楕円曲線暗号(ECC)の脆弱性攻撃による解読例

2020 年 3 月 1 日　後　保範（ISCPC）

1. ECC の係数と点

(1) ECC の係数例

$y^2 = x^3 + ax + b \pmod p$

$p = 19$,　$a = 3$,　$b = 10$,　位数 r=17 は 2.で定義。

(2) ECC 上の点の例（ Q=[x,y] ）

$Q = [13,2]$：　$y^2 = 2^2 = 4$,　$x^3+ax+b = 13^3+3*13+10 = 2246 = 4 \pmod{19}$

$y^2 = x^3+ax+b \pmod p$が成立するので Q は(1)の ECC 上の点

2. ECC の加算結果と位数(r)

$Q_1=Q$, $Q_2=Q_1+Q$, $Q_3=Q_2+Q$,...,$Q_{17}=Q_{16}+Q$ の結果を示す。+処理は後述。

[0,0]は無限遠点と言われる不動点。正式には [∞,∞]だが、[0,0]で表す。

位数 r は r*Q=[0,0]なる整数。Q_{17}=[0,0]なので r=17。*処理は後述。

Q_1= [13,2],　Q_2= [9,14],　Q_3= [6,15],　Q_4= [5, 13],　Q_5= [2, 9],

Q_6= [11,14],　Q_7= [12,11],　Q_8= [18,5],　Q_9= [18, 14],　Q_{10}= [12, 8],

Q_{11}= [11,5],　Q_{12}= [2,10],　Q_{13}= [5,6],　Q_{14}= [6, 4],　Q_{15}= [9, 5],

Q_{16}= [13,17],　Q_{17}= [0, 0]

(1) 加算(+)公式（係数 b と位数 r を使用しない）

公式は参考までに記載。(mod p)は p で割った余り。

(a) 2 倍算(R= 2*P=P+P)

R=[Rx,Ry], P=[Px,Py]とする。

$Rx = t^2 - 2Px \pmod p$.　$Ry = t(Px - Rx) - Py \pmod p$

$t = (3Px^2+a)/(2Py) \pmod p$　　<---係数 a を使う

(b) 加算(R=P+Q), P=Q なら 2 倍算を使用

R=[Rx,Ry], P=[Px,Py], Q=[Qx,Qy]とする。

$Rx = t^2 - Px - Qx \pmod p$,　$Ry = t(Px - Rx) - Py \pmod p$

$t = (Qy - Py)/(Qx - Px) \pmod p$

(2) 乗算(*)の方法

整数 n と点 P の乗算は 2 倍算と加算の組合せで行う。

例えば、Q=11*P なら

$11 = 2^3+2+1$ なので、$P_1=2*P$, $P_2=2*P_1$, $P_3=2*P_2$ を 2 倍算で求め、

$Q = P_3 + (P_1 + P)$と加算で計算する。

(3) ECC 上の点の性質

$Q + [0,0] = Q$： 例で $Q_{18}=Q_{r+1}=Q_1$ となり位数 r(=17)の周期で巡回。

任意の ECC 上の点 P に対し r*P=[0,0]となる r を位数と呼ぶ。

3. ECC による鍵交換例

A と B が通信で 1.(1)の ECC を使用して安全に鍵を交換する。

通信は点 P,Q,R だけで、整数 n,m を送信しないのが味噌。

(1) 鍵交換の通信と計算

step1:

A: 点 P=[11,5]を B に送信

step2: 乱数は r 未満の整数。

A: 乱数 m=7 選定。点 Q=m*P=[18,14]で、Q を B に送信。

B: 乱数 n=11 選定。点 R=n*P=[9,14]で、R を A に送信。

step3:

A: 受信した R=[9,14]で、S=m*R=7*[9.14]=[6,4]を計算。

B: 受信した Q=[18,14]で、T=n*Q=11*[18,14]=[6.4]を計算。

S=T=[6,4]となり、同じ 6 (x 座標を使用)の共通鍵を得る。

(2) 交換の原理

(a) ECC の鍵交換の目的は安全に同じ共通鍵を相手に渡す。

互いに送信した P,Q,R は盗聴されても良い。

情報自体は共通鍵を使用して共通鍵方式で暗号化して送信。

(b) 交換の考え方

P を 1 番として、m*P をすると m 番に進む。次に n*(m*P)すると

n*m 番に進むが r で巡回する。巡回は剰余(mod)となる。

n*m 番の乗算は順序によらず n*m=m*n となり、剰余も同一。

数学では ECC の乗算は交換律が成り立つため。

注) 交換律は行列乗算の様に成立しないものもある。

4. 誕生日のパラドックス

ECC を解読する ρ 法(並列は λ 法)は誕生日のパラドックスで、n 個中で衝突(誕生日が一緒と同じ)するものを探す。この方法では n 個から衝突を見つけるのがほぼ sqrt(n)回になる。23 人なら 50%の確率で同じ誕生日の人がいる。

23 人の根拠は統計理論で sqrt(π/2*365)=23 です。

誕生日のパラドックスをそのまま ECC の解読に適用しようとすると、衝突まですべて記憶が必要です。
ECC-160 ですと、ほぼ $2^{160/2}=2^{80}=10^{24}$=兆の兆倍です。記憶を特徴のある点だけ、例えば x 座標が $p/2^{40}$ 以下とすれば、記憶量がほぼ $1/2^{40}$ 減ります。
ρ法やλ法は特徴点を利用可能にして、メモリ使用量を減らす方法です。
ρ法の反復回数の平均は sqrt(πr/2)です。図 1 に反復回数を sqrt(πr/2)で正規化し、10 万回解読した場合の頻度を示します。平均なので、数倍の差は発生します。1 反復の計算量は 1 回の加算(2 倍算か加算)と同等です。

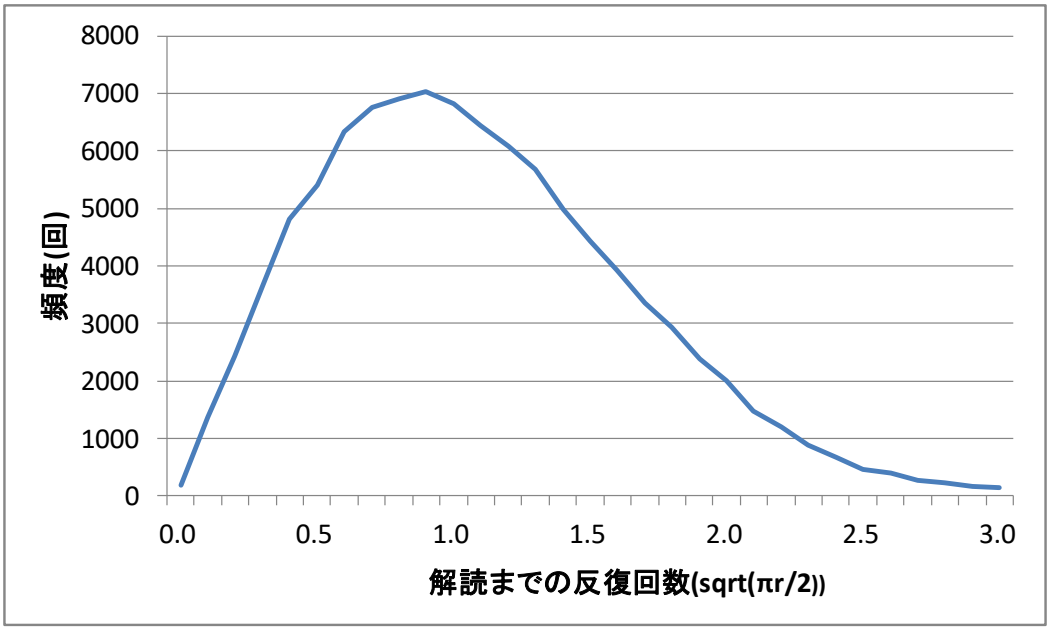

図 1. 40 ビット ECC を 10 万回解読した反復回数の分布

5. ECC 攻撃の係数と点

ECC の式:　$y^2 = x^3 + ax + b \pmod p$

本来の係数：　p = 19,　a = 3,　b = 10,　位数:r=17

暗号化に使用しない b(必然的に r も)を変更できる点 E を算出。

今回の例では E=[9,2]

E=[9,2]で係数 p,a は不変で b が変わり、r も下記に変化する。

b=8,　r=15=3*5

r が小さい素数の積に因数分解されるほど、ECC の解読は高速化する。

ここでは、E 及び b,r の算出方法 は記載しない。

6. 取得したデータで ECC を解読

(1) 高速解読の概念

上記 E で Q_1=E, Q_2=Q_1+E, Q_3=Q_2+E,...,Q_{15}=Q_{14}+E の結果を示す。

Q_1= [9,2],　Q_2= [7,7],　Q_3= [14,1],　Q_4= [12, 10],　Q_5= [3, 14],

Q_6= [11,2],　Q_7= [18,17],　Q_8= [18,2],　Q_9= [11, 17],　Q_{10}= [3, 5],

Q_{11}= [12,9],　Q_{12}= [14,18],　Q_{13}= [7,12],　Q_{14}= [9, 17],　Q_{15}= [0, 0]

今回は Q_{15}=[0,0]で位数 r は 15 となる。

ECC の性質 Q_{k+r}=Q_k から上記は 15 で巡回する。

r=15=3*5 なので、どの Q_k からでも、3 飛びなら 5 回で、5 飛びなら 3 回で元の Q_k に戻る。即ち、3 飛びなら要素数 5 の巡回、5 飛びなら要素数 3 の巡回となる。ECC は元の値に戻るか、[0,0]に到達すると解読される。

位数 r が因数分解されたら、解読対象となる要素数が激減し、ρ法では要素数のほぼ平方根で解読できるので、超高速解読となる。

今回の例では、r が小さいので激減しないが ECC-112 の例を示す。

ECC-112:　r= 4451685225093714776491891542548933：　素数

E=[3,7416258763144326353594885281423 4]で、r は下記に変化する。

r= 4451685225093714764417573581309056

=128591*58789*38923*26497*16087*8431*577*19*3*128

ρ法解読の平均反復数はほぼ sqrt(r)から sqrt(各因数)の合計に変化する。

ECC-112 では 2^{56}=数京回から、数千回に激減する。

最大素数がこの程度まで小さくできれば、完全な量子計算機に匹敵する。

完全な量子計算機は 30～50 年後ごろか？ 完全な量子計算機なら r が素数のままで解読できる。

4Ghz の PC で 100 万反復は約 1 秒で計算可能。よって解読は数ミリ秒。

本解読は暗号化処理の数十倍の計算量で可能。暗号の意味が無くなる。

(2) 高速解読方法

r が合成数なのを利用する。今回は r=15=3*5, E=[9,2]を活用する。

本来 R=n*P を B が計算するはずだったのを、トラップし B が R=n*E の計算結果 R=[9,14]を送るのを盗聴して、整数 n を求める。

S=3*E=[14,1]及び T=5*E=[3,14]とすると、S,T の 1,2,3...倍は下記になる。

S:　[14,1], [11,2], [11,17], [14,18], [0, 0]　：5 で巡回

T:　[3, 14], [3, 5], [0,0]　　：3 で巡回

即ち、S 及び T は位数 r を 5 及び 3 にしたのと同等になる。

位数 r の ECC はρ法でほぼ sqrt(r)の反復数で解読できる。

S の場合は R=n*E の両辺を 3 倍して 3*R=3*(n*E)=n*(3*E)=n*S となり、

H=3*R とすると、H=n*S から n を ρ 法で求める。
E を S,T に置き換えて H=n*S の方法で n を求めると下記になる。
S のケース: n=1,　T のケース:n=2
これは n (mod5)及び n (mod 3)の結果となっている。
次に、中国剰余定理で各剰余から元の n の値に戻すと n=11 となる。
従って、R=n*P の整数 n が解読できる。

7. 鍵盗聴の具体例

共通鍵盗聴の前提条件

(a) 脆弱性を利用し B の ECC 処理の妥当性チェックを外す。
妥当性チェックは点 P=[x,y]が p,a,b で表される ECC 上の点及び
位数 r を使用して r*P=[0,0]が成立することで行う。

(b) A,B の送信は傍受でき、変更して送信可能

(c) A,B の送信を含め、B と他の送受信も通常通り機能

A と B が 1.(1)の ECC を使用して通信し、共通鍵を盗聴する。
共通鍵は情報本体の通信の鍵で、通信内容を完全に元に復号できる。

step1:
A が B に送信する点 P=[11,5]を傍受し、E=[9,2]に変更し B に送る。

step2:
A から B に送信の Q=[18,14]を傍受
B から A に送信の R=[12,9]を傍受。6-(2)で n=11 と解読。
R を n*P=11*[11,5]=[9,14] に置き換え A に送信。

step3:
傍受した Q と解読した n を使用して T=n*Q=11*[18,14]=[6.4]を計算
T の x 座標の 6 が共通鍵となり、盗聴完了。

本方式では、A,B 共に共通鍵 6 が交換でき、通常の通信となる。
step2 で R を n と P で計算して、B から受信した R を計算したものに置き換え A に送信するのは A と B の鍵交換を通常通り行わせるため。

8. 脆弱性攻撃による ECC 解読の概要(具体例)

(1) ECC を解読する脆弱性攻撃
ECC の暗号化が係数 b,r を使用しない特性を利用。
送受信する点が正しい ECC 上の点かチェックする機能を攻撃で停止する。

(2) 解読対象の ECC 例
ECC 係数:　$y^2 = x^3 + ax + b \pmod p$

p= 839269, a= 306829, b= 534648, 位数 r= 839441

解読問題: R=n*P で点 P,R が下記のとき、整数 n を求める。

P=[402527, 332498], R=[277011, 733814]

(3) 解読方針

R=n*P を解読する代わりに P を E に置き換え、Q=n*E の問題に変える。

例では、E=[14,5]にする。Q=n*E が計算され、送信される Q を傍受。

Q= [723631, 174434]を傍受

これから整数 n を求める。

P を E に変更することで、ECC 係数の b と r は下記に変化する。

b= 737289, r= 840650= 43*23*17* 25*2

超高速解読には r が小さい素数(ベキ乗を含む)に分解される必要がある。

(4) Q=n*E から n を解読

(a) r の因数 43 を使用しての解読

s=r/43=19550 を求め

Q=n*E の両辺に s を乗算し s*Q=s*(n*E)=n*(s*E)とする。

T=s*Q, R=s*E とすると、Q=n*E の問題は T=n*R に変化する。

本例では R=[687036, 559703], T=[687036, 559703]である。

この変更により、43*R=43*T=[0,0]になるので位数 r は 840650 から 43 減少する。

T=n*R を ρ 法で解読すると、n=29 が得られる。

ρ 法での平均反復回数は sqrt=sqrt(43π/2)=8 となる。

(b) 因数 23,17,25 及び 2 を使用しての解読

(a)の因数 43 と同様にして解読する。それぞれの n は下記が得られる。

因数 23: n=5	因数 17: n=11
因数 25: n=18	因数 2: n=1

(c) 元の n へ戻す

r の各因数での n の結果は n (mod 因数)となっている。

即ち、n の 43,23,17,25,2 の剰余は 29,5,11,18,1 である。

中国剰余定理で元の n に戻すと n=475093 と解読できる。

中国剰余定理は百五減算とも言われる。それは 105=3*5*7 で、3,5 及び 7 の剰余から 105 未満の元の数が容易に計算可能なためである。