23th Int'l Conf. on Very Large Databases (VLDB'97). Athens: Morgan Kaufmann, 1997. 436～445
12 Cheng J, Ng W. XQzip: Querying Compressed XML Using Structural Indexing. In: 9th Int'l Conf. on Extending Database Technology (EDBT 2004), Heidelberg: Springer-Verlag, 2004. 219～236
13 Arion A, et al. Efficient Query Evaluation over Compressed XML Data. In: 9th Int'l Conf. on Extending Database Technology (EDBT 2004), Heidelberg: Springer-Verlag, 2004. 200～218

(上接第 63 页)

发起者没有和响应者有一致的 C_R 和 R 是因为我们不能保证最后一条消息一定到达发起者 I。这不影响安全性，因为对响应者 R 来说，他确信是与发起者 I 执行协议，与 I 共享秘密。对 I 来说，如果他在此认证基础上建立了安全联合，那么这个安全联合也一定是和 R 建立的，并且他们有一致的、秘密的密钥集。

结论 IKE2 协议的身份及消息认证是为了保证密钥的安全。我们证明了在两种认证方式下，发起者和响应者都能实现他们的认证目标。在分析上我们把 $SK\{h\}=\{h\}_{SK\text{-}e}$，$H_{SK\text{-}a}(HDR,\{h\}_{SK\text{-}e})$简化为 $SK\{h\}=\{h\}_{SK\text{-}e}$，这已经能够达到安全目标，增加的 $H_{SK\text{-}a}(HDR,\{h\}_{SK\text{-}e})$主要是验证整个消息的数据完整性。同时我们发现在主动攻击情况下，发起者的身份不能得到保护，我们认为在许多应用中需要为发起者提供主动攻击下的身份保护。其次我们可以看到虽然 IKE2 的消息结构非常复杂，但减少的消息交换回合无疑提高了协议效率，毕竟计算时间比网络传输时间要少的多，减少的消息回合也能更有效地抵抗拒绝服务攻击。IKE2 的另一个优点是协议的可选冗余度减少了，这有利于它的商业应用。

为了分析 IKE2 协议，我们扩展了串空间的诚实理论。由于增加了入侵模型，因此扩展串空间能够分析包含丰富密码原语的安全协议。本文的分析也是扩展串空间理论的一次实际应用，我们相信它能在更多的复杂协议分析中发挥作用。

参 考 文 献

1 Maneki A P. Honest Functions and their Application to the Analysis of Cryptographic Protocols. In: Proc. of the 12th IEEE Computer Security Foundations, Workshop[C], 1999. 83～89
2 Fábrega F J T, Herzog J C, Guttman J D. Honest Ideals on Strand Spaces. In: Proc. of the 11th IEEE Computer Security Foundations Workshop[C], 1998. 66～77
3 Fábrega F J T, Herzog J C, Guttman J D. Strand Spaces: Why is a Security Protocol Correct?. In: Proc. [C], 1998 IEEE Symposium on Security and Privacy, 1998. 160～171
4 Fábrega F J T, Herzog J C, Guttman J D. Strand Spaces: Proving Security Protocols Correct. Journal of Computer Security[J], 1999(7): 191～230
5 Harkins D, Kaufman C, Kent S, et al. Internet Key Exchange (IKEv2) Protocol. http://www.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-ipsec-ikev2-11.txt. 2003. Work in progress
6 Moore K. The Internet IP Security Domain of Interpretation for ISAKMP. RFC 2407, November 1998
7 Maughan D, Schertler M, Chneider M, et al. Internet Security Association and Key Management Protocol (ISAKMP). RFC 2408, November 1998
8 Harkins D, Carrel D. The Internet Key Exchange (IKE). RFC 2409, November 1998
9 Aiello W, Bellovin S M. Efficient, DoS Resistant, Secure Key Exchange for Internet Protocols. In: Proc. of the ACM Computer and Communications Security (CCS) Conf, Washington, DC,. November 2002
10 Ferguson NSchneier B. A Cryptographic Evaluation of IPSec. http://www.counterpane.com/ipsec.html. 1999
11 Kaufman C, et al. Code-preserving Simplifications and Improvements to IKE. Internet Draft, Internet Engineering Task Force, July 2001
12 Kaufman C, Perlman R. Analysis of IKE. In: IEEE Trans. on Network Computing, November 2000