Side Channel Attacks Cryptanalysis Against Block Ciphers Based on FPGA Devices

*Anestis Bechtsoudis , **Nicolas Sklavos

* Computer Engineering and Informatics Department, University of Patras, HELLAS, e-mail : *mpechtsoud@ceid.upatras.gr*
** Informatics & MM Dept., Technological Educational Institute of Patras, HELLAS, e-mail : *nsklavos@ieee.org*

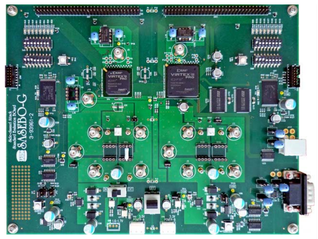
➢ Introduction

✓ Cryptographic primitives' mathematical object has been proved that is secure enough! Does this security level implies also in concrete hardware implementations?

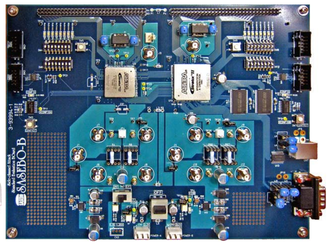
✓ Every hardware implementation of ciphers has additional information leakage (exec. time, consumption, radiation, heat etc), which may lead the attacker to reveal secret parameters of the algorithm.

✓ Reconfigurable hardware (FPGAs) is ideal for evaluation

➢ SASEBO – FPGA Devices

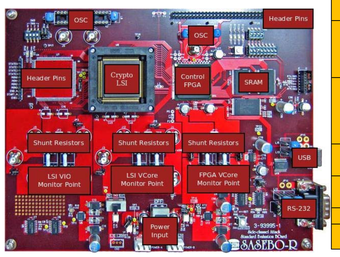


SASEBO – G



SASEBO – B

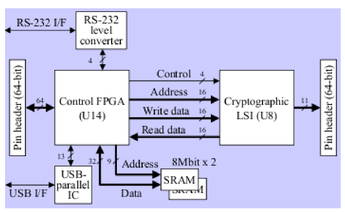
- **Sasebo-R Detail View**



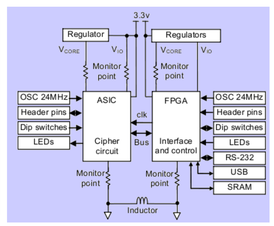
Sasebo-R (Component View)

Size	230 x 180 x 1.6 mm^3 , FR-4, eight layers
Devices	Cryptographic LSI (130nm process, 160-pin QFP)
	Control FPGA (xc2vp30-5FG676C)
Power Supply	Two 3.3V DC power supply lines
	1.2V interntal regulators
	Alternative 1.2V supply line for the LSI
Monitor Points	Shunt resistors inserted at the V_{CORE} , V_{IO} and GND lines
Internal Bus	32-bit bus between the LSI and the FPGA
I/F	USB and RS-232
Clocks	24MHz oscillator for each device

Sasebo-R Basic Features

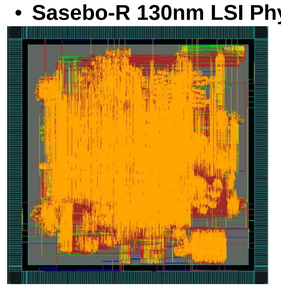


Sasebo-R I/O Signals

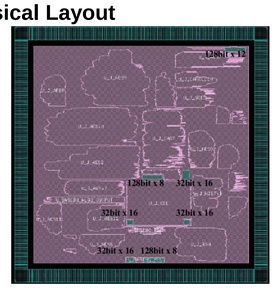


Sasebo-R Block Diagram

- **Sasebo-R 130nm LSI Physical Layout**

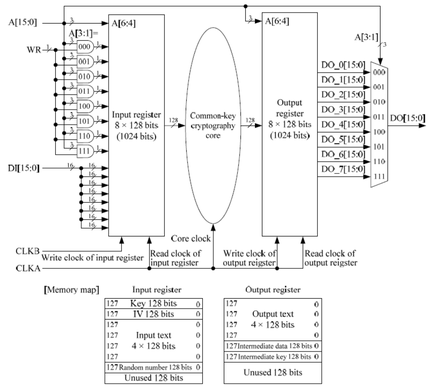


Top View (excl. power lines)

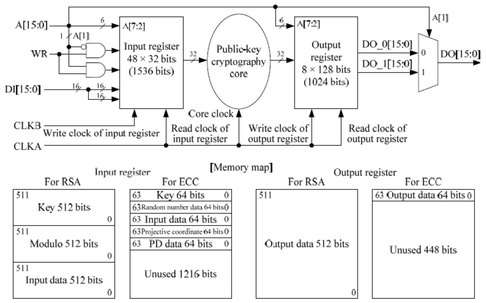


Register Array Allocation

- **Ciphers Implemented in LSI**



Common-Key Cryptographic Algorithms Interface Circuit (AES, DES, Camellia, MISTY1, SEED, CASt128)



Public-Key Cryptographic Algorithms Interface Circuit (RSA, ECC)

- **LSI Main Functionalities:**

✓ Computes the cryptographic algorithms.
✓ Interfaces with control FPGA on SASEBO-R
✓ Generates a trigger signal for sampling information such as power consumption.
✓ Some other special operations for specific AES implementations

➢ Examined Block Ciphers

- *AES (128-bits key length)*
  1. S-Box implemented using composite field (enc./dec.)
  2. S-Box implemented using case statement (enc.)
  3. S-Box implemented using AND-XOR (1-Stage) (enc.)
  4. S-Box implemented using AND-XOR (3-Stage) (enc.)
  5. CTR mode supported – Pipelined
  6. For DPA countermeasure (Masked AND, MDPL, Threshold Implementation, WDDL, Pseudo RSL)
- *DES (enc./dec.)*
- *MISTY1 (enc./dec.)*
- *Camellia (128-bits key length, enc./dec.)*
- *SEED (enc./dec.)*
- *CAST128 (enc./dec.)*

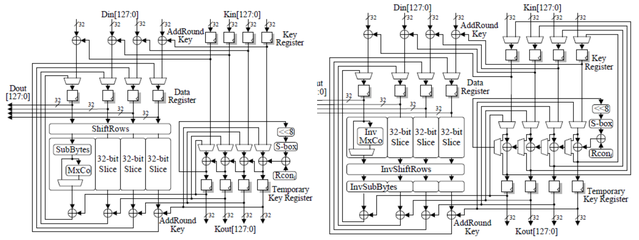
➢ AES Composite Field Implementation

Algorithm	AES
Data Block Length	128 bits
Key Length	128 bits
Functions	Encryption/Decryption
Mode of Operation	Electronic Code Book (ECB)
Description Language	Verilog-HDL
S-Box	Composete Field GF(((2^2)^2)^2) Base
Throughput	128 bits / 10 clocks
Round Key Generation	On-the-fly

AES Macro Overview

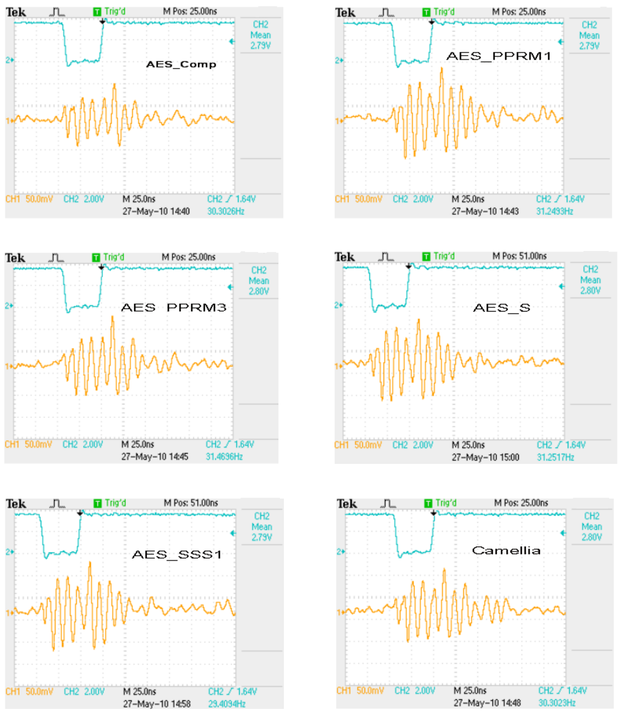
Port Name	Direction	Width	Description
Kin	In	128	Key Input
Din	In	128	Data Input
Dout	Out	128	Data Output
Krdy	In	1	Secret Key is lacthed in internal register
Drdy	In	1	Plaintext latched & enc. process begin
EncDec	In	1	Encr. (EncDec=0) and decr. (EncDec=1)
RSTn	In	1	Reset
EN	In	1	Enable
CLK	In	1	System Clock
BSY	Out	1	Busy status flag
Kvld	Out	1	Round-key generation completed
Dvld	Out	1	Cipher(plain)text ready on data output port

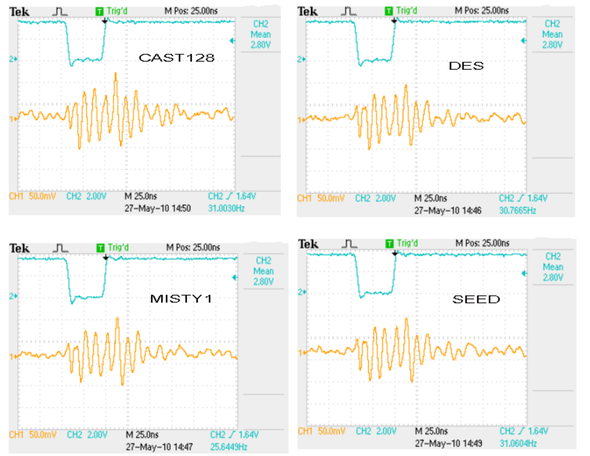
I/O Ports



Encryption Datapath *Decryption Datapath*

➢ Power Analysis of Block Ciphers





✓ The voltage difference across the shunt resistor (in series with power input) divided by the resistance, is the circuit's power consumption.

✓ ***Simple Power Analysis (SPA):***
- Directly interpreting power consumption measurements
- Can yield information about device's operation and key info.
- Easy to prevent (avoid key conditional branching)

✓ ***Differential Power Analysis (DPA):***
- *Statistical analysis and error correction techniques to extract information correlated to secret keys.*
- *Much more powerful attack than SPA*
- *More difficult to prevent*
- *Two phases – Data Collection and Data Analysis*

Attack Method	Description	Attacked Segment
DPA	Analyzes correlation between set of power traces and a particular intermediate 1-bit value corresponding to the guessed partial key	10th round
M-DPA	Examines the correlation between power traces and the Hamming weight of a particular intermediate multi-bit value corresponding to a guessed partial key	10th round
B-DPA	Versatile attack that combines the DPA results for each bit of a particular intermediate multi-bit value corresponding to a guessed partial key	10th round
CPA	Analyzes a correlation between power traces and the Hamming distances of the transitioning of a register that stores a particular intermediate value corresponding to a guessed partial key	Data output
PPA	Extend of CPA with weighing to the Hamming distances	Data output
M2-DPA	Analyzes a correlation between two certain segments in the power traces	10th round
W2-DPA	Computes the difference of the means of power trace squares	10th round

Attack Methods Against AES Circuits

➢ References

[1] P. Kocher, J. Jaffe and B. Jun: "Differential power analysis", CRYPTO 1999.

[2] J. Kesley, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers".

[3] ISO/IEC 18033-3:2005, "Information technology – Security techniques – Encryption Algorithms – Part3: Block ciphers".

[4] S. Mangard, E. Oswald and T. Popp, "Power Analysis Attacks", Springer Science Business Media, LLC, 2007

[5] "Side-channel Attack Standard Evaluation Board (SASEBO)," RCIS, AIST http://www.rcis.aist.go.jp/special/SASEBO/index-en.html

[6] "Cryptographic Hardware Project", Computer Structures Laboratory, Tohoku University. http://www.aoki.ecei.tohoku.ac.jp/crypto/

[7] "Power Analysis Attacks on SASEBO", RCIS, AIST, January 2010