Risc-v 开发

基于飞利信 MCU 的安全应用开发

北京飞利信科技股份有限公司

2018 年 5 月

国密算法体系介绍

1 简介

国密算法体系包括对称算法、非对称算法、杂凑算法。

1.1 对称密码

对称密码主要是分组密码和流密码及其应用。分组密码中将明文消息进行分块加密输出密文区块，而流密码中使用密钥生成密钥流对明文消息进行加密。世界上应用较为广泛的包括 DES、3DES、AES，此外还有 Serpent，Twofish，MARS 和 RC6 等算法。对称加密的工作模式包括电码本模式(ECB 模式)，密码反馈模式(CFB 模式)，密码分组链接模式(CBC 模式)，输入反馈模式(OFB 模式)等。

1.2 非对称密码

公钥密码体制由 Diffie 和 Hellman 所提出。1978 年 Rivest，Shamir 和 Adleman 提出 RAS 密码体制，基于大素数分解问题。基于有限域上的离散对数问题产生了 ElGamal 密码体制，而基于椭圆曲线上的离散对数问题产生了椭圆曲线密码密码体制。此外出现了其他公钥密码体制，这些密码体制同样基于困难问题。目前应用较多的包括 RSA、DSA、DH、ECC 等。

1.3 杂凑算法

杂凑算法又称 hash 函数，就是把任意长的输入消息串变化成固定长的输出串的一种函数。这个输出串称为该消息的杂凑值。一个安全的杂凑函数应该至少满足以下几个条件。

1）输入长度是任意的；

2）输出长度是固定的，根据目前的计算技术应至少取 128bits 长，以便抵抗生日攻击；

3）对每一个给定的输入，计算输出即杂凑值是很容易的；

给定杂凑函数的描述，找到两个不同的输入消息杂凑到同一个值是计算上不可行的，或给定杂凑函数的描述和一个随机选择的消息，找到另一个与该消息不同的消息使得它们杂凑到同一个值是计算上不可行的。

杂凑函数主要用于完整性校验和提高数字签名的有效性，目前已有很多方案。这些算法都是伪随机函数，任何杂凑值都是等可能的。输出并不以可辨别的方式依赖于输入；在任何输入串中单个比特的变化，将会导致输出比特串中大约一半的比特发生变化。

2 国密算法

为了保障密码安全，国家密码管理办公室制定了一系列密码标准，包括SSF33、SM1（SCB2）、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法等等。其中SSF33、SM1、SM4、SM7、祖冲之密码是对称算法；SM2、SM9是非对称算法；SM3是哈希算法。目前已经公布算法文本的包括祖冲之序列密码算法、SM2椭圆曲线公钥密码算法、SM3密码杂凑算法、SM4分组密码算法等。

2.1 SM1 对称密码

SM1 算法是分组密码算法，分组长度为128位，密钥长度都为 128 比特，算法安全保密强度及相关软硬件实现性能与 AES 相当，算法不公开，仅以 IP 核的形式存在于芯片中。

采用该算法已经研制了系列芯片、智能 IC 卡、智能密码钥匙、加密卡、加密机等安全产品,广泛应用于电子政务、电子商务及国民经济的各个应用领域(包括国家政务通、警务通等重要领域)。

2.2 SM2 椭圆曲线公钥密码算法

SM2 算法就是ECC椭圆曲线密码机制，但在签名、密钥交换方面不同于ECDSA、ECDH等国际标准，而是采取了更为安全的机制。另外，SM2推荐了一条256位的曲线作为标准曲线。

ECC椭圆曲线密码体制Koblitz和Miller在1985年各自引入密码学。椭圆曲线的Weierstrass方程为 $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$，其上面的所有点和无穷远点构成一个加法交换群，其中无穷远点是加法零元。此群的加法法则可以由弦切法所给出，具体见下图。

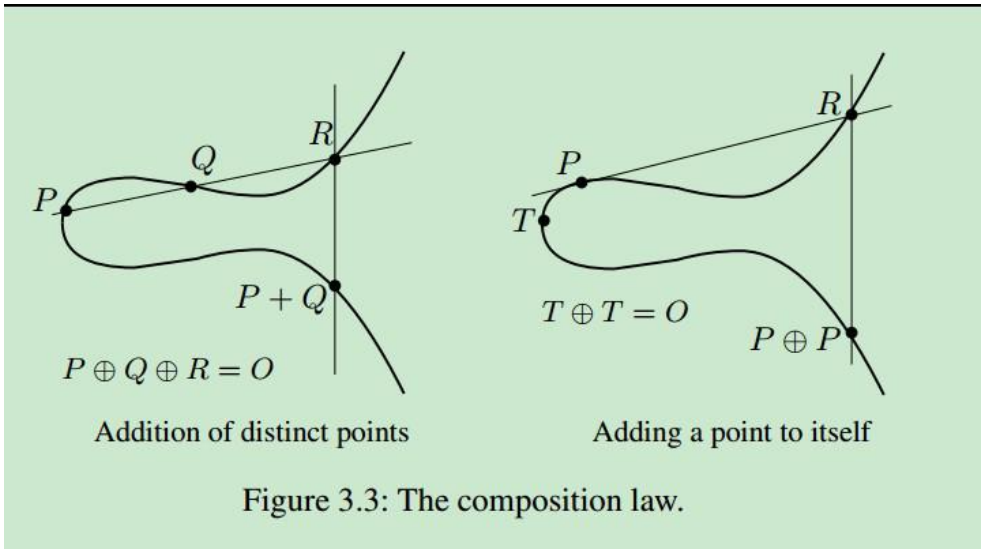


Figure 3.3: The composition law.

左图中是两个不同点 P 和 Q 的加法，右图为相同的点 P 和 P 的加法。由弦切法便可以给出椭圆曲线上的加法方程。多倍点运算是指：给定一点 P 和一个整数 k，计算 kP，即 k 个 P 点的和。椭圆曲线上的离散对数问题为：给定点 P 和 kP，计算整数 k。椭圆曲线密码体制的安全性便是建立在椭圆曲线离散对数问题之上。

SM2 标准包括总则，数字签名算法，密钥交换协议，公钥加密算法四个部分，并在每个部分的附录详细说明了实现的相关细节及示例。

SM2 算法主要考虑素域 F_p 和 F_{2^m} 上的椭圆曲线，分别介绍了这两类域的表示，运算，以及域上的椭圆曲线的点的表示，运算和多倍点计算算法。然后介绍了编程语言中的数据转换，包括整数和字节串，字节串和比特串，域元素和比特串，域元素和整数，点和字节串之间的数据转换规则。详细说明了有限域上椭圆曲线的参数生成以及验证，椭圆曲线的参数包括有限域的选取，椭圆曲线方程参数，椭圆曲线群基点的选取等，并给出了选取的标准以便于验证。最后给出椭圆曲线上密钥对的生成以及公钥的验证，用户的密钥对为（s，sP），其中 s 为用户的私钥，sP 为用户的公钥，由于离散对数问题从 sP 难以得到 s，并针对素域和二元扩域给出了密钥对生成细节和验证方式。总则中的知识也适用于 SM9 算法。

在总则的基础上给出了数字签名算法（包括数字签名生成算法和验证算法），密钥交换协议以及公钥加密算法（包括加密算法和解密算法），并在每个部分给出了算法描述，算法流程和相关示例。

数字签名算法适用于商用应用中的数字签名和验证，可满足多种密码应用中的身份认证和数据完整性，真实性的安全需求。**密钥交换协议**适用于商用密码应用中的密钥交换，可满足通信双方经过两次或可选三次信息传递过程，计算获取一个由双方共同决定的共享秘密密钥（会话秘钥）。**公钥加密算法**适用于国家商用密码应用中的消息加解密，消息发送者可以利用接收者的公钥对消息进行加密，接收者用对应的私钥进行解，获取消息。

数字签名算法，密钥交换协议以及公钥加密算法都使用了国家密管理局批准的 SM3 密码杂凑算法和随机数发生器。数字签名算法，密钥交换协议以及公钥加密算法根据总则来选取有限域和椭圆曲线，并生成密钥对，具体算法，流程和示例见 SM2 标准。

SM2 算法和 RSA、对称算法等强度对比如下。

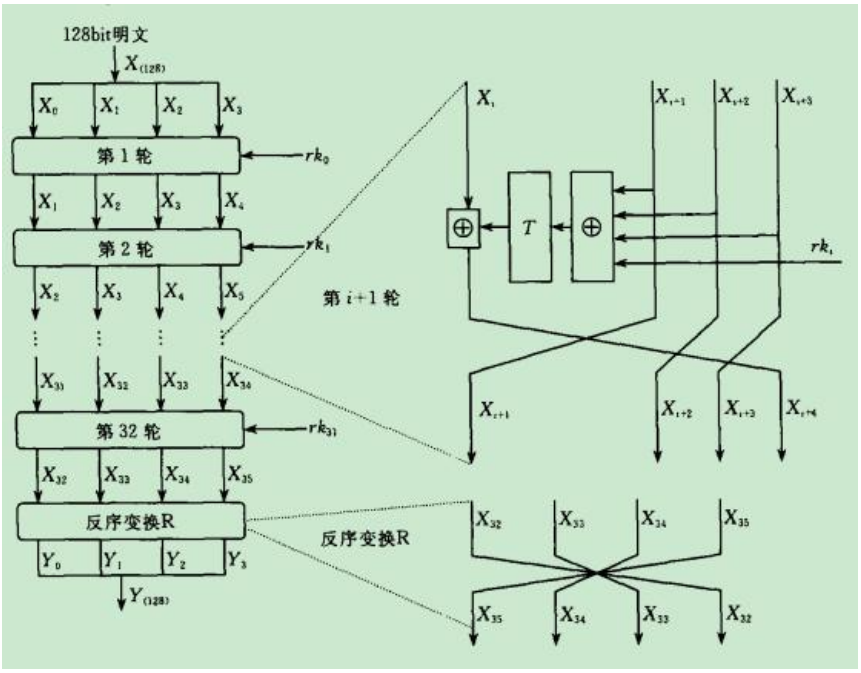
保密级别	对称密钥长度	RSA 密钥长度	ECC 密钥长度	保密年限
80	80	1024	160	2010
112	112	2048	224	2030
128	128	3072	256	2040
192	192	7680	384	2080
256	256	15360	512	2120

2.3 SM3 杂凑算法

SM3 密码杂凑算法给出了杂凑函数算法的计算方法和计算步骤，并给出了运算示例。此算法适用于商用密码应用中的数字签名和验证，消息认证码的生成与验证以及随机数的生成，可满足多种密码应用的安全需求。在 SM2，SM9 标准中使用。此算法对输入长度小于 2 的 64 次方的比特消息，经过填充和迭代压缩，生成长度为 256 比特的杂凑值，其中使用了异或，模，模加，移位，与，或，非运算，由填充，迭代过程，消息扩展和压缩函数所构成。具体算法及运算示例见 SM3 标准。

2.4 SM4 对称算法

此算法是一个分组算法，用于无线局域网产品。该算法的分组长度为 128 比特，密钥长度为 128 比特。加密算法与密钥扩展算法都采用 32 轮非线性迭代结构。解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。此算法采用非线性迭代结构，每次迭代由一个轮函数给出，其中轮函数由一个非线性变换和线性变换复合而成，非线性变换由 S 盒所给出。具体流程图如下：



其中 rk_i 为轮密钥，合成置换 T 组成轮函数。轮密钥的产生与上图流程类似，由加密密钥作为输入生成，轮函数中的线性变换不同，还有些参数的区别。SM4 算法的具体描述和示例见 SM4 标准。

2.5 SM7 对称密码

SM7 算法，是一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。SM7 的算法文本目前没有公开发布。SM7 适用于非接 IC 卡应用包括身份识别类应用(门禁卡、工作证、参赛证)，票务类应用(大型赛事门票、展会门票)，支付与通卡类应用（积分消费卡、校园一卡通、企业一卡通、公交一卡通)。

2.6 SM9 非对称算法

SM9 是基于对的标识密码算法，与 SM2 类似，包含四个部分：总则，数字签名算法，密钥交换协议以及密钥封装机制和公钥加密算法。在这些算法中使用了椭圆曲线上的对这一个工具，不同于传统意义上的 SM2 算法，可以实现基于身份的密码体制，也就是公钥与用户的身份信息即标识相关，从而比传统意义上的公钥密码体制有许多优点，省去了证书管理等。

密码中双线性对 $e:G_1\times G_2\to G_T$ 满足如下条件：

双线性性：对任意的 $P\in G_1$，$Q\in G_2$，以及 $a,b\in Z_N$，有 $e(aP,bQ)=e(P,Q)^{ab}$；

非退化性：$e(P,Q)\neq 1$，其中 P 为 G_1 的生成元，Q 为 G_2 的生成元；

可计算性：存在有效的算法计算 $e(P,Q)$。

其中G_1，G_2为椭圆曲线上的加法群，而G_T为有限域的乘法群。在椭圆曲线对中，根据G_1与G_2是否关系，以及椭圆曲线上的自同态，可以将对分成三种类型，需要考虑在超奇异椭圆曲线，常椭圆曲线上来选取对。常用的对有 Weil 对，Tate 对，Ate 对，以及最优对等。基于对的标识密码算法建立在一些对的难解问题，例如双线性 Diffie-Hellman 问题，双线性逆 DH 问题等。椭圆曲线上的双线性对为$e: E(F_{q^k})[r] \times E(F_{q^k}) / rE(F_{q^k}) \to F_{q^k}^{*}$

其中 k 为$E(F_q)$的嵌入次数。双线性对的双线性的性质是基于对的标识密码算法的基础。

SM2 中的总则部分同样适用于 SM9，由于 SM9 总则中添加了适用于对的相关理论和实现基础。椭圆曲线双线性对定义和计算在扩域上进行，总则中给出了扩域的表示和运算，考虑F_{p^m}和F_{3^m}上的椭圆曲线。数据类型转换同样包括整数与字节串，比特串和字节串，字节串和域元素，点和字节串之间的转换，其中字节串和域元素之间的数据类型转换涉及到扩域。系统参数的生成比 SM2 复杂，涉及到对的相关参数，验证也相应地复杂。并在附录 B 里面详细地描述了计算对的算法 Miller 算法，并给出了 Tate 对，Ate 的计算，以及适合对的椭圆曲线的生成。

基于总则中的椭圆曲线以及对的基本选取，给出系统参数组，系统主密钥和用户密钥的产生。用户密钥由系统的主密钥和用户标识共同产生。SM9 给出了数字签名算法（包括数字签名生成算法，数字签名验证算法），密钥交换协议，以及密钥封装机制和公钥加密算法（包括密钥封装算法，加密盒解密算法）。数字签名算法适用于接收者通过签名者的标识验证数据的完整性和数据发送者的身份，也适用于第三方确定签名及所签数据的真实性。密钥交换协议可以使用通信双方通过双方的标识和自身的私钥经过两次或者可选三次信息传递过程，计算获取一个由双方共同决定的共享秘密密钥。密钥封装机制和公钥加密算法中，利用密钥封装机制可以封装密钥给特定的实体。公钥加密和解密算法即基于标识的非对称秘密算法，该算法使消息发送者可以利用接收者的标识对消息进行加密，唯有接收者可以用相应的私钥对该密文进行解密，从而获取消息。基于对的算法中同样使用了国家密管理局批准的 SM3 密码杂凑算法和随机数发生器，密钥封装机制和公钥加密算法中使用了国家密码管理局批准的对称密码算法和消息认证码函数。基于对的数字签名算法，密钥交换协议以及密钥封装机制和公钥加密算法的具体算法，流程图和示例见 SM9 标准。

2.7 祖冲之对称算法

祖冲之密码算法由中国科学院等单位研制，运用于下一代移动通信 4G 网络 LTE 中的国际标准密码算法。祖冲之密码算法（ZUC）的名字源于我国古代数学家祖冲之，祖冲之算法集是由我国学者自主设计的加密和完整性算法，是一种流密码。它是两个新的 LTE 算法的核心，这两个 LTE 算法分别是加密算法 128-EEA3 和完整性算法 128-EIA3。ZUC 算法由 3 个基本部分组成，依次为:1、比特重组；2、非线性函数 F；3、线性反馈移位寄存器(LFSR)。