Leakage and Tamper Resilient Permutation-Based Cryptography

Christoph Dobraunig[1], Bart Mennink[2], **Robert Primas**[1]

ACM CCS 2022

[1]Graz University of Technology [2]Radboud University Nijmegen

Motivation

- "Black box" model very popular in crypto
  - Attacker knows algorithm but only sees inputs/outputs
  - No information about secret key
  - Attacker cannot observe/influence the internal state
- Clear since 1990's that black boxes are a very optimistic assumption
  - Easy to mount side-channel attacks [Koc96; KJJ99]
  - Easy to mount fault attacks [BDL97; BS97]

Motivation

- “Black box” model very popular in crypto
  - Attacker knows algorithm but only sees inputs/outputs
  - No information about secret key
  - Attacker cannot observe/influence the internal state
- Clear since 1990’s that black boxes are a very optimistic assumption
  - Easy to mount side-channel attacks [Koc96; KJJ99]
  - Easy to mount fault attacks [BDL97; BS97]

Motivation: Cost of Algorithmic Countermeasures

- Combined runtime/area overheads [BBC+20]:
  - Profiled Power Analysis: $1 - 5\times$
  - Differential Power Analysis: $5 - 100\times$
- Especially problematic for embedded devices:
  - Smart cards, root of trust silicon, ...
- Standardization effort by NIST: Lightweight Cryprography (LWC) [NIS18]
  - More performance than AES but same 128-bit security
  - Allow cheaper algorithmic countermeasures
  - Leakage resilience: Prevent physical attacks on mode-level

Motivation: Cost of Algorithmic Countermeasures

- Combined runtime/area overheads [BBC+20]:
  - Profiled Power Analysis: $1 - 5\times$
  - Differential Power Analysis: $5 - 100\times$
- Especially problematic for embedded devices:
  - Smart cards, root of trust silicon, ...
- Standardization effort by NIST: Lightweight Cryprography (LWC) [NIS18]
  - More performance than AES but same 128-bit security
  - Allow cheaper algorithmic countermeasures
  - Leakage resilience: Prevent physical attacks on mode-level

Motivation: Cost of Algorithmic Countermeasures

- Combined runtime/area overheads [BBC+20]:
  - Profiled Power Analysis: $1 - 5\times$
  - Differential Power Analysis: $5 - 100\times$
- Especially problematic for embedded devices:
  - Smart cards, root of trust silicon, . . .
- Standardization effort by NIST: Lightweight Cryprography (LWC) [NIS18]
  - More performance than AES but same 128-bit security
  - Allow cheaper algorithmic countermeasures
  - Leakage resilience: Prevent physical attacks on mode-level

Accumulated Interference

- Previous analysis of LR often in bounded leakage model
  - Adversary can choose any leakage function with bounded range [DP08]
  - Each new primitive call leaks $\leq \lambda$ bits $\rightarrow$ simplification!
  - Fault attacks are not considered
- This work:
  - More practical framework for evaluating leakage resilience
  - Closer fit to actual attacks (observable leakage)
  - Also captures fault attacks

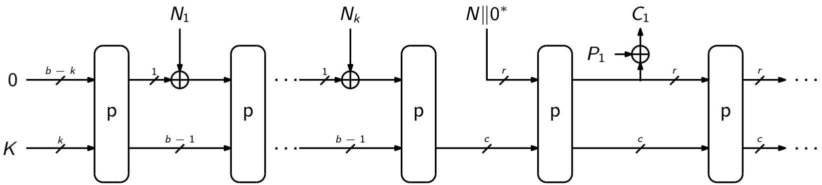
Accumulated Interference

- Previous analysis of LR often in bounded leakage model
  - Adversary can choose any leakage function with bounded range [DP08]
  - Each new primitive call leaks $\leq \lambda$ bits $\rightarrow$ simplification!
  - Fault attacks are not considered
- This work:
  - More practical framework for evaluating leakage resilience
  - Closer fit to actual attacks (observable leakage)
  - Also captures fault attacks

Accumulated Interference

- Accumulated gain (AG) represents leakage and tampering
- We bound leakage as the AG over time: $\mathrm{AG}(i)$
  - More accurate bounds on $\mathrm{AG}(i)$ derived through measurements
- Suited for permutation-based cryptography
  - Discussion example: Asakey
  - Direct implications for the NIST LWC finalist Isap [DEM+20]

Asakey: Nonce-based Stream Encryption

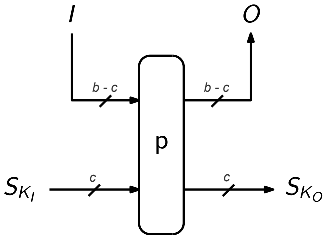


- Asakey ≈ encryption part of Isap [DEM+20]
- Nonce is absorbed bit by bit
  - Sponge-variant of GGM construction [GGM86]
  - Attacker observes at most 2 different inputs under same key

Accumulated Interference

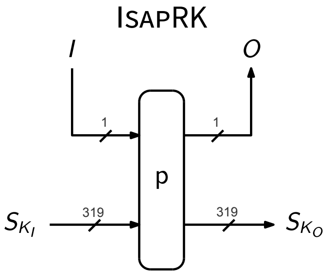
$$\mathbf{Adv}^{\text{i-ai}}_{\textsc{Asakey}}(\mathsf{A}) \le \sum_{i=1}^{p} \left(\frac{1}{2^{k-\tau-\mathrm{AG}(i)}} + \frac{\nu^{Q-q}_{r-\tau,c-\tau} + 1}{2^{c-\tau-\mathrm{AG}(i)}} + \frac{Q + 2qk + 1}{2^{b-\tau-\mathrm{AG}(i)}} \right) + \frac{(Q+2qk)q + 2\nu^{Q-q}_{r-\tau,c-\tau}}{2^{c-\tau}} + \frac{\binom{Q+2qk+1}{2} + 2\binom{Q+qk+1+p}{2}}{2^{b-\tau}}$$

Accumulated Interference: Estimating $\mathrm{AG}_{\mathtt{ATK}}(\boldsymbol{X}, \boldsymbol{q}, r)$



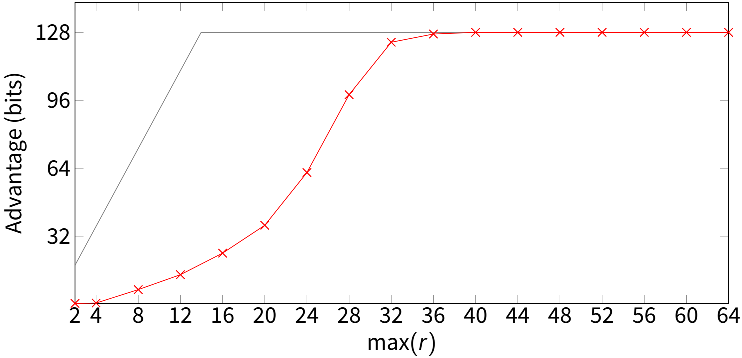
- $\mathrm{AG}_{\mathtt{ATK}}(\boldsymbol{X}, \boldsymbol{q}, r)$
  - $\mathtt{ATK} \in \{\mathtt{SPA}, \mathtt{DPA}, \mathtt{SFA}, \ldots\}$
  - $\boldsymbol{X}$ inputs to p
  - $\boldsymbol{q}$ evaluations of p per input
  - r maximal number of X_i with the same inner part

Accumulated Interference: Estimating $\mathrm{AG}_{\texttt{ATK}}(\boldsymbol{X}, \boldsymbol{q}, r)$



- $\mathrm{AG}_{\texttt{ATK}}(\boldsymbol{X}, \boldsymbol{q}, r)$
  - $\texttt{ATK} \in \{\texttt{SPA}, \texttt{DPA}, \texttt{SFA}, \ldots\}$
  - $\boldsymbol{X}$ inputs to p
  - $\boldsymbol{q}$ evaluations of p per input
  - r maximal number of X_i with the same inner part

Accumulated Interference: Estimating $\mathrm{AG}_{\mathtt{DPA}}(\boldsymbol{X}, \boldsymbol{q}, r)$



Evaluation Setup: Chipwhisperer-Lite with XMEGA128D4 target

Implications for AsaKey

- Importance of construction is to bound r and $\max(\boldsymbol{q})$
- AsaKey only bounds $r = 2$
  - Helps against attacks like DPA, SFA, SIFA, …
- $\max(\boldsymbol{q})$ unbounded
  - DFA still possible
- In the paper: Strengthened AsaKey
  - Bounds $\max(\boldsymbol{q})$ to a small constant
  - Stateful scheme that steadily increases the nonce
  - Stores intermediate states during nonce absorption

Conclusion

- More realistic framework to model side-channel and fault attacks for LR crypto
- Introduced (strengthened) ASAKEY as a discussion example
- Discussion of attacks like DPA, DFA, SFA, SIFA, …
- Open: Better construction to bound $\max(\boldsymbol{q})$?

Questions

Bibliography I

[BBC+20] Davide Bellizia, Olivier Bronchain, Gaëtan Cassiers, Vincent Grosso, Chun Guo, Charles Momin, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. **Mode-Level vs. Implementation-Level Physical Security in Symmetric Cryptography - A Practical Guide Through the Leakage-Resistance Jungle**. CRYPTO (1). Vol. 12170. Lecture Notes in Computer Science. Springer, 2020, pp. 369–400.

[BDL97] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. **On the Importance of Checking Cryptographic Protocols for Faults (Extended Abstract)**. EUROCRYPT '97. Vol. 1233. LNCS. Springer, 1997, pp. 37–51. DOI: 10.1007/3-540-69053-0_4. URL: https://doi.org/10.1007/3-540-69053-0%5C_4.

[BS97] Eli Biham and Adi Shamir. **Differential Fault Analysis of Secret Key Cryptosystems**. Advances in Cryptology – CRYPTO '97. Vol. 1294. LNCS. Springer, 1997, pp. 513–525. DOI: 10.1007/BFb0052259. URL: https://doi.org/10.1007/BFb0052259.

Bibliography II

[DEM+20] Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, Bart Mennink, Robert Primas, and Thomas Unterluggauer. **Isap v2.0**. IACR Transactions on Symmetric Cryptology 2020.S1 (2020), pp. 390–416. URL: https://doi.org/10.13154/tosc.v2020.iS1.390-416.

[DP08] Stefan Dziembowski and Krzysztof Pietrzak. **Leakage-Resilient Cryptography**. FOCS 2008. IEEE Computer Society, 2008, pp. 293–302. DOI: 10.1109/FOCS.2008.56. URL: https://doi.org/10.1109/FOCS.2008.56.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. **How to construct random functions**. J. ACM 33.4 (1986), pp. 792–807.

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. **Differential Power Analysis**. Advances in Cryptology – CRYPTO '99. Vol. 1666. LNCS. Springer, 1999, pp. 388–397. DOI: 10.1007/3-540-48405-1_25. URL: https://doi.org/10.1007/3-540-48405-1_25.

Bibliography III

[Koc96] Paul C. Kocher. **Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems.** CRYPTO ’96. Vol. 1109. LNCS. Springer, 1996, pp. 104–113. DOI: 10.1007/3-540-68697-5_9. URL: https://doi.org/10.1007/3-540-68697-5%5C_9.

[NIS18] NIST. **Lightweight Cryptography**. https://csrc.nist.gov/Projects/lightweight-cryptography. 2018.