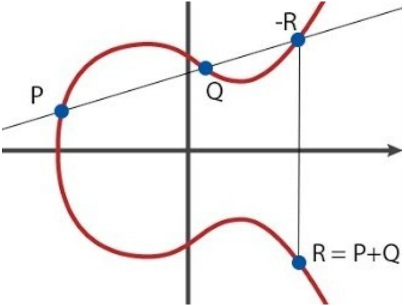
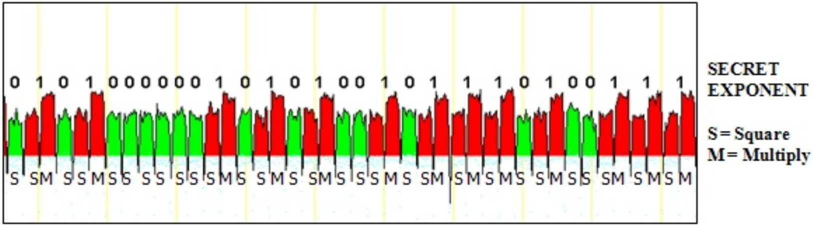
Differential Analysis Attacks and Countermeasures in Elliptic Curve Cryptography

Tiawna L. Cayton
tlcayton2@cs.ucsb.edu



What is SCA?

- Any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses
- Examples: Timing, power consumption, electromagnetic leaks, sound



Avoiding SPA

Algorithm 1 Double-and-Add Always

input P
$Q[0] \leftarrow P$
for i from $l-2$ to 0 do **do**
  $Q[0] \leftarrow 2Q[0]$
  $Q[1] \leftarrow Q[0] + P$
  $Q[0] \leftarrow Q[d_i]$
end for
output $Q[0]$

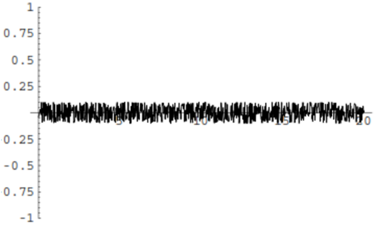
DPA on ECC

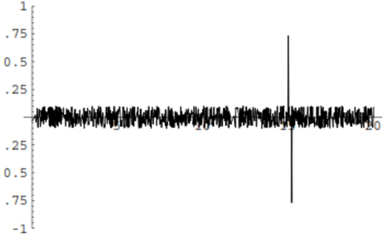
- For computing $Q = dP$
- Let $d = (d_{m-1}, ..., d_0)_2$ be the binary expansion of multiplier d
- Say the attacker knows the highest bits, $d_{m-1}, ..., d_{j+1}$, of d
- Then he **guesses** that the next bit $d_j = 1$
- He randomly chooses several points $P_1, ...P_t$ and computes $Q_r = \left(\sum_{i=j}^{m-1} d_i\right) P_r$ for $1 \leq r \leq t$
- Using a boolean selection function g, he prepares two sets, S_{true} and S_false
- S_{true} contains the set P_r such that $g(Q_r) = true$ and S_{false} contains the set P_r such that $g(Q_r) = false$

DPA on ECC

- Let $C(r)$ denote the side-channel information associated to the computation of kP_r by the device

$$\langle C(r)\rangle_{P_r \in S_{true}} - \langle C(r)\rangle_{P_r \in S_{false}}$$





Countermeasures Against DPA

- Randomization of Private Exponent
- Blinding the Point P
- Randomized Projective Coordinates

Randomization of the Private Exponent by Exponent Splitting

- Let k be a small random number generated for every run
- $Q = dP$ is calculated by first calculating $R = kP$, then calculating $Q = (d - k)R$
- This method requires knowledge of both k and $d - k$ to recover the value of d, if k is random each time, this protects against DPA

Randomization of the Private Exponent

- Let $\#\mathcal{E}$ be the number of points in the curve. $Q = dP$ is done by the following algorithm:

1. Select a random number r of size n bits.
2. Compute $d' = d + r \cdot \#\mathcal{E}$.
3. Compute the point $Q = d'P$. We have $Q = dP$ since $\#\mathcal{E}P = \mathcal{O}$

- This makes the attack infeasible because d' changes at each new execution of the algorithm.

Blinding the Point P

- Let R be a secret random point on the curve for which we know $S = dR$
- Use scalar multiplication to compute $d(R + P)$
- Subtract S to get $Q = dP$

- The points R and $S = dR$ can be initially stored and refreshed at each execution by computing $R \leftarrow (-1)^b 2R$ and $S \leftarrow (-1)^b 2S$ where b is a random bit generated at each execution.
- This makes the attack infeasible because the point $P' = P + R$ to be multiplied by d is not known to the attacker.

Blinding P Using Isomorphisms

- We say two elliptic curves E and E' are *isomorphic over* $\mathbb{K}$
- Because field isomorphisms induce group isomorphisms, we can randomize the scalar multiplication as follows.
- Let ψ be a random isomorphism from $E_{/\mathbb{K}}$ to $E'_{/\mathbb{K}}$, we can compute $Q = dP$ using,

$$Q = \psi^{-1}(d(\psi(P)))$$

Randomized Projective Coordinates

- Using a system of projective coordinates where
$$(X, Y, Z) = (\lambda X, \lambda Y, \lambda Z)$$
for every $\lambda \neq 0$ in the finite field.
- We can use a random λ before each new execution of the scalar multiplication algorithm of $Q = dP$.
- The randomization can also be completed after each point addition and doubling.
- This make the attack infeasible because the attacker cannot predict any specific bit of the binary representation of P in projective coordinates.

Conclusion

- Unless protected, implementations of ECC are vulnerable to DPA
- Countermeasures can be simple to implement and do not have to impact efficiency in a significant way
- It may be possible to exploit information leakage through side channels in a different way

References

- Jean-Sębastien Coron. Resistance against differential power analysis for elliptic curve cryptosystems. In Ç.K. Koç and C.Paar, editors, **Cryptographic Hardware and Embedded Systems (CHES '99)**, volume 1717 of **Lecture Notes in Computer Science**, pages 292-302. Springer-Verlag, 1999.
- M.Anwar Hasan. Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems. In Ç.K. Koç and C. Paar, editors, **Cryptogrpahic Hardware and Embedded Systems (CHES 2000)**, volume 1965 of **Lecture Notes in Computer Science,** pages 93-108. Springer-Verlag, 2000.
- Marc Joye and Christophe Tymen. Protections against differential analysis for elliptic curve cryptography. In Ç.K. Koç, D. Naccache, and C. Paar, editors, **Cryptogrpahic Hardware and Embedded Systems (CHES 2001)**, volume 2162 of **Lecture Notes in Computer Science,** pages 377-390. Springer-Verlag 2001.
- Elena Trichina and Antonio Bellezza. Implementation of elliptic curve cryptography with built-in counter measures against side channel attacks. In B.S. Kaliski Jr. et al., editors, **Cryptogrpahic Hardware and Embedded Systems (CHES 2002)**, volume 2523 of **Lecture Notes in Computer Science,** pages 98-113. Springer-Verlag 2003.
- Tetsuya Izu and Tsuyoshi Takagi. A fast parallel elliptic curve multiplication resistant against side channel attacks. In D. Naccache and P. Paillier, editors, **Public-Key Cryptography (PKC 2002)**, volume 2274 of **Lecture Notes in Computer Science,** pages 280-296. Springer-Verlag 2002.

Questions?