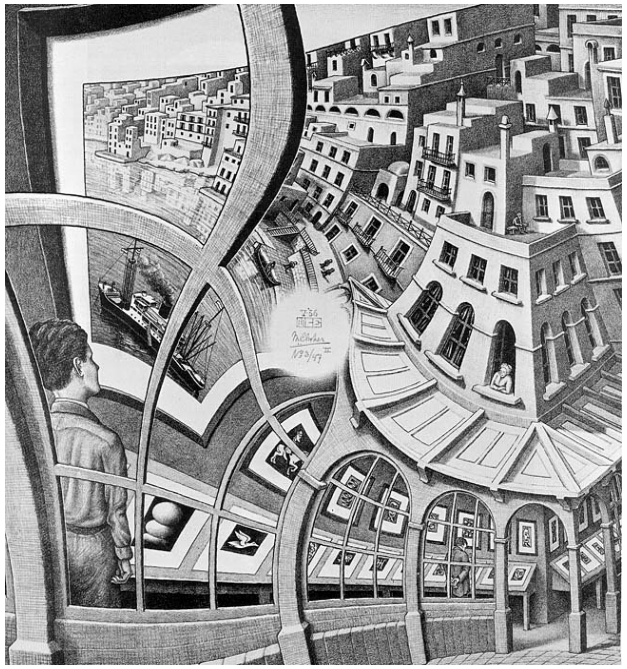
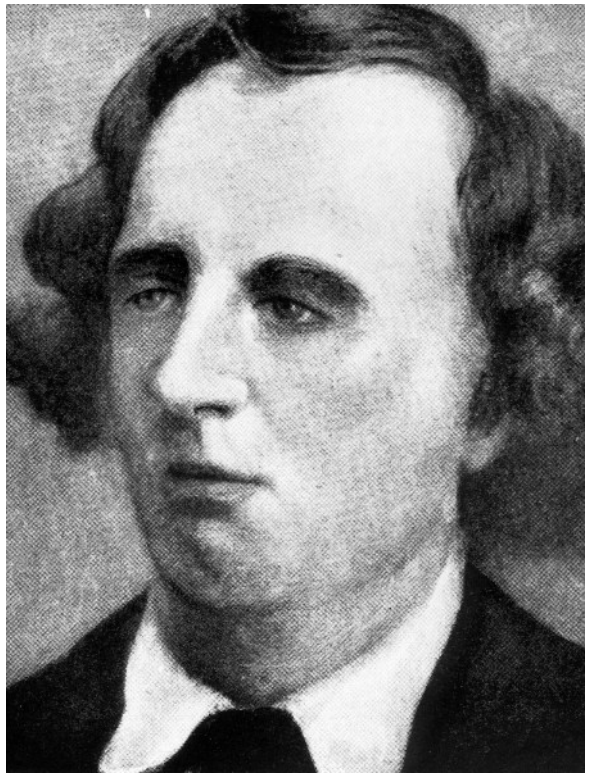


Новая схема атаки методом анализа сбоев (fault attack) на реализации криптоалгоритмов для эллиптических кривых

Алексей Чиликов,
Passware

Олег Тараскин, МИФИ

Эллиптические кривые



Karl Weierstrass (1815 - 1897)

Элл. кривая над полем K:

1. Мн-во точек (X, Y), где X и Y принадлежат K и удовл. уравнению:

Y^2 + a1*X*Y + a3*Y = X^3 + a2*X^2 + a4*X + a6
(ур-е в форме Вейерштрасса)

2. Точка на бесконечности O

Это абелева группа со следующей операцией сложения элементов (точек):

Для всех точек P, P + O = O + P = P
Если P = (X, Y) и Q = (X, -Y) то P + Q = O
(т.е в этом случае Q = - P)

Общая формула сложения точек

- Если P = (X1, Y1), Q = (X2, Y2) то P + Q = R,
  R(X3, Y3) опр. формулами:

  X3 = L^2 + a1*L – (X1 + X2)
  Y3 = -Y1 – L*(X3 – X1) + a1*X3 – a3
  где значение L :
  L = (3*X1^2 + 2*a2*X1 + a4 – a1*Y1) / (2*Y1 + a1*X1 + a3)
  если P равно Q
  L = (Y1 – Y2)/(X1 – X2) - в противном случае

  (Обратим внимание: отсутствует член a6 ур-я Вейерштрасса, на чем и будет основана атака)

Скалярное умножение точки на число

Пусть имеется точка P(x,y) и натуральное число n. Скалярным умножением точки P на число n называется точка Q , которая представляет собой результат сложения :

Q = P+P+…+P (n сложений) Обозначается: Q = n*P

Трудноразрешимые теоретико-числовые задачи:

1. Elliptic Curve Discrete Logarithm Problem (ECDLP) : по известным P и Q найти n
2. Elliptic Curve Decision Diffie-Hellman Problem(ECDDHP) : по заданным точкам P, Q = n*P,

   R = m*P найти точку S = n*m*P

   Для решения данных задач не найдено даже субэкспоненциальных алгоритмов (за искл. некоторых специальных случаев кривых)

Применение элл. кривых в криптографии

Идея применить кривые в криптографии принадлежит Victor Miller и Neal Koblitz (1985 г)

Victor Miller (справа)
(конференция EuroCrypt 2007)

Neal Koblitz

- Diffie-Hellman (DH) → Elliptic curve Diffie-Hellman (ECDH)
- Digital Signature Algorithm (DSA) → Elliptic Curve Digital Signature Algorithm (ECDSA)
- ElGamal Cryptosystem → ElGamal Cryptosystem on Elliptic Curves
- ГОСТ Р 34.10 – 94 → ГОСТ Р 34.10-2001
- VKO R 34.10-94 → VKO R 34.10-2001 (RFC 4357)

Метод анализа сбоев (fault attack) Классификация математических моделей :

- Степень контроля местоположения (времени)
  - Без контроля
  - Слабый контроль
  - Полный контроль
- Количество поврежденных битов:
  - Один бит
  - Небольшое число бит (напр. один байт)
  - Произв число бит заданной перем.

- Продолжительность воздействия:

  Кратковременное воздействие (после прекр. биты возвращаются в правильное состояние)

  Постоянное повреждение (после прекр. биты остаются в поврежденном состоянии)

  Деструктивное повреждение (физ. структура может быть разрушена)

Схема атаки

Цель атаки – устройство, реализующее скалярное умножение произвольной входной точки на заданное число d (секретный ключ) и

выдающее на выход результат умножения - точку.

Любая fault атака привязяна к конкретной реализации. Рассмотрим простейшую - скалярное умножения по методу “binary left to right”

Схема атаки

Constants: d – секретный ключ
Input: P – базовая точка
Output: Q = d*P
Q = O
for(i = n-1; i >= 0; i--)
{
    Q = Q + Q   - удвоение
    if(d[i] == 1)
        Q = Q + P   - сложение
}
return Q

где d[i] - i-й бит числа d,
O – “точка на бесконечности” т.е. единичный элемент группы точек

Схема атаки

- Воздействие - на промеж. рез-ты вычисл. Q, а именно на X – координату величины Q.
- Пусть мы проводим модификацию Q перед последним удвоением. Обозн. через Q[i] значение Q после i шагов. При обычном исполнении Q[i+1] = 2*Q[i] + d[i]*P, а перед последним шагом Q[n-1] -> Q`[n-1]. На последнем шаге Q`[n-1] сначала будет удвоена, затем к ней возможно будет прибавлена P
- Операции сложения и удвоения будут формально произведены по формулам сложения и удвоения для элл. кривых.

Схема атаки

Т.к. в ф-лах слож. и удвоения не участвует член ур-я Вейерштрасса a6, то результат можно рассматривать как точку на новой кривой.

Обозн. полученную точку через R’

$2*R' + d[n-1] *P = Q'[n-1]$

имеет хотя бы одно решение относ. R’

и знач. Y коорд. Совпадает с Y коорд. Q[n-1]

Схема атаки

Таким образом общий сценарий:

1. Опред. Истинное Q[n] и измененное Q’[n]
2. Найти мн-ва реш. ур-ний

   2*R + t*P = Q[n], на нач. кривой

   2*R’ + t*P = Q’[n], на новой. кривой

для обоих возм значений t - 0 или 1

3. Найти пересеч. мн-в Y координат решений
4. Если для некоторого t мн-ва Y пусто, то соотв. знач t != d[n-1]

5.В прот. случ. Т явл. допустимым.

- “New Fault Attack on Elliptic Curve Scalar Multiplication “ Alexey Chilikov, Oleg Taraskin
- IACR, ePrint