DOI:10.16186/j.cnki.1673-9787.2006.04.020
第25卷第4期 河南理工大学学报 Vol.25 No.4
2006年8月 JOURNAL OF HENAN POLYTECHNIC UNIVERSITY Aug.2006

单向函数与对称密码体制

童亚拉
（湖北工业大学 理学院，湖北 武汉 430068）

摘要：可靠的密码学是建立在数学和形式化的计算机科学产生的结论之上的，本文从计算理论的角度阐述了构建对称密码体制所需的数学背景：算法复杂性与问题复杂性的关系；NP问题与密码学的关系；密钥长度与密码安全的关系．从保长和置换的概念入手，说明了构造对称密码体制的理论基础——单向置换和单向函数，并以计算机口令系统为实例说明了如何构造对称密码系统．

关 键 词：复杂性；可计算性理论；密钥；单向置换；单向函数；对称密码体制
中图分类号：TP301.5 文献标识码：A 文章编号：1007-7332（2006）04-0338-03

0 引 言

可靠的密码学是建立在数学和形式化的计算机科学产生的结论之上的，它是计算复杂性理论的重要实践领域．因为计算复杂性理论提供了一种分析不同密码技术和算法计算复杂性的方法，它对密码算法及技术进行比较，然后确定它们的安全性．

算法的复杂性即运行它所需的计算能力；密码算法则是用于加密和解密的数学函数，通常是两个相关函数．理论上，密码设计者都期望对其密码的任何攻击算法具有指数级的时间复杂性．事实上，在实际应用中的密码，其对应的攻击算法是超多项式时间复杂性的，并不能保证今后永远不会发现非多项式时间的攻击算法．

密码学的基础是一些难于求解的问题，并在此基础上构建加密算法，它要求攻击者在破译加密算法时必须做大量工作．NP问题与密码学的关系是：公开密钥算法能用非确定性多项式时间算法进行攻击．如已知密文C，密码分析者只需猜测一个明文X和一个密钥K，然后在输入X和K的基础上，以多项式时间运行加密算法，检查结果是否等于C；若相等，则表明该密文被破译．实际上，它给出了对此类密码算法进行密码分析复杂性的上限，也是密码分析者所需确定的多项式时间算法．而这个结论不是对所有的密码类型都适合，尤其不适合一次一密的加密方式，因为对于任何密文C，运行加密算法求解时可能有许多对X和K产生C，但大多数X都毫无意义，因而没有合法明文[1]．

密钥是加密和解密算法使用的一段信息，算法的安全性是基于密钥的安全性而不是基于算法细节的安全性，因此算法可以被公开、被分析，也可以产生大量使用某种算法的产品．即便攻击者知道算法也不可能获得明文，因为他不知道该算法所使用的密钥．如果密钥太短或不够长，可通过蛮力搜索整个密钥空间发现它．使密码绝对安全的惟一办法是使用与所发送报文一样长的密钥，但在通信量很大的情况下，密钥可能相当大，实际使用起来很不方便；用中等长度的密钥进行不限量安全通讯时，虽然可对密钥空间进行蛮力搜索，但搜索太慢，所以密码在实践中都有足够的安全性．正因为现在还没有办法保证使用中等长度密钥的密码是绝对安全的，即在数学上无法证明能快速地找到密钥，所以人们常通过实践证据来保证其安全性，即依赖密码专家对密码的质量进行评估，请他们破译密码，对他们都不能破译的密码，我们就会增加对该密码安全的信心，尽管这种方法存在明显不足，但却是目前为止惟一可行的正确选择．

收稿日期：2006-02-11
基金项目：高等学校博士学科专项科研基金资助项目（20030486049）
作者简介：童亚拉（1966-），女，讲师，湖南桃源人，从事计算机应用技术、软件理论等方面的研究．
E-mail：Junyan921217@Yahoo.com.cn

1　对称密码系统

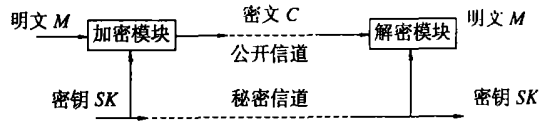

图 1　对称加密/解密示意

Fig.1　Diagram of encrypt/crack technology

对称算法有时又叫传统密码算法，就是加密密钥和解密密钥是相同的，或者虽不相同，但可从其中一个推导出另一个，因而又称“单密钥体制”. 对称密码系统为用户提供一个双向通道：A 和 B 共享一个密钥，使用该密钥，他们既然可以向对方发送加密信息，也可以解密对方发来的信息，这是对称性的一个主要优点[2]. 对称加密的算法是公开的，交换信息的双方不必交换加密算法，而是采用相同的加密算法，但需要交换加密密钥.

2　单向函数

如果对每一个 w，w 和 $f(w)$ 的长度相等，则称函数 $f:\sum^{*}\to\sum^{*}$ 是保长的；保长函数不会把两个不同的字符串映射到同一个字符串，即当 $x\neq y$ 时，$f(x)\neq f(y)$，则函数 f 是置换函数.

假定用概率图灵机 M 计算概率函数 $M:\sum^{*}\to\sum^{*}$，这里对每一个输入 w 和输出 x，令

$$Pr[M(w)=x]$$

为 M 从输入 w 开始停机在接受状态且停机时带的内容为 x 的概率.

由于 M 对输入 w 有可能不在接受状态停机，故

$$\sum_{x\in\sum^{*}} Pr[M(w)=x]\leqslant 1,$$

这里，f 表示容易计算的单向函数，M 表示企图反演 f 的多项式时间概率算法，$Pr_{[M(w)]}$ 所表示的概率是在 M 所作的随机选择和 w 的随机选取上获得的.

3　单向置换与单向函数

单向置换是一种简单的单向函数.

定义：单向置换是具有下述两条性质的保长置换 f：

(1) f 是多项式时间可计算的；

(2) 对于每一台多项式时间概率图灵机 M、每一个 k 和充分大的 n，如果取长度 n 的随机串 w，并且对输入 w 运行 M，则

$$Pr_{M,w}[M(f(w))=w]\leqslant n^{-k}.$$

定义：单向函数是具有下述两条性质的保长置换 f：

(1) f 是多项式时间可计算的；

(2) 对于每一台多项式时间概率图灵机 M、每一个 k 和充分大的 n，如果取长度 n 的随机串 w，并且对输入 w 运行 M，则

$$Pr_{M,w}[M(f(w))=y,\quad \text{其中 } y=f(w)]\leqslant n^{-k}.$$

对于单向置换，任何多项式时间概率算法只能以很小的概率反演 f，即不大可能从 $f(w)$ 计算出 w；对于单向函数，任何多项式时间概率算法不大可能找到一个映射到 $f(w)$ 的 y[3].

4　密码应用中的单向函数

用复杂性理论作为密码学基础的一个优点是它有助于论证密码安全性时澄清所做的假设，因此假设存在单向函数，能构造出安全的对称密码系统.

单向函数是对称密码体制的中心. 单向函数计算起来容易，但其求逆的过程非常困难. 若已知 x，计算 $f(x)$ 容易；但已知 $f(x)$，却难于计算出 x，这里“难”的意思是即使让世界上所有的计算机同时运算，从 $f(x)$ 计算出 x 也要花费数百万年时间. 虽然按严格的数学定义并不能证明单向函数的存在性，也没有实际的证据能构造出单向函数，但可以有效地利用它们. 例如在有限域中计算

x^2 很容易，但计算 $\sqrt{x}$ 却难得多．因为没法解开用单向函数加密的明文，所以用单向函数作加密函数毫无意义，但有一类特殊的单向函数，它在一个方向易于计算而反方向难于计算，但如果知道某个秘密也能很容易在另一个方向上计算出这个函数．也就是说，已知 x 易于计算 $f(x)$，而已知 $f(x)$ 却难于计算 x．但有一秘密消息 y，一旦给出 $f(x)$ 和 y 就很容易计算 x，单向陷门函数就是这样一个特殊的单向函数.

假设存在单向函数，则可构造出安全性可证的对称密码系统，一个简单的应用实例就是口令系统．我们知道，计算机没必要知道口令而只需有能力区别有效口令和无效口令，通过单向函数能很容易地实现，即计算机存储的是口令的单向函数而不是口令本身．在口令系统中，用户必须键入口令才能访问某个资源，系统以加密方式保存用户口令数据库，这是为了当数据库偶然地或故意地不受保护时保护它们．口令数据库经常是不加保护的，使得各种应用程序能够读它们和验证口令．当用户键入一条口令后，系统先对它加密，然后判断它是否与数据库中存储的形式相匹配，从而验证其有效性．很明显，加密方式是很难反演的，很难从口令的加密形式得到不加密的口令，所以选择单向函数作为口令加密函数.

5 结 论

计算复杂性理论是分析密码技术的计算要求和研究破译密码难度的基础，在现代密码中，密码系统的破译常归结为求解某个数学问题，求解数学问题算法的复杂性可通过计算复杂性理论来描述，因此计算复杂性理论为破译密码提供了实际的度量方法．单向函数为构建对称密码体制奠定了基础，它有助于论证密码安全性时所做的假设，因此算法与问题的复杂性理论已成为现代密码系统设计与分析的重要基础[4]．

参考文献：

[1] BRUCE SCHNEIER. 应用密码学：协议、算法与 C 源程序 [M]. 吴世忠，祝世雄，张文政，等译. 北京：机械工业出版社，2000：164-167.

[2] CHARLES P. Pfleeger & Shari Lawrence Pfleeger, Security in Computing [M]. 3rd Edition. China Machine Press, 2003：644-645.

[3] MICHAEL SIPSER. 计算理论导引 [M]. 张立昂，王捍贫，黄 雄，译. 北京：机械工业出版社，2000：247-248.

[4] 朱文余，孙 琦. 计算机密码应用基础 [M]. 北京：科学出版社，2000：95-98.

One-way Function and Symmetrical Cryptosystem

TONG Ya-la

(*School of Science, Hubei University of Technology, Wuhan* 430068, *China*)

Abstract: Reliable cryptograph is set up in math and formal computer science. According to the computational theory, the paper expounds mathematical background for public-key cryptosystem including: the complexity of algorithm and problem, relationship between the length of key and security of cryptogram. And also in the concept of length holding and permutation, one-side permutation and one-way Function, which are the theoretical base of constructing symmetrical cryptosystem are introduced. Finally as an applying example, password system in computer shows how to construct symmetrical cryptosystem.

Key words: Algorithm; Computational Theory; Complexity; Secret Key; One-side Permutation; One-way Function; Symmetrical Cryptosystem

（责任编校 杨玉东）