多态性密钥交换协议的位独立性安全分析

尹毅峰[1] 丁汉清[1] 胡予濮[2]
(郑州轻工业学院计算机与通信工程学院 郑州 450002)[1]
(西安电子科技大学网络信息安全教育部重点实验室 西安 710071)[2]

摘 要 Diffie-Hellman协议是用于正规场景中的基于离散对数的密钥交换算法,该算法要求通信双方建立长期可信任的伙伴关系。基于多态性Diffie-Hellman密钥交换协议,提出更加安全的多态性密钥交换协议设计方案,在交换协议中附加了通信双方的身份信息,可以由通信双方各自的伪随机序列产生器来共同设计多态性S-盒,这种多态性S-盒在非正规的场景中可以得到广泛应用。

关键词 多态性密码,多态性虚拟S-盒,多态性密钥交换协议,位独立性准则
中图法分类号 TP393 **文献标识码** A

Research on BIC Security Mechanisms of the Polymorphic Key Exchange Protocol

YIN Yi-feng[1] DING Han-qing[1] HU Yu-pu[2]
(School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China)[1]
(Key Laboratory of Computer Network and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China)[2]

Abstract Diffie-Hellman key exchange algorithm, which is used in regular scenes based on the discrete logarithm problem, demands that both of two communication parties struck up a lively conversation long-term dependable fellowship. A much more secure polymorphic key exchange algorithm was proposed based on the Diffie-Hellman key exchange algorithm. The identity information of two parties can be appended to the agreement. Both communication parties use their PRNGs to finish the polymorphic virtual S-box together. The polymorphic S-box can become a broad agreement in irregular scenes.

Keywords Polymorphic cipher, Polymorphic virtual S-box, Polymorphic key exchange algorithm, Bit independence criterion

1 引言

会话密钥在安全的对称密码系统中具有至关重要的作用,生成数量足够大且随机的会话密钥能确保双方成功实现保密通信。Diffie-Hellman密钥交换算法是正规场景中会话密钥协商的典型协议。这种协议的有效性依赖于计算离散对数的难度,因此其设计成本较高,适用于建立长期信任关系的通信双方。

多态性密码(the Polymorphic Cipher,简记为PMC)是C. B. Roellgen在2004年提出的一种全新的非正规对称型加密理论[1],该理论属于流密码的范畴,在具体实现上又是分组密码和流密码的混合,为自编译类的加密算法提供了一种全新的密码反馈模式,其安全性主要依赖于自编译系统的不可读性,主要思想是提供一组候选单向函数$\{f_1, f_2, \cdots, f_n\}$或者一组安全子系统,利用攻击方攻击所产生的参数启动自编译系统,进行函数或者子系统的交叉组合,经过多轮迭代后,输出的序列满足密码学特性,可以抵抗差分密码分析和穷举攻击。C. B. Roellgen提出的多态性密码理论的主要应用场景是磁盘或者U盾等存储介质的加密,基于自编译系统不可读的工作原理,通信伙伴可以在被敌方攻击的同时产生安全的输出序列。

传统正规密码系统与多态性密码具有以下区别:传统正规密码在实施过程中要考虑密钥的效率,由于生成的密钥成本较高,正规密码系统采用标准化的安全证书,但是安全证书过于标准,证书生成的代价较高,其应用场景比较适合长期的通信伙伴使用;作为非正规的加密算法,多态性密码采用非正规的加密算法,具有随意性、随机性和方便性的特点,可以在广泛非正规的应用场景中为临时的通信伙伴提供快速安全的加密算法。

2 多态性密钥交换协议模型

以下是一个本文设计的基于多态性密码理论的密钥交换协议模型:

事先存在一个公开的含有自编译系统的虚拟函数

到稿日期:2011-04-29 返修日期:2011-07-14 本文受国家重点基础研究发展计划(973计划)课题(2009CB320404),郑州轻工业学院博士基金(2010BSJJ005)资助。
尹毅峰(1971-),男,副教授,主要研究方向为网络安全、多态性密码,E-mail:yinyifeng@yeah.net;丁汉清(1970-),男,副教授,主要研究方向为移动通信;胡予濮(1955-),男,教授,博士生导师,主要研究方向为网络与信息安全。

$F(x,y)$

其中 x,y 为待定参数。

A,B 分别拥有秘密 X 和 Y。

A 将秘密 X 代入虚拟函数，将 $F(X,y)$ 发送给 B，同时 B 也将 $F(x,Y)$ 发送给 A；

A 再将 X 代入 $F(x,Y)$，计算得到 $F(X,Y)$，同样 B 也将 Y 代入 $F(X,y)$ 得到 $F(X,Y)$；

交互完成。

攻击方 C 可以得到 $F(X,y)$ 和 $F(x,Y)$，但是由于自编译系统的不可读性，C 无法得到 X 和 Y，因此无法计算出 $F(X,Y)$。

若 C 要强行破解 $F(X,y)$ 和 $F(x,Y)$，由于 $F(x,y)$ 的自编译系统的作用，随着每次破解，C 将面临 $F(X,y)$ 和 $F(x,Y)$ 的变异函数类 $\{F^{(1)}(X,y),F^{(2)}(X,y),\cdots,F^{(n)}(X,y)\}$，$\{F^{(1)}(x,Y),F^{(2)}(x,Y),\cdots,F^{(n)}(x,Y)\}$。

3 基于自编译的多态性密钥交换协议设计方案

多态性密码理论提供了可实现的自编译密码通用模式[2]，利用构造复杂的迭代密码，可以对抗差分密码分析[3,4]和穷举攻击，该密码理论已经被用于磁盘文件的加密。本文将 PMC 用来解决在公用信道中通信双方的密钥协商难题。

以下是基于自编译的多态性密钥交换协议：

$$F(x_1,x_2,x_3,x_4,x_5,y_1,y_2,y_3,y_4,y_5)=S_a\circ S_b \tag{1}$$

式中，$x_1,x_2,x_3,x_4,x_5,y_1,y_2,y_3,y_4,y_5$ 为待定参数，S_a 和 S_b 分别为两个安全子系统。

子系统 S_a 可描述为

$$S_a=(p_1f_{a1}+p_2f_{a2}+\cdots+p_{16}f_{a16})\circ f_{Hash(m_{(i)(3)}m_{(i)(2)}m_{(i)(1)}m_{(i)(0)})} \tag{2}$$

式中，$p_i(i=1,2,\cdots,16)$ 为候选单向函数 f_{ai} 发生的概率；$m_{(i)(3)}m_{(i)(2)}m_{(i)(1)}m_{(i)(0)}$ 为 vu_a,vd_a,tu_a,td_a 所构成长序列中的连续 4 个比特位。

同理，子系统 S_b 可描述为

$$S_b=(q_1f_{b1}+q_2f_{b2}+\cdots+q_{16}f_{b16})\circ f_{Hash(m'_{(i)(3)}m'_{(i)(2)}m'_{(i)(1)}m'_{(i)(0)})} \tag{3}$$

式中，$q_i(i=1,2,\cdots,16)$ 为候选单向函数 f_{bi} 发生的概率；$m'_{(i)(3)}m'_{(i)(2)}m'_{(i)(1)}m'_{(i)(0)}$ 为 vu_b,vd_b,tu_b,td_b 所构成长序列中的连续 4 个比特位。

A 拥有秘密 k_a,vu_a,vd_a,tu_a,td_a，B 拥有秘密 k_b,vu_b,vd_b,tu_b,td_b。A 将秘密 k_a,vu_a,vd_a,tu_a,td_a 代入虚拟函数 $F(x_1,x_2,x_3,x_4,x_5,y_1,y_2,y_3,y_4,y_5)$，将 $F(k_a,vu_a,vd_a,tu_a,td_a,y_1,y_2,y_3,y_4,y_5)$ 发送给 B，同时 B 也将 $F(x_1,x_2,x_3,x_4,x_5,k_b,vu_b,vd_b,tu_b,td_b)$ 发送给 A；

A 再将 k_a,vu_a,vd_a,tu_a,td_a 代入 $F(x_1,x_2,x_3,x_4,x_5,k_b,vu_b,vd_b,tu_b,td_b)$，计算得到 $F(k_a,vu_a,vd_a,tu_a,td_a,k_b,vu_b,vd_b,tu_b,td_b)$，同样 B 也将 k_b,vu_b,vd_b,tu_b,td_b 代入 $F(x_1,x_2,x_3,x_4,x_5,k_b,vu_b,vd_b,tu_b,td_b)$ 得到 $F(k_a,vu_a,vd_a,tu_a,td_a,k_b,vu_b,vd_b,tu_b,td_b)$；

交互完成。

攻击方 C 可得到 $F(k_a,vu_a,vd_a,tu_a,td_a,y_1,y_2,y_3,y_4,y_5)$ 和 $F(x_1,x_2,x_3,x_4,x_5,k_b,vu_b,vd_b,tu_b,td_b)$，但是由于自编译系统的不可读性，$C$ 无法得到 k_a,vu_a,vd_a,tu_a,td_a 和 k_b,vu_b,vd_b,tu_b,td_b，因此无法计算出 $F(k_a,vu_a,vd_a,tu_a,td_a,k_b,vu_b,vd_b,tu_b,td_b)$。

若 C 要强行破解 $F(k_a,vu_a,vd_a,tu_a,td_a,y_1,y_2,y_3,y_4,y_5)$ 和 $F(x_1,x_2,x_3,x_4,x_5,k_b,vu_b,vd_b,tu_b,td_b)$，由于安全子系统 S_a 和 S_b 内部的自编译系统的作用，随着每次破解，C 最终将面临 $F(k_a,vu_a,vd_a,tu_a,td_a,y_1,y_2,y_3,y_4,y_5)$ 的变异函数类

$$\begin{Bmatrix} F^{(1)}(k_a,vu_a,vd_a,tu_a,td_a,y_1,y_2,y_3,y_4,y_5) \\ F^{(2)}(k_a,vu_a,vd_a,tu_a,td_a,y_1,y_2,y_3,y_4,y_5) \\ \cdots \\ F^{(n)}(k_a,vu_a,vd_a,tu_a,td_a,y_1,y_2,y_3,y_4,y_5) \end{Bmatrix}$$

和 $F(x_1,x_2,x_3,x_4,x_5,k_b,vu_b,vd_b,tu_b,td_b)$ 的变异函数类

$$\begin{Bmatrix} F^{(1)}(x_1,x_2,x_3,x_4,x_5,k_b,vu_b,vd_b,tu_b,td_b) \\ F^{(2)}(x_1,x_2,x_3,x_4,x_5,k_b,vu_b,vd_b,tu_b,td_b) \\ \cdots \\ F^{(n)}(x_1,x_2,x_3,x_4,x_5,k_b,vu_b,vd_b,tu_b,td_b) \end{Bmatrix}$$

C 无法得到 $F(k_a,vu_a,vd_a,tu_a,td_a,k_b,vu_b,vd_b,tu_b,td_b)$。

4 双方协商多态性 S-盒设计方案

定义 1(多态性虚拟 S-盒) 密钥协议双方在通信前各自持有含本身信息的随机参数组 $paras_a$ 和 $paras_b$，利用控制密钥调用多态性密码中置换函数构造出左(右)子算法集，该子算法集在未获得另一随机参数组的情况下，不具备混淆和置换能力，称为多态性虚拟 S-盒。

在构造 S-盒之前，可以先设置一个公开的含有自编译系统的虚拟函数，通信双方共同构造 S-盒的协议步骤如下：

Step1 A 和 B 作为通信的双方，采用自编译器和 Hash 映射相结合的方法将各自的私钥 k_a、k_b 加密，并将网络中获得的 4 个随机种子 vu,vd,tu,td 构成长序列，作为 PRNG 的参数，A 得到一个 PRNG 的左半参数组 $paras_a\{k_a\oplus G(vu_a),k_a\oplus G(vd_a),k_a\oplus G(tu_a),k_a\oplus G(td_a)\}$，将其代入 PRNG，设计一个半成品的 S-盒，即左半盒 S_a：

$$S_a=F(k_a,k_a\oplus G(vu_a),k_a\oplus G(vd_a),k_a\oplus G(tu_a),k_a\oplus G(td_a),y_1,y_2,y_3,y_4,y_5)$$

同样，B 得到右半参数组：

$$paras_b\{k_b\oplus G(vu_b),k_b\oplus G(vd_b),k_b\oplus G(tu_b),k_b\oplus G(td_b)\}$$

也设计出半成品 S-盒—右半盒 S_b：

$$S_b=F(x_1,x_2,x_3,x_4,x_5,k_b,k_b\oplus G(vu_b),k_b\oplus G(vd_b),k_b\oplus G(tu_b),k_b\oplus G(td_b))$$

Step2 利用公开的信道，A 将自己所生成的 S_a 发送给 B，同样 B 将 S_b 发送给 A。

Step3 A 再一次将自己所掌握的序列 $paras_a$ 代入 S_b 的左部，得到一个完整的 S-盒：

$$S_a=F(k_a,k_a\oplus G(vu_a),k_a\oplus G(vd_a),k_a\oplus G(tu_a),k_a\oplus G(td_a),k_b,k_b\oplus G(vu_b),k_b\oplus G(vd_b),k_b\oplus G(tu_b),k_b\oplus G(td_b))$$

B 也再一次将自己所掌握的序列 $paras_b$ 代入 S_a 的右部，得到和 A 相同的完整 S-盒：

$$S_a=F(k_a,k_a\oplus G(vu_a),k_a\oplus G(vd_a),k_a\oplus G(tu_a),k_a\oplus G(td_a),k_b,k_b\oplus G(vu_b),k_b\oplus G(vd_b),k_b\oplus G(tu_b),k_b\oplus G(td_b))$$

交互完成。

5 安全性分析

本文所设计的这种多态性密钥交换协议可以用于设计快

速安全的 S-盒，因此，其安全性也可以采用 S-盒的 3 个设计标准来衡量。安全的 S-盒必须满足输出位独立性、非线性[5,6]和严格雪崩这些准则，其中严格雪崩准则的安全性分析工作已经进行了研究[7,8]，本文主要研究这种新型密钥交换协议的输出位独立性准则的性能。

5.1 输出位独立性分析

攻击者对所截取的半 S-盒 S_a 和 S_b 进行相关性分析操作时，可以将海明重量为 1 长度为 n 的所有序列(0,0,…,0,1)，(0,0,…,1,0)，…，(1,0,…,0,0)作为参数代入 S_a 或 S_b，试图求解 S_a 或 S_b 的相关关系，本文则利用输出位独立性准则的性能。

相关系数是描述两个随机变量之间的相关程度的指标。两个随机变量的关系可分为独立和相关，在相关中，又可以分为线性和非线性相关，非线性的种类非常多，至今无实用指标来区分它们，但线性相关可以用线性相关系数来描述，这个指标在线性方面的应用已经非常成熟，并得到国际的认可和通用。利用相关系数可以分析输出序列的位独立性特性。其中 $Cov(x,y)$为 x 与 y 之间的协方差，$Cov(X,Y)=E(XY)-E(X)E(Y)$。

若 X 与 Y 独立，则 $Cov(X,Y)=0$。

随机变量和的方差与协方差的关系

$$D(X+Y)=D(X)+D(Y)+2Cov(X,Y) \tag{4}$$

$$D(\sum_{i=1}^{n}X_i)=\sum_{i=1}^{n}D(X_i)+2\sum_{i<j}\sum Cov(X_i,X_j) \tag{5}$$

若 $X_1,X_2,\cdots,X_n$ 两两独立，上式化为

$$D(\sum_{i=1}^{n}X_i)=\sum_{i=1}^{n}D(X_i) \tag{6}$$

相关系数在−1～+1 之间，绝对值越接近 1 表示两个变量之间的相关程度越高，接近 0 表示相关性越差，0 表示没有相关性。

利用 $BIC(f)=\max_{j\neq k}BIC(a_j,a_k)$可以衡量函数 f 满足 BIC 的程度，严格地讲，若 f 完全满足 BIC，则必须 $BIC(f)=0$。

为了验证改进方法输出位独立性准则，在实验中对输出进行量化分析，可以利用海明距离来观察海明距离为 1 的两个输入向量和两个输出向量的改变程度，从统计学角度对同一个随机性检测项目中 2 个独立的参数所应满足的条件进行了研究[9]，用概率统计输出序列中两个 Bit 的相关程度。实验中选取了不同长度的输出序列，$n=8,16,32,64,128$，图 1 显示了节点上所安装的系统在一个时段内因所截获的 d_i 和 u_i 的位而引起的输出序列的变化情况，统计了不同长度输出序列所得到的相关性系数，随着 n 的增大，相关性系数取值快速下降，根据本文所构造的强单向函数 f 得到的 $BIC(f)$来分析改进后的多态密码是否满足位独立性准则。

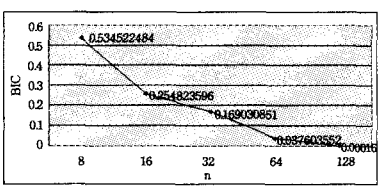

图 1 不同长度的输出序列所获得的 BIC 相关系数

5.2 与 Diffie-Hellman 密钥交换算法比较

利用虚拟 S-盒实现的多态性 S-盒密钥交换协议可以弥补 Diffie-Hellman 算法中的不足之处：

1. 由于虚拟 S-盒中包含了通信双方的相关信息，无论是网络对等点的数据包信息还是用户特定的签名信息都可用作单方的控制密钥，有利于进行身份认证。

2. 由于这种改进型算法中的目的构件双方共享多态性 S-盒，内部的候选函数算法时间复杂度小，双方一次性生成的 S-盒可以根据公开的明文产生周期较长的加密序列，以此序列对通信内容进行 XOR 操作，速度较快，可以避免阻塞性拒绝服务攻击。

3. 不易遭受中间人的攻击：如果第三方 C 在和 A 通信时扮演 B；和 B 通信时扮演 A，A 和 B 都与 C 协商了一个虚拟 S-盒，A 保留虚拟 S-盒的左半部分实际参数，B 保留虚拟 S-盒右半部分实际参数，然而 C 即是拥有通信双方的含有部分实际参数的两个虚拟 S-盒，在未取得 A 和 B 完整参数的控制密钥的情况下，C 无法运行这个虚拟 S-盒。此时的两种情况为：

(1)B 与 C 共同构建了 $S_c\circ S_b$，A 和 C 共同构建了 $S_a\circ S_c$，这两个 S-盒的内部算法与 $S_a\circ S_b$ 完全不同，C 得不到 $S_a\circ S_b$。

(2)由于多态性虚拟 S-盒的生成速度很快，A 和 B 可以多次发送多组不同的虚拟 S-盒，随机协商，进行比对，防止 C 扮演截获并解析报文。

结束语 Diffie-Hellman 密钥协议是双方共同构造密钥的典型协议，原有多态性密码的密钥协商也采用了此方法，但此方法的不足之处是算法的时间复杂度较高，不利于加载个体信息，在抵抗欺骗攻击方面仍存在缺点。因此本章中对原有的 PMC 的密钥协商协议进行了改进，提出基于自编译理论的多态性密钥交换协议，双方的 S-盒的目的是用于产生长周期的 XOR 加密序列，双方可以随时协商，更换 S-盒内部的加密算法，一次性产生，可也产生一批长周期的加密序列，这种多态性 S-盒在非正规的场景中可以得到广泛应用。

参 考 文 献

[1] Roellgen C B. Polymorphic Cipher Theory [OL]. http://www.pmcciphers. com/technology/roellgen02generalizedPMCmodel. pdf, 2004

[2] Langford S K, Hellman M E. Different linear cryptanalysis[C]// Advanced in Cryptology CRYOTO'94 (INCS839). 1994:5-12

[3] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4(1):3-72

[4] Langford S K, Hellman M E. Different linear cryptanalysis[C]// Advanced in Cryptology -CRYOTO' 94 (LNCS839). Berlin: Springer-Verlag, 1994:5-12

[5] Zhang Mu-xiang, Chan A. Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers[C]//CRYPTO 2000. Berlin Heidelberg: Springer Verlag, 2000:501-514

[6] Abuelyman E S, Alsehibani A A S. An Optimized Implementation of the S-Box using Residues of Prime Numbers[J]. International Journal of Computer Science and Network Security, 2008, 8:304-309

[7] Yin Yi-feng, Li Xin-she, Hu Yu-pu, Fast S-box security mechanism research based on the polymorphic cipher[J]. Information Sciencesl, 2008, 178(6):1603-1610

[8] Li Xin-she, Du Xiao-hui, Yin Yi-feng, et al. Improvement of the Polymorphic Cipher and its Analysis of the Strict Avalanche Criterion[J]. Journal of Beijing University of Technology, 2009, 35(6):851-855

[9] Fan Li-min, Feng Deng-guo, Chen Hua. On the parameter selection of randomness test[J]. Journal on Communications, 2009, 30(1):1-6