哪些密码算法支撑着你手机的安全?

彭 真

1、3GPP 标准空口的安全机制

3GPP 标准中，手机与基站之间通过无线信号传递信息，传输信息的安全依赖于空中接口（简称空口）的安全。空口信息包括数据信息和信令信息，空口的安全性保护分为空口的机密性保护和完整性保护。空口信息加密 UEA 和信令签名 UIA 允许采用不同的密码算法，以满足不同运营商或者国家对安全算法的选择。目前标准化的密码算法有 KASUMI 算法、SNOW 3G 算法、AES 算法和 ZUC 算法，这些算法不仅支撑了手机终端的安全性，也支撑了其它移动终端的安全性。

1.1 空口的机密性保护

空口机密性保护用于保护空口信息（包括数据和信令）的机密性，使数据以密文形式传输，即使截获也不能泄露任何明文信息。发送端以 128 比特加密密钥 KEY、32 比特 COUNT（计数器值）、5 比特 BEARER（承载标识）、1 比特 DIRECTION（上下行方向指示，0 表示上行，1 表示下行）和 LENGTH（明文长度）作为加密算法输入参数，计算出密钥流，与明文进行异或，产生密文后发送。接收端接收到密文后，利用与发送端相同的参数 KEY、COUNT、BEARER、DIRECTION、LENGTH 以及和发送端相同的加密算法，将产生的密钥流与收到的密文进行异或操作恢复出明文。

在 3G 系统中，3GPP 定义了基于 KASUMI 的机密性算法 f8。在 LTE 系统中，除一种无效的加密算法（EEA0）用于无 SIM 状态下紧急呼叫外，LTE 系统共定义了三种 128-EEA 加密算法，用于用户信息的机密性保护，分别为：

（1）128-EEA1（UEA2）：基于 SNOW 3G 算法，密钥长度为 128 比特，初始向量（IV）为 128 比特；

（2）128-EEA2：基于 CTR 模式的 AES 算法（AES-CTR），密钥长度为 128 比特；

（3）128-EEA3：基于 ZUC 算法，密钥长度为 128 比特，初始向量（IV）为 128 比特。

1.2 空口的完整性保护

空口完整性保护用于保护空口信息（信令数据）的完整性，使信令数据在传输过程中即使更改也能被发现，避免出现伪造信令而带来危害。发送端利用完整性保护密钥 KEY、COUNT、BEARER、DIRECTION 和消息本身作为完整性保护算法的输入，生成一个 32 比特的完整性认证码，附在消息后面。发送端将消息本身和认证码一起发送给接收

端；接收端利用和发送端相同的 KEY，以及接收到的消息本身和 COUNT、BEARER、DIRECTION 作为完整性保护算法的输入计算出一个 32 比特的完整性认证码，与收到的认证码进行比较。如果一致，则认为收到的消息和发送的消息是一致的，即没有被篡改；如果不一致，则舍弃该信令。

在 3G 系统中，3GPP 定义了基于 KASUMI 的完整性保护算法 f9。在 LTE 系统中，除一种无效的完整性保护算法（EIA0），LTE 系统定义了三种 128-EIA 加密算法，具体为：

（1）128-EIA1（UIA2）：基于 SNOW 3G 的完整性保护算法，密钥长度为 128 比特；

（2）128-EIA2：基于 CMAC 模式的 AES 算法（AES-CMAC），密钥长度为 128 比特；

（3）128-EIA3：基于 ZUC 的完整性保护算法，密钥长度为 128 比特。

2、3GPP 标准中的密码算法

2.1 KASUMI 算法

KASUMI 算法是 WCDMA 中的标准算法，是一个 8 轮 Feistel 结构分组密码算法。密钥长度为 128 比特，分组长度为 64 比特。基于 KASUMI 算法的 f8 和 f9 算法分别用于无线链路空中接口的机密性和完整性保护。

f8 算法用于无线链路的机密性保护。f8 是一个流密码算法，使用机密性密钥 CK 加密 / 解密数据分组，数据分组介于 1~5114 比特。f8 算法以 KASUMI 算法为基础，使用 KASUMI 算法的输出反馈（OFB）模式作为密钥流生成器，产生的加 / 解密密钥与明文数据进行异或操作生成密文。

f9 算法用于无线链路的完整性保护。f9 使用完整性密钥 IK 计算给定的输入消息，产生一个 32 比特的 MAC，消息长度介于 1~5114 比特。f9 算法以 KASUMI 算法为基础，使用 KASUMI 算法的密码分组链接（CBC-MAC）模式生成 64 比特的消息摘要，摘要的最左边 32 比特作为 MAC-A 的输出。

2.2 SNOW 3G 算法

SNOW 3G 是一种面向字的流密码算法，输入为 128 比特的密钥 KEY 和 128 比特的初始向量 IV，内部状态为 608 比特。LTE 系统中，算法 1 称为 128-EEA1（UEA2）和 128-EIA1（UIA2）算法，统一使用 SNOW 3G 作为核心。

UEA2 算法用于无线链路的机密性保护。UEA2 算法是一个流密码算法，加密 / 解密分组数据，数据长度介于 1~20000 比特。UEA2 使用 128 比特的密钥，生成一组与数据无关的密钥流，与数据明文按位异或，得到数据密文。

UIA2 算法用于无线链路的完整性保护。UIA2 算法将 128 比特的密钥和各输入参数作为 SNOW 3G 算法的输入，生成 5 个 32 比特的密钥流。使用这些密钥流，计算出数据的消息鉴权码 MAC-1，长度为 32 比特，数据长度介于 1~20000 比特。UIA2 算法基于泛杂凑函数和 GMAC 模式。

2.3 AES 算法

AES 是一个典型的分组密码算法，分组长度为 128 比特，密钥长度为 128、192、256 比特，迭代轮数分别为 10、12、14 轮。在 LTE 系统中，算法 2 称为 128-EEA2 和 128-EIA2 算法，统一使用 AES 算法作为核心算法。目前在 LTE 中只使用 128 比特长的密钥，即 AES-128 算法。

128-EEA2 算法用于无线链路的机密性保护。128-EEA2 使用 CTR 模式的 AES 算法，密钥长度为 128 比特。AES-CTR（Counter，计数器）模式是以 AES 算法为基本单元，以 CTR 模式对数据进行加密。解密时使用和加密相同的计数器，将计数器产生的密钥流和密文做异或运算可得明文。

128-EIA2 算法用于无线链路的完整性保护。128-EIA2 基于 CMAC(Cipher-based Message Authentication Code) 模式的 128 位 AES 算法实现，即 AES-CMAC 算法。AES-CMAC 算法以一串密钥和可变长度的消息体 M 和消息长度作为输入，以 MAC 作为输出。

2.4 ZUC 算法

ZUC 是一个面向字的流密码算法，一个 128 比特的初始密钥 KEY 和一个 128 比特的初始向量（IV）作为输入，输入一串 32 位字的密钥字序列。祖冲之算法集（ZUC）是由我国学者自主设计的加密和完整性算法，包括祖冲之算法、加密算法 128-EEA3 和完整性算法 128-EIA3，是我国的算法技术第一次成为国际标准，也是我国商用密码和移动通信领域的重大突破。在 LTE 系统中，算法 3 称为 128-EEA3 和 128-EIA3 算法，统一使用 ZUC 算法作为核心算法。

128-EEA3 算法用于无线链路的机密性保护。128-EEA3 是一个流密码算法，使用机密性密钥 CK 加密 / 解密分组数据，数据分组长度介于 1~65504 比特。128-EEA3 算法使用 ZUC 算法作为密钥流生成器，通过将明文直接与 ZUC 产生的流密码进行异或实现加密。

128-UIA3 算法用于无线链路的完整性保护。128-EIA3 算法使用完整性密钥 IK 计算给定的输入消息，输出一个 32 比特的 MAC，消息长度介于 1~65504 比特。128-EIA3 算法使用泛杂凑函数和 ZUC 算法，根据明文每比特的值进行判定，将 ZUC 产生的密钥流做迭代运算产生 MAC 值。

3 结论

本文介绍了当前 3GPP 标准中的四个密码算法：KASUMI、SNOW 3G、AES 和 ZUC 算法，以及分别以这些算法为核心的空口机密性和完整性保护算法，深入学习和理解密码算法的原理和应用对于移动通信安全具有重要意义。