IPASJ International Journal of Electrical Engineering (IIJEE)
Web Site: http://www.ipasj.org/IIJEE/IIJEE.htm
A Publisher for Research Motivation..... Email: editoriijee@ipasj.org
Volume 5, Issue 2, February 2017 ISSN 2321-600X

PROPOSE AND REALIZATION OF AN ASIP-BASED CRYPTO PROCESSOR FOR IDEA AND SAFER K-64

Miss. Puja Pancholi

Indian Institute of Technology, Patna

ABSTRACT

A New crypto processor is planned during this paper for International encryption algorithmic program (IDEA), and Secure And quick secret writing Routine with 64-bit Key (SAFER K- 64). The utilised platform relies on Application Specific Instruction set Processors (ASIP). Instruction set consists of each general purpose and specific directions for cryptography. each secret writing and coding functions area unit enforced for plan. additionally, either six or eight rounds may be selected once SAFER K-64 is used. coming up with method for all of the most important parts among the processor core is given thoroughly. the entire instruction set is written in Register remodel Language (RTL). Then, the whole processor is simulated, tested and enforced victimisation synthesizable structural VHDL code.

I. INTRODUCTION

I NTERNATIONAL encryption algorithmic program (IDEA) was initial delineated by X. Lai and J. L. Massey in 1991 [1]. it had been originally known as Improved planned secret writing normal (IPES), and it had been given as another to encryption normal (DES). It falls into the class of radial block scientific discipline algorithms. it's radial, as a result of the subkeys necessary for coding area unit accomplishable from the secret writing ones by an easy transformation. On the opposite hand, block ciphering attribute implies that it operates on a fixed-length cluster of bits. It takes a 64-bit plaintext along side associate degree initial non-public 128-bit key as inputs, associate degreed it returns 64- bit ciphertext as an output. The initial 128-bit key provides a key area of two 128. However, plan is classed as weak keys thanks to terribly straightforward key schedule. this suggests a really tiny fraction of key area is painted in apply. the entire method consists of eight reiterative identical sphericals along side a final round. Secure And Fast Encryption Routine, with 64-bit Key (SAFER K-64) is another block cipher algorithm which was first presented by J. L. Massey in 1993 [2]. It takes a 64- bit plaintext as well as an initial private 64-bit key, and it returns the same block length ciphertext. The original version is composed of six iterative rounds together with a final round. Following recommendations use either eight or ten rounds.

Many different structures have been proposed in the literature [3-6] in order to implement IDEA cryptographic algorithm. Different parallel techniques [7] as well as various architectures such as both serial and parallel implementations [8] have also been presented. additionally, a crypto processor has been introduced in [9], which implements different cryptographic algorithms including IDEA. However, generating subkeys is omitted as the presented processor does not support division and modulo arithmetic. Eventually, several modular arithmetic implementations have also been presented to accelerate the required operations [10, 11]. Application Specific Instruction set Processors (ASIPs) are the alternative programmable platforms compared to traditional Application Specific Integrated Circuits (ASICs). ASIP makes a balance between cost and speed, while todays deep submicron geometries brings about manufacturing problems in terms of cost and complexity [12]. On the other hand, ASIPs benefit from having specific instructions to execute a special task faster in comparison to general purpose processors. In ASIP, the entire task divides into both hardware and software aspects. It combines the best of two worlds, and hence it has the advantage of both software flexibility and hardware efficiency at the same time [13]. In this paper, the ASIP-based IDEA crypto processor presented in [14] is modified in order to support both IDEA and SAFER K-64 crypto algorithms. Designing process for both algorithms is presented with all the specifics. additionally, the whole extended processor is simulated, tested, and implemented on FPGA. The instruction set follows the main concept of ASIP, and thence it consists of each general purpose further as specific directions for cryptography. All the directions area unit written in Register Transfer Language (RTL) considering most RTL-level similarity. each secret writing and coding functions area unit enforced for plan in spite of the absence of dividing operator. Moreover, it's attainable for a code developer to settle on either six or eight intermediate rounds for SAFER K-64. The planned style advantages from code programmability and low hardware complexness. the remainder of the paper is organized as follows: Section a pair of

consists of a quick outline of each plan and SAFER K-64 algorithms. The planned ASIP processor is comprehensively given in section three through 5 subsections. Section four contains simulation, test, and implementation results. Finally, section five concludes the paper.

II. PLANNED DESIGN

A. the most Specific directions the particular directions area unit those that area unit dedicated for secret writing. every intermediate spherical in plan is taken into account as a particular instruction and it's known as plan programmer (ICO). the ultimate spherical is additionally taken into consideration as another specific instruction known as plan Final programmer (IFC). identical construct is used for the second crypto algorithmic program. SAFER K-64 programmer (SCO), and SAFER K-64 Final programmer (SFC) area unit 2 outlined specific directions for the second algorithmic program. The coder might choose the popular technique for secret writing. To encipher initial 64-bit plaintext, the programmer instruction has got to be dead r times. The r parameter for plan is eight, and for SAFER K-64 might be either six or eight. As mentioned before, it's up to program designer to pick the amount of iterations just in case SAFER K-64 is chosen. the right Final programmer instruction has got to be dead further.

ALSU configuration for crypto processor supporting each plan and SAFER K-64 algorithms is delineate in Fig. 3. The Xi ($0 \leq i \leq 3$) specific registers area unit additional to save lots of intermediate results made once every spherical. Moreover, the Ki ($0 \leq i \leq 7$) specific registers area unit additional with the aim of holding subkeys required for every spherical. Therefore, it's not needed to confer with the memory whereas death penalty the programmer and also the Final programmer directions. It ends up in fewer range of Clock cycles Per Instruction (CPI) and consequently higher turnout. the whole instruction set (Appendix B) is written in Register Transfer Language (RTL). most RTL-level similarity is taken into consideration to use each native and shared buses at the same time to a attainable extent in one clock cycle. The CPI for the ICO instruction is fifty five (T0 to T54) as well as Fetch, Decode, and Execute cycles. Therefore, a 6-bit Sequence Counter (SC) is required. Bitwise XOR, modulo-216 addition, and modulo 216+1 multiplication area unit the 3 operations among the entire plan algorithmic program. A 16-bit adder is adequate perform modulo addition. The output carry has got to be eliminated during this case. However, modulo multiplication is way a lot of sophisticated. Meier associate degreed Zimmermann have given an algorithmic program as an answer [15], that offers the simplest performance [16].

2) SAFER K-64: in contrast to ICO, the SCO instruction encompasses a larger range of operations. though most RTLlevel similarity has taken into consideration, 119 clock cycles area unit still needed to end the instruction. To avoid enlarging the present sequence counter, a secondary 6-bit counter is supplemented. once the primary SC (T) reaches the last attainable range (T63), the second (T') starts investigating from zero, and also the initial one is disabled. 2 dominant flags (T63- Flag and T'-Flag) area unit wont to avoid conflict between RTL conditions. the subsequent RTLs confirm however the usage of the second counter is feasible. once the second counter starts operational, the primary SC is disabled and it remains at the 63rd state (T63). If T63-Flag='1', it indicates that it's the last time that the primary SC (SC1) is employed. Otherwise, the second SC (SC2) is operating. In addition, when SC1 reaches 63, the value of SC2 is unknown and hence, there is a possibility for conflict. The T'-Flag is only activated when the first counter is disabled. Therefore, similar conditions are differentiated this way.

B. Other Specific Instructions and Instruction Types

Other than the instructions which are required for encryption, other specific instructions are also needed for load and store procedures. Considering both algorithms, the subkeys of each round have to be loaded from memory to the Ki registers. The initial plaintext has to be loaded to the Xi registers, and vice versa the obtained ciphertext has to be stored to the memory. IDEA Load Data (ILD) and IDEA Load Keys (ILK) are two specific instructions for loading plaintext and subkeys, respectively. The ILD loads four successive memory rows to Xi ($0 \leq i \leq 3$) registers. The ILK loads six successive memory rows to Ki ($0 \leq i \leq 5$) registers. The IDEA Store Data (ISD) stores X0 to X3 registers in 4 successive memory rows. The SAFER K-64 Load Data (SLD), SAFER K-64 Load Keys (SLK), and SAFER K-64 Store Data (STD) have the similar function as the ones presented for IDEA. However, 16 subkeys have to be loaded for each round of SAFER K-64. The existing eight Ki registers are adequate to save all 16 subkeys of one round due to the fact that the subkeys are byte oriented. Therefore, two subkeys are able to be saved in one register. Although it is possible to save the eight input blocks in X0 to X3, four other specific registers (X4 to X7) are added as an act of simplification. This also leads to CPI reduction for SCO and SFC instructions. Although the second byte of Xi ($0 \leq i \leq 7$) registers does not utilized, both plaintext and ciphertext are stored in both bytes of memory rows to reach maximum memory utilization. assumptive the higher than directions area unit programmed within a loop, the particular address is calculated by equivalent. 1, during which N is that the range of iterations in an exceedingly loop, V could be a counter

variable that is initial adequate N associate degreed it decreases one unit whenever an iteration ends, and m is that the range of serial memory words associated with either load or store directions. The m parameter is four for ILD, ISD, SLD, and SSD. It equals 6(8) for ILK(SLK). The N parameter is saved in ACL register and it's to be set zero whenever the directions aren't within a loop.

III. TAKE A LOOK AT AND IMPLEMENTATION

The planned crypto system is delineate in Fig. 8. The given crypto processor supports general purpose along side specific directions for each plan and SAFER K- sixty four. Synthesizable structural VHDL code is employed to check and implement the given structure. The secret writing and coding take a look at vectors given in [21] area unit used to check the concept cryptography. The take a look at vectors (plaintext, initial key, and ciphertext) in positional representation system area unit as follows. the alternative operation ends up in getting identical plaintext. In addition, the subsequent code has got to be programmed so as to encipher a 64-bit plaintext with plan. Addr1 is that the memory address from that the initial key's hold on. The plaintext is hold on in memory from address Addr2. The obtained ciphertext is hold on to the memory address Addr3. Finally, Addr4 is that the address wherever the counter variable is saved.

IV. CONCLUSION

The IEK instruction generates all the secret writing subkeys. Since solely 64-bit information area unit to be encrypted, the ILD instruction isn't utilised within a loop and also the passed parameter is zero. In addition, ACL register has initial to be cleared. A counter variable is required so as to make a loop that rotates eight times. Therefore, ACL is loaded with the amount 8. Within the loop, ILK loads six subkeys to the Ki registers, and ICO performs one round of IDEA. Then, the counter variable decreases one unit and if it becomes zero, it is the end of loop. The last subkeys are loaded and IFC performs the final round. At last, the encrypted data are stored in memory.

REFERENCES

[1]. A new ASIP-based crypto processor has been presented in this paper supporting two cryptographic algorithms (IDEA and [1] X. Lai and J.L. Massey, “A proposal for a new block encryption standard”, Advances in Cryptology-EUROCRYPT90, Berlin, Germany: Springer-Verlag, pp. 389-404, 1991.
[2]. J.L. Massey, “SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm”, Cambridge Security Workshop Proceedings on Fast Software Encryption, pp. 1-17, 1993.
[3]. A. Hamalainen, M. Tomminska, and J. Skytta, “6.78 gigabits per second implementation of the IDEA cryptographic algorithm”, 12th International Conference on Field Programmable Logic and Applications, pp. 760-769, 2002.
[4]. S. Wolter, H. Matz, A. Schubert, and R. Laur, “On the VLSI implementation of the international data encryption algorithm IDEA”, Symposium on IEEE International Circuits and Systems, ISCAS95, Seattle, WA, USA, pp. 397-400, 1995.
[5]. I. Gonzalez, S. Lopez-Buedo, F.J. Gomez, and J. Martinez, “Using partial reconfiguration in cryptographic applications: an implementation of the IDEA algorithm”, 13th International Conference on Field Programmable Logic and Application, pp. 194-203, 2003.
[6]. N. Sklavos and O. Koufopavlou, “Asynchronous low power VLSI implementation of the International Data Encryption Algorithm”, IEEE eight th International Conference on natural philosophy, Circuits and Systems, ICECS01, Vol. 3, pp. 1425-1428, 2001.
[7]. J.M. Granado, M.A. Vega-Rodriguez, J.M. Sanchez-Perez, and J.A. Gomez-Pulido, “IDEA and AES, 2 scientific discipline algorithms enforced victimisation partial and dynamic reconfiguration”, electronics Journal, Vol. 40, No. 6, pp. 1032-1040, June 2009.
[8]. O.Y.H. Cheung, K.H. Tsoi, M.P. Leong, and M.P. Leong, “Tradeoffs in Parallel and Serial Implementations of the International encryption algorithmic program IDEA”, In Proceedings of the scientific discipline Hardware and Embedded Systems Workshop, CHES, Paris, pp. 333-347, 2001.
[9]. R. Buchty, Cryptonite A Programmable Crypto Processor design for Hih-Bandwidth Applications, PhD thesis, Technische Universitat Munchen, LRR, Sep. 2002.
[10]. R. Modugu, Y.-B. Kim, and M. Choi, “Design and performance mensuration of economical plan (International encryption Algorithm) crypto-hardware victimisation novel standard arithmetic components”, Instrumentation and Measurements Technology Conference (I2MTC), Austin, TX, pp. 1222-1227, 2010
[11]. SAFER K-64). BUS configuration, ALS unit, and register banks have been altered with the aim of reducing clock cycles for major specific instructions and reaching a low-complex design at the same time. The FPGA-based .