用ECC签名验证-ecdsa(Elliptic Curve Digital Signature Algorithm)

- (1)签名
- r = k*G ; k是随机数
- s = (m+r*d)/k ; m是明文或hash，d是私钥

- (2)验证
- (m/s)*G+(r/s)*R == r
- (m/s)*G+(r/s)*R = mG/s + rR/s =(mG+rdG)/s = (m+rd)G/((m+rd)/k) = kG
- 如果伪造m或d，都无法通过验证。

用ECC签名验证 - ecnr(Elliptic Curve Nyberg-Rueppel Signature)

- (1)签名
- r = k*G+m
- s = k-r*d

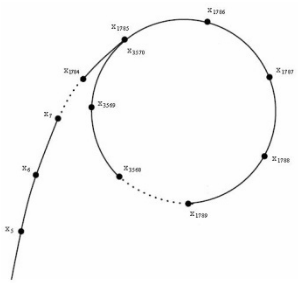
- (2)验证
- r - (s*G+r*R) == m
- r - (s*G+r*R) = r - ((k-rd)G + rdG)= r - (kG-rdG+rdG) = r - kG = kG+m-kG = m

椭圆曲线算法安全性

- 椭圆曲线算法的安全性取决于给定kP和P时确定k的难度，这被称为椭圆曲线对数问题。
- 已知获取椭圆曲线对数的最快方法是Pollard rho法。
- 椭圆曲线算法可以使用比RSA小得多的密钥长度来提供同等的安全。

ECDLP主要攻击

- Pohlig – Hellman 方法
- 平方根方法：一般算法

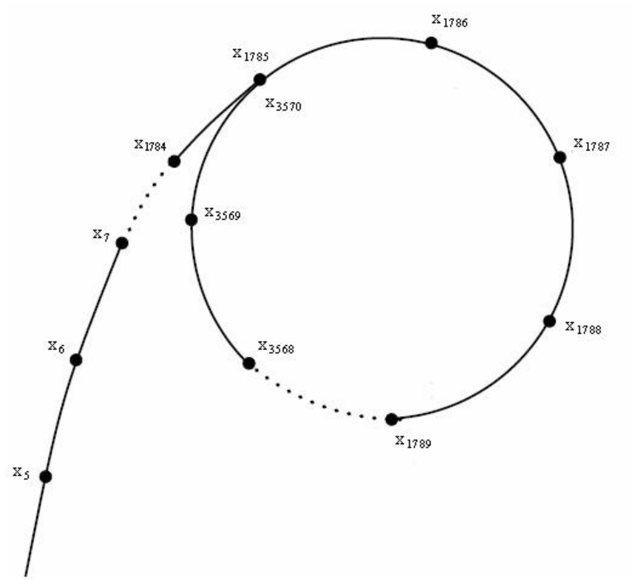


- 特殊曲线：
  Additive Reduction (1998Semaev, Araki/Satoh, Smart),
  Multiplicative Reduction (MOV 1993, Frey-Ruck1994),
- 指标计算：
  Weil Descent (Frey1998, Hess, Gaudry, Diem, Scholten)
  Summation polynomial(Semaev2004)

Pollard Rho 算法

- Pollard, J. M. (1978). "Monte Carlo methods for index computation (mod p)". Mathematics of Computation 32 (143): 918–924.

$$X_{i+1} = f(X_i) = \begin{cases} Q + X_i & X_i \in S_1, \\ 2X_i & X_i \in S_2, \\ P + X_i & X_i \in S_3. \end{cases}$$



- Pollard rho and its parallelized variants are at present known as the best generic algorithms for ECDLP

椭圆曲线算法安全性

➢ 对于相同的密钥长度，ECC和RSA所需的计算工作量相当。因此，使用密钥长度比相对安全的RSA短的ECC具有计算优势。

Table 10.3 **Comparable Key Sizes in Terms of Computational Effort for Cryptanalysis (NIST SP-800-57)**

Symmetric Key Algorithms	Diffie–Hellman, Digital Signature Algorithm	RSA (size of n in bits)	ECC (modulus size in bits)
80	$L = 1024$ $N = 160$	1024	160–223
112	$L = 2048$ $N = 224$	2048	224–255
128	$L = 3072$ $N = 256$	3072	256–383
192	$L = 7680$ $N = 384$	7680	384–511
256	$L = 15,360$ $N = 512$	15,360	512+

Note: L = size of public key, N = size of private key.

椭圆曲线算法安全性 - 旁路攻击

- 椭圆曲线密码学和其他的离散对数不同，在离散对数中可以用相同的程序处理平方以及乘法，但椭圆曲线上的加法在加倍（P = Q）和一般加法（P ≠ Q）上会因为使用的座标系统而有显著的不同。
- 因此有关旁路攻击（例如时间或功耗分析）的防护就格外的重要，例如用固定模式窗口（fixed pattern window，也称为comb）的方式（不会增加运算时间）。另外也可以使用爱德华曲线（Edwards curve），这是一类特别的椭圆曲线，其中的加倍和加法可以用同一个运算完成。

- 另一个ECC系统的威胁是来自于差分故障分析的风险，特别是在智能卡上的应用。

椭圆曲线算法安全性 － 旁路攻击

BINALG

Input : P and d

Output: $Q = dP$

$Q \leftarrow P$
For i from l–2 to 0 do
  $Q \leftarrow 2Q$
  If $d_i = 1$ then $Q \leftarrow Q+P$
Return Q

(a) Binary algorithm

BINALG′

Input: P and d

Output: $Q[0] = dP$

$Q[0] \leftarrow P$
For i from l–2 to 0 do
  $Q[0] \leftarrow 2Q[0]$
  $Q[1] \leftarrow Q[0]+P$
  $Q[0] \leftarrow Q[d_i]$
Return $Q[0]$

(b) Double-and-add algorithm

Fig. 1: Scalar point multiplication algorithms

椭圆曲线算法安全性 - 旁路攻击

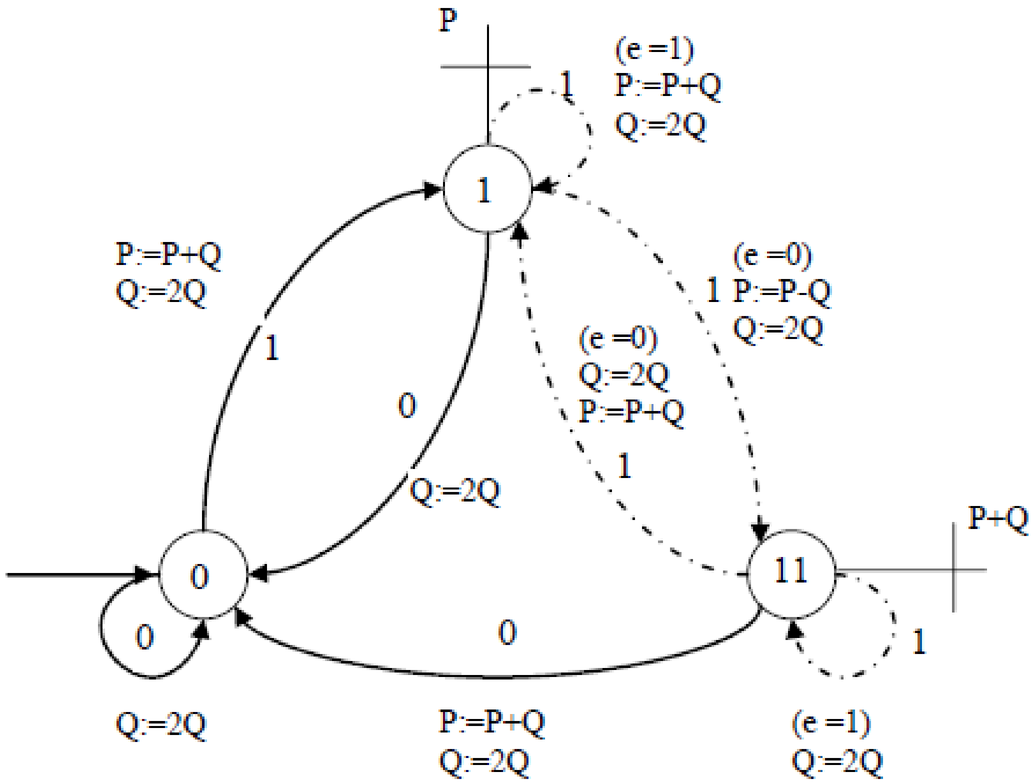


Fig. 2: Randomized Automaton 1 [4]

椭圆曲线算法安全性 – 后门

- 密码学专家担心，美国国家安全局（NSA）可能已在至少一个以椭圆曲线为基础的伪随机发生器中置入kleptographic后门。前美国中央情报局（CIA）职员爱德华·斯诺登所泄漏的内部摘要暗示，NSA在双椭圆曲线确定性随机比特生成器标准中加入后门。微软公司的研究人员针对此标准中一个的疑似后门进行分析，并得出结论：拥有此算法私钥的攻击者，可以只根据32字节的PRNG输出，找到加密的密钥。
- 密码学家发起了“SafeCurves”计划，整理并列出安全性易实现且设计过程完全公开可验证的曲线，以减少曲线被植入后门的可能性。

椭圆曲线算法安全性 – 量子计算攻击

- 如果攻击者拥有大型量子计算机，那么他可以使用Shor算法解决离散对数问题，从而破解私钥和共享秘密。目前的估算而言，椭圆曲线会比RSA更先遭到量子计算机的破解。
- 目前还不存在建造如此大型量子计算机的科学技术，因此椭圆曲线密码学至少在未来十年（或更久）依然是安全的。但是密码学家已经积极展开了后量子密码学的研究。其中，超奇异椭圆曲线同源密钥交换（SIDH）有望取代当前的常规椭圆曲线密钥交换（ECDH）。

IEEE TRANSACTIONS ON COMPUTERS, VOL. 69, NO. 11, NOVEMBER 2020 1681

Side-Channel Analysis and Countermeasure Design on ARM-Based Quantum-Resistant SIKE

Fan Zhang, *Member, IEEE*, Bolin Yang, Xiaofei Dong, Sylvain Guilley, *Member, IEEE*, Zhe Liu, *Senior Member, IEEE*, Wei He, Fangguo Zhang, and Kui Ren, *Fellow, IEEE*

椭圆曲线－ Curve25519

- Curve25519是著名密码学家Daniel J. Bernstein在2006年独立设计的椭圆曲线加密算法，与现有的任何椭圆曲线算法完全独立。
- 在密码学中，Curve25519是一种椭圆曲线，提供128位安全性（256位密钥），专为Elliptic Curve Diffie－Hellman （ECDH）密钥协议方案而设计。

- 使用的曲线是$y^2 = x^3 + 486662x^2 + x \bmod 2^{255} - 19$
- Curve25519的构造避免了许多潜在的实现陷阱，比如timing attack、Pohlig－Hellman algorithm attack。

椭圆曲线 - Curve25519

- 特点:

- 速度快。25519系列曲线是目前最快的椭圆曲线加密算法，性能远远超过NIST系列。
- 完全开放设计。算法各参数非常明确，没有任何可疑之处，而目前广泛使用的椭圆曲线是NIST，系数有来历不明的随机种子，如：secp256k1

椭圆曲线 - Ed25519

- Ed25519是使用SHA-512（SHA-2）和Curve25519的EdDSA签名方案。
- Ed25519旨在提供与128位对称密码相当的攻击阻力。公钥长256位，签名长512位。
- Ed25519不使用依赖secret数据的分支操作和数组索引步骤，因此免于许多旁路攻击。

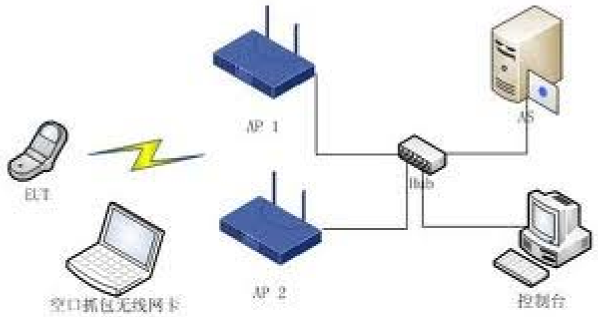
ECC在国外现实应用

- 比特币与ECC
- SSH：ECDSA，ECDH
- TLS
- Austrian e-ID Card奥地利电子身份证

我国的ECC产业化

- 商密标准：SM2椭圆曲线公钥密码算法

国家商用密码管理办公室
www.oscca.gov.cn



- WIPA
  ECDSA，ECDH
- 可信计算
  - 《可信计算密码支撑平台功能与接口规范》国家密码管理局2007年12月
- ……

当前ECC标准

- ANSI X9：62，63，92，…
- IEEE：1363-2000，P1363a，P1363.2，P802.15.3/4，…
- ISO：14888-3，9496，15496，18033-2，…
- FIPS：186-2，2XX，…
- NESSIE，IPA Cryptrec，…
- SECG：SEC1，SEC2，…
- IETF：PKIX，IPSec，SMIME，TLS，…
- SET，MediaPlayer，5C，WAP，…
- China：SM2

ECC的当前的研究与实现

- 更快速实现：
  新算法(Edwards curves)，软件，硬件，

- 标准化与新产品
  Certicom, RSA,
  NIST, IEEE P1363……
  RFID,

公钥密码学的研究热点

1980 1990 2000 2010 2020

RSA (整数分解**问题**)

ECC(**短的密钥, 离散对数问题困难**)

基于配对的密码体制**(IBE)**

后量子密码体制(**格, 纠错码问题**等)

证明gcd(n, u)=an+bu

- 设n/u的商为q, 余数为r， 则有 r = n-q*u
- 若gcd(n, u)=k， 则r一定也包含因子k， 因此有 gcd(n, u) = gcd(u, r)
- 由此可得求gcd(n, u)的Euclid算法如下：

```
y=n;
x=u;
while(x!=0)
{
    q = y/x;
    r = y%x;
    y=x;
    x=r;
}
```

- 当除数x=0时， 被除数y=gcd(n, u)

证明gcd(n, u)=an+bu

- 现用数学归纳法证明上述算法中的被除数y及除数x可以表示成:

  $y_i = a1_i*n + b1_i*u$ (a)

  $x_i = a2_i*n + b2_i*u$ (b)

- 其中y_i及x_i表示Euclid算法第i次循环中计算q、r时的被除数及除数。
- 当i=0时，只要取$a1_i=1$，$b1_i=0$，$a2_i=0$，$b2_i=1$，则(a)(b)成立。

证明gcd(n, u)=an+bu

- 设i=j时，(a)(b)成立，则当i=j+1时，

$$y_{j+1} = x_j = a2_j*n + b2_j*u$$

$$x_{j+1} = y_j \% x_j = a1_j*n + b1_j*u - q_j*(a2_j*n + b2_j*u)$$

$$= (a1_j-q_j*a2_j)*n + (b1_j-q_j*b2_j)*u$$

- 其中q_j表示Euclid算法第j次循环中计算出来的商。显然，当i=j+1时，取

$$a1_{j+1} = a2_j,\ b1_{j+1} = b2_j$$

$$a2_{j+1} = (a1_j-q_j*a2_j),\ b2_{j+1} = (b1_j-q_j*b2_j)$$

- 即可使(a)(b)成立。
- 因此，Euclid算法中的y及x均可以表示成an+bu的形式，而当x=0时，y就是gcd(n, u)，于是有gcd(n, u)=an+bu。

（补充）证明gcd(n, u)= an+bu - 证明gcd(n, u) = gcd(u, r)

- 设n/u的商为q, 余数为r， 则有 r = n-q*u
- 设n，u最大公约数为c
- n=a*c
- u=b*c
- r=n-q*u=a*c-q*b*c=c*（a-q*b）
- 需证明b和a-q*b互质（反证法）：
  - 假如b和a-q*b不互质，设b=x*d， a-q*b=y*d
  - u=b*c=x*c*d
  - n=a*c=c*（y*d+q*b）=c（y*d+q*x*d）=c*d*（y+qx）
  - 得n，u的一个因子为c*d>c, 与前面假设n，u最大公约数为c矛盾
- 由于b和a-q*b互质
- 因此gcd（n，u）=gcd（u，r）=c

ECC算法的数学基础 - Euler准则

- $y^2 = x \bmod p$
- 设p>2是一个素数，x是一个整数，gcd(x,p)=1，则
- （1） x是模p的平方剩余当且仅当
  - $x^{(p-1)/2} \equiv 1 \pmod p$
- （2） x是模p的平方非剩余当且仅当
  - $x^{(p-1)/2} \equiv -1 \pmod p$

证明Euler准则

- 若方程有解$y \in Z_p$，则x是模p的平方剩余：$y^2 = x \bmod p$
- 设p>2是一个素数，x是一个整数，gcd(x,p)=1，则x是模p的平方剩余的充要条件是：$x^{(p-1)/2} \equiv 1 \pmod p$
- 证明：
- (1) 必要性
- 因为$y^2 = x \bmod p$，并且gcd(x,p)=1，所以一定有 gcd(y, p)=1；
- 根据Fermat小定理知，$y^{p-1} \equiv 1 \bmod p$，因此
- $x^{(p-1)/2} = (y^2)^{p-1/2} = y^{p-1} = 1 \bmod p$

证明Euler准则

- (2) 充分性
- 因为$x^{(p-1)/2} \equiv 1 \pmod{p}$，且x mod p $\in Z_p$，不妨设$x \in Z_p$。而$Z_p=\{0,1,2,\cdots,p-1\}$是有限域，$Z_p^*=\{1,2,3,\cdots p-1\}$在模p乘法运算下是一个循环群，所以一定存在$Z_p^*$的一个生成元b，使得下式成立：

  $x=b^i \bmod p$，$1 \leqslant i \leqslant p-1$

- 例如：$1=4^2 \bmod 5$；$2=3^3 \bmod 5$；$3=2^3 \bmod 5$；$4=3^2 \bmod 5$；
- 因此，$1 = x^{(p-1)/2} = (b^i)^{(p-1)/2} = (b^{p-1})^{i/2} \bmod p$
- 因为b的阶为p-1，即$b^{p-1} \bmod p = 1$，所以i必定是偶数，于是x模p的平方根有整数解，并且其值为$\pm b^{i/2} \bmod p$。

（补充）证明Euler准则 – 原根

原根：

- 对于两个正整数gcd(a,m)=1，由欧拉定理可知，存在正整数d≤m-1， 比如说欧拉函数d=φ(m)，即小于等于m的正整数中与m互质的正整数的个数，使得$a^d \equiv 1 \pmod m$。
- 由此，在gcd(a,m)=1时，定义a对模m的指数$\delta_m(a)$为使$a^d \equiv 1 \pmod m$成立的最小的正整数d。由前知$\delta_m(a)$一定小于等于φ(m)，若$\delta_m(a) = \varphi(m)$，则称a是模m的原根。

原根存在定理：一个数 m 存在原根当且仅当 $m = 2, 4, p^\alpha, 2p^\alpha$，其中 p 为奇素数，$\alpha \in \mathbb{N}^*$。

原根的性质：

- 对正整数(a,m) = 1，如果 a 是模 m 的原根，那么 a 是整数模n乘法群（即加法群 Z/mZ的可逆元，也就是所有与 m 互素的正整数构成的等价类构成的乘法群）Zn的一个生成元。

Thank you！