INTERNATIONAL JOURNAL OF TECHO-ENGINEERING

ISSN : 2057-5688

AN AREA EFFICIENT UNIVERSAL CRYPTOGRAPHY PROCESSOR OF SMART CARD

RACHAPUTI HEMALATHA[1] K MANOJ PAVAN KUMAR[2]

[1] PG. Scholar, Department of ECE, *CHEBROLU ENGINEERING COLLEGE*, Chebrolu, Andhra Pradesh, India.

[2] Assistant Professor, Department of ECE, *CHEBROLU ENGINEERING COLLEGE*, Chebrolu, Andhra Pradesh, India.

ABSTRACT:

Cryptography circuits for smart cards and portable electronic devices provide user authentication and secure data communication. These circuits should, in general, occupy small chip area, consume low power, handle several cryptography algorithms, and provide acceptable performance. This paper presents, for the first time, a hardware implementation of three standard cryptography algorithms on a universal architecture. The microcoded cryptography processor targets smart card applications and implements both private key and public key algorithms and meets the power and performance specifications and is as small as 2.25 mm2 in 0.18- m 6LM CMOS. A new algorithm is implemented by changing the contents of the memory blocks that are implemented in ferroelectric RAM (FeRAM). Using FeRAM allows nonvolatile storage of the configuration bits, which are changed only when a new algorithm instantiation is required.

Keywords: FeRAM, 6LM CMOS, microcoded, storage.

1. INTRODUCTION:

THE rapid growth of portable electronic devices with limited power and area has opened a vast area of low-power and compact circuit design opportunities and challenges for VLSI circuit designers. Cellular phones, PDAs, and smart cards are examples of portable electronic products that are becoming an integral part of everyday life. The popularity of these devices necessitates special considerations for their security subsystems. Unlike computer network security systems that impose less stringent limitations on the area and power consumption but put more emphasis on high throughput (several Gigabit/s), portable applications demand security hardware with more restrictions on area and power and less on throughput (several hundred kilobit/s to a few Megabit/s). This difference in requirements dictates a different approach in the design and implementation of the security systems for these devices

Since next-generation, multipurpose smart cards will be used for a wide range of applications, their security system must implement both private (symmetric) and public (asymmetric) key algorithms, to accommodate various application requirements. Private key algorithms with high throughput are suitable for data communication, while public key algorithms with much lower throughput are suitable for private key exchange and authentication. Among all available algorithms, data encryption standard (DES), advanced encryption standard (AES), and elliptic curve cryptography (ECC), which are approved by standards organizations [1]–[3], are selected for this application. DES, for past compatibility, and AES, for high security and throughput, are the major candidates for private key algorithms, and ECC is the best candidate for the public key algorithm for its encryption efficiency. RSA, which is also a standard public key algorithm, is not considered in this design for three reasons. First, it is believed that 160-b ECC provides the same level of security as 1024-b RSA. Thus, ECC will be a better choice when implementation area is a key factor in the design. Second, RSA uses binary addition of large numbers and needs binary adders that are either slow for carry propagation or large for look-ahead carry generation. Third, a larger number of bits in RSA means wider buses, which adds to the area and power consumption of the design, both of which are scarce resources in smart cards.

A cryptography system can be implemented in either software or hardware. Software implementations allow multiple algorithms to be supported on the same hardware platform, but they are usually slow and cannot meet the required specifications. Moreover, they are considered to be more vulnerable to side-channel attacks compared to other implementations. Side-channel attacks use physical measurements on the device, for example, the power consumption of the processor, to detect the encryption/decryption key [4]–[6]. On the other hand, hardware implementations which support high throughput do not allow for flexibility and, hence, are not suitable for smart cards. Flexible field-programmable gate array (FPGA) implementations are not a good choice either, because they need large area and power which cannot be supported on smart cards.

Based on the physical constraints for smart cards set by the International Standard Organization (ISO) [7], the maximum chip area on a smart card is limited to 25 mm. Considering the nonvolatile and volatile memories, CPU, and other peripheral circuits required on the chip, it is desirable to fit the security subsystem in as small an area as possible. One of the objectives of this study is to investigate the minimum required chip area for the implementation of the security circuits satisfying the algorithm agility, power consumption, and throughput requirements.

2. LITERATURE SURVEY:

This chapter has the survey of the work done by various researchers in the field of encryption algorithm. The possibility of improvement in the work and motivation has been stated clearly. There is also a brief description of some of the encryption algorithms which are used for encrypting and decrypting in different systems.

Data Encryption Standard (DES) is the most well-known cryptographic mechanism in history [1]. It begins with the work of Feistel at IBM in the early 1970s and culminating in 1977 with the adoption as a U.S. Federal Information Processing Standard for encrypting unclassified information. The most striking development in the history of cryptography came in 1976 when Diffie and Hellman published a transaction [2]. Before the modern era, cryptography was concerned solely with message confidentiality i.e. encryption conversion of messages from the comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable without secret knowledge. In recent decades, the field has expanded beyond confidentiality concerns to include techniques for authentication, digital signatures, interactive proofs, and secure computation.

Ruth M. Davis [3] provides a hardware-implementable algorithm for enciphering data, which has been adopted as a Federal standard to provide a high level of cryptographic protection against various attacks.

WhitfleldDiffieet. al [4] describes cryptographic technology, which examines the forces driving public development of cryptography. The paper describes how one can secure the message over the telephone lines.

Ingrid Verbauwhede [5] described Security and Performance Optimization of a New DES Data Encryption Chip. Novel CAD tools are used at different steps in the design process for simulation. The result is a single chip of 25 mm in 3-pm double-metal CMOS. Functionality tests show that a clock of 16.7 MHz can be applied, which means that a 32-Mbit/s data rate can be achieved for all eight byte modes.

James E. Katz [6] provides Social Aspects of Telecommunications Security Policy that describes a system that offers a variety of convenient and powerful services while meeting the legitimate needs of the individual for privacy and of society for security.

H. Bonnenbergt [7] described the VLSI implementation of a new block cipher. The chip that runs with a maximum clock frequency of 33 MHz permitting a data conversion rate of more than 55 Mbits/s performs data encryption and decryption in a single hardware unit.

K.H. Mundt [8] presented superscript ASIC technology that facilitated a new device family for data encryption in which semi-custom cell-based ASIC technology is described to get 100Mbits/ s encryption speed on silicon applying 1 micron design rules.

C. Boyd [9] provides the modern data encryption in which proposed standard for digital signatures based on RSA were introduced. A. Curigert describes VINCI: VLSI Implementation of the new secret-key block Cipher IDEA. VINCI's IDEA premier silicon realization, integrates high-speed encryption and decryption, comprehensive key management functions, and all standardized cipher modes of operation in their ordinary and high-speed adapted versions.

3. PROPOSED SYSTEM:

In this section, a brief introduction of the three implemented algorithms which are essential in the understanding of the remainder of the paper are provided. Interested readers are referred for additional details.

Data Encryption Standard (DES)

This is a well-established algorithm that has been used for more than two decades (since 1977) in military and commercial data exchange and storage. The algorithm is designed to encipher and decipher blocks of data consisting of 64 b using a 56-b key. A block to be enciphered is subjected to an initial permutation (IP), then to 16 rounds of a complex key-dependent permutation, and, finally, to another permutation which is the inverse of the IP, , as shown in Fig. 1. The function f() in this figure is the heart of this algorithm and consists of an expansion, XOR, lookup table (LUT), and permutation, as depicted in Fig. 2. To decipher, it is necessary to apply the very same algorithm to an enciphered message block, using the same key.

Since the processing power of current computers is much higher than those of two decades ago, a brute-force attack (checking all possible key combinations to decipher an encrypted ciphertext) to this algorithm is possible in a relatively short time (possibly as short as a few minutes [21]). For this reason, this algorithm is no longer considered to be a secure algorithm for many applications by the National Institute of Standards and Technology (NIST). A more secure algorithm based on DES which is still supported by NIST is called the triple data encryption algorithm (Triple DES, 3DES, or TDEA) depicted in Fig. 3. In this figure, DES represents encryption and represents decryption. 3DES involves applying DES, then , followed by a final DES to the plain text using three different key options [1], which results in a cipher text that is much harder to break.

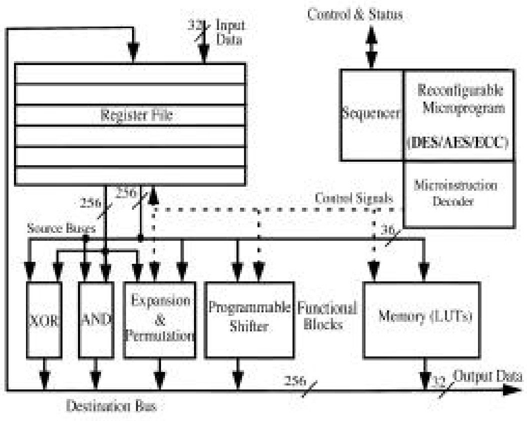


Fig. 6. Detailed cryptoprocessor architecture.

4. RESULTS EXPLANATION

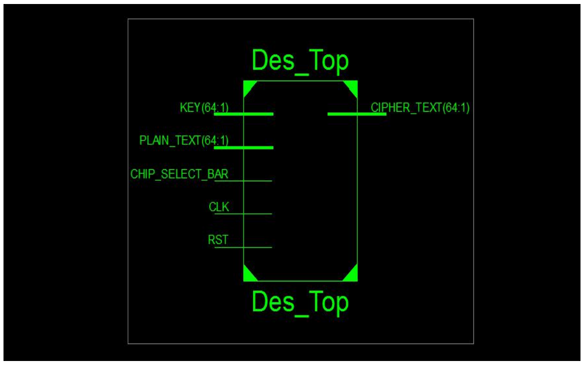


Fig.4.1. RTL diagram.

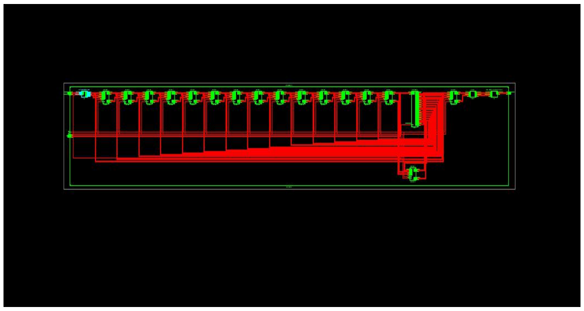
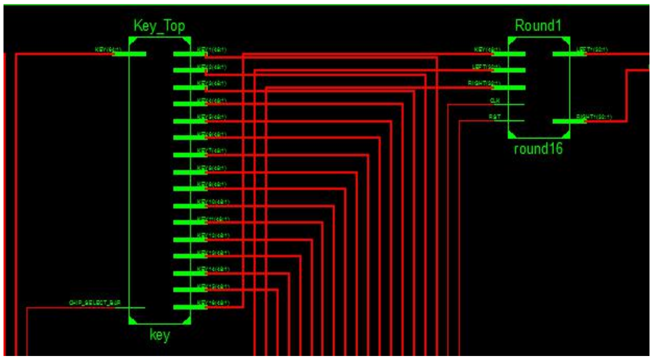


Fig.4.2. schematic diagram.



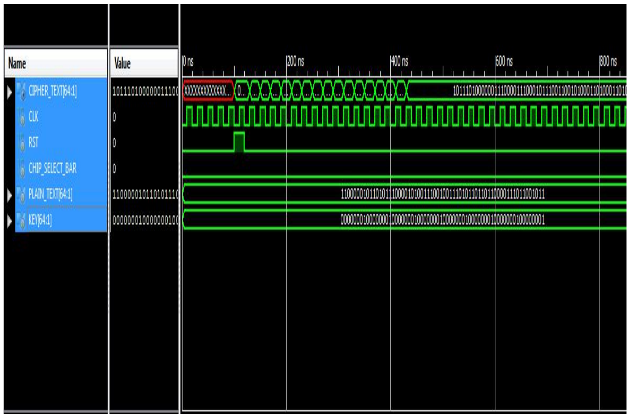


Fig.4.3.Simultion results.

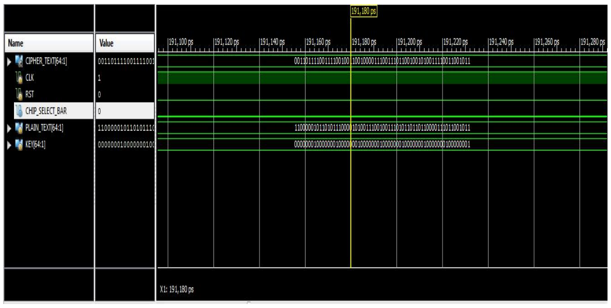


Fig.4.4.Simulation results.

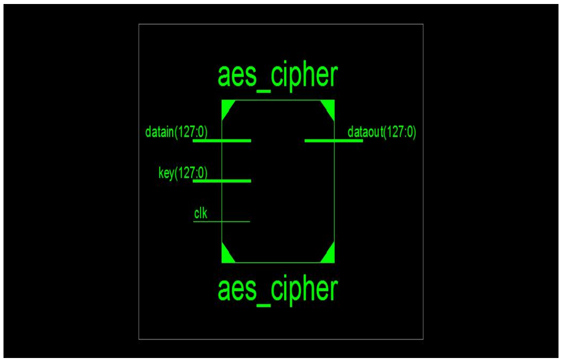


Fig.4.5. AES

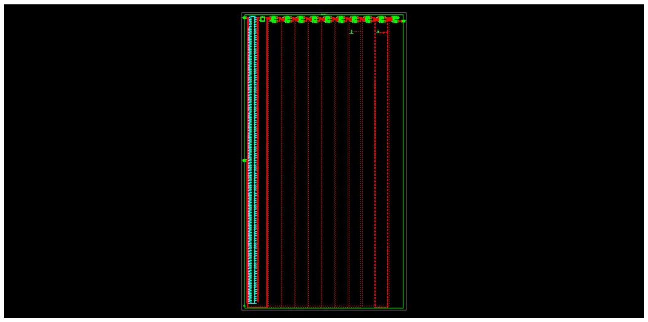


Fig.4.6. Model diagram.

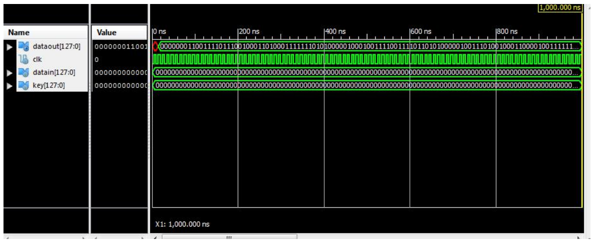
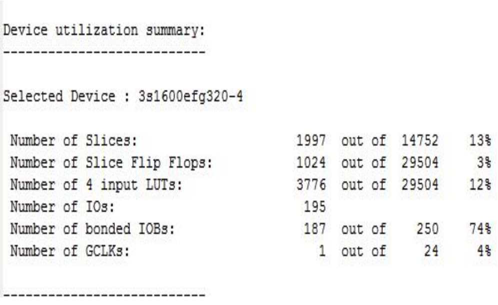


Fig.4.7. FINAL AREA

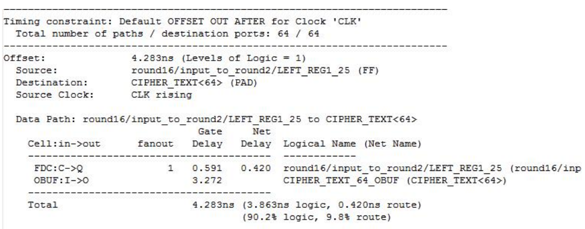


```
Device utilization summary:
---------------------------


Selected Device : 3s1600efg320-4


 Number of Slices:                    1997  out of  14752    13%
 Number of Slice Flip Flops:          1024  out of  29504     3%
 Number of 4 input LUTs:              3776  out of  29504    12%
 Number of IOs:                        195
 Number of bonded IOBs:                187  out of    250    74%
 Number of GCLKs:                        1  out of     24     4%


---------------------------
```



```
---------------------------------------------------------------------------
Timing constraint: Default OFFSET OUT AFTER for Clock 'CLK'
  Total number of paths / destination ports: 64 / 64
---------------------------------------------------------------------------
Offset:              4.283ns (Levels of Logic = 1)
  Source:            round16/input_to_round2/LEFT_REG1_25 (FF)
  Destination:       CIPHER_TEXT<64> (PAD)
  Source Clock:      CLK rising

  Data Path: round16/input_to_round2/LEFT_REG1_25 to CIPHER_TEXT<64>
                                Gate     Net
    Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
    ----------------------------------------  ------------
     FDC:C->Q              1   0.591   0.420  round16/input_to_round2/LEFT_REG1_25 (round16/inp
     OBUF:I->O                 3.272          CIPHER_TEXT_64_OBUF (CIPHER_TEXT<64>)
    ----------------------------------------
    Total                      4.283ns (3.863ns logic, 0.420ns route)
                                       (90.2% logic, 9.8% route)
```

Fig.4.8. TIME DELAY

5. CONCLUSION:

This design presents, for the first time, a universal cryptography processor for smart-card applications that supports both private and public key cryptography algorithms. We achieved this by expressing the primitives of three important algorithms for smart cards (DES, AES, and ECC) in terms of simple logical operations that maximize the number of common blocks among them. This approach resulted in a cryptoprocessor that meets the power consumption and performance specifications of smart cards and occupies 2.25 mm in 0.18- m CMOS when SRAM memory blocks are used. This area represents just 9% of the maximum available smart-card die area of 25 mm . Using FeRAM instead of SRAM memory blocks provides nonvolatile configuration at no extra area overhead.

REFERENCES:

[1] Data Encryption Standard (DES), Oct. 1999. Fed. Inf. Process. Standards Pub..

[2] Advanced Encryption Standard (AES), Nov. 2001. Fed. Inf. Process. Standards Pub..

[3] IEEE Standard Specifications for Public-Key Cryptography, Jan. 2000.

[4] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Investigation of power analysis attacks on smartcards," in Proc. USENIX Workshop Smartcards Technology, Chicago, IL, May 1999, p. 151 and 161.

[5] K. Okeya and K. Sakurai, "A multiple power analysis breaks the advanced version of the randomized addition-subtraction chains countermeasure against side channel attacks," in Proc. IEEE Inf. Theory Workshop, 2003, pp. 175–178.

[6] S. B. Ors, F. Gurkaynak, E. Oswald, and B. Preneel, "Power-analysis attack on an ASIC AES implementation," in Proc. Inf. Technol.: Coding Computing, vol. 2, 2004, pp. 546–552.

[7] Smart Cards Standards, 1995–2004. Int. Standard Org..

[8] International Standard Organization/International Electrotechnical Commission ISO/IEC 14 443 standard.

[9] [Online]. Available: http://www.mips.com/ProductCatalog/P_MIPS324KFamily/productBrief

[10] J. Goodman and A. P. Chandrakasan, "An energy-efficient reconfigurable public-key cryptography processor," IEEE J. Solid-

State Circuits, vol. 36, no. 11, pp. 1808–1820, Nov. 2001.

[11] P. H. W. Leong and I. K. H. Leung, “A microcoded elliptic curve processor using FPGA technology,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 10, no. 5, pp. 550–559, Oct. 2002.

[12] J. H. Kim and D. H. Lee, “A compact finite field processor over GF(2 m) for elliptic curve cryptography,” in Proc. ISCAS, vol. 2, pp. 340–343.

[13] S. Masui, T. Ninomiya, M. Oura, W. Yokozeki, K. Mukaida, and S. Kawashima, “A ferroelectric memory-based secure dynamically programmable gate array,” IEEE J. Solid-State Circuits, vol. 38, no. 5, pp. 715–725, May 2003.