8-27-2019

Implementing a lightweight Schmidt-Samoa cryptosystem (SSC) for sensory communications

Qasem Abu Al-Haija
Tennessee State University

Ibrahim Marouf
King Faisal University

Mohammad M. Asad
University of Bristol

Kamal Al Nasr
University of Texas at San Antonio

Recommended Citation

Qasem Abu Al-Haija, Ibrahim Marouf, Mohammad M. Asad, Kamal Al Nasr, "Implementing a lightweight Schmidt-Samoa cryptosystem (SSC) for sensory communications", International Journal on Smart Sensing and Intelligent Systems. Volume 12, Issue 1, Pages 1-9, DOI: https://doi.org/10.21307/ijssis-2019-006

exeley INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS

Article | DOI: 10.21307/ijssis-2019-006 Issue 1 | Vol. 12 (2019)

Implementing a lightweight Schmidt-Samoa cryptosystem (SSC) for sensory communications

Qasem Abu Al-Haija[1,*], Ibrahim Marouf[2], Mohammad M. Asad[3] and Kamal Al Nasr[4]

[1]Department of Computer Information and Systems Engineering, Tennessee State University, Nashville, TN.

[2]Department of Electrical Engineering, King Faisal University, Al-Hofuf, 31982, Al-Ahsa, Saudi Arabia.

[3]Department of Electrical and Electronic Engineering, University of Bristol, Bristol, BS8, 1QU, UK.

[4]Department of Computer Science, University of Texas at San Antonio, San Antonio, 78249, TX.

*E-mail: qabualha@my.tnstate.edu

This paper was edited by Silvia Diaz.

Received for publication May 12, 2019.

Abstract

One of the remarkable issues that face wireless sensor networks (WSNs) nowadays is security. WSNs should provide a way to transfer data securely particularly when employed for mission-critical purposes. In this paper, we propose an enhanced architecture and implementation for 128-bit Schmidt-Samoa cryptosystem (SSC) to secure the data communication for wireless sensor networks (WSN) against external attacks. The proposed SSC cryptosystem has been efficiently implemented and verified using FPGA modules by exploiting the maximum allowable parallelism of the SSC internal operations. To verify the proposed SSC implementation, we have synthesized our VHDL coding using Quartus II CAD tool targeting the Altera Cyclone IV FPGA EP4CGX22CF19C7 device. Hence, the synthesizer results reveal that the proposed cryptographic FPGA processor recorded an attractive result in terms of critical path delay, hardware utilization, maximum operational frequency FPGA thermal power dissipation for low-power applications such as the wireless sensor networks.

Keywords

Cryptography, Computer arithmetic, Schmidt-Samoa Cryptosystem, Wireless sensors.

The technology of wireless sensor networks (WSNs) is in the front part of the investigation of the computer networks and it could be the next technologic market of a huge sum of money. A WSN contains hundreds to thousands of small sensors where these sensors are designed to be self-organized wireless networks. A sensor node is usually a node for sensing, a router node is a node for relaying data, and a base station node is a node for exchanging data with other networks, also known as sink node. Figure 1 shows the structure of the wireless sensor network system (Yang, 2014). The information (data) are accumulated from the sensor node about the physical change and then transmitted to the base station (sink node), which is connected to the cyber world or the satellite network. The collected data are finally received by an application through the cyber world or the satellite network. It is not a requirement that sensor nodes have constant location usually majority of them are randomly set out to monitor a sensor field. The communication between sensor nodes mostly happened via an on-board transceiver. Each sensor node consists of power supply, microcontroller, transducer, and a transceiver. The transducer formulates electrical signals relative to the sensed physical phenomena or natural variations. The microcontroller process and store the generated electrical signal. The transceiver receives and transmits commands from a task manager node usually a computer.

Sensor nodes have limited processing power, storage, bandwidth, and energy. This limitation makes provision of the security in sensor networks not an easy task (Polastre et al., 2004). A WSN has no fixed infrastructure; the sensor nodes are

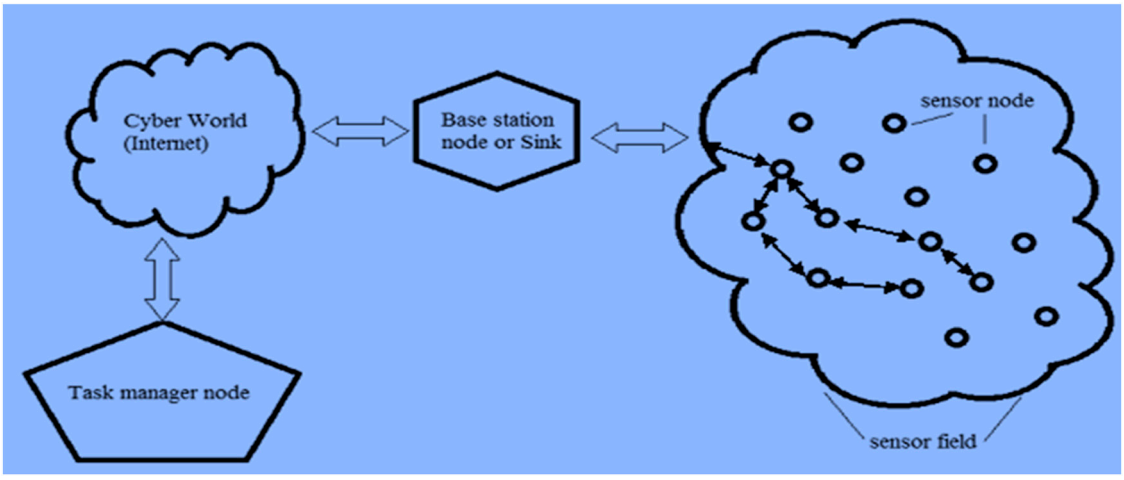

Figure 1: The structure of common wireless sensor network, where sensor nodes can talk to one or more neighboring nodes.

scattered in a special domain, which makes the network threatened by attackers in many ways of attacking (Radzevych and Mathew, 2003). For this reason, an efficient approach must be proposed in order to make WSNs secure. The applicable distribution techniques use the key management techniques (Wu and Tseng, 2006) – such as cryptographic public key to provide security issues. Public key schemes (Paar and Pelzl, 2010) are preferred to use due to many reasons such as the non-existence of the secure communication channels. Schmidt-Samoa cryptosystem (SSC) (Abu Al-Haija et al., 2018a) is an example of a public key cryptosystem that can be used to secure data transmission over non-secure communication networks.

SSC is an asymmetric cryptographic technique that is significantly based on modular arithmetic involving large prime number used for data encryption and decryption. The usage of the large prime number and modular arithmetic is to provide different security services such as confidentiality, integrity, authentication, and non-repudiation. The security of the SSC algorithm is considerably based on the difficulty of its integer factorization problem in which an integer is decomposed to its product of smaller numbers (usually prime numbers). The complexity in this method arises when factoring a very large number because there is no such known efficient algorithm. Although SSC is proved to be very secure (Samoa, 2006), there is no such a perfect system. SSC is vulnerable to some known attacks such as Brute-force attack, Man-in-the-Middle attack, and Side Channel attack. Generally, all public key cryptography algorithms suffer from these attacks (Abu Al-Haija et al., 2018a).

In this paper, we are proposing a lightweight parallelized architecture of 128-bit SSC Cryptosystem for wireless sensor communications. To verify the proposed architecture, we have implemented the proposed crypto algorithm using VHDL (LaMeres, 2017) to describe the compressor on the Altera Cyclone IV FPGA chip family (Altera Corporation, 2012a). The completed design of SSC composes several design modules including the random number generation (Tian et al., 2009; Abu Al-Haija et al., 2018b), primality testing (Ishmukhametov and Mubarakov, 2013; Asad et al., 2017a), arithmetic addition units (Ercegovac and Lang, 2004; Marouf et al., 2017a), arithmetic multiplication unit (Karatsuba and Ofman, 1963; Asad et al., 2017b; Asad et al., 2019), greatest common divisor (GCD), and least common multiple (LCM) units (Brent and Kung, 1984; Stein, 2009; Marouf et al., 2017b), modular exponentiation unit (Walter, 2010; Marouf et al., 2017c), and modular inverse unit (Hlaváč and Lórencz, 2013; Al-Haija et al., 2018). Finally, we have synthesized the resulting hardware coding using Quartus II CAD design tool (Altera Corporation, 2012b), which confirms that SSC can be used as an efficient and comparable alternative to RSA for securing the wireless sensor networks (Abu Al-Haija et al., 2014). To the best of our knowledge, the hardware design of SSC cryptosystem, that maintains maximum parallelism between its underlying computation modules to optimize the system performance factors, has not been investigated previously. Thus, the proposed work is considered new in this area of coprocessors implementations.

The rest of this paper is organized as follows. Section “Sensor security architecture” describes

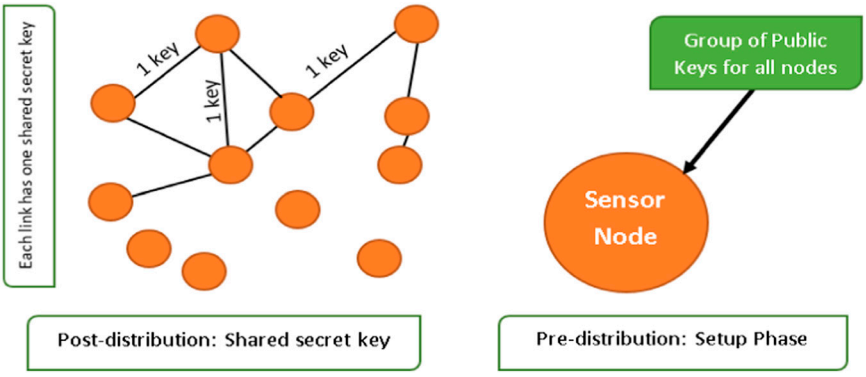

Figure 2: Stages of key agreement in each sensor node.

the sensor security architecture using parallelized Schmidt-Samoa cryptosystem and provides the proposed implementation approach and environment as well as cost factors explanations. Section "Cost factor results and analysis" presents and discusses the synthesize results and analysis by considering several design scenarios. Finally, Section "Conclusions" concludes the paper.

Sensor security architecture

As every other emerging technology and since the world shifts to this new technology of WSNs, a handful of legal implications that must be clarified over time are arises. One of the most questionable issues is the use of the data that is collected and the ownership dilemma. Who owns these collected data? And how it can be used? The legal community still need to address and legislate roles for these legal issues as WSN applications growing fast and affect our daily lives. Figure 2 shows the two stages of sharing a secret key for each sensor node.

Schmidt-Samoa cryptosystem (SSC) is a public key cryptosystem. It is heavily based on modular arithmetic involving a large prime number. The challenge of SSC algorithm is the ability to factor out the public key. However, as the size of the key increases, the factorization problem becomes even more complicated (Paar and Pelzl, 2010). Factoring a number means defining that number as a product of prime numbers. To initiate the secure communication session between sensors, the receiver sensor node starts by choosing two large prime numbers (p, q) and then follows the complete SSC algorithm diagram illustrated in Figure 3 which encompasses three stages: key generation stage, encryption stage, and decryption stage (Abu Al-Haija et al., 2018a).

Figure 4 demonstrate the simplified view for the Schmidt-Samoa Cryptoprocessor design. Indeed, SSC works in two modes: encryption and decryption and it encompasses five control signals that coordinate the internal processes inside the coprocessor, including three input control signals, i.e., clock trigger, enable, and reset, and two output control signals, i.e., ack. and ready. Also, to run the SSC coprocessor in the active mode of encryption or decryption process during the sensory communication sessions, it, first, initialized with SSC_Initializing stage to reset all control signals, clear all registers, and enable/disable the internal nodules such as the multipliers and adders.

Indeed, the initialization stage is much more complicated of that shown in Figure 4 and it needs to be emphasized and detailed to demonstrate the comprehensive process of secure compunction. Therefore, Figure 5 illustrates the detailed comprehensive

Key Generation Phase

1. Pickup two large primes: P, Q.
2. Calculate the public key N, where: $N = P^2Q$
3. Calculate the private key d, where: $d = N^{-1} \ mod \ LCM\ (P-1, Q-1)$

Encryption Phase

1. Convert the text message to numbers of 128-bit digests
2. Encrypt the plaintext message digests using N
3. Encrypt the plaintext message digests (M) as follows: $C = M^N \ mod \ N$

Decryption Phase

1. Calculate the decryption modulus $E = PQ$
2. Decrypt the ciphertext message digests (C) as follows: $M = C^d \ mod \ E$
3. Convert the numbers of 128-bit digests to text message

Figure 3: Complete diagram of Schmidt-Samoa algorithm.

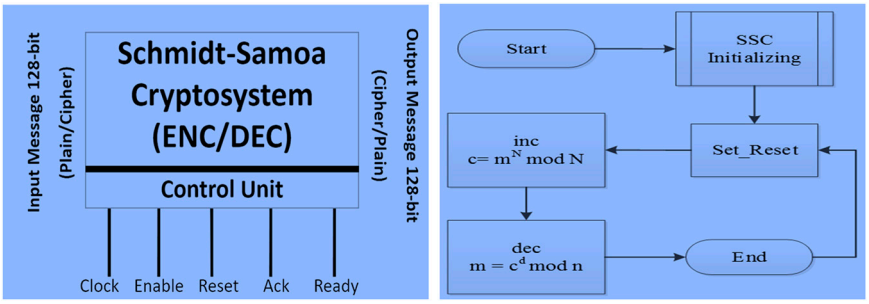

Figure 4: Schmidt-Samoa Cryptoprocessor – simplified view.

internal parallel architecture of SSC Coprocessor stages. According to the figure, the process is initiated by the prime random number generation to generate both large primes p and q. Concurrently, the multiplication module is activated to compute p^2 in parallel to generating q and then generate public key $N=p^2q$. At the same time, the least common multiple of both numbers (p–1, q–1) is computed to generate the private key d and the decryption modulus n in parallel. Thereafter, the system can start a secure communication session by encrypting and/or decrypting messages. Note that, both processes can be executed independently using parallel modular exponentiation units.

Cost factor results and analysis

In the last decade, many research works have been proposed to study several metrics and constraints of WSN such as security, energy consumptions, and many others. Indeed, the literature is very rich with research works that address the security issue and its impact on other factors of WSN such as Abu Al-Haija (2011), Hwang et al. (2013), Alam and De (2014), Koutsopoulos and Hal-

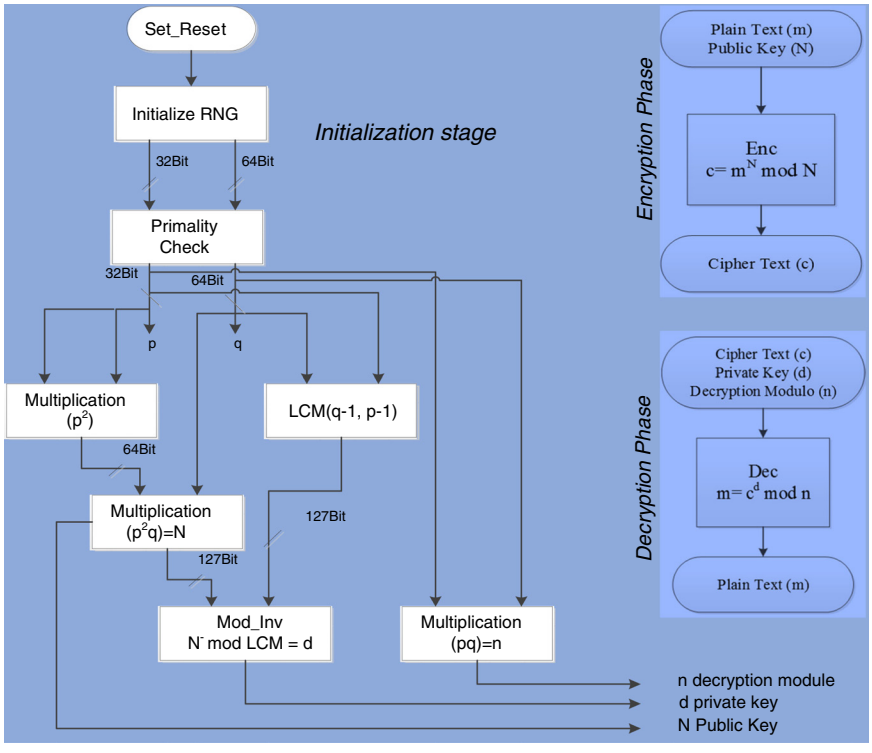

Figure 5: The comprehensive internal architecture of SSC Coprocessor.

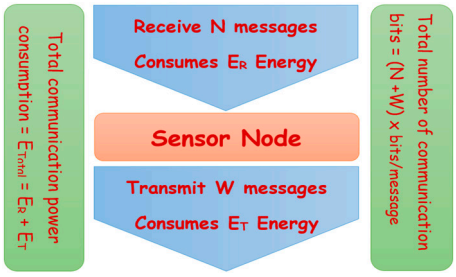

Figure 6: Communication process in each sensor node.

kidi (2014), Kumar et al. (2014), Panja et al. (2014), Patil and Kumar (2014), Rault et al. (2014), Suman et al. (2014), Brumancia and Sylvia (2015), Chelli (2015), Chowdhury et al. (2015), Daniel and Roslin (2015), Ghormare and Sahare (2015), Anbuchelian et al. (2016), Balakrishn and Swetha (2016), Shahdad et al. (2016), Wang et al. (2016), Zorbas et al. (2016), Abu Al-Haija et al. (2017a), Abu Al-Haija et al. (2017b). However, the state-of-art works lack the detailed discussion and experimentation of SSC with the lightweight implementation that can prolong the network lifetime, and to use energy-efficient and securely protocols. The communication energy consumption of sensor node is comprised of the energy required from transmitting and receiving a number of bits over a given communication distance as illustrated in Figure 6 (communication process in each sensor node). Therefore, any promising design should focus on improving the performance for the sensor security while maintaining the minimum amount of energy consumption due to key exchange and coprocessor computations.

Indeed, SSC is a public key cryptosystem employs the properties of prime numbers alongside the congruent to produce a very secure hard to break cryptosystem. Consequently, to accomplish the proposed robust SSC cryptoprocessor, one should carefully select the underlying modules to the efficient coprocessor design that optimize the performance factors of the cryptosystem. In this work, we have implemented the lightweight parallelized architecture of high radix 128–bit SSC Cryptosystem that can be used to secure by the data communications for wireless sensor

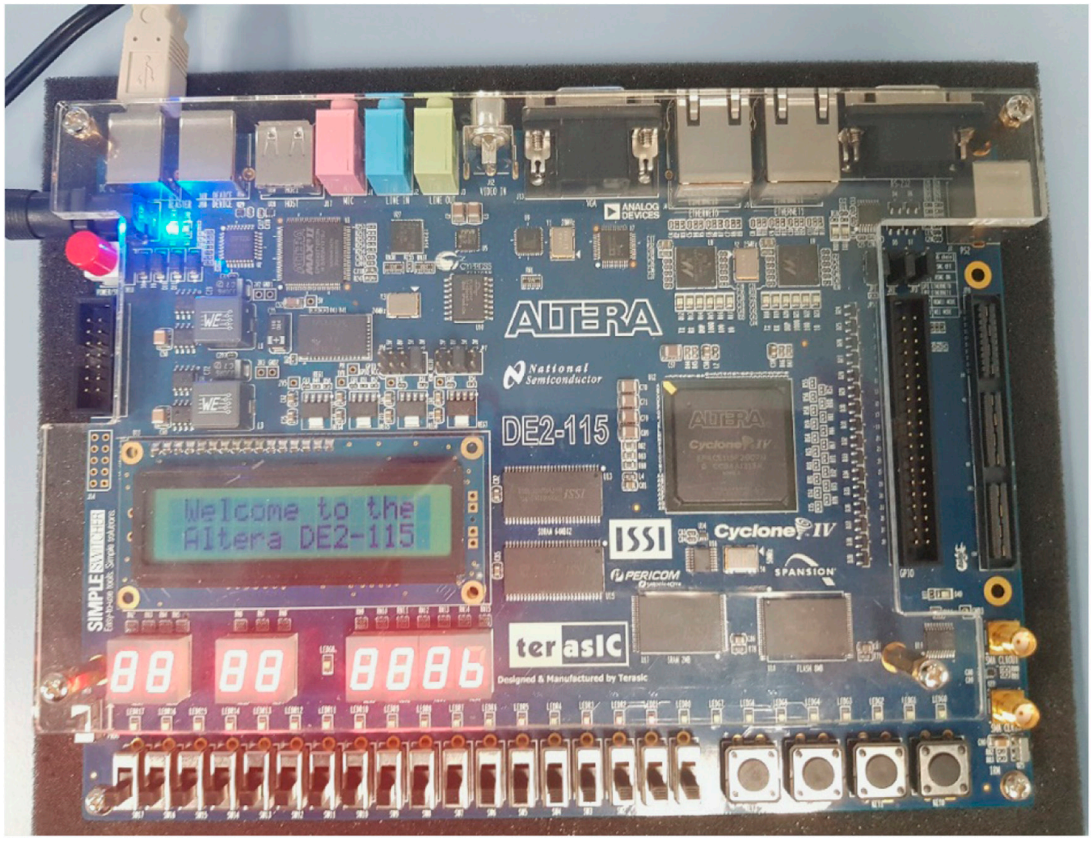

Figure 7: Target FPGA Kit: Altera Cyclone IV (EP4CGX22CF19C7) device.

Table 1. Cost factor analysis for the FPGA design of 128-bit SSC Cryptoprocessor.

Design area analysis	**The number of logic elements (LEs)**	**58,719 LEs**
	The number of four-input look-up table	234,876 LUTs
	The number of registers	29,883
	Memory utilization	50%
	Total number of I/O pins	389
	I/O utilization	76%
Design timing analysis	**Total path delay for critical clock cycle**	**25.02 ns**
	Maximum frequency	40 MHz
	Critical clock cycles to perform SSC process	5 million clocks
	Total processing delay to perform SSC process	125 ms
Design power analysis	**Dynamic thermal power dissipation (I/O assignments and operations)**	**102.6 mW**
	Static thermal power dissipation	148.7 mW
	Total FPGA thermal power dissipation	251.3 mW

networks. We have synthesized the proposed FPGA design using Quartus II tool targeting Altera Cyclone IV EP4CGX22CF19C7 FPGA device and simulated using ModelSim 10.1 simulator tool to verify the functionality of the SSC Cryptoprocessor. Our target FPGA device is shown in Figure 7.

To achieve the best performance, we have pipelined the partial operations of SSC processor to exploit the maximum possible parallelism between the internal units to gain in speed and enhance the design performance. Also, since the completed design of SSC includes several design modules, we have implemented each module with efficient and scalable algorithms as follows: for random number generation, we have used a hybrid two-stage RNG that combines both TRIVIUM and LFSR (Abu Al-Haija et al., 2018b). For primality testing (PT) module, we have implemented MILLAR-RABIN mechanism since it is considered as one of the most powerful prime test algorithms (Asad et al., 2017a). For the addition operation, we have performed all the internal computations for SSC in a redundant fashion using the carry save adder (CSA) (Ercegovac and Lang, 2004) which improve the performance of the overall system while we have used a conventional addition for the last step of computation by employing Kogge-Stone Adder (KSA) (Marouf et al., 2017a) since its considered as one of the fastest two-operands adders. For the arithmetic multiplication module, we developed our own multiplier by using Wallace Tree CSA Based Radix-8 Booth Multiplier (Asad et al., 2019). For the least common multiple (LCM) using the GCD reduction method with pulse minus GCD (Marouf et al., 2017b) used to implement the greatest common divisor operation. For modular exponentiation, we have implemented the right-to-left modular exponentiation based on NAF representation (Marouf et al., 2017c). For modular inverse, we have implemented the Extended Euclidian Algorithm for modular inverse (Al-Haija et al., 2018).

Finally, Table 1 shows the performance analysis for the FPGA design of 128-bit SSC Cryptoprocessor for three design factors: design area, design timing, and design power dissipation. The results of this table have been obtained by synthesizing our VHDL code for SSC the computer-aided design (CAD) tools of Quartus II system for ALTERA kits. Indeed, we have run the simulation several times to verify the functionality of each internal module and to validate cost factors to finalize on the SSC process, i.e., encryption/decryption process. Finally, the proposed 128-bit SSC should a comparable result for other well-known practicable public key cryptosystems (Abu Al-Haija et al., 2014) in terms of all cost factors.

Conclusions

Cryptography plays an important role in the security of wireless sensor communication networks since they defend the networks against cyber-attacks and unauthorized access. The efficient and robust

management of sensory systems' security requires the development of energy-aware and secure schemes with best resource utilization and management. This is achieved by the integration of the proper Cryptoprocessor with the nodes of wireless sensor networks (WSN). Schmidt-Samoa Cryptoprocessor (SSC) is a powerful public key crypto algorithm that derives its robustness from the difficulty large integer factorization problem. Recently, many research works tried to present efficient hardware/software implementations and architectures for SSC which carries major advantages in speed, reliability, and innovation. Indeed, SSC starts to be in-use up to provide security solutions for data confidentiality for several IoT, cloud applications, and cyber-physical systems (CPS). In this paper, we are reporting on the lightweight 128-bit SSC coprocessor design to provide security for data communicated through sensor nodes of WSN. The study takes advantage of the fixability and reconfigurability of field programmable gate array (FPGA) such as Altera Cyclone chip family. Eventually, the proposed parallelized architecture has been synthesized to evaluate the different design factors including: (i) the hardware design area in terms of LEs, LUTs, registers, I/O pins, and hardware utilization percentages, (ii) the design timing in terms the critical path delay, the number of clock cycles, and the maximum operational frequency in MHz, and (iii) the design total FPGA power including dynamic and static power dissipations consumption. To sum up, the experimental results showed that that the proposed SSC Cryptoprocessor recorded an attractive result for low-power applications such as the security of wireless sensor networks.

Literature Cited

Abu Al-Haija, Q. 2011. Toward secure non-deterministic distributed wireless sensor network using probabilistic key management approaches. *Journal of Information Assurance and Security* 6(1):010–018.

Abu Al-Haija, Q., Al Tarayrah, M., Al-Qadeeb and H., Al-Lwaimi, A. 2014. A Tiny RSA Cryptosystem Based on Arduino Microcontroller Useful for Small Scale Networks. International Symposium on Emerging Inter-networks, Communication and Mobility (EICM 2014), Elsevier, Canada , Auburn, Washington, USA.

Abu Al-Haija, Q., Asad, M. M. and Marouf, I. 2018a. A systematic expository review of Schmidt-Samoa Cryptosystem. *International Journal of Mathematical Sciences and Computing* 4(2):12–21, 10.5815/ijmsc.2018.02.02.

Abu Al-Haija, Q., Enshasy, H. and Smadi, A. 2017b. Estimating energy consumption of Diffie Hellman encrypted key exchange (DH-EKE) for wireless sensor network. 2017 IEEE International Conference on Intelligent Techniques in Control, Optimization & Signal Processing (INCO'17), 23–25 March 2017, Srivilliputhur, India.

Abu Al-Haija, Q., Manasra, G. F. and Al Tarayrah, M. 2017a. Communication power analysis of applying MQV Key agreement scheme for wireless sensor network. 2017 IEEE International Conference on Intelligent Techniques in Control, Optimization & Signal Processing (INCO'17) 17-20 AUGUST 2014, Niagara Falls, Canada.

Abu Al-Haija, Q., Marouf, I. and Asad, M. M. 2018b. A double stage implementation for 1-K Pseudo RNG using LFSR and TRIVIUM. *Journal of Computer Science and Control Systems* 11(1):639–646.

Alam, S. and De, D. 2014. Analysis of security threats in wireless sensor network. *International Journal of Wireless & Mobile Networks* 6(2):1–12.

Al-Haija, Q., AlShuaibi, A. and Al Badawi, A. 2018. Frequency analysis of 32-bit modular divider based on extended GCD algorithm for different FPGA chips. *International Journal of Computers & Technology* 17(1): 7133–7139, available at: https://doi.org/10.24297/ijct.v17i1.6992

Altera Corporation 2012a. *Cyclone IV device handbook*, Vol. 1, CYIV-5V1-2.2, Altera Corporation, available at: www.altera.com/San Jose, California, United States.

Altera Corporation 2012b. *Introduction to Quartus II software: ver 10.0*, Altera Corporation, Intel Quartus II MNL-01055-1.0, San Jose, California, United States.

Anbuchelian, S., Lokesh, S. and Baskaran, M. 2016. Improving security in wireless sensor network using trust and metaheuristic algorithms. 3rd International Conference on Computer & Information Sciences (ICCOINS) 233–241.

Asad, M. M., Marouf, I. and Abu Al-Haija, Q. 2017a. Investigation study of feasible prime number testing algorithms. *Acta Technica Napocensis – Electronics and Telecommunications* 58(3):11–15.

Asad, M. M., Marouf, I. and Abu Al-Haija, Q. 2017b. Review of fast multiplication algorithms for embedded systems design. *International Journal of Scientific & Technology Research* 6(8):238–242.

Asad, M. M., Marouf, I. and Abu Al-Haija, Q. 2019. Radix-8 design alternatives of fast two operands interleaved multiplication with enhanced architecture. *International Journal of Advanced Network, Monitoring and Controls* 4(2):15–27.

Balakrishn, T. and Swetha, R. N. 2016. Development of Arm7 based sensor interface for industrial Wireless Sensor Network (WSN) in IoT environment. *International Journal of Eminent Engineering Technologies* 4(3):54–60.

Brent, R. P. and Kung, H. T. 1984. Systolic VLSI arrays for polynomial GCD computation. *IEEE Transactions on Computers* C-33(8)731–736.

Brumancia, E. and Sylvia, A. 2015. A profile based scheme for security in clustered wireless sensor networks. IEEE International Conference on Communications & Signal Processing (ICCSP2015) 823–828.

Chelli, K. 2015. Security issues in wireless sensor networks: attacks and countermeasures. World Congress on Engineering (WCE 2015), Vol. 1, London, U.K., 1–3 July 2015.

Chowdhury, A., Tanzila, F. A., Chowdhury, S. and Haque, M. M. 2015. An Efficient Security Architecture for Wireless Sensor Networks using Pseudo-inverse Matrix. 18th International Conference on computer and Information Technology (ICCIT), pp. 396–400.

Daniel, A. and Roslin, E. 2015. a review on existing security frameworks with efficient energy preservation techniques in wireless sensor networks. IEEE International Conference on Communications and Signal Processing (ICCSP 2015) 658–662.

Ercegovac, M. D. and Lang, T. 2004. *Digital arithmetic* 1, Morgan Kaufmann Publishers, Elsevier, San Antonio, TX.

Ghormare, S. and Sahare, V. 2015. Implementation of data confidentiality for providing high security in wireless sensor network. IEEE 2nd International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS 2015), 19–20 MARCH 2015, Coimbatore, India.

Hlaváč, J. and Lórencz, R. 2013. Arithmetic unit for computations in GF(p) with left-shifting multiplicative inverse algorithm, architecture of computing systems, ARCS 2013. *Lecture Notes in Computer Science* 7767:268–279.

Hwang, L. C., Lee, C. C. and Hwang, M. S. 2013. A n2 + n MQV key agreement protocol. *The International Arab Journal of Information Technology* 10(2):137–142.

Ishmukhametov, S. and Mubarakov, B. 2013. On practical aspects of the Miller-Rabin primality test. *Lobachevskii Journal of Mathematics* 34(4):304–312.

Karatsuba, A. and Ofman, Y. 1963. Multiplication of multidigit numbers on automata. *Soviet Physics, Doklady* 595–596.

Koutsopoulos, I. and Halkidi, M. 2014. Distributed energy-efficient estimation in spatially correlated wireless sensor networks. *Computer Communications* 45(1):47–58.

Kumar, E. S., Kusuma, S. M. and Kumar, B. P. V. 2014. A random key distribution based artificial immune system for security in clustered wireless sensor networks. IEEE Students' Conference on Electrical, Electronics and Computer Science 1–2 MARCH 2014, Bhopal, India.

LaMeres, B. J. 2017. Introduction to logic circuits & logic design with VHDL. Electronics and Electrical Engineering, Springer, Heidelberg, Germany.

Marouf, I., Asad, M. M. and Abu Al-Haija, Q. 2017b. Reviewing and analyzing efficient GCD/LCM algorithms for cryptographic design. *International Journal of New Computer Architectures and their Applications, Society of Digital Information and Wireless Communication* 7(1):1–7.

Marouf, I., Asad, M. M. and Abu Al-Haija, Q. 2017c. Comparative study of efficient modular exponentiation algorithms. *An International Journal of Advanced Computer Technology* 6(8):2381–2389.

Marouf, I., Asad, M. M., Bakhuraibah, A. and Abu Al-Haija, Q. 2017a. Cost analysis study of variable parallel prefix adders using Altera Cyclone IV FPGA kit. IEEE International Conference on Electrical & Computing Technologies & Applications, (ICECTA) 19–21 NOVEMBER 2017, Ras Al Khaimah, UAE.

Paar, C. and Pelzl, J. 2010. *Understanding cryptography*, Springer-Verlag, Berlin and Heidelberg, available at: https://doi.org/10.1007/978-3-642-04101-3

Panja, B., Scott, Z. and Meharia, P. 2014. Security in wireless sensor networks for health monitoring helmet with anomaly detection using power analysis and probabilistic model. IEEE Conference on Wireless Sensors (ICWiSE 2014) 26–28.

Patil, S.D. and Kumar, V. 2014. Secure health monitoring in wireless sensor networks with mobility-supporting adaptive authentication scheme. *International Journal of Computer Networking, Wireless and Mobile Communications* 4(1):27–34.

Polastre, J., Szewczyk, R., Sharp, C. and Culler, D. 2004. *The mote revolution: low power wireless sensor network devices*, Computer Science Department, University of California, Berkeley, CA.

Radzevych, V. A. and Mathew, S. 2003. Security in wireless sensor networks: key management approaches. PPt File, University at Buffalo – The State University of New York, Computer Science and Engineering, New York, USA.

Rault, F., Bouabdallah, A. and Challal, Y. 2014. Energy efficiency in wireless sensor networks: a top-down survey. *Elsevier Computer Networks* 67:104–122.

Samoa, K. S. 2006. A new Rabin-type trapdoor permutation equivalent to factoring. *Electronic Notes in Theoretical Computer Science* 157(3):79–94, available at: https://eprint.iacr.org/2005/278.pdf

Shahdad, S. Y., Sabahath, A. and Parveez, R. 2016. Architecture, issues and challenges of wireless mesh network. International Conference on Communication and Signal Processing (ICCSP 2016), Melmaruvathur 0557–0560.

Stein, W. 2009. Elementary number theory: primes, congruence, and secrets: a computational approach. *Number Theory and Discrete Mathematics* 1:1–172.

Suman, S. B., Kumar, P. V. R. and Kumar, E. S. 2014. Random keying technique for security in wireless sensor networks based on memetics. *International Journal of Computer Science: Theory and Application* 2(1):25–31.

Tian, Y., Chen, G. and Li, J. 2009. On the design of Trivium. *Beijing Daxue Xuebao Ziran Kexue Ban/ Acta Scientiarum Naturalium Universitatis Pekinensis* 5 1–13, available at: http://eprint.iacr.org/2009/43.

Walter, C. D. 2010. Right-to-left or left-to-right exponentiation? 1st International Workshop on Constructive Side-Channel Analysis and Secure Design, Darmstadt.

Wang, N., Zhou, Y. and Xiang, W. 2016. An energy efficient clustering protocol for lifetime maximization in wireless sensor networks. IEEE Global Communications Conference (GLOBECOM 2016) 1–6USA.

Wu, S. and Tseng, Y. 2006. *Wireless ad hoc networking* 1, Taylor and Francis Group, Auerbach Publications 139–160, CRC Press, Boca Raton, Florida, USA.

Yang, S. H. 2014. *Wireless sensor networks: Principles, Design and Applications. Signals and Communication Technology. Springer Nature*, Springer-Verlag, 2–4, Heidelberg, Germany.

Zorbas, D., Raveneau, P. and Doudane, Y. G. 2016. Assessing the cost of RF-power harvesting nodes in wireless sensor networks. IEEE Global Communications Conference (GLOBECOM 2016) 4–8 DECEMBER 2016, Washington, DC USA.