Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices

Dennis R. E. Gnad, Jonas Krautter, Mehdi B. Tahoori
Leaky Noise ???

Noise that leaks information?

Yes, ...
Motivation

Future:
- Everything Mixed-Signal
- Everything Networked / Multi-User

New security threats?

digital circuits affect analog subsystem
Paper at a Glance

- **Goal:** Prove Information Leakage inside Chip: Digital (Attacker) → Analog → Digital (Victim)

- **Method:**
  - Sample ADC during cryptographic algorithm
  - Leakage Assessment + Correlation Power Analysis (CPA)

- **Results:**
  - Most tested platforms leak
  - Successful key recovery with CPA

---

**ADC** = Analog-to-Digital Converter
Outline

- Background & Related Work
- Experimental Setup
- Results
- Conclusion
Outline

- Background & Related Work
- Experimental Setup
- Results
- Conclusion

Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices - CHES 2019
Background: Power Distribution Networks (PDNs)

- Supplies current to all transistors in a chip
- Complex network: Resistors (R), Capacitors (C), Inductors (L)
  - Some *by design*, others unwanted = *parasitic*
- Circuit activity causes voltage fluctuations by current changes \(i(t)\)

\[
V_{\text{noise}} = L \frac{di(t)}{dt} + i(t)R
\]
Detailed Adversarial Model – Possible Attack Vectors

- ADC – or any sensor (e.g. Temperature)
- Logical Isolation: Memory Protection, etc.
- **Victim** leaks information into analog part
  - Affects ADC!

**1. Attacker:** acquires leakage by ADC

**2. Attacker** with remote access to ADC data

"Leaky Noise"
Background: Power Analysis and Leakage Assessment

Power Analysis Side-Channel Attacks (Kocher et al. 1999)
- Secret key recovery by analyzing power measurement traces
- Correlation Power Analysis (CPA), Brier et al. 2004
  - Correlate power measurements with secret key-based hypothesis

Leakage Assessment (Goodwill et al. 2011, Schneider et al. 2015)
- Compare:
  - Set of power traces from random encryptions
  - Set of power traces from fixed (same) encryptions
- Statistical difference indicates leakage, allow attacks

\[
\begin{align*}
&\text{Welch’s } t\text{-test:} \\
&t = \frac{\mu_{\text{random}} - \mu_{\text{fixed}}}{\sqrt{\frac{s^2_{\text{random}}}{n_{\text{random}}} + \frac{s^2_{\text{fixed}}}{n_{\text{fixed}}}}} \\
&|t| > 4.5 \text{ considered sufficient}
\end{align*}
\]
Selected related work

- “Inside Job” (Schellenberg et al. DATE’18), extended by (Zhao et al. S&P’18)
  - CPA inside FPGA or FPGA-SoC
  - Indirect voltage measurement

- “Screaming Channels” (Camurati et al. CCS’18)
  - Mixed-Signal Chip, leak over radio, in proximity
  - Digital $\rightarrow$ Analog $\rightarrow$ Receiver (Attacker)

- “Side-channel leakage across borders” (Schmidt et al. CARDIS’10)
  - Successful power analysis on I/O port pins of various chips

- Here: Digital $\rightarrow$ Analog $\rightarrow$ Digital possible on-chip?
Outline

- Background & Related Work
- Experimental Setup
- Results
- Conclusion
Experimental Setup

Platforms

- Espressif ESP32
  - ESP32-devkitC – Dual-Core Xtensa CPU, Wifi, .. @ 80MHz

- ST Microelectronics STM32
  - L4 IoT Node – Single-Core ARM CPU, Wifi On-Board, .. @ 80MHz
  - F407 Discovery – Single-Core ARM CPU, Ethernet @ 168MHz

Software provided by both vendors:

- mbedTLS – AES and modular exponentiation (used in RSA, ..)
- FreeRTOS
- GCC with standard compiler optimization “-Os”
Experimental Setup

Microcontroller

*Victim Task*

Encryption

*Attacker Task*

Measurement

ADC trace

UART TX

UART RX

{Vdd, GND, N/C}

Workstation

Leakage Assessment

or CPA

ADC trace

Encryption Request

ADC=Analog-to-Digital Converter

Voltage Noise, Crosstalk, .. “Leaky Noise”
Outline

- Background & Related Work
- Experimental Setup
- Results
- Conclusion
Basic Test: Compare ADC with Oscilloscope

- STM32F407 Discovery
- ADC not connected (‘N/C’)
- 1,000 traces
Leakage Assessment Prerequisites

- Modular Exponentiation
- 1,000 traces averaged
- Fixed + Random Encryptions

\[
t = \frac{\mu_{\text{random}} - \mu_{\text{fixed}}}{\sqrt{\frac{s^2_{\text{random}}}{n_{\text{random}}} + \frac{s^2_{\text{fixed}}}{n_{\text{fixed}}}}}
\]

\( t \)-test:
Leakage Assessment Results Summary

- AES: 1,000,000 traces, Modular Exponentiation: 100,000 traces
- ADC not always noisy ($\sigma=0$)
- Most cases with noise leaky, $|t| >> 4.5$

<table>
<thead>
<tr>
<th>Platform</th>
<th>AES-128 (Fast ADC)</th>
<th>Modular Exponentiation (Slow ADC)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Vdd</td>
<td>GND</td>
</tr>
<tr>
<td>ESP32-devkitC</td>
<td>yes</td>
<td>$\sigma=0$</td>
</tr>
<tr>
<td>STM32L4 IoT Node</td>
<td>yes</td>
<td>$\sigma=0$</td>
</tr>
<tr>
<td>2x STM32F407 Discovery</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
Correlation Power Analysis Attack on AES

- STM32F407 Discovery
- CPA:
  - 10 Million traces, simple alignment applied
  - Ciphertext-based
- 1. Default setup: ADC@GND, 168MHz, -Os Optimization
  - Less than 25 ADC samples for full AES
  - 2 secret key bytes recovered with high confidence
- 2. Simplified setup: ADC@Vdd, 56MHz, -O0 Optimization:
  - ~60 samples for full AES
  - 6 secret key bytes recovered with high confidence
Correlation Power Analysis results (best bytes)

- **GND, -Os Optimization**
  - "Hard"

- **Vdd, -O0 Optimization**
  - "Easy"

![Graph showing correlation power analysis results](image)

- Correct key byte correlation
- Incorrect key byte correlations

~ 2 Million Traces

~ 500k Traces
“Leaky Noise” – Conclusion

Data-dependent noise

Attacker can recover the data

Feasible:
- Attacks across security domains in Mixed-Signal Chips
- Remote power analysis attacks

Application developers: Prevent ADC-use during cryptography
SoC integrators: Consider digital noise a security risk
Potentially: Always apply power analysis countermeasures (?!)

Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices - CHES 2019
Thanks for your Attention!

Acknowledgements: Kevin Schäfer from Rutronik & All Reviewers

Questions?
Following: Backup Slides
Tasks Experimental Setup in FreeRTOS

Simplified Flow:

Figure 3: Description of one loop iteration of the two FreeRTOS tasks.
## Experimental Setup – Software Details

<table>
<thead>
<tr>
<th>Platform</th>
<th>Framework</th>
<th>mbedTLS</th>
<th>FreeRTOS</th>
<th>Compiler(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Espressif ESP32-devkitC</td>
<td>ESP-IDF 3.1&lt;sup&gt;1&lt;/sup&gt;</td>
<td>2.12.0</td>
<td>8.2.0 Xtensa Port&lt;sup&gt;2&lt;/sup&gt;</td>
<td>xtensa gcc 5.2.0&lt;sup&gt;3&lt;/sup&gt; esp32ulp 2.28.51&lt;sup&gt;4&lt;/sup&gt;</td>
</tr>
<tr>
<td>ST Microelectronics STM32F407VG Discovery</td>
<td>STM32CubeMX&lt;sup&gt;5&lt;/sup&gt;</td>
<td>4.26.1, 5.0.1</td>
<td>2.6.1</td>
<td>9.0.0</td>
</tr>
<tr>
<td>ST Microelectronics STM32L475 IoT Node</td>
<td>STM32CubeMX&lt;sup&gt;5&lt;/sup&gt;</td>
<td>4.26.1</td>
<td>2.6.1&lt;sup&gt;7&lt;/sup&gt;</td>
<td>9.0.0</td>
</tr>
</tbody>
</table>

---

5. STM32CubeMX Eclipse plug-in [https://www.st.com/en/development-tools/stsw-stm32095.html](https://www.st.com/en/development-tools/stsw-stm32095.html), 4.26.1 was used for leakage assessment, 5.0.1 was used for the CPA attack in Subsection 4.5.
7. For this platform, none was provided in CubeMX, but the version from STM32F407VG worked directly
### Experimental Setup – Sampling Details

Table 1: Overview of the Experiments, repeated for ADC Pin = \{Vdd, GND, N/C\}

<table>
<thead>
<tr>
<th>Platform</th>
<th>Sampling Style</th>
<th>Algorithm</th>
<th>Samplerate / #Samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESP32-devkitC @80MHz</td>
<td>CPU</td>
<td>AES-128</td>
<td>104 kHz / 16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RSA-2048</td>
<td>20.4 kHz / 2600</td>
</tr>
<tr>
<td>STM32L475 IoT Node @80MHz</td>
<td>DMA</td>
<td>AES-128</td>
<td>684 kHz / 64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RSA-2048</td>
<td>40 kHz / 4096</td>
</tr>
<tr>
<td>STM32F407VG Discovery @168MHz</td>
<td>DMA</td>
<td>AES-128</td>
<td>980 kHz / 32</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RSA-2048</td>
<td>88 kHz / 4096</td>
</tr>
</tbody>
</table>
Different ADC sampling styles covering less or more voltage noise in the ADC data. DMA needs to be used for continuous sampling, while CPU-based will always introduce gaps.

Continuous Sampling with ADC-DMA or Oscilloscope:
- Setup → ADC → ADC → ADC → ADC → ADC → ADC → ADC
- DMA → DMA → DMA → DMA → DMA → DMA → DMA

Covered Voltage Noise:

Sampling with CPU-based ADC function calls:
- Setup → ADC → Store → Setup → ADC → Store → Setup

Covered Voltage Noise:

Time
Background: Mixed-Signal and Analog

- Digital & Analog in one chip: Mixed-signal
  - Often shared PDN
  - Well-known: Digital circuits cause noise in analog part
- Analog Components integrated with Digital
  - Analog-to-Digital Converters (ADCs), DACs, …
  - Noise typically analyzed in signal processing terms
    - i.e. not considered data-correlated, security-relevant
Leakage Assessment

- Tries to prove a statistical dependency

Method:
- Acquire two sets of side-channel traces:
  1. Encryption with the same fixed message
  2. Encryption with various random messages
- Pearson’s correlation between the two sets (Welch’s t-test)

Goal:
- Show that it is possible to distinguish them using the side-channel
- If the test succeeds, we can speak of leakage

\[
t = \frac{\mu_{\text{random}} - \mu_{\text{fixed}}}{\sqrt{\frac{s_{\text{random}}^2}{n_{\text{random}}} + \frac{s_{\text{fixed}}^2}{n_{\text{fixed}}}}}
\]
Leakage

- Existing leakage shows that an attack probably exists
- No information on:
  - Easiness/hardness of an attack
  - How the attack can be done (used intermediate values, ..)

Order of Leakage

- Higher-order statistical moments can be used
- Sometimes only leakage in a higher order can be assessed
Formulas Power Analysis and Leakage Assessment

\[ P_{hyp} = HW(SBox^j(K_{hyp} \oplus S_i)) \]

\[ t = \frac{\mu_r - \mu_{fixed}}{\sqrt{\frac{S_r^2}{n_r} + \frac{S_{fixed}^2}{n_{fixed}}}} \]
Leakage Assessment Trace (ADC on GND, STM32F407)

Modular Exp.

AES

Final $|t|$-value after 100000 traces

Leakage threshold $|t| = 4.5$

ADC sample time step

Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices - CHES 2019
All Leakage Assessment Results

Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices - CHES 2019
Leakage Assessment Example

- Modular Exponentiation
- STM32F407 Discovery
- ADC connected to GND
- 1,000 → 100,000 Traces

![Graph showing leakage assessment example]
Correlation Power Analysis (best byte)

- Vdd, -O0 Optimization

“Easy”
Correlation Power Analysis (best byte)

- GND, -Os Optimization

"Hard"