# A Survey on Various Cryptanalytic Attacks on the AES Algorithm

Harshali Zodpe
and
Arbaz Shaikh
School of Electronics and Communication Engineering, Dr. Vishwanath Karad MIT World Peace University, Pune, India

The Advanced Encryption Standard (AES) Algorithm is popularly being used for securing classified information of Military and Banking services. This has led to intensifying the research on various attacks on AES algorithm either to test the security of the algorithm itself or to obtain the secret information i.e. the key. The AES algorithm is constantly subjected to various cryptanalytic attacks since its release in 2001. However, most of these attacks are theoretical and have been incapable of breaking the AES algorithm completely. These attacks are performed on the reduced rounds of the AES algorithm are compared with the brute force attack for time and data complexity. The brute force attack tries all possible values of keys and is the most effective technique of cryptanalytic technique. This research paper presents an extensive survey on various existing cryptanalytic attacks on the AES Algorithm.

Keywords: Advanced Encryption Standard, cryptanalytic attacks, time and data complexity.

## 1. INTRODUCTION

Due to the immense growth in the field of Internet Communication, security of data plays a vital role in communicating large amount of data. The channel used for communicating the data between the sender and the receiver might be unsafe [Z'aba and Maarof [2006a]]. Several procedures and methods are used by public and private organizations to protect the sensitive data from invaders. Cryptography is employed securely to store and communicate the sensitive data that play an important role in information technology. Cryptography is one of the most important and modern methods of using encryption and decryption to defend the data from attack [Genelle et al. [2009]]. Cipher text that is an unreadable type of format is obtained from plaintext i.e. original data through encryption whereas decryption is the opposite of encryption i.e. obtaining original data from the cipher text [Abdullah [2017]]. To perform these processes, mathematical calculation like substitution and permutation are used by cryptography with or without a key. Cryptography is broadly categorized into symmetric and asymmetric cryptography. Symmetric cryptography makes use of the same key for encryption and decryption data. The Asymmetric cryptography depends on a couple of non-similar keys for encryption and decryption [Bedoui et al. [2016]]. The durability and efficiency of asymmetric key is less than that of symmetric key. Some of the common symmetric algorithms are Advanced Encryption Standard (AES), Blowfish, Simplified Data Encryption Standard (SDES), and 3DES [Bedoui et al. [2016]]. Due to growth in technology different types of attacks are regularly found. The main purpose of the attacker is to wreck the code of encryption and decode the secret message and the private key [Li et al. [2009]]. There are various kinds of cryptanalytic attacks on the AES algorithm [Floissac and L'Hyver [2011]].

In this paper, the authors have discussed the AES standard (Encryption and Decryption) and surveyed the different types of cryptographic attacks on the AES algorithm. The rest of the paper is as follows: Key generation, followed by AES (Encryption and Decryption structure) and its round function.

## 2. HISTORY OF AES ALGORITHM

The AES algorithm is preceded by the Data Encryption Standard (DES) algorithm. The DES algorithm, which has a 64-bit size, was found to be easily weak to exhaustive attacks due to its inadequate key size. To overcome the disadvantages of DES, AES encryption standard was introduced. As compared to DES, the operations involved in the AES algorithm are more compact and due to larger key size need high computational power for an exhaustive attack. AES is an encryption standard that was introduced in 2001 by the United States Government to replace the DES algorithm. AES is widely utilized within the encryption system and became the mainstream of the hardware encryption algorithm. It was found that AES could be a minimum six times faster and cheaper than DES. AES encryption algorithm is a symmetric block cipher that uses an encryption key and various rounds for encryption. It uses one block of 128-bits at a time in AES encryption. The encryption and decryption of 128-bit data block can use three distinct types of keys in AES viz. 128-bit, 192-bit, and 256-bit, which are designated as AES-128, AES-192, and AES-256 [Zhang et al. [2019]]. There are 10-rounds in the AES encryption and decryption process using 128-bit key. There are mainly two steps in AES. The first process is the key generation and an-other is AES encryption. In key generation process, ten sub-keys of 128-bit each are generated from the input 128-bit key using various transformations viz., SubWord, RotWord and Rcon. The AES encryption process involves 10-rounds and each round includes operations viz. substitution bytes, shift rows, mix columns and add round key [Barenghi et al. [2010], Yu et al. [2018]].

### 2.1 Key Generation Method

2.1.1 *SubWord:.* This operation replaces the four byte input word from the 4*4 matrix with the value stored in the S-box to generate the output word [Park et al. [2010], Chen and Yen [2003]].

2.1.2 *RotWord:.* This operation cyclically shifts the bytes in the 4*4 matrix [Chen and Yen [2003], Yuan et al. [2018]].

2.1.3 *Rcon:.* After performing SubWord and RotWord operations, the last operation performed on the 4*4 matrix is XORing with the round constant Rcon [Chong and Jean-Jacques [2008], Kim [2012]].

### 2.2 AES Encryption AND Decryption

AES performs all its estimates on bytes. These 16-bytes are in order of 4*4 matrix. The AES encryption and decryption process contains various operations as shown in Figure 1.

As shown in Figure 1, the 128-bit AES encryption and decryption process goes through ten rounds and includes the Add Round Key (ARK), Substitute Bytes (SB), Shift Rows (SR) and Mix Columns (MC) operations. The Add Round Key uses the keys generated by the key generation method as explained in **?**]. The description of the various operations involved in the AES encryption and decryption process are as further explained in detail.

2.2.1 *Substitute Bytes (SB):.* Each byte in the 4*4 matrix is substituted with value from the predefined S-box table. For substitution, the higher nibble of the byte from the 4*4 matrix is considered as a row number and the lower nibble as a column number of the predefined S-box table and the intersection point become the new byte [Shan et al. [2015]]. This operation is performed on all the 16 bytes and the new results are arranged to form a 4*4 matrix. The sub byte is also known as byte by byte substitution. Similar operation is performed during decryption and is known as Inverse sub byte.

2.2.2 *Shift Rows (SR):.* In shift rows operation each rows are shifted towards left. The initial row is not moved. Subsequent row is moved towards left by one position. The third row does shift towards left by couple positions and later fourth row move towards left by three positions.

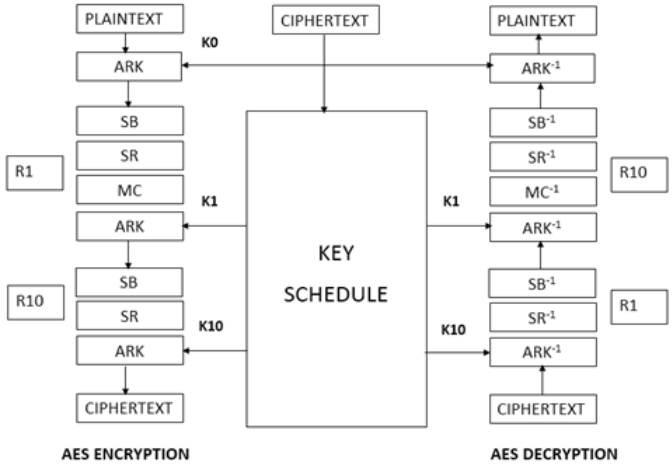


Figure 1. AES Rounds

These results are then arranged within the 4*4 matrix. Similar operation is performed during decryption and is known as Inverse Shift row [Lumbiarres-López et al. [2018]].

2.2.3 *Mix Columns (MC).* Every column of 4 bytes is soon converted engaging a specific function. This function gets input from the 4-bytes of the first column and outputs forming entirely new bytes, which restore the foremost column. Then we get a singular 4*4 matrix consisting of 16 unique bytes. Corresponding steps are used during decryption known as Inverse Mix column [Lumbiarres-López et al. [2018]].

2.2.4 *Add round Key:.* The 4*4 matrix is taken into account as 128-bit or 16-bytes are XOR with the generated key and if this is last round then the output becomes Cipher text. Corresponding steps are used during decryption known as Inverse Add round key [Lumbiarres-López et al. [2018]].

## 3. CRYPTANALYTIC ATTACKS ON THE AES ALGORITHM

Cryptography attacks are often a threat to the security of secret and confidential data. Cryptanalysis is the study of techniques for obtaining the meaning of encrypted information, without access to the secret information that is typically required to do so. Typically, this involves knowing how the system works and finding a secret key [Y.Oren et al. [2010]]. Cryptanalysis is also referred to as codebreaking or cracking the code. Cryptanalysis is also a way to test the strength of the cryptosystem. The cipher text is generally the easiest part of a cryptosystem to obtain and, therefore, is an important part of cryptanalysis [Ali and Mukhopadhyay [2011]]. Depending on what information is available and what type of cipher is being analysed, cryptanalysts can follow one or more at-tack models to crack a cipher. There are various kinds of attacks which are explained toward the cryptosystem [Karaklajić et al. [2013]]. Some attacks are easily readable while others required higher mathematical knowledge. The various types of cryptanalytic attacks are explained as follows:

### 3.1 Brute-force attack:

A Brute force attack is one of the sole attacks. During this attack, the attacker analyses to decrypt the message within the probable hidden key. A brute-force attack involves efficiently reviewing possible key combinations until the proper keys are detected.
With the technological advancements and with the availability of high performance computational platforms, the brute force attack is the best possible attack [Zodpe and Sapkal [2018]].

### 3.2 Ciphertext-only attack:

In cipher text-only attack, the attacker has full access various encrypted messages. Its ultimate aim is to urge back the plain text messages or a hidden key without knowing the plaintext or secret key [Khan and Mahanta [2014]]. After getting the encrypted key subsequent process is used to interrupt all the possible other messages that were encrypted by this key. While designing encryption algorithms, it is crucial to defend them toward Cipher text-only attacks, as they are the initial point for all cryptanalysis [Lin et al. [2018], Gan et al. [2017]]. Thus, the strategically analysed Ciphers are normally not very susceptible to these sorts of attacks [Nakai et al. [2014]].

### 3.3 Side channel attack:

The Side channel attacks observe power utilization and electromagnetic discharge when a tool is performing cryptographic activity. Side channel attacks guide toward electronic devices and systems which are comparably easy and cheap. The attackers can employ different side channel methods to collect information and deduce hidden Cryptographic keys [Atobe et al. [2012]].

### 3.4 Boomerang:

This attack deals with differential critical analysis by chosen plaintext and cipher text. The boomerang attack is an adaptive technique and its main aim is to break cipher in dual parts as well as in every part differential is applied. There is no alternate to this attack on AES. This attack, reduces the data complexity to 239 and 271 in the fifth and the sixth round. The whole time complexity of the attack is set at 232 and 271 for each reduced round with memory complexity of 233. There are no alternatives to this attack on AES [Li et al. [2019]].

### 3.5 Power analysis attack:

A power analysis attack is one of the side channel attack. The attacker studies the amount of power required to run the Cryptographic hardware device, the amount of power used, and thus the way long the facility is required to run the operations [Barenghi et al. [2010]]. The attacks can be prospective to select cryptographic keys and different hidden data from the cryptographic hardware [Martinasek and Zeman [2013]]. The various power analysis attacks in cryptographic hardware are as follows:

3.5.1 *Simple power analysis (SPA):.* Simple power analysis is a side-channel attack during which, it won't show the traces of the devices over time through visually in graphical form. Simple power analysis shows the variation in power consumption when different operations are being performed by the device. Simple power analysis is beneficial within the data-dependent features when the traces are show able during an anonymous presence [Safta et al. [2016]].

3.5.2 *Differential power analysis (DPA):.* Differential power analysis is additionally a side-channel attack that is employed to provide the statistical examination of power consumption within the cryptographic hardware. One technique is to limit the signal to noise ratio lesser the ratio, the larger the quantity of indication required to present an attack. Temporary noise is typically introduced into the device by fluctuating clocks, emulate odd wait states, odd data, or duplicate operations [Ni et al. [2017]].

### 3.6 Differential fault analysis attack (DFA):

In 2002, a new attack technique viz., the differential fault analysis was introduced to recover whole cryptographic keys while injecting faults within/during runtime [Takahashi et al. [2007]]. Fault is often injected by varying the facility level in hardware devices or by changing memory bit. DFA attacks are the most common attack in hardware and software of the devices. DFA has two fault injection techniques in AES, fault injected in the intermediate state and another one is a vital scheduling technique [Ali and Mukhopadhyay [2011]].

### 3.7 Square Attack:

The square attack is also known as saturation attack which is one of the devoted attack on a block cipher. The attack is implemented on AES and follows some properties of square cipher [Yu and Wei [2009]]. The A-set is a set of plaintext because of which the attack examining the propagation of attack are done by XOR. There are 256 set of plaintexts which are different in some of the bytes whereas some are similar in other bytes. The attack can be enforced to AES depraved to 4 rounds. The extension of the attack by adding end and start of cipher for whole six rounds. The prediction of few keys are assigned in the first round, fifth and sixth round for meeting the criteria.
The partial sum technique is the best square attack on the AES algorithm [Ferguson et al. [2000]].

### 3.8 Collision Attack:

Random alteration can be identified in AES in the three rounds as they are based on square attacks. AES form the random permutation that could be detected in the four rounds explained by Gilbert and Minier the author who compared the square attack. The phenomenon between collision and partial function were exploited by the cipher. In this the complexity of the plaintext of 2140 was replaced by 232, which deducts seven rounds in AES. Concluded that the complexity was reduced due to this modification was much faster than brute force attack [Gilbert and Minier [2000]].

### 3.9 Impossible Differential attack:

This type of attack has an impact on performance of Mix column transformation. For example, it implies on two plaintexts which are different in one byte, therefore the deduction in the cipher text of AES are not similar in the four rounds [Chen et al. [2014]]. The following bytes position: (0,0), (1,3), (2,2), (3,1), (0,1), (1,0), (2,3), (3,2), (0,2), (1,1), (2,0), (3,3) nor (0,3), (1,2), (2,1), (3,0). Incorrect key bytes are excluded if the difficult event happens.
Biham and Keller were the first to introduce the attack on AES-128 to reduce it to five rounds. Later the time complexity of 2122 by reaching sixth round and using 291.5 plaintext was improved by Cheon. In the same way by decreasing it to seven rounds for AES-192 and AES-256.Phan managed the technique that the attack requires 292 (AES-192) and 292.5 (AES-256) chosen plaintexts with time complexities of 2186(AES-192) and 2250.5(AES256). Concluded up to six rounds on AES-128 will be the best as well as difficult differential attack that breaks into seven rounds [Z'aba and Maarof [2006b], Cheng et al. [2016]].

### 3.10 Algebraic Attacks:

The main focus of this attack is on inside algebraic structure in AES. Rather than statistical, the attack is algebraic in nature. This attack deals with the derivation system of quadratic simultaneous equation as well as examining the internals of cipher. To retrieve the key specific algorithm is used in Sparse Linearization (XSL) attack solve the equations.
Pairs of cipher text and plaintext are created in interpolation attack which are done with the help of polynomials. The entire expression of cipher can be linked if and only it has compact algebraic expression. If they have low degree there is a manageable complexity in the polynomial of plaintext. Therefore, pairs of plaintext and cipher text can be determined in small amount by coefficient of polynomial. Coefficient of polynomials are explained by the formula known as Lagrange interpolation formula [Dobbertin et al. [2004], Kazmi et al. [2017]].

Table-1 shows the comparative analysis of few cryptanalytic attacks based on key size, number of rounds, time complexity, data complexity and memory. It is observed from the table that due to the high time and data complexity required for the cryptanalysis of AES algorithm, the algorithm is still secure.

| Attack | Key Size | No. of Rounds | Time Complexity | Data Complexity | Memory | References |
|---|---|---|---|---|---|---|
| Square | All | 6 | $2^{72}$ | $2^{32}$ | $2^{32}$ | Yu and Wei [2009] |
| Collision | 256 | 7 | $2^{140}$ | $2^{32}$ | $2^{32}$ | Gilbert and Minier [2000] |
| Impossible Differential | 128 | 6 | $2^{122}$ | $2^{91.5}$ | $2^{89}$ | Z'aba and Maarof [2006b] |
| Impossible Differential | 192 | 7 | $2^{186}$ | $2^{92}$ | $2^{153}$ | Z'aba and Maarof [2006b] |
| Impossible Differential | 256 | 7 | $2^{250.5}$ | $2^{92.5}$ | $2^{153}$ | Z'aba and Maarof [2006b] |
| Boomerang | 128 | 5 | $2^{39}$ | $2^{39}$ | $2^{33}$ | Li et al. [2019] |
| Boomerang | 128 | 6 | $2^{71}$ | $2^{71}$ | $2^{33}$ | Li et al. [2019] |

Table I: Summary of various attacks on the AES Algorithm

## 4. CONCLUSION AND FUTURE WORK

This paper presents an extensive survey of various cryptanalytic attacks on the AES algorithm. Most of the cryptanalytic attacks on the AES algorithm, reported in literature are impractical due to the large key size of AES algorithm. However, the emerging research in quantum cryptology and high performance computing pose a threat to AES-128. Taking into consideration, the attacks presented and available computational power, the AES algorithm is still expected to survive for a long period of time.

## References


Abdullah, A. 2017. Advanced encryption standard (aes) algorithm to encrypt and decrypt data. *Cryptography and Network Security*, pp.1–12.

Ali, S. and Mukhopadhyay, D. 2011. A differential fault analysis on aes key schedule using single fault. In *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*. IEEE Computer Society, Los Alamitos, CA, USA, pp.35–42.

Atobe, Y., Shi, Y., Yanagisawa, M., and Togawa, N. 2012. Dynamically changeable secure scan architecture against scan-based side channel attack. *2012 International SoC Design Conference (ISOCC)*, pp.155–158.

Barenghi, A., Bertoni, G., Breveglieri, L., Pellicioli, M., and Pelosi, G. 2010. Low voltage fault attacks to aes and rsa on general purpose processors. *IACR Cryptol. ePrint Arch. 2010,* 5, pp.130.

Bedoui, M., Mestiri, H., Bouallegue, B., and Machhout, M. 2016. A reliable fault detection scheme for the aes hardware implementation. In *2016 International Symposium on Signal, Image, Video and Communications (ISIVC)*. pp.47–52.

Chen, C.-N. and Yen, S. 2003. Differential fault analysis on aes key schedule and some countermeasures. In *Australasian Conference on Information Security and Privacy 2003 (ACISP 2003)*, . of Lecture Notes in Computer Science, Ed. Springer, pp.118–129.

Chen, P., cheng Liao, F., and ru Wei, H. 2014. Related-key impossible differential attack on a lightweight block cipher mibs. *Journal on Communications 35,* 2, pp.190–193.

Cheng, L., Xu, P., and Wei, Y. 2016. New related-key impossible differential attack on mibs-80. In *2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS)*. pp.203–206.

Chong, K. and Jean-Jacques, Q. 2008. New differential fault analysis on aes key schedule: Two faults are enough. *International Conference on Smart Card Research and Advanced Applications Springer-Verlag, London 5189*, pp.48–60.

Dobbertin, H., Knudsen, L., and Robshaw, M. 2004. The cryptanalysis of the aes - a brief survey. In *Lecture Notes in Computer Science*. pp.1–10.

Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D., and Whiting, D. 2000. Improved cryptanalysis of rijndael. *Fast Software Encryption. FSE 2000. Lecture Notes in Computer Science 1978,* 2 (04), pp.213–230.

Floissac, N. and L'Hyver, Y. 2011. From aes-128 to aes-192 and aes-256, how to adapt differential fault analysis attacks on key expansion. In *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography*. pp.43–53.

Gan, Q., Yu, S., Li, C., Lü, J., Lin, Z., and Chen, P. 2017. Design and arm-embedded implementation of a chaotic map-based multicast scheme for multiuser speech wireless communication. *International Journal of Circuit Theory and Applications 45,* 11, pp.1849–1872.

Genelle, L., Giraud, C., and Prouff, E. 2009. Securing aes implementation against fault attacks. In *2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. pp.51–62.

Gilbert, H. and Minier, M. 2000. A collision attack on 7 rounds of rijndael. In *In AES Candidate Conference*. pp.230–241.

Karaklajić, D., Schmidt, J., and Verbauwhede, I. 2013. Hardware designer's guide to fault attacks. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems 21,* 12, pp.2295–2306.

Kazmi, A. R., Afzal, M., Amjad, M. F., and Rashdi, A. 2017. Combining algebraic and side channel attacks on stream ciphers. In *2017 International Conference on Communication Technologies (ComTech)*. pp.138–142.

Khan, A. K. and Mahanta, H. J. 2014. Side channel attacks and their mitigation techniques. In *2014 First International Conference on Automation, Control, Energy and Systems (ACES)*. pp.1–4.

Kim, C. H. 2012. Improved differential fault analysis on aes key schedule. *IEEE Transactions on Information Forensics and Security 7,* 1, pp.41–50.

Li, K., Qu, L., Sun, B., and Li, C. 2019. New results about the boomerang uniformity of permutation polynomials. *IEEE Transactions on Information Theory 65,* 11, pp.7542–7553.

Li, W., Gu, D., Wang, Y., Li, J., and Liu, Z. 2009. An extension of differential fault analysis on aes. In *2009 Third International Conference on Network and System Security*. pp.443–446.

Lin, Z., Yu, S., and Lii, J. 2018. Chosen ciphertext attack on a chaotic stream cipher. In *2018 Chinese Control And Decision Conference (CCDC)*. pp.5390–5394.

Lumbiarres-López, R., López-García, M., and Cantó-Navarro, E. 2018. Hardware architecture implemented on fpga for protecting cryptographic keys against side-channel attacks. *IEEE Transactions on Dependable and Secure Computing 15,* 5, pp.898–905.

Martinasek, Z. and Zeman, V. 2013. Innovative method of the power analysis. *Radioengineering 22,* 2 (06), pp.586–594.

Nakai, T., Shibatani, M., Shiozaki, M., Kubota, T., and Fujino, T. 2014. Side-channel attack resistant aes cryptographic circuits with rom reducing address-dependent em leaks. *2014 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp.2547–2550.

Ni, Y., Cui, X., Wang, T., Fan, Y., Han, Q., Liu, K., and Cui, X. 2017. Improving dfa on aes using all-fault ciphertexts. In *2017 IEEE 12th International Conference on ASIC (ASICON)*. pp.283–286.

Park, J., Moon, S., Choi, D., Kang, Y., and Ha., J. 2010. Fault attack for the iterative operation of aes s-box. *5th International Conference on Computer Sciences and Convergence Information Technology*, pp.550–555.

Safta, M., Svasta, P., Dima, M., Marghescu, A., and Costiuc, M. 2016. Design and setup of power analysis attacks. In *2016 IEEE 22nd International Symposium for Design and Technology in Electronic Packaging (SIITME)*. pp.110–113.

Shan, W., Fu, X., and Xu, Z. 2015. A secure reconfigurable crypto ic with countermeasures against spa, dpa, and ema. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 34,* 7, pp.1201–1205.

Takahashi, J., Fukunaga, T., and Yamakoshi, K. 2007. Dfa mechanism on the aes key schedule. In *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2007)*. pp.62–74.

Y.Oren, Kirschbaum, M., Popp, T., and Wool, A. 2010. Algebraic side-channel analysis in the presence of errors. *Mangard S., Standaert FX. (eds) Cryptographic Hardware and Embedded Systems, CHES 2010. CHES 2010. Lecture Notes in Computer Science, vol 6225. Springer, Berlin, Heidelberg. 6225*, pp.428–442.

Yu, L., Zhang, D., Wu, L., Xie, S., Su, D., and Wang, X. 2018. Aes design improvements towards information security considering scan attack. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. pp.322–326.

Yu, X. and Wei, H. 2009. The square attack of reduced-round camellia. In *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*. pp.244–247.

Yuan, Y., Yang, Y., Wu, L., and Zhang, X. 2018. A high performance encryption system based on aes algorithm with novel hardware implementation. In *2018 IEEE International Conference on Electron Devices and Solid State Circuits (EDSSC)*. pp.1–2.

Zhang, J., Wu, N., Li, J., and Zhou, F. 2019. A novel differential fault analysis using two byte fault model on aes key schedule. *IET Circuits, Devices  Systems 13,* 5, pp.661–666.

Zodpe, H. and Sapkal, A. 2018. An efficient aes implementation using fpga with enhanced security features. *Journal of King Saud University - Engineering Sciences 32*, pp.115–122.

Z'aba, M. R. and Maarof, M. A. 2006a. A survey on the cryptanalysis of the advanced encryption standard. In *The Postgraduate Annual Research Seminar 2006 (PARS 2006)*. pp.97–102.

Z'aba, M. R. and Maarof, M. A. 2006b. A survey on the cryptanalysis of the advanced encryption standard. *Proceedings of the Postgraduate Annual Research Seminar 2006*, pp.97–102.

**Dr. Harshali Zodpe** is an Associate Professor in Dr. Vishwanath Karad MIT World Peace University, Pune (India). She has done her PhD in Electronics Engineering from College of Engineering, Pune. She has completed her M.Tech in VLSI Design from Shri. Ramdeobaba Kamla Nehru Engineering College, Nagpur and B.E in Electronics Engineering from Visvesvaraya National Institute of Technology, Nagpur. She has more than 13 years of teaching experience. Her areas of interests are VLSI, Cryptography and Embedded systems. She has published and presented papers in various reputed International Journals and Conferences.

**Arbaz Shaikh** is pursuing M.Tech (VLSI and Embedded Systems) in Dr. Vishwanath Karad MIT World Peace University, Pune (India). He has completed his Bachelor's from Vikhe Patil College of Engineering, Ahmednagar. His research interest include mathematical modelling of systems, cryptography and designing digital systems.