A Cautionary Note: Side-Channel Leakage Implications of Deterministic Signature Schemes

Hermann Seuschek, Johann Heyszl, Fabrizio De Santis

Technische Universität München EISEC
Fraunhofer Institute AISEC

January 20, 2016
Third Workshop on Cryptography and Security in Computing Systems, Prague

Outline

- Motivation and introduction
- Recap: ECDSA digital signatures
- RFC 6979: Principles and side-channel vulnerability
- EdDSA: Principles and side-channel vulnerability
- Side-channel attacks on SHA-2 and SHA-3
- Conclusion and future work

Motivation

- ElGamal-like digital signature schemes (e.g. ECDSA) require a random number for the ephemeral (short-term) key
- Security depends on the quality of this random number
  - Designers are not always aware of this (e.g. PS3 hack in 2010)
  - Embedded systems cannot always guarantee this
- Idea: remove need for high-quality randomness
- Solution: deterministic generation of ephemeral key from message and private key
- Problem: derivation of ephemeral may reveal private key through a side-channel

Recap: ECDSA Digital Signature Generation

Signing message m using private key d where n is the order of the base point P

(a) choose cryptographically secure random $k \in \{1, 2, \dots, n-1\}$

(b) $(x_1, y_1) = k \cdot P$

(c) $r = x_1 \bmod n$, if $r = 0$ go back to (a)

(d) $s = k^{-1} \cdot (\mathrm{H}(m) + d \cdot r) \bmod n$, if $s = 0$ go back to (a)

(e) signature for m is the pair (r, s)

Attacks Exploiting bad Randomness

Trivial case: two signatures (r, s) and (r, s') of different messages m, m' using the same private key (d) and ephemeral key (k)

$$s = k^{-1} \cdot (\mathrm{H}(m) + d \cdot r) \bmod n \tag{1}$$

$$d = \frac{s \cdot k - \mathrm{H}(m)}{r} \bmod n \tag{2}$$

$$s - s' = k^{-1} \cdot (\mathrm{H}(m) - \mathrm{H}(m')) \bmod n \tag{3}$$

$$k = \frac{\mathrm{H}(m) - \mathrm{H}(m')}{s - s'} \bmod n \tag{4}$$

More sophisticated attacks known, e.g. Nguyen and Shparlinsky only require some bits of k [NS03]

RFC6979: Scheme by Thomas Pornin [Por13]

Based on HMAC-DRBG (deterministic random bit generator) [KBC97][BK12]

$$HMAC(K, m) = H\left((K \oplus opad)|H((K \oplus ipad)|m)\right) \tag{5}$$

The first step of the HMAC-DRBG updates K_i in the following way

$$K_1 = HMAC(K_0 = 0, m = (V_0|0x00|d|H(m))) \tag{6}$$

After substitution Equ.6 in Equ.5:

$$K_1 = H\left(opad|\color{red}{H(ipad|V_0|0x00|d|H(m))}\right) \tag{7}$$

Side-Channel Vulnerability of RFC6979

$$\boxed{H(\underbrace{ipad|V_0|0x00|}_{\text{fixed, known}}\overbrace{d}^{\text{fixed, unknown}}\underbrace{|H(m)}_{\text{variable, known}})}$$

Differential side-channel attacks possible!

EdDSA: Scheme by Bernstein et al. [BDL+12]

Signing message m using private key d

(a) The private key is hashed $\mathrm{H}(d) = (h_0, h_1, \ldots, h_{2b-1})$

(b) The first half of the hash value is used to derive $a = 2^{b-2} + \sum_{3 \leq i \leq b-3} 2^i h_i$ and public key $A = a \cdot P$

(c) Deterministic ephemeral key $r = \mathrm{H}(h_b, h_{b+1}, \ldots, h_{2b-1} | m)$

(d) $R = r \cdot P$

(e) $S = (r + \mathrm{H}(R, A, m)a) \bmod n$

(f) The signature for m is the pair (R, S)

Side-Channel Vulnerability of EdDSA

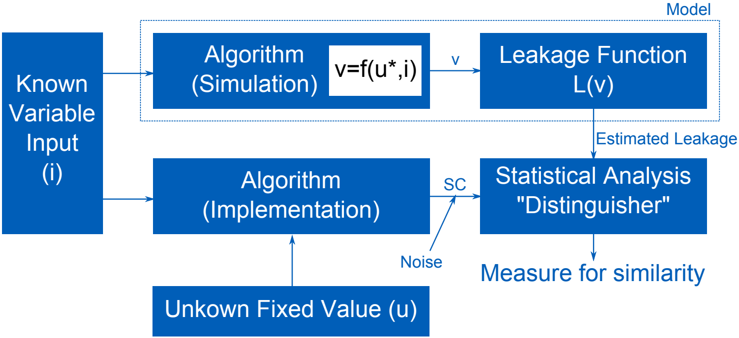
$$\boxed{r = H(\overbrace{h_b, h_{b+1}, \ldots, h_{2b-1}}^{\text{fixed, unknown}} \mid \underbrace{m}_{\text{variable, known}})}$$

Differential side-channel attacks possible!

Long-term key d not directly observable, but r and a are revealed

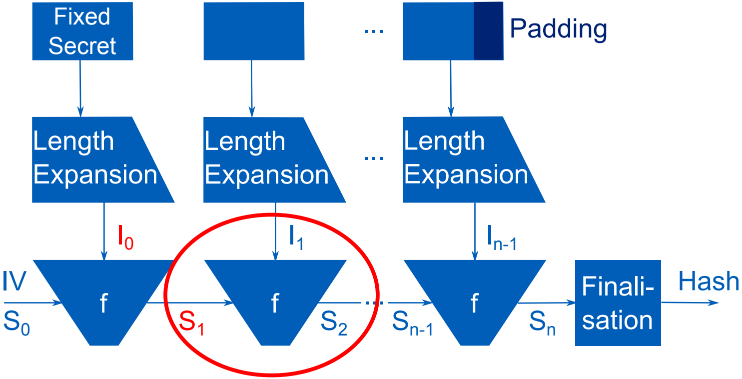
$$S = (r + \mathrm{H}(R, A, m)a) \bmod n \Rightarrow a = \frac{S - r}{\mathrm{H}(R, A, m)} \bmod n$$

Differential Side-Channel Attacks



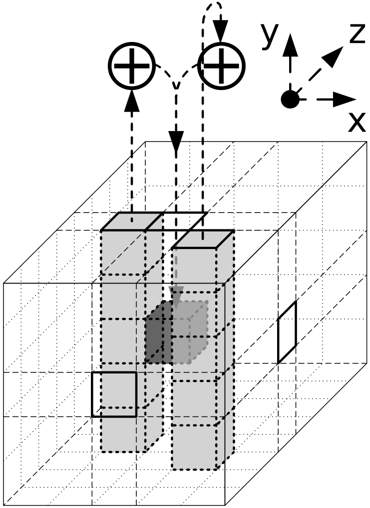
Differential Side-Channel Attacks on SHA-2

- McEvoy et al. [MTMM07] presented a successful side-channel attack on HMAC-SHA-256
- Attack targets the compression function and reveals S_1



Differential Side-Channel Attacks on SHA-3

- 1600 bit state initially zero
- State absorbs block of data
- State XORed with previous one and applied to Keccak function
- Keccak function: 24 rounds of 5 sequential operations
- Attack on θ-operation by Taha et al.[TS13]
- Attack directly reveals secret input



Source: http://keccak.noekeon.org/ (CC BY 3.0)

Conclusion and Future Work

- Deterministic ephemeral keys bear side-channel risks
- System parameters influence the success rate for attacks
- Open Topics:
  - Perform actual attacks
  - Propose countermeasures (which again need randomness!)

Thank You!
Any Questions?

References I

- DanielJ Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang, *High-speed high-security signatures*, no. 2, 77–89.
- Elaine B. Barker and John M. Kelsey, *Sp 800-90a. recommendation for random number generation using deterministic random bit generators*, Tech. report, Gaithersburg, MD, United States, 2012.
- H. Krawczyk, M. Bellare, and R. Canetti, *HMAC: Keyed-Hashing for Message Authentication*, RFC 2104 (Informational), February 1997, Updated by RFC 6151.

References II

- Robert McEvoy, Michael Tunstall, ColinC. Murphy, and WilliamP. Marnane, *Differential power analysis of hmac based on sha-2, and countermeasures*, Information Security Applications (Sehun Kim, Moti Yung, and Hyung-Woo Lee, eds.), Lecture Notes in Computer Science, vol. 4867, Springer Berlin Heidelberg, 2007, pp. 317–332 (English).

- PhongQ. Nguyen and IgorE. Shparlinski, *The insecurity of the elliptic curve digital signature algorithm with partially known nonces*, Designs, Codes and Cryptography **30** (2003), no. 2, 201–217 (English).

- T. Pornin, *Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)*, RFC 6979 (Informational), August 2013.

References III

Mostafa M. I. Taha and Patrick Schaumont, *Side-Channel Analysis of MAC-Keccak*, 2013 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2013, Austin, TX, USA, June 2-3, 2013, 2013, pp. 125–130.