密码协议形式化分析的计算合理性

王全来[1,2],王亚弟[1],韩继红[1]
WANG Quan-lai[1,2],WANG Ya-di[1],HAN Ji-hong[1]

1.解放军信息工程大学 电子技术学院,郑州 450004
2.解放军防空兵指挥学院,郑州 450052
1.Institute of Electronic Technology,the PLA Information Engineering University,Zhengzhou 450004,China
2.The PLA Air Defense Forces Command College,Zhengzhou 450052,China
E-mail:wql_lai@126.com

WANG Quan-lai,WANG Ya-di,HAN Ji-hong.Computational soundness of formal analysis of cryptographic protocols. Computer Engineering and Applications,2007,43(21):8-11.

Abstract: Based on the Abadi-Rowgaway computational soundness theorem of formal encryption,this paper proposes and proves our computational soundness theorem of formal analysis of cryptographic protocols.Through the analysis for group key distribution protocols,our soundness theorem is stronger and powerful in adaptive attacks.This paper proposes formal definitions of security for group key distribution protocols both in the formal methods and the computational methods,then proves soundness of the formal definition.

Key words: formal method;computational method;soundness theorem;cryptographic protocol analysis

摘 要:基于 Abadi-Rowgaway 的形式化加密的计算合理性定理,提出和证明了密码协议形式化分析的计算合理性定理。通过对群密钥分配协议安全性的分析,说明定理对协议的可选择攻击具有较强的分析能力,提出了群密钥分配协议的形式化方法与计算方法下安全性的形式化定义,并证明了其合理性。

关键词:形式化方法;计算方法;合理性定理;密码协议分析
文章编号:1002-8331(2007)21-0008-04 **文献标识码**:A **中图分类号**:TP393

1 引言

在密码协议的分析中,形式化方法采用抽象的运行模型,密码学运算和对象是抽象的数据类型,计算方法基于更加详尽的运行模型,能够说明更多类型的协议攻击者,计算方法能够提供很强的安全性保证。如何将形式化安全性证明转化为计算模型中协议安全性的计算断言是当前的研究热点,文献[1]在这个方向上进行了有意义的研究,[1]中的 Abadi-Rowgaway 计算合理性定理说明如果表达式满足某个特定的条件(即不包含加密循环),则攻击者不能有效确定他所收到的值是表达式的还是模式的计算结果,但是对于密码协议的安全性分析,这个结果太简单,因为 Abadi-Rowgaway 定理涉及的仅是一方在已认证信道上向另一方发送一个单消息以及一个被动攻击者监视信道,文献[2]将[1]扩展到多个消息/用户的情形,但[2]没有说明消息是可变选择时的情况。

基于文献[1],论文提出了密码协议形式化分析的计算合理性定理,这个合理性定理可以分析在已认证信道上多方进行通信的协议,协议的运行模型包括一个能够观察信道上所有消息并能够改变协议运行流的攻击者,但不能修改、删除合法用户之间交换的消息。本文的结果改进了[1]的结果,并将这个合理性定理用于群密钥分配协议[3,4]的分析,而且提出了计算方法和形式化方法下的多点传送密钥分配协议安全性的形式化定义,证明了如果协议在形式化方法中是安全的,则协议的实现在计算方法中也是安全的。

2 基础知识

2.1 语法

设 $Keys$ 为有限密钥符号集合,$Const$ 为有限常数集合,给定安全参数 η,设 $Keys::=\{K_1,\cdots,K_n\}$,设 Exp 为基本表达式集合,其语法如下:

$M\rightarrow(M,M)|\{M\}_{K_1}|\{M\}_{K_2}|\cdots|\{M\}_{K_n}$

$M\rightarrow Keys\cup Const$ 中的每个符号,其中规则 $M\rightarrow(M,M)$ 表示对操作,$M\rightarrow\{M\}_{K_i}$ 表示用密钥 K_i 的加密。

对 $M\in Exp$,消息密钥 $MsgKeys(M)$ 是在 M 的子表达式中作为明文出现的密钥,用于加密子表达式的密钥称为加密密钥

基金项目:国家重点基础研究发展规划(973)(the National Grand Fundamental Research 973 Program of China under Grant No.TG 1999035801)。
作者简介:王全来(1970-),男,博士研究生,研究方向为密码学及其应用、信息安全;王亚弟(1953-),男,教授,博士生导师,研究方向为信息和网络安全;韩继红(1966-),女,副教授,研究方向为信息系统安全。

$EncKeys(M)$。在 M 中 K_i 加密 K_j,记为 $K_i \rightarrow_M K_j$,如果 M 包含一个子表达式 $\{M'\}_{K_i}$ 使得 $K_j \in MsgKeys(M')$;一个密钥是可恢复的,如果该密钥在 $MsgKeys(M)$ 中,记所有可恢复的密钥为 $RecKeys(M)$,所有不可恢复的密钥记为 $UEncKeys(M)$。

2.2 形式化语义

本文的模式定义不同于文献[1]中模式的定义,模式定义体现了加密方案满足选择明文攻击下语义安全[5]的概念。记 $struct(M)$ 为表达式 $M \in Exp$ 的结构,通过用符号 K' 替代 M 中所有的消息密钥、用 K 替代 M 中所有的加密密钥并用 c 替代 M 中所有的常数得到,其中 $K, K' \notin Keys, c \notin Const$ 是新鲜符号。

定义 1 (模式)对 $M \in Exp$,给定密钥集合 T,M 的模式记为 $pat(M,T)$,满足下述规则:

(1)如果 $M \in Keys \cup Const$,则 $pat(M,T)=M$;

(2)如果 $M=(M_1,M_2)$,则 $pat(M,T)=(pat(M_1,T),pat(M_2,T))$;

(3)如果 $M=\{M'\}_{K_i}$ 且 $K_i \in T$,则 $pat(M,T)=\{pat(M',T)\}_{K_i}$;

(4)如果 $M=\{M'\}_{K_i}$ 且 $K_i \notin T$,则 $pat(M,T)=\{struct(M')\}_{K_i}$。

M 的模式 $pattern(M)$ 定义为 $pat(M,RecKeys(M))$。

两个表达式 $M_1, M_2 \in Exp$ 是等价的,记为 $M_1 \equiv M_2$,如果 $pattern(M_1)=pattern(M_2)$;取决于重命名的等价关系记为 $M_1 \cong M_2$,如下:

定义 2 $M_1 \cong M_2$,当且仅当存在一个单射 $\sigma: Keys \rightarrow Keys$,使得 $M_1 \equiv \sigma M_2$,其中 σM_2 是对 M_2 中的密钥应用 σ 得到的结果。

2.3 计算语义

设对称加密方案 $\Pi=(\kappa,\varepsilon,D)$,$k^m(\eta)$ 为随机变量,表达式的计算语义以 η 为输入,并如下进行:

(1)分布 $k^{n+2}(\eta)$ 生成密钥向量 τ,其中 $n=|Keys|$,将 $Keys \cup (K,K')$ 中的所有密钥映射到 τ 的所有元素上,对 $i=1,\cdots,n$,$\tau[i]$ 对应于 K_i,$\tau[n+1]$ 对应于 K',$\tau[n+2]$ 对应于 K;

(2)对表达式 M,给定 τ,M 的比特串表示 $[[M]]_{\Pi,\tau}$ 为:

①如果 $M \in Const \cup c$,则 $[[M]]_{\Pi,\tau}$ 是 M 的比特串表示;

②如果 $M=K_i \in Keys$,则 $[[M]]_{\Pi,\tau}=\tau[i]$;如果 $M=K'$,则 $[[M]]_{\Pi,\tau}=\tau[n+1]$;

③如果 $M=(M_1,M_2)$,对 $M_1, M_2 \in \mathrm{Exp}'$,则 $[[M]]_{\Pi,\tau}$ 是 $([[M_1]]_{\Pi,\tau}, [[M_2]]_{\Pi,\tau})$ 的随机变量;

④如果 $M=\{M'\}_{K_i}$,对 $M' \in \mathrm{Exp}'$ 和 $K_i \in Keys$,则 $[[M]]_{\Pi,\tau}$ 是 $\varepsilon_{\tau[i]}[[M']]_{\Pi,\tau}$ 的随机变量;如果 $M=\{M'\}_K$,对 $M' \in \mathrm{Exp}'$,则 $[[M]]_{\Pi,\tau}$ 是 $\varepsilon_{\tau[n+2]}[[M']]_{\Pi,\tau}$ 的随机变量。

2.4 加密方案的安全性

对于抵制选择明文攻击是语义安全[5]的加密方案 $\Pi=(\kappa,\varepsilon,D)$,设 orcale $LR_{\Pi,b}$ 是一个程序,该程序用 κ 生成密钥 k,对每次询问 (M_0,M_1),都用密文 $\varepsilon_k(M_b)$ 进行应答,其中 M_0 和 M_1 等长,Π 是 IND-CPA 安全[6]的定义为:

定义 3 加密方案 Π 是 IND-CPA 安全的,如果对任一概率多项式时间的区分子 D,$\mathrm{Adv}_{\Pi}^{\mathrm{IND-CPA}}(D,\eta)=|\mathrm{Prob}[D^{LR_{\Pi,0}(\eta)}(\eta)=1]-\mathrm{Prob}[D^{LR_{\Pi,1}(\eta)}(\eta)=1]|$ 是 η 的可忽略函数。

3 密码协议形式化分析的合理性定理

3.1 合理性定理

对攻击者想得到可变选择表达式序列的计算结果进行建模,给定 Π,设 A 为概率多项式时间攻击者,发送由基本表达式组成的询问,第 i 个询问记为 $(M_0[i],M_1[i])$,对询问的选择取决于初始时随机采样的比特 $b(b \in \{0,1\})$;选定 b,A 用 oracle $O_{\Pi,b}$ 应答,$O_{\Pi,b}$ 选取 τ,并对每个询问用 $[[M_b[j]]]_{\Pi,\tau}$ 中的样本应答,具体如下:

oracle $O_{\Pi,b}(\eta)$	$\mathrm{Expt}_{\Pi}(A)$
设 $\tau \leftarrow k^{n+2}(\eta)$	设 $b \leftarrow \{0,1\}$,选定 η,运行 $A^{O_{\Pi,b}(\eta)}(\eta)$

对第 j 个询问 $(M_0[j],M_1[j])$,以 $[[M_b[j]]]_{\Pi,\tau}$ 中的一个样本进行应答

设 q 为 A 的询问的数量,$M_b=M_b[1\cdots q]$ 为由 $O_{\Pi,b}$ 加密的表达式序列,$M_0 \cong M_1$ 成立。在给出合理性定理之前,首先给出定义:

定义 4 $M_b[1\cdots q]$ 是合法的,如果满足下述两个性质:

(1)表达式 M_0 和 M_1 不包含加密循环;

(2)在 $M_b[1\cdots q]$ 中没有不可恢复的加密密钥,对 $i<j\leqslant q$

$UEncKeys(M_b[1\cdots i]) \cap MsgKeys(M_b[j])=\varnothing$

第一个性质在[1]中已经出现,第二个性质说明在密钥分配和配置阶段密钥的使用情况,在分配阶段,密钥为消息;在配置阶段,密钥用于加密其他的消息和密钥,定义这个性质的原因在于如果一个密钥首先用于加密消息,随后被泄漏,则先前收到的消息模式会发生改变。

$Expt_{\Pi}(A)$ 中的攻击者是合法的,如果 A 所发送的询问使得序列 $M_0[1]\cdots M_0[q]$ 和 $M_1[1]\cdots M_1[q]$ 都是合法序列,且 $M_0 \cong M_1$ 成立,设 A 的优势为 $\mathrm{Adv}_{\Pi}(A,\eta)=|\mathrm{Prob}[A^{O_{\Pi,0}(\eta)}(\eta)=1]-\mathrm{Prob}[A^{O_{\Pi,1}(\eta)}(\eta)=1]|$。

下面给出合理性定理:

定理 1 如果是 IND-CPA 安全的,则对合法攻击者 A,$Adv_{\Pi}(A,\eta)$ 是 η 的可忽略函数。

3.2 定理证明

3.2.1 合法表达式序列的序

对非循环表达式 $M \in Exp$,加密关系定义了 M 中密钥的一个偏序,对 $i<j\leqslant q$,$M[1\cdots i]$ 中没有不可恢复加密密钥是 $M[j]$ 中的消息密钥表示对 $i=1,\cdots,q$,$M[1\cdots i]$ 中没有不可恢复加密密钥能够在 $M[1\cdots(i+1)]$ 中被恢复出来,因此 $\mathrm{UEncKeys}(M[1\cdots 1]) \subseteq \mathrm{UEncKeys}(M[1\cdots 2]) \subseteq \cdots \subseteq \mathrm{UEncKeys}(M[1\cdots q])$ 为一个单调递增序列,这使得 M 的不可恢复加密密钥与集合 q 分开,记为 UEnc_i,UEnc_i 包含 $M[i]$ 中的加密密钥,但 UEnc_i 不在 $M[1]\cdots M[i-1]$ 中。

定义 4 表示对 $i<j\leqslant q$,UEnc_j 中没有密钥能够加密 UEnc_i 中的密钥,由 M 是非循环的,对 $M[1\cdots i]$,可以找到一个良序 $\leqslant$,使得对 $K_{i'} \in \mathrm{UEnc}_{i_1}$ 和 $K_{j'} \in \mathrm{UEnc}_{j_1}$,有 $K_{i'} \leqslant K_{j'}$,在所有的序中选择具有这个性质的第一个序,记为 $\leqslant_{M[1\cdots i]}$。

3.2.2 混合 oracle

定理 1 采用混合证明的方法,定义一个 $(2n+2)$ 混合 oracle 集合,并将合法攻击者区分这些 oracle 中的任一相邻对成功的

概率与区分它们相应实例成功的概率关联起来,接着应用这个关联证明具有不可忽略概率的合法攻击者如何完成对Π的IND-CPA安全性的成功攻击。

用 $O^0_{\Pi,0},\cdots,O^n_{\Pi,0},O^n_{\Pi,1},\cdots,O^0_{\Pi,1}$ 表示混合 oracle,两端混合 $O^0_{\Pi,0}$ 和 $O^0_{\Pi,1}$ 分别对应于 $b=0$ 和 $b=1$ 时 $O_{\Pi,b}$ 的两个实例,$O^0_{\Pi,0}$ 的行为与 $O^1_{\Pi,0}$ 的行为类似,以此类推到 $O^n_{\Pi,0}$;同样 $O^n_{\Pi,1}$ 的行为与 $O^{n-1}_{\Pi,1}$ 的行为类似,以此类推到 $O^0_{\Pi,1}$,对 $i=1,\cdots,n$,$O^i_{\Pi,0}$ 的定义为:

定义 5 oracle $O^i_{\Pi,0}(\eta)$

(1)设 $\tau\leftarrow\kappa^{n+2}(\eta)$;

(2)对第 j 个询问 $(M_0[j],M_1[j])$,如下应答:

①计算序 $\leqslant_{M_0[1\cdots j]}$,并设 S 为 $M_0[j]$ 中且在 $\leqslant_{M_0[1\cdots j]}$ 中是最小的 i 个密钥集合;

②设 M^{new} 为用 $\{struct(M')\}_{K_i}$ 替代 $M_0[j]$ 中所有形式为 $\{M'\}_{K_i}$ 的子表达式的表达式;

③返回模式 $[[M^{new}]]_{\Pi,\tau}$。

同样定义 oracle $O^i_{\Pi,1}$,不同之处在于①和②,即 $M_0[j]$ 用 $M_1[j]$ 代替,$\leqslant_{M_0[1\cdots j]}$ 用 $\leqslant_{M_1[1\cdots j]}$ 代替,由此推导出下述引理,限于篇幅,省略引理的证明过程:

引理 1 只要 oracle 收到合法攻击者的询问,$O^n_{\Pi,0}$ 和 $O^n_{\Pi,1}$ 具有相同的行为,即对任一询问序列,其中一个应答的分布与另一个应答的分布完全相同。

对 $i\in[n],b\in\{0,1\}$,A 区分 $O^i_{\Pi,b}$ 和 $O^{i-1}_{\Pi,b}$ 的优势为 $Adv_{\Pi,i,b}(A,\eta)=|Prob[A^{O^i_{\Pi,b}(\eta)}(\eta)=1]-Prob[A^{O^{i-1}_{\Pi,b}(\eta)}(\eta)=1]|$。

引理 2 说明这个优势与 $Expt_\Pi(A)$ 中优势的关系:

引理 2 $\sum_{i=1}^{n}\sum_{b\in\{0,1\}}Adv_{\Pi,i,b}(A,\eta)\geqslant Adv_\Pi(A,\eta)$

3.2.3 归约

给定合法攻击者 A,构造区分子 D,使得 A 在 $Expt_\Pi(A)$ 中成功的攻击可以有效地转变为 D 的攻击,D 在 $Expt_\Pi^{IND-CPA}$ 中的优势是 A 区分 $(O^i_{\Pi,b},O^{i-1}_{\Pi,b})$ 优势的 1/poly 倍,即 $Adv_\Pi^{IND-CPA}(D,\eta)=\frac{1}{n}E_{i\leftarrow[n],b\leftarrow\{0,1\}}(Adv_{\Pi,i,b}(A,\eta))=\frac{1}{n}\sum_{i=1}^{n}\sum_{b\in\{0,1\}}\frac{1}{n}\cdot\frac{1}{2}\cdot Adv_{\Pi,i,b}(A,\eta)$

由引理 2 可得 $Adv_\Pi^{IND-CPA}(D,\eta)\geqslant\frac{1}{2n^2}Adv_{\Pi,i,b}(A,\eta)$,因此 A 的不可忽略概率就意味着 D 的不可忽略概率,由此可以证明合理性定理。

设 E 为表示 D 选取 i'、b' 和 i 的事件,使得对 $j\in[n]$,下面条件中的一个成立:

(1)K_i 是 $\leqslant_{M_b[1\cdots j]}$ 的第 i' 个密钥;

(2)i' 大于 $M_{b'}[1\cdots j]$ 中不可恢复加密密钥的数量,且 K_i 不属于集合 $UEncKeys(M_{b'}[1\cdots j])\cup RecKeys(M_{b'}[1\cdots j])$。

当 E 发生时,如果给定 D 对 $LR_{\Pi,0}$(或 $LR_{\Pi,1}$)的访问权,则 A 接收所有响应就如同从 $O^{i'-1}_{\Pi,b'}$ 中接收一样,良序 $\leqslant_{M_{b'}[1]},\cdots,\leqslant_{M_{b'}[1\cdots q]}$ 的定义使得它们中的第 i' 个密钥与 $\leqslant_{M_b[1\cdots j]}$ 中的密钥完全一样,这表示 E 发生的概率等于选取 i 的概率,因为 i 是随机均匀选取的,其概率至少为 $1/n$,即 $Prob[E]=1/n$。

D 的优势函数:

$$\begin{aligned}Adv_\Pi^{IND-CPA}(D,\eta)&=|Prob[D^{LR_{\Pi,0}(\eta)}(\eta)=1]-Prob[D^{LR_{\Pi,1}(\eta)}(\eta)=1]|=\\&|Prob[D^{LR_{\Pi,0}(\eta)}(\eta)=1\wedge E]-Prob[D^{LR_{\Pi,1}(\eta)}(\eta)=1\wedge E]|=Prob(E)|Prob[D^{LR_{\Pi,0}(\eta)}(\eta)=1|E]-Prob[D^{LR_{\Pi,1}(\eta)}(\eta)=1|E]|=\\&\frac{1}{n}E_{i'\leftarrow[n],b'\leftarrow\{0,1\}}|Prob[A^{O^{i'}_{\Pi,b'}(\eta)}(\eta)=1]-Prob[A^{O^{i'-1}_{\Pi,b'}(\eta)}(\eta)=1]|=\\&\frac{1}{n}E_{i'\leftarrow[n],b'\leftarrow\{0,1\}}(Adv_{\Pi,i',b'}(A,\eta))\end{aligned}$$

这就是所要求的 D 的优势,至此证明了定理 1。

4 合理性定理的应用

通过多点传送密钥分配协议来说明定理 1 在实际密码协议分析中的应用,其中用户集合通过多点传送信道进行通信,集合中的一些用户(称为群成员)共享一个只有他们知道的秘密密钥,为了保持该群密钥的安全性,当有新成员加入或有旧成员离开群时,认证中心(称为群中心)广播消息使群成员更新密钥,这样做的目的是确保不是群的成员就不能计算群密钥。

这个问题文献[3-4,7]研究过,但这些文献很少涉及公式化一个合理的计算模型并用密码学方法证明其安全性,这些工作在证明协议的安全性时使用了 Dolev-Yao 模型,但却没有明确说明这样的分析如何关联到协议的实际安全性,而本文的合理性定理对形式化方法中协议安全性质的证明与计算方法中协议安全性质的证明的关联提供了一个有效的方法,即协议安全性质的证明可以从形式化观点转变为计算观点。

4.1 计算方法下的安全性

多点传送密钥分配协议 $p=\{I,G,U\}$,其中 I 为初始化程序,G 为群中心用于计算更新密钥消息的程序,U 为群成员 $U=\{u_1,\cdots,u_n\}$ 运行的程序,分别如下:I 以 η 为输入,输出群中心初始状态 s_0^G、用户初始状态 $s_0^1,\cdots,s_0^n$ 和初始群成员关系 $G_0\subset U(G_0=\varnothing)$;群中心程序 G 以 η、当前状态 s_t^G 和命令 com_t 为输入,返回消息 m_t 和群中心的更新状态 s_{t+1}^G,其中命令 com_t 既可是增加新用户的命令 $add(u_i)$ 也可是删除旧用户的命令 $del(u_i)$;群成员程序 U 以 η、$i\leqslant n$、u_i 的前一个状态 s_{t-1}^t 和当前更新密钥消息 m_t 为输入,输出串 k_t^i 和 u_i 的更新状态 s_t^i,k_t^i 对当前群 G_t 中的每个成员 u_i 都是一样的,称这个值为 t 时刻的群密钥,记为 k_t。

对议 $p=\{I,G,U\}$,考虑实验 $Expt_p^{gkd}$:首先 I 生成群中心和用

户的初始状态,给定不诚实用户集合 $B\subset U$ 及其初始状态$\{s_0^i|u_i\in B\}$,随后攻击者发送命令 $com_1,\cdots,com_t$ 并且对每个命令 $com_{t'}$,给定更新密钥消息 $m_{t'}$,设 $k_1,\cdots,k_t$ 为诚实用户在 $1,\cdots,t$ 时刻分别计算出的群密钥,$T\subseteq\{1,\cdots,t\}$为群中没有不诚实用户时的时间常数集合,$\bar{k}_T=\{k_i:i\in T\}$为相应的密钥,安全性要求是设$\bar{k}_T'$为$|T|$个均匀独立选取的密钥集合,b 为随机比特,在实验结束时,给定$\bar{k}_T$或$\bar{k}_T'$,攻击者的目标是正确猜出 b 的值。

设 $p_A(B,b)$为 A 在 Expt_p^{gkd} 中输出 1 的概率,A 的优势如下:

$$\mathrm{Adv}_p^{gkd}(A,B,\eta)=|p_A(B,0)-p_A(B,1)|$$

定义 6 多点传送密钥分配协议是安全的,如果对所有概率多项式时间攻击者 A 和集合 $B\subset U$,$\mathrm{Adv}_p^{gkd}(A,B,\eta)$是 η 的可忽略函数。

4.2 形式化方法下计算合理的安全性

设 $p_F=\{I_F,G_F,U_F\}$,其中 I_F 与 I 类似,不同之处在于 I_F 将每个用户的状态初始化为不变的唯一密钥 K_t,并将群中心的状态初始化为唯一密钥集合$\{K_1,\cdots,K_n\}$;群中心程序 G_F 接收命令 $\mathrm{add}(u_i)$和 $\mathrm{del}(u_i)$,对每个命令 com_t,返回 M_t,t 时刻 G_F 的内部状态由所有唯一密钥、更新密钥消息和群成员关系 G_t 组成;U_F 以 $i\leqslant n$ 为输入,返回密钥 K_t^i,设$\bar{M}_t$ 表示$(M_1,\cdots,M_t)$,对 $B\subset U$,K_B 表示用户的唯一密钥集合,Dolev-Yao 模型中多点传送密钥分配协议的安全性定义为:

定义 7 多点传送密钥分配协议 p_F 是安全的,如果对每个命令序列 $com_1,\cdots,com_t,B\subset U$,设 $K_{t'}$和 $G_{t'}$分别为在 t'时刻的群密钥和群成员集合,T 为使得 $B\cap G_{t'}=\emptyset$ 的所有 t'的集合,则有$((\bar{M}_t,K_T),K_B)\cong((\bar{M}_t,K_T'),K_B)$其中 $K_T=\{K_{t'}:t'\in T\}$,K_T'是$|T|$个新鲜密钥的集合。

由定理 1,给出关联定义 6 和定义 7 的定理 2:

定理 2 设 p_F 为 Dolev-Yao 模型下的多点传送密钥分配协议,且对命令序列 $com_1,\cdots,com_t$,群中心返回的更新密钥消息序列 $M_1,\cdots,M_t$ 是合法序列。设 Π 是 IND-CPA 安全的,如果 p_F 在 Dolev-Yao 模型下是安全的(定义 7),则 p_F^{Π}在计算方法下也是安全的(定义 6)。

证明(反证法):假设 p_F 满足定义 7,但 p_F^{Π}不满足定义 6。设 A 为可计算的攻击者,$B\subset U$,使得 $\mathrm{Adv}_p^{gkd}(A,B,\eta)$是不可忽略函数,给定 A 和 B,构造攻击者 A',A'首先对 B 中用户的唯一密钥询问自己的 oracle,并用 B 及相应的密钥调用 A,对于 A 的每个询问 $com_{t'}$,A'利用 G_F 来确定 $M_{t'}$,并确定相应的计算表示,最后 A'对(K_T,K_T')询问自己的 oracle,并将响应传给 A,这样 A 的输出就是 A'的输出。

给定 p_F 任一次运行,其更新密钥消息序列是合法序列,并且 K_T 中的密钥从不用作消息的加密密钥,由定理 1,可以证明 A'是合法攻击者,则 A'在 Adv_{Π}中的优势与 A 在 $\mathrm{Expt}_{p_F^{\Pi}}^{gkd}$ 中的优势完全一样,即如果后者是一个不可忽略的量,则前者也是,与假设矛盾,证毕。

很多实际的密钥分配方案(如文献[3])都满足定理 1 的前提条件,即要求所有的由协议产生的更新密钥消息序列都是合法序列,而且这些协议在形式化方法中很容易进行安全性证明,如果协议是安全的,则它的实现在计算方法中也是安全的。

5 结论

本文提出和证明了密码协议形式化分析的计算合理性定理,其中协议的攻击者可以发送一个可变选择的表达式序列,而不是文献[1]中的简单表达式;通过对群密钥分配协议的分析,证明了本文的计算合理性定理是可行和有效的,而且提出了群密钥分配协议的形式化方法与计算方法下安全性的形式化定义,并证明了该定义的合理性。本文所考虑的是对称加密运算,但该方法可以扩展到其他的密码学运算中。

(收稿日期:2007 年 4 月)

参考文献:

[1] Abadi M,Rogaway P.Reconciling two views of cryptography (the computational soundness of formal encryption)[J].Journal of Cryptology,2002,15(2):103-127.

[2] Abadi M,Jurgens J.Formal eavesdropping and its computational interpretation [C]//LNCS 2215:Proceedings of the 4th International Symposium on the Theoretical Aspects of Computer Software,2001:82-94.

[3] Rafaeli S,Hutchinson D.A survey of key management for secure group communication[J].ACM Computing Survey,2003,35(3):309-329.

[4] Wong C K,Gouda M,Lam S S.Secure group communication using key graphs[J].IEEE/ACM Transactions on Networking,2000,8(1):16-30.

[5] Goldwasser S,Micali S.Probabilistic encryption[J].Journal of computer and system science,1984,28(2):270-299.

[6] Mao Wenbo.Modern cryptography:theory and practice[M].Beijing:Publishing House of Electronics Industry,2004.

[7] Canetti R,Garay J,Itkis G,et al.Multicast security:taxonomy and some efficient constructions[C]//INFOCOM 1999.IEEE,1999,2:708-716.