International Journal of Computer Sciences and Engineering
Vol.**11**, Issue.**11**, pp.**22-34**, November **2023**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Survey Paper

Faults Attacks on Modern & Post Quantum Crypto Systems, Countermeasures and Evaluation

Venu Nalla[1], G. Padmavathi[2*], Dharavath Narendar[3], U. Surya Kameswari[4]

[1]Acharya Nagarjuna University Guntur; CRRao AIMSCS, Hyderabad
[2,3]CRRao AIMSCS, Hyderabad
[4]Acharya Nagarjuna University Guntur

**Corresponding Author: padmavathi@crraoaimscs.res.in*

Received: 01/Oct/2023; **Accepted**: 04/Nov/2023; **Published**: 30/Nov/2023. **DOI**: https://doi.org/10.26438/ijcse/v11i11.2234

Abstract: From and practical fault attacks have been published that pose a serious threat to most of the crypto-algorithms the time of announcement of new cryptanalytic attack called fault attack proposed by Bellcore in Sep 1996, multiple theoretical. Fault attacks circumvent the intricate mathematics of ciphers and swiftly extract the cipher's secret key. This is achieved by disrupting the system's normal behaviour, inducing faults that result in its faulty operation. The efficiency of these attacks has been improved over a period of time in making them more practical. Because of this, multiple techniques to counter the attacks are also published, that increase the complexity of attacks with the goal of making them impossible in the future. This paper covers the various fault attacks & countermeasures on symmetric, asymmetric and Post-Quantum crypto (PQC) algorithms along with various ways of resistance evaluation &their rating.

Keywords: SCA, Fault attacks, Symmetric, Asymmetric, PQC, Evaluation

1. Introduction

Cryptography plays major role in security of devices and the data stored in them by resisting attackers/hackers trying for unauthorized access of private and confidential data. Thanks to cryptanalysis techniques, for helping these crypto-algorithms to evolve into much stronger versions. As technology progresses, several new/modified attacks will come forth. One such attack is fault attack.

Faults may occur accidently or can be intentional. Accidental faults are natural like anomalies happening in electronic equipment's, alpha particle effects on semiconductor electronics, etc. But in fault attacks, faults are of intentional in nature and induced by adversary to get internal information of the system.

A fault attack belongs to the category of side-channel attacks, wherein a deliberate fault is introduced into a cryptographic implementation to expose the secret key utilized by the cipher as shown in *figure 1*. By examining the differential characteristics of nonlinear operations within the algorithm, the secret key can be deduced when provided with cipher texts from both correct and faulty implementations. Typically, a faulty ciphertext is discovered by applying external influences to a device that incorporates the algorithm, such as introducing voltage variations, glitches, lacerations, and more. Remarkably, even tamper-resistant devices remain susceptible to fault attacks.

The resilience of cryptographic systems is seriously threatened by side-channel fault attacks. Conventional security solutions that just concentrate on algorithmic strength are no longer enough since attackers can take advantage of the implementation's physical features. It is essential to comprehend the particular issues brought about by these attacks in order to create effective countermeasures. To protect systems from these hidden risks, issues including information leakage, non-invasive data extraction, and the possible compromise of cryptographic keys need to be closely examined.

Nowadays, side-channel fault attacks are very important to understand in cyber security. Strong defenses against these sneaky threats are required since embedded systems are widely used in commonplace products like smart cards, secure communication protocols and Internet of Things (IoT) devices. Side-channel fault attacks can compromise sensitive information, such as financial transactions or national security data. For this reason, it is imperative to resolve these vulnerabilities as soon as possible.

The necessity to compile information and insights about side-channel fault attacks at one place is what spurred this survey. This survey seeks to provide academics, practitioners, and policymakers with the necessary knowledge to strengthen cryptographic systems against these emerging dangers by offering a current state of research, practical implications, and proposed mitigations. Maintaining the integrity of our digital

infrastructure and staying ahead of prospective adversaries need a proactive understanding of side-channel fault attacks, which is becoming increasingly important as the cyber security landscape changes.

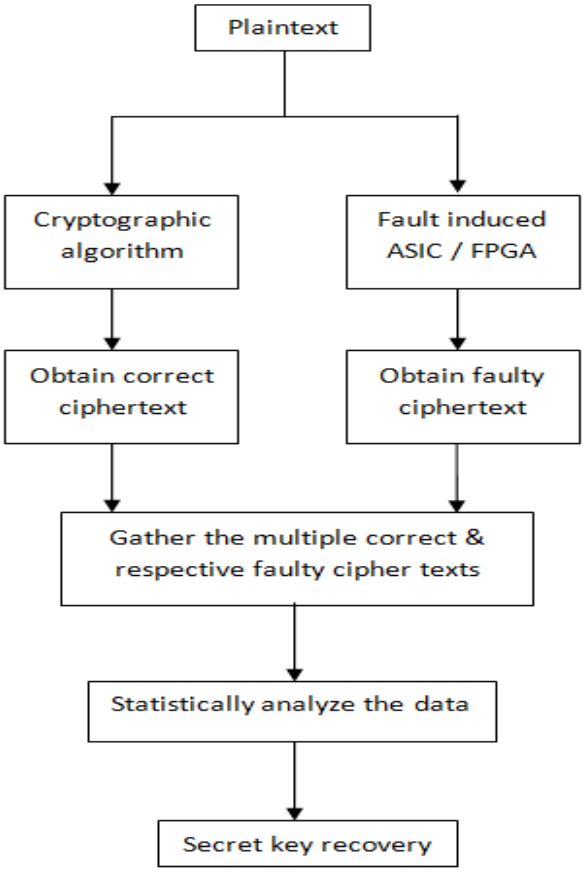

Figure 1: General Fault attack model

This paper describes, various fault attacks and their respective counter measures so far in the literature. Crypto research can be pictured as a cycle of attacks & countermeasures. Most of the countermeasures doesn't stop the attacks but increase the complexity in mounting the attacks. So, evaluation of the resistance of crypto devices is also vital. Hence, this paper also includes a discussion on evaluation and parameters for rating them

From this point, the content is structured in the following manner. Section-2 covers fault models and projects light into various parameters involved in it. Section-3 briefly describes various fault analysis methods. Section-4 shows fault attacks on various categories of algorithms and Section-5 puts light on various countermeasures. Section-6 gives evaluation techniques and various parameters used for rating the crypto algorithms. Conclusion follows in section-7.

1.1 Fault Models

Generally, fault attacks intend to break the security of functionality of a system by forcing it to an unintended behaviour. For this to happen, attacker injects concentrated hardware fault by purposely disturbing the operation of the system, exploits the effect of fault and break the system security. Origin of vulnerability will be at hardware level while exploitation will be at software level.

In this attack scenario, the attacker is unable to directly modify the structure of the chip or program's binary but can control the operating condition of the processor at hardware level. The attacker may also give input to the intended code and keep track of effects of unusual operation at software level through its output.

The more the model is constrained, the attack will be proportionally easier but it becomes proportionally more difficult in practical scenarios.

1.1.1 Modelling with abstract levels

Fault attack can be modelled in various abstract levels in both the major parts of the attack as mentioned below:

In the process of fault Injection, the abstract levels are

- Transistor level
- Logic level (targets can be gates and flip-flops)
- RTL level (targets can be ALU, REG's, MEM)

And while exploiting the fault, the abstract levels are

- Arithmetic level (as shown in *figure 2*)
- Cryptographic primitives' level
- Protocol level

1.1.2 Modelling with parameters

Fault attacks can also be modelled using following parameters of the fault being injected into the system.

1.1.2.1 Granularity of the fault

It can be explained as either number of bits affected by injection of fault which can be flipping a particular bit, random bit, stuck-at zero, stuck-at one, etc or as an impact on the target system ranged from single bit to few bits (up to a word). It can be non-invasive (like no physical damage to device, modify working conditions, etc.), semi-invasive (like chip de-capsulation, milling, etching, cleaning, etc.) or invasive (like to establish electrical contact to chip, modification, destruction, etc.) in nature. Non-invasive may require moderate knowledge of equipment, semi-invasive can be done with affordable equipment and invasive may require expensive equipment.

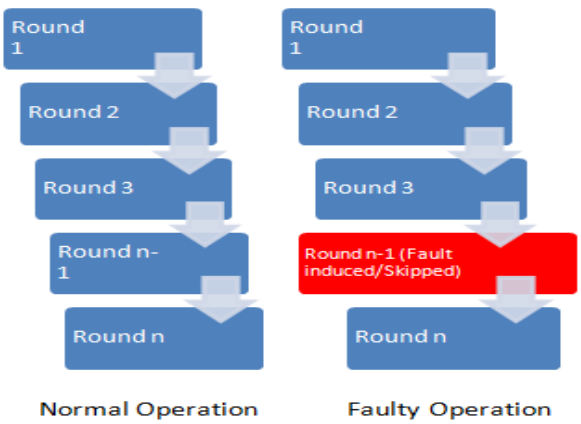

Figure 2: Example of fault injection into cryptographic implementation

1.1.2.2 Type of fault
The attackers can induce fault which can be input-output type (where fault can be directly induced at input) or can induce at positions which allows malfunction in memory, clock circuit, etc. The fault on hardware can be of instruction level, micro architecture level, circuit level or in side-channels like temperature, circuit voltage, EM radiation, etc.

1.1.2.3 Source of fault
There are several sources to inject fault into the system. Some of them are Clock glitch, Voltage glitch, Underfeeding, Heating, EM pulse, Light pulse, Light radiation, Focused Ion beam, LASER beam, Localized EM pulse, etc.

1.1.2.4 Intensity of fault
It can be described as an amount of the strain induced on the processor due to physical factors.

1.1.2.5 Efficiency of the fault
It can be explained as a precision in injecting fault which is how precisely or loosely, attacker can choose the fault value.

1.1.2.6 Repeatability of the fault
It is ability where whether attacker can produce same or similar fault in spatial or temporal domains of the system.

1.1.2.7 Feasibility of the fault
It refers to real-time aspects like budget& equipment required for the setup, Expertise level required to operate the setup, duration of the fault which can be permanent, transient or destructive.

2. Fault attack techniques – Related Work

Fault attacks are attacks which use side channel for injecting faults into devices to make them misbehave for certain amount of time. These attacks are actively being studied since 1996 by the research communities. Skorobogatov and Anderson executed the initial practical fault attack in 2001 in which photo-flash is used to flip a bit in memory [1].

Later to above attack, various attacks have emerged in both symmetric and public key crypto systems. Bao et al., mounted a first attack on public key crypto system using transient faults [2]. Fiat-Shamir and Schnorr, attacked RSA using active fault attacks [3]. Marc J and Jean-Jacques Q, have chosen to attack on signing key of RSA Montgomery instead of message [4]. Joye & Quisqater and Klima & Rosa, have also carried out successful fault attacks on RSA crypto systems [5,6]. Voyiatzis and Serpares, mounted successful attack on Fiat-Shamir schemes[7]. The inaugural practical differential fault attack on symmetric key crypto system is performed by Biham and Shamir, where attack was on DES [8]. Jacob et al., have used fault attacks to extract secret data from obfuscated ciphers [9]. Biehl et al., attackedElliptic curve crypto system (ECC) using DFA [10]. ZhengY, attacked random number generators using faults [11]. Even though there are multiple fault attacks, some research works defined fault attacks in general steps where each author took different abstract levels.

2.1 Implementation techniques of FA
According to Sayandeep Saha et al., fault attacks can be implemented in broadly three steps; Distinguisher Identification (wrong key guess moves the distinguisher to a uniform distribution while correct key guess makes it a non-uniform distribution), Divide-and-Conquer(divide into subparts which are independent in nature and can be computed efficiently) and Estimating the Number of Possible Key Candidates (If distinguisher reduces search space to a sufficient level, then attack may be successful with less faults and vice versa) [12].

According to Bilgiday yuce et al., fault attacks can be implemented in broadly five steps which are Injection of fault, Manifestation of fault, Propagation of Fault, Fault observation& Exploitation of Fault [13]. Their implementation techniques are in the *table-1*.According to Christophe Giraud et al., fault attacks can be categorized according to the origin of the introduced fault [101]. The first fault attack induced faulty behaviour in smart cards by glitch attack, where glitch is non-invasively applied to one of the chip contacts (Vcc pin, GND pin or Clock pin). The light attacks, uses energy of a light as emission, (from materials like flash camera, Laser, etc.) to disturb the silicon inside the chip [1,25,102]. The memory cells or logical gates can be easily disturbed by this photoelectric current and reciprocate to it. The parameters to be considered are energy of the light beam, light beam, light wave length, duration of emission and location of the attack. Magnetic attack is a semi-invasive attack, uses magnetic field on component to create local current which may generate a transient fault [104]. The parameters to be considered are power of magnetic field, localization on the chip and its duration.

Table-1: Generalized Fault attack steps and their implementation

Generalized FA steps	Implementation
Fault injection	Hardware controlled fault injection techniques • Tampering with clock pin [16]. • Tampering with supply voltage pin [20]. • Tampering with operating temperature [21]. • Combination of temperature, frequency & voltage [16]. • Optical fault injection [25]. • EM fault injection [30].
	Software controlled fault injection techniques • Manipulating the DVFS interface [31]. • Triggering memory disturbance errors [37].
Fault manifestation	• Location of fault [38]. • Size of fault [39]. • Effect of fault [39]. • Duration of fault [40].
Fault propagation	• I-Mem, I-fetch, I-Decode: o Opcode part: another instruction executed o Source operand addresses: they will be retrieved from wrong location. • O-fetch: faulty address or value of destination register, faulty update of flags • Execute: faulty address or value of destination register, faulty update of flags • Store: faulty address or value of destination register, faulty update of flags • Register file: incorrect source operands being

	fetched from register file • D-Mem & Conditional flags: absence of impact.
Fault observation	• Faulty cipher text • Abrupt change in the consumption of power in device [56]. • Micro architectural effects in performance counter [41].
Fault exploitation	• Using fault models o Corruption in data flow of target program (which can set, reset, flip or random nature in bit, byte or word) [39]. o Skipping an instruction execution [44]. o Skipping multiple instruction [47]. o replacing an instruction [20]. o altering the conditional branch value [50]. o loop counters tampering [51]. • Cryptanalysis using fault injection o DFA [53,60]. o Biased fault analysis [64,65]. o Safe error analysis [66,68]. o Algorithm specific fault analysis [71,72]. • Assisting SCA [73,77,80,88]. • Fault enable logical attacks [20,24,31,37,44,93,94]. • Assisting reverse engineering [96,97].

Sayandeep Saha et al., proposed a novel strategy called as Fault Template Attack (FTA), which involves fault templets to efficiently exploit fault characteristic from various locations of fault occurrence through which distinguishable fault patterns are constructed thereby recovering the key [105]. Multiple fault locations are exploited for this attack even though fault is given at a single location.

The effectiveness of the strategy is evident in its ability to target the middle rounds of the cipher, all without requiring complete access to the CT and its nature (whether it is correct or faulty). The main observation is that the fault induced at one AND gate input depends on other input value. In other words, fault propagation depends on data being processed. By this observation, attacks on masking schemes are performed which is one area of countermeasures of fault attacks.

2.2 Classification of various FA

Anubhab Bakshi et al., broadly classified FA into three major areas as given in *table-2* [106]. In order to extract sensitive information, Difference based Fault Analysis focuses on purposefully introducing faults and monitoring the differential effects on the output of the cryptographic system. On the other side, collision-based fault analysis causes collisions during computing in order to examine the patterns that emerge, with the goal of exploiting these collisions to undermine system security. By using statistical techniques, Statistical Fault Analysis analyses the overall efficacy and relevance of purposefully induced defects on cryptographic algorithms. Each method provides distinct insights into cryptographic systems vulnerabilities, giving analysts and attackers a variety of options for compromising or assessing the security of targeted systems.

2.3 Automated Frameworks of FA

Several efforts were made on automated frameworks for evaluating effectiveness of fault attacks i.e., given a cipher, attack prone areas will be analysed automatically. The first step of cipher-level automation in fault analysis are made by Fan Zhang et al. (requires manual effort in algebraic form representation of cipher and then SAT solver identifies vulnerabilities) [34]. Punit Khanna et al. (requires manual efforts in identifying non-linear operations of cipher and then identifies vulnerabilities using fault propagation patterns) [35].

Table-2: Classification of Fault attacks

Category	Fault attack	Goal
Difference based FA	Differential Fault Attack (DFA) [8].	Observes the differences in the output when correct & faulty inputs are processed
	Algebraic Fault Attack (AFA) [14].	Focus on exploiting mathematical relationships in the cryptographic algorithm that may be exposed due to faults
	Impossible Differential Fault Attack (IDFA) [15].	Exploits the concept of "impossible differentials" in the cryptographic algorithm
	Linear Fault Attack (LFA) / Integral Fault Attack (IFA) [17].	Exploits linear relationships in the cryptographic algorithm
Collision based FA	Collision Based Fault Attack (CFA) [18].	Create collisions and observes respective outputs to deduce information about the internal state of the system.
	Internal Differential Fault Attack (InDFA) [113].	Creates differential effects in the algorithm's internal state, leading to observable differences in the next computations
	Safe error analysis (SEA)/Ineffective Fault Analysis (IFA) [66].	to assess the resilience of a cryptographic system against unintentional errors that may occur during normal operation
Statistical based FA	Non-uniform error value attack (NUEVA) [26].	Exploits the non-uniformity of the errors to gain information about the internal state of the system.
	Non-Uniform faulty value attack (NUFVA) [27].	Similar to NUEVA but focus here is on the faults causing specific values or patterns in the system's computation
	Fault sensitivity analysis (FSA) [28].	Locates vulnerable points in the algorithm where faults are likely to have a more impact on security of the system.
	Differential fault intensity analysis (DFIA) [61].	Understands the intensity of faults leading to optimization of the fault injection process for maximum impact
Others	Statistical Ineffective Fault Attack (SIFA) [29].	Attacker observes the areas where faults do not have a statistically significant impact on the desired information.
	Persistent fault attack (PFA) [32].	The goal is to observe the cumulative effects of persistent faults on the cryptographic system.
	Fault Intensity Map Analysis (FIMA) [33].	Creates a map that characterizes the intensity or strength of faults across different points in a cryptographic algorithm

Some fully automated frameworks using machine learning approaches are proposed in literature like:

- Sayandeep Saha et al. used association rule mining approach [12].
- Sayandeep Saha et al. used data mining approach [36].
- Sayandeep Saha et al. used random forest approach, etc [42].

Work on software-level automation techniques is carried out by Jakub Breier et al., which focuses on assembly level implementation and reveals vulnerabilities hidden in cipher-level approaches [43]. They stated an example that if substation layer and permutation layer are combined as a lookup table then cipher-level approaches may over look any new vulnerability. Analysis of equations formed in these techniques is performed by Xiaolu Hou et al., automatically by using SMT solver [45].

Work on hardware-level automation techniques is performed by Jan Burchard et al. and Mael Gay et al., where the cipher's hardware specifications are utilized to generate a roster of faults using an exploited fault model, which is then represented in CNF (Conjunctive Normal Form) and examined through a SAT solver [46,48].

Sayandeep Saha et al., developed for the first time, a completely automated machine learning based framework which exploits fault space characterization in block ciphers [42]. When this machine learning framework is trained using a range of exploitable fault instances within a cipher, it becomes capable of predicting potential attacks on the same cipher. It is evaluated on to standard LW-block ciphers (LED and PRESENT) and obtained results showed training accuracy between 85-93%. Later, they also proposed a strategy which reduces misclassifying of exploitable faults which successfully reduced false negatives by fully testing around 20% of total fault samples. They also studied effect of DFA on three structurally similar S-Boxes (PRESENT, SERPENT and SKINNY) in which S-Box of SKINNY has displayed more DFA resistance compared to remaining two ciphers.

3. Algorithmic attacks

Fault attacks have bypassed security of several standard crypto systems. Here we focus on popular algorithms attacked by Fault Attacks and their attack complexities.

3.1 Symmetric crypto system:

Data Encryption Standard (DES) was first widely used symmetric key modern cipher and Biham and Shamir performed successful DFA where only 50-200 ciphertext were required [8].

Advanced Encryption Standard (AES) has replaced DES in year 2000 and being widely used till present and multiple DFA attacks are published on AES. Giraud et al. performed Bit attack using around 50 Ciphertext and Byte attack using around 250 Ciphertext [57]. Dusart et al. performed four fault models and 120bit key was retrieved with 10 ciphertexts [49]. Chien-Ning and Surg-Ming performed DFA which targets KSA and retrieved 128-bit key in 6 ciphertexts and also performed Byte-attack of key schedule and retrieved 128bit key in 22 ciphertexts [52]. Takahashi J et al. adopted new rule-based approach and retrieved 80bit key in just 2 ciphertexts and extended this attack to retrieve 88bit key effectively (Remaining keys 28bit & 20bit respectively are brute-forced) [54].

3.2 Asymmetric crypto-system

RSA was first popular public key cryptosystem and first famous fault attack was done by Boneh et al. [3]. And it is shortly improved by Lenstra where factorization on modulus N of CRT-RSA was performed with just one pair of correct-faulty ciphertext [58].

Digital Signature algorithms (DSA) are primarily used for message authentication and Bao et al., performed DFA attack on it [2]. The secret key was gradually obtained by sequentially toggling individual bits of the key. So, the complete key was retrieved by using one correct & 160 faulty signature on same unknown messages.

Elliptic Curve Cryptography (ECC) has fault attacks which generally try to transfer the computations from a secure curve to a less resilient curve by attacking curve parameters or the scalar multiplications. Biehl et al., attacked scalar multiplication where by inducing 1 bit fault, retrieved scalar information [10]. This attack underwent enhancements by Ciet and Joye [71]. Two types of SEA attacks are performed on ECC which are Computational Safe-Error Attacks (which inject a transient random computational fault in ALU) and Memory Safe-Error Attacks (which injects a fault, inside a memory location or a register) [70,114]. Sakamoto et al., performed fault attack using L´opez-Dahab algorithm [55]. Dominguez-Oviedo et al, performed invalid-curve attack on scalar multiplication of Montgomery ladder elliptic curve [99].

ECDSA's first fault attack was performed by Giraud and Knudsen by retrieving secret key using 2300 faulty signatures and it is an extended work of Dottax [59,62]. Bl¨omer et al. introduced new method called Sign change attack where attack will be more challenging to detect the attack as the points will remain within the curve [63]. Schmidt et al. performed a fault attack which retrieves subpart of ephemeral key for various signatures (50 faulty signatures were used to get 160 bits key) [67]. Jarvinen et al. elaborated upon Giraud's fault attack targeting signature schemes which says that the biased faults can make attack more efficient [69].

3.3 Post-Quantum cryptography

Campbell thinks that due to unexpected worldwide progress and the secrecy surrounding secret research programs run by organizations and governments throughout the world, existing timetables to facilitate the development of quantum computers with fault tolerance on a large scale are overestimated [140]. Saki et al. mentioned that several insider and outsider threat models, including fault injection, are present for quantum computers [137]. And stated that, hardware designs with 1000 qubits could appear quite soon, enhancing device utilization &financial rewards in quantum

clouds to achieve profitability through multi-tenant computing while also potentially opening the door to a fault injection assaults [138,139].

In a groundbreaking finding, Shor presented a method that, with the assistance of a quantum computer, can efficiently solve traditionally hypothesized challenging problems involving factorization and discrete logarithm within polynomial time [122]. The US NIST established a standardization procedure for post-quantum cryptography (PQC) in 2016, to help with the transition and to withstand future attacks to this new technology. The research community has recently shown multiple fault attacks on PQC algo's [108,109,111,112,116,117,118,119,121]. The significant challenge lies in employing these attacks on PQC schemes, given their substantial key sizes (kB), while the attacks can only unveil a limited number of bits in each attempt. Nonetheless, even a limited quantity of exposed key bits could potentially lower the security level beneath the threshold mandated by the PQC standard. Keita Xagawa et al. examined each KEM candidates from NIST PQC Round 3 [136]. The importance lies in performing the equality test through re-encryption during the process of decapsulation since all KEM schemes employ different iterations of the Fujisaki-Okamoto transformation. They demonstrated that introducing a single instruction-skipping defect in the decapsulation operations causes SABRE, NTRU, KYBER, SIKE, and BIKE to practically bypass the equality test.

Various categories of post-quantum cryptographic algorithms exist, including hash-based, lattice-based, code-based, isogeny-based, and multivariate-based algorithms. Among these, multivariate algorithms stand out for their efficiency on resource-constrained devices; however, they do come with the drawback of having significantly large key size while Lattice-based schemes, on the other hand, have comparatively smaller keys and perform well in the constrained environments too.

3.3.1 Code-based cryptography

The foundation of code-based cryptography relies on the difficulty of recovering a code word after applying a random error correction code. Due to the size of their public keys, code-based cryptosystems are not now widely used, but they will be a viable option if the RSA/ECC cryptographic framework is compromised by the development of quantum computers. Due to their built-in capacity to repair errors, code-based cryptographic cryptosystems are quite often resilient to attacks based on faults.

3.3.2 Hash-based Cryptography

In Hash-based Cryptography, according to Eisenbarth et al., since unique one-time signature keys are preferably utilized just once, there is a substantial leakage resistance against DPA-like assaults [130]. A fault model is put out by Shoufan that depends on toggling two control bits to lower the SHA-512 algorithm's round number [135]. An attack was performed on a keyed-hash message authentication code, resulting in the extraction of its secret key.

3.3.3 Lattice-based Cryptography

Lattice-based Cryptography is vulnerable to fault attacks in NTRU cryptosystems used for digital signatures and encryption. Countermeasures for these fault attacks were presented in [113]. Leon Groot Bruinderink and Peter Pessl demonstrated how DFA can be used against deterministic lattice-based signature systems, how & when these systems are susceptible to single random faults, and also demonstrated how the reuse of nonce caused by a fault enables the extraction of the secret key [118]. They also demonstrated approaches that may quickly produce and then effectively take advantage of a partial nonce-reuse. This situation results in legitimate signatures and enables getting around several common defensive systems.

3.3.4 Isogeny-based cryptography

As a work of Isogeny-based cryptography, Élise Tasso has examined the viability of Ti's theoretical fault injection attack [128]. Using electromagnetic fault injection on an ARM Cortex A53 combined with the right and wrong public key generation, they can decipher the secret. The significance of this attack lies in the retrieval of the static key, a private key that sees repeated usage over an extended duration.

3.3.5 Multivariate Cryptography

In Multivariate Cryptography, a side-channel attack against the broken encryption system Sash was suggested by Okeya et al. [134]. Furthermore, Hashimoto et al. demonstrated fault attacks against MPKC schemes (both Big-Field type and Stepwise Triangular System (STS) type) [131].

3.4 Miscellaneous attacks

Saad Islam et al. demonstrated that nonce randomization mitigation is insufficient against fault attacks and proposed the bit-tracing attack for the LUOV scheme and the Signature Correction Attack for the Dilithium scheme [107]. In order to accomplish the Row-hammer attack on several post-quantum signature schemes, they utilized SPOILER, which can identify contiguous memory in regular conditions and without the need for any special privileges [110,112,114,115,123]. They have also used the Plundervolt attack to show weaknesses in the Dilithium signature method. The attack relies on software undervolting of CPU voltages.

Aymeric Genêt demonstrated how SPHINCS-type architectures on embedded devices may be easily attacked by low-cost fault injections (such as simple voltage glitch injection on the targeted platform) enabling adversary to quickly gather enough fake signatures to produce a universal forgery [120].

Fault injection can be powerfully exploited using the Safe-Error Attack (SEA), especially on constant-time implementations like those suggested to the NIST [125,126,127]. SEA is carried out by a separate work where few lattice-based candidates are being decrypted in which SEA assault concentrates on the error distribution. In the study conducted by Luk Bettale, the security implications of safe-error attacks on lattice-based cryptography algorithms were evaluated including Dilithium, KYBER, SABRE, and

NTRU [124]. This study suggests a novel method for carrying out SEA that can be used with more schemes and suggested possible defenses like moving things around and hiding the distribution [119].

4. Countermeasures

Countermeasures play vital role in preventing attacks. Bousselam et al. discussed about sensor-based countermeasures (checks for presence of light, voltage peaks, etc.) and error detection-based countermeasures [74,75] (checks for correctness of the algorithm output). First countermeasures for fault attack on key scheduling of AES algorithm is presented by Chen et al. in which three methods are presented; Parity check, Generate round key only once and Storing key in flash memory [76]. Mestiri et al. presented new scheme for S-Box protection against fault attacks [78]. Barenghi et al. analyzed various software countermeasures and stated that duplication or triplication of the instructions belonging to vulnerable sections of algorithms can protect AES from almost all of the fault attacks [79].

Fan et al. provided ECC with multiple defense strategies against fault attacks, encompassing *Point validation*, which assesses the point's adherence to the curve, *Curve integrity* that identifies faults in curve parameters, *Coherence check* ensuring result accuracy during computation against a pattern, *Combined curve* that employs a reference curve to spot faults, and *Co-factor multiplication* serving as a defense against small subgroup attacks [81]. Prabu et al. gave insights into Algorithm based, Design based and noise based countermeasures of ECC in [100].

Most of the fault attacks countermeasures are not applied at cipher-level implementation i.e., analysis is done outside the cipher and they use redundancy in some form to get protection against fault attacks. Anubhab Baksi et al. broadly classified fault attack countermeasures in general into classes depending on their redundancy form as shown in *table-3* [106]. Strategies such as algorithmic variety and implementation subtleties provide layers of complexity at the cipher level, thereby repelling potential assaults. Using distinct or specialized devices—passive as well as active—helps to isolate and protect, preventing the compromising of critical functions. Detection-based, infective-based, and preventive-based computation redundancy strengthens resilience against errors and manipulations, ensuring the integrity of cryptographic operations. Additionally, the overall security posture can be enhanced by using protocol techniques including re-keying, tweak and tweak-in-plaintext approaches, and masking plaintext in communication channels. Cryptographic systems can build a strong defense mechanism against a wide range of threats by including these multifaceted countermeasures, making a more secure environment for sensitive data.

Table-3: Various abstract levels of countermeasures of FA

	Countermeasure based on various abstract levels			Remarks
1	Cipher level [82].			Solely depends on the virtue of cipher design itself
2	Using a separate or dedicated device			Passive devices block or shields from external interference while active devices detect any potential stress
	Passive devices [83].	Active devices [84].		
3	Using redundancy in computation			Duplicate the circuit partially or fully to detect faults and detected faults will be handled according to predefined protocols
	Detection based [85,86,87].	Infective based [90].	Preventive based [91].	
4	Using protocol techniques			Tries to prevent fault injections through communication protocols.
	Re-Keying [92,95].	Tweak and tweak-in-plaintext [98].	Masking plaintext [89].	

Some countermeasures were also given for PQC. Leon Groot Bruinderink and Peter Pessl demonstrated three generic countermeasures and their applicability & efficacy against the fault attacks - Double computation, Verification-after-sign, and additional randomness (like deterministic noise sampling) [118]. Buffer qubits were suggested by the authors of to prevent cross-talk induced fault injection [139]. Reference [107] pointed that, PQC systems already offer mitigating methods for fault attacks such as randomizing the nonce values, requiring randomly generated vinegar's, and adding a random salt to each message.

5. Evaluation and rating

The evaluation of fault attack resistance is required for any individual product. Some of the certification procedures are:

- Common Criteria (CC) [23].
- EMVCo [103].
- FIPS 140-2 [22].

The most popular and widely followed procedure is common criteria certification process which is termed as CC. CC is brought up by global security certification community and involves certification bodies (certifies the product after evaluation), vendors (person with copyright on the product to be certified) and labs (Evaluator who tests and reviews the product) for rating the product. The aim of this consortium is to give enough assurance for long (many years) working of the product. This process is complex, takes more time (in months) and also costly. Seven Evaluation Assurance Levels (EALs) are available as shown in *figure 3*. You can be more certain that the security functional requirements have been satisfied the higher the level. One major drawback is that security improvement done to the product will void the certification and whole process have to be done again i.e., even minor improvements will take months to be certified.

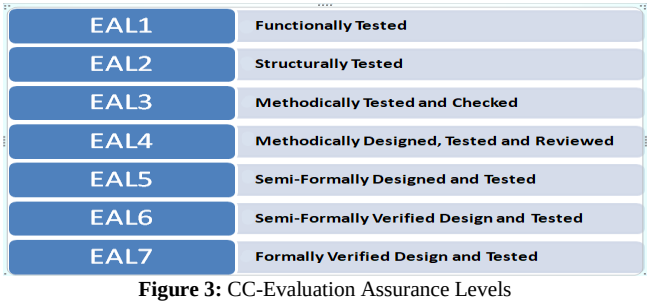

Figure 3: CC-Evaluation Assurance Levels

Whatever might be the certification process, a white-box type (only information related to design and implementation) evaluation is done to the product. Bilgiday Yuce et al. stated that the evaluation process will broadly consist of two steps; Vulnerability Analysis (reviews and tests the vulnerability of the product against possible threats) and Penetration testing (tests and measures resistance of the product against all possible attacks) [13]. And parameters considered for the attack rating are product knowledge, equipment, expertise, time, ability to configure target and number of target samples.

6. Conclusions

This paper covers most of the Side channel fault attacks on various standard cryptosystems published in literature. Various fault attack models of different abstract levels and several fault attacks are also covered in this paper. The countermeasures for fault attacks are mentioned in general while also covered for standard algorithms. Resistance evaluation & rating are also covered.

Fault attacks performance depends primarily on non-linear functions of the crypto-algorithm and due to this; it is possible to recover the key by parts instead of exponential complexity. The common flow of the research on fault attacks is a cycle of countermeasure following the attack which further follows attack (improved version). This cycle may continue unendingly with PQC too.

I second Mostafa Taha et.al. Statement that we are not yet equipped to use any post-quantum cryptography strategy into use in real-world embedded systems [129]. Before achieving a reasonable level of security, a significant amount of study still needs to be done.

Conflict of Interest

The Authors affirm that they have no conflicts of interest to disclose. There are no financial or personal affiliations between any of the writers and any organizations or entities that might be perceived to have an influence on the research. There are no conflicting interests to declare, and the research was self-funded.

Funding Source

The author(s) funded all of this study on their own. The financial assistance for this work came from no outside organizations or funding sources.

Authors' Contributions

Venu Nalla and G Padmavathi researched literature, conceived the study, data collection & analysis. Venu Nalla and Dharavath Narendar wrote the manuscript. G Padmavathi and U Surya Kameswari have done a critical review of all the drafts of the manuscript. All authors reviewed and edited the final draft of the manuscript.

References

[1]. Skorobogatov P. and Anderson R., "Optical Fault Induction Attack," in Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems-CHES, Vol. **2523**, pp.**13-15, 2002.**

[2]. Bao F., Deng H., Han Y., Jeng B., Narasimhalu D., and Ngair T., "Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults" in Proceedings of the International Workshop on Security Protocols, France, pp.**115-124, 1997.**

[3]. Dan Boneh, Richard A. DeMillo & Richard J. Lipton "On the Importance of Checking Cryptographic Protocols for Faults" in Proceedings of the 16th annual international conference on Theory and application of cryptographic techniques, Berlin, August Vol.**1233**, pp.**37-51, 1997.**

[4]. Marc J. and Jean-Jacques Q., "Faulty RSA Encryption," Technical Report CG-1997/8, UCL Crypto Group, **1997.**

[5]. Joye, Marc and Jean-Jacques Quisquater. "Attacks on systems using Chinese remaindering." Journal of Cryptology (1996): n. pag.

[6]. Vlastimil Klima and Tomas Rosa," Attack on Private Signature Keys of the OpenPGP Format, PGP(TM) Programs and Other Applications Compatible with OpenPGP" Cryptology ePrint Archive, Paper 2002/076 available at: http://eprint.iacr.org/2002/076. Pdf

[7]. A.G. Voyiatzis, and D.N. Serpanos, "A fault-injection attack on Fiat-Shamir cryptosystems" in Proceedings of the 24th International Conference on Distributed Computing Systems Workshops, Tokyo, Japan March, pp.**23-24, 2004.** https://doi.org/10.1109/ICDCSW.2004.1284096.

[8]. Eli Biham & Adi Shamir "Differential Fault Analysis of Secret Key Cryptosystems," in Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, USA, Vol.**1294**, pp.**513-525, 1997.**

[9]. Matthias Jacob, Dan Boneh & Edward Felten, "Attacking an Obfuscated Cipher by Injecting Faults" in Proceedings of ACM workshop on Digital Rights Management, USA, pp.**16-31, 2002.**

[10]. Biehl I., Meyer B., and Muller V., "Differential Fault Attacks on Elliptic Curve Cryptosystems," in Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology, USA , pp.**131-146, 2000.**

[11]. Zheng Y., "Breaking Real World Implementations of Cryptosystems by Manipulating Their Random Number Generation," in Proceedings of the 29th Symposium on Cryptography and Information Security, Japan, pp.**1-7**, May 6 **1997.**

[12]. Sayandeep Saha, Ujjawal Kumar and Debdeep Mukhopadhyay and Pallab Dasgupta; Differential Fault Analysis Automation; Cryptology ePrint Archive, Paper 2017/673; **2017.** https://eprint.iacr.org/2017/673.

[13]. Bilgiday Yuce, Patrick Schaumont, Marc Witteman, "Fault Attacks on Secure Embedded Software: Threats, Design and Evaluation" Journal of Hardware and Systems Security 2, pp.**111–130, 2018.** https://doi.org/10.1007/s41635-018-0038-1

[14]. Nicolas T Courtois, Keith Jackson, and David Ware. "Fault-algebraic attacks on inner rounds of des". e-Smart'10 Proceedings: The Future of Digital Security Technologies, Sophia Antipolis, France, 22-24 September, **2010.**

[15]. Eli Biham, Louis Granboulan, and Phong Q. Nguyen. "Impossible fault analysis of RC4 and differential fault analysisof RC4". In proceedings of the 12th International Workshop, FSE 2005, Paris, France, February 21-23, pp.**359-367, 2005.**

[16]. T. Korak and M. Hoefler, "On the Effects of Clock and Power Supply Tampering on Two Microcontroller Platforms," in the proceedingsof the 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography, Busan, Korea (South). 23-23 September, pp.**8–17, 2014**. https://doi.org/10.1109/FDTC.2014.11

[17]. Zhiqiang Liu, Dawu Gu, Ya Liu, and Wei Li. "Linear fault analysis of block ciphers", in the proceedings of 10th international conference on Applied Cryptography and Network Security ACNS 2012, Singapore, June 26-29, 2012. pp.**241-256, 2012.**

[18]. Johannes Bl□omer and Volker Krummel. “Fault based collision attacks on AES”, in the proceedings of Third International Workshop on Fault Diagnosis and Tolerance in Cryptography, Yokohama, Japan, pp.106-120, October 10, 2006.

[19]. Dhiman Saha and Dipanwita Roy Chowdhury. “Encounter: On breaking the nonce barrier in differential faultanalysis with a case-study on PAEQ”, in the proceedings of the 18th International Conference on Cryptographic Hardware and Embedded Systems, CHES, CA, USA, August 17-19, pp.**581-601, 2016.**

[20]. N. Timmers, A. Spruyt, and M. Witteman, “Controlling PC on ARM using fault injection,” in Fault Diagnosis and Tolerance in Cryptography(FDTC), Santa Barbara, CA, USA, August 16-16, pp.**25–35, 2016.** https://doi.org/10.1109/FDTC.2016.18

[21]. M. Hutter and J.-M. Schmidt, “The temperature side channel and heating fault attacks,” in the proceedings of the 12th International Conference on Smart Card Research and Advanced Applications, Berlin, Germany, November 27-29, pp.**219–235, 2013**. http://dx.doi.org/10.1007/978-3-319-08302-5_15

[22]. National Institute of Standards and Technology (NIST), “Security requirements for cryptographic modules,” FIPS PUB 140-2, 2001, https://www.emvco.com/processes-forms/product-approval/. https://doi.org/10.6028/NIST.FIPS.140-3

[23]. “Common Criteria Community,” https://www.commoncriteria portal.org

[24]. T. Korak, M. Hutter, B. Ege, and L. Batina, “Clock glitch attacks in the presence of heating,” , in the proceedings of the 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Busan, Korea (South), September 23, pp.**104–114, 2014.** https://doi.org/10.1109/FDTC.2014.20

[25]. S. P. Skorobogatov and R. J. Anderson, “Optical fault induction attacks,” in proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems, 01st January pp.**2–12, 2003.**

[26]. Ronan Lashermes, Guillaume Reymond, Jean-Max Dutertre, Jacques J. A. Fournier, Bruno Robisson, and AssiaTria. “A DFA on AES based on the entropy of error distributions”, in the proceedings of the 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium, September 9, pp.**34-43, 2012.** https://doi.org/10.1109/FDTC.2012.18

[27]. Patrick Schaumont Nahid Farhady Ghalaty, Bilgiday Yuce. “Analyzing the efficiency of biased-fault based attacks”, IEEE Embedded Systems Letters, June, Vol.**8**, Issue.**2**, pp.**33-36, 2016.** https://doi.org/10.1109/LES.2016.2524652

[28]. Yang Li, Kazuo Sakiyama, ShigetoGomisawa, Toshinori Fukunaga, Junko Takahashi, and Kazuo Ohta. “Fault sensitivity analysis”. In the proceedings of the 12th international workshop on Cryptographic Hardware and Embedded Systems, CHES, Santa Barbara, CA, USA, August 17-20, pp.**320-334**, **2010.**

[29]. Christoph Dobraunig, Maria Eichlseder, Thomas Korak, Stefan Mangard, Florian Mendel, and Robert Primas. “SIFA: exploiting ineffective fault inductions on symmetric cryptography”. IACR Transactions on Cryptographic Hardware and Embedded Systems, pp.**547-572, 2018.** https://doi.org/10.13154/tches.v2018.i3.547-572

[30]. R. Velegalati, R. Van Spyk, and J. van Woudenberg, “Electro magnetic fault injection in practice,” in International Cryptographic Module Conference (ICMC), **2013.**

[31]. A. Tang, S. Sethumadhavan, and S. Stolfo, “CLKSCREW: Exposing the perils of security-oblivious energy management,” in the proceedings of the 26th USENIX Security Symposium (USENIX Security17), Vancouver, BC, Canada, August 16–18, pp.**1057–1074, 2017.**

[32]. Fan Zhang, Xiaoxuan Lou, Xinjie Zhao, Shivam Bhasin, Wei He, Ruyi Ding, Samiya Qureshi, and KuiRen, “Persistent fault analysis on block ciphers”, IACR Transactions on Cryptographic Hardware and Embedded Systems, August Vol.**2018**, Issue.**3**, pp.**150-172, 2018**. https://doi.org/10.13154/tches.v2018.i3.150-172

[33]. KeyvanRamezanpour, Paul Ampadu, and William Diehl. “A statistical fault analysis methodology for the ascon authenticated cipher”, in 2019 IEEE International Symposium on Hardware Oriented Security and Trust, HOST, McLean, VA, USA, pp.41-50, May 5-10 2019. http://dx.doi.org/10.1109/HST.2019.8741029

[34]. Fan Zhang, Shize Guo, Xinjie Zhao, Tao Wang, Jian Yang, Francois-Xavier Standaert, and Dawu Gu. “A frameworkfor the analysis and evaluation of algebraic fault attacks on lightweight block ciphers”, IEEE Trans. Information Forensics and Security, May, Vol.**11**, Issue.**5**, pp.**1039-1054, 2016.** https://doi.org/10.1109/TIFS.2016.2516905

[35]. Punit Khanna, Chester Rebeiro, and AritraHazra. “Xfc: A framework for exploitable fault characterization in block ciphers”, in the proceedings of the 54th Annual Design Automation Conference (DAC), Austin TX USA pp. 1-6. IEEE, 18th june 2017. https://doi.org/10.1145/3061639. 3062340

[36]. Sayandeep Saha, Debdeep Mukhopadhyay, and Pallab Dasgupta. “Expfault: An automated framework for exploitable fault characterization in block ciphers”, IACR Transactions on Cryptographic Hardware and Embedded Systems, Volume 2018, Issue 2, pp. 242-276, 8th May 2018. https://doi.org/10.13154/tches.v2018.i2.242-276

[37]. A. Kurmus, N. Ioannou, N. Papandreou, and T. Parnell, “From random block corruption to privilege escalation: A file system attack vector for rowhammer-like attacks,” in the proceedings of the 11th USENIX Conference on Offensive Technologies (WOOT), Berkeley, CA, United States, 14-15 August 2017.

[38]. D. Karaklajic, J. Schmidt, and I. Verbauwhede, “Hardware Designer’s Guide to Fault Attacks,” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 21, no. 12, pp. 2295–2306, December 2013. http://dx.doi.org/10.1109/TVLSI.2012.2231707

[39]. M. Otto, “Fault attacks and countermeasures,” Ph.D. dissertation, University of Paderborn, 2005.

[40]. S. Anceau, P. Bleuet, J. Cl´edi`ere, L. Maingault, J. Rainard, and R. Tucoulou, “Nanofocused x-ray beam to reprogram secure circuits,” in the proceedings of the international conference on, Cryptographic Hardware and Embedded Systems (CHES), 2017, pp. 175–188, 25th August 2017.

[41]. S. Bhattacharya and D. Mukhopadhyay, “Formal fault analysis of branch predictors: attacking countermeasures of asymmetric key ciphers,” Journal of Cryptographic Engineering, vol. 7, no. 4, pp. 299–310, 9th May 2017. https://link.springer.com/article/10.1007/s13389-017-0165-6

[42]. Sayandeep Saha, Dirmanto Jap, SikharPatranabis, Debdeep Mukhopadhyay, Shivam Bhasin, and Pallab Dasgupta. “Automatic characterization of exploitable faults: A machine learning approach”, IEEE Transactions on Information Forensics and Security, Volume: 14, Issue: 4: pp. 954-968, 31st August 2019. https://doi.org/10.1109/TIFS.2018.2868245

[43]. Jakub Breier, Xiaolu Hou, and Yang Liu. “Fault attacks made easy: Differential fault analysis automation on assembly code”, IACR Transactions on Cryptographic Hardware and Embedded Systems, Volume 2018, Issue 2, pp. 96-122, 08th May 2018. https://doi.org/10.13154/tches.v2018.i2.96-122

[44]. G. Barbu, H. Thiebeauld, and V. Guerin, “Attacks on java card 3.0 combining fault and logical attacks,” in the proceedings of the International Conference on Smart Card Research and Advanced Applications, pp. 148–163, April 14-16 2010.

[45]. Xiaolu Hou, Jakub Breier, Fuyuan Zhang, and Yang Liu. “Fully automated dierential fault analysis on software implementations of block ciphers” IACR Transactions on Cryptographic Hardware and Embedded Systems, Volume 2019, Issue 3, pp. 1-29, May 2019. https://doi.org/10.13154/tches.v2019.i3.1-29

[46]. Mael Gay, Tobias Paxian, Devanshi Upadhyaya, Bernd Becker, and Ilia Polian. “Hardware-oriented algebraic fault attack framework with multiple fault injection support”, In 2019 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC, Atlanta, GA, USA, pp. 25-32, 24th August 2019. https://doi.org/10.1109/FDTC.2019.00012

[47]. S. Nashimoto, N. Homma, Y.-i. Hayashi, J. Takahashi, H. Fuji, and T. Aoki, “Buffer overflow attack with multiple fault injection and a proven countermeasure,” Journal of Cryptographic Engineering, vol. 7, no. 1, pp. 35–46, 2017. http://dx.doi.org/10.1007%2Fs13389-016-0136-3

[48]. Jan Burchard, Ma~nl Gay, Ange-Salome MessengEkossono, Jan

Horacek, Bernd Becker, Tobias Schubert, MartinKreuzer, and Ilia Polian. "Autofault: towards automatic construction of algebraic fault attacks", 2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Taipei, Taiwan, pp. 65-72. IEEE, 25-25 September 2017. https://doi.org/10.1109/FDTC.2017.13

[49]. Dusart P., Letourneus G., and Vivolo O. "Differential Fault Analysis on AES," in proceedings of the 1st international Conference on Applied Cryptography and Network Security, China, vol.2846, pp. 293-306, 2003.

[50]. M.-L. Potet, L. Mounier, M. Puys, and L. Dureuil, "Lazart: A symbolic approach for evaluation the robustness of secured codes against control flow injections," in the proceedings of the 7th Seventh International Conference on Software Testing, Verification and Validation (ICST), pp. 213–222, 31 march – 04th April 2014. https://doi.org/10.1109/ICST .2014.34

[51]. H. Choukri and M. Tunstall, "Round reduction using faults," FDTC, vol. 5, pp. 13–24, January 2005.

[52]. Chien-Ning C. and Sung-Ming Y., "Differential Fault Analysis on AES Key Schedule and Some Countermeasures," in Proceedings of the 8thAustralasian conference on Information security and privacy, Australia, pp. 118-129, 2003.

[53]. Eli Biham & Adi Shamir "Differential Fault Analysis of Secret Key Cryptosystems," in Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, USA, vol. 1294, pp. 513-525, 1997.

[54]. Takahashi J., Fukunaga, T., and YamakoshiK.,"DFA Mechanism on the AES Key Schedule," in the proceedings of Workshop on Fault Diagnosis and Tolerance in Cryptography, Vienna, pp. 62-74, 10th September 2007. https://doi.org/10.1109/FDTC.2007.13

[55]. H. Sakamoto, Y. Li, K. Ohta, and K. Sakiyama. "Fault sensitivity analysis against elliptic curve cryptosystems", Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Nara, Japan, pp. 11–20, Sept 2011. https://doi.org/10.1109/FDTC.2011.17

[56]. Wu, J., Shi, Y., & Choi, "M. Measurement and Evaluation of Power Analysis Attacks on Asynchronous S-Box", IEEE Transactions on Instrumentation and Measurement, 2012, 61, 2765-2775.

[57]. C. Giraud, "DFA on AES," in the proceedings of the 4th international Conference on Advanced Encryption Standard-AES, Bonn, Germany, pp. 27–41, May 10-12 2004. http://dx.doi.org/10.1007/11506447_4

[58]. A.K. Lenstra. "Memo on RSA Signature Generation in the Presence of Faults", Manuscript, 1996.

[59]. C. Giraud and E. Knudsen. "Fault Attacks on Signature Schemes", in the proceedings on Australasian Conference on Information Security and Privacy, pp 478–491, 2004.

[60]. S. S. Ali, D. Mukhopadhyay, and M. Tunstall, "Differential fault analysis of AES: towards reaching its limits", Journal of Cryptographic Engineering, vol. 3, no. 2, pp. 73–97, 2013. http://dx.doi.org/10.1007/s13389-012-0046-y

[61]. N. F. Ghalaty, B. Yuce, M. Taha, and P. Schaumont, "Differential fault intensity analysis," conference on Fault Diagnosis and Tolerance in Cryptography (FDTC), pp. 49–58, 23 September 2014. http://dx.doi.org/10.1109/FDTC.2014.15

[62]. E. Dottax, "Fault Attacks on NESSIE Signature and Identification Schemes", November 2002.

[63]. J. Bl¨omer, M. Otto, and J.-P. Seifert. "Sign Change Fault Attacks on Elliptic Curve Cryptosystems", in proceedings of the 3rd international Workshop on Fault Diagnosis and Tolerance in Cryptography, pp.36–52, October 2006. https://doi.org/10.1007/11889700_4

[64]. T. Fuhr, E. Jaulmes, V. Lomn´e, and A. Thillard, "Fault attacks on AES with faulty ciphertexts only," 10th Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), At: Los Alamitos, CA, USA, pp. 108–118, 20th August 2013. https://doi.org/10.1109/FDTC.2013.18

[65]. K. J¨arvinen, C. Blondeau, D. Page, and M. Tunstall, "Harnessing biased faults in attacks on ECC-based signature schemes," Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pp. 72–82, 2012. https://doi.org/10.1109/FDTC.2012.13

[66]. M. Joye, Q. Jean-Jacques, Y. Sung-Ming, and M. Yung, "Observability analysis-detecting when improved cryptosystems fail," in Cryptographers Track at the RSA Conference, New York, USA, pp. 17–29, 01st January 2002. https://doi.org/10.1007/3-540-45760-7_2

[67]. J. Schmidt and M. Medwed. "A fault attack on ecdsa", Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pp. 93–99, 06th Sept 2009. https://doi.org/ 10.1109/FDTC.2009.38

[68]. D. Karaklajic, J. Fan, and I. Verbauwhede, "A Systematic M Safe-error Detection in Hardware Implementations of Cryptographic Algorithms," International Symposium on Hardware-Oriented Security and Trust (HOST), San Francisco, CA, USA, pp. 96–101, 03-04 June 2012. https://doi.org/10.1109/HST.2012.6224327

[69]. K. Jarvinen, C. Blondeau, D. Page, and M. Tunstall. "Harnessing Biased Faults in Attacks on ECC-Based Signature Schemes", in proceedings of the 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC, pp. 72–82, Washington, DC, USA, 09th September 2012. https://doi.org/10.1109/FDTC.2012.13

[70]. S.-M. Yen, S. Kim, S. Lim, and S.-J. Moon, "RSA speedup with Chinese remainder theorem immune against hardware fault cryptanalysis", IEEE Transactions on Computers, Volume: 52, Issue: 4, pp. 461–472, 02nd April 2003. https://doi.org/10.1109/TC.2003.1190587

[71]. M. Ciet and M. Joye, "Elliptic curve cryptosystems in the presence of permanent and transient faults," Designs, codes and cryptography, vol. 36, no. 1, pp. 33–43, July 2005. http://dx.doi.org/10.1007/s10623-003-1160-8

[72]. P.-A. Fouque, R. Lercier, D. R´eal, and F. Valette, "Fault attack on elliptic curve montgomery ladder implementation," 5th Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC, Washington, DC, USA, pp. 92–98, 10th August 2008. https://doi.org/10.1109/FDTC.2008.15

[73]. P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in the proceedings of Annual International Cryptology Conference Advances in cryptology, pp.388-397, 16th December 1999.

[74]. K. Bousselam, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "On Countermeasures against Fault Attacks on the Advanced Encryption Standard", In: Joye, M., Tunstall, M. Fault Analysis in Cryptography. Information Security and Cryptography, Springer, Berlin, Heidelberg, pp. 89–108, 01st January 2012. https://doi.org/10.1007/978-3-642-29656 -7_6

[75]. M. Karpovsky, K. Kulikowski, and A. Taubin, "Differential fault analysis attack resistant architectures for the advanced encryption standard", in the proceedings on Smart Card Research and Advanced Applications VI, pp. 177–192. Springer US, January 2004. http://dx.doi.org/10.1007/1-4020-8147-2_12

[76]. C.-N. Chen and S.-M. Yen, "Differential Fault Analysis on AES Key Schedule and Some Countermeasures", in the proceedings of the Australasian Conference on Information Security and Privacy Information Security and Privacy, pp. 118–129. Springer Berlin Heidelberg, 01st January 2003.

[77]. S. Tillich and C. Herbst, "Attacking state-of-the-art software countermeasures–a case study for aes", in the proceedings of 10th International Workshop on Cryptographic Hardware and Embedded Systems, Washington, D.C., USA, pp. 228–243, August 2008. http://dx.doi.org/10.1007/978-3-540-85053-3_15

[78]. H. Mestiri, N. Benhadjyoussef, M. Machhout, and R. Tourki, "An FPGA implementation of the AES with fault detection countermeasure", 2013 International Conference on Control, Decision and Information Technologies (CoDIT), pp. 264–270, 06-08 May 2013. https://doi.org/10.1109/CoDIT.2013. 6689555

[79]. A. Barenghi, L. Breveglieri, I. Koren, G. Pelosi, and F. Regazzoni, "Countermeasures Against Fault Attacks on Software Implemented AES:Effectiveness and Cost", WESS '10 in proceedings of the 5th Workshop on Embedded Systems Security, New York, NY, USA, pp. 1-10, 24th October 2010. https://doi.org/10.1145/1873548.1873555

[80]. B. Chevallier-Mames, M. Ciet, and M. Joye, "Low-cost solutions for preventing simple side-channel analysis: Side-channel atomicity," IEEE Transactions on computers, Volume: 53, Issue: 6, pp. 760–768, 19th April 2004. https://doi.org/10.1109/TC.2004.13

[81]. J. Fan and I. Verbauwhede, “An updated survey on secure ECC implementations: Attacks, countermeasures and cost”, In D. Naccache, Cryptography and Security: From Theory to Applications, volume 6805 of Lecture Notes in Computer Science, Springer BerlinHeidelberg, pp. 265–282, January 2012. http://dx.doi.org/10.1007/978-3-642-283680_18

[82]. Anubhab Baksi, “Classical and Physical Security of Symmetric Key Cryptographic Algorithms”, 1st edition, Springer Singapore, pp. XII-288, 18th December 2021.

[83]. Hagai Bar-El, Hamid Choukri, David Naccache, Michael Tunstall, and Claire Whelan, “The sorcerer's apprentice guide to fault attacks”, Proceedings of the IEEE Volume: 94, Issue: 2, pp. 370-382, 23rd January 2004. https://doi.org/10.1109 /JPROC.2005.862424

[84]. Wei He, Jakub Breier, and Shivam Bhasin, “Cheap and cheerful: A low-cost digital sensor for detecting laser fault injection attacks”, in the proceedings of the 6th International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2016, Hyderabad, India, , pp. 27-46, December 14-18, 2016. http://dx.doi.org/10.1007/978-3-319-49445-6_2

[85]. Jakub Breier, Dirmanto Jap, and Shivam Bhasin, “The other side of the coin: Analyzing software encoding schemes against fault injection attacks”, in 2016 IEEE International Symposium on Hardware Oriented Security and Trust HOST, McLean, VA, USA, pp. 209-216, May 3-5, 2016,

[86]. Batya Karp, Ma□el Gay, Osnat Keren, and Ilia Polian, “Detection and correction of malicious and natural faults in cryptographic modules”, in the proceedings on 7th International Workshop on Security Proofs for Embedded Systems, colocated with CHES 2018, Amsterdam, The Netherlands, pp. 68-82,September 10, 2018.

[87]. Tobias Schneider, Amir Moradi, and Tim Guneysu, “Parti- towards combined hardware countermeasures against side-channel and fault-injection attacks”, in 36th Annual International Cryptology Conference Advances in Cryptology -CRYPTO 2016:, Springer Berlin, Heidelberg, pp. 302-332, 21st July 2016. http://dx.doi.org/10.1007/978-3-662-53008-5_11

[88]. M. Witteman and M. Oostdijk, “Secure application programming in the presence of side channel attacks,” in RSA conference, Riscure The Netherlands. January 2008.

[89]. Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, and NidhalSelmane, “Fault injection resilience”, in 2010 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC, Santa Barbara, California, USA, pp. 51-65, 21st August, 2010. https://doi.org/10.1109/FDTC.2010.15

[90]. Benedik tGierlichs, Jorn-Marc Schmidt, and Michael Tunstall, “Infective computation and dummy rounds: Faultprotection for block ciphers without check-before-output”, in proceedings of 2nd International Conference on Cryptology and Information Security in Latin America, Progress in Cryptology - LATINCRYPT 2012, Santiago, Chile, pp. 305-321,October 7-10,2012. http://dx.doi.org/10.1007/978-3-642-33481-8_17

[91]. Nicolas Moro, Karine Heydemann, Emmanuelle Encrenaz, and Bruno Robisson, “Formal verification of a software countermeasure against instruction skip attacks”, Journal of Cryptographic Engineering, Volume 4 Issue 3, pp. 145-156, 26th February 2014. http://dx.doi.org/10.1007/s13389-014-0077-7

[92]. Marcel Medwed, Francois-Xavier Standaert, Johann Grobschadl, and Francesco Regazzoni, “Fresh re-keying: Securityagainst side-channel and fault attacks for low-cost devices”, in the proceedings of International Conference on Cryptology in Africa in Cryptology - Progress in Cryptology AFRICACRYPT 2010, Third, Stellenbosch, South Africa, pp. 279-296, May 3-6, 2010. http://dx.doi.org/10.1007/978-3-642-12678-9_17

[93]. A. Vasselle, H. Thiebeauld, Q. Maouhoub, A. Morisset, and S. Ermeneux, “Laser-induced fault injection on smart phone bypassing the secure boot,” in 2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). IEEE, Taipei, Taiwan, pp. 41–48, 25th September 2017. https://doi.ieeecomputersociety.org/10.1109/FDTC.2017.18

[94]. N. Timmers and C. Mune, “Escalating privileges in linux using voltage fault injection,” 2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Taipei, Taiwan, pp. 25–35, 25th September 2017. https://doi.org/ 10.1109/FDTC.2017.16

[95]. Marcel Medwed, Christophe Petit, Francesco Regazzoni, Mathieu Renauld, and Francois-Xavier Standaert, “Freshre-keying II: securing multiple parties against side-channel and fault attacks”, International Conference on Smart Card Research and Advanced Applications- 10th IFIP WG 8.8/11.2, CARDIS 2011, Leuven, Belgium, pp. 115-132, September 14-16 2011.

[96]. M. San Pedro, M. Soos, and S. Guilley, “Fire: Fault injection for reverse engineering”, 5th IFIP WG 11.2 International Workshop on Information Security Theory and Practices. Security and Privacy of Mobile Devices in Wireless Communication in WISTP, Heraklion, Crete, Greece, pp. 280–293, 1-3 June 2011.

[97]. H. Le Bouder, S. Guilley, B. Robisson, and A. Tria, “Fault injection to reverse engineer des-like cryptosystems,” FPS 2013 International Symposium on Foundations and Practice of Security Foundations and Practice of Security, pp. 105–121, 01st january 2014.

[98]. SikharPatranabis, DebapriyaBasu Roy, and Debdeep Mukhopadhyay, “Using tweaks to design fault resistant ciphers”, 2016 29th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID), Kolkata, India, pp. 585-586, 04-08 January 2016.

[99]. A. Dominguez-Oviedo, M. Hasan, and B. Ansari,” Fault-Based Attack on Montgomerys Ladder Algorithm”, Journal of Cryptology, Volume 24 Issue2 pp.346–374, April 2011. https://dx.doi.org/10.1007/s00145-010-9087-5

[100]. Prabu, Maha & Shanmugalakshmi, R., “An Overview of Side Channel Attacks and Its Countermeasures using Elliptic Curve Cryptography”, International Journal on Computer Science and Engineering, 2010.

[101]. C. Giraud and H. Thiebeauld, "A Survey on Fault Attacks", in Smart Card Research and Advanced Applications VI CARDIS, Kluwer, pp. 159-176, 2004.

[102]. F. Beck, “Integrated Circuit Failure Analysis – A Guide to Preparation Techniques”, Wiley, pp. 190, February 1998. ISBN: 978-0-471-97401-7

[103]. “EMVCo Product Approval Processes,” http://nvlpubs. nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

[104]. D. Samyde, S. Skorobogatov, R. Anderson, and J.-J. Quisquater, “On a NewWay to Read Data from Memory”, in First International IEEE Security in Storage Workshop, Greenbelt, MD, USA, pp. 65–69, 11th December 2002.

[105]. S. Saha, A. Bag, D. B. Roy, S. Patranabis, D. Mukhopadhyay, A. Canteaut, et al, "Fault template attacks on block ciphers exploiting fault propagation", 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques Advances in Cryptology - EUROCRYPT 2020, pp. 612-643, 1st May 2020.

[106]. A. Baksi, S. Bhasin, J. Breier, D. Jap and D. Saha, "Fault attacks in symmetric key cryptosystems", journal ACR Cryptol ePrintArch, Volume 2020, pp. 1267. https://dblp.org/db/journals/iacr/iacr2020.html#BaksiBBJS20

[107]. Saad Islam’ “Software-Induced Fault Attacks on Post-Quantum Signature Schemes”, PhD thesis, School of Electrical & Computer Engineering, Worcester Polytechnic Institute, Singapore, 2021.

[108]. Nina Bindel, Johannes Buchmann, and Juliane Kr¨amer, “Lattice-based signature schemes and their sensitivity to fault attacks”, in 2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pages 63–77, 2016.

[109]. Nina Bindel, Juliane Kramer, and Johannes Schreiber, “Special session: hampering fault attacks against lattice-based signature schemes countermeasures and their efficiency”, in 2017 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS), Seoul, Korea (South), pp. 1–3, 15-20 October 2017.

[110]. Finn de Ridder, Pietro Frigo, Emanuele Vannacci, Herbert Bos, Cristiano Giuffrida, and Kaveh Razavi, “SMASH: Synchronized many-sided row hammer attacks from JavaScript”, in 30th USENIX Security Symposium (USENIX Security 21), pp. 1001–1018, 11-13 August 2021.

[111]. Thomas Espitau, Pierre-Alain Fouque, BenoˆıtG´erard, and Mehdi

Tibouchi, “Loop-abort faults on lattice-based fiat-shamir and hash-andsign signatures”, in International Conference on Selected Areas in Cryptography, pp. 140–158. Springer, 2016.

[112]. P. Frigo, E. Vannacc, H. Hassan, V. der Veen, O. Mutlu, C. Giuffrida, H. Bos, and K. Razavi, “Trrespass: Exploiting the many sides of target row refresh” in 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, pp. 747–762, 18-21 May 2020.

[113]. A. Kamal and A. Youssef, “Strengthening hardware implementations of NTRUEncrypt against fault analysis attacks”, Journal of Cryptographic Engineering, Volume4 Issue 3, pp.227-240, 30th May 2013. http://dx.doi.org/ 10.1007/s13389-013-0061-7

[114]. Saad Islam, Ahmad Moghimi, Ida Bruhns, Moritz Krebbel, Berk Gulmezoglu, Thomas Eisenbarth, and Berk Sunar, “SPOILER: Speculative load hazards boost rowhammer and cache attacks” in 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, pp. 621–637, 14th August 2019.

[115]. Patrick Jattke, Victor van der Veen, Pietro Frigo, Stijn Gunter, and Kaveh Razavi, “Blacksmith: Scalable rowhammering in the frequency domain”, in 2022 IEEE Symposium on Security and Privacy (SP), volume 1, San Francisco, CA, USA, pp.716-734, 22-26 May 2022. https://doi.ieeecomputersociety.org/10.1109/SP46214.2022.9833772

[116]. Juliane Kr¨amer and MirjamLoiero, “Fault attacks on uov and rainbow”, COSADE 2019: International Workshop on Constructive Side-Channel Analysis and Secure Design, pp. 193–214, 16th March 2019.

[117]. Koksal Mus, Saad Islam, and Berk Sunar, “QuantumHammer: A practical hybrid attack on the luov signature scheme”, in Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Worcester, MA,USA, pp. 1071–1084, 9-13 November 2020.

[118]. Groot Bruinderink, L., Pessl, “Differential fault attacks on deterministic lattice signatures”, IACR Transactions on Cryptographic Hardware and Embedded Systems, Volume 2018, Issue 3, pp. 21–43, 14th August 2018. https://doi.org/10.13154/tches.v2018.i3.21-43.

[119]. Peter Pessl and Lukas Prokop, “Fault attacks on cca-secure lattice kems”, IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 37–60, February 2021. http://dx.doi.org/10.46586/tches.v2021.i2.37-60

[120]. Genêt A, Kannwischer MJ, Pelletier H, McLauchlan, “Practical fault injection attacks on sphincs”, IACR Cryptology ePrint Archive 2018:674.

[121]. Prasanna Ravi, Mahabir Prasad Jhanwar, James Howe, Anupam Chattopadhyay, and Shivam Bhasin, “Exploiting determinism in latticebased signatures: practical fault attacks on pqm4 implementations of nist candidates”, in proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, pp. 427–440, 02nd July 2019.

[122]. Peter W Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, SIAM Journal on Computing, Volume 26 Issue 5, pp. 1484–1509, 01st October 1997. https://doi.org/10. 1137/S00975 39795293172

[123]. Y. Tobah, A. Kwong, I. Kang, D. Genkin, and K. G. Shin, “Spechammer: Combining spectre and rowhammer for new speculative attacks”, in 2022 IEEE Symposium on Security and Privacy (SP) (SP), San Francisco, CA, USA, pp.1362–1379, 22-26 May 2022.

[124]. Bettale, L., Montoya, S., Renault, “Safe-error analysis of post-quantum cryptography mechanisms”, in 18th Workshop on Fault Detection and Tolerance in Cryptography, FDTC 2021, Milan, Italy, pp. 39–44, 17 September 2021, IEEE (2021). https://doi.org/10.1109/FDTC53659.2021.00015

[125]. S. Yen and M. Joye, “Checking before output may not be enough against fault-based cryptanalysis,” IEEE Transactions on Computers, Volume: 49, Issue: 9, pp. 967-970, September 2000. https://doi.org/10.1109/12.869328

[126]. A. Berzati, C. Canovas-Dumas, and L. Goubin, “A survey of differential fault analysis against classical RSA implementations,” in Fault Analysis in Cryptography, Springer, Berlin, Heidelberg, pp. 111–124, 21st June 2012. ISBN: 978-3-642-29655-0

[127]. C. Clavier, “Attacking Block Ciphers”, Fault Analysis in Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, Jan. 2012, doi: 10.1007/978-3-642-29656-7_2.

[128]. Ti Y.B, “Fault attack on super-singular isogeny cryptosystems”, in PQCrypto 2017 International Workshop on Post-Quantum Cryptography”, Springer, Cham, pp. 107-122, 04th June 2017.

[129]. Mostafa Taha and Thomas Eisenbarth, “Implementation Attacks on Post-Quantum Cryptographic Schemes”, IEEE International Conference on Anti-Cybercrime Cryptology (ICACC), Worcester, USA, 09 November 2015, https://eprint.iacr.org/2015/1083

[130]. T. Eisenbarth, I. von Maurich, and X. Ye, “Faster hash-based signatures with bounded leakage”, in SAC 2013 International Conference on Selected Areas in Cryptography, Springer-Verlag, Berlin, Heidelberg, pp. 223-243, 14th August 2013.

[131]. Y. Hashimoto, T. Takagi, and K. Sakurai, “General fault attacks on multivariate public key cryptosystems”, in proceedings on the 4th International Workshop on Post-Quantum Cryptography, Taipei, Taiwan, pages 1-18, 29th November 2011.

[132]. A. Kamal and A. Youssef, “Fault analysis of the NTRUSign digital signature scheme”, Cryptography and Communications, Volume 2, Issue 4, pp. 131-144, 06th January 2012. https://doi.org/10.1007/s12095-011-0061-3

[133]. A. A. Kamal and A. Youssef, “Fault analysis of the NTRUEncrypt cryptosystem”, IEICE transactions on fundamentals of electronics, communications and computer sciences, 94(4), 01st April, pp.**1156-1158, 2011.** http://dxdoi.org/10.1587/transfun.E94.A.1156

[134]. K. Okeya, T. Takagi, and C. Vuillaume, “On the importance of protecting delta; in SFLASH against side channel attacks”, in proceedings on International Conference on Information Technology: Coding and Computing, Las Vegas, NV, USA, 05-07 April, pp.**560-568, 2004.**

[135]. A. Shoufan, "A fault attack on a hardware-based implementation of the secure hash algorithm SHA-512," 2013 International Conference on Reconfigurable Computing and FPGAs (ReConFig), Cancun, Mexico, 09-11 December, pp.**1-7, 2013.** doi: 10.1109/ReConFig.2013 .6732292.

[136]. Keita Xagawa, Akira Ito, Rei Ueno, Junko Takahashi, and Naofumi Homma, “Fault-injection attacks against nist’s post-quantum cryptography round 3kem candidates”, in International Conference on the Theory and Application of Cryptology and Information Security, Springer, December pp.**33–61, 2021**. https://doi.org/10.1007/978-3-030-92075-3_2

[137]. Abdullah Ash Saki, MahabubulAlam, Koustubh Phalak, Aakarshitha Suresh, Rasit Onur Topaloglu, and Swaroop Ghosh. 2021, “A survey and tutorial on security and resilience of quantum computing”, In 2021 IEEE European Test Symposium (ETS), Bruges, Belgium, 24-28 May, pp.**1-10, 2021.**

[138]. P. Das, S. S. Tannu, P. J. Nair, and M. Qureshi, “A Case for Multi- Programming Quantum Computers,” in proceedings of the 52nd Annual IEEE/ACM MICRO, New York, NY, USA, 2019, 12 October, pp.**291–303, 2019.** https://doi.org/10.1145/3352460.3358287

[139]. A. A. Saki, M. Alam, and S. Ghosh, “Analysis of crosstalk in NISQ devices and security implications in multi-programming regime”, in the proceedings on ACM/IEEE International Symposium on Low Power Electronics and Design, 10th August pp.**25–30, 2020.** https://doi.org/10.1145/3370748.3406570

[140]. Robert E. Campbell, Sr.; Mitigating Quantum Computing Threats and Attacks. PhD thesis, Capital Technology University, **2020.**

AUTHORS PROFILE

Venu Nalla is presently working as a research associate in CRRAO AIMSCS, Hyderabad. He did his M.Tech (VLSI & Computer Engineering) from IIIT Hyderabad. He is pursuing his Ph.D. (Computer Science & Engineering Dept.) from Acharya Nagarjuna University, Guntur. He is also a programmer with proficiency in C & Python. His areas of interest are Cryptology, Side Channel Cryptanalysis and High Performance Computing.

G. Padmavathi is working as an assistant professor in CRRAO AIMSCS, Hyderabad. She received Gold medal in M.Sc. (Maths) from Acharya Nagarjuna University, Guntur, Andhra Pradesh, India. Awarded Ph.D. in Mathematics from JNTUH University, Hyderabad. She has published research papers in reputed international and national journals and conferences, including IEEE and they're also available online. She holds one patent publication derived from her research. She has 20 years of combined experience in teaching & Research. Her main research interest includes Cryptology, Machine learning, Modeling and Analysis.

Dharavath Narendar is presently working as a research associate in CRRAO AIMSCS, Hyderabad. He did his M.Tech (CSE) from National Institute of Technology Karnataka, Surathkal. He is pursuing his Ph.D. (Computer Science & Engineering Dept.) from Acharya Nagarjuna University, Guntur. His areas of interest are Network Security and Cryptology.

U. Surya Kameswari earned her B.Sc& M.Sc in Computer Science from Andhra University in 2005 and 2007 respectively. She earned a M.Tech. in Information Technology from Karnataka State Open University in 2012 and Ph.D in Computer Science and Engineering from Acharya Nagarjuna University in 2020. She is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Acharya Nagarjuna University, Andhra Pradesh. She has been a member of IAENG since 2015 and a member of CSTA since 2012. She has published research papers in reputed international and national journals and conferences, including IEEE and they're also available online. Her main research work focuses on Data Mining, Big Data Analytics, Machine Learning, and Data Science. She holds one Indian patent publication derived from her research. She has 15 years of teaching experience and 11 years of research experience.

