密码学·一般概念（下）

——中国密码学会 组编

密钥撤销（Key revocation）：密钥在生存期内被撤销而失效。

密钥编排（Key schedule）：分组密码中由工作密钥扩展生成轮密钥的过程。

密钥空间（Key space）：所有可能的密钥组成的集合。

密钥传送（Key transport）：实体间传送受保护的密钥的过程。

密钥更新（Key update）：用一个新的密钥来替代旧密钥的过程。

背包问题（Knapsack problem）：给定一个正整数集合$\{a_1，a_2，...，a_n\}$和一个正整数 s，确定是否存在该集合的一个子集，使其元素的总和等于 s。

已知明文攻击(Know-plaintext attack) 密码攻击的一种类型，密码攻击者拥有相当数量的明密文对。

大整数因子分解问题（Large integer factorization problem）将一个大合数分解为素数因子乘积的问题。

线性复杂度（linear complexity）生成一个给定序列的最短现行反馈移位寄存器的级数。

主密钥（Master key）处于对称密码系统层次化密钥结构中的最高层，对其他密钥进行加密的密钥。

抗抵赖（Non-repudiation）也称不可否认。证明一个操作或事件已经发生且无法否认的机制。

单向函数（One-way function）给定输出易于计算输出，但是给定输出要找到其对应的输入是计算不可行的函数。

单向陷门函数（One-way trapdoor function）带一个秘密陷门的单向函数，知道陷门很容易求该函数的逆，否则求逆是困难的。

口令（Password）用于访问验证的字符串。

完善保密性（Perfect secrecy）从信息论的角度由密文得不到明文的任何信息。

明文（Plain text/clear text）待加密的数据。

明文空间（Plaintext space）所有可能的明文组成的集合。

私钥（Private key）非对称加密算法中只能由拥有者使用的密钥。

可证明安全（Provable security）密码算法或协议的安全性的一种评价方法，指破译一种密码算法或协议的难度可归结为一个公认的困难问题的求解。

公钥（Public key）非对称密码算法中可以公开的密钥。

量子密码（Quantum cryptography）基于量子测不准原理和量子计算技术等的密码理论。

随机数（Random number）不可预测的时变参数。

会话密钥（Session key）处于层次化密钥结构中的最底层，仅在一次会话中使用的密钥。

严格雪崩准则（Strict Avalanche Criterion, SAC）密码变换的一种设计准则，任一输入比特改变时，每一输出比特改变的概率都为 0.5。

零知识证明（Zero-knowledge proof）一种协议，协议的一方（称为证明者）在不向另一方（称为验证者）提供任何有用的信息的条件下，向验证者证明某个论断是正确的。