

Differential Power Analysis

Differential power analysis (DPA) [KJJ99], a powerful **physical attack**, can break the security of cryptographic scheme through its implementation.

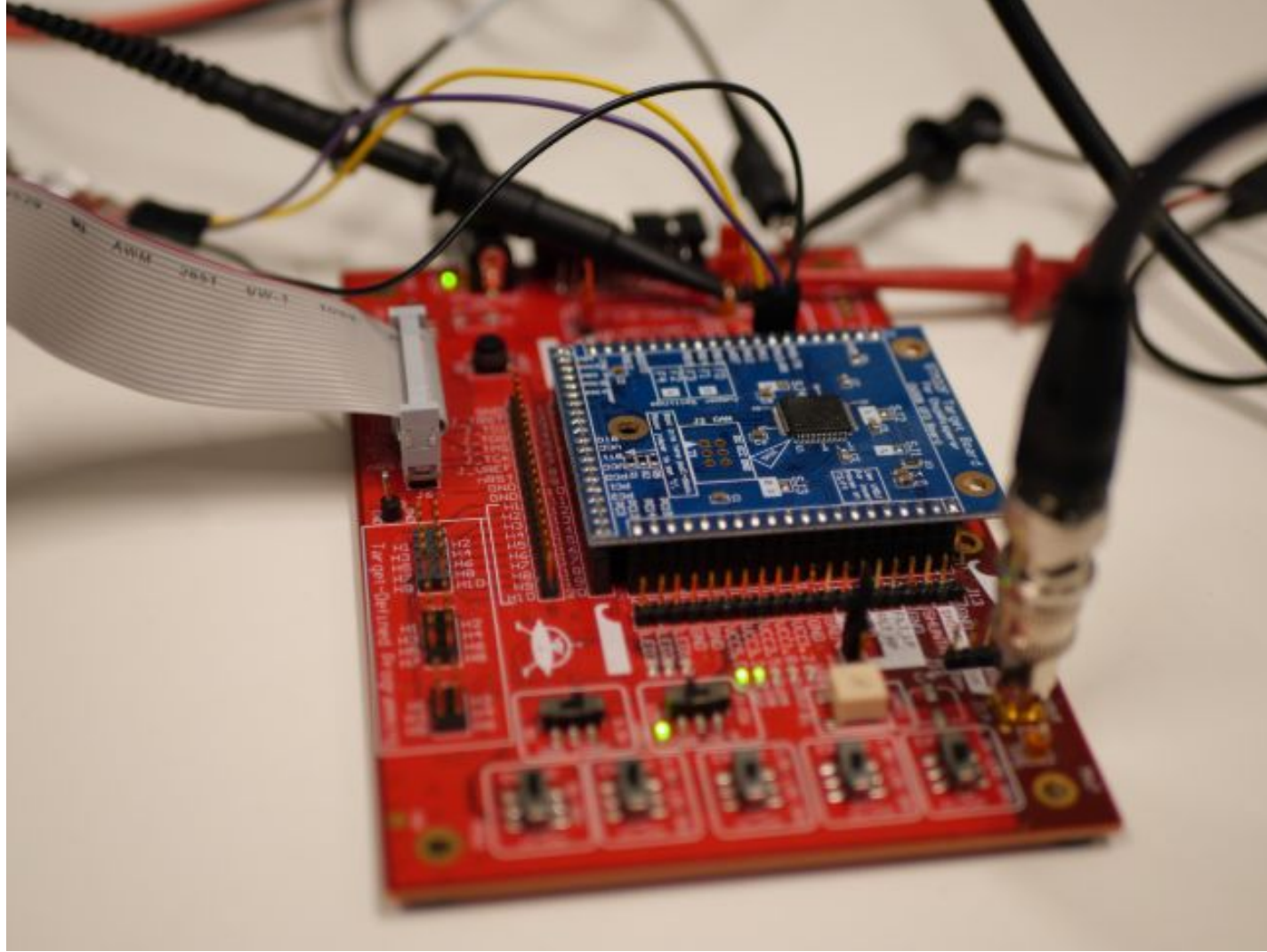
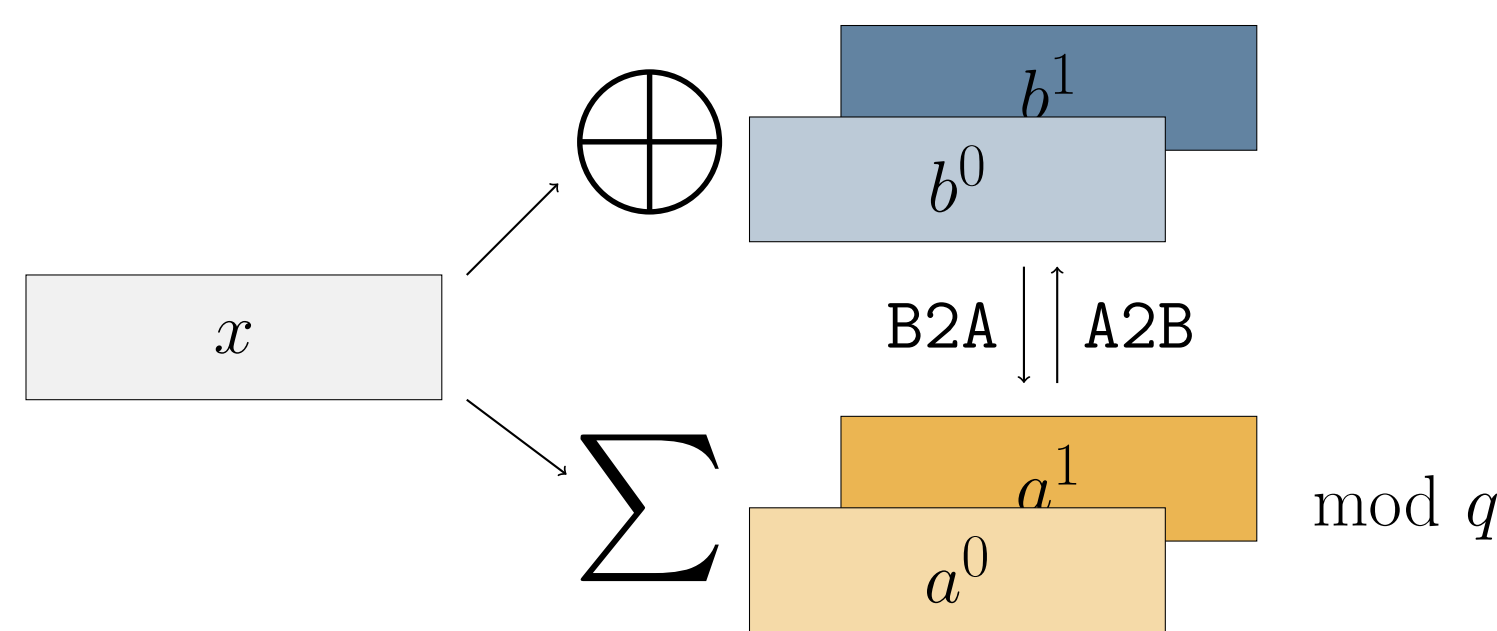


Figure 1. A physical attacker can extract long-term secrets through DPA.

Masking

Dedicated countermeasures, including **masking**, are required but they are **costly** (latency, randomness, memory).



Some schemes require a mix of arithmetic and Boolean masking, and thus *mask conversions*, for example:

- Lattice-based post-quantum cryptography: ML-KEM and ML-DSA
- Hash functions: SHA-1, SHA-2, and BLAKE
- ARX ciphers: SPECK, Salsa20, ChaCha20

A2B and B2A Conversions

Arithmetic-to-Boolean (A2B) and Boolean-to-arithmetic (B2A) conversions are **costly**, and thus a good target for optimization.

- **Boolean circuit-based (BC) techniques**: implement a Boolean circuit using masked gates (e.g., SecAND, SecXOR,...).
- **Table-based (T) techniques**: manipulating tables with pre-computed (intermediate) values.

Table 1. First-order k -bit A2B and B2A conversions.

Method	Type	Cost		
		Computation	Memory	Randomness
A2BGoubin [Gou01]	BC	$\mathcal{O}(k)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$
A2BCorGroVad [CGV14]	BC	$\mathcal{O}(k)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$
A2BCGTV [CGTV15]	BC	$\mathcal{O}(\log k)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$
A2BBroCas [BC22]	BC	$\mathcal{O}(k)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$
A2BCorTch [CT03]	T	$\mathcal{O}(2^k)$	$\mathcal{O}(2^k)$	$\mathcal{O}(1)$
B2AGoubin [Gou01]	BC	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$
B2ACorGroVad [CGV14]	BC	$\mathcal{O}(k)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$
B2ABetCorZei [BCZ18]	BC	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$
B2ASPOG [SPOG19]	BC	$\mathcal{O}(k)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$

Threshold Implementations: AtiB and BtiA

Based on [Pic24], we propose new techniques: **AtiB_s** and **BtiA_s**, where the **share count** s is dependent on the functional degree d° (and thus bit width k) of the TI construction:

- **First-order** A2B and B2A conversions
- **Power-of-two** moduli ($q = 2^k$)
- **No fresh randomness**

Power sets

A critical component of the proposed method is the accumulation of the **power set of shares**. A power set is *the set that contains all subsets of a given set*.

$$\begin{aligned} \mathcal{P}_1 &= \{0\} & \mathcal{P}_2 &= \{0, 1, \{0, 1\}\} \\ \mathcal{P}_3 &= \{0, 1, 2, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\} \end{aligned}$$

Example: given input sharing $x^{(i)}$ with $i \in \{1 \dots s\}$, compute:

$$t = \sum_{i \in \mathcal{P}_3} \left(\bigoplus_{j \in \mathcal{I}} x^{(j)} \right)$$

For $\mathcal{P}_3$, this is:

$$\begin{aligned} t &= x^{(0)} + x^{(1)} + x^{(2)} \\ &+ (x^{(0)} \oplus x^{(1)}) + (x^{(0)} \oplus x^{(2)}) + (x^{(1)} \oplus x^{(2)}) \\ &+ (x^{(0)} \oplus x^{(1)} \oplus x^{(2)}) \end{aligned}$$

Optimized Implementation

The proposed, TI-based methods allow for significant optimizations.

Lazy Modular Reduction

Modular reduction is cheap (power-of-two moduli), and can be delayed until after the accumulation is completed.

Avoid Re-Computation

There are common terms in power set accumulation, re-computation can be avoided. For example: $j = \{0, 1\}$

$$t \leftarrow t + (x^{(0)} \oplus x^{(1)})$$

and $j = \{0, 1, 2\}$:

$$t \leftarrow t + ((x^{(0)} \oplus x^{(1)}) \oplus x^{(2)})$$

Performance Evaluation

We implement the novel methods in C for Arm Cortex-M4 (STM32F407G) and measure **latency** (median of 1000 executions) as number of clock cycles and **randomness** as number of (32 bit) RNG calls.

- **Advantage: randomness cost**. Unlike all other techniques, our TI-based approaches *do not require any fresh randomness*.
- **Disadvantage: latency**. For larger bit widths k , other methods will outperform the TI-based approaches.

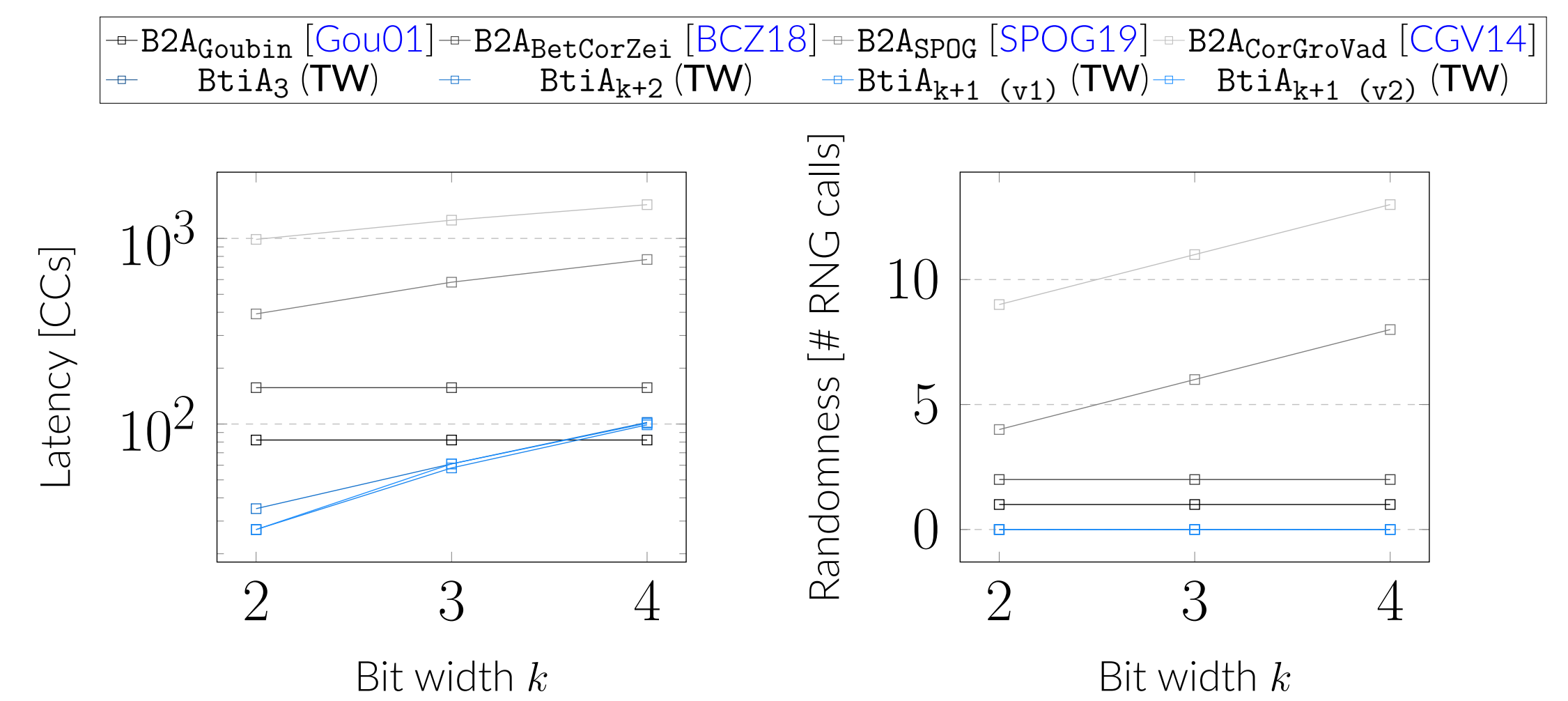


Figure 2. Performance of novel, optimized TI-based B2As (TW) and state-of-the-art gadgets on Arm Cortex-M4.

Core Observation: all **AtiB** and **BtiA** methods can be implemented using **simple arithmetic and bitwise operations** ($\gg, \ll, \&, \oplus, +, -$).

Future Work

TI-based methods for A2B and B2A conversions are proposed, which do not require any randomness and are competitive for small bit widths. To the best of our knowledge, **AtiB** and **BtiA** does not apply to real-world parameter sets (yet). Ongoing and future work includes:

- Extend supported parameter sets
- **Formal** (machine-checked) **verification**
- **Practical security evaluation**

References

- [BC22] Olivier Bronchain and Gaëtan Cassiers. Bitslicing arithmetic/boolean masking conversions for fun and profit with application to lattice-based KEMs. *IACR TCHES*, 2022(4):553–588, 2022.
- [BCZ18] Luk Bettale, Jean-Sébastien Coron, and Rina Zeitoun. Improved high-order conversion from Boolean to arithmetic masking. *IACR TCHES*, 2018(2):22–45, 2018.
- [CGTV15] Jean-Sébastien Coron, Johann Großschädl, Mehdi Tibouchi, and Praveen Kumar Vadnala. Conversion from arithmetic to Boolean masking with logarithmic complexity. In Gregor Leander, editor, *FSE 2015*, volume 9054 of *LNCS*, pages 130–149. Springer, Berlin, Heidelberg, March 2015.
- [CGV14] Jean-Sébastien Coron, Johann Großschädl, and Praveen Kumar Vadnala. Secure conversion between Boolean and arithmetic masking of any order. In Lejla Batina and Matthew Robshaw, editors, *CHES 2014*, volume 8731 of *LNCS*, pages 188–205. Springer, Berlin, Heidelberg, September 2014.
- [CT03] Jean-Sébastien Coron and Alexei Tchulkine. A new algorithm for switching from arithmetic to Boolean masking. In Colin D. Walter, Çetin Kaya Koç, and Christof Paar, editors, *CHES 2003*, volume 2779 of *LNCS*, pages 89–97. Springer, Berlin, Heidelberg, September 2003.
- [Gou01] Louis Goubin. A sound method for switching between Boolean and arithmetic masking. In Çetin Kaya Koç, David Naccache, and Christof Paar, editors, *CHES 2001*, volume 2162 of *LNCS*, pages 3–15. Springer, Berlin, Heidelberg, May 2001.
- [KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 388–397. Springer, Berlin, Heidelberg, August 1999.
- [Pic24] Enrico Piccione. Threshold implementations of cryptographic functions between finite abelian groups. *Cryptology ePrint Archive*, Report 2024/439, 2024.
- [SPOG19] Tobias Schneider, Clara Paglialonga, Tobias Oder, and Tim Güneysu. Efficiently masking binomial sampling at arbitrary orders for lattice-based crypto. In Dongdai Lin and Kazuo Sako, editors, *PKC 2019, Part II*, volume 11443 of *LNCS*, pages 534–564. Springer, Cham, April 2019.

Funding Acknowledgements

