Reducing Risks Through Simplicity

(High Side-channel Security for Lazy Engineers)

Olivier Bronchain Tobias Schneider François-Xavier Standaert

Table of Contents

Motivation

From previous presentation, hard points in masking are:

- **Composability** of gadgets,
- **Quadratic cost** in the number of shares,
- **Leakage independence** is not ensured because of physical effects.

How to get high security ?

Masking a key homomorphic wPRF:

$$< m, k > \oplus \eta = \sum_{i=1}^{d} (< m, k_i > \oplus \eta_i)$$

- **Composability** is trivial with linear refresh,
- **Linear cost** in with d,
- **Leakage indepence** by processing the shares serially.

Learning With Rounding (LWR) wPRF

Main advantages:

- Deterministic noise by using rounding,
- Circuit does not depends on the number of shares,
- Reduced manipulation of a share.

$$\lfloor < m, k > \rfloor = \sum_{i=1}^{d} \lfloor < m, k_i > \rfloor$$

Disadvantages:

- **Cost in** $d \log d$ because of correction factors,
- **Large Key size** which induces a large constant,
- **Hash Function** needed for turn it into a PRF.

Implementation (Global)

The FPGA architecture is composed of:

- **Hash Function**: Keccak
- **PRG**: AES in LR mode or a LFSR, two extreme cases
- **Memory**: to store the key shares and randomness
- **Refresh**: use each time a share is fetched from the memory
- **Scalar Product**: to generate the session key

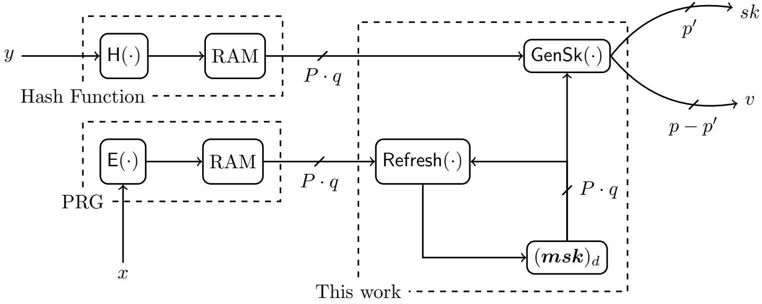


Figure: Re-keying architecture.

Implementation ($\mathsf{GenSk}(\cdot)$)

The main circuit is really simple. The number of parallel multiplication can be tuned to:

- increase the data throughput but large randomness needed per cycle,
- add algorithm noise.

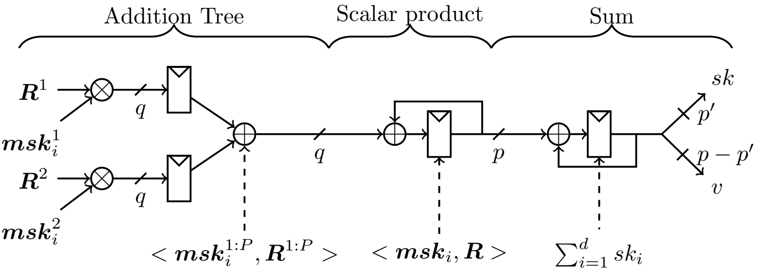


Figure: Circuit for $\mathsf{GenSk}(\cdot)$

AES-DOM

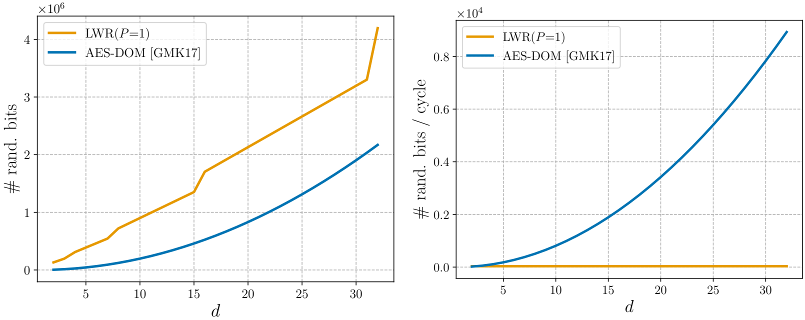
How does it compare with a Block cipher ?

AES-DOM is:

- Open-source protected VDHL,
- Constant number of cycles with d,
- Quadratic cost in area and randomness,
- 8-bits serial bus.

Randomness

- Both implementations need more of less the same amount,
- LWR still requires more randomness for 32 shares,
- but a constant number of random bits per cycle.



(a) Total number of rand. bits. (b) Number of rand. bits per cycle.

Figure: Randomness requirement depending on the masking order d.

The rand. is the bottleneck for both when expensive

Area Cost

LWR becomes rapidly cheaper than AES-DOM.

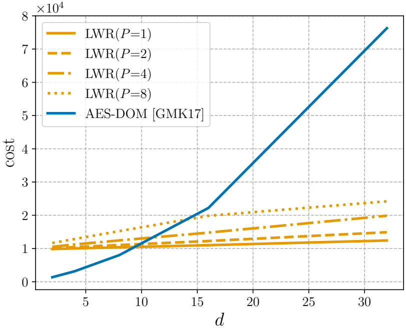
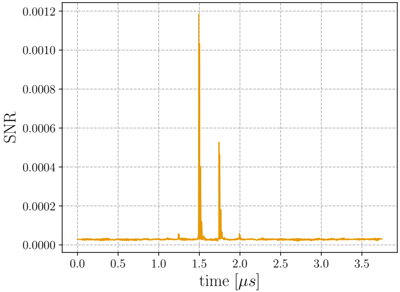


Figure: Influence of the number of share on the cost of the implementation.

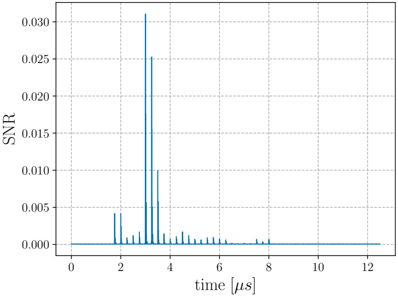
Signal-to-Noise Ratio

SNRs on LWR is:

- is 20 times smaller,
- contained in 2 cycles while 22 in the AES.



(a) LWR: mutliplication output.

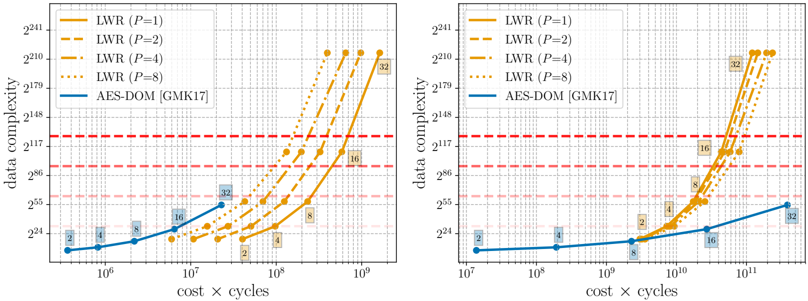


(b) AES-DOM: Sbox output.

Figure: Signal-to-Noise Ratio (SNR).

Conclusion

- Strong randomness, LWR better for high security
- More confidence in leakage independence assumption.



(a) LFSR PRG. (b) LR-PRG.

Figure: cost×cycles metric versus data complexity.

Thanks

(a) Clyde

(b) Shadow

Figure: Spook team