Side channel attack against hardware shuffled AES implemenation

Ghita Harcha,[1]; Vianney Lapôtre[1], ; Cyrille Chavet[1], Philippe Coussy[1]
[1]Lab-STICC (UMR 6285 CNRS)
Université Bretagne Sud

Objective and constraint

- the Advanced Encryption Standard (AES) is a symmetric cryptographic algorithm mathematically secure has been proven to be vulnerable against side channel attack.
- our purpose is to complexity side channel attack for a hardware architecture while maximizing the performance and minimizing the area overhead.

AES Algorithm

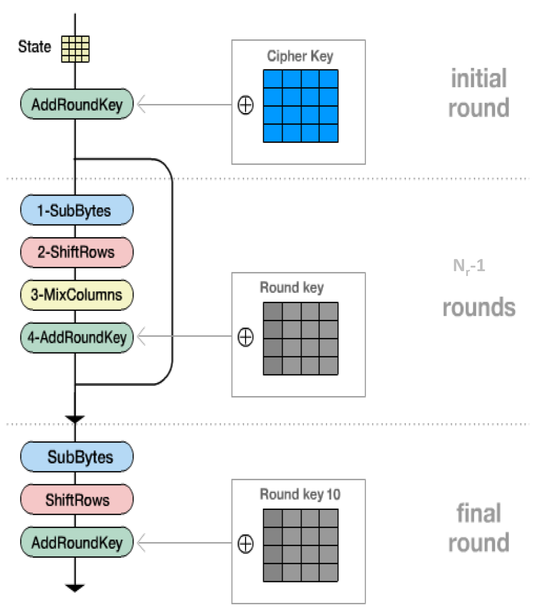

Figure 1. AES Algorithm.

➢AES (Rijndael) cryptographic algorithm established by the U.S. National Institute of Standards and Technology (NIST).
➢The key can be used both of encryption and decryption.
➢The standard AES uses 128-bit message block length (i.e. 16 bytes) and 128-bit key length. 192 and 256-bit key lengths are also supported by AES

Attack/countermeasures

- Power Analysis attack exploits the correlation between the power consumption and the intermediate in the state of the art we can find (Differnatial analysis attack, Template Attack…).
- Several countermeasures have been proposed to secure the AES algorithm in software and hardware implementation and can be divide into two main groups:
  - Hiding: uniformization and randomization of the power consumption.
  - Masking: randomize the intermediate value that is processed.

Our contribution

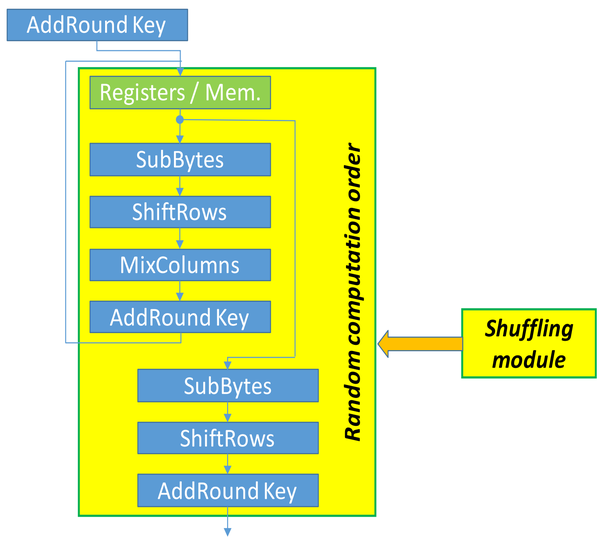

Figure 2. shuffled AES.

➢The architecture of the AES-28 implementation has a 8-bit data path which allow 16! Permutation on the (addroundkey, subyte and the shiftrows) and the first half of the mix column operation (the Galois multiplication)

➢The key scheduling is computed on the fly.

➢The order of computation and storage of the full encryption is random

➢The permutation order is generated by a shuffling module and can be controlled with a TRNG

➢The shuffling module is composed of a 16X16 Benes 16 4-bit register and a wide multiplexer.

Area/performance results comparison

8-bit AES implementation/performance	Unprotected Implementation	Shuffled impelmentation			
	Chu and Benaissa **[1]**	Patranabis S et al XC5VLX50 One round shuffling **[2]**	Patranabis S et al XC5VLX50 two round shuffling **[2]**	Sasdrich P, Güneysu T XC6SLX4 **[3]**	This work XC6SLX4
Clock frequency	73Mhz	82,44Mhz	70,02Mhz	90Mhz	74.025 Mhz
latency	160	n/a	n/a	1471	300
toungput	58.13Mbps	n/a	n/a	7.82Mbps	31,584Mbps
slice	80	403	503	24	176
Slice LUT	n/a	842	1188	94	468
Slice Register	n/a	464	689	29	204

Table 1. result and comparaison.

To estimate the area overhead, we chose a compact AES Implementation [1] and we implemented it on a Spartan-6 then we modified it for shuffling, we shuffled implementation have the smallest latency among shuffled implementation. and the area have an overhead of x2 compared to the unprotected compact AES implementation

Cpa attack against unprotected/protected AES

disabled permutation

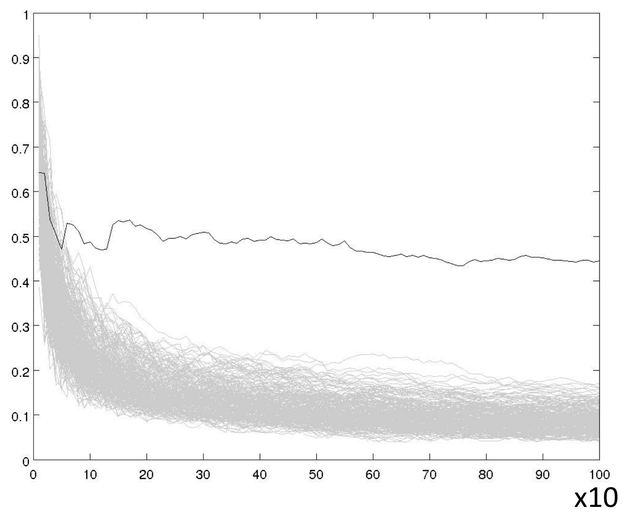

Figure 3. CPA Attack on AES without permutation .

Enabled permutation

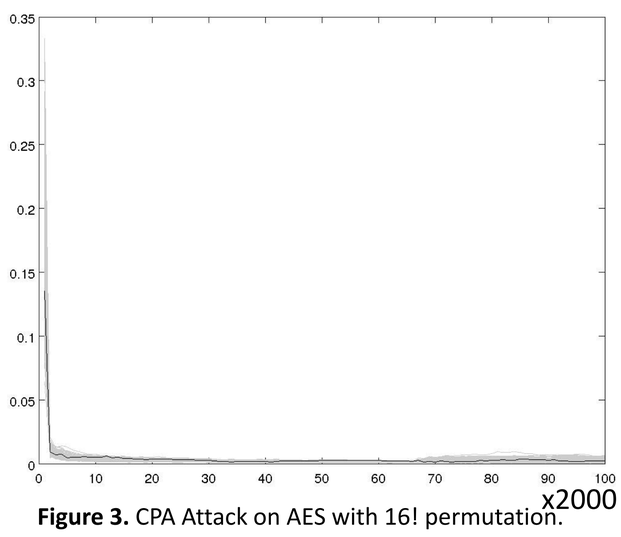

Figure 3. CPA Attack on AES with 16! permutation.

We performed a CPA attack with no permutation with the hamming weight model and all the key byte were recovered with 300 power traces, and by attacking only the 16 points of the spit we managed to recover one byte of the key after 230000 power traces.On [2] CPA attack was performed and the secret key was recovered with a factor of 250.

Conclusion

The shuffled implementation have an area and latency overhead of 2 time the compact implementation [1],compared to related work [3] the latency is lower ,the security is evaluated to have a coefficient of 250.
This work is in progress, until now we have simulated 1300000 power traces and 2 Bytes were recovered the factor is superior to 4000 .
We the hamming weigh model the randomization on storage cannot be evaluated, in the future we will perform CPA attack on measured power traces and perform a TVLA evaluation.

Contact

Harcha Ghita
Lab-STICC (UMR 6285 CNRS)
Email:ghita.harcha@univ-ubs.fr

References

[1] Hamalainen P, Alho T, Hannikainen M, Hamalainen TD. Design and implementation of low-area and low-power AES encryption hardware core. In9th EUROMICRO conference on digital system design (DSD'06) 2006 Aug 30 (pp. 577-583). IEEE
[2] Sasdrich P, Güneysu T. A grain in the silicon: SCA-protected AES in less than 30 slices. In2016 IEEE 27th International Conference on Application-specific Systems, Architectures and Processors (ASAP) 2016 Jul 6 (pp. 25-32). IEEE.
[3] Patranabis S, Roy DB, Vadnala PK, Mukhopadhyay D, Ghosh S. Shuffling across rounds: A lightweight strategy to counter side-channel attacks. In2016 IEEE 34th International Conference on Computer Design (ICCD) 2016 Oct 2 (pp. 440-443). IEEE.