A first-order chosen-plaintext DPA attack on the third round of DES

Oscar Reparaz, Benedikt Gierlichs
KU Leuven, imec - COSIC
CARDIS 2017

Once upon a time...

Differential Power Analysis

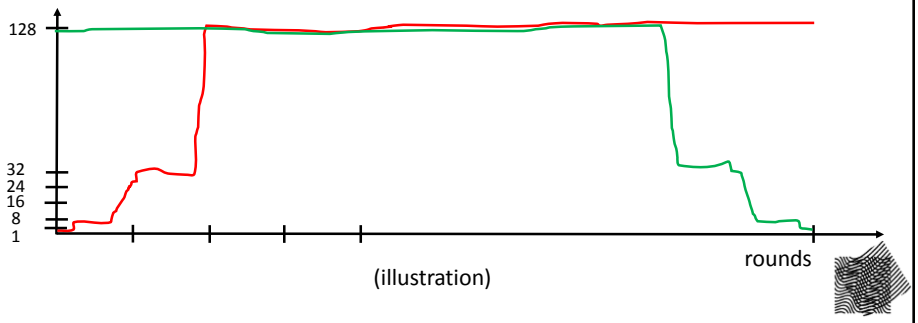
Paul Kocher, Joshua Jaffe, and Benjamin Jun

Cryptography Research, Inc.
870 Market Street, Suite 1088
San Francisco, CA 94102, USA.
http://www.cryptography.com
E-mail: {paul,josh,ben}@cryptography.com.

Abstract. Cryptosystem designers frequently assume that secrets will be manipulated in closed, reliable computing environments. Unfortunately, actual computers and microchips leak information about the operations they process. This paper examines specific methods for analyzing power consumption measurements to find secret keys from tamper resistant devices. We also discuss approaches for building cryptosystems that can operate securely in existing hardware that leaks information.

Divide and conquer in DPA

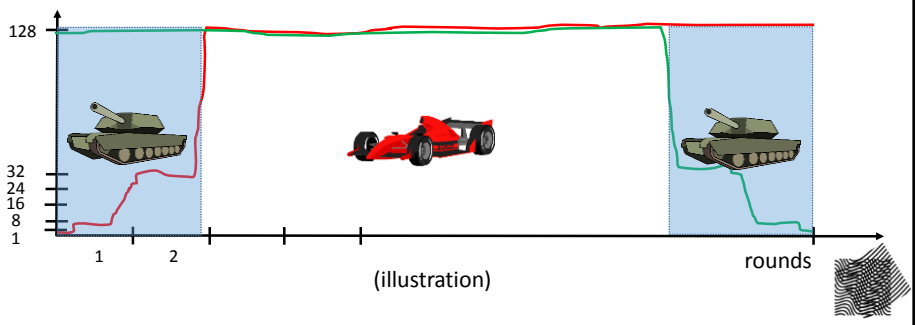
- Implementations of cryptographic algorithms slowly mix the input with the key
- Example: block cipher AES-128



(illustration)

Divide and conquer in DPA

- DPA on first (last) two rounds is easier than cryptanalysis
- First (last) two rounds need to be protected
- Inner rounds? Countermeasures are expensive.



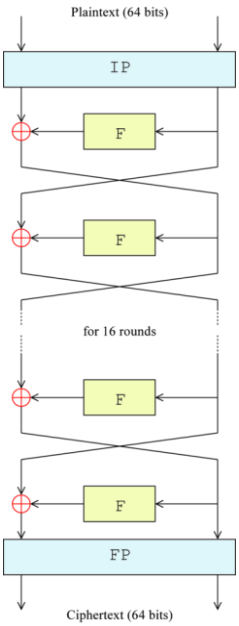
(illustration)

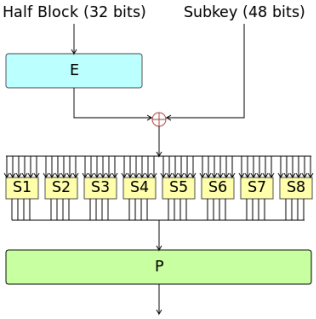
Attacks on inner rounds

- Based on detecting collisions
  - Different intermediates have the same value
  - Some form of cryptanalysis
  - ➢ All rounds of DES and AES have to be protected
  - Not DPA**!** Requires strong leakage from inner rounds
- Based on deactivating part of the state
  - Fix part of inputs to a constant
    $V = S(p_1 + k_1) + S(p_2 + k_2) + S(p_3 + k_3) + S(p_4 + k_4)$
  - Fix p2, p3 and p4 $V = S(p_1 + k_1) + c$
  - Reduce effort from 2^{4w} to 2^{2w}

What about DPA on DES?

DES





[image source: wikipedia]

What about DPA on DES?

- First round S-box outputs depend on 6 key bits
- Second round S-box outputs depend on ≤ 36 key bits
- Third round S-box output depends on ....

- DPA on first (last) two rounds is easier than cryptanalysis
- No need to protect inner rounds against DPA?

Contribution

- We present “A first-order chosen-plaintext DPA attack on the third round of DES”
  - Requires ability to choose inputs
  - Otherwise standard DPA attack
  - Complexity is that of 2-3 DPA attacks on the first round of DES + some minimal differential cryptanalysis
  - Two steps
    - DPA with chosen inputs to deactivate part of the state and Jaffe‘s trick to push unknown constants into the key guess
      - Recovers “blinded“ round 2 keys
    - Differential cryptanalysis to recover round 1 keys
      - Unblind round 2 keys
      - Invert key schedule

Step 1

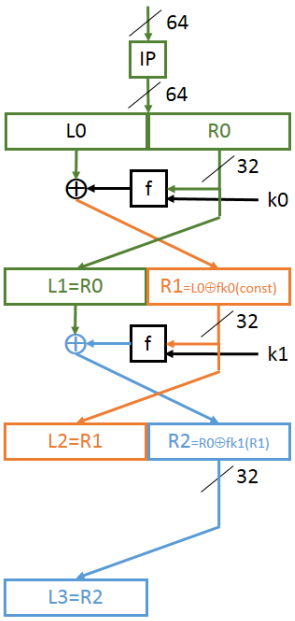
- Target leakge of L3
- Choose inputs s.t. L0 varies and R0 const
- Recover blinded round 2 key

$$k_1 \oplus E(C) = k_1 \oplus E[F_{k_0}(R_0)]$$

- Repeat with different const R0‘ and R0‘‘
- Recover also

$$k_1 \oplus E(C')$$

$$k_1 \oplus E(C'')$$



Step 2: untangle terms k1 and E(C)

- Classic differential attack on 1 round Feistel to recover k0
- Consider differences

$$\gamma = (k_1 \oplus E(C)) \oplus (k_1 \oplus E(C'))$$
$$\gamma' = (k_1 \oplus E(C')) \oplus (k_1 \oplus E(C''))$$
$$\gamma'' = (k_1 \oplus E(C'')) \oplus (k_1 \oplus E(C))$$
$$\gamma = E(C) \oplus E(C')$$
$$= E(F_{k_0}(R_0)) \oplus E(F_{k_0}(R'_0))$$

- First round output differences after E (invertible)
- We know the input difference R0 ⊕ R0‘

Step 2: untangle terms k1 and E(C)

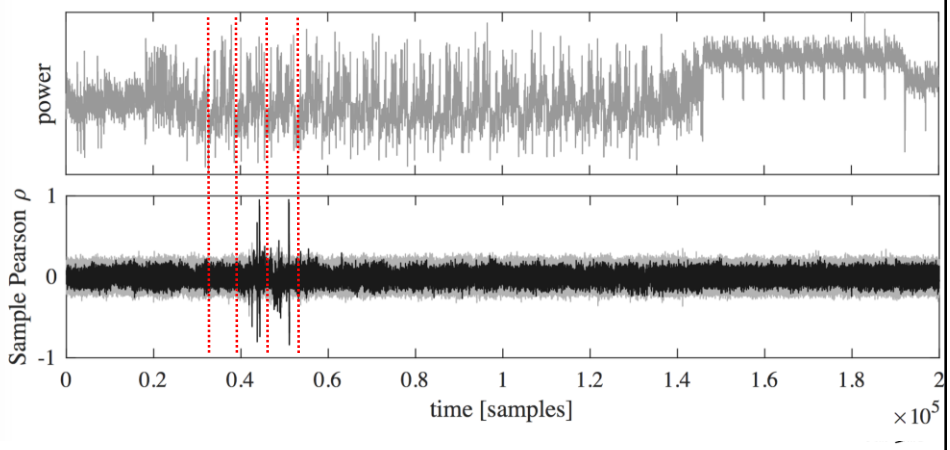
- Given input and output difference, key recovery differential attack for K0
- Divide and conquer: S-box by S-box, simple
- For one S-box
  - Guess on 6-bit key
  - Compute S-box output difference for R0 and R0‘
  - Apply E
  - Equals corresponding part of γ? Discard key guess if not.
- Repeat for other output differences γ‘ and γ‘‘
- Intersection of key candidates is expected to yield unique and correct K0

Step 2: untangle terms k1 and E(C)

- Given K0 compute $C = F_{k_0}(R_0)$
- And unblind the DPA recovered $k_1 \oplus E(C)$
- Invert DES key schedule to obtain DES key

Validation

- Unprotected SW DES on 8-bit µC, 200 measurements



Validation

- Step 1

$R_0 = 88\ 00\ 17\ FD$, recovered key $k_1 \oplus E[F_{k_0}(R_0)] = 25\ 0D\ 02\ 24\ 15\ 00\ 06\ 1F$
$R'_0 = A9\ 60\ 1B\ 9F$, recovered key $k_1 \oplus E[F_{k_0}(R'_0)] = 2A\ 34\ 11\ 1A\ 31\ 08\ 05\ 23$.
$R''_0 = 3E\ 57\ 8B\ 11$, recovered key $k_1 \oplus E[F_{k_0}(R''_0)] = 0B\ 2B\ 2D\ 11\ 0B\ 27\ 37\ 09$.
$R'''_0 = 3E\ 3E\ 3E\ 3E$, recovered key $k_1 \oplus E[F_{k_0}(R'''_0)] = 0B\ 2E\ 39\ 18\ 1F\ 2F\ 32\ 19$.

- Step 2

$k_0 = 17\ 00\ 21\ 0C\ 15\ 18\ 3D\ 0F \implies k_1 = 14\ 12\ 37\ 30\ 19\ 09\ 1F\ 0C$
$k_0 = 17\ 00\ 21\ 1F\ 15\ 18\ 3D\ 0F \implies k_1 = 14\ 12\ 37\ 30\ 19\ 09\ 1F\ 0C$
$k_0 = 17\ 00\ 21\ 23\ 15\ 18\ 3D\ 0F \implies k_1 = 14\ 12\ 3F\ 30\ 1B\ 29\ 1F\ 0C$
$k_0 = 17\ 00\ 21\ 30\ 15\ 18\ 3D\ 0F \implies k_1 = 14\ 12\ 3F\ 30\ 1B\ 29\ 1F\ 0C$

Validation

- Step 2 does not yield a unique result
- Solutions
  - Perform step1 with more different constants
  - Check if K0 and K1 are compatible with DES key schedule
  - Invert key schedule for each (K0,K1) pair and check resulting DES key with a plaintext / ciphertext pair

$k_0 = 17\ 00\ 21\ 0C\ 15\ 18\ 3D\ 0F \implies k_1 = 14\ 12\ 37\ 30\ 19\ 09\ 1F\ 0C$
$k_0 = 17\ 00\ 21\ 1F\ 15\ 18\ 3D\ 0F \implies k_1 = 14\ 12\ 37\ 30\ 19\ 09\ 1F\ 0C$
$k_0 = 17\ 00\ 21\ 23\ 15\ 18\ 3D\ 0F \implies k_1 = 14\ 12\ 3F\ 30\ 1B\ 29\ 1F\ 0C$
$k_0 = 17\ 00\ 21\ 30\ 15\ 18\ 3D\ 0F \implies k_1 = 14\ 12\ 3F\ 30\ 1B\ 29\ 1F\ 0C$

- DES key 3B 38 98 37 15 20 F7 5E

Discussion

- Distance leakage: hardware implementation leaks HD(L2,L3)
  - No problem
- Optimization: how to choose input differences to minimize key candidates after step 2
  - All first round S-boxes should be active (non-zero difference)
- How many different inputs do we need?
  - For just two, we get < 2^{28} keys after step 2
  - Can be filtered with consistency check / brute force
- Influence of the key schedule
  - DES round keys K0 and K1 are strongly correlated
  - We did not exploit this fact → attack applies to any key schedule
  - If two rounds keys are not sufficient, peel off 2 rounds and proceed

Summary

- A first-order chosen-plaintext DPA attack on the third round of DES
  - Simple
  - Resilient to noise (it is DPA; we do not use collisions)
  - Recovers full DES keys
- Remind once again that outer and inner rounds of Feistel ciphers must be protected

Thank you for your attention