现代密码学

SM2数字签名算法

信息与软件工程学院

SM2公钥密码算法

- SM2是中国国家密码管理局颁布的中国商用公钥密码标准算法，它是一组椭圆曲线密码算法，其中包含加解密算法、数字签名算法。
- 2004年，由中国科学院软件研究所张振峰研究员主持研制完成
- 2010年12月，首次公开发布
- 2012年3月，成为中国商用密码标准（GM/T 0003-2012）
- 2016年8月，成为中国国家密码标准（GB/T 32918-2016）
- 2017年11月3日，在第55次ISO/IEC联合技术委员会信息安全技术分委员会(SC27)德国柏林会议上,含有我国SM2与SM9数字签名算法的ISO/IEC14888-3/AMD1《带附录的数字签名第3部分:基于离散对数的机制-补篇1》获得一致通过,成为ISO/IEC国际标准,进入标准发布阶段。

符号

- **A,B**：使用公钥密码系统的两个用户。
- ***a,b***：F_q中的元素，它们定义F_q上的一条椭圆曲线E。
- d_B：用户B的私钥。
- $E(F_q)$：Fq上椭圆曲线E 的所有有理点(包括无穷远点O)组成的集合。
- F_q：包含q个元素的有限域。
- G：椭圆曲线的一个基点，其阶为素数。
- ***Hash*( )**：密码杂凑函数。
- H_v( )：消息摘要长度为v比特的密码杂凑函数。
- ***KDF*( )**：密钥派生函数。
- M：待加密的消息。
- M'：解密得到的消息。
- n：基点G的阶(n是$\#E(Fq)$的素因子)。
- O：椭圆曲线上的一个特殊点，称为无穷远点或零点，是椭圆曲线加法群的单位元。
- P_B：用户B的公钥。
- q：有限域Fq中元素的数目。
- **x||y**：x与y的拼接，其中x、y可以是比特串或字节串。

$[k]P$：椭圆曲线上点P的k倍点，即，$[k]P=\underbrace{P+P+\cdots+P}_{k个}$，$k$是正整数。

$[x,y]$：大于或等于x且小于或等于y的整数的集合。

$\lceil x \rceil$：顶函数，大于或等于x的最小整数。例如$\lceil 7 \rceil=7$, $\lceil 8.3 \rceil=9$。

$\lfloor x \rfloor$：底函数，小于或等于x的最大整数。例如$\lfloor 7 \rfloor=7$, $\lfloor 8.3 \rfloor=8$。

$\#E(F_q)$：$E(F_q)$上点的数目，称为椭圆曲线$E(F_q)$的阶。

SM2的基本参数

基于素数域 F_p 的SM2算法参数如下：

- F_p 的特征p，为 m 比特长的素数 p ，要尽可能大，但太大会影响计算速度;通常选择160比特大小。
- 长度不小于192比特的比特串 $SEED$ ；
- F_p 上的2个元素 a,b，满足 $4a^3+27b^2\neq 0$ ，定义

$$E(F_p): y^2 = x^3 + ax + b(modp)$$

- 基点 $G=(x_G,y_G)\in E(F_p), G\neq O$ ；
- G 的阶 n 为 m 比特长的素数，满足 $n>2^{191}$ 且 $n>4\sqrt{p}$
- $h=\frac{|E(F_p)|}{n}$ 称为余因子，其中 $|E(F_p)|$ 是曲线 $E(F_p)$ 的点数。

种子和曲线的产生

$SEED$ 和 a,b 的产生算法如下：

（1）任意选取长度不小于192比特的比特串 ；

（2）计算 $H=H_{256}(SEED)$ ，记 $H=(h_{255},h_{254},\cdots,h_0)$ ，其中 H_{256} 表示256比特输出的SM3哈希算法；

（3）取 $R=\sum_{i=0}^{255}h_i 2^i$ ；

（4）取 $r=R \bmod p$ ；

（5）在 F_p 上任意选择2个元素 a,b ，满足 $rb^2=a^3 \bmod p$ ；

或者令 $\boldsymbol{b=r}$ ，取 F_p 中元素 $\boldsymbol{a}$ 为某固定值；

（6）若 $4a^3+27b^2=0 \bmod p$ ，则转向 （1）；

（7）所选择的 F_p 上曲线是 $E(F_p):y^2=x^3+ax+b(modp)$ ；

（8）输出 $(SEED,a,b)$ 。

密钥产生

设签名方为 A，A的秘密钥取为 $\{1,2,\cdots,n-1\}$的一个随机数 d_A，其中 n 是基点G的阶。

A 的公开钥取为椭圆曲线上的点：

$$P_A=d_AG$$

其中$G=G(x,y)$是基点。

预处理

- 设ID_A是A的长度为$entlen_A$比特的标识，$ENTL_A$是由$entlen_A$转换而成的两个字节
- A计算$Z_A = H_{256}(ENTL_A||ID_A||a||b||x_G||y_G||x_A||y_A)$
- 其中a，b是椭圆曲线方程的参数、x_G，y_G是基点G的坐标，x_A，y_A是P_A的坐标。这些值转换为比特串后，再用H_{256}作用得到256比特的输出。
- B验证签名时，也需计算Z_A。

签名算法

设待签名的消息为M，A做以下运算：

①取 $\bar{M}=Z_A\|M$ ；

②计算 $e=H_v(\bar{M})$，将 e 转换为整数，H_v 是输出为 v 比特长的哈希函数；

③用随机数发生器产生随机数

$$k \leftarrow_R \{1,2,\cdots,n-1\}$$

④计算椭圆曲线点 $C_1=kG=(x_1,y_1)$ ；

⑤计算 $r=(e+x_1) \bmod n$，若$r=0$或 $r+k=n$ 则返回③；

⑥计算 $s=((1+d_A)^{-1}\cdot(k-r\cdot d_A)) \bmod n$

若$s=0$则返回③；

⑦消息M的签名为 (r,s) 。

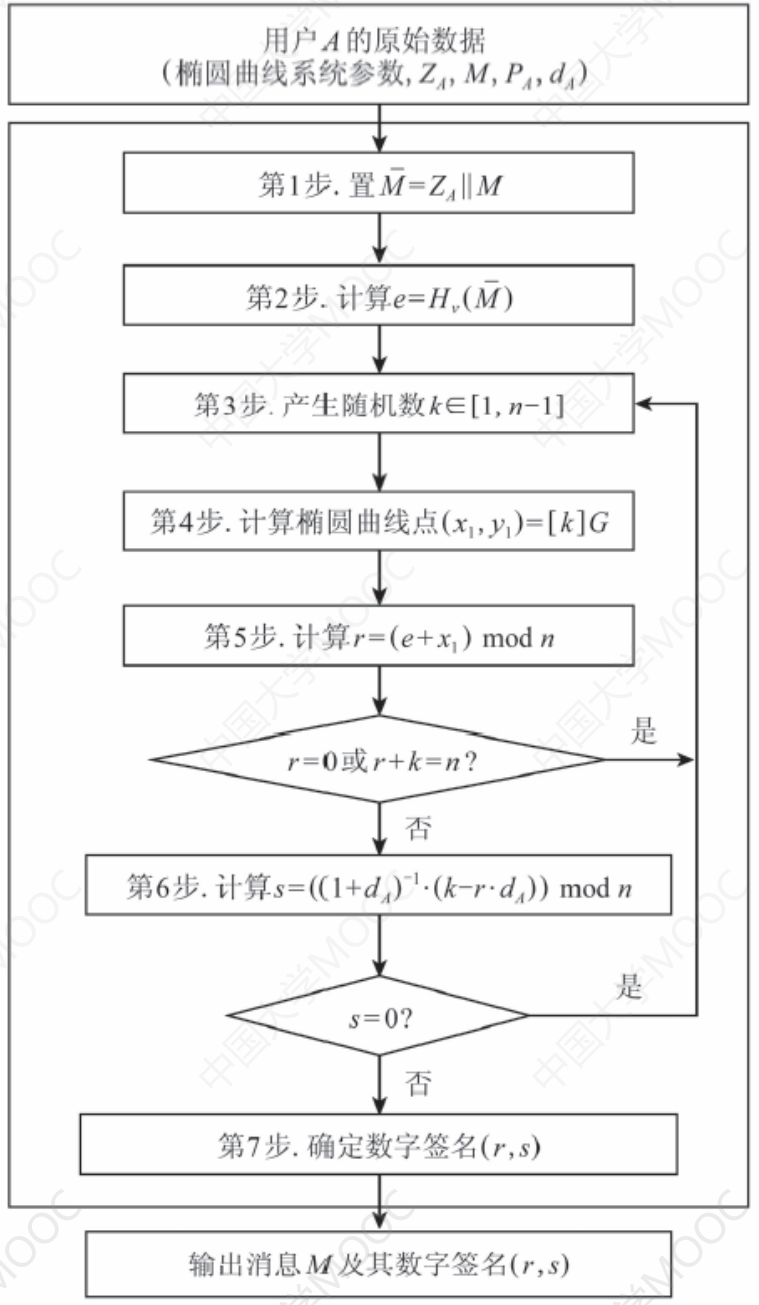

图 1　SM2 数字签名生成流程

验证算法

B收到消息M'及其签名(r',s')后，执行以下验证运算：

①检验$r'\in[1,n-1]$是否成立，若不成立则验证不通过；

②检验$s'\in[1,n-1]$是否成立，若不成立则验证不通过；

③置$\bar{M}'=Z_A\|M'$；

④计算$e'=H_v(\bar{M}')$，将e'转换为整数；

⑤计算$t=(r'+s')\bmod n$，若**$t=0$**；则验证不通过；

⑥计算椭圆曲线点$(x_1',y_1')=s'G+tP_A$；

⑦计算$R=(e'+x_1')\bmod n$，检验$R=r'$是否成立，若成立则验证通过；否则验证不通过。

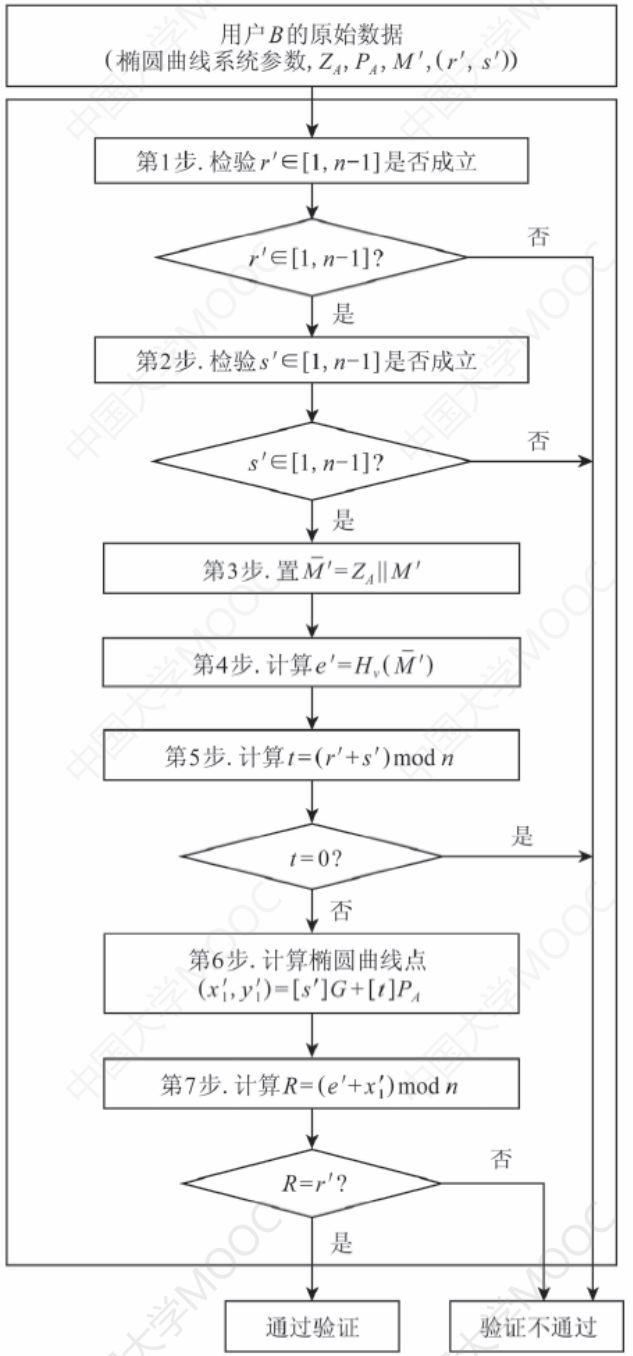

图 2　SM2 数字签名验证流程

正确性证明

- 正确性：如果 $\bar{M}'=\bar{M},(r',s')=(r,s)$，则 $e'=e$ ，要证 $R=r'=r$，只需证 $x_1'=x_1$，因此需证明 $C_1=s'G+tP_A$ 。 $C_1=kG=(x_1,y_1)$

$$
\begin{aligned}
s'G+tP_A &= s'G+(r'+s')P_A = s'G+(r'+s')d_AG \\
&= (s'+r'd_A+s'd_A)G = (s'(1+d_A)+r'd_A)G \\
&= (k-r'd_A+r'd_A)G = kG
\end{aligned}
$$

- 所以有 $x_1'=x_1$

感 谢 聆 听!

xynie@uestc.edu.cn