第十四章　网络安全协议的分析与验证技术

我们在前三部分已经阐述了非常丰富的网络安全协议的例子，包括安全的实例和不安全的实例，甚至深入分析和证明过个别协议的安全性质，然而一个始终没有解决的问题是：如何系统地分析和验证协议的安全性？这是计算机安全领域的核心问题与技术之一，目前已经发展出丰富的成果，对此我们在这一章做一个导论性的阐述。

严格证明协议(为与该领域的术语一致，下面常称网络安全协议为密码协议)的安全性首先需要一种系统化的模型表达技术。这类模型不止一种，而且每种模型的表达能力和分析能力各有所长。我们在本章选择的是所谓 strand-图模型[1]，这是一个非常直观而又容易精确化的协议模型，实际上读者在第 9 章已经初步接触过这种表示方法。strand-图本质上就是分布式系统中的 Lamport-图，但在消息表示方面加入了密码算子。因此，strand-图和 Lamport-图一样，都是表达并发进程之间交换消息的时空过程。这一章首先建立协议的 strand-图的精确概念，以及基于 strand-图表达的攻击者的普遍模型，然后用 strand-图的性质刻画关于协议安全性的几个普遍结论，最后用 strand-图模型来具体分析和证明几个协议的安全性质。

这一章的讨论比较数学化，但实际上理解其内容并不需要读者具备任何特殊的数学知识，所需要的只是细致和耐心。此外，和任何精确的理论一样，一方面形式化的数学模型是实现严格的分析所必须的，但另一方面读者在任何时候都不要被表面上的形式化掩盖了对背后直观概念的理解，而应该时时注意两者的联系。

14.1　协议的 strand-图模型

14.1.1　消息代数与 strand-图

strand-图的基本元素是一个常元符号集合 $\mathscr{A}$、一个密钥符号集合 $\mathscr{K}$、一个明文集合 $\mathscr{T}$和一个变元集合 $\mathscr{V}$，并且这四个基本集合互不相交。在此之上进一步构造出消息、事件和 strand。

消息是一个形式表达式，为强调其形式结构今后也常称为消息表达式或消息式，其递归定义如下：

[1] 关于 strand 这一词汇目前没有统一规范的中文翻译，我们暂取英文文献的原始名称。

(1) $\mathscr{A} \cup \mathscr{T} \cup \mathscr{V} \cup \mathscr{K}$中的元素都是消息式；

(2) 若 M、N 是消息式，则 M,N 是消息式；

(3) 若 M 是消息式，K∈$\mathscr{K}$是密钥符号，则$\{M\}_K$是一个消息式。

两个消息式 M、N 之间有一种极其重要的半序关系—子项关系，记做 M∠N，定义如下：

(1) M∠M

(2) 若 M∠N 则对任意的 k 有 M∠$\{N\}_k$

(3) 若 M∠N 则对任意的 N_1 有 M∠N_1N、M∠NN_1

这里要特别强调该定义并不(!)蕴涵 K∠$\{M\}_K$。

根据定义不难验证(1)子项关系∠是半序关系；(2)若 K≠K_1，$\{h\}_K$∠$\{h_1\}_{K1}$，则必有$\{h\}_K$∠h_1。

协议的所有消息式的集合称为一个消息代数，它满足以下自由代数性质[2](Freeness Assumptions)：

(1) $\{M_1\}_{K1}=\{M_2\}_{K2}$ 当且仅当 $M_1=M_2$ 及 $K_1=K_2$

(2) $M_1N_1= M_2N_2$ 当且仅当 $M_1=M_2$ 及 $N_1=N_2$

(3) $M_1M_2 \neq \{M\}_K$

(4) $M_1M_2 \notin \mathscr{K} \cup \mathscr{T}$

(5) $\{M\}_K \notin \mathscr{K} \cup \mathscr{T}$

注意最后两条蕴涵密钥 K 无结构，即 K 是原子项。

若 M 是消息式，则+M 或-M 表示一个事件，分别表示发送消息 M 和接收消息 M。

strand 是一个事件序列及一个指定的消息作用点，作用点的位置用下划线表示：

$$s = E_1,E_2,\ldots,E_{i-1},\underline{E_i},E_{i+1},\ldots,E_s$$

称 s=…,$\underline{+t}$,…是正号的，s=…,$\underline{-t}$,…是负号的。设 $E_i=\pm M$，记 un_term(E_i)=M。不标记作用点位置的事件序列称做一个迹(trace)。

设 s’ = $E'_1,E'_2,\ldots E'_{k-1},\underline{E'_k},E'_{k+1},\ldots,E'_r$ 也是个 strand，s 和 s’ 有关系 s<s’ 若 $E'_1=E_1,\ldots, E'_i=E_i$ 且 k=i+1；s 和 s’ 有关系 s→s’ 若 i=k 且 $E_i=+M, E'_i=-M$。

广义 strand-图是一个有向图(S，D)，S 是 strand 的一个集合，有向边<s,s’>∈D 若 s<s’ 或 s→s’，并且有性质：

(1)若 s’∈S 且 s<s’，则 s∈S;

(2)若 s’∈S, s’ = …, $\underline{-M}$,…, 则必有且仅有一个 s∈S，s = …,$\underline{+M}$,…，使 s→s’。

无圈的广义 strand-图称做 strand-图。

[2] 自由消息代数等价于完全忽略攻击者可以利用的任何数学关系，例如 x⊕x=0 这样的关系。这当然是一种理想模型，也是目前大多数研究工作的假设。考虑数学关系的非自由代数模型处理起来要复杂得多。

下面的定理说明为什么在实际应用中仅考虑无圈的广义 strand-图。

定理 14.1 广义strand-图是无圈有向图当且仅当其中所有的消息作用点可按Lamport时序协议排成线性序。

证明：事实上，广义 strand-图中的顶点关系<和→的解释分别与 Lamport 时序协议中的本地事件和消息传输事件之间因果关系的解释完全一致，故按 Lamport 时序协议对消息作用点时间的排序的结果就等价于对 strand-图的顶点按边的方向一致的排序，因此结论立刻成立。□

因此，strand-图上顶点间的连通关系就是顶点间的因果关系，且仅有这种图是协议过程的合理模型，因此以后仅考虑 strand-图，该半序关系记做*-关系。图 14-1 是对该定理的解释，其中图 14-1(a)不能按 Lamport 时序协议对消息作用点的时间排序(t4<t1<t2<t3<t4，矛盾)；　图 14-1(b)能按 Lamport 时序协议对消息作用点的时间排序(完全序 t1<t2<t3<t4)；图 14-1 (c) 也能按 Lamport 时序协议对消息作用点时间排序(半序 t1<t2, t3<t2, t3<t4, t1<t4)，图 14-1 (d)是图 14-1 (c)的 strand-图。

根据半序关系的普遍性质，立刻有：

定理 14.2 strand-图顶点的任何非空子集$\{S_1,\ldots,S_n\}$必存在*****-极小元，即存在这样的 S_k, 从任何其它的 S_i 出发都没有能到达 S_k 的路径。□

例如，图 14-1(b)中的 S_1, 图 14-1(c)中的 S_1 和 S_2' 就是极小元。注意极小元未必唯一。S 是一组顶点的极小元，即任何其它的顶点都不是 S 的“因”，但可能是也可能不是 S 的“果”。今后简称*****-极小元为极小元。

引理 14.3　S 是 strand-图 $\mathscr{G}$ 的顶点集合，具有这样的性质：若 m、m'∈ $\mathscr{G}$ 且 un_term(m)= un_term(m'), 则 m∈S 当且仅当 m'∈S。设 x*是 S 的极小元，则 x*必是正号的。

证明　若 x*为负号，设 x*=…,-M,…，由 strand-图的定义知 $\mathscr{G}$ 中必存在 y=…,+M,…，y→x*，并由 S 的性质知 y∈S，但这显然与 x*的极小性矛盾。□

$\mathscr{G}$ 是 strand-图，$\mathscr{M}$ 是给定的消息集合。strand x∈$\mathscr{G}$ 定义做 $\mathscr{M}$ 的入口点，若存在 M∈$\mathscr{M}$ 使 x=…,+M,…且对任何 y∈$\mathscr{G}$ 、y<x 都有 un_term(y) ∉ $\mathscr{M}$。特别是，给定消息 M、集合 $\mathscr{M}$ ={N: M∠N}，称 $\mathscr{M}$ 的入口点 x 是消息 M 的源生 strand 或 M 在 x 上源生。若 x 属于 strand-图 G，也称 M 在 G 上源生。若 G 有且仅有一个 strand x 使 M 在 x 上源生，则称 M 在 G 上唯一源生。

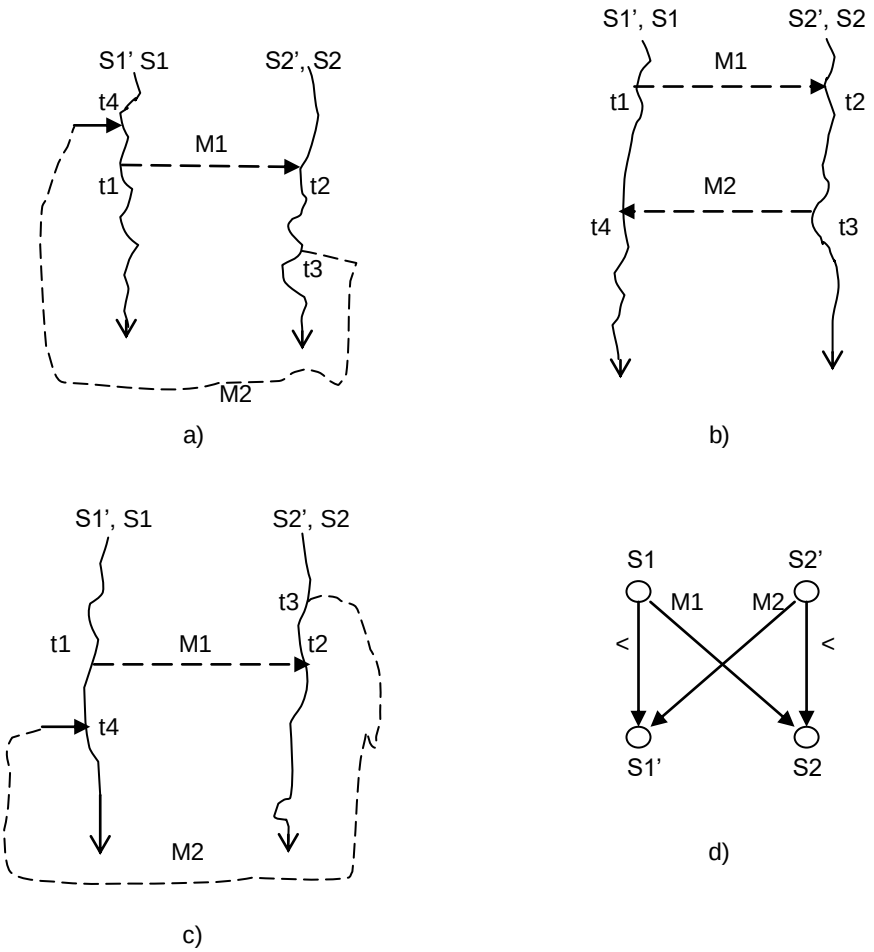

图 14-1　Lamport-图和 strand-图

引理 14.4　$\mathscr{G}$是 strand-图，t 是给定的消息，n*是顶点集合 S(t)={x∈$\mathscr{G}$: t∠un_term(x)}的极小元，则 n*是 t 的源生 strand。

证明　注意到 S(t)具有引理 14-3 中集合 S 的性质，故 n*必为正号：n*=…,+t,…。若 n*非 t 的源生 strand，则存在 n<n*使 n=…,$+t_1$,…、t∠t_1，但这与 n*的极小性相矛盾。□

s 是一个 strand，其作用域 R(s)定义做在 strand-图上以顶点 s 为根、应用有向图遍历算法能达到的所有顶点的集合。

若 Lamport 时序协议能将 strand-图的顶点排成线性序，则该图称为 strand-树。

定理 14.5　一个 strand-图是一棵 strand-树 iff 存在且只有一条遍历所有顶点的有向路径。

证明是显然的。图 14-1(b)就是一棵 strand-树。

14.1.2　攻击者 strand

定义攻击者-strand 是有以下迹的 strand 之一：

(1) M-strand: +t, $t \in T_p$，T_p 是 $\mathscr{T}$ 的一个子集;

(2) F-strand: ^{-}g, $g \in \mathscr{A}$

(3)Tee-strand: ^{-}g,+g,+g

(4) C-strand: ^{-}g, ^{-}h, +gh

(5) S-strand: –gh, +g, +h

(6) K-strand:+K, $K \in K_p$, K_p 是攻击者已知的密钥集合；

(7) E-strand: –k, –h, $+\{h\}_k$, $k \in \mathscr{K}$

(8) D-strand: $-k^{-1}$, $-\{h\}_k$, +h, $k^{-1} \in K_p$

所有这些攻击者-strand 的涵义都是很直观的，例如，Tee-strand(-g+g+g)表示重复所截获的消息；S-strand(–gh+g+h)表示将所截获的、有两个联结子项的消息一分为二且分别播放这两个子项；E-strand(–k–h+$\{h\}_k$)表示用截获的密钥对消息加密以生成一个新消息；D-strand($-k^{-1}-\{h\}_k$+h)表示用截获的密钥对截获的密文解密以得到明文[3]。图 14-2 是这些攻击者 strand 的图表示。

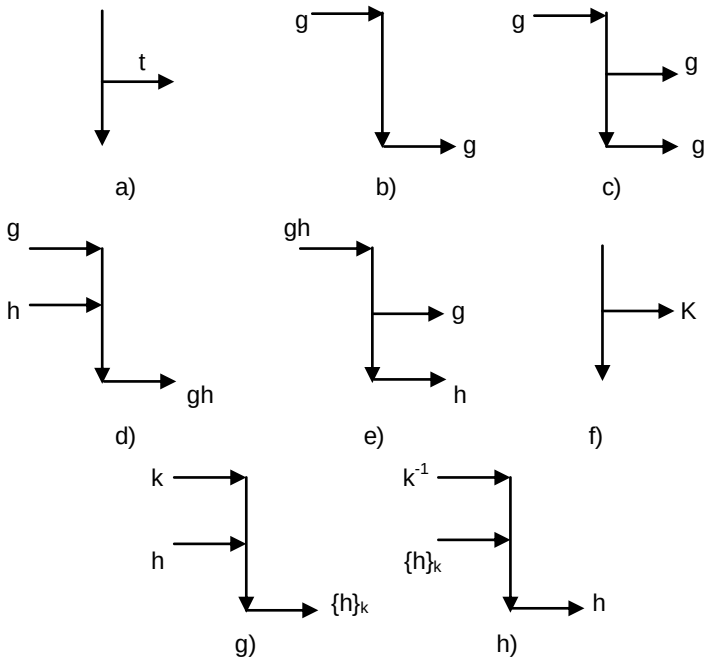

图 14-2 攻击者 strand

[3] K^{-1} 表示(公钥或私钥)K 对应的(私钥或公钥)密钥。

所有这些 strand 完全表达了一般意义上的 Dolev-Yao 攻击模型，即适当组合它们可以表达出任何 Dolev-Yao 攻击能力。例如图 14-3 是对经典的 Needham-Schroeder 协议攻击的第一步，这里组合了一个 D-strand 和一个 E-strand。

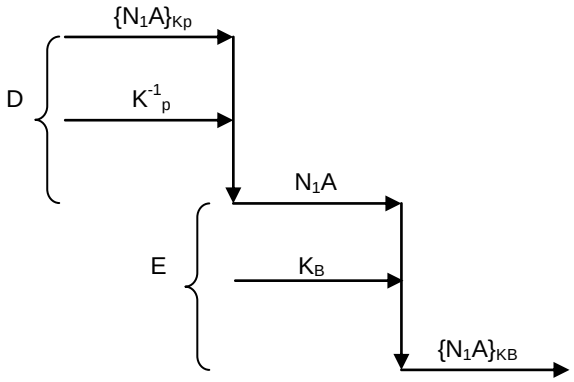

图 14-3 组合的攻击者 strand

14.2 消息代数的理想

一个协议所允许的所有消息表达式构成这一协议的消息代数。消息代数对协议的分析与验证起着重要作用，这一点不应使读者感到意外，事实上消息代数所表达的正是协议的密码结构。这一节刻画消息代数的精细结构，它们构成下一节要证明的几个普遍性结论的理论基础。

L 是消息代数，$K\subset\mathcal{K}$，消息代数的 K-理想[4]是一个满足以下条件的集合 $I\subset\mathcal{L}$：

(1) 对任何 $h\in I$、$g\in L$，有 $gh\in I$ 和 $hg\in I$

(2) 对任何 $h\in I$、$k\in K$，有 $\{h\}_k\in I$

对给定的消息集合 H 和 $K\subset K$，含 H 的极小 K-理想记做 $I_K[H]$，特别是 H={h}时记做 $I_K[h]$。I 是 L 的 K-理想，今后记为 $I\lhd_K L$。

下面是几个有用的事实。

设 $K\subset\mathcal{K}$，递归地定义两个消息式 M、N 之间的 K-子项关系如下，记做 $M\angle_K N$：

(1) $M\angle_K M$

(2) 若有 $k_0\in K$ 使 $N=\{N_0\}_{k0}$ 且 $M\angle_K N_0$，则有 $M\angle_K N$

(3) 若 $M\angle_K N$ 则对任意的 N_1 有 $M\angle_K N_1 N$、$M\angle_K N N_1$

则 $g\angle_K h$ *iff* $g\in I_K[h]$，即 $I_K[h]=\{t: h\angle_K t\}$(见习题 14-3 及其提示)。

设 $K\subset\mathcal{K}$，$I_1\lhd_K\mathcal{L}$、$I_2\lhd_K\mathcal{L}$，则 $I_1\cap I_2\lhd_K\mathcal{L}$、$I_1\cup I_2\lhd_K\mathcal{L}$(习题 14-4)，并且(习题 14-5)

[4] 熟悉一点近世代数的读者会看出这里理想的概念确实“很象”环(ring)的理想(ideal)的定义。

(1) $I_K[H]=\{t:$ 存在 $h\in H$ 使 $h\angle_K t\}$

(2) $I_K[H]=\cup_{x\in H}I_K[x]$

(3) $I_K[H_1\cup H_2]=I_K[H_1]\cup I_K[H_2]$

(4) $I_K[H_1\cap H_2]\subseteq I_K[H_1]\cap I_K[H_2]$

对 K_1、$K_2\subset K$ ，恒有 $I_{K1}[H]\cup I_{K2}[H]\subseteq I_{K1\cup K2}[H]$、$I_{K1\cap K2}[H]\subseteq I_{K1}[H]\cap I_{K2}[H]$。

称一个消息式 M 是简约的，若 $M\neq M_1M_2$。因此若 M 是简约的则或者 $M\in\mathcal{T}$ 或者 $M=\{h\}_K$。

引理 14.6　$K\in K^*$，$S\subset\mathcal{Q}$，对所有的 $s\in S$，s 不为形式$\{g\}_K$。如果$\{h\}_K\in I_{K^*}[S]$则必有 $h\in I_{K^*}[S]$。

证明　假若$\{h\}_K\in I_{K^*}[S]$但 $h\notin I_{K^*}[S]$，于是 $I^*= I_{K^*}[S]-\{h\}_K\subset I_{K^*}[S]$且显然 $S\subseteq I^*$(因为$\{h\}_K\notin S$)。I^*是 K-理想：事实上，对任何 $u\in I^*$ 和任意的消息式 a 显然 au、ua 都不等于$\{h\}_K$(自由代数性质(3))但都属于(理想)$I_{K^*}[S]$，故 $au、ua\in I^*$；又对 $u\in I^*$、$k_1\in K^*$有$\{u\}_{k1}\in I_{K^*}[S]$且$\{u\}_{k1}\neq\{h\}_k$(否则由自由代数性质(1)有 $h=u\in I_{K^*}[S]$，与开头的假设矛盾)，因此 I^* 是含 S 的 K-理想，故 $I_{K^*}[S]\subseteq I^*$ 但这又与 $I^*\subset I_{K^*}[S]$矛盾。□

引理 14.7　$k\in K^*$，$K^0\subset\mathcal{K}$，$S\subset\mathcal{Q}$，所有的 $s\in S$ 都是简约的且不为形式$\{g\}_k$。如果$\{h\}_k\in I_{K0}[S]$则必有 $k\in K^0$。

证明　假若$\{h\}_k\in I_{K0}[S]$但 $k\notin K^0$，于是 $I^*= I_{K0}[S]-\{h\}_K\subset I_{K0}[S]$且显然 $S\subseteq I^*$。I^*是 K_0-理想：对任何 $u\in I^*$ 和任意的消息式 a 显然 au、ua 都不等于$\{h\}_K$，故 au、$ua\in I^*$；又对 $u\in I^*$、$k_1\in K^0$有$\{u\}_{k1}\in I_{K^*}[S]$且$\{u\}_{k1}\neq\{h\}_k$(否则由自由代数性质(1)有 $k=k_1\in K^0$，与开头的假设矛盾)，因此 I^* 是含 S 的 K^0-理想，故 $I_{K0}[S]\subseteq I^*$ 但这又与 $I^*\subset I_{K0}[S]$矛盾。□

引理 14.8　$K\subset\mathcal{K}$，$S\subset\mathcal{Q}$，所有的 $s\in S$ 都是简约的。若 $gh\in I_K[S]$，则或者 $g\in I_K[S]$或者 $h\in I_K[S]$。

证明　由习题 14-5(1)，存在 $s\in S$ 使 $s\angle_K gh$，由于 s 简约故 $s\angle_K g$ 或 $s\angle_K h$，再次应用习题 14-5(1)得 $g\in I_K[S]$或者 $h\in I_K[S]$。□

14.3　strand-图理论的几个普遍结论

今后用 K_P 表示攻击者已知的密钥集合，它反映了攻击者的知识。若 $t\angle$un_term(y)，则称 t 是 strand y 上的消息式的子项。对一个 strand-图 G，除攻击者 strand 之外的其它 strand 称为合法 strand。

定理 14.9　G 是一个 strand-图，$k \in \mathcal{K} - K_P$。如果 k 非源生于[5]任何合法的 strand，则在 G 的任何 strand y 上 k 都不可能是其消息式的子项。特别地，攻击者不可能得到 k(否则 k 将是 G 的某个攻击者 strand 的消息子项)。

证明　假若不然，则 S(k)={n∈G: k∠un_term(n)}非空。设 n*是 S(k)的极小元，由引理 14.4，n*是 k 的源生 strand。由定理的条件，k 非源生于任何合法 strand，因此 n*只能是攻击者 strand。以下对每一种攻击者 strand 逐一分析，证明这是不可能的。

(1) 若 n*是 M-strand: +t, $t \in T_p$，T_p 是 $\mathcal{T}$的一个子集：因为 $\mathcal{K}$、$\mathcal{T}$不相交，这不可能。

(2) 若 n*是 F-strand: - g：因为 n*是正号的，这不可能。

(3) 若 n*是 Tee-strand: -g,+g,+g：因为 n*是正号的，故 n*=-k+k+k 或 n*=-k+k+k，但由 strand 图的定义，必存在 strand s=…+k…∈G，s→-k+k+k<n*，从而 s *-小于 n*但显然 s∈S(k)，矛盾。

(4) 若 n*是 C-strand: -g, -h, +gh：因为 n*是正号的，故 n*=-g-h+gh，从而不妨设 k∠g，于是由 strand 图的定义，必存在 strand s=…+g…∈G，s→=-g-h+gh<n*，从而 s *-小于 n*但显然 s∈S(k)，矛盾。

(5) 若 n*是 S-strand: –gh, +g, +h：与情形(4)同理论证，这是不可能的。

(6) 若 n*是 K-strand:+k, $k \in K_p$：由定理的条件，$k \notin K_p$。

(7) 若 n*是 E-strand: $-k_0$, –h, $+\{h\}_{k0}$, $k_0 \in \mathcal{K}$：因为 n*是正号的，故 n*=$-k_0$–h+$\{h\}_{k0}$ 从而 k∠h，接下来仿照(4)同理论证这是不可能的。

(8) 若 n*是 D-strand: $-k_0^{-1}$, $-\{h\}_{k0}$, +h, $k_0 \in \mathcal{K}$ ：n*=$-k_0^{-1}$–$\{h\}_{k0}$+h 从而 k∠h，进而 k∠$\{h\}_{k0}$，接下来仿照(4)同理论证这是不可能的。□

不难验证一个有用的事实：$I \subset \mathcal{L}$，G 是一个 strand-图，n*是 S(I)={n∈G: un_term(n)∈I}的极小元，则 n*是 I 的入口点[6]。进一步说，I 定义做 G-诚实的，如果作为其入口点的攻击者 strand 只能是 M-strand 或 K-strand。直观地看，如果 I 是 G-诚实的则对 I 中消息的任何攻击只能依靠猜测。

定理 14.10　G 是一个 strand-图，$S \subset \mathcal{T} \cup K^0$，$K^* \subseteq K^0$，$K^0 \subseteq S \cup K^{*-1}$，则 $I_{K^*}[S]$是 G-诚实的。

证明　$I=I_{K^*}[S]$，注意到 $I \cap K^0 = S \cap K^0$ (显然 $S \cap K^0 \subseteq I \cap K^0$；又对于 $k \in I \cap K^0$ 有 $s \in S$ 使 s∠k，但由自由代数性质(4)和(5)知 k 是原子项，故 k=s∈S 从而 $I \cap K^0 \subseteq S \cap K^0$)，因此 $K^0 - I = K^0 - S \subseteq K^{*-1}$。由条件 $S \subset \mathcal{T} \cup K^0$ 知 S 的元素都是简约的且不形如$\{g\}_K$，因此引理 14.6

[5] 见 14.1.1 的定义。
[6] 同上。

到 14.8 适用。

设攻击者 strand m 是 I 的入口。首先注意到 m 不可能是 F-或 Tee-类型。

假若 m 是 C-strand，由于 m 是正号，因此 m=-g-h+gh，gh∈I。由引理 14.8，g∈I 或 h∈I，但这与 m 的 I-入口性质相矛盾。

假若 m 是 S-strand，不妨设 m=-gh+g+h，g∈I。I 是理想，故 gh∈I，与 m 的 I-入口性质相矛盾。

假若 m 是 E-strand，则 m=-k-h+$\{h\}_k$，$\{h\}_k$∈I。由引理 14.6 有 h∈I，与 m 的 I-入口性质相矛盾。

假若 m 是 D-strand，则 m=-k_0^{-1}-$\{h\}_{k0}$+h，h∈I。m 是 I-入口故 k_0^{-1}∉I，从而 k_0^{-1}∉S，再由条件 K^0⊆S∪K^{*-1}，知 k_0^{-1}∈K^{*-1} 从而 k_0∈K*，于是$\{h\}_{k0}$∈I，这又与 m 的 I-入口性质相矛盾。

因此，m 只能是 M-或 K-strand。□

下面是定理 14.10 的两个有用的推论。

定理 14.11　G 是一个 strand-图，K^0=S∪K^{*-1}，S 与 K_p 不相交。如果存在一个 strand m∈G 使 un_term(m)∈I_{K*}[S]，则必存在合法 strand n∈G 使 n 是 I_{K*}[S]的入口。

证明　假若不然，则 I_{K*}[S]-入口只有攻击者 strand。由定理的条件，{m∈G: un_term(m)∈I_{K*}[S]}非空，故有极小元 m*，因此 m*是 I_{K*}[S]-入口。因为 m*只能是攻击者 strand，由定理 4-10 知 m*只能是 M-strand 或 K-strand。

因 K^0=S∪K^{*-1} 故 S⊂K^0，从而 I_{K*}[S]∩$\mathscr{T}$为空，由此 m 不可能是 M-strand。因 S 与 K_p 不相交，故 m 也不是 K-strand。这与上一段的结论矛盾。□

定理 14.12　G 是一个 strand-图，K^0=S∪K^{*-1}，S 与 K_p 不相交。如果 G 的任何合法-strand 都不是 I_{K*}[S]的入口，那么任何形如$\{g\}_k$，k∈S 的消息项都不可能源生于攻击者 strand。

证明　由定理 14.11，对 G 的任何 strand m，un_term(m)∉I=I_{K*}[S]。假若 t=$\{g\}_k$，k∈S 源生于攻击者 strand m，不难验证 m 不可能是 F、Tee、K、M、C 和 S 类型。

假若 m 是 E 类型，m=–k_0–h+$\{h\}_{k0}$，但 k_0∉I，因此 k_0∉I 故 k_0≠k。由于$\{g\}_k$∠$\{h\}_{k0}$ 知$\{g\}_k$∠h，这与 m 的 I-入口性质矛盾。

假若 m 是 D 类型，n*=–k_0^{-1}–$\{h\}_{k0}$+h，$\{g\}_k$∠h，从而$\{g\}_k$∠$\{h\}_{k0}$，这又与 m 的 I-入口性质矛盾。□

14.4　协议的安全性质

当协议表示为 strand-图时，协议的安全性质也就转化为 strand-图应具有的结构特征。这里讨论最重要、最常用的两个安全性质—身份认证性质和保密性质—所对应的 strand-图的结构特征。

强身份认证性质如下刻画：

协议的 strand-图 G 若含有带参数失量 x 的接受方-strand s(x)，则一定含有带对应参数失量 y 的发起方 strand t(y)，且 t(y)在 G 上唯一。

如果不要求唯一性，就得到弱身份认证性质：

协议的 strand-图 G 若含有带参数失量 x 的接受方-strand s(x)，则一定含有带对应参数失量 y 的发起方 strand t(y)。

保密性质：

消息 z 在协议的 strand-图 G 上是保密的，若对任何 strand $n \in G$ 有 $un\_term(n) \neq z$。

14.5　协议分析的例子

这一节应用前面建立的普遍理论来具体证明两个协议的安全性，一个是在第 9 章详细讨论过的 Needham-Schroeder-Lowe 协议，另一个是 Otway-Rees 协议。这里将严格定义并证明这些协议的身份鉴别性质和保密性质。

14.5.1 Needham-Schroeder-Lowe 协议

$\mathscr{T}_{names} \subset \mathscr{T}$，Needham-Schroeder-Lowe 协议的 init-strand 是迹为

$$+\{N_a A\}_{KB}-\{N_a N_b B\}_{KA}+\{N_b\}_{KB}$$

的 strand，其中 $A、B \in \mathscr{T}_{names}$，$N_a、N_b \in \mathscr{T}$，$N_a \notin \mathscr{T}_{names}$，记做 $init[A,B,N_a,N_b]$。

resp-strand 是迹为

$$-\{N_a A\}_{KB}+\{N_a N_b B\}_{KA}-\{N_b\}_{KB}$$

的 strand，其中 $A、B \in \mathscr{T}_{names}$，$N_a、N_b \in \mathscr{T}$，$N_b \notin \mathscr{T}_{names}$，记做 $resp[A,B,N_a,N_b]$。

由上面两种 strand 连同攻击者 strand 组成的 strand-图定义做 NSL strand-图。下面的定理表明协议的弱身份鉴别性质成立。和以前一样，K_p 表示攻击者已知密钥的集合。

定理 14.13　G 是一个 NSL strand-图，$s=resp[A,B,N_a,N_b]\in G$，$k_A^{-1}\notin K_p$，$N_a\neq N_b$，N_b 在 G 上唯一源生，则必存在 $t=init[A,B,N_a,N_b]\in G$。

在证明之前，注意定理的条件都是自然的：$k_A^{-1}\notin K_p$ 意味着攻击者未知 A 的私钥；只要 N_a、N_b 是随机数，$N_a\neq N_b$ 和 N_b 在 G 上唯一源生都是可满足的(从计算密码学的观点看，这两个条件不成立的概率可忽略)。

我们用下面一系列的引理来证明这一定理。先约定几个特殊的符号：$n_0=^{-}\{N_aA\}_{KB}\underline{+\{N_aN_bB\}_{KA}}^{-}\{N_b\}_{KB}$，$n_3=^{-}\{N_aA\}_{KB}+\{N_aN_bB\}_{KA}\underline{^{-}\{N_b\}_{KB}}$，$n^*=\underline{^{-}\{N_aA\}_{KB}}+\{N_aN_bB\}_{KA}{}^{-}\{N_b\}_{KB}$，$v_0=\{N_aN_bB\}_{KA}$，如图 14-4。

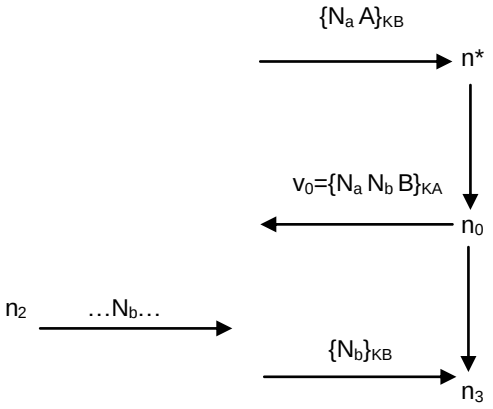

图 14-4 NSL 的接受方 strand

引理 14.14　N_b 源生于 n_0。因此由定理 14.13 的条件得 N_b 唯一源生于 n_0。

证明　只要检验 $N_b\angle un_term(n^*)$不成立。$un\_term(n^*)=\{N_aA\}_{KB}$，因此只要检验 $N_a\neq N_b$ 和 $A\neq N_b$，而前者是定理的条件，后者是因为 $N_b\notin\mathcal{T}_{names}$。证毕。

引理 14.15　$S=\{n\in G: N_b\angle un\_term(n)$，但 $v_0\angle un_term(n)$不成立$\}$，n_2 是 S 的极小元，则 n_2 是合法 strand 且是正号的。

证明　显然 $n_3\in S$，故 S 非空，从而 n_2 存在。又 S 满足引理 4-3 的条件，故 n_2 正号。

假若 n_2 是攻击者 strand，下面逐一分析这是不可能的。

若 n_2 是 M-strand：$n_2=\underline{+N_b}$，这意味着 N_b 源生于 n_2，但引理 14.14 已证明 N_b 唯一源生于 n_0，矛盾。

若 n_2 是 F-strand：$n_2=\underline{^{-}N_b}$，这显然不成立。

若 n_2 是 Tee-strand：不妨设 $n_2=^{-}N_b\underline{+N_b}+N_b$，显然这时存在 $m=\ldots\underline{+N_b}\ldots\in S$ 使 $m\rightarrow\ ^{-}N_b+N_b+N_b<n_2$，即 n_2 不是 S 的极小元，矛盾。

若 n_2 是 C-strand：$n_2=^{-}g^{-}h\underline{+gh}$，$N_b\angle gh$ 但 $v_0\angle gh$ 不成立。不妨设 $N_b\angle g$，显然 $v_0\angle$

g 不成立，因此存在 m=…+g…∈S 使 m→−g−h+gh<n_2，即 n_2 不是 S 的极小元，矛盾。

若 n_2 是 E-strand：n_2=–k_0–h+$\{h\}_{k0}$ 从而 N_b∠h 但 v_0∠h 不成立，接下来仿照 C-strand 的情形论证这是不可能的。

若 n_2 是 D-strand：k_0∈$\mathscr{K}$，n_2=–k_0^{-1}–$\{h\}_{k0}$+h，N_b∠h 但 v_0∠h 不成立，从而 N_b∠$\{h\}_{k0}$ 且 v_0∠$\{h\}_{k0}$(假若 v_0∠$\{h\}_{k0}$ 不成立，由前面的论证立得 n_2 不是 S 的极小元)，因此 v_0=$\{h\}_{k0}$ 从而有 h= N_aN_bB、k_0=K_A，故存在 m=…+K_A^{-1}…∈G 使 m→–k_0^{-1}–$\{h\}_{k0}$+h<n_2，但 k_A^{-1}∉K_p，由定理 14.9 知 k_A^{-1} 只能源生于合法 strand，但显然 NSL strand-图上不存在这样的合法 strand，矛盾。

若 n_2 是 S-strand：不妨设 n_2=–gh+g+h，N_b∠g 但 v_0∠g 不成立，于是必有 v_0∠h。令 T={m∈G: m<n_2 且 gh∠un_term(m)}，显然没有合法的 NSL-strand 能满足 T 的条件，因此 T 的元素都是攻击者 strand，设其极小元为 m*。

显然 m*不能是 M、F、Tee、K 类型的攻击者 strand，不难验证 m*也不能是 S、E、D、C 类型的攻击者 strand。□

引理 14.16　设 t 是含 n_2 的极大合法 strand，则存在 n_1 使 n_1<n_2<t 且 un_term(n_1)={N_a N_b B}$_{KA}$。

证明　如图 14-5，N_b 唯一源生于 n_0(引理 14.14)，n_2≠n_0(v_0∠un_term(n_0)但 v_0∠un_term(n_2)不成立)，因此 N_b 非源生于 n_2，存在 n_1 使 n_1<n_2<t 且 N_b∠un_term(n_1)。由 n_2 的极小性质，v_0=$\{N_aN_bB\}_{KA}$∠un_term(n_1)。注意到没有合法 NSL-strand 含有密文形式的真子项，故 v_0=un_term(n_1)。□

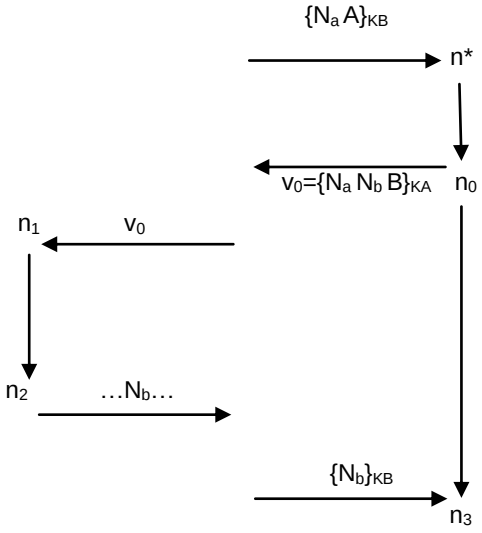

图 14-5 NSL 的身份鉴别性质

引理 14.17　含 n_1 和 n_2 的合法 strand t 必是 init[A,B,N_a,N_b]。

证明　直接检验 t 不能是 resp[A,B,N_a,N_b]。□

综合以上结果，定理 14.13 成立。这一弱身份鉴别性质不难推广到强身份鉴别性质，即定理 14.18(证明留做习题 14.11)。

定理 14.18　G 是 NSL strand-图，条件同定理 14.13 且 N_a 在 G 上唯一源生，则引理 14.17 中的 strand t=init[A,B,N_a,N_b]唯一。

对原始 Needham-Schroeder 协议以上分析会得出什么结论？事实上前面的论证仍然有效，特别是引理 14.16 有下面的形式：

引理 14.16*　设 t 是含 n_2 的极大合法 strand，则存在 n_1 使 $n_1<n_2<t$ 且 un_term(n_1)=$\{N_a N_b\}_{KA}$。

因为$\{N_a N_b\}_{KA}$不含标识 B，因此引理 14.17 的形式是：

引理 14.17*　含 n_1 和 n_2 的合法 strand t 必是 init[A,C,N_a,N_b]，这里 C 是某个参与者标识。

回顾第 9.1 节描述的攻击，这一弱形式的结论正是那里的攻击得以成功的原因！

下面的定理精确表达了协议的保密性质。

定理 14.19　G 是一个 NSL strand-图，s=resp[A,B,N_a,N_b]∈G，$k_A^{-1}\notin K_p$，$k_B^{-1}\notin K_p$，$N_a\neq N_b$，N_b 在 G 上唯一源生，则对所有满足 N_b∠un_term(m)的 m∈G，或者有$\{N_a N_b B\}_{KA}$∠un_term(m)，或者有$\{N_b\}_{KB}$∠un_term(m)。特别地，$N_b\neq$un_term(m)。

证明　沿用定理 14.13 中的记号，记 $v_3=\{N_b\}_{KB}$，集合 S={n∈G: N_b∠un_term(n)但 v_0∠un_term(n)和 v_3∠un_term(n)均不成立}。定理结论即断言 S 为空。假若 S 非空，设 n*是 S

的极小元，下面用两个引理来推出矛盾。

引理 14.20　n*不是 G 的合法 strand。

证明　假若 n*合法，首先注意 n*不在 s 上，这是因为 v_0=un_term(n_0)，而 $n_0 \notin S$。

n*不在 resp-strand $s_1 \neq s$ 上，否则 $n^*=\{NN_bC\}_{KD}$ 或 $n^*=\{N_bNC\}_{KD}$。若 $n^*=\{N_bNC\}_{KD}$，则 $s_1=-\{N_bD\}_{KC}+\{N_bNC\}_{KD}-\{N\}_{KC}$，$v_0 \angle \{N_bD\}_{KC}$ 不成立、$v_3 \angle \{N_bD\}_{KC}$ 不成立，故 $s_2=-\underline{\{N_bD\}_{KC}}+\{N_bNC\}_{KD}-\{N\}_{KC} \in S$ 但 s_2 显然小于 n*，与 n*的极小性矛盾；若 $n^*=\{NN_bC\}_{KD}$，$N \neq N_b$，则 N_b 源生于 n*，与引理 14.14 矛盾。

n*也不在 init-strand t 上，否则 $t=+\underline{\{N_bD\}_{KC}}-\{N_bNC\}_{KD}+\{N\}_{KC}$ 或 $+\{ND\}_{KC}-\{NN_bC\}_{KD}+\underline{\{N_b\}_{KC}}$。若 $t=+\underline{\{N_bD\}_{KC}}\ldots$，显然与 4-14 矛盾；若 $t=+\{ND\}_{KC}-\{NN_bC\}_{KD}+\underline{\{N_b\}_{KC}}$，由于 C≠B(否则 v_3=un_term(n*))，故 $+\{ND\}_{KC}-\underline{\{NN_bC\}_{KD}}+\{N_b\}_{KC} \in S$，与 n*的极小性矛盾。□

引理 14.21　n*不是攻击者 strand。

事实上不难仿照引理 14.15 证明该引理(留做习题 14.12)。至此，定理 14.19 得证。□

关于相反方向的身份鉴别性质可以用完全类似的方法证明：

定理 14.22　G 是一个 NSL strand-图，$t=init[A,B,N_a,N_b] \in G$，$k_A^{-1} \notin K_p$，$k_B^{-1} \notin K_p$，$N_a$ 在 G 上唯一源生，则必存在 resp[A,B,N_a,N_b]的长度为 2 的子 strand $s \in G$。

定理 14.23　G 是一个 NSL strand-图，$t=init[A,B,N_a,N_b] \in G$，$k_A^{-1} \notin K_p$，$k_B^{-1} \notin K_p$，$N_a$ 在 G 上唯一源生，则对所有满足 $N_a \angle$un_term(m)的 $m \in G$，或者有$\{N_aA\}_{KB} \angle$un_term(m)，或者有$\{N_aN_bB\}_{KA} \angle$un_term(m)。特别地，$N_a \neq$un_term(m)。

14.5.2 Otway-Rees 协议

图 14-6 是 Otway-Rees 协议的 strand-图，其中的消息式如下：

$M_1 = M\ A\ B\ \{N_a\ M\ A\ B\}_{KAS}$

$M_2 = M\ A\ B\ \{N_a\ M\ A\ B\}_{KAS}\{N_b\ M\ A\ B\}_{KBS}$

$M_3 = M\ \{N_a\ K_{AB}\}_{KAS}\{N_b\ K_{AB}\}_{KBS}$

$M_4 = M\ \{N_a\ K_{AB}\}_{KAS}$

A、B 是进程标识，S 是双方均信任的服务器，N_a、N_b 是动态生成的随机数，K_{AB} 是动态生成的会话密钥，用于 A、B 之间通讯，K_{AS}、K_{BS} 分别是 A 和 S、B 和 S 之间的对称加密钥。

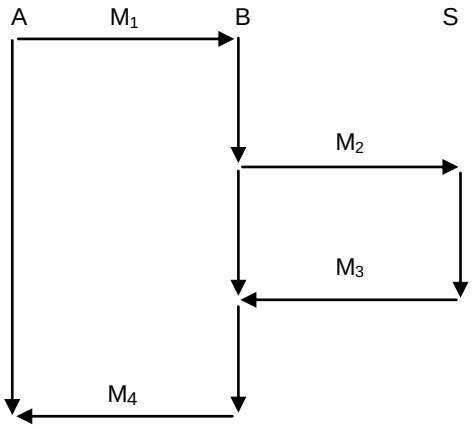

图 14-6 Otway-Rees 协议

与 14.5.1 小节一样，引进集合 $\mathscr{T}_{\text{names}} \subset \mathscr{T}$，A、B$\in \mathscr{T}_{\text{names}}$，M、$N_a$、$N_b \notin \mathscr{T}-\mathscr{T}_{\text{names}}$，协议的 init-strand 是迹为

$$+M\ A\ B\{N\ M\ A\ B\}_{KAS}\ -M\{N\ K\}_{KAS}$$

的 strand，记做 init[A, B, N, M, K]；resp-strand 是迹为

$$-M\ A\ B\ H+M\ A\ B\ H\{N\ M\ A\ B\}_{KBS}\ -M\ H_1\{N\ K\}_{KBS}+M\ H_1$$

的 strand，记做 resp[A, B, N, M, K, H, H_1]；serv-strand 是迹为

$$-M\ A\ B\{N_a\ M\ A\ B\}_{KAS}\{N_b\ M\ A\ B\}_{KBS}+\ M\ \{N_a\ K_{AB}\}_{KAS}\{N_b\ K_{AB}\}_{KBS}$$

的 strand，记做 serv[A, B, N_a, N_b, M, K]，其中 $K \notin K_p \cup \{K_{AS}: A \in \mathscr{T}_{\text{names}}\}$，$K=K^{-1}$。

引理 14.24　serv-strand 的集合、init-strand 的集合和 resp-strand 的集合互不相交。

证明　直接验证(留做习题 14-13)。□

称以上 strand 和攻击者 strand 组成的 strand-图为 OR strand-图。下面的定理刻画协议的保密性质。

定理 14.25　G 是 OR strand-图，A、B$\in \mathscr{T}_{\text{names}}$，K 在 G 上唯一源生，$K_{AS}$、$K_{BS} \notin K_p$，s=serv[A, B, N_a, N_b, M, K]。令 $S^0=\{K_{AS}, K_{BS}, K\}$，$K^*=\mathscr{K}-S^0$，则对任何 m$\in$G 有 un_term(m)$\notin I_{K^*}[K]$。

证明　只要证明(更强的命题)对任何 m$\in$G 有 un_term(m)$\notin I_{K^*}[S^0]$。注意到 $S^0 \cap K_p$ 为空、$K^*=K^{*-1}$、$\mathscr{K}=K^* \cup S^0$，由定理 14.10 只要证明没有合法节点是 $I_{K^*}[S^0]$的入口。

假若不然，设合法节点 m 是 $I_{K^*}[S^0]$的入口，因此 un_term(m)$\in I_{K^*}[S^0]$，从而 K_{AS}, K_{BS}, K 之一是 un_term(m)的子项。但显然 Otway-Rees 协议没有一个合法 Starnd 以 K_{AS} 或 K_{BS} 为消息子项，因此 K 必是 un_term(m)的子项。

如果 m 是正号，即存在一个合法 strand s=…+m…，则 K 是 un_term(m)的子项意味着：

s=serv[.,.,.,.,.,.]，m=+M_3 而 K 是会话密钥，或

s=resp[.,.,.,.,.,H,.]，m=+M_4 而 K 是 H 的子项。

因为 H 是 M_3 的子项而 M_3 为负，因此在第二种情形 m 显然不是 $I_{K^*}[S^0]$的入口。在第一种情形，un_term(m)=M$\{N_a\ K\}_{KAS}\{N_b\ K\}_{KBS}$，注意到 S^0 的元素显然都是简约的，故由引理 14.8 有 $M\in I_{K^*}[S^0]$或$\{N_aK\}_{KAS}\in I_{K^*}[S^0]$或$\{N_bK\}_{KBS}\in I_{K^*}[S^0]$。但这都不可能：由理想的定义知 $M\notin I_{K^*}[S^0]$，由 $K^*=\mathcal{K}-S^0$ 及引理 14.7 知$\{N_aK\}_{KAS}\notin I_{K^*}[S^0]$、$\{N_bK\}_{KBS}\notin I_{K^*}[S^0]$。□

现在分析协议的身份鉴别性质。

引理 14.26　G 是 OR strand-图，$X\in\mathcal{T}_{name}$，$K_{XS}\notin K_p$，则不存在形如$\{g\}_{KXS}$的消息项源生于 G 中的攻击者-strand。

证明　$S=\{K_{XS}\}$，$K^*=K$。首先证明没有合法-strand 是 $I_{K^*}[S]$的入口，或等价地，K_{XS} 不可能源生于合法 strand。事实上，注意到密钥 K 源生于合法 strand 仅当 K 是一个会话密钥，这时的合法 strand 是 serv[.,.,.,.,K,.,.]。由于 K_{XS} 不是会话密钥，因此 K_{XS} 不可能源生于合法 strand。再应用定理 14.12，即得结论。□

引理 14.27　G 是 OR strand-图，$\{H\}_{KXS}$ 源生于 G 中的一个合法 strand s：

若 s 是 serv-strand，则 H=NK，$N\in\mathcal{T}$，$K\in\mathcal{K}$；

若 s 是 init-strand，则 H=NMXC，$N\in\mathcal{T}$，X、$C\in\mathcal{T}_{name}$；

若 s 是 resp-strand，则 H=NMCX，$N\in\mathcal{T}$，X、$C\in\mathcal{T}_{name}$。

证明　设$\{H\}_{KXS}$ 源生于 strand s=…+m…：

若 s 是 init-strand，则只能有 s=+M_1…=+MAB$\{NMAB\}_{KAS}$…，即 H 形如 NMXC。

若 s 是 resp-strand，则只能有 s=$-M_1+M_2-M_3+M_4$ 或 s=$-M_1+M_2-M_3+M_4$。显然 M_2 中的明文有形式 H=NMCX。M_4 中的密文项不是在 resp-strand 上源生的。

同理论证 s 是 serv-strand 时的情形。□

引理 14.28　G 是 OR strand-图，s 是 G 中的一个合法 strand s：

若$\{N\ K\}_{KXS}$ 源生于 s，则或者 s=serv[A, X, N_1, N, M, K]、或者 s=serv[X, B, N, N_1, M, K]，并且每种情形都有 K 源生于 s；

若$\{N\ M\ A\ B\}_{KAS}$ 源生于 s，A≠B，则 s=init[A, B, N, M, K]且 N 源生于 s；

若$\{N\ M\ A\ B\}_{KBS}$ 源生于 s，A≠B，则 s=resp[A, B, N, M, K, H, H_1]且 N 源生于 s；

证明　这是引理 14.27 的直接推论。□

定理 14.29　G 是 OR strand-图，A≠B，N_a 在 G 上唯一源生，K_{AS}、$K_{BS}\notin K_p$。如果存在 t=

init[A, B, N_a, M, K]∈G，则存在 N_b∈$\mathscr{T}$、resp[A, B, N_b, M, *, *, *]的子-strand r∈G 和 s=serv[A, B, N_a, N_b, M, K]∈G，且 r 的长度≥2。

证明　定理的条件意味着 t=+MAB$\{N_aMAB\}_{KAS}$−M$\{N_aK\}_{KAS}$。$K_{AS}\notin K_p$，由引理 14.26 知 $\{N_aK\}_{KAS}$ 源生于 G 中的某个合法 strand β。由引理 14.28，β=serv[A,X,N_a,N_b,M*,K]或 serv[X,A,N_b,N_a,M*,K]，X∈$\mathscr{T}_{name}$。

对 β=serv[A,X,N_a,N_b,M*,K]=−M_2+M_3，有$\{N_aM^*AX\}_{KAS}$∠M_2。由引理 14.26，$\{N_aM^*AX\}_{KAS}$ 源生于一个合法 strand β*，由引理 14.28 知 N_a 源生于同一个 β*。既然 N_a 唯一源生，故 β=β*，因此 M*=M、X=B、r=resp[A,B,N_b,M,.,.,.]。

由引理 14.26，$\{N_bMAB\}_{KBS}$ 源生于 G 中的某个合法 strand γ。由引理 14.28，γ=resp[A,B,N_b,M,.,.,.]=−M_1+M_2…，即 γ 的长度≥2。

对 β=serv[X,A,N_b,N_a,M*,K]=−M_2+M_3，有$\{N_aM^*XA\}_{KAS}$∠M_2。由引理 14.26，$\{N_aM^*AX\}_{KAS}$ 源生于一个合法 strand ξ*，由引理 14.28 知 N_a 源生于同一个 ξ*。N_a 唯一源生故 ξ=ξ*，再由引理 14.28 知 X=A=B，与 A≠B 矛盾。□

定理 14.30　G 是 OR strand-图，A≠B，N_b 在 G 上唯一源生，K_{AS}、$K_{BS}\notin K_p$。如果存在 resp[A, B, N_b, M, K, H, H_1]的长度至少为 3 的子-strand r∈G，则存在 init[A, B, *, M, *]的长度至少为 1 的子 strand t∈G 和 s=serv[A, B, *, N_b, M, K]∈G。

证明　定理的条件意味着 r=−MABH+MABH$\{N_bMAB\}_{KBS}$−MH*$\{N_bK\}_{KBS}$…，接下来的证明与定理 14.29 非常相似，读者不难自行完成。□

上面的定理是关于 Otway-Rees 协议的身份鉴别性质的精确刻画。注意定理 14.29 和 14.30 的结论都不够强，并且不能再进一步增强以达到身份鉴别性质的要求。实际上，这一结论蕴涵了对协议的攻击是可能的，见图 14-7。于是，我们从对于协议 strand-图模型的精确刻画导出了一种攻击途径。图中有两个 serv-strand：S=serv[A, B, N_a, N_b, M, K_{AB}]，S*= serv[A, B, N_a, N_b, M, K^*_{AB}]。消息式如下：

$$M_1 = M\ A\ B\ \{N_a\ M\ A\ B\}_{KAS}$$

$$M_2 = M\ A\ B\ \{N_a\ M\ A\ B\}_{KAS}\{N_b\ M\ A\ B\}_{KBS}$$

$$M_3 = M\ \{N_a\ K_{AB}\}_{KAS}\{N_b\ K_{AB}\}_{KBS}$$

$$M^*_3 = M\ \{N_a\ K^*_{AB}\}_{KAS}\{N_b\ K^*_{AB}\}_{KBS}$$

$$M_4 = M\ \{N_a\ K_{AB}\}_{KAS}$$

$$M^*_4 = M\ \{N_a\ K^*_{AB}\}_{KAS}$$

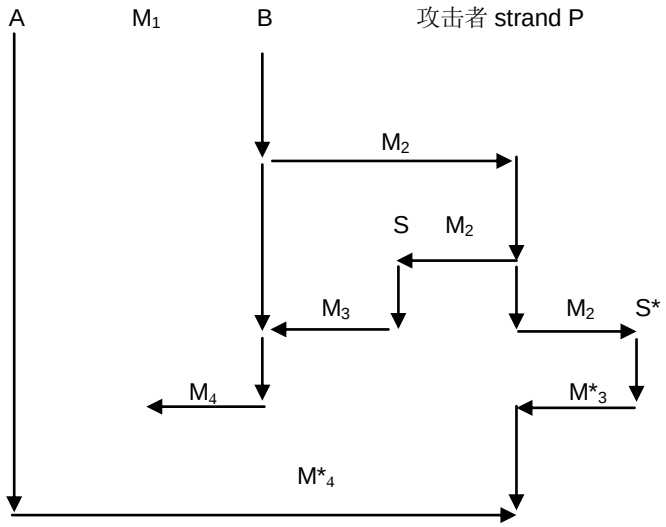

图 14-7 对 Otway-Rees 协议的一种攻击

14.6 小结与进一步学习的指南

strand 图理论发表于 Fabrega、Jonathan 和 Guttman 的论文，该文写得非常深入浅出：

Fabrega. F.J.T., Herzog J.C and Guttman J.D., *strand Spaces: Proving Security Protocols Correct*, Journal of Computer Security, 7(1999), 191-230.

strand-图属于 Dolev-Yao 模型，这是密码协议分析的最一般性的形式分析框架，他们的经典论文在该领域被广泛引用：

Dolev D.and Yao C.A. *On the security of public-key protocols*. IEEE Transactions on Information Theory, 1983, 29(2): 198~208。Yao 在计算密码学领域也有经典性的贡献，他在 2000 年获 Turing 奖,是获该奖的第一位华裔计算机科学家。

形式模型的自动求解是这样一类技术，它把协议是否具有某种安全性质这一命题转化为协议的形式模型能否满足某种形式方程(组)的可满足性问题。除了直观(但很有效)的 *strand*-图模型，其它重要类型的密码协议形式模型还有 *Abadi-Gordon* 进程代数/spi 演算模型、FRD/CPS 进程代数模型和 *Mitchell-Scedov* 概率进程代数模型，第 9 章最后提及的逻辑方法也属于其中之一。对每一种形式模型都可以发展一套专门的自动分析技术，甚至可以说，创造各种形式模型的目的就在于寻求各种有效的自动分析技术。关于 *strand*-图模型的自动分析技术的系统讨论可以参考第 8 章介绍过的作者的专著第 10-11 章，此外其第 12-13 章还进一步讨论了最新的形式分析方法与计算密码学方法相结合的技术。关于各种形式模型及其自动分析技术的很好的综述可以参考 C. Meadows *Formal Methods for Cryptographic Protocol*

Analysis: Emerging Issues and Trends, IEEE Journal on Selected Areas in Communication, 2003, 21(1):44-54

最后需要指出关于第 14.4 节所建立的消息保密性质的一个微妙的事实：那里对消息 z 的保密性质的形式安全刻画只相当于要求攻击者在任何情况下都得不到完整的秘密表达式 z 本身，但并不排除可以得到 z 的某种部分信息。例如，z 是一个协商生成的保密会话密钥，如果攻击者能够得到 z 的 50%的比特，按照这里的定义该协议将是安全的！显然这不太符合现实需要，换句话说，形式模型所蕴涵的安全目标似乎不够充分，从而降低了形式分析理论的安全性结论的现实意义。这实际上也是各种形式模型理论及其分析技术所存在的普遍问题，解决的办法是结合所谓计算密码学技术；但另一方面，形式分析方法有一个无可替代的优点是可以实现自动分析，从而最终有可能把协议的安全分析与验证归结为纯粹代数式的演算！由此读者不难想象，真正既有效率又充分保证安全性的分析途径可能是将形式模型技术和计算密码学技术两者想结合，事实确实如此。将这两种风格迥异的计算机密码学联系起来的经典结果是发表于 2000 年的著名的 *Abadi-Rogaway* 定理，概要地说，这一定理表明如果形式表达式满足某种形式法则，则它的计算密码学语义确实满足计算密码学意义上的安全性质。关于这方面的深入讨论见上面提到的作者的专著，一个浅显的导引见第 8 章介绍的 W.Mao 的教科书最后一篇“可证明的安全性”。

习　题

14-1 证明子项关系$\angle$是半序关系。

14-2 证明：若 $K\neq K_1$，$\{h\}_K\angle\{h_1\}_{K1}$，则必有$\{h\}_K\angle h_1$。

14-3 回顾 14.2 节关于$\angle_K$的定义，证明 $g\angle_K h$ iff $g\in I_K[h]$，即 $I_K[h]=\{t: h\angle_K t\}$。

提示：$h\angle_K t$ 则对任何 s 有 $h\angle_K ts$、$h\angle_K st$，且对任何 $k_0\in K$ 有 $h\angle_K\{t\}_{k0}$，故$\{t: h\angle_K t\}\vartriangleleft_K\mathscr{L}$ 且显然含有 h；又由 $I_K[h]$的构造推出对任何 $t\in I_K[h]$有 $h\angle_K t$，故 $I_K[h]=\{t: h\angle_K t\}$。

14-4 $K\subset\mathscr{K}$，$I_1\vartriangleleft_K\mathscr{L}$、$I_2\vartriangleleft_K\mathscr{L}$，则 $I_1\cap I_2\ \vartriangleleft_K\mathscr{L}$、$I_1\cup I_2\ \vartriangleleft_K\mathscr{L}$。

14-5 (1)$I_K[H]=\{t:$ 存在 $h\in H$ 使 $h\angle_K t\}$

(2) $I_K[H]=\cup_{x\in H}I_K[x]$

(3) $I_K[H_1\cup H_2]=I_K[H_1]\cup I_K[H_2]$

(4) $I_K[H_1\cap H_2]\subseteq I_K[H_1]\cap I_K[H_2]$

提示：(1)由习题 14-3 的方法同理论证，(2)是(1)和习题 14-3 的推论，(3)、(4)是(2)的推论。

14-6　K_1、$K_2 \subset \mathscr{K}$，则

(1) $I_{K1}[H] \cup I_{K2}[H] \subseteq I_{K1 \cup K2}[H]$

(2) $I_{K1 \cap K2}[H] \subseteq I_{K1}[H] \cap I_{K2}[H]$

14-7 应用习题 14-5(1)重新证明引理 14-5 和引理 14-6。

提示(引理 14-5 的证明)：由$\{h\}_K \in I_{K^*}[S]$知存在 $s \in S$ 使 $s \angle_{K^*} \{h\}_K$。因 $s \neq \{h\}_K$ 故必有 $s \angle_{K^*} h$，即 $h \in I_{K^*}[S]$。

14-8　补足定理 14.9 中省略的论证。

14-9　$I \subset \mathscr{L}$，G 是一个 strand-图，n*是 S(I)={n∈G: un_term(n) ∈I}的极小元，则 n*是 I 的入口点。

14-10　回顾引理 14.15 的证明，验证 m*也不能是 S、E、D、C 类型的攻击者 strand。

14-11 证明定理 14.18。

14-12 仿照引理 14.15 证明引理 14.21。

14-13 证明引理 14.24。