Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

6th INTERNATIONAL CONFERENCE ON
PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS
(PKIA 2025)

SEPTEMBER 3-4th, 2025

An HLS-driven Architectural Design for the PRESENT Lightweight Block Cipher

Atul M.[1], Diksha Shekhawat [2,3], Jugal Gandhi [2,3], M. Santosh [2,3], Jai Gopal Pandey [2,3]

[1]Birla Institute of Technology and Science (BITS) Pilani, Goa Campus-403726, India
[2]CSIR- Central Electronics Engineering Research Institute (CEERI), Pilani- 333031, India
[3]Academy of Scientific and Innovative Research (AcSIR), Ghaziabad- 201002, India

https://pkiindia.in

Social Media /pkiindia

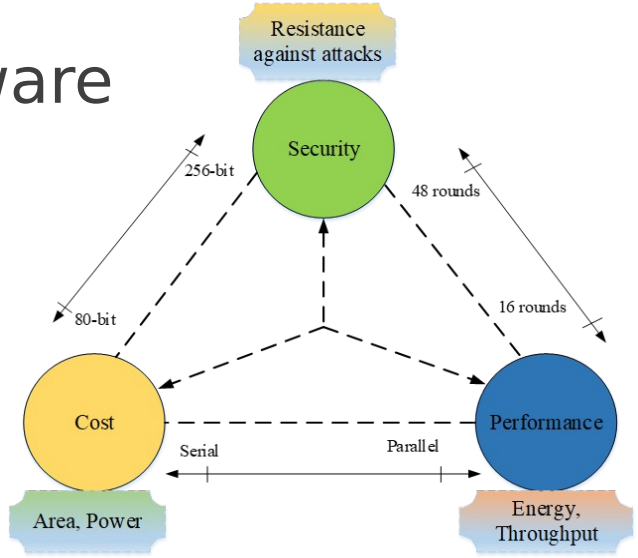
IEEE BANGALORE SECTION

Outline

- Motivation and Introduction of the Work
- PRESENT Cipher
- Research Gap
- Hardware Architecture of PRESENT Cipher
- Experimental Setup
- Overhead Analysis
- Conclusion
- References

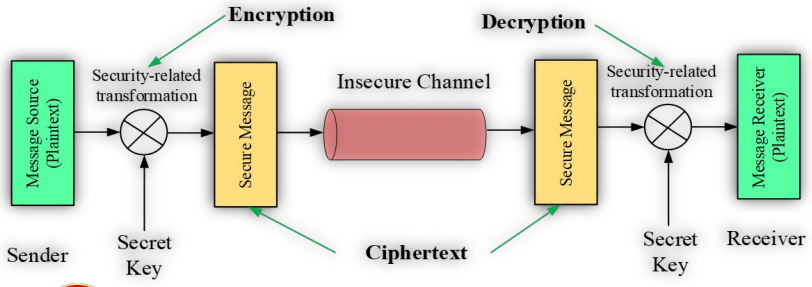
Motivation for the Work

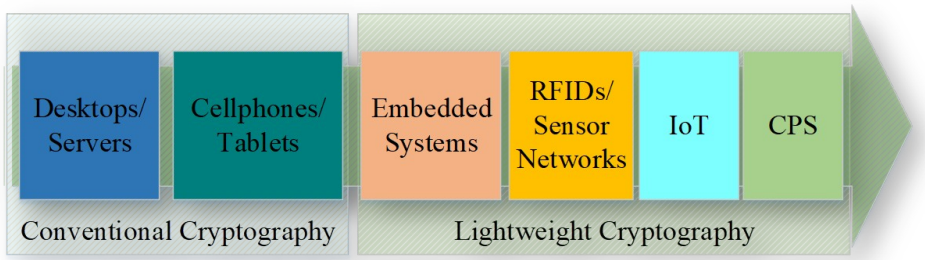
- IoT/edge infrastructures rely on deployment of tiny computing devices
- Pervasive computing infrastructure
  - Sensing, computing, controlling and communication
- Emerging authentication-based applications
  - Smart cities, smart grid, digital locker, biometric data, recognition, bank transactions, gadgets, etc.
- Secure communication is very essential
- Need secure, high-performance, area-efficient hardware implementation of ciphers
- Trade-offs: security, cost and performance
- General-purpose ciphers are slow, take large area
- *Lightweight* ciphers for constrained environments
  - ISO/IEC SC27 lightweight cryptography standards

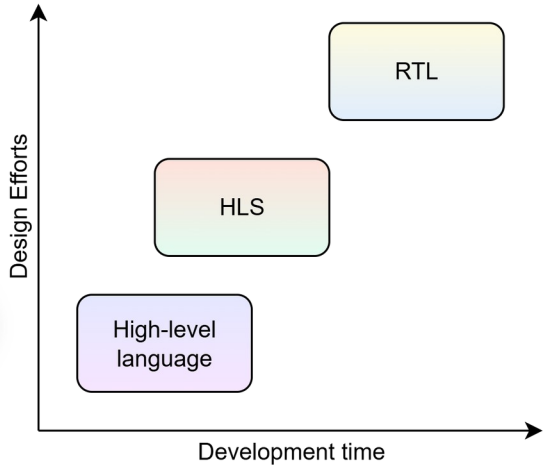


Introduction

- Resource-constrained devices necessities lightweight ciphers
- The PRESENT cipher is a lightweight symmetric key block cipher
  - Substitution permutation network (SPN) structure
  - Supports 80-bit and 128-bit key sizes
- The cipher has 64-bit input/encrypted output combination
- Traditionally, HDLs used to design and implement hardware
- HLS → Hardware design and implementation tool
  - Hardware can be modelled at a higher level of abstraction
  - C/C++/Python languages

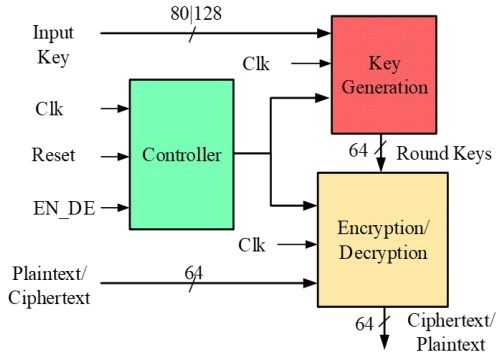


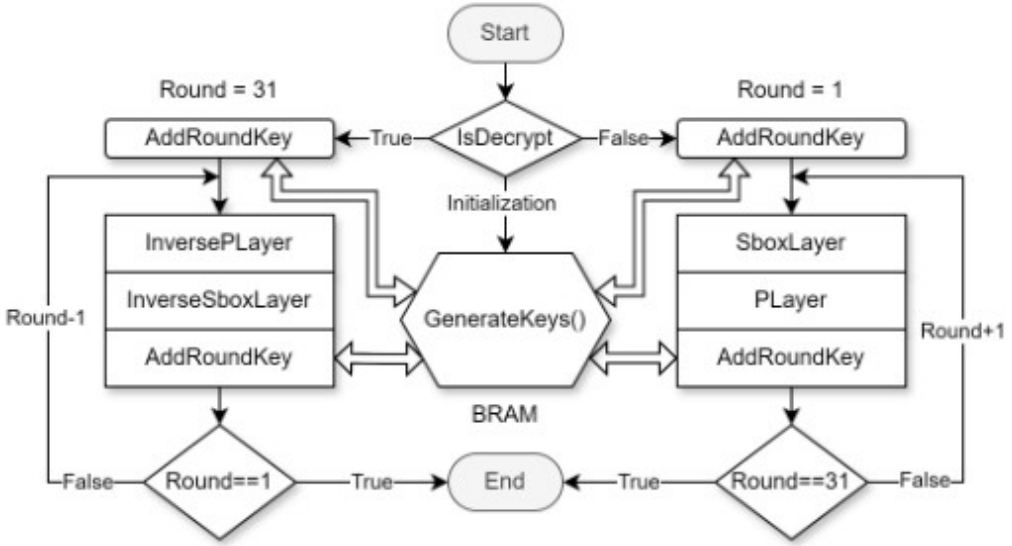




The PRESENT Cipher

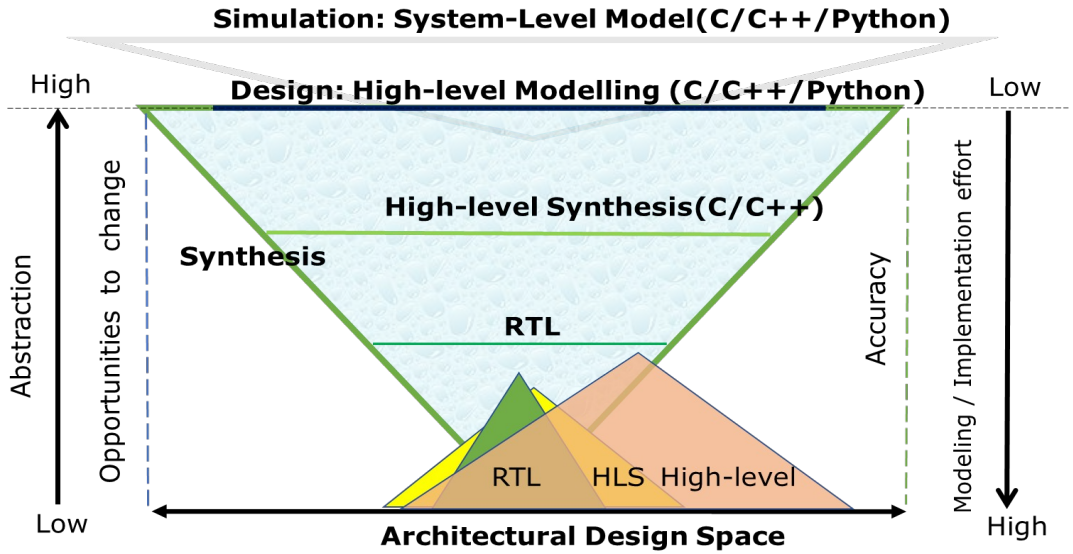
- PRESENT is a symmetric ultra-lightweight block cipher [NIN17]
- The cipher is based on SPN, with a round-based processing
- To improve the security of hardware implementations
  - Keying can be generated using hardware primitives such as PUFs [PAN19]
- In PRESENT, the state is a 1-D array of 64 bits
  - Supports shift operations
  - Parallel access over the data





[NIN17]: L.Nino, C. Andres, *et. al*, "Lightweight Hardware Architectures for the Present Cipher in FPGA," IEEE Transactions On Circuits And Systems–I: Regular Papers, VOL. 64, NO. 9, 2017.
[PAN19]: J. C. Pandey,, T. Goel, and A. Karmakar. "Hardware architectures for PRESENT block cipher and their FPGA implementations." IET Circuits, Devices & Systems 13.7 (2019): 958-969.

Research Gaps



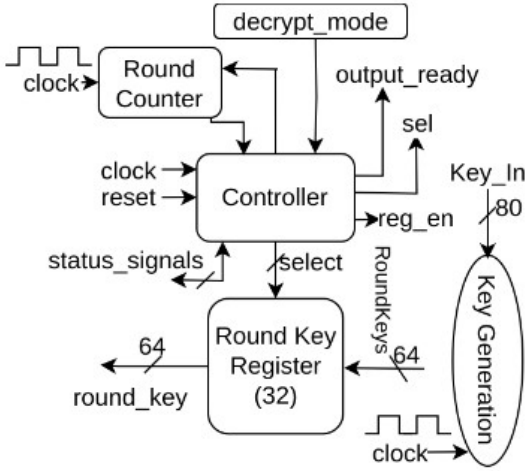
- High-level to hardware implementation
- PRESENT with latency-resource trade-offs [NIN17], [PAN19]
- Streamlined HLS-based design [SAH18]
- An optimized HLS implementation of PRESENT, comparable to RTL

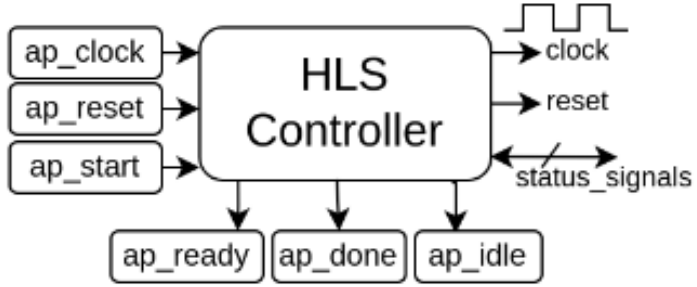
[NIN17]: L.Nino, C. Andres, *et. al*, "Lightweight Hardware Architectures for the Present Cipher in FPGA," IEEE Transactions On Circuits And Systems–I: Regular Papers, VOL. 64, NO. 9, 2017.
[PAN19]: J. G. Pandey,, T. Goel, and A. Karmakar. "Hardware architectures for PRESENT block cipher and their FPGA implementations." IET Circuits, Devices & Systems 13.7 (2019): 958-969.
[SAH18]: R. Saha, P. P. Banik, and K.-D. Kim, "HLS based Approach to Develop an Implementable HDR Algorithm," Electronics, vol. 7, no. 11, p. 332, 2018.

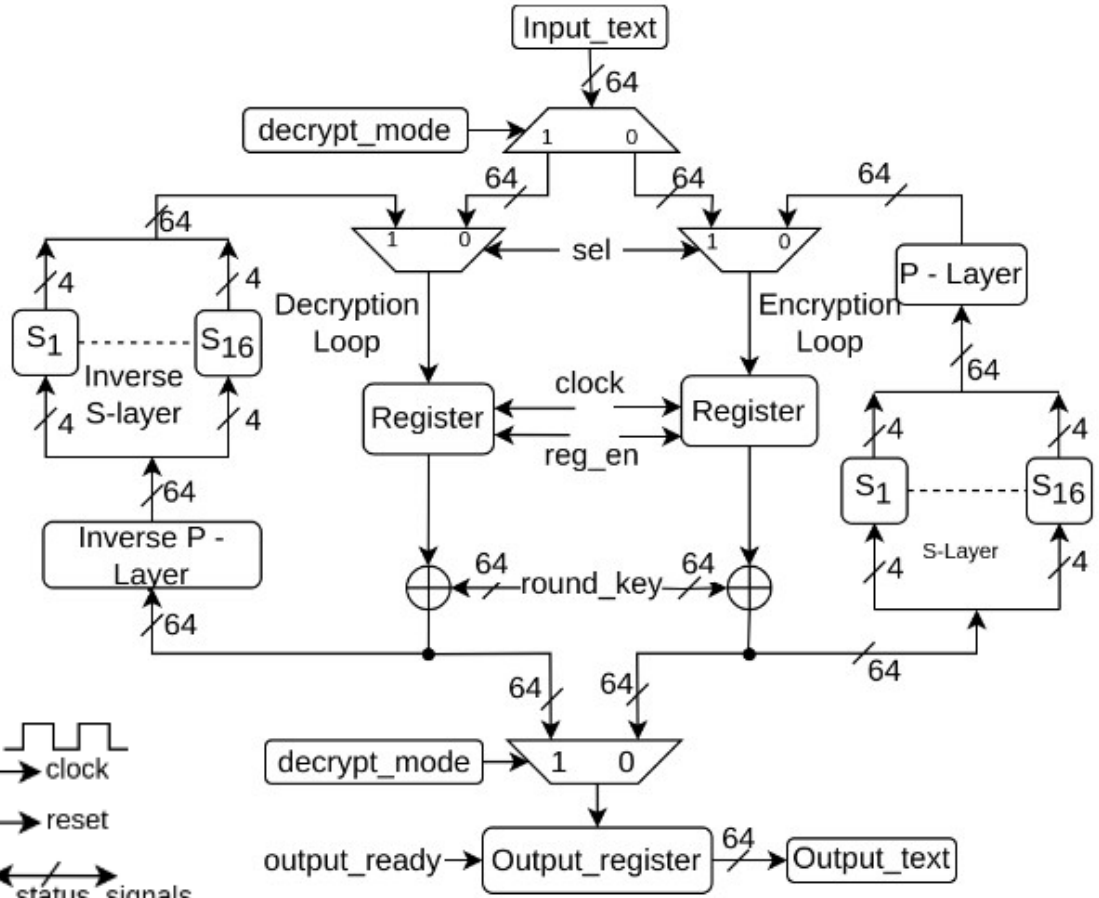
An HLS-based Architectural Approach

Algorithm 1: Round Key in PRESENT Algorithm

```
1  procedure GenerateRoundKeys()
2  N_round ← 1                                  ▷ Initialize the round
3  while N_round < 32 do
4  |   addRoundKey(STATE, K_N_round)
5  |   sBoxLayer(STATE)
6  |   pLayer(STATE)
7  |   N_round ← N_round + 1
8  end
9  addRoundKey(STATE, K_N_round)
10 end
```







Experimental Setup

- Modeling → C (C++)
- AMD Xilinx Vitis HLS 2024.1
- Design → AMD Xilinx's Vivado 2022.1
  - FPGA → AMD Xilinx Zedboard (Zynq 7000 Series → XC7Z020CLG400-1)
- The HLS IP of PRESENT is wrapped with an AXI4 LITE interface
  - To control it with the processor (dual-core Arm Cortex-A9 MPCore)

Results: FPGA Implementations

Table 1: FPGA Implementation Results of PRESENT Cipher for Encryption, Decryption, and Combined Encryption, Decryption

Parameters	LUTs	FFs	BRAM	Slices	Latency (in cycles)	Maximum Frequency (MHz)	Latency (ns)	Latency (ns) x (LUTs + FFs)
Encryption	285	371	0	95	67	224.00	299.10	192.2*k*
Decryption	376	342	2	117	102	215.65	473.00	339.6*k*
Combined Encryption-Decryption	664	559	2	201	106	203.62	520.60	636.7*k*

Table 2: PS-PL Implementation Results

Parameters	LUTs	FFs	BRAM	Slices	Maximum Datapath Delay (ns)	Maximum Frequency (MHz)
Proposed Work	1366	1541	1	477	6.046	154.27.7*k*

Results: Performance Comparison

Table 3: Comparison with Existing HLS and RTL Implementation of PRESENT Cipher with the Proposed Work

Parameters	LUTs	FFs	Latency (in cycles)	Maximum Frequency (MHz)	Latency	Latency (ns) x (LUTs + FFs)
RTL [PAN17]	221	224	33	278	119 *ns*	53*k*
RTL [VAR19]	213	213	32	368	87 *ns*	37*k*
HLS [VAR19]	466	765	29*k*	125	233 *µs*	286*M*
Proposed Work	285	371	67	224	300 *ns*	196*k*

Time period of clock=4.48 ns

- Proposed implementation has reduced
  - 38.84% in LUTs and 51.50% in FFs
  - 99.77% in latency
- Maximum frequency is improved by 79.20%

[VAR19]: A. Varici, G. Saglam, S. Ipek, A. Yildiz, S. G¨oren, A. Aysu, D. Iskender, T. B. Aktemur, and H. F. Ugurdag, “Fast and Efficient Implementation of Lightweight Crypto Algorithm PRESENT on FPGA Through Processor Instruction Set Extension,” in 2019 IEEE East-West Design & Test Symposium (EWDTS), pp. 1–5, IEEE, 2019.
[PAN17]: J. G. Pandey, T. Goel, and A. Karmakar, “An Efficient VLSI Architecture for PRESENT Block Cipher and its FPGA Implementation,” in VLSI Design and Test: 21st International Symposium, VDAT 2017, Roorkee, India, June 29–July 2, 2017, Revised Selected Papers 21, pp. 270–278, Springer, 2017.

Conclusion

- Proposed an optimized version of PRESENT cipher
  - Design and implementation using HLS
  - Offers better performance with improved resource utilization
- It outperforms the previous HLS implementation
- Comparable to RTL designs
  - In terms of efficiency and resource utilization
- Integrated into a PS-PL system
  - Created an IP core controlled through software

References

1. A. Jangir, D. Shekhawat, and J. G. Pandey, “An FPGA Prototyping of the GIFT Cipher for Image Security Applications,” in 2021 4th international conference on security and privacy (ISEA-ISAP), pp. 1–6, IEEE, 2021.
2. S. Lahti, P. Sjovall, J. Vanne, and T. D. Hamalainen, “Are We There Yet? A Study on the State of High-Level Synthesis,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 38, no. 5, pp. 898–911, 2019.
3. R. Saha, P. P. Banik, and K.-D. Kim, “HLS based Approach to Develop an Implementable HDR Algorithm,” Electronics, vol. 7, no. 11, p. 332, 2018.
4. R. Mill´on, E. Frati, and E. Rucci, “A comparative study between HLS and hdl on soc for image processing applications,” arXiv preprint arXiv:2012.08320, 2020.
5. M. Sarg, A. H. Khalil, and H. Mostafa, “Efficient HLS Implementation for Convolutional Neural Networks Accelerator on an SoC,” in 2021 International Conference on Microelectronics (ICM), pp. 1–4, IEEE, 2021.
6. J. G. Pandey, T. Goel, M. Nayak, C. Mitharwal, A. Karmakar, and R. Singh, “A High-performance VLSI Architecture of the PRESENT Cipher and its Implementations for SoCs,” in 2018 31st IEEE International System-on-Chip Conference (SOCC), pp. 96–101, IEEE, 2018.
7. L. Daoud, F. Hussein, and N. Rafla, “Optimization of advanced encryption standard (AES) using vivado high level synthesis (HLS),” 2019.
8. J. Gandhi, D. Shekhawat, M. Santosh, and J. G. Pandey, “Security Evaluation of Lightweight SBoxes,” in 2023 IEEE International Symposium on Smart Electronic Systems (iSES), pp. 315–318, IEEE, 2023.
9. A. Varici, G. Saglam, S. Ipek, A. Yildiz, S. G¨oren, A. Aysu, D. Iskender, T. B. Aktemur, and H. F. Ugurdag, “Fast and Efficient Implementation of Lightweight Crypto Algorithm PRESENT on FPGA Through Processor Instruction Set Extension,” in 2019 IEEE East-West Design & Test Symposium (EWDTS), pp. 1–5, IEEE, 2019.
10. J. G. Pandey, T. Goel, and A. Karmakar, “An Efficient VLSI Architecture for PRESENT Block Cipher and its FPGA Implementation,” in VLSI Design and Test: 21st International Symposium, VDAT 2017, Roorkee, India, June 29–July 2, 2017, Revised Selected Papers 21, pp. 270–278, Springer, 2017.

Acknowledgement

- Anusandhan National Research Foundation (ANRF)
  - This work is supported by the ANRF under CRG Grant No.CRG/2023/001748

Thank You!