Hamming Distance Power Model Analysis
of AES at Architecture Level

Marek Repka[1], Lubos Gaspar[2], Pavol Zajac[1], and Viktor Fischer[2]

[1]Institute of Computer Science and Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava, Ilkovičova 3, SK-812 19 Bratislava, Slovak Republic.

[2]Laboratoire Hubert Curien, Rue du Prof. Benoit Lauras 18, 42000 Saint-Etienne, France.

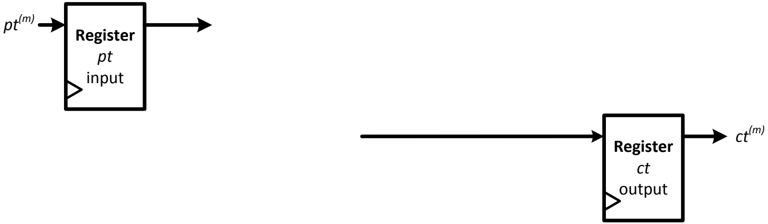
ISCAMI 2012
Session 12
Talk #2 on 13rd May 2012

[1]This work was supported by: National Security Authority of the Slovak Republic, and the grant VEGA 1/0244/09, and the project APVV SK-FR SK-FR-0011-09, and the project FREESIC Grant agreement no: 285205 REA EK.

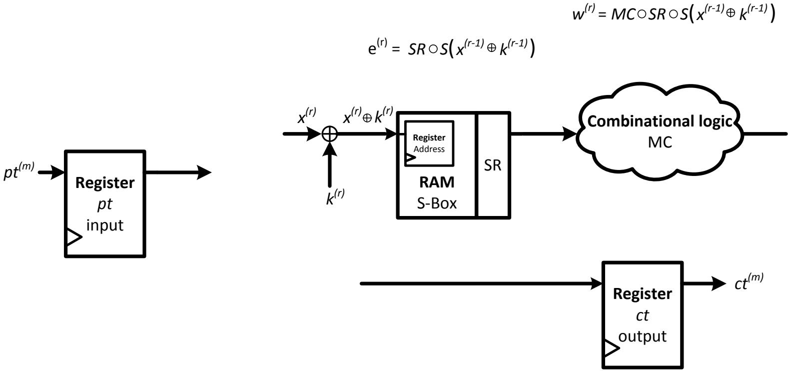
Part I. HD power model analysis with respect to:

1. known data, and
2. architecture design.

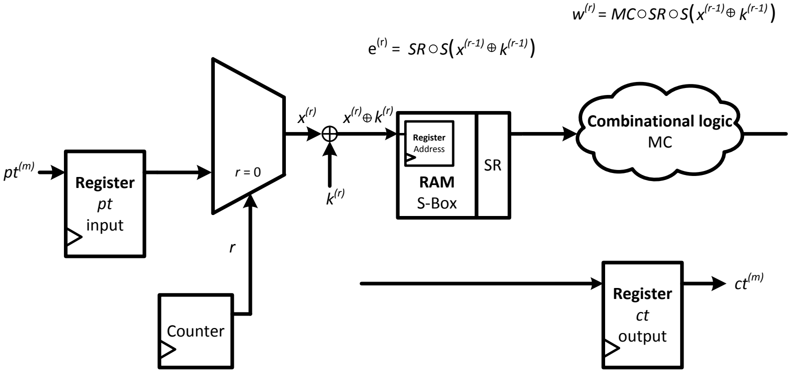
AES Architecture 1



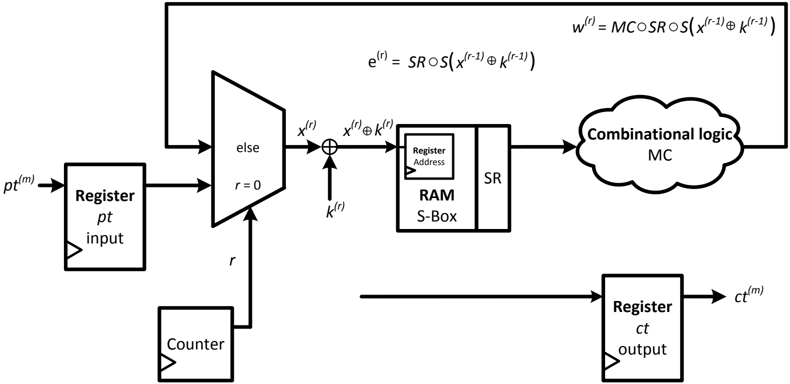
AES Architecture 1



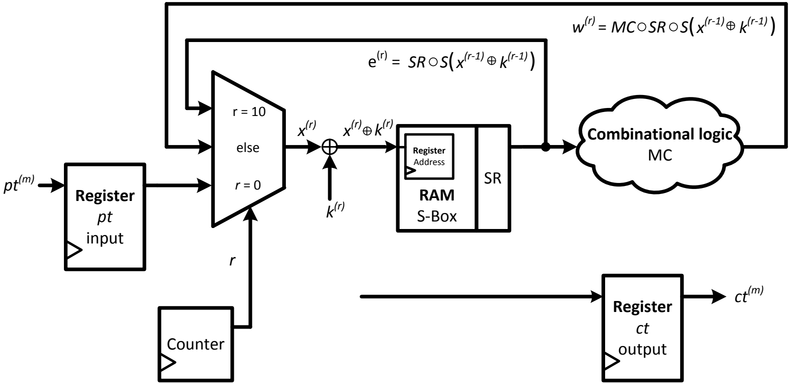
AES Architecture 1



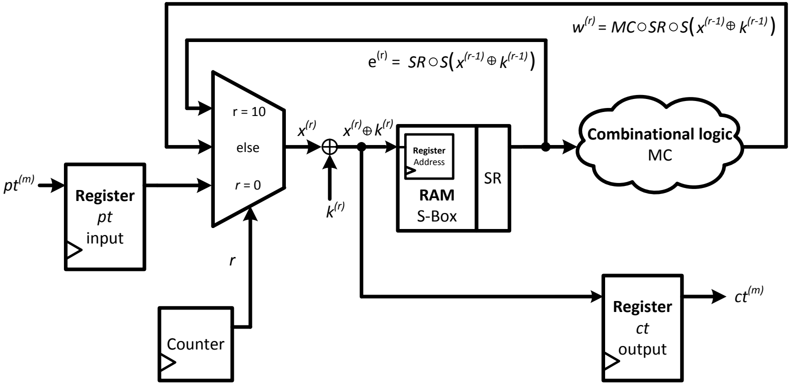
AES Architecture 1



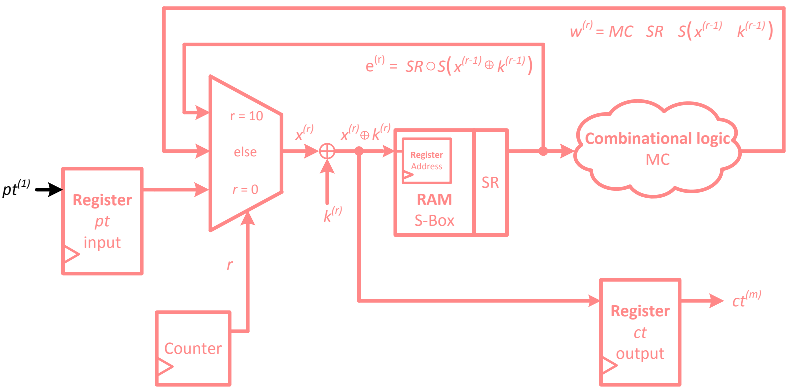
AES Architecture 1



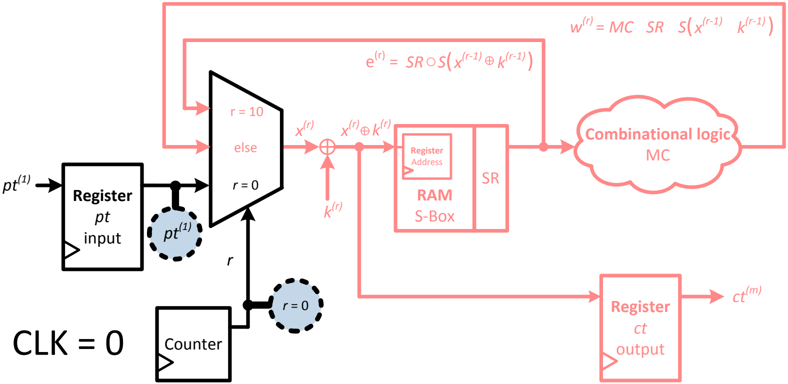
AES Architecture 1



Plaintext only attack

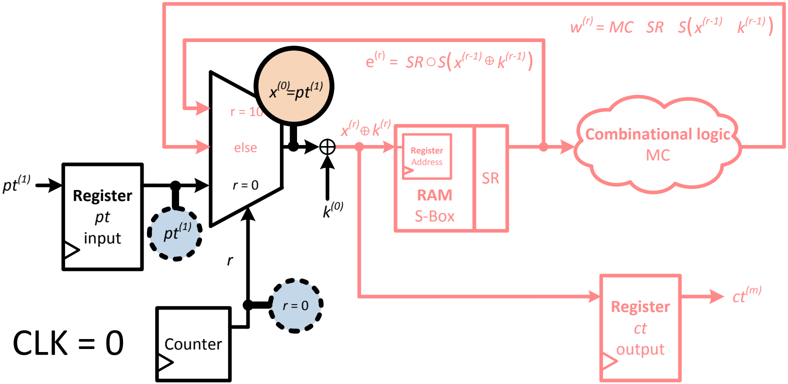


Plaintext only attack



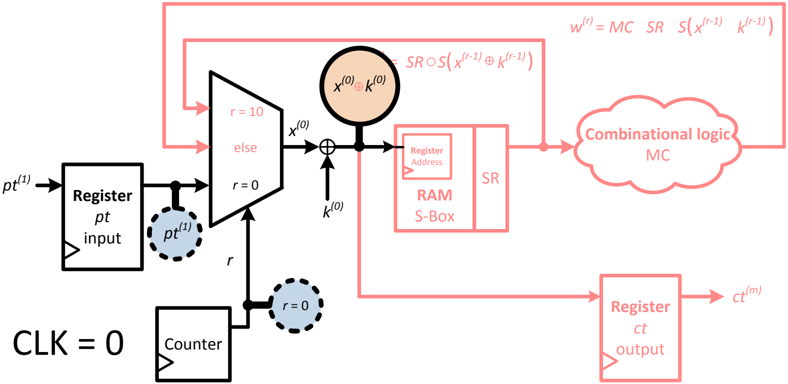
CLK = 0

Plaintext only attack

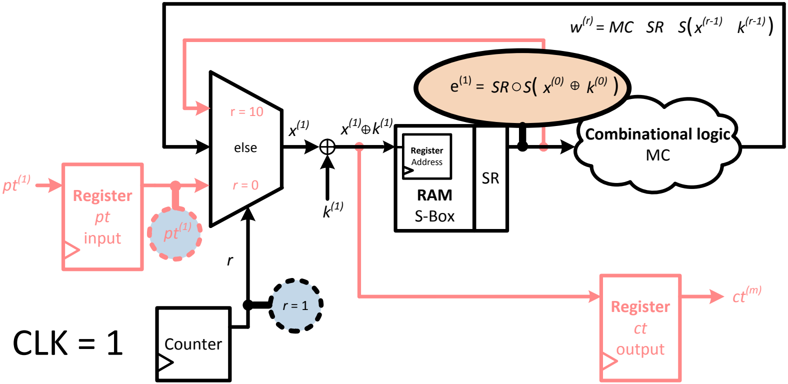


CLK = 0

Plaintext only attack

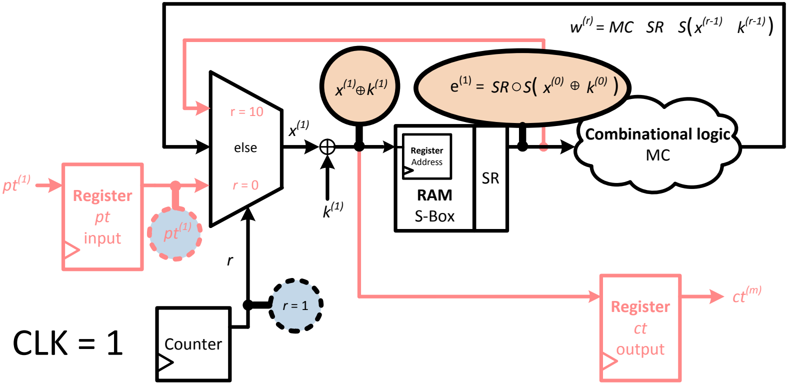


Plaintext only attack



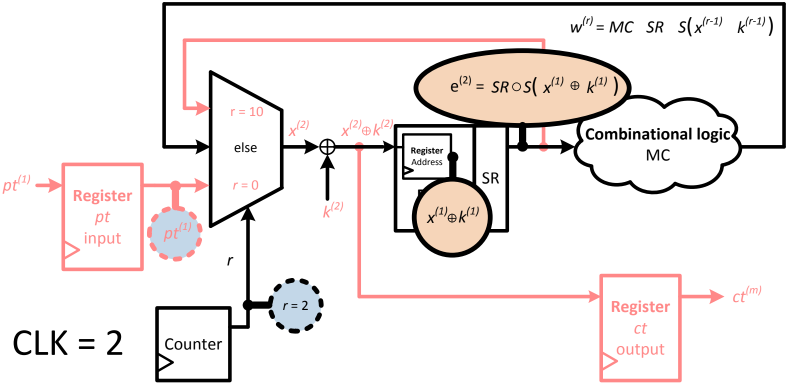
CLK = 1

Plaintext only attack



CLK = 1

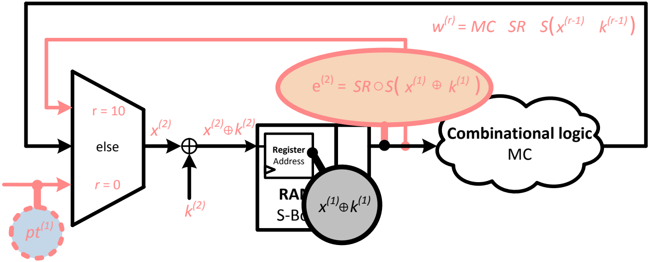
Plaintext only attack



CLK = 2

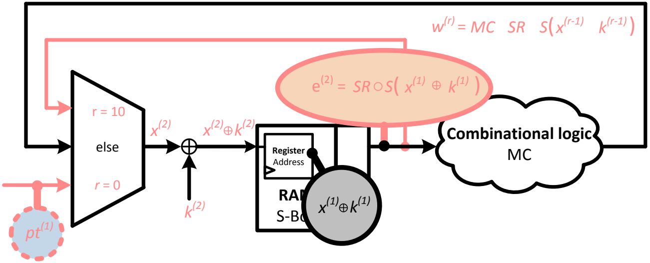
Plaintext only attack

CLK = 2



Plaintext only attack

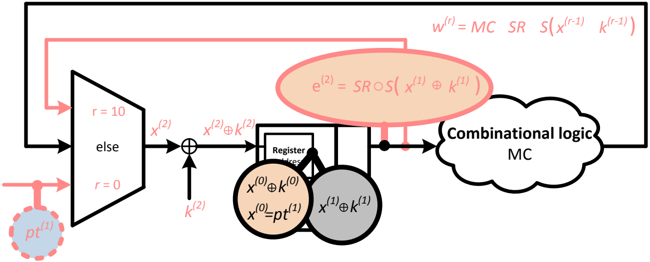
CLK = 2



$$x^{(1)} = w^{(1)} = MC \circ SR \circ S\left(x^{(0)} \oplus k^{(0)}\right)$$

Plaintext only attack

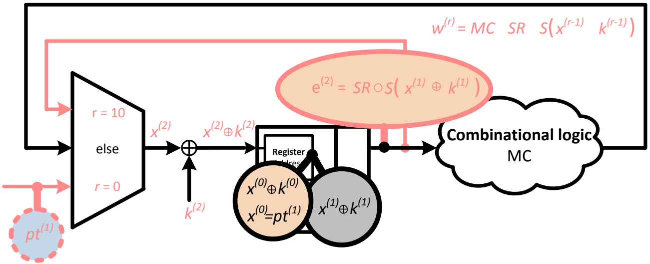
CLK = 2



$$x^{(1)} = w^{(1)} = MC \circ SR \circ S\left(x^{(0)} \oplus k^{(0)}\right)$$

Plaintext only attack

CLK = 2

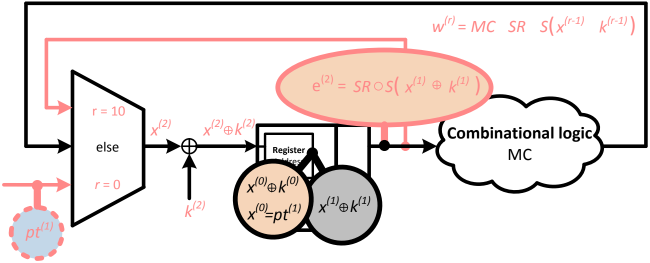


$$x^{(1)} = w^{(1)} = MC \circ SR \circ S\left(x^{(0)} \oplus k^{(0)}\right)$$

$$HD\left(w^{(1)}_{i,j} \oplus k^{(1)}_{i,j},\, pt^{(m)}_{SR^{-1}(i,j)} \oplus k^{(0)}_{SR^{-1}(i,j)}\right)$$

Plaintext only attack

CLK = 2

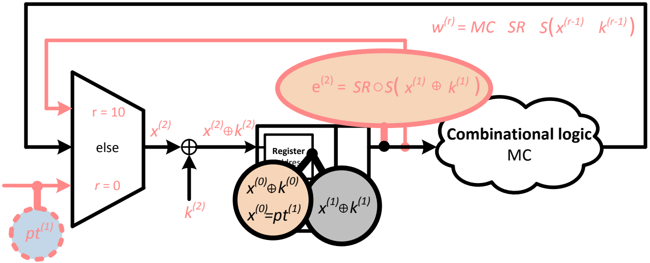


$$x^{(1)} = w^{(1)} = MC \circ SR \circ S\left(x^{(0)} \oplus k^{(0)}\right)$$

$$H_{\left(k_{i,j}^{(1)}, \left(k_{SR^{-1}(i,j)}^{(0)}\right)_{0 \leq i \leq 3}\right)} = HD\left(w_{i,j}^{(1)} \oplus k_{i,j}^{(1)}, pt_{SR^{-1}(i,j)}^{(m)} \oplus k_{SR^{-1}(i,j)}^{(0)}\right)$$

Plaintext only attack

CLK = 2

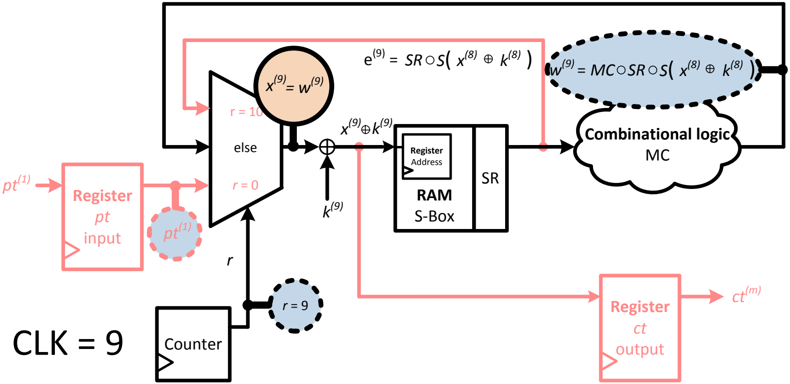


$$x^{(1)} = w^{(1)} = MC \circ SR \circ S\left(x^{(0)} \oplus k^{(0)}\right)$$

$$H_{\left(k^{(1)}_{i,j},\left(k^{(0)}_{SR^{-1}(i,j)}\right)_{0\leq i\leq 3}\right)} = HD\left(w^{(1)}_{i,j} \oplus k^{(1)}_{i,j}, pt^{(m)}_{SR^{-1}(i,j)} \oplus k^{(0)}_{SR^{-1}(i,j)}\right)$$

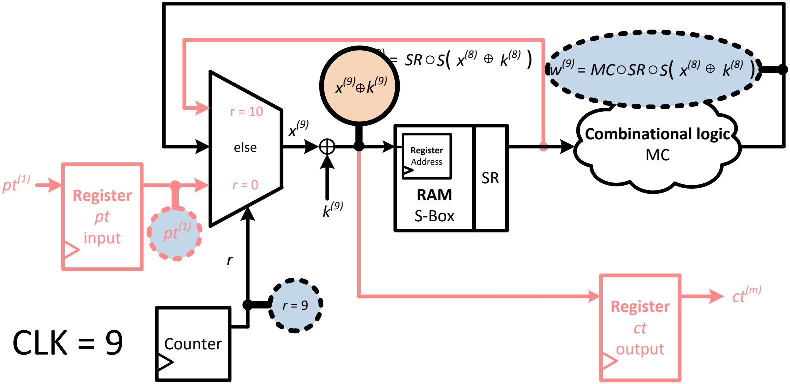
Complexity $O(2^{40})$

Ciphertext only attack

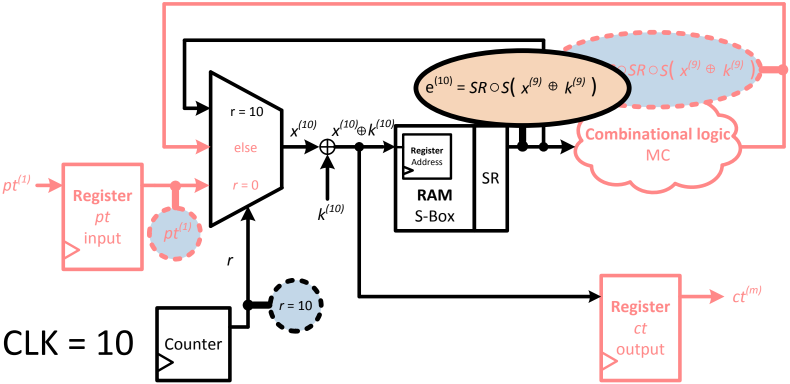


CLK = 9

Ciphertext only attack

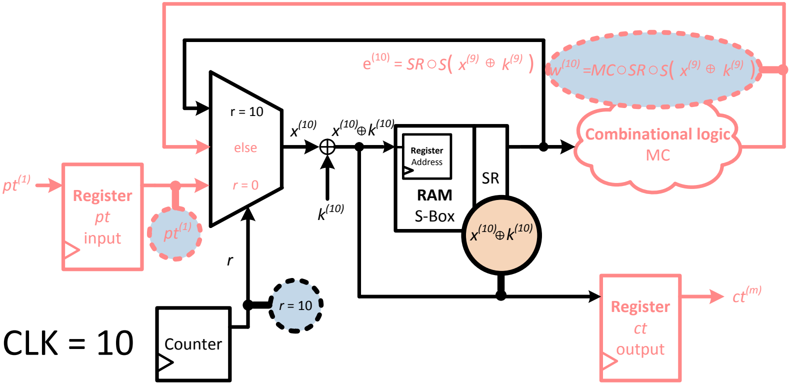


Ciphertext only attack

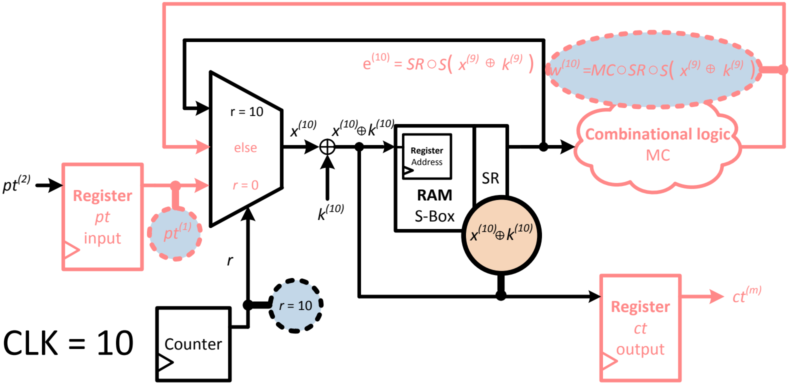


CLK = 10

Ciphertext only attack

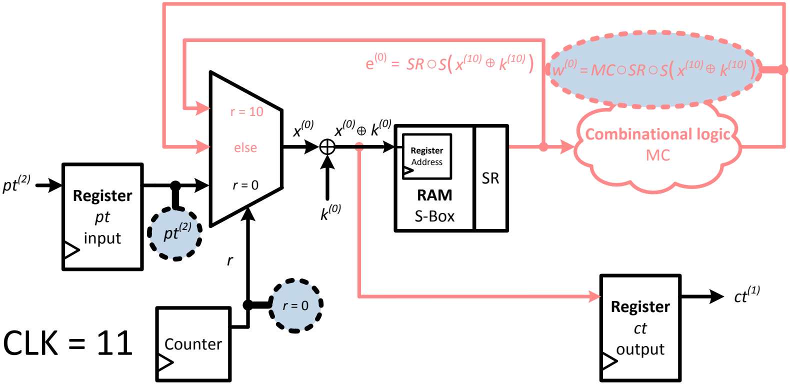


Ciphertext only attack

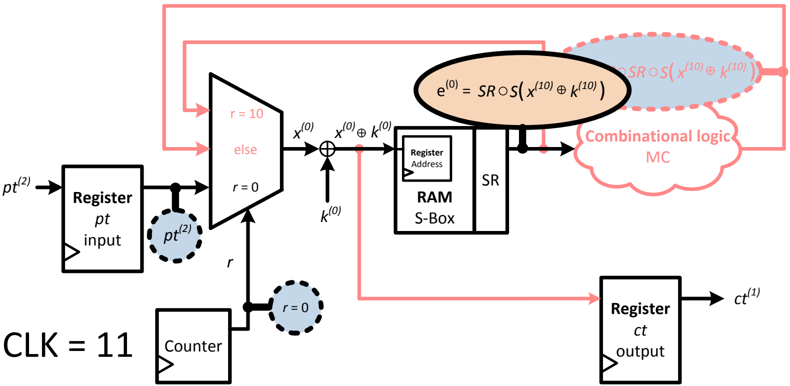


CLK = 10

Ciphertext only attack



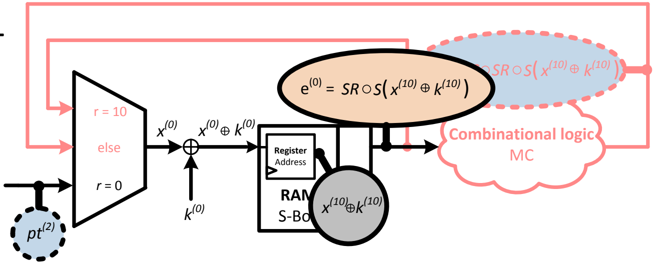
Ciphertext only attack



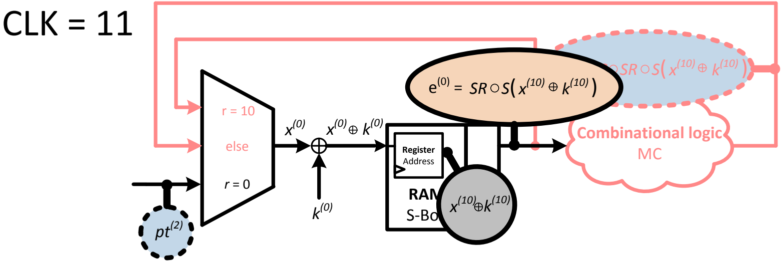
CLK = 11

Ciphertext only attack

CLK = 11



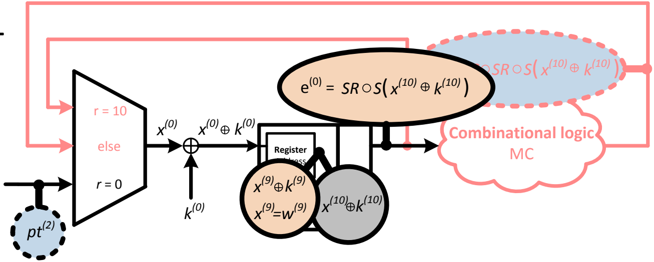
Ciphertext only attack



$$ct^{(m)} = x^{(10)} \oplus k^{(10)}$$

Ciphertext only attack

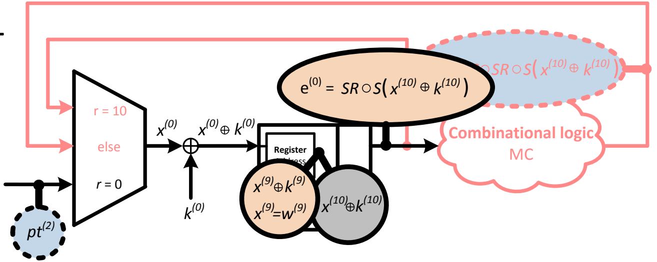
CLK = 11



$$ct^{(m)} = x^{(10)} \oplus k^{(10)}$$

Ciphertext only attack

CLK = 11

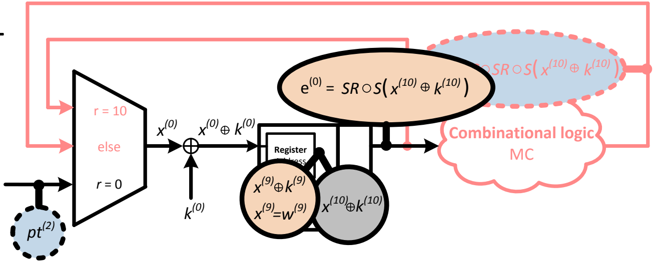


$$ct^{(m)} = x^{(10)} \oplus k^{(10)}$$

$$x^{(9)} \oplus k^{(9)} = SR^{(-1)} \circ S^{(-1)} \left(ct^{(m)} \oplus k^{(10)} \right)$$

Ciphertext only attack

CLK = 11



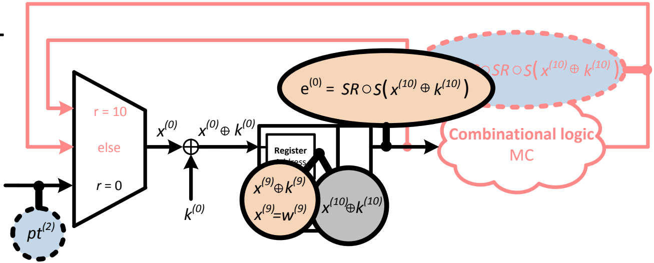
$$ct^{(m)} = x^{(10)} \oplus k^{(10)}$$

$$x^{(9)} \oplus k^{(9)} = SR^{(-1)} \circ S^{(-1)}\left(ct^{(m)} \oplus k^{(10)}\right)$$

$$H_{k_{i,j}^{(10)}} = HD\left(S^{-1}(ct_{i,j}^{(m)} \oplus k_{i,j}^{(10)}),\, ct_{SR^{-1}(i,j)}^{(m)}\right)$$

Ciphertext only attack

CLK = 11



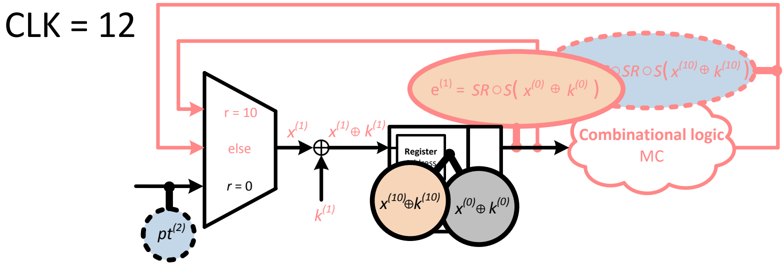
$$ct^{(m)} = x^{(10)} \oplus k^{(10)}$$

$$x^{(9)} \oplus k^{(9)} = SR^{(-1)} \circ S^{(-1)}\left(ct^{(m)} \oplus k^{(10)}\right)$$

$$H_{k_{i,j}^{(10)}} = HD\left(S^{-1}(ct_{i,j}^{(m)} \oplus k_{i,j}^{(10)}), ct_{SR^{-1}(i,j)}^{(m)}\right)$$

Complexity $O(2^8)$

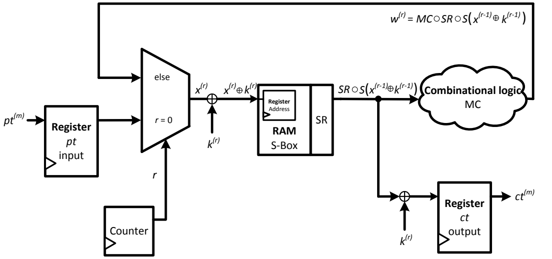
Plaintext and ciphertext attack

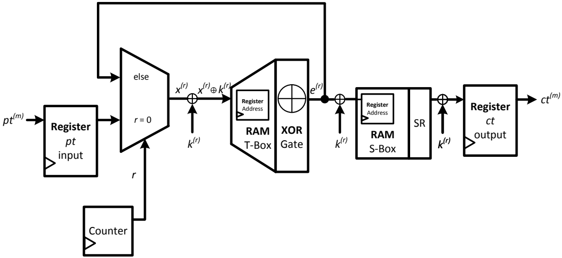


$$H_{k_{i,j}^{(0)}} = HD\left(pt_{i,j}^{(m)} \oplus k_{i,j}^{(0)}, ct_{i,j}^{(m-1)}\right).$$

The complexity is $O(2^8)$

Next Two Architectures





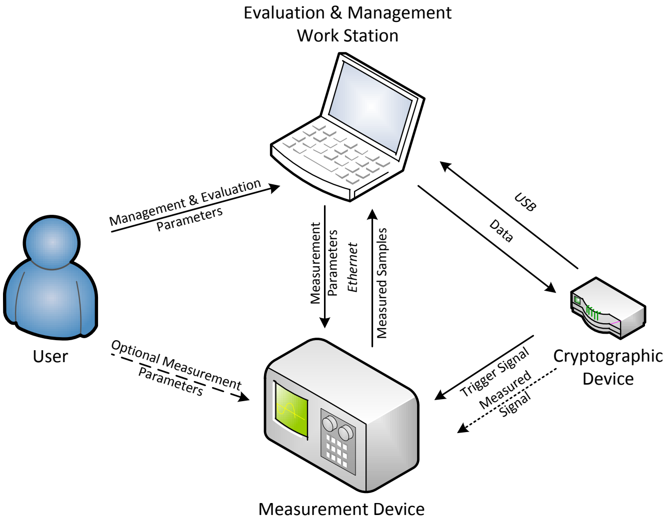
Complexities in respect to the presented architectures

Table: Comparison of all AES architectures with respect to the HD power model hypotheses complexity. Plaintext and ciphertext attack (PCA), plaintext only attack (POA), ciphertext only attack (COA).

Architecture	PCA	POA	COA
1	2^8	2^{40}	2^8
2	2^{16}	2^{40}	2^{16}
3	2^{16}	2^{40}	2^{16}

Part II. Results from a CPA attack against AES-128 using HD power model

Block scheme of the measurement setup we used



List of the tools and its attributes for the measure setup

Tool	Attributes
Cryptographic Device:	FPGA Actel Fusion M7AFS600 256FBGA, Cypress microcontroller.
Cryptographic Algorithm:	AES 128b, 128b datapath, i.e. 16 Sboxes, 33.33MHz.
Measurement Device:	Oscilloscope WavePro 740Zi (4 GHz Bandwidth, 4 Input Channels, 40 GS/s on 2 Ch Max Sample Rate).
Evaluation & Management Work Station:	Intel(R) Core(TM) i7-2630QM CPU @ 2.00GHz, RAM 12GB.
Attack implementation:	C++, 7 threads, 100K traces per 6.5 seconds, 2000 samples (50ns) per trace.
Measurement implementation:	C++, 1 thread, 100K traces per 38 seconds, 2000 samples (50ns) per trace.

We implemented two experimental implementations AES-LR-32b and AES-128b:

AES-LR-32b Experimental implementation of the AES final round. Four S-boxes and AddRoundKey operation were implemented. Since the MixColumn operation is not applied in the final round, and the ShiftRows is just a linear operation which does not need any combinational logic elements such as XOR, NOR, NAND, the MixColumn and ShiftRows operations were not implemented.

AES-128b Full AES-128 with 128-bit data path, i.e. with 16 S-boxes performed in parallel, were implemented.

Implemented AES architectures

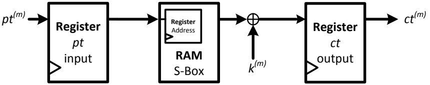


Figure: AES-LR-32b architecture

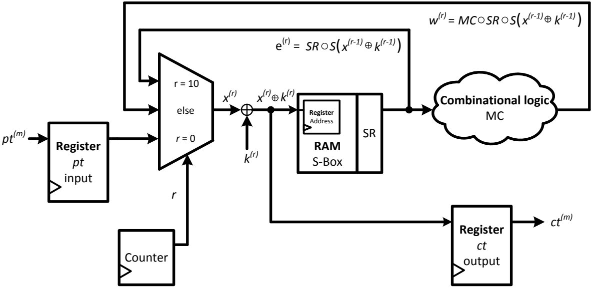


Figure: AES-128b architecture

Statistical data collection description

Using the Measurement setup, and using our developed applications, we conducted two attacks:

AES-LR-32b
: We measured 7K5 power traces. Thus, we encrypted 7K5 random texts, uniformly distributed, with one randomly generated key drawn from the uniform distribution, too.

AES-128b
: We measured 30K power traces similarly as for AES-LR-32b.

For both AES-LR-32b and AES-128b implementations, we computed the statistical data from 100 random realisations of the attack using our developed application.

Exploiting more Knowledge about the Implementation

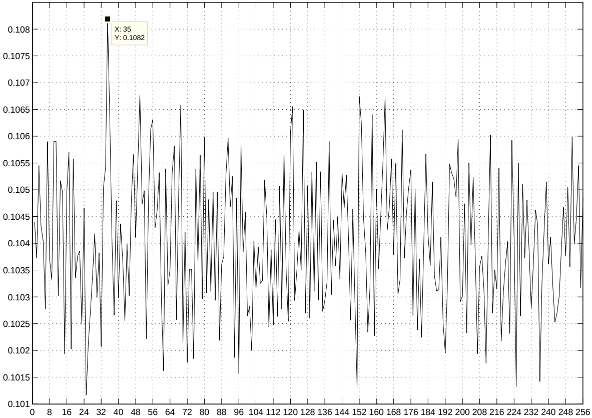


Figure: Correlation coefficient for the correct key hypothesis using more information about the implementation. Attack against AES-128b. On the x-axis, the value of the possible key is shown. The correlation coefficient is shown on the y-axis.

Influence of MixColumn to CPA

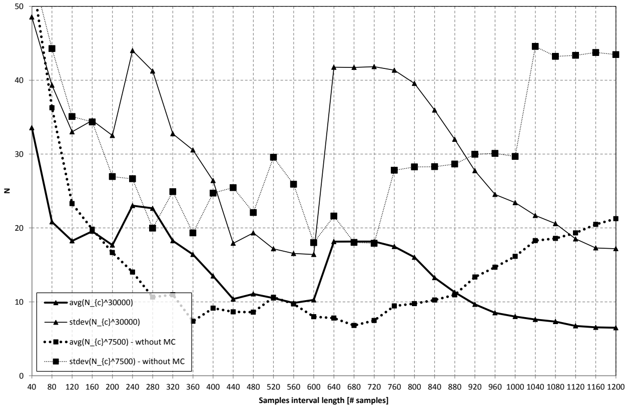


Figure: Impact of MixColumn operation to CPA with respect to samples interval length. N_c is the order of the correct key hypothesis. In the graph, average value and standard deviation of the N_c for both implementations AES-LR-32b and AES-128b are plotted.

Average Correlation Coefficient During One AES Round

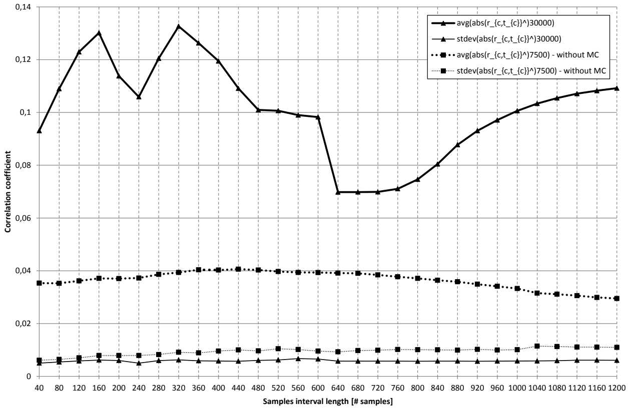


Figure: Average value of the maximal correlation coefficient for the correct key hypothesis in samples interval.

When the exploitable data-dependent function is preformed

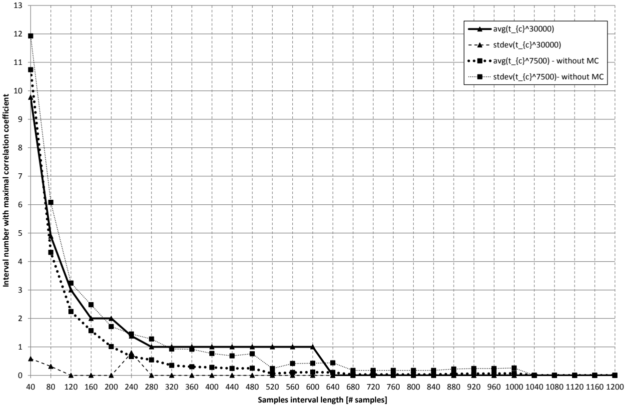


Figure: Interval number in which the correlation coefficient was maximal for the correct key hypothesis.

Successfulness of CPA Attack During One Round of AES

Figure: Attack successfulness for the AES-128b with respect to the samples interval length. This graph is illustrated for cases when 13, 6, 3, 1 keys candidates with the biggest correlation coefficient are taken into account, i.e. 1-\alpha_12^30000, 1-\alpha_5^30000, 1-\alpha_2^30000, 1-\alpha_0^30000 respectively.

Part III. Conclusions

We:

1. analysed several AES architectures with respect to HD power model (HDPM) construction,
2. found out that the complexity of HDPM depends on known data and architecture design,
3. developed C++ applications for measuring leakage information, CPA attack, and statistical data collection
4. conducted CPA attack against full AES-128 implemented in FPGA Actel Fusion.