*ACM International Conference on Computing Frontiers 2016*

# Adaptable AES Implementation with Power-Gating Support

*Subhadeep Banik, Andrey Bogdanov*
*Technical University of Denmark*
*DTU Compute*

*Tiziana Fanni, Carlo Sau and Luigi Raffo*
*Università di Cagliari*
*Dept. of Electrical and Electronics Eng.*
*tiziana.fanni@diee.unica.it*

*Francesca Palumbo*
*Università di Sassari*
*PolComIng Information Engineering Unit*

*Francesco Regazzoni*
*Università della Svizzera Italiana*
*Advanced Learning and Research Institute*

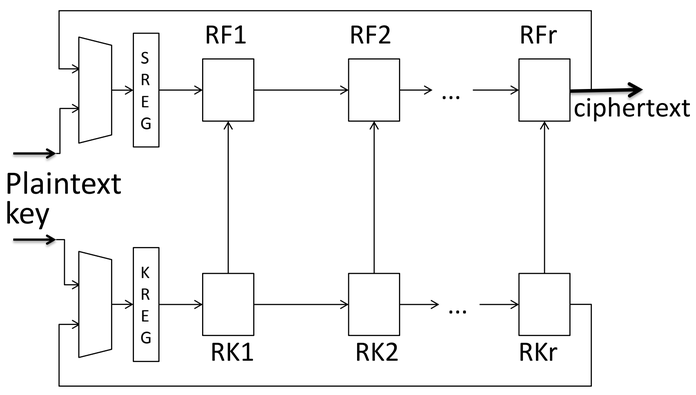
*The research leading to these results has received funding from RPCT (L.R. 7/2007, CRP-18324) project.*

## Abstract

We present a **reconfigurable** design of the **Advanced Encryption Standard** capable of adapting at run-time to the requirements of the target application. Reconfiguration is achieved by activating only a specific subset of all the instantiated processing elements. Further, we explore the effectiveness of **power gating** and **clock gating** methodologies to minimize the energy consumption of the processing elements not involved in computation.

## AES: Advanced Encryption Standard

AES is algorithm selected by the Institute of Standards and Technology to be the standard block cipher.



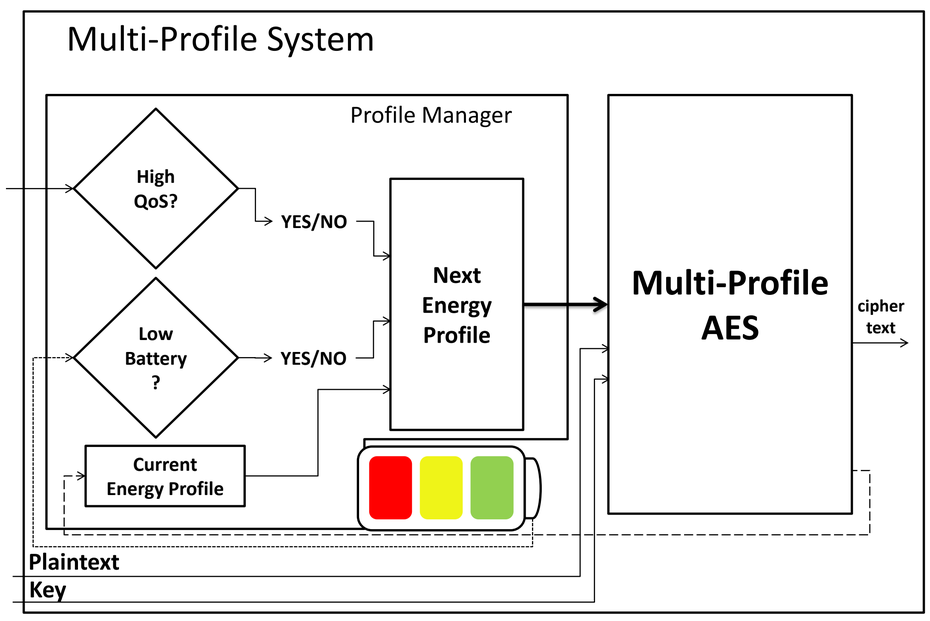

AES implementations range from high speed unrolled implementations to extremely small designs suitable for RFIDs. Thus a large number of devices can encrypt data using the same algorithm.

## Multi-Profile AES implementation

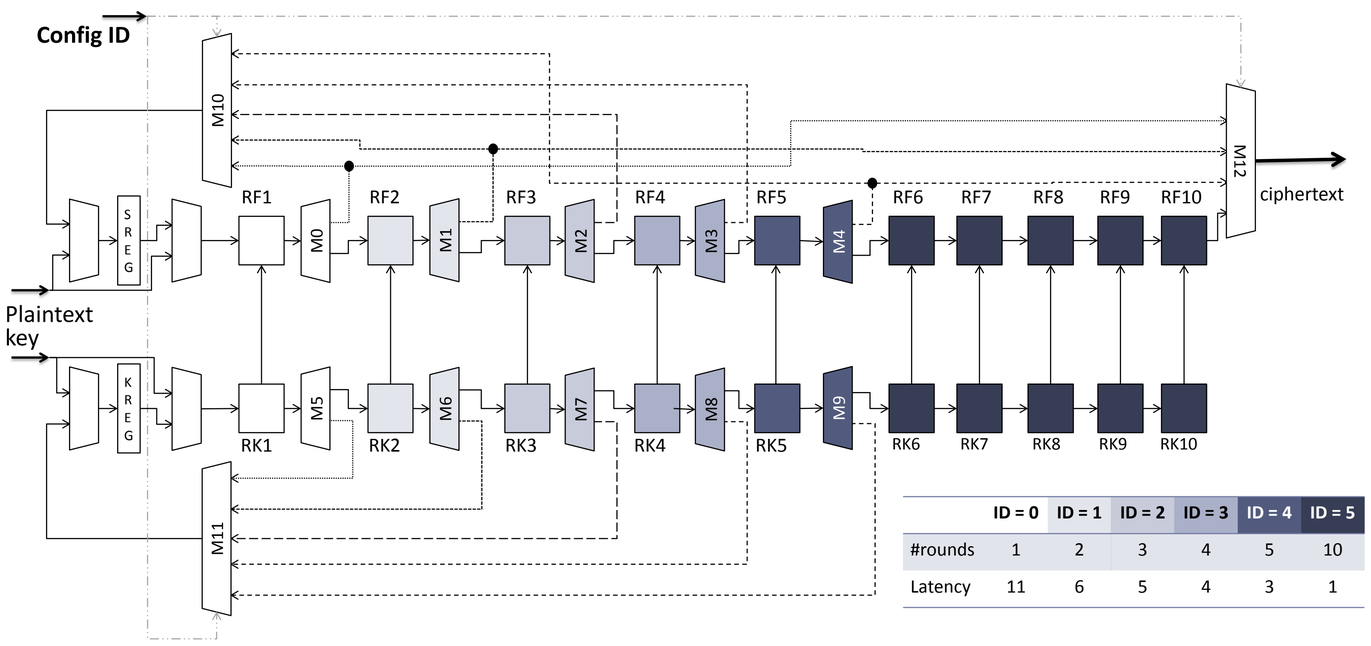
**Problem statement:**
nodes connecting different devices of the internet of things have to be capable of communicating efficiently with all of them, despite the different throughput achieved by the specific device.

**Solution: multi-profile AES implementation**

- if the remnant battery is lower than a pre-defined threshold the Profile Manager might select a less energy consuming profile;
- if the connected device is requesting for higher speed it might select a more latency efficient profile.




## Coarse Grain Reconfigurable AES

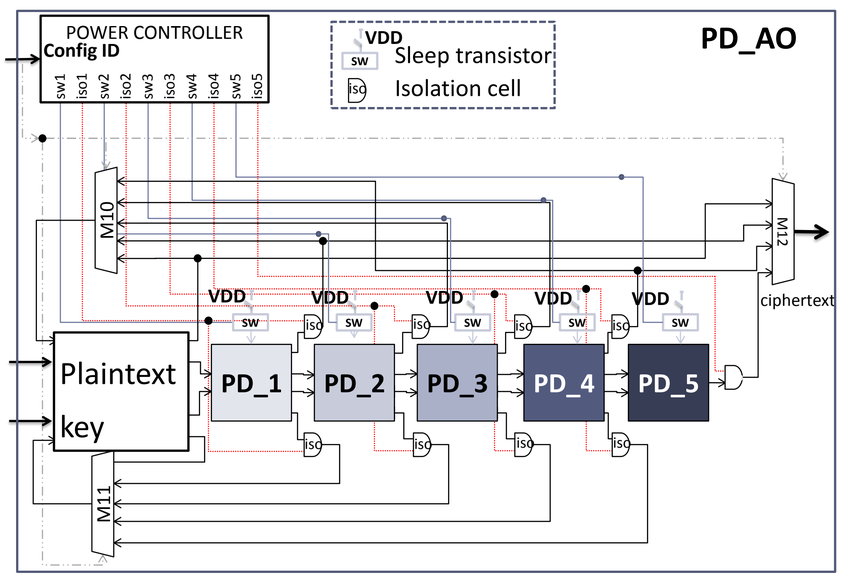



| | ID = 0 | ID = 1 | ID = 2 | ID = 3 | ID = 4 | ID = 5 |
|---|---|---|---|---|---|---|
| #rounds | 1 | 2 | 3 | 4 | 5 | 10 |
| Latency | 11 | 6 | 5 | 4 | 3 | 1 |

**Coarse Grained Reconfigurable AES** architecture capable of unrolling up to 10 rounds.
Depending on the Configuration ID, the multiplexers change the connections among the RFs and RKs blocks, enabling different AES configurations.

According with the enabled configuration, the **CGR-AES** features different **encryption latency** and different **energy consumption** per encrypted block and is able to adapt with the requirements of the target application.

## Power Gated Coarse Grain Reconfigurable AES

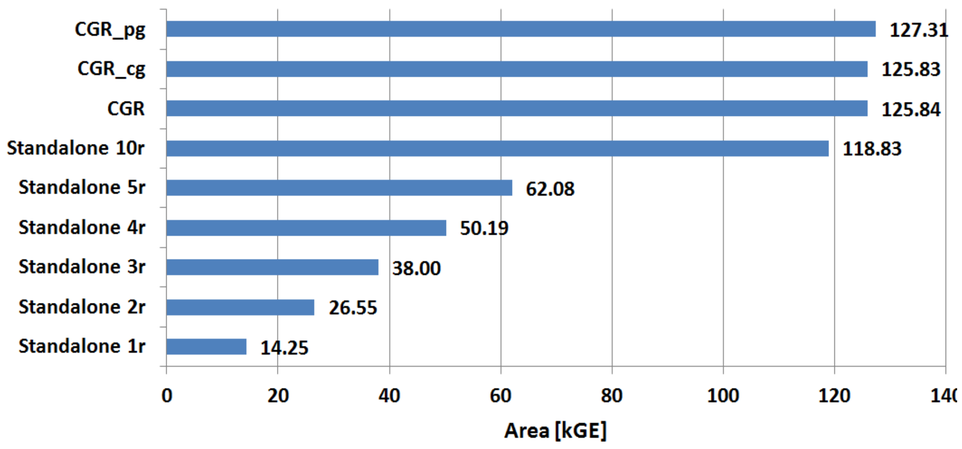



**Power gating** is applied at a **coarse-grain level** to the rounds not involved in the current computation. The configurations on the system correspond to six different Power Domains (PDs).

By setting a specific Config ID, it is possible to switch off one or more PDs. All the not switchable logic (power controller, isolation cells) is inserted in the Always On PD (PD AO).

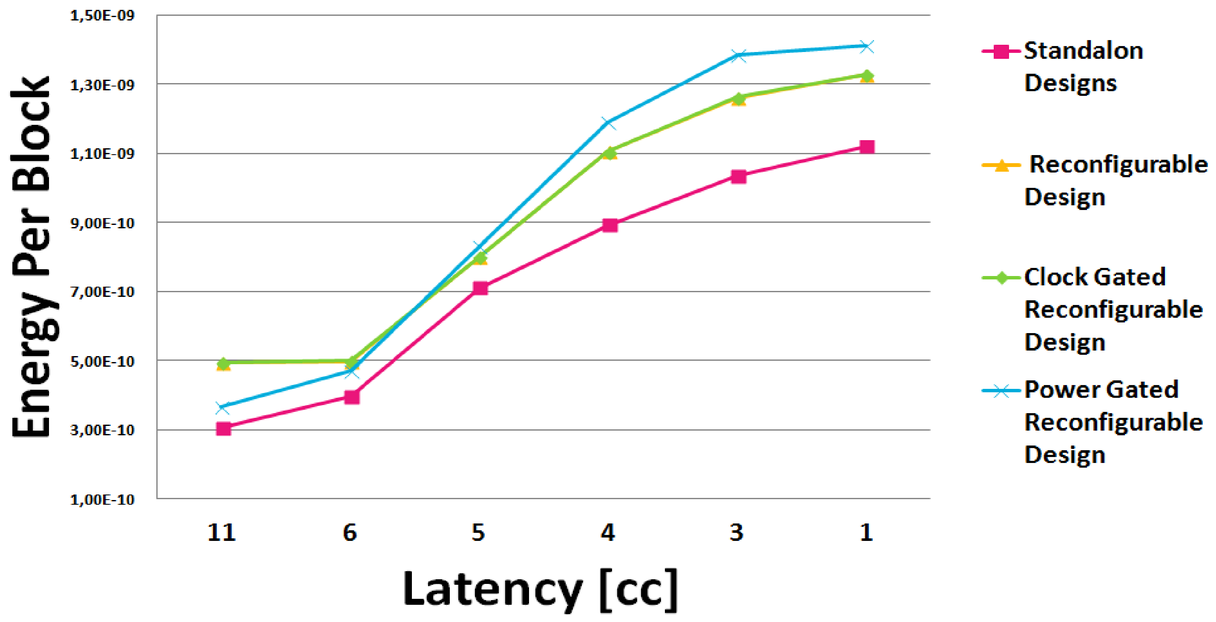
## Performance Evaluation on Asic

**Standalone Nr:** the standalone implementation of the AES algorithm, where N indicates the number of r unrolled rounds of the specific implemented cipher.
**CGR:** the CGR capable of mimicking all the unrolled standalone designs, since it allows the execution of AES algorithm with 1, 2, 3, 4, 5, or 10 unrolled round(s).
**CGR cg:** the CGR with clock gating provided by the synthesizer.
**CGR pg:** the CGR with power gating applied.




Design occupation is reported in Gate Equivalents (GE).
All CGR designs require approximately 6% additional gates compared with the standalone design instantiating 10 unrolled rounds (Standalone 10r).

TSMC 90 nm CMOS low power library.




More unrolled rounds achieve higher performance, but cause higher energy consumption due to the additional logic:
**Standalone 10R:** the most performing design, but the most energy consuming.
**Standalone 1R:** the best design in terms of energy, but the one with the highest latency.

## Conclusions

The proposed implementation allows selecting dynamically the amount of rounds to be computed in the same clock cycle, thus trading energy consumption with throughput.
Our results shows that coarse-grained reconfigurability could be an appealing approach to implement flexible designs of cryptographic algorithms. We also demonstrated that power consumption caused by the unused processing elements can be further reduced using power gating.