一、利用椭圆曲线密码实现数字签名

- 利用素域$GF(p)$上的椭圆曲线和$GF(2^m)$域上的椭圆曲线都可以构成椭圆曲密码线签名方案
- 这里只介绍素域$GF(p)$上的椭圆曲线密码签名方案
- 一个椭圆曲线密码由下面的六元组描述：
  - $T= <p,a,b,G,n,h>$
  - 其中，p为大于3的素数，p确定了有限域GF（p）；元素$a,b \in GF(p)$，a和b确定了椭圆曲线；G为循环子群E_1的生成元，n为素数且为生成元G的阶，G和n确定了循环子群E_1。h为余因子，$h=|E| / n$ 。
  - $y^2=x^3+ax+b \bmod p$

一、利用椭圆曲线密码实现数字签名

椭圆曲线密码数字签名

(1) 密钥选择

- $y^2=x^3+ax+b \bmod p$
  全体解点和无穷远点构成群，G为其循环子群E_1的生成元，n为素数且为G的阶。
- 用户的私钥：
  随机数$d \in \{1,2,\cdots,n-1\}$
- 用户的公开钥：
  Q点，$Q=dG$
  由Q求d，要求解椭圆曲线离散对数。

ELGamal密码数字签名

(1)密钥选择

- 选P是一个大素数，p-1有大素数因子，α是一个模p的本原元，将p和α公开作为密码基础参数。
- 用户的私钥：
  随机数x，$1< x < p-1$。
- 用户的公钥：
  $y = \alpha^x \bmod p$
  由y求x，要求解离散对数。

一、利用椭圆曲线密码实现数字签名

(2)产生签名（*SIG*）

设明文为m，$0\leqslant m\leqslant n-1$

① 选择一个随机数k，$k\in\{1,2,\cdots,n-1\}$；

② 计算点$R(x_R, y_R)=kG$，并记 $r=x_R$；

③ 利用私钥d 计算：

$s=(m-dr)k^{-1} \bmod n$ ；

④ 以<r,s>作为m的签名，并以<m，r，s>的形式发给接收方。

m	r	s

(2) 产生签名

设明文为m，$0\leqslant m\leqslant p-1$

① 随机地选择一个整数 k，$1<k<p-1$，且$(k，p-1)=1$；

② 计算$r=\alpha^k \bmod p$

③ 利用私钥x计算:

$s=(m-xr)k^{-1} \bmod p-1$

④ 取（r，s）作为m的签名，并以<m，r，s>的形式发给接收方。

m	r	s

一、利用椭圆曲线密码实现数字签名

(3) 验证签名（*VER*）

① 计算s^{-1} **mod** n；

② 利用公密钥 Q 计算：

$U(x_U, y_U) = s^{-1}(mG-rQ)$；

③ 如果$x_U = r$，则签名$<r,s>$为真，否则签名为假。

证明：因为$s=(m-dr)k^{-1}$ mod n，故，$s^{-1}=(m-dr)^{-1}k$ mod n，

$U(x_U, y_U) = (m-dr)^{-1}k(mG-rQ)$

$=(m-dr)^{-1}(mkG-krdG)$

$=(m-dr)^{-1}(mR-rdR)$

$=(m-dr)^{-1}R(m-dr)=R(x_R, y_R)$

所以 $x_U = x_R = r$.

(3) 验证签名

- 用户B用A的公钥y验证：

  $\alpha^m = y^r r^s \bmod p$，

  若成立则签名为真，否则签名为假。

- 可验证性证明如下：

  因为$s=(m-xr)k^{-1} \bmod p-1$，

  所以 $m=xr+ks \bmod p-1$，

  故 $\alpha^m = \alpha^{xr+ks} = (\alpha^x)^r(\alpha^k)^s = y^r r^s \bmod p$，故签名可验证。

一、利用椭圆曲线密码实现数字签名

(4) 椭圆曲线密码签名的应用

- 安全，密钥短、软硬件实现节省等特点。
- **2000**年美国政府已将椭圆曲线密码引入数字签名标准**DSS**。
- 我国也颁布了椭圆曲线密码签名标准**SM2**。

二、中国商用公钥密码SM2签名算法

1、 推荐使用256位素域*GF*(*p*)上的椭圆曲线：

$$y^2 = x^3 + ax + b$$

曲线参数：

p **= 8542D69E 4C044F18 E8B92435 BF6FF7DE 45728391 5C45517D 722EDB8B 08F1DFC3**

a **= 787968B4 FA32C3FD 2417842E 73BBFEFF 2F3C848B 6831D7E0 EC65228B 3937E498**

b **= 63E4C6D3 B23B0C84 9CF84241 484BFE48 F61D59A5 B16BA06E 6E12D1DA 6E12D1DA**

n **= 8542D69E 4C044F18 E8B92435 BF6FF7DD 29772063 0485628D 5AE74EE7 C32E79B7**

h **=1**

Gx **= 421DEBD6 1B62EAB6 746434EB C3CC315E 32220B3B ADD50BDC 4C4E6C14 7FEDD43D**

Gy **= 0680512B CBB42C07 D47349D2 153B70C4 E5D7FDFC BFA36EA1 A85841B9 E46E09A2**

2、密钥：

- 私钥是随机数：d，$d \in [1，n\text{-}1]$
- 公钥是点：$P = dG$

二、中国商用公钥密码SM2签名算法

3、产生签名的算法（SIG）

- 设A发签名消息给B。
- 设待签名消息为M，ID_A是A的标识符，$ENTL_A$是ID_A的长度，d_A是A的私钥，基点$G = (x_G, y_G)$，A的公钥 $P_A=d_AG = (x_A, y_A)$。

  Z_A=Hash ($ENTL_A \parallel ID_A \parallel a \parallel b \parallel x_G \parallel y_G \parallel x_A \parallel y_A$),
- 这里，Hash=SM3

① 置$M^*=Z_A \parallel M$;

② 计算e = Hash(M^*);

③ 用随机数发生器产生随机数$k\in[1, n\text{-}1]$;

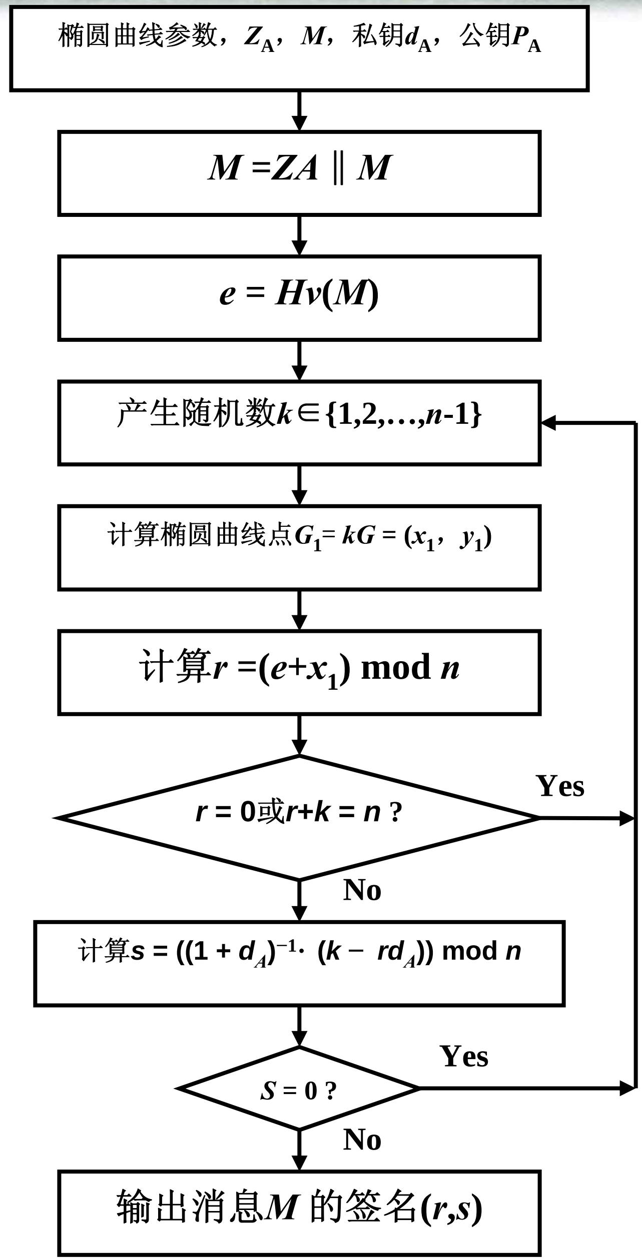
④ 计算椭圆曲线点$G_1(x_1, y_1)=kG$;

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 以(r,s)作为对消息M 的签名。

产生签名算法框图



椭圆曲线参数，Z_A，M，私钥d_A，公钥P_A
$\bar{M} = Z_A \parallel M$
$e = H_v(\bar{M})$
产生随机数$k \in \{1,2,\ldots,n-1\}$
计算椭圆曲线点$G_1 = kG = (x_1, y_1)$
计算$r = (e+x_1) \bmod n$
$r = 0$或$r+k = n$?
Yes
No
计算$s = ((1 + d_A)^{-1} \cdot (k - rd_A)) \bmod n$
$S = 0$?
Yes
No
输出消息M的签名(r,s)

二、中国商用公钥密码SM2签名算法

- 比较SM2签名算法与传统签名算法

① 传统椭圆曲线密码签名算法是原理性的算法，而SM2是实用性的标准算法

② 两者的基本思想一致：

  - 都是以 r, s 为签名
  - 以 kG 产生 r
  - 以 d, r, k 产生 s

武汉大学

二、中国商用公钥密码SM2签名算法

③两者有许多不同

- 传统椭圆曲线签名直接使用m产生签名；
- 而SM2使用$M^* = Z_A \| M$， $e = \mathrm{Hash}(M^*)$
- SM2使用了用户参数和系统参数，起到一定的认证作用，提高了安全性：
  - ID_A是A的标识。$ENTL_A$是ID_A的长度。基点是$G = (x_G, y_G)$
  - A的私钥是d_A，A的公钥是$P_A = d_A G = (x_A, y_A)$
  - $Z_A = \mathrm{Hash}\ (ENTL_A \| ID_A \| a \| b \| x_G \| y_G \| x_A \| y_A)$
- 传统椭圆曲线签名算法计算：点R（x_R, y_R）$= kG$，并记$r = x_R$；
- SM2计算：点$G_1(x_1, y_1) = kG$，且计算$r = (e + x_1) \bmod n$；

武漢大學

二、中国商用公钥密码SM2签名算法

③ 两者有许多不同

- 传统椭圆曲线签名算法计算：

  $s=(m-dr)k^{-1} \bmod n$ ；

- SM2计算：$s = ((1 + d_A)^{-1} \cdot (k - r \cdot d_A)) \bmod n$。$M$ 没有直接出现，而是通过r参与其中；私钥d_A作用了两次。
- SM2增加了合理性检查，确保签名正确，提高安全性。
- 例如第⑤中检查$r+k=n$是否等于n。

如果$r+k=n$，则$k = -r \bmod n$，会使$s = ((1 + d_A)^{-1} \cdot (k - r \cdot d_A)) \bmod n = ((1 + d_A)^{-1} \cdot (-r)(1 + d_A)) = -r \bmod n$ 。$s = -r \bmod n$，显然是不合适的。

二、中国商用公钥密码SM2签名算法

4、验证签名的算法（VER）

- 设B接收到的消息为M'，签名为(r', s')，P_A为A的公钥。
- 这里，Hash=SM3

① 检验$r' \in [1, n\text{-}1]$是否成立，若不成立则验证不通过；

② 检验$s' \in [1, n\text{-}1]$是否成立，若不成立则验证不通过；

③ 置$M^* = Z_A \parallel M'$；

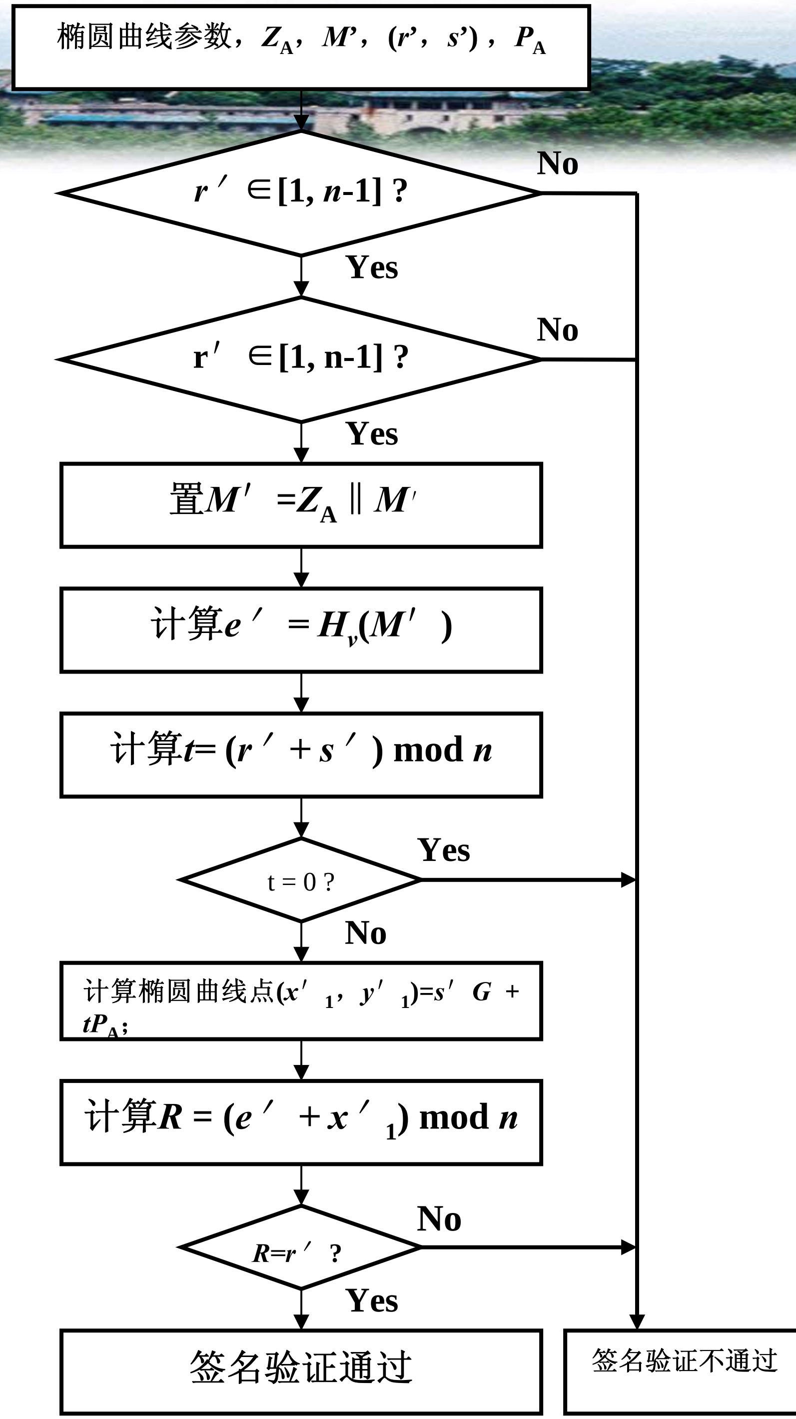
④ 计算$e' = \mathrm{Hash}(M^*)$；

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$G_1'(x_1'; y_1') = s'G + tP_A$；

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。

验证签名算法框图



椭圆曲线参数，Z_A，M'，(r', s')，P_A
$r' \in [1, n-1]$?
No
Yes
r′ ∈[1, n-1] ?
No
Yes
置$M' = Z_A \parallel M'$
计算$e' = H_v(M')$
计算$t = (r' + s') \bmod n$
t = 0 ?
Yes
No
计算椭圆曲线点$(x'_1, y'_1) = s'G + tP_A$;
计算$R = (e' + x'_1) \bmod n$
$R = r'$?
No
Yes
签名验证通过
签名验证不通过

二、中国商用公钥密码SM2签名算法

5、验证的正确性

① 因为产生签名算法的第⑤和第⑥步都是**mod** n运算，且要求$r\neq 0$且$s\neq 0$，这样就确保了$r\in[1, n\text{-}1]$且$s\in[1, n\text{-}1]$。如果签名没有被篡改和错误，则必有$r' = r\in[1, n\text{-}1]$且$s' = s\in[1, n\text{-}1]$。对此进行检验，可发现签名(r,s)是否被篡改或有错误，确保其完整性。这说明验证签名算法①和②的验证是合理的。

二、中国商用公钥密码SM2签名算法

5、验证的正确性

② 签名时确保了$r \neq 0$ 且$s \neq 0$，如果$t = r + s = 0 \bmod n$，则$r+s$是n的整数倍。但是，由于$r \in [1, n\text{-}1]$且$k \in [1, n\text{-}1]$，所以$2 \leqslant r+k \leqslant 2n\text{-}2$。又由于签名时确保了$r+k \neq n$，所以$r+k$不是$n$的整数倍。据签名算法⑥ 有，$s = \dfrac{k - rd}{1 + d}$

所以 $r + s = r + \dfrac{k - rd}{1 + d} = \dfrac{r + k}{1 + d}$，于是 $r + s = \dfrac{r + k}{1 + d}$ 也不是n的整数倍。

否则，因d和$1+d$都是正整数，这导致$(r+k)$是n的整数倍，与前面$r+k$不是n的整数倍矛盾。$r+s$不是n的整数倍，即 $r + s \bmod n \neq 0$。这说明，如果r'和s'没有被篡改或错误，则有$r' = r$和$s' = s$，则有$t = (r' + s') = (r + s) \bmod n \neq 0$。这说明验证签名算法⑤的验证是合理的。

二、中国商用公钥密码SM2签名算法

5、验证的正确性

③ 可验证性的证明：

- 一方面，$sG + tP_A = sG + (r+s)(dG) = (s+rd+sd)G$。
- 另一方面，因为 $s = \dfrac{k - rd}{1 + d}$

  ，故有 $(s + rd + sd) = s(1 + d) + rd = \dfrac{k - rd}{1 + d}(1 + d) + rd = k$

  所以 $sG + tP_A = kG = G_1(x_1, y_1)$。如果$x_1'$和$e'$没有被篡改或错误，则有$e' = e$，$x_1' = x_1$。根据产生签名算法⑤，$r = (e+x_1) \bmod n$，又根据验证签名算法⑦，$R = (e' + x_1') \bmod n$。
- 所以在$e' = e$，$x_1' = x_1$的条件下，有$R = r$ 。

二、中国商用公钥密码SM2签名算法

- **SM2 签名验证算法的一个显著特点是，其中加入了较多的检错功能。**
- 因为这是收信者对收到的签名数据进行验证，而签名数据是经过信道传输过来的，由于信道干扰和对手的篡改，因此，签名数据中含有错误或被篡改的可能性是存在的。
- 把错误和篡改检测出来，对提高签名验证系统的数据完整性、系统可靠性和安全性是有益的。
  - 验证算法中的①检查签名分量*r'*的合理性
  - 验证算法中的②检查签名分量*s'*的合理性
  - 验证算法中的⑤检查*t*的正确性

武漢大學

二、中国商用公钥密码SM2签名算法

6、SM2数字签名方案的应用

- 安全。
  - 目前尚没有发现求解椭圆曲线离散对数问题的亚指数算法。
- 软硬件实现规模小，方便。
  - **160位的椭圆曲线密码的安全性，相当于1024位的RSA密码。**
- 实现难点：
  - 倍点运算。
- 目前最大的应用是二代身份证。

谢　谢！