From Gray-box to White-box Cryptography

Aleksei Udovenko

University of Innsbruck, May 17th 2023

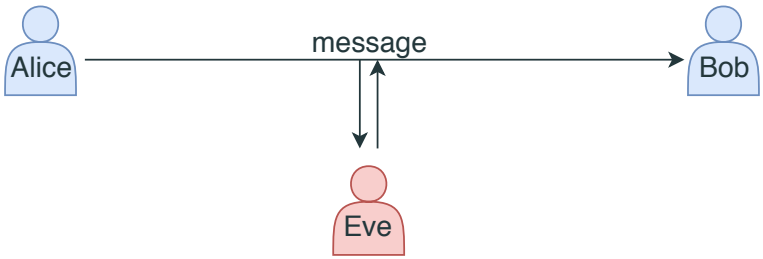
SnT, University of Luxembourg

Outline

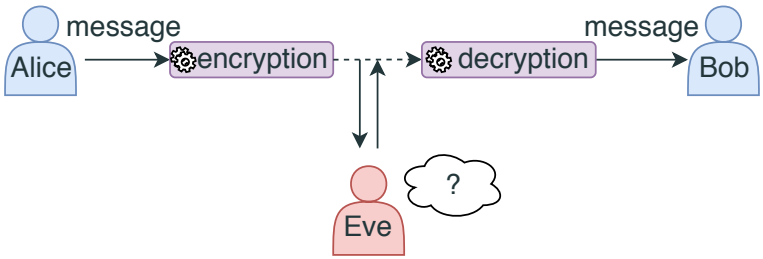
Plan

Symmetric-key Encryption

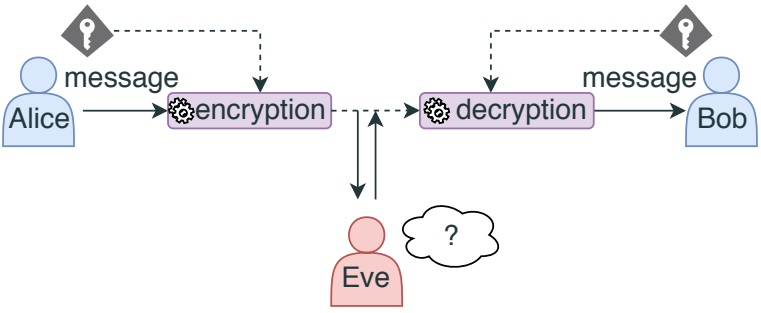
Symmetric-key Encryption



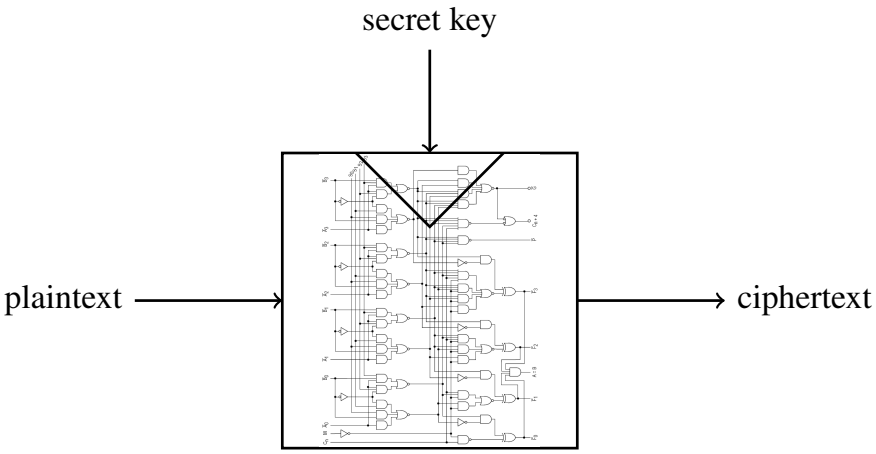
Symmetric-key Encryption



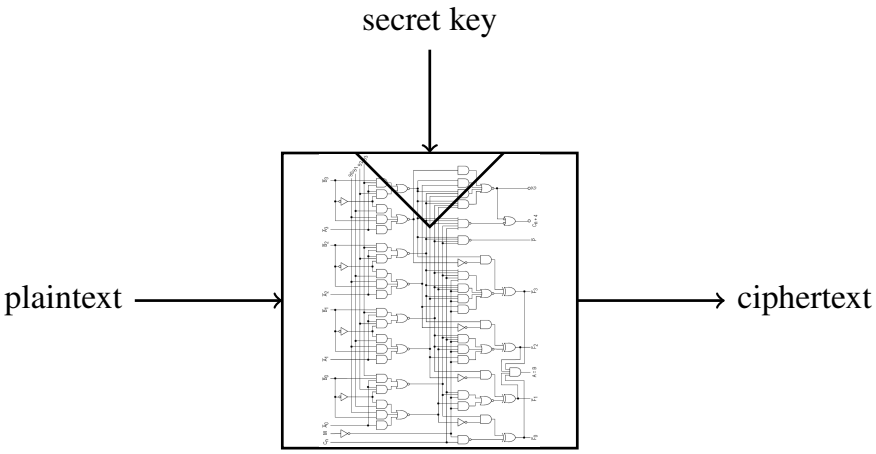
Symmetric-key Encryption



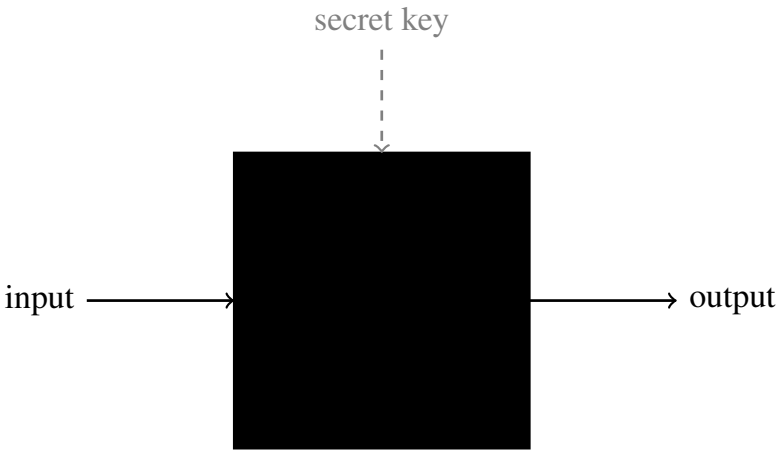
Block Cipher



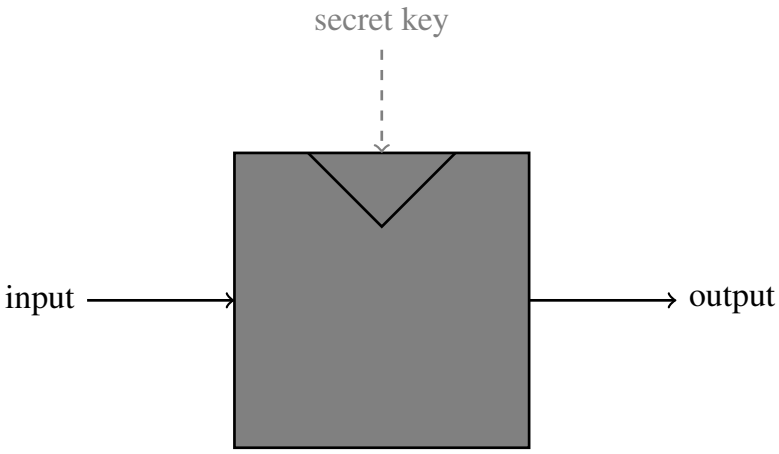
Black-box Model



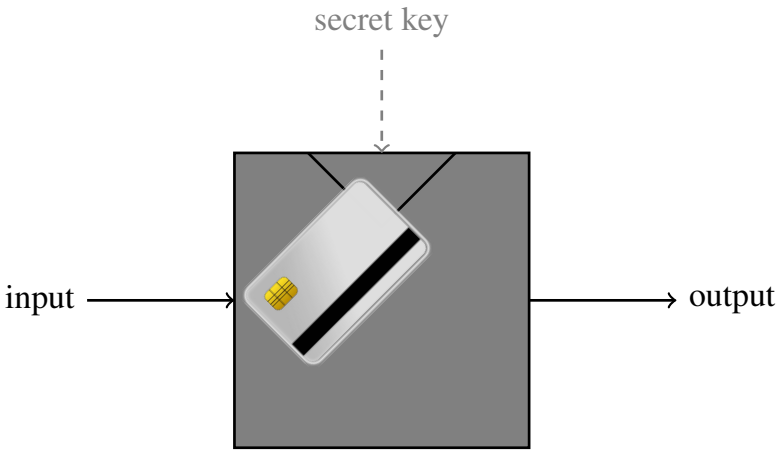
Black-box Model



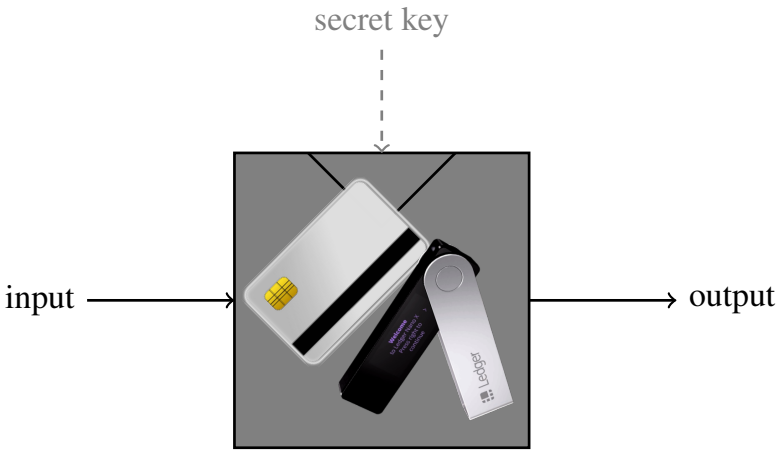
Gray-box Model (Side Channels)



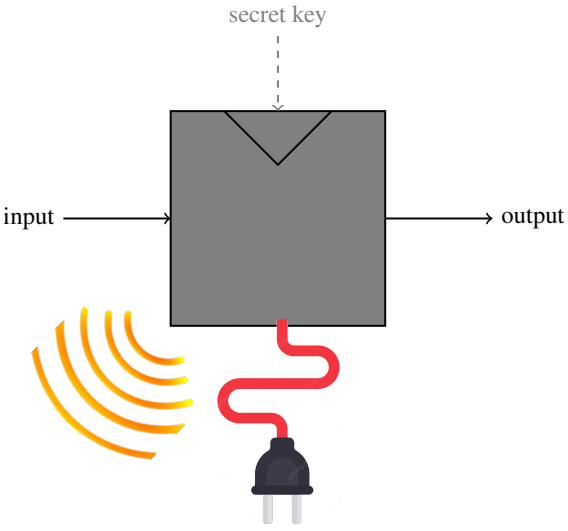
Gray-box Model (Side Channels)



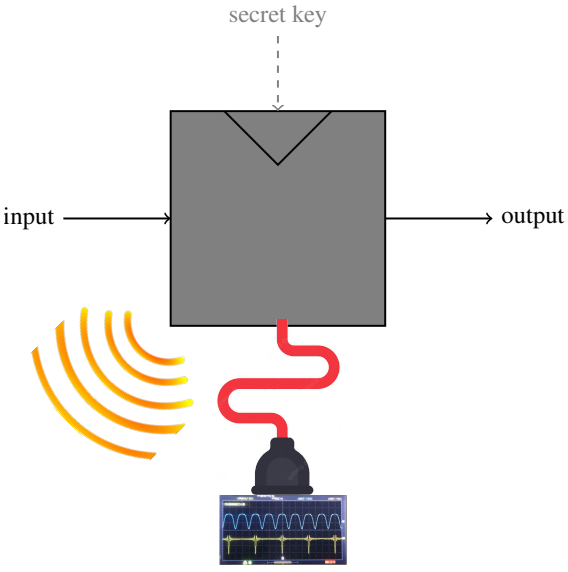
Gray-box Model (Side Channels)



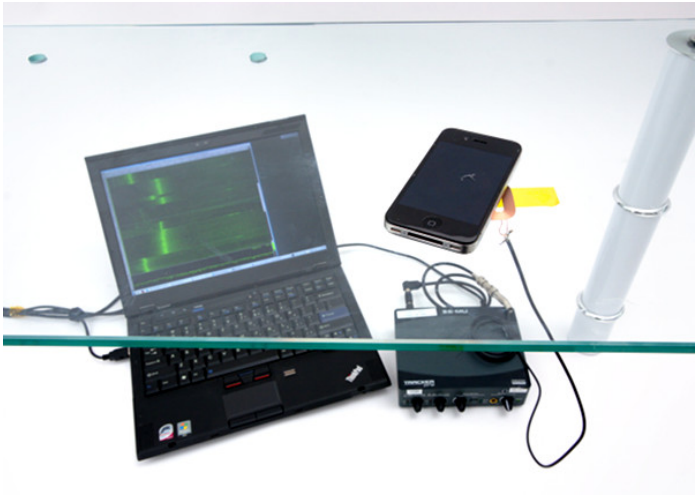
Gray-box Model (Side Channels)



Gray-box Model (Side Channels)

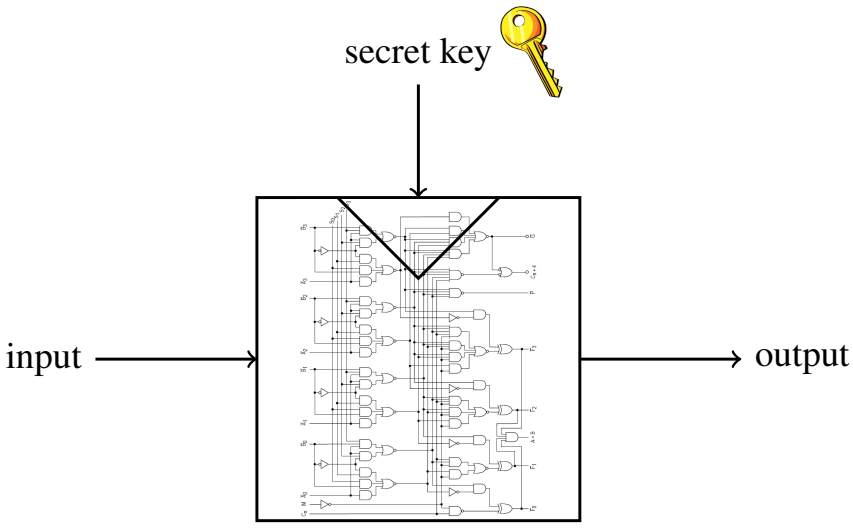


Gray-box Model (Side Channels)

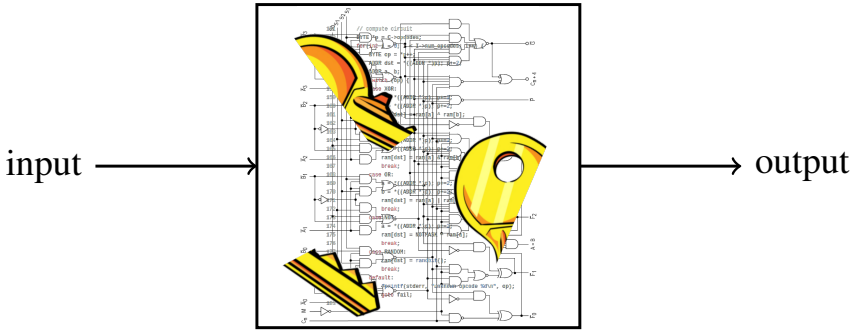


Breaking ECDSA on iPhone 4 using a $2 probe and a sound card. [GPPTY16]

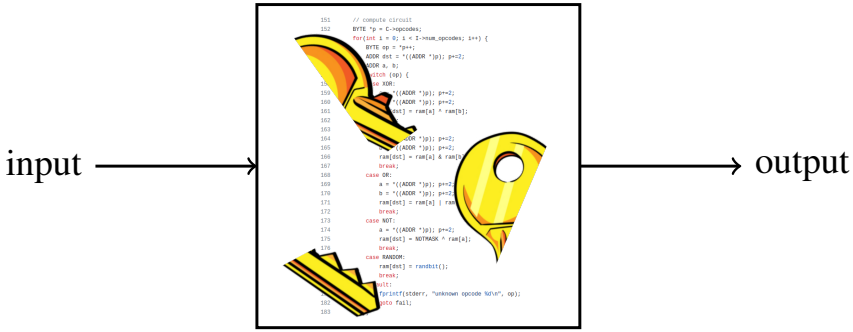
White-box Model [ChoEisJohVOor02]



White-box Model [ChoEisJohVOor02]



White-box Model [ChoEisJohVOor02]



Why White-box Model?

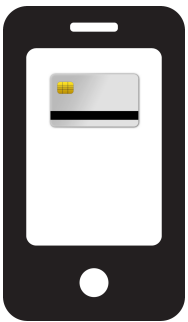
1. [DH76] Public-key encryption (very fast decryption)

Why White-box Model?

1. [DH76] Public-key encryption (very fast decryption)
2. [ChoEisJohVOor02] Digital Rights Management (e.g., Widevine)

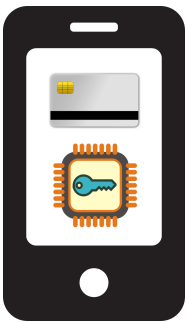
Why White-box Model?

1. [DH76] Public-key encryption (very fast decryption)
2. [ChoEisJohVOor02] Digital Rights Management (e.g., Widevine)
3. Mobile payments (Host Card Emulation)



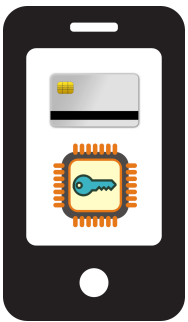
Why White-box Model?

1. [DH76] Public-key encryption (very fast decryption)
2. [ChoEisJohVOor02] Digital Rights Management (e.g., Widevine)
3. Mobile payments (Host Card Emulation)
4. Secure Element emulation in software



Why White-box Model?

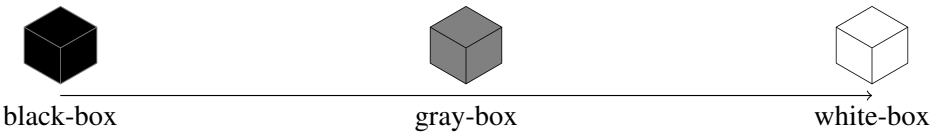
1. [DH76] Public-key encryption (very fast decryption)
2. [ChoEisJohVOor02] Digital Rights Management (e.g., Widevine)
3. Mobile payments (Host Card Emulation)
4. Secure Element emulation in software
5. General cryptographic obfuscation: advanced protocols



White-box History Overview

black-box gray-box white-box

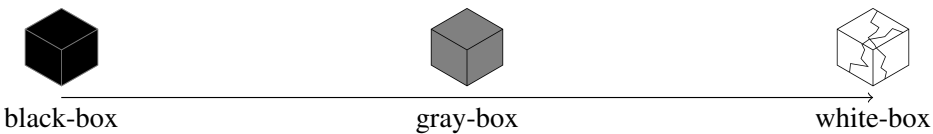
2002 [ChoEisJohVOor02] seminal proposal (table-based)



White-box History Overview

2002 [ChoEisJohVOor02] seminal proposal (table-based)

2004 [BilGilEch04] dedicated practical attack on the CEJVO scheme

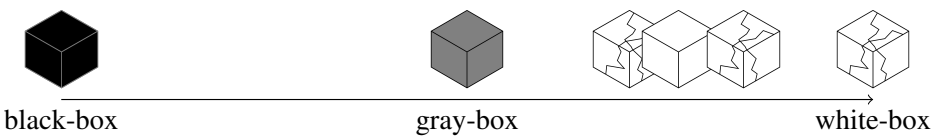


White-box History Overview

2002 [ChoEisJohVOor02] seminal proposal (table-based)

2004 [BilGilEch04] dedicated practical attack on the CEJVO scheme

2004-now dozens of design attempts and attacks, all broken



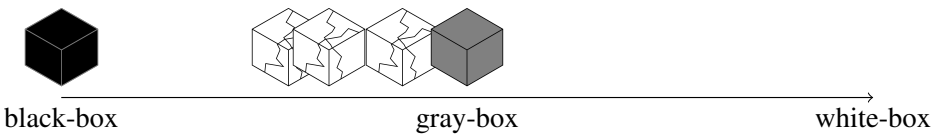
White-box History Overview

2002 [ChoEisJohVOor02] seminal proposal (table-based)

2004 [BilGilEch04] dedicated practical attack on the CEJVO scheme

2004-now dozens of design attempts and attacks, all broken

2015-2016 [SMH15; BHMT16; SMG16]
gray-box attacks break "white-box" designs (correlation, faults)



White-box History Overview

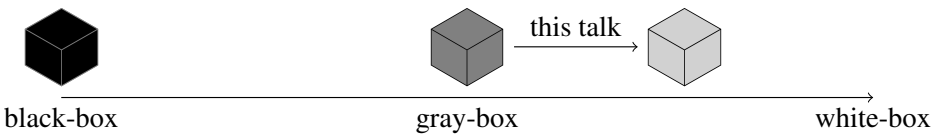
2002 [ChoEisJohVOor02] seminal proposal (table-based)

2004 [BilGilEch04] dedicated practical attack on the CEJVO scheme

2004-now dozens of design attempts and attacks, all broken

2015-2016 [SMH15; BHMT16; SMG16]
gray-box attacks break "white-box" designs (correlation, faults)

2018-2023 [GPRW20; Bir**Udo**18; SEL21; Bir**Udo**21]
algebraic attacks and countermeasures (this talk)



White-box History Overview

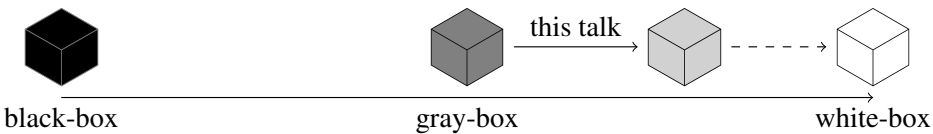
2002 [ChoEisJohVOor02] seminal proposal (table-based)

2004 [BilGilEch04] dedicated practical attack on the CEJVO scheme

2004-now dozens of design attempts and attacks, all broken

2015-2016 [SMH15; BHMT16; SMG16]
gray-box attacks break "white-box" designs (correlation, faults)

2018-2023 [GPRW20; Bir**Udo**18; SEL21; Bir**Udo**21]
algebraic attacks and countermeasures (this talk)



Plan

Differential Power Analysis [KocJafJun99]

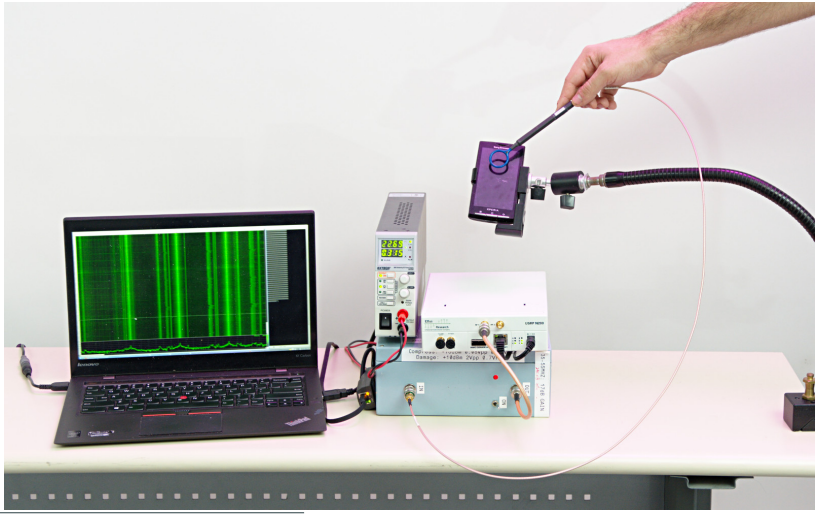
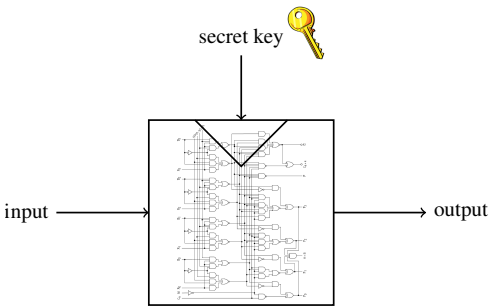
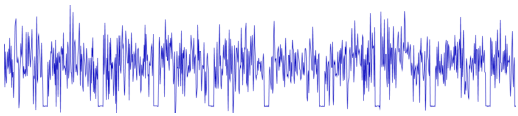


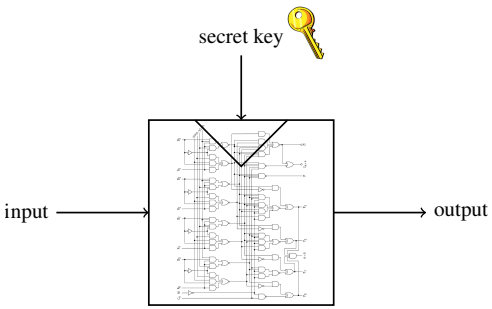
Figure: [GPPTY16] (CCS 2016)

Differential Power Analysis [KocJafJun99]

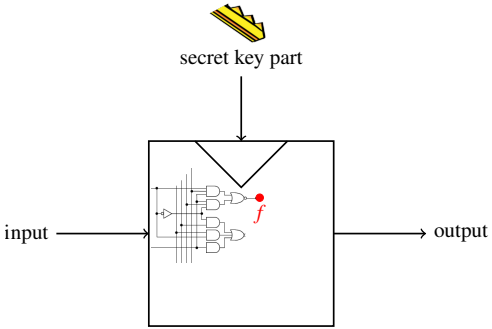


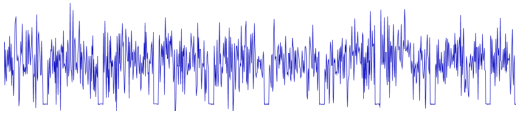


Differential Power Analysis [KocJafJun99]

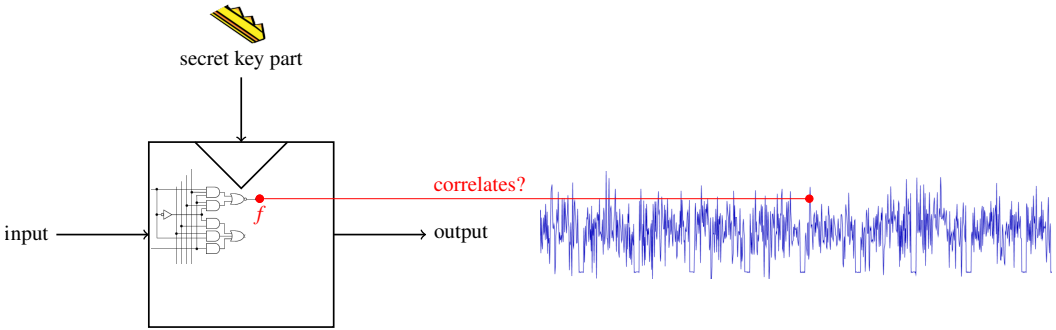


Differential Power Analysis [KocJafJun99]

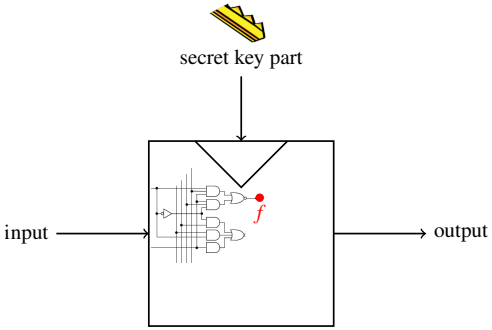




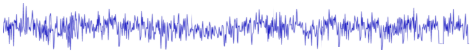
Differential Power Analysis [KocJafJun99]



Differential Power Analysis [KocJafJun99]

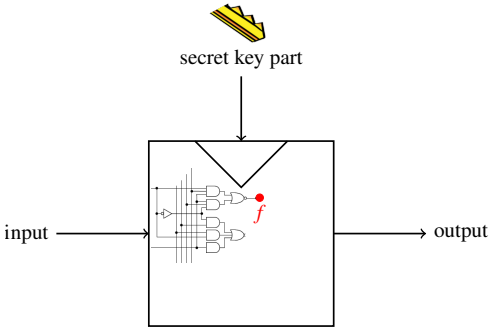


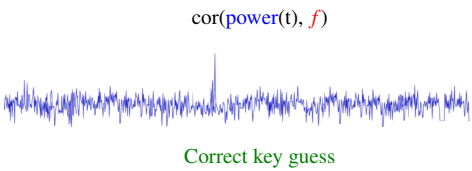
cor(power(t), f)



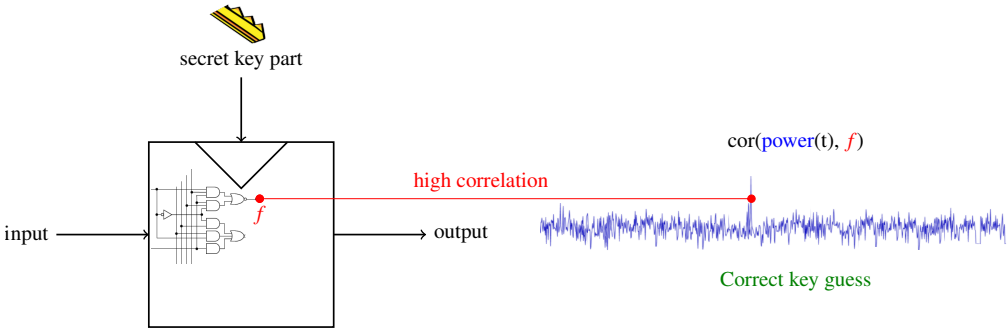
Wrong key guess

Differential Power Analysis [KocJafJun99]





Differential Power Analysis [KocJafJun99]



Countermeasure 1 - Linear Masking [ISW03]

- Based on *Secret Sharing*
- Every intermediate value f is represented as

$$f = x_1 + \ldots + x_n$$

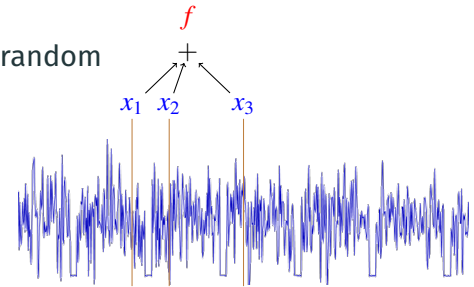
- where $x_1, \ldots, x_{n-1}$ are sampled uniformly at random
- Computations on tuples $(x_1, \ldots, x_n)$

Countermeasure 1 - Linear Masking [ISW03]

- Based on *Secret Sharing*
- Every intermediate value f is represented as

$$f = x_1 + \ldots + x_n$$

- where $x_1, \ldots, x_{n-1}$ are sampled uniformly at random
- Computations on tuples $(x_1, \ldots, x_n)$



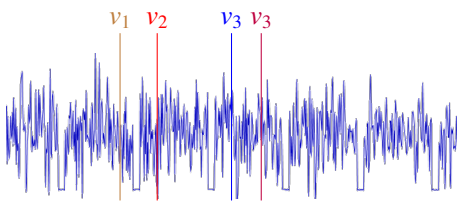
Effect 1: combinatorial explosion in locations

Effect 2: noise amplification

Countermeasure 2 - Shuffling [KocJafJun99; HOM06]

Program:

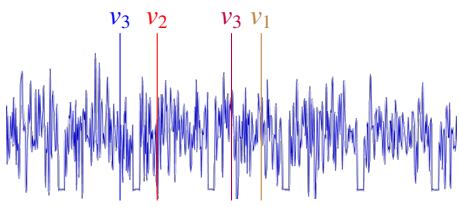
1. Operation 1
2. Operation 2
3. Operation 3
4. Operation 4



Countermeasure 2 - Shuffling [KocJafJun99; HOM06]

Program:

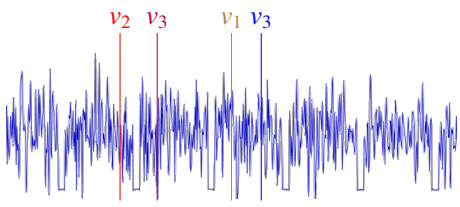
1. Operation 3
2. Operation 2
3. Operation 4
4. Operation 1



Countermeasure 2 - Shuffling [KocJafJun99; HOM06]

Program:

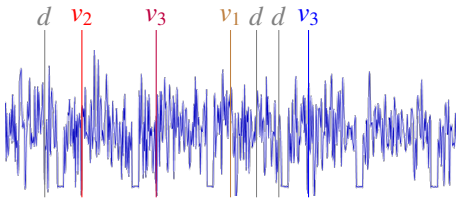
1. Operation 2
2. Operation 4
3. Operation 1
4. Operation 3



Countermeasure 2 - Shuffling [KocJafJun99; HOM06]

Program:

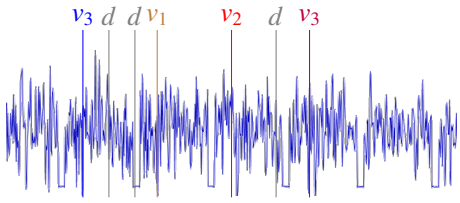
1. Dummy operation
2. Operation 2
3. Operation 4
4. Operation 1
5. Dummy operation
6. Dummy operation
7. Operation 3



Countermeasure 2 - Shuffling [KocJafJun99; HOM06]

Program:

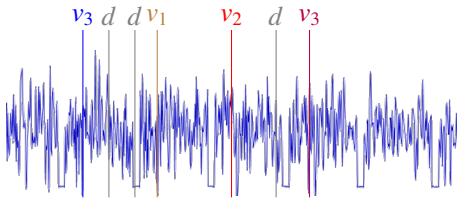
1. Operation 3
2. Dummy operation
3. Dummy operation
4. Operation 1
5. Operation 2
6. Dummy operation
7. Operation 4



Countermeasure 2 - Shuffling [KocJafJun99; HOM06]

Program:

1. Operation 3
2. Dummy operation
3. Dummy operation
4. Operation 1
5. Operation 2
6. Dummy operation
7. Operation 4



- **Effect:** (small) noise amplification (aid masking)

Algebraic Attack

- DPA breaks "White-box" designs [BHMT16]
- Linear masking in white-box?

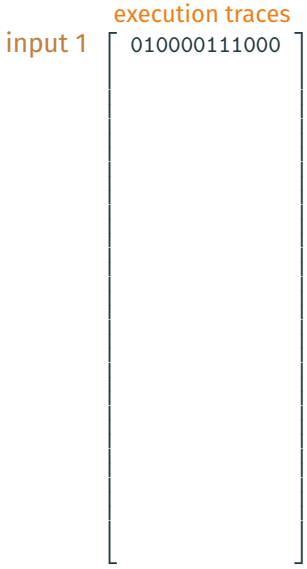
Algebraic Attack

- DPA breaks "White-box" designs [BHMT16]
- Linear masking in white-box?
- Problem: no measurement noise!
- Only *locations* of shares $x_1, \ldots, x_n$ are unknown

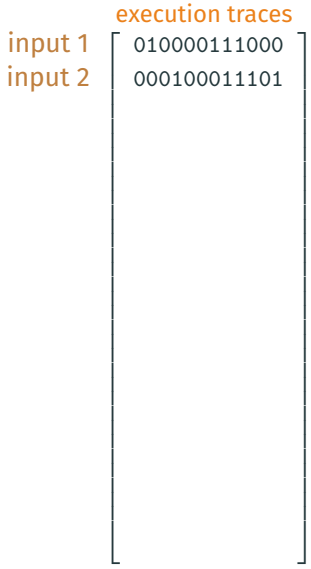
Algebraic Attack

- DPA breaks "White-box" designs [BHMT16]
- Linear masking in white-box?
- Problem: no measurement noise!
- Only *locations* of shares $x_1, \ldots, x_n$ are unknown
- Find them using linear algebra [GPRW20; Bir**Udo**18]

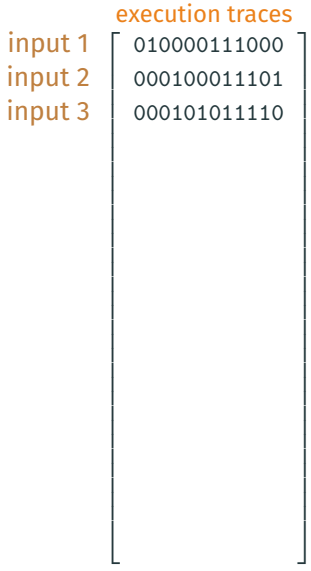
Algebraic attack - Illustration



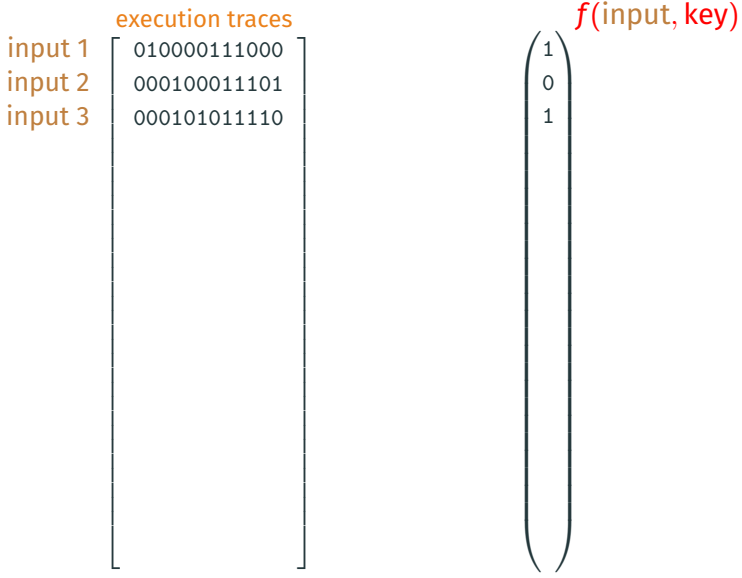
Algebraic attack - Illustration



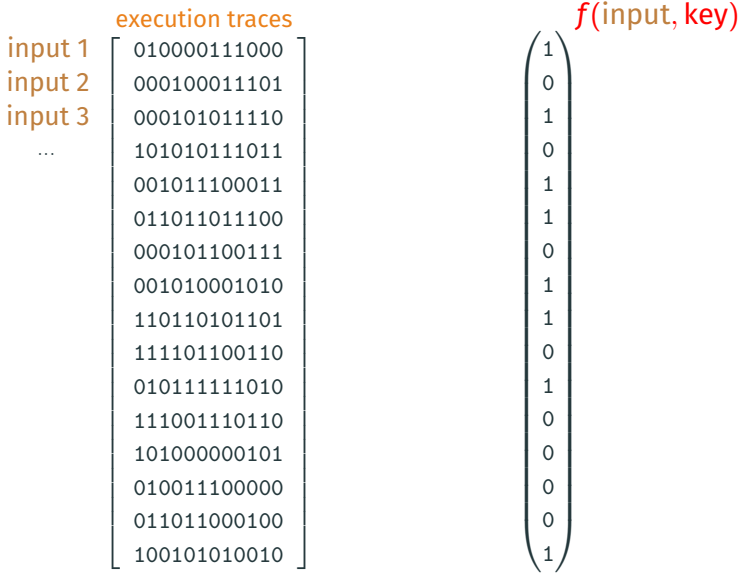
Algebraic attack - Illustration



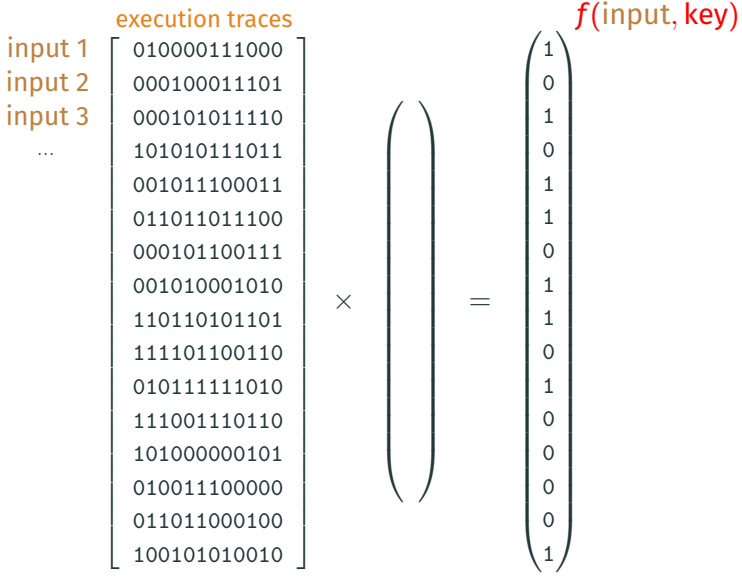
Algebraic attack - Illustration



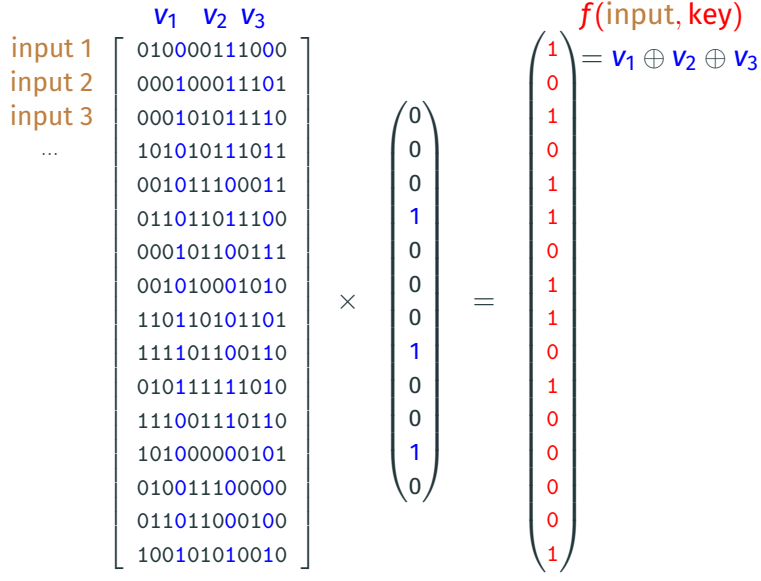
Algebraic attack - Illustration



Algebraic attack - Illustration



Algebraic attack - Illustration



Nonlinear Masking [BirUdo18] (ASIACRYPT 2018)

- First security model against algebraic attacks (gray-box style)
- First nonlinear quadratic scheme:

$$f = ab + c$$

Nonlinear Masking [BirUdo18] (ASIACRYPT 2018)

- First security model against algebraic attacks (gray-box style)
- First nonlinear quadratic scheme:

$$f = ab + c$$

- Security proof
- Generalized and improved in [SEL21]

Nonlinear Masking [BirUdo18] (ASIACRYPT 2018)

- First security model against algebraic attacks (gray-box style)
- First nonlinear quadratic scheme:

$$f = ab + c$$

- Security proof
- Generalized and improved in [SEL21]

Algorithm 3 Minimalist Quadratic Masking Scheme.

function Encode(x, r_a, r_b)
  return $(r_a, r_b, r_a r_b \oplus x)$

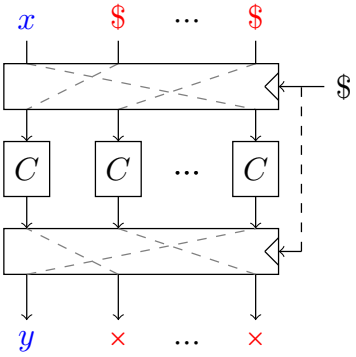
function Decode(a, b, c)
  return $ab \oplus c$

function EvalXOR$((a, b, c), (d, e, f), (r_a, r_b, r_c), (r_d, r_e, r_f))$
  $(a, b, c) \leftarrow$ Refresh$((a, b, c), (r_a, r_b, r_c))$
  $(d, e, f) \leftarrow$ Refresh$((d, e, f), (r_d, r_e, r_f))$
  $x \leftarrow a \oplus d$
  $y \leftarrow b \oplus e$
  $z \leftarrow c \oplus f \oplus ae \oplus bd$
  return (x, y, z)

function EvalAND$((a, b, c), (d, e, f), (r_a, r_b, r_c), (r_d, r_e, r_f))$
  $(a, b, c) \leftarrow$ Refresh$((a, b, c), (r_a, r_b, r_c))$
  $(d, e, f) \leftarrow$ Refresh$((d, e, f), (r_d, r_e, r_f))$
  $m_a \leftarrow bf \oplus r_c e$
  $m_d \leftarrow ce \oplus r_f b$
  $x \leftarrow ae \oplus r_f$
  $y \leftarrow bd \oplus r_c$
  $z \leftarrow am_a \oplus dm_d \oplus r_c r_f \oplus cf$
  return (x, y, z)

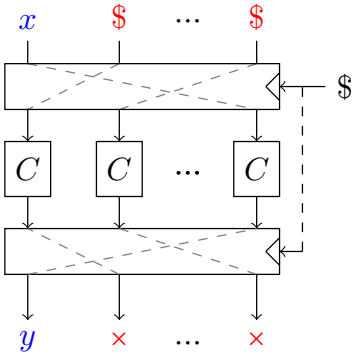
function Refresh$((a, b, c), (r_a, r_b, r_c))$
  $m_a \leftarrow r_a \cdot (b \oplus r_c)$
  $m_b \leftarrow r_b \cdot (a \oplus r_c)$
  $r_c \leftarrow m_a \oplus m_b \oplus (r_a \oplus r_c)(r_b \oplus r_c) \oplus r_c$
  $a \leftarrow a \oplus r_a$
  $b \leftarrow b \oplus r_b$
  $c \leftarrow c \oplus r_c$
  return (a, b, c)

Dummy Shuffling [BirUdo21] (EUROCRYPT 2021)



- Extension of basic shuffling
- Dummy slots are essential!

Dummy Shuffling [BirUdo21] (EUROCRYPT 2021)



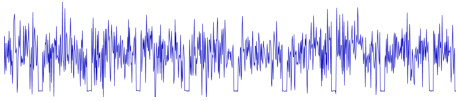
- Extension of basic shuffling
- Dummy slots are essential!

Resulting Protection:

- Very *efficient*
- Any-degree protection
- Provably secure (restricted) (Boolean functions framework)

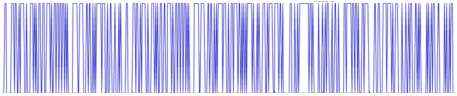
Summary

1. DPA breaks ad-hoc white-box designs



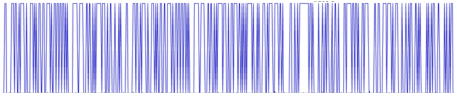
Summary

1. DPA breaks ad-hoc white-box designs



Summary

1. DPA breaks ad-hoc white-box designs

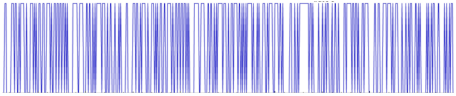


2. Linear masking prevents DPA

$$f = x_1 + \ldots + x_n$$

Summary

1. DPA breaks ad-hoc white-box designs



2. Linear masking prevents DPA

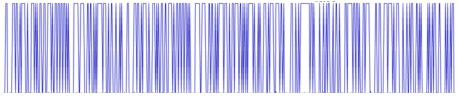
$$f = x_1 + \ldots + x_n$$

3. Algebraic attack breaks linear masking (in white-box)

$$\text{TraceMatrix} \times z = f(\text{input}, \text{key})$$

Summary

1. DPA breaks ad-hoc white-box designs



2. Linear masking prevents DPA

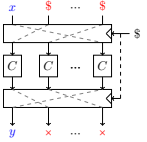
$$f = x_1 + \ldots + x_n$$

3. Algebraic attack breaks linear masking (in white-box)

$$\text{TraceMatrix} \times z = f(\text{input}, \text{key})$$

4. Countermeasures: nonlinear masking and dummy shuffling

$$f = ab + c$$



WhibOx competitions 2017, 2019 (white-box AES implementations)

Pseudonym	Identities	Score
cryptolux	Alex Biryukov, Aleksei Udovenko (University of Luxembourg)	406
grothendieck	Leandro Marin (University of Murcia and Philips)	78
sebastien-riou	Sébastien Riou	66

Pseudonym	Identities	Score
cryptolux	Alex Biryukov, Aleksei Udovenko (University of Luxembourg)	3308.28
white_mountain	*anonymous*	728.22
Mugiwara	Stéphane Cauchie	666.08

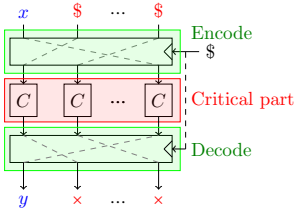
1. (Ongoing) Evaluation of mixed correlation-algebraic attacks (LPN)

$$\text{TraceMatrix} \times z = f(\text{input}, \text{key}) + \text{error}$$

1. (Ongoing) Evaluation of mixed correlation-algebraic attacks (LPN)

$$\text{TraceMatrix} \times z = f(\text{input}, \text{key}) + \text{error}$$

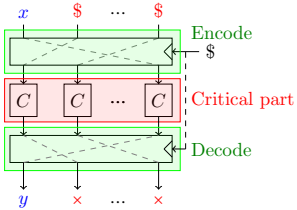
2. Extending algebraic security model to fully white-box (pseudorandomness, encoding and decoding stages)



1. (Ongoing) Evaluation of mixed correlation-algebraic attacks (LPN)

$$\text{TraceMatrix} \times z = f(\text{input}, \text{key}) + \text{error}$$

2. Extending algebraic security model to fully white-box (pseudorandomness, encoding and decoding stages)



3. New nonlinear masking schemes? (degree ≥ 4 is still an open problem)

$$f = abcd + e?$$

Beyond Algebraic Attacks


Fault countermeasures (white-box specifics)


Pseudo-randomness protection


Combination of countermeasures


Structure-hiding methods

Beyond Algebraic Attacks


Fault countermeasures (white-box specifics)


Pseudo-randomness protection


Combination of countermeasures


Structure-hiding methods

Overall strategy: provably-secure components, *small* steps, scientific approach

Conclusions

White-box cryptography: 20-year-old challenging open problem

Should we try to extend the gray-box model first?

References I

[BHMT16] J. W. Bos, C. Hubain, W. Michiels, and P. Teuwen, “Differential computation analysis: Hiding your white-box designs is not enough,” in *CHES 2016*, B. Gierlichs and A. Y. Poschmann, Eds., ser. LNCS, vol. 9813, Springer, Heidelberg, Aug. 2016, pp. 215–236. DOI: 10.1007/978-3-662-53140-2_11 (cit. on pp. 25–31, 49–51).

[BilGilEch04] O. Billet, H. Gilbert, and C. Ech-Chatbi, “Cryptanalysis of a white box AES implementation,” in *SAC 2004*, H. Handschuh and A. Hasan, Eds., ser. LNCS, vol. 3357, Springer, Heidelberg, Aug. 2004, pp. 227–240. DOI: 10.1007/978-3-540-30564-4_16 (cit. on pp. 25–31).

[Bir**Udo**18] A. Biryukov and A. Udovenko, “Attacks and countermeasures for white-box designs,” in *ASIACRYPT 2018, Part II*, T. Peyrin and S. Galbraith, Eds., ser. LNCS, vol. 11273, Springer, Heidelberg, Dec. 2018, pp. 373–402. DOI: 10.1007/978-3-030-03329-3_13 (cit. on pp. 25–31, 49–51, 59–61).

References III

[BirUdo21] A. Biryukov and A. Udovenko, “Dummy shuffling against algebraic attacks in white-box implementations,” in *EUROCRYPT 2021, Part II*, A. Canteaut and F.-X. Standaert, Eds., ser. LNCS, vol. 12697, Springer, Heidelberg, Oct. 2021, pp. 219–248. DOI: 10.1007/978-3-030-77886-6_8 (cit. on pp. 25–31, 62, 63).

[ChoEisJohVOor02] S. Chow, P. A. Eisen, H. Johnson, and P. C. van Oorschot, “A white-box DES implementation for DRM applications,” in *Digital Rights Management Workshop*, ser. Lecture Notes in Computer Science, vol. 2696, Springer, 2002, pp. 1–15 (cit. on pp. 17–31).

[DH76] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976. DOI: 10.1109/TIT.1976.1055638 (cit. on pp. 20–24).

[GPPTY16] D. Genkin, L. Pachmanov, I. Pipman, E. Tromer, and Y. Yarom, “ECDSA key extraction from mobile devices via nonintrusive physical side channels,” in *ACM CCS 2016*, E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi, Eds., ACM Press, Oct. 2016, pp. 1626–1638. DOI: 10.1145/2976749.2978353 (cit. on pp. 16, 33).

[GPRW20] L. Goubin, P. Paillier, M. Rivain, and J. Wang, “How to reveal the secrets of an obscure white-box implementation,” *Journal of Cryptographic Engineering*, vol. 10, no. 1, pp. 49–66, Apr. 2020. DOI: 10.1007/s13389-019-00207-5 (cit. on pp. 25–31, 49–51).

[HOM06] C. Herbst, E. Oswald, and S. Mangard, “An AES smart card implementation resistant to power analysis attacks,” in *ACNS 06*, J. Zhou, M. Yung, and F. Bao, Eds., ser. LNCS, vol. 3989, Springer, Heidelberg, Jun. 2006, pp. 239–252. DOI: 10.1007/11767480_16 (cit. on pp. 43–48).

[ISW03] Y. Ishai, A. Sahai, and D. Wagner, “Private circuits: Securing hardware against probing attacks,” in *CRYPTO 2003*, D. Boneh, Ed., ser. LNCS, vol. 2729, Springer, Heidelberg, Aug. 2003, pp. 463–481. DOI: 10.1007/978-3-540-45146-4_27 (cit. on pp. 41, 42).

[KJJ99] P. C. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in *CRYPTO’99*, M. J. Wiener, Ed., ser. LNCS, vol. 1666, Springer, Heidelberg, Aug. 1999, pp. 388–397. DOI: 10.1007/3-540-48405-1_25.

[KocJafJun99] P. C. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in *CRYPTO’99*, M. J. Wiener, Ed., ser. LNCS, vol. 1666, Springer, Heidelberg, Aug. 1999, pp. 388–397. DOI: 10.1007/3-540-48405-1_25 (cit. on pp. 33–40, 43–48).

[SEL21] O. Seker, T. Eisenbarth, and M. Liskiewicz, “A white-box masking scheme resisting computational and algebraic attacks,” *IACR TCHES*, vol. 2021, no. 2, pp. 61–105, 2021, https://tches.iacr.org/index.php/TCHES/article/view/8788, ISSN: 2569-2925. DOI: 10.46586/tches.v2021.i2.61-105 (cit. on pp. 25–31, 59–61).

[SMG16] P. Sasdrich, A. Moradi, and T. Güneysu, “White-box cryptography in the gray box - - A hardware implementation and its side channels -,” in *FSE 2016*, T. Peyrin, Ed., ser. LNCS, vol. 9783, Springer, Heidelberg, Mar. 2016, pp. 185–203. DOI: 10.1007/978-3-662-52993-5_10 (cit. on pp. 25–31).

[SMH15] E. Sanfelix, C. Mune, and J. de Haas, *Unboxing the white-box. Practical attacks against obfuscated ciphers*, Black Hat Europe 2015, 2015 (cit. on pp. 25–31).

[Whibox2017] E. Prouff *et al.*, *CHES 2017 Capture The Flag Challenge. The WhibOx Contest*, https://whibox-contest.github.io/2017/, 2017 (cit. on p. 69).

[Whibox2019] A. Bogdanov *et al.*, *CHES 2019 Capture The Flag Challenge. The WhibOx Contest, 2nd Edition*, https://whibox-contest.github.io/2019/, 2019 (cit. on p. 69).