转变中的密码学

Cryptology in Transition

ABRAHAM LEMPEL,

Department of Electrwal Engmeertng, Technton–Israel Instttute of Technology, Hatfa, Israel 翻译：李晓峰 (cy_lxf@

V1.0

2023 年 10 月 26 日

摘要

本综述的重点是最近提出的实现方案，以及与密码复杂性有关的公钥密码系统问题的新概念。此外，还简要概述了经典密码学，当今密码学的基本原则，以及现在官方的 DES 加密标准。

前言

这项工作旨在向读者传达公钥密码学目前所处的过渡阶段和不断发展的技术状态。这种过渡是多方面的: 在相关范围内，它已经从处理军事和外交通信的政府垄断演变为一般商业的主要关注，特别是银行业，以及最近的广大公众。它的技术已经从纸笔和各种机械设备扩展到大型、高速的电子计算机。它的安全重点也从统计的不确定性转变为计算的复杂性。最后，但并非最不重要的是，在概念上它已经从传统的 pri- vat -key 方案发展到公钥密码系统——提供即时隐私和双向认证的术语。

*译者目前为北京联合大学智慧城市学院信息安全老师。

†译文来自于经典文献翻译项目 https://gitee.com/uisu/InfSecClaT, 欢迎大家加入经典翻译项目，为更多的人能够获取这些经典文献所传递信息做一点贡献。

这个例子是由作者 Shimon Even 和 Yacov Yacobi 共同推导出来的。它演示了一个密码，即使在选择的明文攻击下，破解其密钥的问题也是 NP-完

全的。然而，给定足够的已知明文，以接近 1 的概率，可以将破解密钥规约为在 n 个未知数中求解 n 个独立线性方程的简单问题，其中 n 是密钥位的数量。

该方案是一种传统的私钥分组密码，其总体结构如图 1 所示。密钥长度为 n 位，$K = (x_l x_2 \dots x_n)$ ，消息是长度为 m 的二进制块，其中 $m = [log_2(1 + \sum_{j=1}^{n} a_j)]$，$A = (a_l a_2 \dots a_n)$ 是一个任意的具有正整数分量 a_j 的背包，假设密码分析者知道。要获得消息 M 的密文 C，请按照以下步骤进行:

- 在本地生成一个特别随机 (ad hoc random) 二进制向量 R;
- 计算 $s = A(K \oplus R)^T$;
- 集合 $C = (M \oplus S, R)$, 此处 $S = binary(s)$

注意密文长度是 $m+n$，$M \oplus S$ 的 m 位后面跟着 R 的 n 位，并且对于每个 m 生成一个新的 R。解密也很简单: 因为合法的接收者知道 K，他可以把 K 加到接收到的 R 中，计算出 s，从中他可以得到 S，从而得到 M。

从密码分析者的角度来看，最糟糕的情况是，对于他所有已知的明文，特设向量 (ad hoc vector) R 保持不变。然后，在已知和选择明文攻击下，破解密钥需要解决方程 $s = A(K \oplus R)^T$, 给定 s, A 和 R 求 K。当然，这相当于解决 NP-完全的背包问题。

一个可能性更大的事件是，给定足够多的已知明文，密码分析师将有 n 对 (M_i, C_i) ，其中 $C_i = (M_i \oplus S_i, R_i)$ ，$i = 1, 2 \dots n$，使得 n 个向量 $U_i = 1^n - 2R_i$ 在实数上是线性无关的 (1^n 是 n 个 1 的向量)。对于每一个 $i = 1, 2, \dots, M$，我们有

$$K \oplus R_i = K + R_i - 2(K * R_i)$$

其中 * 表示分量乘法 (componentwise multiplication)。因此：

$$K \oplus R_i = R_i + K * U_i$$

并且

$$\begin{aligned} s_i &= A(K \oplus R_i)^T \\ &= A(R_i + K * U_i)^T \\ &= AR_i^T + A(K * U_i)^T \\ &= AR_i^T + (U_i * A)K^T \end{aligned}$$

令 $t_i = s_i - AR_i^T$, 将 n 个方程写成矩阵形式，我们得到

$$\begin{bmatrix} t_1 \\ t_2 \\ \dots \\ t_n \end{bmatrix} = \begin{bmatrix} U_1 \\ U_2 \\ \dots \\ U_n \end{bmatrix} \begin{bmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{bmatrix}$$

由于 U_i 是独立的，并且对于所有 j 都有 $a_j > 0$，可以很容易地解出密钥分量 x_i。可以证明 (见 LEMP78，附录 1)$N \geq n$ 对 (M, C) 产生 n 个线性无关的 U, 对于 $N = n$ 的概率下界约为 1/3; 当 $N = n+1$ 时，下界加倍，随着 $N - n$ 的增加，下界迅速趋近于 1。

这个例子并不是要以任何方式减损作为加密方案基础的难题的潜在有用性。我们的目的只是提醒读者，NP-完备的复杂性度量，以及在 NPC 类中困难问题的公认难度并未解决，就加密复杂性而言可能超出了上面复杂度的上下文。通过将 Merkle-Hellman 方案与我们的示例进行比较，进一步强调了所涉及的复杂性。这两种方案都是基于背包问题，虽然还不清楚破解 MH 方案是否是 NPC，但我们的例子中的方案肯定是这样的。然而，破解后者非常简单，而破解 MH 方案的可行方法尚未找到。

还应该指出，示例方案的大部分 (如果不是全部) 弱点是由于 C 对 M 的线性依赖。长期以来，密码中的线性一直被认为是密码学家的诅咒和密码分析者的福音。我们在第 3 节的末尾讨论了这个问题，就是具有某种线性的方案中的隐私和身份验证之间的权衡时。

很容易修改我们示例的方案，使其密码分析像任何已知的一样困难。例如，可以用 $M^s \pmod{pq}$ 代替 $M \oplus S$ ，就像在 RSA 方案中一样，或者用 DES(M, S) 代替 $M \oplus S$，也就是说，通过将 DES 方案应用于 M, 而 S 作为 DES 密钥。我们不提这一点，是为了提出另一个方案，其难解性是一个猜想问题。如前所述，我们认为需要的是努力建立一些在密码复杂性背景下真正有效的标准，然后才尝试发明符合这些标准的方案。正如 RABI77 中所指出的那样，我们离实现这一目标还很遥远。

致谢

作者很高兴地感谢我在准备这项调查时得到的帮助。特别感谢 Martin Cohn 在内容和风格上提供的宝贵帮助，感谢 Martin Hellraan 帮助修

改 Sperry 的原始报告，并感谢 Ron Graham 和 Adl Shamir 允许描述他们的未发表的方案。作者也感谢与 Len Adleman,Shimon Even,Leland Gardner,Martin Hellman, Ralph Merkle, Nick Plppenger, Michael Rabin, Ron Rivest, Adi Shamir, Ned Sloane, Shmuel Wmograd, and Yacob Yacobi 的有益讨论

参考文献