J Cryptogr Eng (2016) 6:325–337
DOI 10.1007/s13389-016-0117-6

REGULAR PAPER

Hardware attacks: an algebraic approach

Samer Moein[1] · Fayez Gebali[1] · T. Aaron Gulliver[1]

Received: 23 July 2015 / Accepted: 26 January 2016 / Published online: 10 February 2016

Abstract Many VLSI chips now contain cryptographic processors to secure their data and external communications. Attackers target the hardware to imitate or understand the system design, to gain access to the system or to obtain encryption keys. They may also try to initiate attacks such as denial of service to disable the services supported by a chip, or reduce system reliability. In this paper, an algebraic methodology is proposed to examine hardware attacks based on the attack properties and associated risks. This methodology is employed to construct algorithms to develop hardware attack and defence strategies. It can also be used to predict system vulnerabilities and assess the security of a system.

Keywords Hardware attack · Hardware security · Overt attack · Covert attack · Adjacency matrix

1 Introduction

VLSI system designers must now consider the security of a system against internal and external hardware attacks. Significant research has being done to develop cryptographic algorithms and hardware to provide security to systems and their users. Of particular concern are hardware attacks and methods of detecting and counteracting their effects.

Most hardware attack classification models proposed in the literature are based on the level at which an attacker accesses the system [1]. Further, side channel attacks have been classified based on the awareness of the attacks [2]. Unfortunately, these classifications are overlapping and qualitative in nature. Both system designers and users require a classification which is relevant and useful. Recently, a new approach to classifying hardware attacks was introduced [3,4] which is based on a comprehensive examination of attack features. The main advantage is the association of quantitative descriptors with each attack. Thus, this method can be used to identify the requirements to successfully launch or defend against an attack. Therefore, this hardware attack classification is used in this paper to illustrate the proposed methodology, but it can be employed with any classification.

Many types of hardware attacks have been identified. One monitors and analyzes the execution time needed during cryptographic processing. This attack was first discussed in [5], and the first practical implementation was presented in [6]. A timing attack against the RSA algorithm using the Chinese remainder theorem (CRT) was given in [7]. An attack against the Rijndael algorithm was presented in [8]. An attack against the Patterson algorithm within the McEliece public key cryptosystem (PKC) was given in [9], and against the secret permutation in the McEliece PKC in [10]. A detailed study of this type of attack was presented in [11]. Another approach monitors the power consumption by measuring the radiated electromagnetic power [12–14]. The acoustic signals from an encryption coprocessor can also be monitored to obtain key information [15–18]. Optically enhanced power analysis is an innovative technique that can be used to reveal the current in transistors [19–24]. Diffused reflections from computer displays can be employed to reconstruct the data on the screen [25,26]. Other examples of hardware attacks

✉ Samer Moein
samerm@uvic.ca

Fayez Gebali
fayez@ece.uvic.ca

T. Aaron Gulliver
agullive@ece.uvic.ca

[1] Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada

include data remanence [27,28] and failure analysis [29–31]. Additional attacks are discussed in [1–4,32].

New techniques are constantly being developed to attack the system hardware, and countermeasures for these attacks must be designed. What is required is a comprehensive catalog of attacks which can be expanded as new attacks arise. The proposed methodology can be used to establish and update this catalog based on the properties of each attack. This can be used by security designers to test their systems against emerging threats.

From an attacker perspective, the proposed methodology provides the attacks which match their capabilities and awareness. From a defender perspective, it can be used to identify system vulnerabilities and develop countermeasures. The proposed methodology is flexible and so can incorporate new attacks. Obsolete attacks can also be removed. This methodology is based on a set of attack criteria. Further, weights can be specified for the criteria so that detailed comparisons can be made. Thus as technology changes, the risk levels and weights can be adjusted based on the attacker and/or defender capabilities.

The contributions of this paper are as follows:

1. An algebraic methodology is developed for investigating hardware attacks. This provides the first quantitative representation of these attacks. It can be used to easily identify security risks, and study the relationships between hardware attack criteria.
2. Algorithms are presented which can be used in designing attack methodologies based on the criteria relationships and weights as well as the current attacker capabilities.
3. Algorithms for a defender are presented which can be used to predict and quantify system vulnerabilities. These can determine attacks that affect system security and so can be used to develop countermeasures to protect the system. Moreover, they can identify attacks that the system is secure against.

The remainder of this paper is organized as follows. Section 2 reviews hardware attack properties and categorizes these properties. The L_1-norm is used in Sect. 3 to determine the attack risks. Section 4 presents an algebraic approach to investigating hardware attacks, and Sect. 5 presents algorithms based on this methodology. Finally, Sect. 6 provides some concluding remarks.

2 Hardware attacks

The goal of hardware attacks is to access a system to obtain stored information, determine the internal structure of the hardware, or inject a fault. A quantified hardware attack classification based on four properties was proposed in [3,4]. The four properties are accessibility (A), resources (R), time (T), and awareness (W), as shown in Fig. 1, and these are used in this paper to illustrate the proposed methodology. The awareness property (W) divides hardware attacks based on the evidence left of an attack on a system. Thus there are two categories, covert and overt. An attack is covert when the victim is not aware that it is taking place. Conversely, an attack is overt when the victim is aware that it has occurred. As in [3,4], we consider three levels for (A), (R) and (T), but additional levels can be added if required.

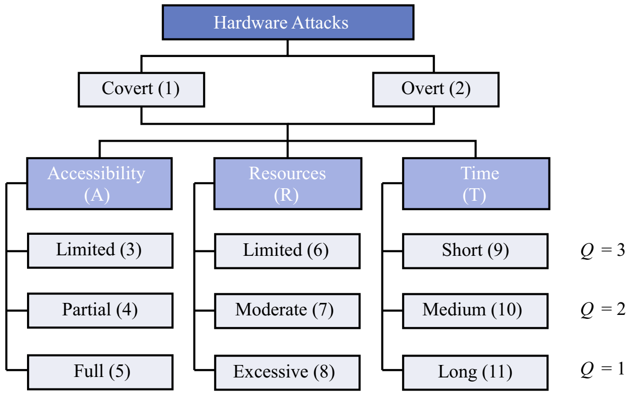

Fig. 1 Hardware attack classification

The accessibility property (A) classifies hardware attacks based on the required level of access to a system. This property is divided into three categories: limited, partial, and full access. Limited access refers to no physical connection to the hardware, while with partial access an attacker can connect to the hardware or scan it. Full access means that the attacker can reach the gate level of a chip. The A levels are then {full access, partial access, limited access} $\equiv \{1, 2, 3\}$.

The resources property (R) refers to the equipment and manpower needed to successfully launch an attack. This property is divided into three categories: limited, moderate, and excessive resources. Limited resources ($R <$ \$10,000) includes equipment such as an IC soldering/desoldering station, digital multimeter, universal chip programmer, prototyping boards, power supply, oscilloscope, logical analyzer, and signal generator. Moderate resources (\$10,000 $\leq R \leq$ \$100,000) includes equipment such as a laser microscope, laser interferometer navigation, infrared imaging, and photomultipliers. Excessive resources ($R >$ \$100,000) includes equipment such as a laser cutter, focused-ion beam (FIB), and scanning electron microscope (SEM). The R levels are then {excessive resources, moderate resources, limited resources} $\equiv \{1, 2, 3\}$.

The time property (T) refers to the amount of time, effort, and experience required to execute an attack. This property is divided into three categories: short, medium, and long time. Short time refers to an attack that takes less than a few days to succeed, while medium time refers to an attack that succeeds within weeks, and long time refers to an attack that succeeds

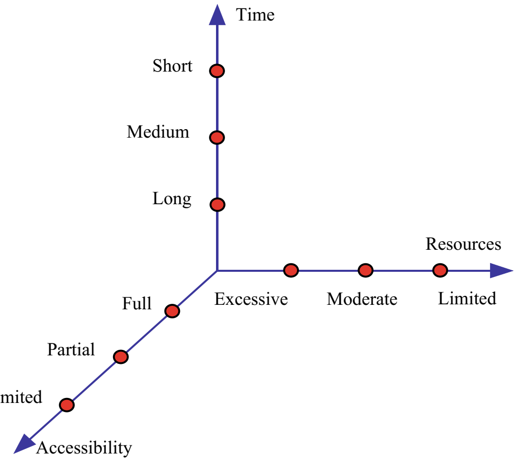

Fig. 2 3D representation of the accessibility (A), resources (R), and time (T) hardware attack properties

within months. The T levels are then {long time, medium time, short time} $\equiv \{1, 2, 3\}$.

Figure 2 shows a three-dimensional (3D) model where each axis represents one of the properties accessibility (A), resources (R), and time (T). This is based on the approach to quantifying covert hardware attacks in [4], and overt hardware attacks in [3]. With this model, an attack is represented as a point in 3D space whose coordinates are $\mathbf{p} = (a, r, t)$, $1 \leq a, r, t \leq 3$. Each point may map to multiple hardware attacks, while an attack maps to a unique point based on the capabilities of the attacker or defender. The focus in [3,4] was on placing attacks within the 3D ART model based on the requirements to be successful. To illustrate the proposed methodology, in this paper attacks are located within the 3D ART model based on risk levels.

3 Attack risk levels

In this section, three attack levels, high, medium and low, are considered based on the results in [3,4]. Note that as capabilities and technology change the level of an attack can change. For example, deprocessing (DEP) may migrate from low risk to medium risk based on the resources required. Regardless of the awareness, a hardware attack requires certain levels of accessibility, resources, and time, a, r, and t, respectively, to succeed. Based on these values, a risk level can be assigned to an attack with respect to the target system. The L_1-norm of the attack point $\mathbf{p}$ in the 3D ART space is given by

$$L_1 = a + r + t. \tag{1}$$

Based on (1), attacks can be quantized into levels. In this paper, three levels are considered: high risk, medium risk, and low risk.

3.1 High risk attacks

High risk attacks are hardware attacks that require limited capabilities for execution. These attacks require limited resources and little time, so there is typically no evidence left and thus are often covert. Attacks belonging to this level are simple and so many attackers have the necessary resources and expertise. Therefore, this attack level is the most dangerous. Examples of high risk attacks from [3,4] are:

1. Simple electro-magnetic (SEMA) attack
2. Differential electro-magnetic (DEMA) attack
3. Frequency based analysis (FBA) attack
4. Simple power analysis (SPA) attack
5. Fault injection (FIT) attack.

A high risk attack has an L_1-norm that satisfies the following inequality

$$8 \leq L_1 \leq 9. \tag{2}$$

3.2 Medium risk attacks

Medium risk attacks require capabilities beyond those for a high risk attack, but less than for a low risk attack. Attacks belonging to this level typically require access inside the system or higher permission to access the system than for a high risk attack. For example, the attacker has access to the chip surface but not to the internal circuitry. The attacker may need more time (e.g. to collect data and analyze it), and more resources compared to that for high risk attacks. Attacks belonging to this level cannot be accomplished without sufficient time, resources, and accessibility, which makes them harder than high risk attacks. Therefore, the number of attackers with the necessary resources and expertise will be smaller than that for high risk attacks. Examples of medium risk attacks from [3,4] are:

1. Differential power analysis (DPA) attack
2. Timing (TA) attack
3. Acoustic (ACA) attack
4. Optically enhanced position-locked power analysis (OPLP) attack
5. Optical emanation (OEA) attack
6. Covert JTAG port (C-JTAG) attack
7. Data remanence (DRA) attack
8. Fault analysis (FAT) attack
9. Overt JTAG port (O-JTAG) attack
10. Advanced imaging techniques (AIT) attack.

A medium risk attack has an L_1-norm that satisfies the following inequality

$$5 \leq L_1 \leq 7. \tag{3}$$

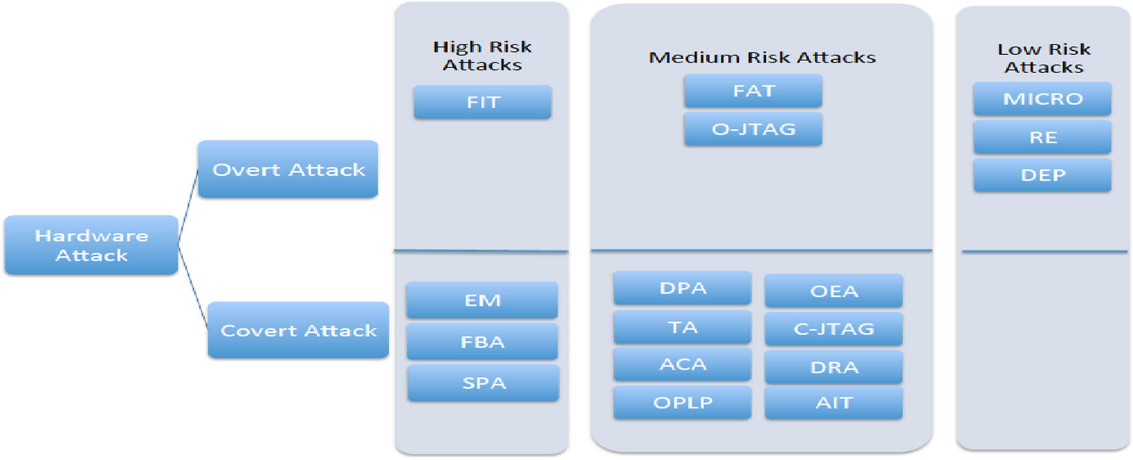

Fig. 3 Hardware attacks

3.3 Low risk attacks

Low risk attacks require significant knowledge, equipment and/or time to succeed. Modern chips are multilayer and complicated, so an attack that requires decapsulating a chip to access its internal components can be very difficult to undertake. This type of attack requires full access to the chip, so they are typically not covert. Attacks belonging to this level can usually only be executed by research agencies, governments, organizations, or universities. Therefore, the number of attackers for this level will be much less than for the other levels. Examples of low risk attacks from [3] are:

1. Microprobing (MICRO) attack
2. Reverse engineering (RE) attack
3. Deprocessing (DEP) attack.

A low risk attack has an L_1-norm that satisfies the following inequality

$$3 \leq L_1 \leq 4. \tag{4}$$

The attacks given in this section and the associated risk levels will be used to illustrate the proposed methodology in the next section. These attack and their risk levels are shown in Fig. 3. Note that the levels are based on the results in [3,4], and levels based on other classifications can also be employed.

4 Algebraic approach to hardware attacks

The proposed algebraic approach to hardware attacks is based on the hardware attack classification shown in Fig. 1. The numbers in parentheses next to each criterion is the corresponding index, and Q is the associated risk. There are several steps in the methodology for both an attacker and a defender. These steps are described in this section.

4.1 Hardware attack table

Developing a hardware attack table is the first step in the proposed approach. This table is updated by an attacker or defender whenever there is a new attack or a new criteria, or if there are changes in capabilities. It contains weights based on the attacks and associated criteria. Table 1 includes examples of hardware attacks that have been proposed in the literature.

4.1.1 Criteria weights

Consider a system that may be vulnerable to the attacks given in Sect. 3 as shown in Fig. 3. The risk levels in this figure (based on Fig. 2), are employed with a weight W_i for each criteria in Table 1. For a given attack, the weight assigned by an attacker or defender satisfies

$$0 \leq W_i(\text{Attack}) \leq 1, \tag{5}$$

where i is the criterion index. In Table 1, an empty element corresponds to a weight of 0, which indicates that the criterion for the given attack is impossible or secure. A weight $W_i = 1$ indicates that the criterion for the given attack is available or unsecure. For simplicity, $W_i = 1$ is assumed for all criteria that can affect the system to demonstrate the methodology.

The weighted risk for an attack is based on the risk for the criteria (Q_i) shown in Fig. 1 and the corresponding weights W_i

$$W_R(\text{Attack}) = \sum_{i=1}^{n} W_i(\text{Attack}) \times Q_i, \tag{6}$$

Table 1 Hardware attack table

	Criteria											
	Awareness		Accessibility			Resources			Time			
	Covert	Overt	Limited access	Partial access	Full access	Limited resources	Moderate resources	Excessive resources	Short time	Medium time	Long time	
Index i	1	2	3	4	5	6	7	8	9	10	11	
Risk Q_i	–	–	3	2	1	3	2	1	3	2	1	W_R
Hardware attacks												
SEMA	x		W			W			W			
DEMA	x		W			W				W		
FBA	x		W			W				W		
SPA	x			W		W			W			
FIT		x		W		W			W			
DPA	x			W		W				W		
TA	x			W		W				W		
ACA	x			W		W				W		
OPLP	x			W		W				W		
OEA	x		W				W			W		
C-JTAG	x			W		W				W		
DRA	x			W		W				W		
FAT		x		W		W				W		
O-JTAG		x		W		W				W		
AIT	x			W			W			W		
MICRO		x			W		W				W	
RE		x			W			W			W	
DEP		x			W			W			W	
W_C	–	–										
N[a]	–	–										

[a] N is the number of attacks a criterion is involved in

where n is the number of criteria. If an attacker cannot satisfy one of the criteria for an attack (weight is zero), the weighted risk is set to 0. The range of W_R is

$$0 \le W_R(\text{Attack}) \le L_1. \tag{7}$$

4.1.2 Weighted criteria

The weighted criterion is given by

$$W_C(\text{criterion}) = \sum_{j=1}^{m} W_j(\text{Attack}) \times Q_j, \tag{8}$$

where m is the number of attacks considered.

Definition 1 The criteria with the largest value of W_C based on (8) are called the critical weighted criteria

$$\widehat{W_C} = \max_{1 \le i \le n} W_C(i), \tag{9}$$

where i is the criterion index.

4.1.3 Attacker table

An attacker determines the attack weights W_i based on their capabilities and the target system. These weights reflect the ability to satisfy a criterion for a given attack. Using (6), the weighted risk is obtained and entered in the W_R column. It is important for an attacker to know for which attacks $W_R \neq 0$, as these can be used against the target system. The total weight for each criterion from (8) is listed in the W_C row. A goal of an attacker is to increase the criteria weights, particularly the weight of the critical weighted criteria. The best attacks can be considered to be those which have the largest value of W_R and include a critical weighted criterion $\widehat{W_C}$.

4.1.4 Defender table

A defender determines the attack weights W_i based on their system and capabilities. These weights reflect the capacity to defend against an attack which requires a given criterion. Using (6), the weighted risk can be obtained and this is entered in the W_R column. It is important for a defender to know for which attacks $W_R \neq 0$, as these can be used against their system. A goal of a defender is $W_R = 0$ for all attacks to guarantee the security of the system (which is typically not achievable). The total weight for each criterion from (8) is listed in the W_C row. From a defender perspective, countermeasures should be developed to reduce the criteria weights W_C, particularly the weights for the critical weighted criteria $\widehat{W_C}$.

4.1.5 Attack subsets

In Fig. 1, hardware attacks are classified according to four properties. Each attack then has a combination of four risk values based on these properties. For simplicity, here we do not assign weights for the awareness property. An attacker may be able to undertake multiple attacks depending on their capabilities. For example, if an attacker can launch attacks that require partial access to a system, then they can also launch attacks that need only limited access. Conversely, if a security designer succeeds in protecting a system from partial access attacks, it can still be vulnerable to limited access attacks.

Definition 2 The ability of an attacker or defender is a point in the 3D ART space which defines their capability to attack or defend a system, respectively, and is given by

$$\mathbf{p_0} = (a_0, r_0, t_0). \tag{10}$$

The ability is now used to generate subsets of hardware attacks.

Definition 3 Attacker coverage $\mathbf{p_A}$: the set of criteria levels that an attacker satisfies, defined as

$$\mathbf{p_A} = \{a_A, r_A, t_A\}, \tag{11}$$

where

$$a_0 \leq a_A \leq 3,$$
$$r_0 \leq r_A \leq 3,$$
$$t_0 \leq t_A \leq 3.$$

Definition 4 Defender coverage $\mathbf{p_D}$: the set of criteria levels that a defender has protection against, defined as

$$\mathbf{p_D} = \{a_D, r_D, t_D\}, \tag{12}$$

where

$$1 \leq a_D \leq a_o,$$
$$1 \leq r_D \leq r_o,$$
$$1 \leq t_D \leq t_o.$$

4.2 Adjacency matrix for attack properties

We now examine the relationships between the attack criteria using an adjacency matrix. This matrix characterizes the connections between pairs of criteria, and thus shows the sets of attacks that have a pair of criteria in common. It will be used to determine the collective criteria and critical criteria, which are important for an attacker (resp. defender) to attack (resp. protect) a system. We begin with the following definitions.

Definition 5 One weight criterion set $X(i)$: the subset of hardware attacks which contain criterion i, given by

$$X(i) = \{\text{Attack}|W_i(\text{Attack}) > 0\}. \tag{13}$$

Definition 6 Two weight criteria set $X(i, j)$: the subset of hardware attacks that contain criteria i and j, given by

$$X(i, j) = \{\text{Attack}|W_i(\text{Attack}) \cdot W_j(\text{Attack}) > 0\}. \tag{14}$$

Definition 7 Three weight criteria set $X(i, j, k)$: the subset of hardware attacks that contain criteria i, j, and k, given by

$$\begin{aligned} &X(i, j, k) \\ &\quad = \{\text{Attack}|W_i(\text{Attack}) \cdot W_j(\text{Attack}) \cdot W_k(\text{Attack}) > 0\}. \end{aligned} \tag{15}$$

Assuming there are n criteria, the *adjacency matrix* $\mathbf{R}$ is a binary $(0-1)$ square, symmetric $n \times n$ matrix where $r(i, j) = r(j, i) = 1$ indicates that there is a subset $X(i, j)$ of hardware attacks that contain criteria i and j.

$$\mathbf{R} = \left[\begin{array}{c|ccccccc} A & 1 & 2 & 3 & 4 & 5 & \dots & n \\ \hline 1 & 0 & 0 & 1 & 1 & 0 & \dots & 0 \\ 2 & 0 & 0 & 0 & 1 & 1 & \dots & 1 \\ 3 & 1 & 0 & 0 & 0 & 0 & \dots & \vdots \\ 4 & 1 & 1 & 0 & 0 & 0 & \dots & \vdots \\ 5 & 0 & 1 & 0 & 0 & 0 & \dots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ n & 0 & 1 & \dots & \dots & \dots & \dots & 0 \end{array}\right]$$

The adjacency matrix corresponding to the hardware attacks in Table 1 is

$$\mathbf{R_1} = \left[\begin{array}{c|ccccccccccc} A & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ \hline 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 2 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 3 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 4 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 5 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 6 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 7 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 8 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 9 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 10 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 11 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right]$$

where

$$r(i, j) = r(j, i) = 1 \;\Rightarrow X(i) \cap X(j) \neq \emptyset. \tag{16}$$

In $\mathbf{R_1}$, $r(5, 8) \equiv r(\text{full access, excessive resources}) = 1$ indicates that a subset of hardware attacks require the criteria full access and excessive resources. From Table 1, this subset is $X(5, 8) = \{\text{RE, DEP}\}$.

4.2.1 Row entries in R

Assume there are v entries $r(i, j) = 1$ in row i. The relationship among the subsets of criteria in a single row is described by

$$\forall i : r(i, j) = 1 \;\Rightarrow X(i) \cap X(j) \neq \emptyset. \tag{17}$$

Combining any $0 < k \leq v$ combinations of these entries will generate an attack subset. Thus, the number of subsets is

$$\sum_{k=1}^{v} \binom{v}{k} = 2^v - 1. \tag{18}$$

For example, consider row 3 in $\mathbf{R_1}$. There are $v = 5$ non zero entries corresponding to $j = 1, 6, 7, 9, 10$, which gives the subsets

$X(3, 1) = \{\text{SEMA, DEMA, FBA}\}$
$X(3, 6) = \{\text{SEMA, DEMA, FBA}\}$
$X(3, 7) = \{\text{OEA}\}$
$X(3, 9) = \{\text{SEMA}\}$
$X(3, 10) = \{\text{DEMA, FBA, OEA}\}$.

From (18), there are 31 possible subsets.

The subset of hardware attacks that satisfy at least one criteria in addition to criterion i is

$$X^{\cup}(i) = \bigcup_{r(i,j)\neq 0} X(i, j). \tag{19}$$

As an example, suppose that the subset of hardware attacks is required that satisfies one or more of criteria 6 and 7 as well as criterion 3. Using (19) gives

$$\begin{aligned} X^{\cup}(3) &= \bigcup_{j\in\{6,7\}} X(3, j) \\ &= X(3, 6) \cup X(3, 7) \\ &= \{\text{SEMA, DEMA, FBA}\} \cup \{\text{OEA}\} \\ &= \{\text{SEMA, DEMA, FBA, OEA}\} \end{aligned}$$

Conversely, the subset of hardware attacks that have all of a set of criteria including criterion i is given by

$$X^{\cap}(i) = \bigcap_{r(i,j)\neq 0} X(i, j). \tag{20}$$

As an example, suppose the subset of hardware attacks is required that satisfies both criteria 6 and 9 as well as criterion 3. Using (20) gives

$$\begin{aligned} X^{\cap}(3) &= \bigcap_{j\in\{6,9\}} X(3, j) \\ &= X(3, 6) \cap X(3, 9) \\ &= \{\text{SEMA, DEMA, FBA}\} \cap \{\text{SEMA}\} \\ &= \{\text{SEMA}\}. \end{aligned}$$

Since $\mathbf{R}$ is a square, symmetric matrix, the same relationships between the criteria subsets can be obtained using the columns instead of the rows.

Definition 8 Collective criteria ($C(i)$): the number of criteria that can be combined with criterion i to produce a subset of hardware attacks, which is given by

$$C(i) = \sum_{j=1}^{n} r(i, j). \tag{21}$$

Definition 9 Critical criterion ($\hat{i}$): a criterion that can be combined with the maximum number of criteria to produce subsets of hardware attacks, which is given by

$$\hat{i} = \max_{1\leq i\leq n} C(i). \tag{22}$$

The values of (21) for the example are given in Table 2, and show that the range of $C(i)$ is

$$3 \leq C(i) \leq 7. \tag{23}$$

From (23), $\hat{i} = 7$, so that moderate resources (criterion 7) and medium time (criterion 10) are the critical criteria.

Table 2 Collective criteria

i	$C(i)$
1	6
2	6
3	5
4	6
5	5
6	5
7	7
8	3
9	5
10	7
11	3

5 Algorithms

The purpose of this section is to present algorithms to identify sets of candidate attacks based on the attacker/defender table. Three attack algorithms are proposed. These algorithms have the same steps from line 1 to line 3 and from line 5 to line 16.

For a given target system, on line 2 the ability point $\mathbf{p_0} = (a_0, r_0, t_0)$ and awareness are inputs. For example, suppose $\mathbf{p_0} = (2, 2, 2)$ and covert are inputs. Then on line 3, Table 1 is updated with new attacks or changes since the table was last modified. The weights W are obtained according to (5). For simplicity, $W = 1$ is assumed in all cases which indicates that the attacker is able to provide all criteria needed for the attacks. For the defender, this would indicate that the system is vulnerable to numerous attacks. Lines 5–16 calculate the attack coverage using (11) based on the corresponding ability. For the example, the attacker coverage is $\{(2, 2, 2), (2, 2, 3), (2, 3, 3), (3, 3, 3)\}$. Each point corresponds to a set of hardware attacks, namely $\mathbf{p} = (2, 2, 2) = \{\text{AIT}\}$, $\mathbf{p} = (2, 2, 3) = \emptyset$, $\mathbf{p} = (2, 3, 3) = \{\text{SPA}\}$, and $\mathbf{p} = (3, 3, 3) = \{\text{SEMA}\}$. Note that FIT is not included as it is an overt attack. The algorithms then determine a set of attacks based on the ability and requirements.

5.1 Attacks based on criteria relationships

Algorithm 1 is based on the relations between all criteria involved in the hardware attacks. It is used to generate attacks based on a set of one to three preferred criteria, i.e. criteria the attacker is considering to launch an attack. These criteria should belong to different categories. On line 17 in Algorithm 1, (21) is used to solve for the collective criteria, and (22) to obtain the critical criteria. From $\mathbf{R_1}$, the critical criteria are moderate resources (criteria 7) and medium time (criteria 10). On line 18, a subset of hardware attacks is obtained based on a critical criterion using (13). On line 19, two critical criteria are considered (if more than one exists), using (14), The subset for three criteria are obtained using (15) on line 20.

Algorithm 1 Attacks based on criteria relations

```
1: Given: target system
2: Input: $\mathbf{p_0} = (a_0, r_0, t_0)$, Awareness
3: Update the hardware attack table
4: Initialize: $\mathbf{S_T} = \emptyset$
5: Initialize: $a = a_0, r = r_0, t = t_0$;
6: while $a \leq 3$ do
7:    while $r \leq 3$ do
8:       while $t \leq 3$ do
9:          $\mathbf{S_P} = (a_A, r_A, t_A)$;
10:          $\mathbf{S_T} \leftarrow \mathbf{S_T} \cup \mathbf{S_P}$;
11:          $t = t + 1$;
12:       end while
13:       $r = r + 1$;
14:    end while
15:    $a = a + 1$;
16: end while
17: Solve for $C(i)$ and $\hat{i}$ using (21) and (22)
18: Output: one criterion attack set from (13)
19: Output: two criteria attack set from (14)
20: Output: three criteria attack set from (15)
```

5.2 Attacks based on selected attack criteria

Algorithm 2 is based on the preferred criteria and provides attacks which have combinations of these criteria. On line 17 in Algorithm 2, the hardware attack table (Table 3) is used

Algorithm 2 Attacks based on selected attack criteria

```
1: Given: target system
2: Input: $\mathbf{p_0} = (a_0, r_0, t_0)$, Awareness
3: Update the hardware attack table
4: Initialize: $\mathbf{S_T}, \mathbf{S_R}, \mathbf{S_X} = \emptyset, m, k, X = 0$;
5: Initialize: $a = a_0, r = r_0, t = t_0$;
6: while $a \leq 3$ do
7:    while $r \leq 3$ do
8:       while $t \leq 3$ do
9:          $\mathbf{S_P} = (a_A, r_A, t_A)$;
10:          $\mathbf{S_T} \leftarrow \mathbf{S_T} \cup \mathbf{S_P}$;
11:          $t = t + 1$;
12:       end while
13:       $r = r + 1$;
14:    end while
15:    $a = a + 1$;
16: end while
17: Construct $\mathbf{R}$
18: $\upsilon$= number of favourable criteria (18);
19: $k$ = number of combination criteria (18);
20: Solve for $X$ using (18)
21: while $X \geq 1$ do
22:    $\mathbf{S_R} = (i, j)$;
23:    $\mathbf{S_X} = \mathbf{S_X} \cap / \cup \mathbf{S_R}$ [(19) or (20)]
24:    $X = X - 1$;
25: end while
26: Output: Attack set $\mathbf{S_X}$
```

Table 3 Attacker/defender table

	Criteria											
	Awareness		Accessibility			Resources			Time			
	Covert	Overt	Limited access	Partial access	Full access	Limited resources	Moderate resources	Excessive resources	Short time	Medium time	Long time	
Index i	1	2	3	4	5	6	7	8	9	10	11	
Q_i	–	–	3	2	1	3	2	1	3	2	1	W_R
Hardware attacks												
SEMA	x		1			1			1			9
DEMA	x		1			1				1		8
FBA	x		1			1				1		8
SPA	x			1		1			1			8
FIT		x		1		1			1			8
DPA	x			1		1				1		7
TA	x			1		1				1		7
ACA	x			1		1				1		7
OPLP	x			1		1				1		7
OEA	x		1				1			1		7
C-JTAG	x			1		1				1		7
DRA	x			1		1				1		7
FAT		x		1		1				1		7
O-JTAG		x		1		1				1		7
AIT	x			1			1			1		6
MICRO		x			1		1				1	4
RE		x			1			1			1	3
DEP		x			1			1			1	3
W_C	–	–	12	22	3	39	6	2	9	24	3	
N[a]	–	–	4	11	3	13	3	2	3	12	3	

[a] N is the number of attacks a criterion is involved in

to construct **R**. For the example, $\mathbf{R_1}$ is obtained. This matrix provides the relationships between each pair of criteria. On line 18, the number of preferred criteria to launch an attack is selected, i.e. the value of v in (18). On line 19, the number of combinations of preferred criteria is selected, i.e. the value of k in (18). Then on line 20, (18) is used to determine the number of combinations X based on v and k. On line 22, a subset of hardware attacks is generated for each value in $\{1, \ldots, X\}$. On line 23, the common attacks between the sets of attacks are obtained using (20), or they are combined using (19). Finally, line 26 generates the hardware attack set that matches the preferred criteria. This algorithm is used when hardware attacks are required based on one criterion, or when criteria are combined according to specific criteria.

5.3 Attacks based on criteria occurrence

Algorithm 3 selects attacks based on the criteria involved and their weights. Then the best attacks to use against a system are chosen. The highest value of $\hat{N}$ is selected on line 17 in Algorithm 3, the highest value of $\widehat{W_R}$ is selected on line 18, and the highest value of $\widehat{W_C}$ is selected on line 19. One or more of the equations on lines 20–23 is used to generate a hardware attack set based on the critical criteria $\widehat{W_C}$, $\hat{N}$, or both. An attack set can also be chosen that contains $\widehat{W_R}$.

For example, consider a target system with $\mathbf{p_0} = (3, 2, 2)$ and covert as inputs, which means the attacker can have limited access, moderate resources, and moderate time. On line 3, Table 4 is generated. Note that some of the attack criteria differ from those in Table 3 because advanced measuring techniques are available, i.e. the accessibility for SPA is limited access. For illustration purposes, $W = 1$ is assumed to indicate that the attacker meets the criterion needed for an attack, and $W = 0$ to indicate that the criterion is not met. Lines 5–16 calculate the attack coverage using (11) based on the corresponding ability. The attacker coverage is $\{(3, 2, 2), (3, 2, 3), (3, 3, 2), (3, 3, 3)\}$. Each point corresponds to a set of hardware attacks, namely $\mathbf{p} = (3, 2, 2) = \{\text{OEA}\}$, $\mathbf{p} = (3, 2, 3) = \emptyset$, $\mathbf{p} = (3, 3, 2) = \{\text{DEMA, DPA, FBA, TA}\}$, and $\mathbf{p} = (3, 3, 3) = \{\text{SEMA, SPA}\}$. On line 17, the criteria involved in

Algorithm 3 Attacks based on criteria occurrence

```
1: Given: target system
2: Input: $\mathbf{p_0} = (a_0, r_0, t_0)$, Awareness
3: Update the hardware attack table
4: Initialize: $\mathbf{S_T}, \mathbf{S_X}, N, W_R, W_C = \emptyset, \hat{N}, \widehat{W_R}, \widehat{W_C} = 0$;
5: Initialize: $a = a_0, r = r_0, t = t_0$;
6: while $a \leq 3$ do
7:    while $r \leq 3$ do
8:       while $t \leq 3$ do
9:          $\mathbf{S_P} = (a_A, r_A, t_A)$;
10:         $\mathbf{S_T} \leftarrow \mathbf{S_T} \cup \mathbf{S_P}$;
11:         $t = t + 1$;
12:      end while
13:      $r = r + 1$;
14:   end while
15:   $a = a + 1$;
16: end while
17: $\hat{N} = \max N$ from Table 1;
18: $\widehat{W_R} = \max W_R$ from Table 1;
19: Obtain $\widehat{W_C}$ using (9);
20: $\mathbf{S_X} = \widehat{W_R}$ from Table 1 OR
21: $\mathbf{S_X} = \hat{N} \cap \widehat{W_R}$ using (20) OR
22: $\mathbf{S_X} = \hat{N} \cup \widehat{W_C}$ using (19) OR
23: $\mathbf{S_X} = \hat{N} \cup \widehat{W_C} \cap \widehat{W_R}$ using (19) and (20)
24: Output: Attack set $\mathbf{S_X}$
```

the greatest number of attacks is calculated, which is {limited resources, medium time} with a value of 10. On line 18, the highest weighted risk among the attacks is determined, which is 9 corresponding to {SEMA, SPA}. On line 19, the highest weighted criteria is calculated, which is 30 corresponding to {limited resources}. Lines 20–23 provide the hardware attack set. If line 20 is chosen, the set is {SEMA, SPA}, if line 21 is chosen, the set is {SEMA, SPA}, if line 22 is chosen, the set is {SEMA, DEMA, FBA, SPA, DPA, TA}, and if line 23 is chosen, the set is {SEMA, SPA}. The algorithm can be executed multiple times to obtain different attack sets and also whenever criteria change.

5.4 Defence algorithms

The three attack algorithms can also be used by a defender. An attacker uses the output attack sets to launch an attack against a system, while a defender uses the output sets to develop countermeasures to protect their system against these attacks. The algorithms can also be used to examine the system by modifying lines 5–16, as shown in Algorithm 4. The modified algorithms allow the defender to determine the hardware attacks that their capabilities can protect against. Further, they aid the defender in examining their system against new attacks or changes in attack criteria. The defender should consider all possible approaches an attacker may use to launch an attack, so variations of the same attack may exist in the defender table. For example, there could be two DEP attacks, say DEP-1 and DEP-2, where DEP-1 assumes that the attacker uses in-house resources,

Table 4 Attacker table

	Criteria											
	Awareness		Accessibility			Resources			Time			
	Covert	Overt	Limited access	Partial access	Full access	Limited resources	Moderate resources	Excessive resources	Short time	Medium time	Long time	
Index i	1	2	3	4	5	6	7	8	9	10	11	
Q_i	–	–	3	2	1	3	2	1	3	2	1	W_R
Hardware attacks												
SEMA	x		1			1			1			9
DEMA	x		1			1				1		8
FBA	x		1			1				1		8
SPA	x		1			1			1			9
DPA	x		1			1				1		8
TA	x		1			1				1		8
OEA	x		1				1			1		7
ACA	x			0		1				1		0
OPLP	x			0		1				1		0
C-JTAG	x			0		1				1		0
DRA	x			0		1				1		0
AIT	x			0			1			1		0
W_C	–	–	21	0	0	30	4	0	6	20	0	
N[a]	–	–	7	0	0	10	2	0	2	10	0	

[a] N is the number of attacks a criterion is involved in

Table 5 Defender table

	Criteria											
	Awareness		Accessibility			Resources			Time			
	Covert	Overt	Limited access	Partial access	Full access	Limited resources	Moderate resources	Excessive resources	Short time	Medium time	Long time	
Index i	1	2	3	4	5	6	7	8	9	10	11	
Q_i	–	–	3	2	1	3	2	1	3	2	1	W_R
Hardware attacks												
SEMA	x		1			1			1			9
DEMA	x		1			1				0		0
FBA	x		1			1				0		0
SPA-1	x		1			1			1			9
SPA-2	x			0		1			1			0
FIT		x		0		1			1			0
DPA-1	x		1			1				0		0
DPA-2	x			0		1				0		0
TA-1	x		1			1			1			9
TA-2	x		1			1				0		0
TA-3	x			0		1			1			0
ACA	x			0		1				0		0
OPLP	x			0		1				0		0
OEA	x		1				0			0		0
C-JTAG	x			0		1				0		0
DRA	x			0		1				0		0
FAT		x		0		1				0		0
O-JTAG		x		0		1				0		0
AIT	x			0			0			0		0
MICRO		x			0		0				0	0
RE		x			0			0			0	0
DEP-1		x			0			0			0	0
DEP-2		x			0		0				0	0
W_C	–	–	24	0	0	48	0	0	12	0	0	
N[a]	–	–	8	0	0	16	0	0	4	0	0	

[a] N is the number of attacks a criterion is involved in

while DEP-2 assumes the attacker using outsourcing and so requires fewer resources.

For example, consider a target system with $\mathbf{p_0} = (2, 2, 2)$ and covert as inputs. This indicates the security of the system prevents against attacks with partial access, moderate resources, and medium time. The defender employs Algorithm 4 to retrieve the set of attacks that can threaten their system. The defence table obtained is given in Table 5. This shows that some attacks can be executed at different accessibility levels. Thus some attacks are duplicated with different criteria, i.e. SPA-1 with limited access and SPA-2 with partial access depending on the measuring technique employed by an attacker. For illustration purposes, $W = 1$ is assumed to indicate that a criterion is not secure, and $W = 0$ to indicate that a criterion is secure. Lines 5–16 provide the defender coverage which is $\{(2, 2, 2), (2, 2, 1), (2, 1, 2), (2, 1, 1), (1, 2, 2), (1, 2, 1), (1, 1, 2), (1, 1, 1)\}$. Each point corresponds to a set of hardware attacks for which the system is protected, namely $\mathbf{p} = (2, 2, 2) = \{\text{AIT}\}$, $\mathbf{p} = (2, 2, 1) = \emptyset$, $\mathbf{p} = (2, 1, 2) = \emptyset$, $\mathbf{p} = (2, 1, 1) = \emptyset$, $\mathbf{p} = (1, 2, 2) = \emptyset$, $\mathbf{p} = (1, 2, 1) = \{\text{MICRO, DEP-2}\}$, $\mathbf{p} = (1, 1, 2) = \emptyset$, and $\mathbf{p} = (1, 1, 1) = \{\text{RE, DEP-1}\}$. On line 17, the criteria involved in the greatest number of attacks is calculated, which is {limited resources} with a value of 16. On line 18, the highest weighted risk among the attacks is determined, which is 9 corresponding to {SEMA, SPA-1, TA-1}. On line 19, the highest weighted criteria is calculated, which is 48 corresponding to {limited resources}. Lines 20–23 provide the hardware attack set. If line 20 is chosen, the set is {SEMA, SPA-1, TA-1}, if line 21 is chosen, the set is {SEMA, SPA-1, TA-1}, if line 22 is chosen, the set {SEMA,

Algorithm 4 Defence based on criteria occurrence

```
1: Given: target system
2: Input: $\mathbf{p_0} = (a_0, r_0, t_0)$, Awareness
3: Update the hardware attack table
4: Initialize: $\mathbf{S_T}, \mathbf{S_X}, N, W_R, W_C = \emptyset, \hat{N}, \widehat{W_R}, \widehat{W_C} = 0$;
5: Initialize: $a = a_0, r = r_0, t = t_0$;
6: while $a \geq 1$ do
7:    while $r \geq 1$ do
8:       while $t \geq 1$ do
9:          $\mathbf{S_P} = (a_A, r_A, t_A)$;
10:          $\mathbf{S_T} \leftarrow \mathbf{S_T} \cup \mathbf{S_P}$;
11:          $t = t - 1$;
12:       end while
13:       $r = r - 1$;
14:    end while
15:    $a = a - 1$;
16: end while
17: $\hat{N}$ = max $N$ from Table 1;
18: $\widehat{W_R}$ = max $W_R$ from Table 1;
19: Obtain $\widehat{W_C}$ using (9);
20: $\mathbf{S_X} = \widehat{W_R}$ from Table 1 OR
21: $\mathbf{S_X} = \hat{N} \cap \widehat{W_R}$ using (20) OR
22: $\mathbf{S_X} = \hat{N} \cup \widehat{W_C}$ using (19) OR
23: $\mathbf{S_X} = \hat{N} \cup \widehat{W_C} \cap \widehat{W_R}$ using (19) and (20)
24: Output: Attack set $\mathbf{S_X}$
```

SPA-1, TA-1}, and if line 23 is chosen, the set is {SEMA, SPA-1, TA-1}. This indicates that the system is vulnerable to these three attacks. The defender must consider developing countermeasures to these attacks, and the common criterion can be considered as the best approach to achieving this goal. The defender can also execute the other algorithms to examine the system from different perspectives.

6 Conclusion

A methodology was proposed to develop hardware attack and defence strategies. Algorithms were presented to reveal system vulnerabilities and assess the security of a system. This approach is flexible and can easily be adapted to system modifications and changes in attacker and/or defender capabilities, as well as new hardware attacks. The attack criteria were categorized according to four properties: awareness (W), accessibility (A), resources (R), and time (T). For each attack, weights are assigned to the criteria depending on the capability of the attacker or defender to satisfy or protect against the criteria. A binary adjacency matrix was also defined to aid in classifying hardware attacks.

References

1. Skorobogatov, S.: Semi-invasive attacks: a new approach to hardware security analysis. Ph.D. dissertation, University of Cambridge, Cambridge (2005)
2. Zhou, Y., Feng, D.: Side-channel attacks: ten years after its publication and the impacts on cryptographic module security testing. IACR Cryptol ePrint Arch (2005)
3. Moein, S., Gebali, F.: Quantifying overt hardware attacks: using ART schema. In: Computer Science and its Appl. Lecture Notes in Electrical Engineering, vol. 330, pp. 511–516. Springer, New York (2015)
4. Moein, S., Gebali, F., Traore, I.: Analysis of covert hardware attacks. J. Converg. **5**(3), 26–30 (2014)
5. Kocher, P.C.: Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems. In: Advances in Cryptology. Lecture Notes in Computer Science, vol. 1109, pp. 104–113. Springer, New York (1996)
6. Dhem, J.-F., Koeune, F., Leroux, P.-A., Mestré, P., Quisquater, J.-J., Willems, J.-L.: A practical implementation of the timing attack. In: Smart Card Research and Applications. Lecture Notes in Computer Science, vol. 1820, pp. 167–182. Springer, New York (2000)
7. Schindler, W.: A timing attack against RSA with the Chinese remainder theorem. In: Cryptographic Hardware and Embedded Systems. Lecture Notes in Computer Science, vol. 1965, pp. 109–124. Springer, New York (2000)
8. Koeune, F., Quisquater, J.-J.: A timing attack against Rijndael. UCL Crypto Group Technical Report CG-1999/1 (1999)
9. Shoufan, A., Strenzke, F., Molter, H.G., Stöttinger, M.: A timing attack against Patterson algorithm in the McEliece PKC. In: Information, Security and Cryptology. Lecture Notes in Computer Science, vol. 5984, pp. 161–175. Springer, New York (2009)
10. Strenzke, F.: A timing attack against the secret permutation in the McEliece PKC. In: Post-Quantum Cryptography. Lecture Notes in Computer Science, vol. 6061, pp. 95–107. Springer, New York (2010)
11. Rebeiro, C., Mukhopadhyay, D., Bhattacharya, S.: Timing Channels in Cryptography. Springer, New York (2015)
12. Hajime, U., Sho, E., Homma, N., Hayashi, Y., Takafumi, A.: Electromagnetic analysis against public-key cryptographic software on embedded OS. IEICE Trans. Commun. **E98-B**(7), 1242–1249 (2015)
13. Kim, H., Bruce, N., Lee, H.-J., Choi, Y., Choi, D.: Side channel attacks on cryptographic module: EM and PA attacks accuracy analysis. In: Information Science and Applications. Lecture Notes in Electrical Engineering, vol. 339, pp. 509–516. Springer, New York (2015)
14. Quisquater, J.-J., Samyde, D.: Electromagnetic analysis (EMA): measures and counter-measures for smart cards. In: Smart Card Programming and Security. Lecture Notes in Computer Science, vol. 2140, pp. 200–210. Springer, New York (2001)
15. Backes, M., Dürmuth, M., Gerling, S., Pinkal, M., Sporleder, C.: Acoustic side-channel attacks on printers. In: Proc. USENIX Conf. on Security, pp. 307–322 (2010)
16. Berger, Y., Wool, A., Yeredor, A.: Dictionary attacks using keyboard acoustic emanations. In: Proc. ACM Conf. on Computer and Commun. Security, pp. 245–254 (2006)
17. Shamir, A., Tromer, E.: Acoustic cryptanalysis on nosy people and noisy machines. http://www.tau.ac.il/~tromer/acoustic/ec04rump/ (2004). Accessed 23 June 2015
18. Wright, P., Greengrass, P.: Spycatcher: The Candid Autobiography of a Senior Intelligence Officer. Bantam Doubleday Dell, New York (1987)
19. Joye, M., Paillier, P., Schoenmakers, B.: On second-order differential power analysis. In: Cryptographic Hardware and Embedded Systems. Lecture Notes in Computer Science, vol. 3659, pp. 293–308. Springer, New York (2005)
20. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Advances in Cryptology. Lecture Notes in Computer Science, vol. 3659, pp. 388–397. Springer, New York (1999)
21. Kocher, P., Jaffe, J., Jun, B., Rohatgi, P.: Introduction to differential power analysis. J. Cryptogr. Eng. **1**(1), 5–27 (2011)
22. Mahanta, H.J., Azad, A.K., Khan, A.K.: Differential power analysis: attacks and resisting techniques. In: Proc. Inform. Sys. Design

and Intelligent Appl., Advances in Intelligent Systems and Computing, vol. 340, pp. 349–358. Springer, New York (2015)
23. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer, New York (2007)
24. Skorobogatov, S.: Optically enhanced position-locked power analysis. In: Cryptographic Hardware and Embedded Systems. Lecture Notes in Computer Science, vol. 4249, pp. 61–75. Springer, New York (2006)
25. Kuhn, M. G.: Optical time-domain eavesdropping risks of CRT displays. In: Proc. IEEE Symp. on Security and Privacy, pp. 3–18 (2002)
26. Loughry, J., Umphress, D.: Information leakage from optical emanations. ACM Trans. Inf. Syst. Secur. **5**(3), 262–289 (2002)
27. Skorobogatov, S.: Low temperature data remanence in static RAM. University of Cambridge, Computer Laboratory Technical Report 536, (2002)
28. Skorobogatov, S.: Data remanence in flash memory devices. In: Cryptographic Hardware and Embedded Systems. Lecture Notes in Computer Science, vol. 3659, pp. 339–353. Springer, New York (2005)
29. El Mrabet, N., Fournier, J.J.A., Goubin, L., Lashermes, R.: A survey of fault attacks in pairing based cryptography. Cryptogr. Commun. **7**(1), 185–205 (2015)
30. Piscitelli, R., Bhasin, S., Regazzoni, F.: Fault attacks, injection techniques and tools for simulation. In: Proc. Int. Conf. on Design and Technology of Integrated Systems in Nanoscale Era, pp. 1–6 (2015)
31. Wills, K.S., Lewis, T., Billus, G., Hoang, H.: Optical beam induced current applications for failure analysis of VLSI devices. In: Proc. Int. Symp. for Testing and Failure, Analysis, pp. 21–26 (1990)
32. Tehranipoor, M., Wang, C.: Introduction to Hardware Security and Trust (Eds.). Springer, New York (2012)