IEEE
International Conference
on
PKI and Its Applications
(PKIA-2017)
November 14-15, 2017

Hotel Chancery Pavilion, Bangalore

DESIGN AND IMPLEMENTATION OF IP CORE FOR ROADRUNNER-128 BLOCK CIPHER

Mitha Raj*, Shinta Joseph K*, Niveditha K.S*, Josemon Tomy*, Anna Johnson*, Nandakumar R^, Mitu Raj$

*: Jyothi Engineering College , Thrissur
^ : NIELIT, Calicut
$: CDAC ,Trivandrum

PAPER ID : 12

Overview

- ABSTRACT
- INTRODUCTION
- STRUCTURE AND DESIGN OF RRR-128
- FPGA IMPLEMENTATION
- RESULTS AND COMPARISONS
- CONCLUSION

Abstract

- **RoadRunneR-128 -** Recently invented light-weight block cipher, specifically designed for 8-bit platforms [1].

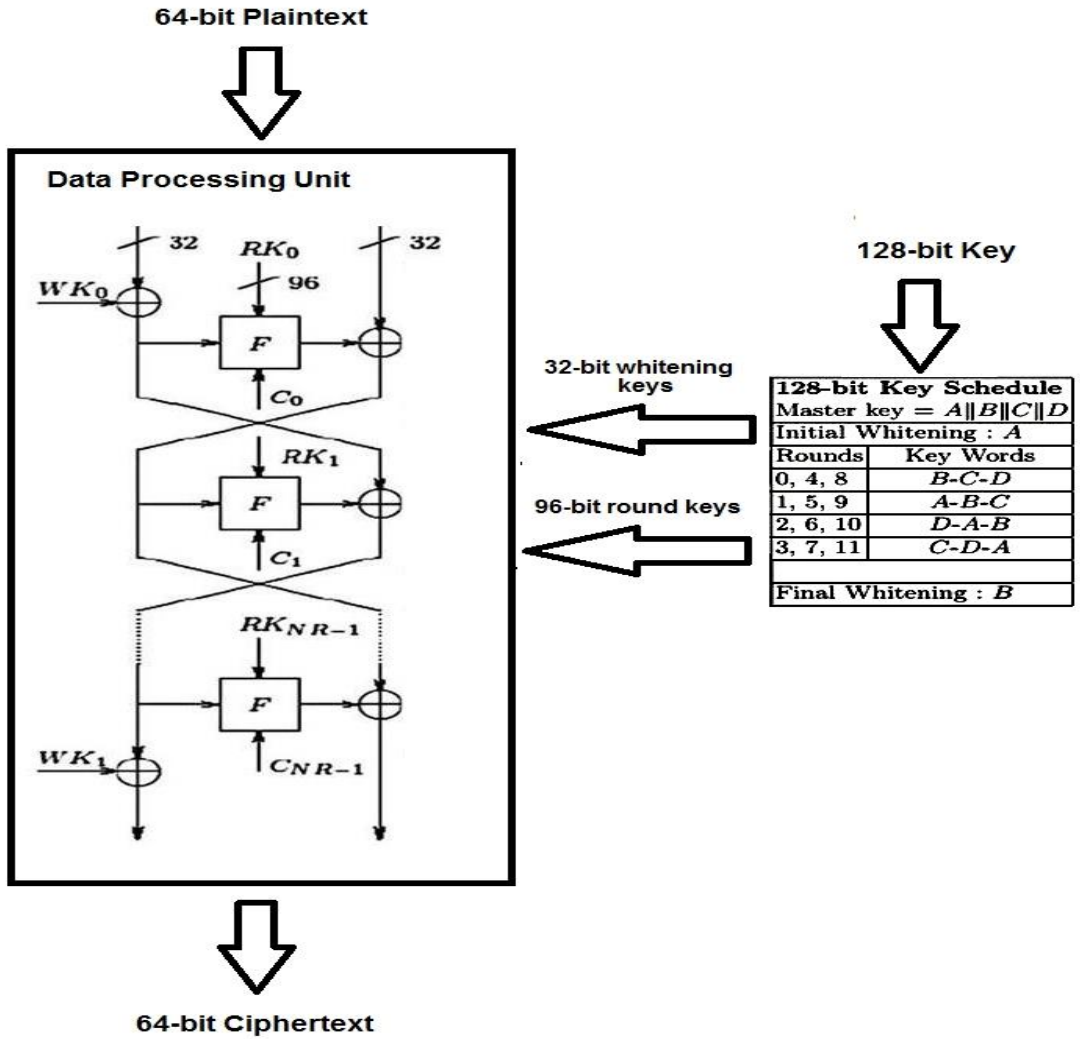
- Design and hardware implementation of IP core for RoadRunneR-128 on FPGA.

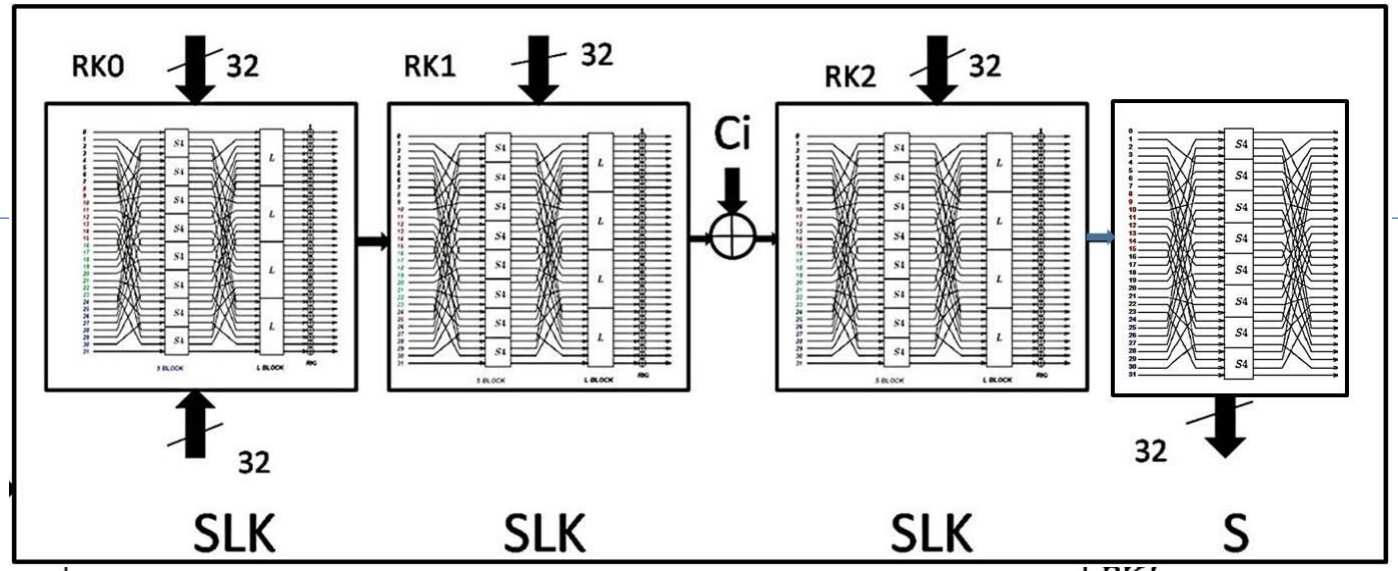
- Evaluation of performance , resource utilization and estimated power consumption of the design on FPGA.

Introduction

- **RoadRunneR-128** is a small and fast Bitslice Block cipher**.**
- Feistel structure**.**
- Key length - 128 bit, Block length - 64 bit.
- Highly optimised for software implementation on 8-bit CPUs.
- Proven security against different cryptographic attacks [1]**.**

Structure of RoadRunneR-128





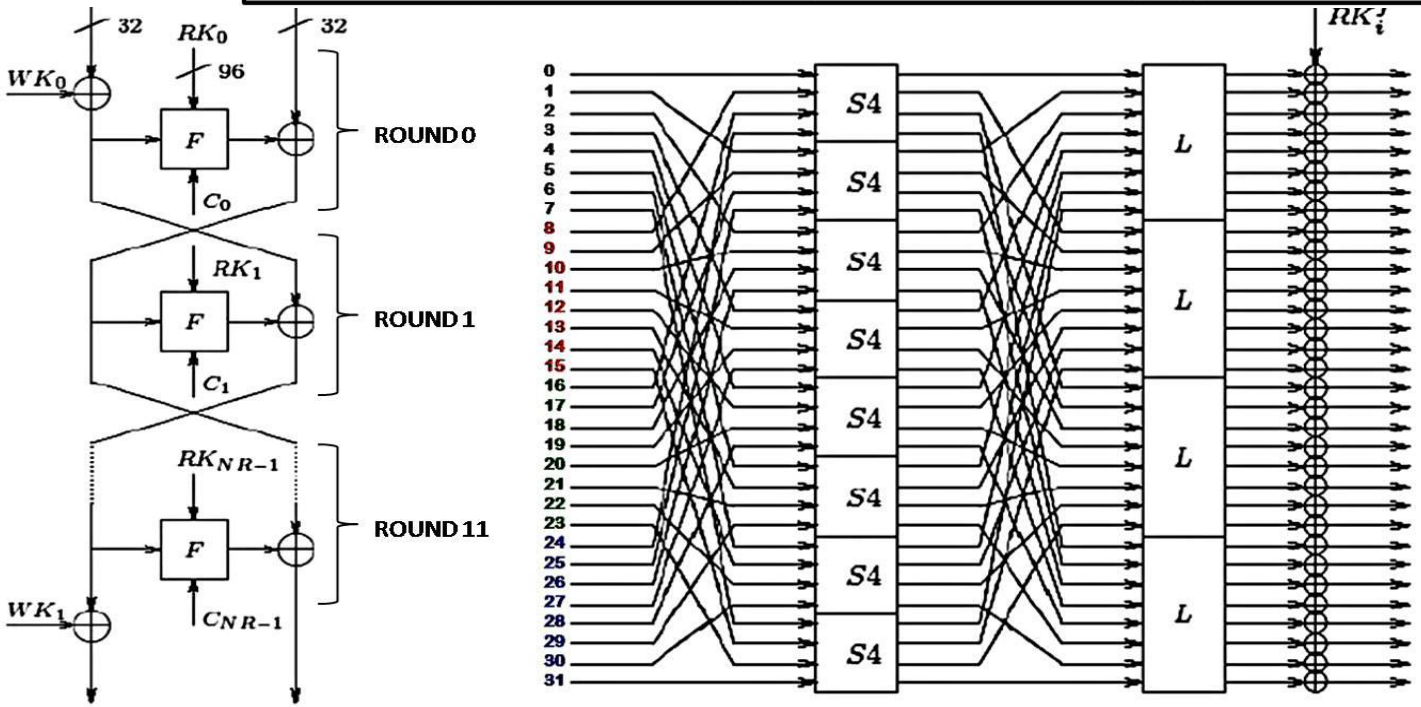
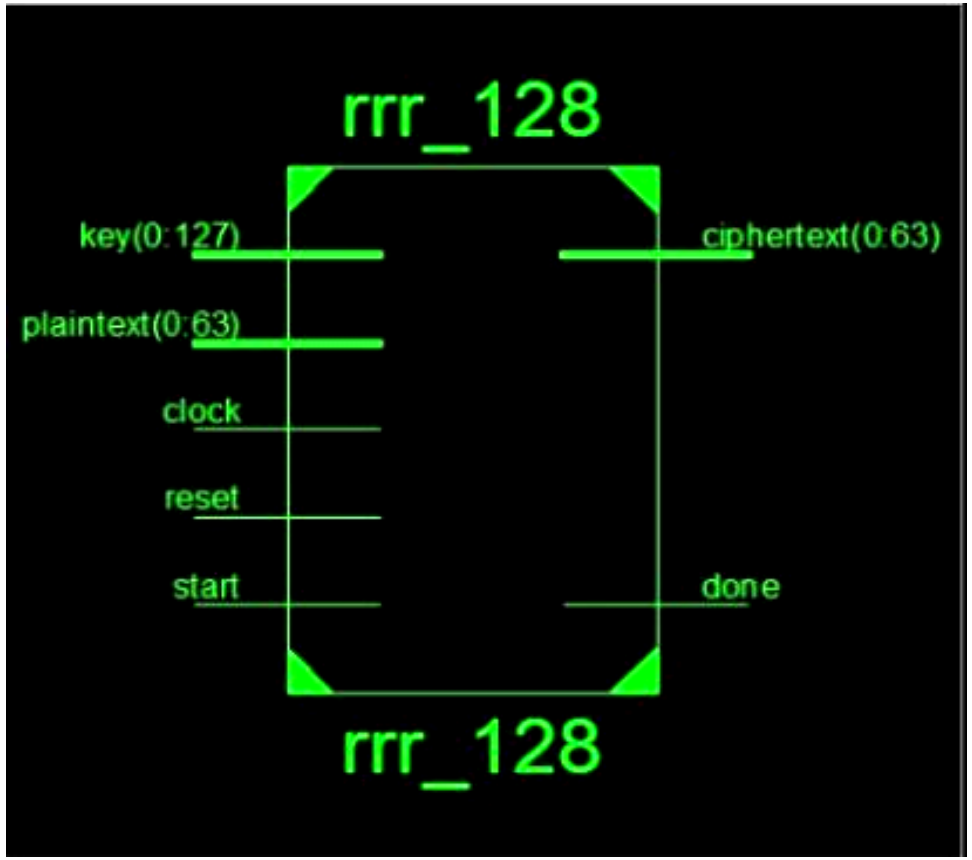


Fig.1 : Detailed diagram

RTL Design

- Data processing and key generation units.
- Designed using Verilog HDL – as finite state machine.
- Pipelining of complex logic to multiple clock cycles.
- 22 clock cycles per round.
- State encoding for low power.
- Test bench development and RTL simulation using Modelsim.

RRR-128 Core's Interface



FPGA Implementation

- Synthesized using Quartus II for Altera FPGA.
- Balanced optimization – Area and speed.
- Successfully verified the timing and analyzed the power.
- Tested in Altera DE1 Cyclone II FPGA.

Simulation and Implementation Results

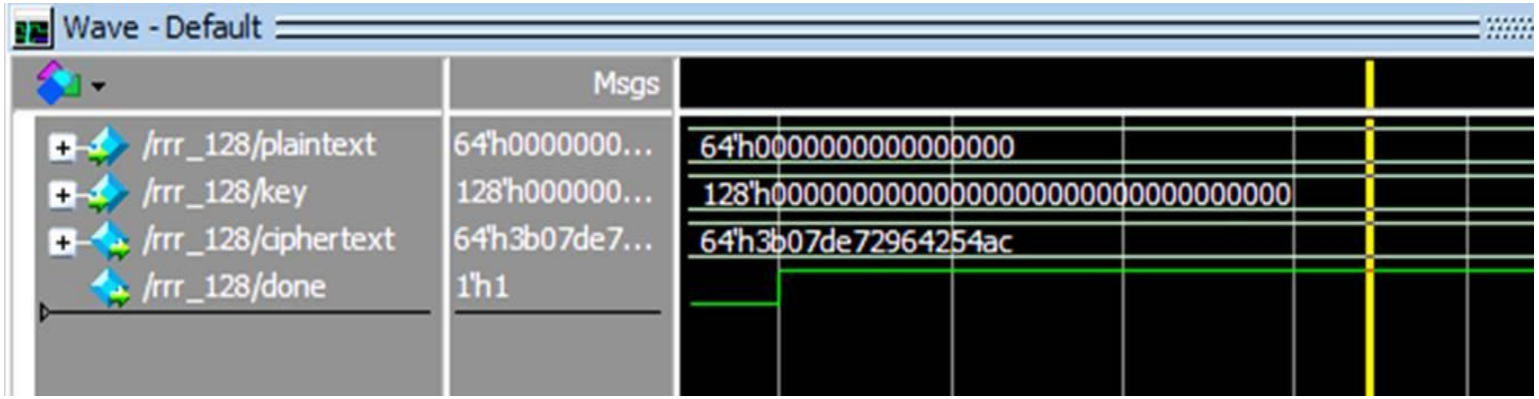


Fig. : RTL Simulation in ModelSim

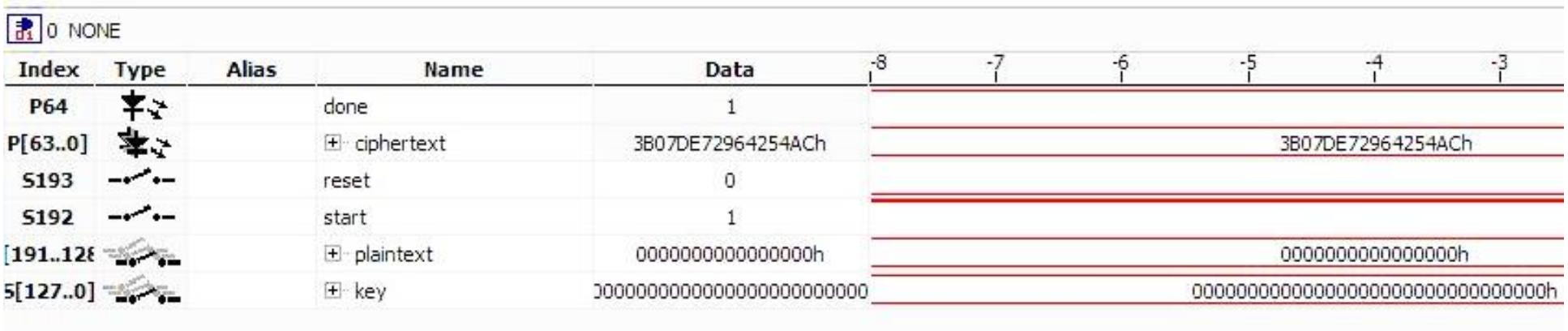


Fig. :Implementation Result in QUARTUS II In-System Memory Content Editor

Results

PERFORMANCE METRIC	
Total area	2% of the hardware (802/33216 Logic Elements)
Maximum clock frequency of operation	272.18 MHz
Estimated power consumption	140.74 mW
Clock cycles to perform the encryption	268 clock cycles
Total encryption time	0.98 µs
Throughput for the implementation	65 Mbps.
Throughput per Area Efficiency	0.081 Mbps/slice

Comparison with other ciphers

Cipher	FPGA/ASIC	Area Utilization	Throughput
RRR-128	Altera DE1 cyclone II FPGA	**2%**	65 Mbps
RRR-128 *[11]*	0.18µs CMOS - ASIC	1400 GE	156 Kbps
Triple DES *[13]*	Altera DE1 cyclone II FPGA	40%	3 Gbps
Curupira – 1 *[14]*	Altera DE1 cyclone II FPGA	40%	200 Kbps
AES-128 *[6]*	Altera DE1 cyclone II FPGA	56%	1.5 Gbps

Cipher	Attacked Rounds
RRR-128 [1]	**6/12**
AES	7/10
PRIDE	26/31
SPECK-128	17/27
PRESENT	26/31
SIMON	26/42

Test Vector Generation Tool

Fig. : RRR-128 Encryptor

Test Vectors

PLAIN TEXT	KEY	CIPHER TEXT
0000_0000_0000_0002	8000_0000_0000_0000 0000_0000_0000_0000	C168_C69A_C195_845E
0010_0020_0030_0040	0000_0000_0000_0001 0000_0000_0000_0001	3109_48CF_D78E_57B4
0010_0200_0000_0000	0001_0000_0000_0001 0001_0000_0000_0001	52BB_4E1A_331D_91BF
FEDC_3210_0002_0000	0123_4567_0000_CDEF 0123_4567_0000_CDEF	E45B_1D93_75E2_7364
1000_1002_5000_4000	1111_2222_3333_4444 1111_2222_3333_4444	0DF2_9A4F_C5BF_5BFF
1023_2050_1147_8124	1000_4000_5000_2222 1000_4000_5000_2222	BB76_8D15_1B18_616F

Conclusion

- Designed and implemented a soft IP core for RoadRunneR-128 block cipher on Altera DE1 cyclone II FPGA.
- Verified functionality and tested on-board.
- Lesser area utilization, reasonable throughput- light weight applications.
- Outperforms its previous implementation, by over 400 times in terms of throughput.
- The work is the first of its kind – further improvement in future.

References

[1] Adnan Baysal, Suhap Sahin, "RoadRunneR: A Small and Fast Bitslice Block Cipher for Low Cost 8-bit Processors," presented at *LightSec 2015*, Bochum, Germany, September 2015. Available: https://eprint.iacr.org/2015/906

[2] Andrey Bogdanov *et al*, "PRESENT: An Ultra-Lightweight Block Cipher," in *Lecture Notes in Computer Science*, vol. 4727. Springer, 2007, pp. 450–466.

[3] François-Xavier Standaert *et al*, "SEA: A scalable encryption algorithm for small embedded applications," in *Lecture Notes in Computer Science*, vol. 3928. Springer, 2006, pp. 222–236.

[4] Martin R. Albrecht *et al*, "Block ciphers - focus on the linear layer (featuring PRIDE)," in *Proc. CRYPTO 2014 - 34th Annual Cryptology Conference*, Santa Barbara, CA, USA, August 17-21, 2014, pp. 57–76.

[5] Wentao Zhang *et al*, "RECTANGLE: A bit-slice ultra-lightweight block cipher suitable for multiple platforms," IACR Cryptology ePrint Archive 2014:84, 2014. [Online]. Available: https://eprint.iacr.org/2014/084.

[6] Ana Krkljić, Branko Dokić, and Velibor Škobić, "FPGA Implementation of AES algorithm," presented at Proceedings of the 5th Small Systems Simulation Symposium 2014, Niš, Serbia, 12th-14th February 2014.

[7] Markus Ullrich *et al*, "Finding optimal bitsliced implementations of 4× 4-bit s-boxes," in *Proc. SKEW 2011 Symmetric Key Encryption Workshop*, Copenhagen, Denmark, June 2011, pp. 16-17.

[8] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici, "Ls-designs: Bitslice encryption for efficient masked software implementations," in *Proc. 21st International Workshop, FSE 2014*, London, UK, March 3-5, 2014, pp. 18-37.

References

[9] Pierre-Alain Fouque and Pierre Karpman, “Security Amplification against Meet-in-the-Middle Attacks Using Whitening,” in *Proc. IMA International conference on Cryptography and Coding*, Oxford, UK, 2013, pp. 252-269.

[10] F. Ferrandi, P. L. Lanzi, G. Palermo, C. Pilato, D. Sciuto and A. Tumeo, "An Evolutionary Approach to Area-Time Optimization of FPGA designs," in *Proc. 2007 International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation*, Samos, 2007, pp. 145-152.

[11] J. Liu, G. Bai and X. Wu, "Efficient Hardware Implementation of Roadrunner for Lightweight Application," 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, 2016, pp. 224-227.

[12] N. S. S. Srinivas and M. Akramuddin, "FPGA based hardware implementation of AES Rijindael algorithm for Encryption and Decryption," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 1769-1776.

[13] Del Rosal, Edni and Kumar, Sanjeev, “A Fast FPGA Implementation for Triple DES Encryption Scheme,” in *Circuits and Systems*, vol. 8, no. 10, pp. 237-246, August 2017.

[14] Chanthini Baskar, C. Balasubramaniyan and D. Manivannan, “Establishment of Light Weight Cryptography for Resource Constraint Environment Using FPGA,” in *Procedia Computer Science*, vol. 78, pp. 165-171, 2016.

[15] Celine Blondeau and Kaisa Nyberg, “Links between truncated differential and multidimensional linear properties of block ciphers and undelying attack complexities,” in *Proc. Advances in Cryptology – EUROCRYPT 2014 – 33rd Annual International Conference on the Theory and Applications of Cryptographic techniques*, Copenhagen, Denmark, May 11-15, 2014, pp. 165-182.

CCA

IEEE
PKIA-2017

Thank You

CDAC