Single Event Effects Tolerant AES-CTR Implementation for Authentication of Satellite Communication

Syed Jahanzeb Hussain Pirzada[1*], Abid Murtaza[2], Liu Jianwei[1], Tongge Xu[1]

[1] School of Cyber Science and Technology, Beihang University, Beijing, China.
[2] School of Electronics and Information Engineering, Beihang University, Beijing, China.

* Corresponding author. Tel.: +86 13121202722; email: jahanzebp@hotmail.com

Manuscript submitted May 30, 2019; accepted August 18, 2019.
doi: 10.17706/ijcce.2019.8.4.178-183

Abstract: Recently, the increase in the use of fast and reliable communication systems has increased the significance and utilization of satellite-based communication systems. The communication systems used in the space environment is more reliable and robust as compared to communication systems used on earth. Because unlike ground communication, the communication systems in space have to bear harsh space environment and its effects like radiations, pressure, and vacuum, which causes anomalies in communication systems. These effects are known as Single Event Effects (SEE), which results in loss of data or sometimes even damage to the equipment. Like ground systems, in satellite, the Advanced Encryption Standard (AES) is a widely used encryption algorithm which is not only used to provide data confidentiality but also used in data authentication & integrity algorithms (e.g. CMAC) as well as in authenticated encryption (AE) algorithm (e.g., AES-GCM). The Substitution Box (S-Box) is a main component of the AES algorithm, which is generally implemented on memory blocks. The memory blocks in space are vulnerable to radiations and mostly affected by SEE; hence, protection techniques against SEE are proposed by researchers. Two methods for implementation of the S-Box algorithm are by a look-up table or by an algorithm. In this work, analysis of using these two methods of the S-Box implementation for SEE is performed. The implementation of both methods is performed on FPGA, and results show that the algorithm implementation is more reliable in the space environment as compared to table-based implementation.

Keywords: Advanced encryption standard, authentication, field programmable gate array, substitution box, and single event effects.

1. Introduction

The curious nature of human beings has led them to explore every corner of this earth for exploring it for benefitting humans. Although the strive of humans to get more and more benefits from the earth did not diminish. The evolution in communication systems and technology have enabled humans to reach space and discover the secrets of space. Therefore, a new era of space exploration has begun for utilization of space technology for the benefit of humankind. The space environment is not like the environment we face on earth. The space environment has high pressure imposed on the objects in space, it contains vacuum instead of air, and there are radiations which affect electronic systems in general and communication systems in particular. Therefore, the communication systems in space are designed to withstand the effects of the space environment. Besides, the advancement in technology for space applications is being used for the development of more sophisticated systems on earth. The data security in communication systems used in space are more critical as the only source of contact between spacecraft and humans on earth is through communication systems. The effects causing an unreliable response of communication systems are under constant development. It has stimulated a trend that challenges researchers to develop equipment and communication systems for the space environment.

In the space environment, the significant effects on communication systems are space radiations. The radiations cause unreliable operation of communication systems. The space radiations cause's effects called the Single Event Effects (SEE); these effects cause the electronics in communication systems to malfunction. The primary source of space radiations is incident cosmic rays and incident high energy protons (mostly origin from solar flares or Van Allen radiation belt around the earth). There are three main types of SEE. The effect of radiations causing a bit to flip is known as Single Event Upset (SEU). The latch-up of memory caused by a high operating current is known as Single Event Latch-up (SEL). The radiations effects causing burn-out of memory is called Single Event Burn-out (SEB). These effects can cause permanent and temporary damages depend on the type of effect on memory. Therefore, in communication systems, the system must be capable of tolerating SEE. The SEE is more effective on memories such as Static Random Access Memory (SRAM). These SEE are not new, and many researchers have diagnosed these effects in the space environment [1], [2]. These effects are more effective in memories, and many researchers worked on the methods to avoid these effects on hardware and software [3]-[5]. The implementation methods for avoiding the SEE are usually focus on the SEU, and these effects consume a large area to implement as compared to the area of the original design. The implementation of Triple Memory Redundancy (TMR) requires triplication of memory resources.

In the scope of security of communication systems for space communication the Consultative Committee for Space Data Systems (CCSDS) recommends the use of Advanced Encryption Standard (AES) algorithm [6]. Although with the increasing trend of high-speed communication the AES in Counter mode (AES-CTR) [7] is utilized widely in much high-speed Authenticated Encryption (AE) algorithms such as Galois Counter Mode (GCM) [8]. In the AES algorithm, amongst the four sub-operations, the Substitution byte (S-byte) operation involves the substitution of byte from Substitution Box (S-Box) consumes memory for implementation. The S-Box can be implemented using the look-up table implementation or algorithm-based implementation. The look-up table implementation or the table-based implementation is usually stored in memory, such as SRAM. However, in the space environment, the memory on exposure to radiations may cause the SEE. On the other hand, in algorithm-based implementation implements the algorithm using logic gates instead of memory. The algorithm-based implementation avoids the memory resources and implements the on logic gates make the implementation less affected by SEE.

The remaining paper is arranged as follows; Section II describes the related work. Section III provides the methodology for the S-Box implementation. Section IV contains the details of implementation results. Finally, Section V summarizes this paper.

2. Related Work

The AES-CTR algorithm is utilized in many applications, such as; wireless communication, and satellite communication. Although, the communication systems in the space environment are affected by the SEE in the presence of radiations. Therefore, some technique of avoiding the SEE on the communication systems must be employed. The security algorithms of communication systems such as the AES-CTR algorithm utilizes memory in hardware for implementation.

S. Morioka *et al*. optimized throughput [9] using the optimization of S-Box for the AES algorithm. He also optimized S-Box to minimize consumption of power [10]; in addition, he tried to reduce area consumption for S-Box implementation [11].

K. Rahimunnisa *et al*. optimized the AES implementation using the modification of S-Box for performance enhancement [12]. In satellite communication, the utilization of the AES algorithm and its implementation follow similar optimization goals such as throughput optimization with S-box modification. C. Thamilarasi [13] implemented the error-tolerant design for data security. Dr. J. A. Jaleel *et al*. implemented the optimization of AES algorithm based on S-Box implementation [14].

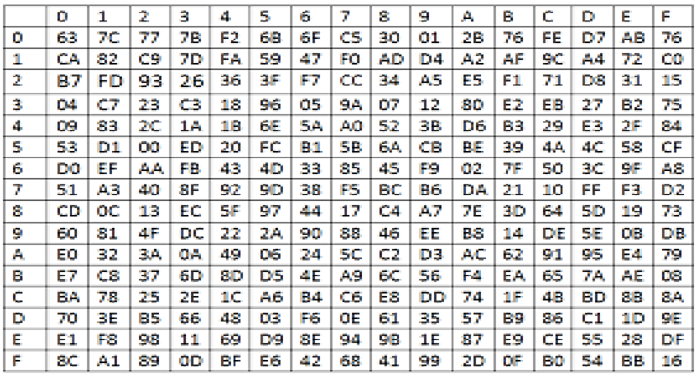
Rijmen *et al*. [15] proposed subfield arithmetic using Galois field. He proposed sub-field arithmetic to avoid the look-up table based implementation. The usage of such algorithm-based implementation can avoid the usage of memory resources.

In space communication, C. J. N. Cheltha *et al*. presented AES algorithm implementation for error-tolerant implementation [16]. They presented a model using the Hamming code for avoiding SEU effects on the AES algorithm for satellite applications. F. Brosser *et al*. [17] have presented a scrubbing technique for implementation for SRAM-based FPGAs. These implementations are mainly focused on the utilization of mitigation techniques for catering the SEE in the space environment.

3. The S-Box Implementation Methodology

The differential and linear cryptographic analysis and algebraic attacks are countered using the S-Byte algorithm using S-Box. In the AES-CTR algorithm, the first and foremost step is the Sub-byte algorithm using the S-Box for byte-substitution. The algebraic formula of S-Box includes activities in a Galois finite field GF (2^8). Although, the S-box values are computed by taking the multiplicative inverse in GF (2^8) followed by calculating the affine transformation.

The S-Box can be implemented using the conventional look-up table method with the look-up table shown in Fig, 1. In the table based S-Box, the implementation is performed using the pre-computed table. This table is conventionally stored on the memory in hardware. The SRAM memory is utilized in hardware for storing these values, which is more affected by SEE in the presence of radiations in the space environment.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	2B	76	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fig. 1. The S-box table.

Alternatively, to implement the sub-byte algorithm using algorithm based S-Box implementation. The implementation involves the implementation of the polynomial directly and calculates the substitution value. The algorithm-based implementation implements the design on logic gates; therefore, the SEE is less effective in the presence of radiations in the space environment. The idea of a logic-only implementation is conceived by A. Satoh *et al*. [11], which is further optimized and explained by D. Canright [18]. The basic idea of implementation is to notice that inversion in GF (2^8) can be decomposed into a sequence of operations in GF (2^4). The operations in GF (2^4) can be expressed in terms of operations in GF (2^2) and the operations in GF (2^2) in terms of operations in GF (2). The operations in GF (2) can be implemented using a simple XOR gate and AND gate. An inverse of one in GF (2) is one, and the inverse of zero does not exist. Thus, the complete inversion in GF (2^8) can be decomposed into a logic circuit composed of logic gates of exclusive-OR and AND gates.

The algorithm-based implementation is utilized in this work for implementation of AES-CTR algorithm for implementation of authentication of satellite security. The AES-CTR algorithm consists of initialization vector (IV) as an input along with the plain text (PT) and secret key (K). The IV is required to be unique value for generation of every cipher-text. Therefore, IV is incremented by 1 every time we use it for generating cipher-text. The output of the AES-CTR algorithm is cipher-text (CT). The diagram shows the algorithm flow in Fig. 2.

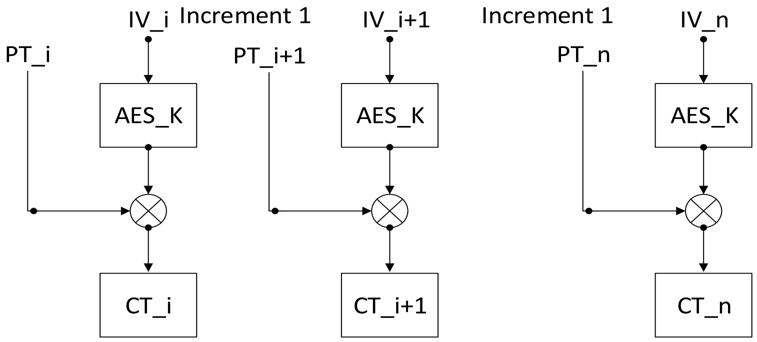
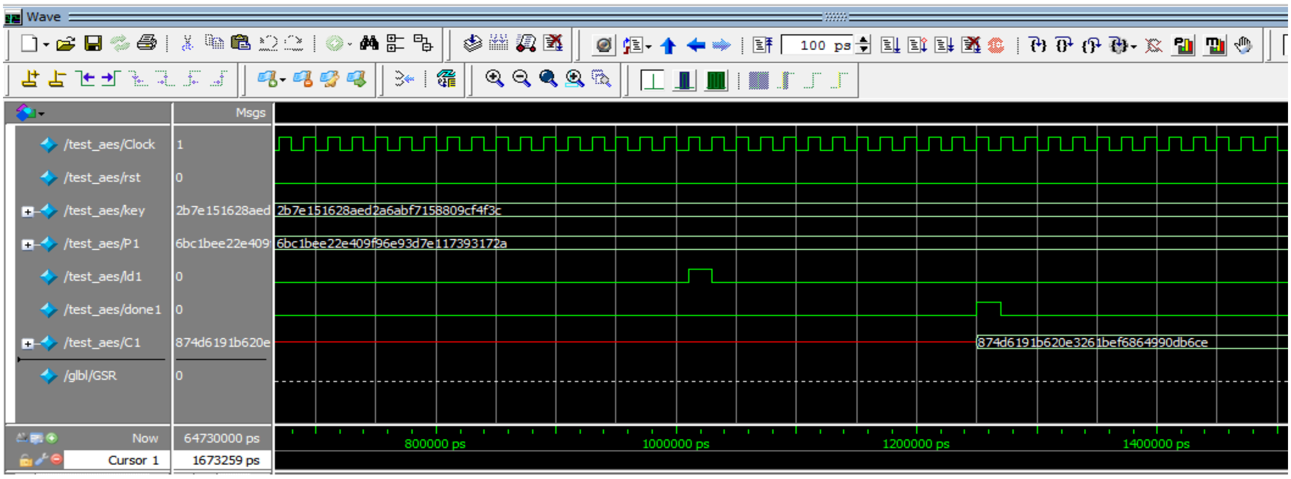


Fig. 2. Flow chart of AES-CTR algorithm.

4. The Implementation Results

The implementation of the AES-CTR algorithm for the authentication of the satellite is performed on Xilinx FPGA using algorithm-based method and table-based method. The implementation is performed using Xilinx ISE software for synthesis on Xilinx FPGA. The Modelsim software is used to simulate the AES-CTR algorithm for S-Box implementation. The AES-CTR algorithm is implemented with both S-Box implementations. In Xilinx FPGAs, the SRAM based Block Random Access Memory (BRAM) is used for storing the data. Therefore, the S-Box is implemented using the table-based method on the BRAM. On the other hand, the S-Box implementation using the algorithm-based implementation is performed on the logic area of FPGA. The simulation results of the AES-CTR algorithm with the S-Box algorithm based implementation is shown in Fig. 3.



```
/test_aes/Clock    1
/test_aes/rst      0
/test_aes/key      2b7e151628aed    2b7e151628aed2a6abf7158809cf4f3c
/test_aes/P1       6bc1bee22e409    6bc1bee22e409f96e93d7e117393172a
/test_aes/ld1      0
/test_aes/done1    0
/test_aes/C1       874d6191b620e    874d6191b620e3261bef6864990db6ce
/glbl/GSR          0
Now                64730000 ps
Cursor 1           1673259 ps
800000 ps    1000000 ps    1200000 ps    1400000 ps
```

Fig. 3. Simulation of the AES-CTR algorithm.

The implementation of algorithm-based method uses the logic block area of Xilinx FPGA, the Implementation using the logic area instead of the memory increases the logic area consumption on the cost of avoiding the BRAM. Although the algorithm-based method for implementation of S-Box protects against the SEE in the space environment. The area utilization for both methods is shown in Table 1.

Table 1. The Resource Utilization

S.No.	Implementation	CLB Utilized	BRAM Utilized	Clock Frequency (MHz)	Clock Cycle (ns)
1	Algorithm-based Method	1135	0	70.3	14.22
2	Table-based Method	869	8	110.85	9.02

The Table 1 shows the resource utilization of both implementations. The algorithm-based method shown an increase in logic area utilization as compared to the table-based method. The clock frequency of implementation is also a bit decreased as compared to the table-based implementation. Although the algorithm-based implementation support against space radiations.

5. Conclusion

In this work, a comparison between the two methods for S-Box implementation of recommended AES algorithm is performed for the security of satellite communication. The method involving algorithm based implementation is more efficient as it does not utilize memories in the satellite communication system. The implementation results show that the reduction in memory utilization reduces the effects of SEE in electronics of communication systems. Hence algorithm based S-Box implementation can protect satellite communication systems against SEE.

References

[1] Underwood, C. I., & Oldfield, M. K. (1999). Observations on the reliability of COTS-device-based solid state data recorders operating in low earth orbit. *Proceedings of the Fifth European Conference on Radiation and its Effects on Components and Systems* (pp. 387-393). Fontevraud, France.

[2] Seidleck, C. M., LaBel, K. A., Moran, A. K., Gates, M., Barth, J. L., Stassinopoulos, E. G., & Gruner, T. D. (1995). Single event effect flight data analysis of multiple NASA spacecraft and experiments; implications to spacecraft electrical designs. *Proceedings of the Third European Conference on Radiation and its Effects on Components and Systems* (pp. 581-588). Arcachon, France.

[3] Wilkinson, J., & Hareland, S. (2005). A Cautionary tale of soft errors induced by SRAM packaging materials. *Journal of IEEE Transactions of Development Material Reliability, 5(3)*, 428-433.

[4] Dodd, P. E., Massengill, L. W., *et al*. (2003). Basic mechanisms and modeling of a single-event upset in digital microelectronics. *Journal of IEEE Transactions on Nuclear Science, 50(3)*, 583-602.

[5] Dominik, L. (2008). System mitigation techniques for single event effects. *Proceedings of the IEEE/AIAA 27th Digital Avionics Systems Conference* (pp. 5.C.2-1-5.C.2-12). St. Paul, MN, USA.

[6] CCSDS. (2012). *CCSDS Cryptographic Algorithms* (CCSDS 352.0-B-1).

[7] NIST. (2001). Recommendation for block cipher modes of operation: Methods and techniques (Special Publication 800-38A). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-38a/final

[8] McGrew, D. A., & Viega, J. (2004). The security and performance of the Galois / Counter Mode (GCM) of operation. *Proceedings of the 5th International Conference on Cryptology in India Security* (pp. 343–55).

[9] Morioka, S., & Satoh, A. (2002). A 10 Gbps full-AES crypto design with a twisted-BDD S-box architecture. *Proceedings of the IEEE International Conference on Computer Design: VLSI in Computers and Processors* (pp. 98-103). Freiberg, Germany.

[10] Morioka, S., & Satoh, A. (2003). An optimized S-box circuit architecture for low power AES design.

Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems: Lecture Notes in Computer Science (pp. 172-186). Berlin, Germany.

[11] Satoh, A., Morioka, S., Takano, K., & Munetoh, S. (2001). A compact Rijndael hardware architecture with S-box optimization*. Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security: Lecture Notes in Computer Science* (pp. 239-254)*.* Berlin, Germany.

[12] Rahimunnisa, K., Sureshkumar, S., & Rajeshkumar, K. (2011). Implementation of AES with new S-box and performance analysis with the modified S-box. *Proceedings of the International Conference on VLSI, Communication & Instrumentation*.

[13] Thamilarasi, C., & Shanmugapriya, K. (2013). A high throughput and error tolerant AES design. *Journal of Advanced Research in Electronics and Communication Engineering, 2(4)*, 420-424.

[14] Jaleel, J. A., Assis, A., & Sherla. A. (2013). Optimization of AES encryption algorithm with S-box. *Journal of Engineering Research and Technology, 6(2)*, 259-268.

[15] Rijmen, V. (2001). Efficient implementation of the Rijndael S-box.

[16] Cheltha, C. J. N., & Velayutham, R. (2011). A novel error-tolerant method in AES for satellite images. *Proceedings of the International Conference on Emerging Trends in Electrical and Computer Technology* (pp. 937-940). Nagercoil.

[17] Brosser, F., Milh, E., Geijer, V., & Larsson-Edefors, P. (2014). Assessing scrubbing techniques for Xilinx SRAM-based FPGAs in space applications. *Proceedings of the International Conference on Field-Programmable Technology* (pp. 296-299). Shanghai, China.

[18] Canright, D. (2005). A very compact S-box for AES. *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 441-455).

Syed Jahanzeb Hussain Pirzada was born at Attock, Pakistan. In 2007, he received his BE degree in electronics engineering from NED University of engineering and technology, Karachi, Pakistan. In 2012, he received an MS degree in electrical, electronics, control and instrumentation engineering from Hanyang University, Seoul, South Korea. Since 2018 he is enrolled for the Ph.D. degree in the School of Cyber Science and Technology at Beihang University, Beijing, China. His research interest is in the field of cryptography for satellite applications.

Abid Murtaza was born at Karachi, Pakistan. In 2010, he received the M.Sc. electronics degree from the University of Karachi, Karachi, Pakistan. He is working with Pakistan's National space agency SUPARCO since 2010. He is currently working towards the Ph.D. degree in space technology applications at Beihang University, Beijing, China. His research interests include information security, space information network, and applications.

Liu Jianwei was born at Shandong, China. He received the BS and MS degrees in electronics and information engineering from Shandong University, Shandong, China in 1985 and 1988 respectively. He received his Ph.D. degree in electronics and communication systems from Xidian University, Shaanxi, China in 1998. He is now the dean of the School of Cyber Science and Technology at Beihang University, Beijing, China. His current research interests include wireless communication networks, cryptography, and information and network security.