International Journal on Optimization and Applications

IJOA. Vol. 4, Issue No. 3, Year 2024, www.ijoa.ma

Fault Injection Attacks on AES Cryptosystems: Vulnerabilities and Protections

1st BOUSLAM Elmehdi

Master's degree in information systems security, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco

elmehdi.bouslam@uit.ac.ma

2nd AMGHNOUSS Redouane

Master's degree in information systems security, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco

redouane.amghnouss@uit.ac.ma

3rd HARBOUCH Taha

Master's degree in information systems security, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco

taha.harbouch@uit.ac.ma

4th DIKOUK OUSSAMA

Master's degree in information systems security, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco

oussama.dikouk@uit.ac.ma

Abstract-This article investigates the vulnerabilities of the Advanced Encryption Standard (AES) to fault injection attacks and explores protective measures against such threats. Fault injection attacks exploit physical and operational weaknesses in cryptographic systems, potentially compromising their security. Through detailed analysis and case studies, this research highlights the susceptibility of AES to various fault injection methods, including voltage glitching, temperature manipulation, differential fault analysis, laser fault injection, and electromagnetic fault injection. The article also reviews current advancements in defensive strategies, ranging from hardware modifications to sophisticated error detection mechanisms.

Keywords- AES, Fault Injection Attacks, Cryptographic Security, Differential Fault Analysis, Protective Measures.

I- Introduction

The Advanced Encryption Standard (AES) is a fundamental cryptographic protocol in the domain of digital security, serving to protect a wide range of information, from personal data to national security communications. While the theoretical foundation of AES is robust and it is widely employed, it is not immune to attacks. Among the most intricate and detrimental threats are fault injection attacks, which pose a significant risk to cryptographic systems. These attacks exploit physical vulnerabilities to introduce errors in the cryptographic process, potentially leading to the disclosure of secret keys and decryption of sensitive information without requiring direct access to plaintext.

The sophistication and efficacy of fault injection techniques, including voltage glitching, temperature manipulation, electromagnetic disturbances, and laser injections, have evolved, posing an escalating danger to cryptographic devices. By manipulating physical conditions to induce operational faults, attackers can modify the behavior of cryptographic algorithms, thereby circumventing traditional security measures. This vulnerability is particularly problematic in environments where hardware is accessible or in scenarios involving high value data, necessitating a comprehensive understanding and mitigation of these risks.

This article seeks to comprehensively evaluate the susceptibilities of AES to various fault injection attacks and to appraise the efficacy of current countermeasures. Through an examination of detailed case studies and recent research results, the study aims to highlight critical weaknesses in existing cryptographic implementations and to propose a framework for enhancing AES security. This encompasses an investigation of pioneering protective technologies and strategies, spanning from integrated hardware solutions to advanced error detection and correction mechanisms.

Furthermore, this discussion encompasses the implications of these vulnerabilities in real-world situations, underscoring the necessity for continual progress in cryptographic research and development. As attackers refine their methods, the cryptographic community must proactively tackle these emerging threats through rigorous testing, advanced security design, and the deployment of adaptive defensive systems that are resilient against numerous fault injection methodologies.

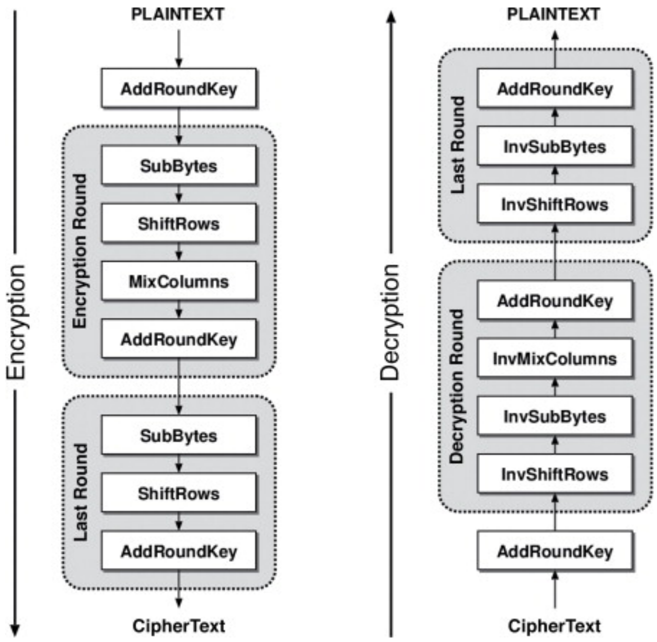
In conclusion, this article endeavors not only to educate about potential risks but also to stimulate further research and practical strides in cryptographic security. In doing so, it seeks to fortify the resilience of AES systems against the evolving landscape of fault injection attacks, thereby ensuring the continued safeguarding of information in an increasingly digitized world.

A - How AES works?

The AES Encryption algorithm (also known as the Rijndael algorithm) is a symmetric block cipher algorithm with a block/chunk size of 128 bits. It converts these individual blocks using keys of 128, 192, and 256 bits. Once it encrypts these blocks, it joins them together to form the ciphertext.

AES is designed as a block cipher, meaning it divides the data into fixed-size blocks (typically 128 bits) and encrypts them individually, transforming plain text into a secure form known as ciphertext. This process enhances the security of transmitted data by ensuring that even identical segments of plain text in different messages produce distinct ciphertext blocks.

To enhance the security of data, AES utilizes numerous cryptographic keys that undergo multiple rounds of processing. The AES standard accommodates key lengths of 128, 192, and 256 bits. Although AES-128 offers adequate protection appropriate for many consumer applications, higher levels of security, such as that required for classified information like Top Secret, necessitate the enhanced security provided by the 192 or 256-bit key lengths. The longer keys, while providing heightened security, also demand more processing power and prolong encryption time, thereby ensuring a trade-off between security demands and performance prerequisites.



Creation of Round keys :

A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.

SubBytes :

This step implements the substitution.

In this step each byte is substituted by another byte. Its performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16 byte (4 x 4) matrix like before.

The next two steps implement the permutation.

ShiftRows :

This step is just as it sounds. Each row is shifted a particular number of times.

•The first row is not shifted

•The second row is shifted once to the left.

•The third row is shifted twice to the left.

•The fourth row is shifted thrice to the left.

MixColumns :

This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

Add Round Keys :

Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes is not considered as a grid but just as 128 bits of data

The last round doesn't have the MixColumns round.

The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.

II- Fault Injection Attacks: An Overview and Case studies on AES

Fault injection attacks are a significant category of active attacks that have the potential to weaken highly secure cryptographic algorithms. These attacks take advantage of the physical weaknesses in cryptographic devices, introducing faults that can jeopardize the security of encryption methods, including the Advanced Encryption Standard (AES).

A - Definition and Methods

Fault injection refers to intentionally tampering with a device in order to disrupt its operations, thus compromising the security of cryptographic devices and potentially stealing data. Attackers use various methods to carry out fault injection:

- **Voltage Glitching:** poses a significant risk to the security of cryptographic systems, particularly those utilizing the Advanced Encryption Standard (AES). This method of injecting faults involves creating temporary voltage reductions that disrupt the regular operations of electronic elements, potentially resulting in incorrect computations or modified behavior in cryptographic devices. As elaborated in the research of Zussa et al. (2014) [1] voltage glitches can be particularly effective in causing timing constraint violations, where the temporary under-powering impacts the synchronization of operations within integrated circuits. This interference can expose cryptographic keys or compromise the encryption process, leading to security breaches. To address these vulnerabilities, the research evaluates a delay-based countermeasure aimed at identifying the emergence of timing violations induced by voltage glitches.

- **Temperature Manupilaton:** Utilization of Temperature and Voltage Manipulation for Differential Cryptanalysis: Methods for controlling temperature and voltage serve as potent techniques for inducing specific faults in cryptographic devices, crucial for effectively executing differential cryptanalysis attacks. Kumar et al. (2014) [2] delves into the use of these cost-efficient methodologies to achieve fault injection accuracies previously believed to be unattainable without sophisticated equipment like lasers. The authors demonstrate that through precise adjustments of supply voltage and ambient temperature, they can generate even the slightest fault effects necessary for cryptanalysis at targeted areas within a chip. This approach is proven to facilitate highly accurate attacks on application-specific integrated circuit (ASIC) implementations of contemporary ciphers such as PRINCE, with only a minimal number of fault injections required to compromise the encryption. These findings underscore the susceptibility of cryptographic hardware to environmental manipulations and suggest that implementations of the Advanced Encryption Standard (AES) could also be vulnerable under similar circumstances.

- **Differential Fault Analysis (DFA):** is a powerful technique in cryptanalysis that exploits hardware faults to uncover cryptographic keys. This method examines faults such as voltage spikes or temperature variations to infer encryption keys from differences between correct and faulty outputs. A recent study of Kim et al. (2012) [3] has exposed the vulnerability of AES implementations with fault protection to sophisticated DFA attacks. The research has introduced enhanced DFA techniques that effectively compromise AES-128, AES-192, and AES-256 standards by strategically inducing faults in the key generation process. These findings underscore the crucial necessity for robust protections against fault attacks and emphasize that traditional DFA countermeasures may prove inadequate when the key schedule is the specific target. This study not only advances our understanding of DFA but also prompts a reassessment of security measures in cryptographic devices to counter these refined fault injection strategies.

- **Laser Fault Injection:** The injection of faults using laser technology presents a significant risk to the security of AES implementations, even those that are equipped with advanced protective measures. A study of Selmke et al. (2016) conducted a trial of laser fault injection on an AES core that was shielded by a specific type of countermeasure [4]. The study brings to light the potential to bypass the protective mechanisms of AES, particularly those that rely on hardware redundancy for detecting faults. Through the precise targeting and manipulation of cryptographic computations using simultaneous laser faults, malicious actors can effectively neutralize security enhancements based on redundancy, such as the aforementioned countermeasure. This approach entails injecting identical faults into multiple branches of a redundant AES setup, thereby undermining traditional protections against differential fault analysis (DFA). The research emphasizes the need for the development of more resilient fault detection methods capable of withstanding the accuracy and stealth of targeted laser attacks. It suggests that relying solely on hardware duplication may be insufficient for applications requiring high-security measures.

- **Electromagnetic Fault Injection (EMFI):** refers to an advanced method of active attack that disrupts the typical operations of cryptographic devices by subjecting them to deliberate electromagnetic disruptions. Maldini et al. (2018) the utilization of genetic algorithms to enhance EMFI is examined, with a focus on optimizing fault-inducing parameters for improved effectiveness [5]. This strategy facilitates a more efficient detection of vulnerabilities in cryptographic implementations like AES. Through systematic adjustments to the electromagnetic pulse properties and the placement of the electromagnetic probe, the genetic algorithm can pinpoint fault-inducing conditions with greater accuracy compared to conventional techniques. The heightened capability to induce faults allows for more thorough exploration of potential weaknesses in the AES implementation, thus underscoring critical areas necessitating robust protective measures.

B - Targeted Components of AES

The Advanced Encryption Standard (AES) is particularly susceptible to fault injection attacks at several critical stages of its operation:

- **Key Schedule**: Any faults in the key schedule can result in partial or complete exposure of the encryption key. Since the key schedule is responsible for expanding the initial key into multiple round keys, any manipulation can jeopardize the entire encryption process.

- **S-Box Computations:** The substitution box (S-Box) utilized in AES is of utmost importance for ensuring non-linearity in encryption. Faults in this area can simplify the output structure, rendering the encryption susceptible to cryptanalysis.

- **MixColumns:** Faults introduced during this transformation can alter the diffusion properties of AES, reducing the complexity needed for secure encryption and making the system vulnerable to attacks that exploit these weaknesses.

III- Vulnerabilities in AES Cryptosystems: Understanding the Impact of Fault Injection Attacks

The Advanced Encryption Standard (AES) is commonly seen as a strong cryptographic framework, providing substantial security advantages for a range of uses, from securing private communications to safeguarding sensitive data in commercial and government settings. Nevertheless, similar to all cryptographic systems, AES is not resistant to all types of attacks. One of the most worrying types of attacks is fault injection attacks, which make use of physical weaknesses to compromise the security of encrypted data.

One of the pivotal methods employed in these attacks is Differential Fault Analysis (DFA). DFA targets specific rounds within the AES encryption process to analyze discrepancies between expected and faulty outputs. By introducing faults during intermediate rounds of AES, attackers are able to detect variations in output that directly correspond to the secret encryption key. This approach was highlighted in Ali et al (2012) [6], which elucidated how injecting faults strategically could enable attackers to discern the entire encryption key with alarming accuracy. The effectiveness of this method is grounded in the predictable structure of AES. AES operates through multiple rounds of permutations and substitutions; by disrupting these operations, the resulting errors can disclose information about the internal state of the cipher. For example, if a fault alters a specific bit in the 8th round, the alterations in the output can directly indicate how bits in the key influence particular transformations. This study illustrated that even faults injected within a limited scope within the AES rounds could empower an attacker to retrieve the entire key with disturbing precision, posing a significant threat to systems reliant on AES for security.

Another notable vulnerability discussed in Fuhr et al. [7] , pertains to attacks that do not necessitate access to or familiarity with the original plaintext. Instead, these attacks depend solely on flawed ciphertexts resulting from compromised encryption processes. Through meticulous examination of the errors within these ciphertexts, arising from targeted fault injections in subsequent encryption rounds, adversaries can effectively derive the secret key. This approach underscores a pivotal vulnerability: the security of AES could be undermined without the need to breach the higher threshold of direct plaintext access. The key novelty of this approach lies in the exploitation of errors directly stemming from faults in the later rounds of AES. These faults can disrupt the final stages of the encryption process, leading to flawed ciphertexts still containing systematic errors based on the precise nature of the fault and its impact on the structure of the AES algorithm. By scrutinizing the distribution and characteristics of these faults, adversaries can trace back to the AES key bits implicated in the specific rounds affected by the faults. This method proves particularly potent as it does not necessitate any knowledge of the plaintext, solely a collection of flawed ciphertexts, thereby broadening the spectrum of potential attack scenarios.

Both studies illustrate critical vulnerabilities in AES when subjected to fault injection attacks. The DFA study emphasizes the risks posed by accessible physical access to the cryptographic device during operation, highlighting the need for physical security measures as part of cryptographic design. Conversely, the study on exploiting faulty ciphertexts reveals a different risk dimension where attackers do not need to control the input to the encryption process, a scenario that could potentially bypass many conventional security measures. Together, these studies underscore the necessity for robust, layered security strategies that address both internal algorithm robustness and external physical security to safeguard against evolving fault injection techniques.

IV- Protective Measures Against Fault Injection Attacks

Fault injection attacks present a critical security challenge to cryptographic systems, exploiting vulnerabilities to disrupt operations and extract sensitive data. These attacks can manipulate hardware or software to introduce errors into cryptographic computations, potentially compromising the security of the system. As these threats evolve, robust countermeasures are essential to ensure the integrity and confidentiality of cryptographic operations. This discussion explores various strategies developed to safeguard systems against such vulnerabilities, including preventive, detection, and response techniques

A- Preventive Techniques:

Preventive techniques aim to forestall fault injection attacks before they can impact the cryptographic process. An effective method discussed by Qiang et al. [8], they introduces two innovative methods that leverage the concept of parity checks to enhance fault detection while balancing security and overhead. These methods are termed "mixed-grained parity check" and "word recombination parity check."

• **Mixed-Grained Parity Check:** This approach applies different levels of granularity in parity checking—finer for security-critical operations and coarser for less critical ones. This method improves fault coverage while managing the overhead effectively.

• **Word Recombination Parity Check:** It reduces hardware overhead by recombining sub-words from different operations to form new words for parity checking. This approach is likened to a fine-grained check but with reduced resource usage.

On another study focuses on software-based countermeasures specifically designed to thwart fault injection attacks during the execution of cryptographic algorithms like AES on ARM platforms [9], suggests selectively applying redundancy to the most sensitive parts of the cryptographic process, such as key fetching and table lookups. This approach aims to prevent successful attacks by reducing the attack surface.

B - Detecting Techniques:

Although the primary focus is on prevention, the preventive mechanisms inherently assist in fault detection. By dispersing the impact of faults across the system state in an unpredictable manner, these strategies help identify anomalies that indicate tampering, thereby enabling early detection of fault injections.

Ahish et al. (2020) [10], discuss the use of a low-power CMOS-based mixed-signal framework to detect Differential Fault Analysis (DFA) based clock-glitch attacks by monitoring power side-channel statistics. The study implements this technique using CMOS current-mode Gilbert Gaussian Circuits-based Gaussian kernels. The method allows for dynamic updates to the statistical model in real-time through a sliding window approach, and it includes adjustable parameters to enhance detection efficiency, such as kernel standard deviation and likelihood threshold.

By leveraging these methods, the system can detect not only intentional clock-glitch attacks during encryption but also unintentional glitches due to external noise or design inefficiencies, further enhancing the robustness of the security implementation.

C – Response Techniques:

In the face of detected faults, employing infective countermeasures is crucial, in the study of Shamit Ghosh et al. (2017) [11] details the use of infective countermeasures, where any detected fault leads to a controlled yet randomized alteration of outputs. This ensures that any data derived from fault-induced computations is rendered useless to the attacker, effectively containing the damage and mitigating any advantage that could be gained from the attack.

V - Recent Advances in Protection Against Fault Injection Attacks on AES Cryptosystems

The cryptographic systems, particularly the Advanced Encryption Standard (AES), must progress in tandem with the evolving cybersecurity threats. The ongoing risk of fault injection attacks has led to numerous technological advancements and state-of-the-art research dedicated to enhancing the resilience of AES against these intrusive methods.

A - Technological Innovations

Recent technological advancements have significantly enhanced the protection mechanisms for AES against fault injection attacks:

• **Integrated Hardware Security Modules (HSMs):** Modern developments in HSMs have introduced sophisticated sensors and active defensive mechanisms capable of detecting and mitigating physical anomalies indicative of fault injections. These modules are specifically designed to operate under hostile conditions where tampering risks are prevalent. They can swiftly trigger protective responses such as immediate shutdowns or transitions to secure operational states, thwarting attackers' attempts to exploit fault-induced errors.

• **Error Correction Code (ECC) Memory:** The adoption of ECC memory in cryptographic devices is another crucial innovation. ECC memory is designed to automatically correct common types of data corruption that could be induced by fault injections, thereby preventing errors that could lead to the leakage of sensitive information or erroneous decryption outputs.

• **Dynamic Cryptographic Algorithms:** Some of the latest approaches include algorithms that dynamically alter their operational parameters in response to detected anomalies. By adjusting their behavior in real-time, these algorithms obscure cryptographic keys and data, thus complicating any attempts by attackers to leverage consistent patterns in fault injections for their gain.

B - Research Frontiers

The frontier of cryptographic research continues to push the boundaries of security with novel strategies aimed at countering fault injection attacks:

• **Quantum Cryptography:** The advent of quantum computing technologies brings with it new methodologies in cryptography, such as Quantum Key Distribution (QKD). Quantum cryptography is seen as a potential game-changer, inherently secure against many forms of eavesdropping and tampering, including sophisticated fault injections, due to the principles of quantum mechanics.

• **Artificial Intelligence in Anomaly Detection:** Leveraging artificial intelligence (AI) and machine learning to enhance fault detection capabilities in cryptographic systems represents a promising research direction. AI models can be trained on extensive datasets of normal and compromised operational states to recognize and respond to patterns indicative of fault injections, potentially preventing attacks before they compromise the system.

• **Advanced Fault Tolerance Designs:** Ongoing research is also focused on developing more robust fault tolerance architectures that incorporate features such as redundancy, self-repair capabilities, and enhanced error detection at a granular level. These designs aim to maintain the overall integrity and security of the cryptographic process, even when parts of the system are compromised.

The ongoing technological innovations and research efforts are vital in ensuring the robustness of AES against the continually evolving threat of fault injection attacks. By staying ahead of potential vulnerabilities through advanced protective measures and proactive research initiatives, the cryptographic community can safeguard the security and privacy of data across digital platforms.

VI. Conclusion

Our investigation has uncovered that despite its resilient design, AES is vulnerable to various fault injection techniques that could compromise cryptographic keys and decrypt sensitive information. It is vital to implement effective countermeasures, encompassing both hardware and software solutions, to bolster the security of AES implementations.

Future research should prioritize the development of more robust cryptographic frameworks capable of withstanding emerging fault injection methods. This entails exploring novel fault detection and response techniques, integrating advanced materials and technologies, and potentially leveraging quantum cryptography to provide intrinsic security against fault attacks.

The continual evolution of fault injection attacks poses a substantial threat to cryptographic systems. It is crucial for the cybersecurity community to maintain vigilance and proactively strengthen the security measures of AES cryptosystems. Collaboration between academic researchers and industry practitioners will be indispensable in advancing the landscape of cryptographic security.

References

[1] Zussa, L., Dehbaoui, A., Tobich, K., Dutertre, J.-M., Maurine, P., Guillaume-Sage, L., Clediere J., Tria, A. (2014). Efficiency of a glitch detector against electromagnetic fault injection. Design, Automation & Test in Europe Conference & Exhibition (DATE), 2014.

[2] Kumar, R., Jovanovic, P., & Polian, I. (2014). Precise fault-injections using voltage and temperature manipulation for differential cryptanalysis. 2014 IEEE 20th International On-Line Testing Symposium (IOLTS).

[3] Kim, C. H. (2012). Improved Differential Fault Analysis on AES Key Schedule. IEEE Transactions on Information Forensics and Security, 7(1), 41–50.

[4] Selmke, B., Heyszl, J., & Sigl, G. (2016). Attack on a DFA Protected AES by Simultaneous Laser Fault Injections. 2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC).

[5] Maldini, A., Samwel, N., Picek, S., & Batina, L. (2018). Genetic Algorithm-Based Electromagnetic Fault Injection. 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC).

[6] Ali, S. S., Mukhopadhyay, D., & Tunstall, M. (2012). Differential fault analysis of AES: towards reaching its limits. Journal of Cryptographic Engineering, 3(2), 73–97.

[7] Fuhr, T., Jaulmes, E., Lomne, V., & Thillard, A. (2013). Fault Attacks on AES with Faulty Ciphertexts Only. 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography.

[8] Maoshen, Z., He, L., Peijing, W., & Qiang L. (2022). Parity Check Based Fault Detection against Timing Fault Injection Attacks. Electronics 2022, 11(24), 4082.

[9] Barenghi, A., Breveglieri, L., Koren, I., Pelosi, G., & Regazzoni, F. (2010). Countermeasures against fault attacks on software implemented AES. Proceedings of the 5th Workshop on Embedded Systems Security - WESS '10.

[10] Shylendra, A., Shukla, P., Bhunia, S., & Trivedi, A. R. (2020). Fault Attack Detection in AES by Monitoring Power Side-Channel Statistics. 2020 21st International Symposium on Quality Electronic Design (ISQED).

[11] Shamit Ghosh , Dhiman Saha, Abhrajit Sengupta and Dipanwita Roy Chowdhury (2017). Preventing fault attacks using fault randomisationwith a case study on AES. International Journal of Applied Cryptography Vol. 3, No. 3 , 225-235.