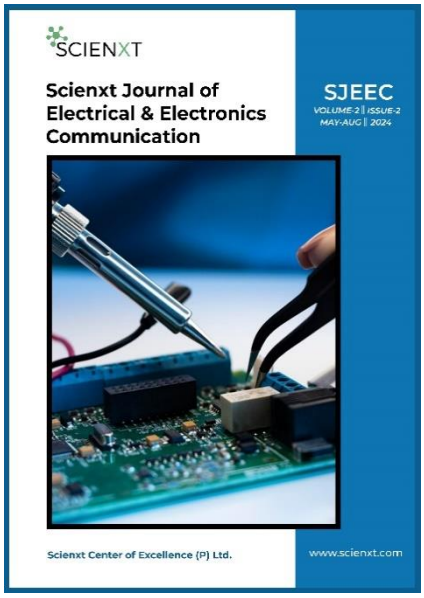


**Scienxt Journal of Electrical & Electronics Communication**
**Volume-2 || Issue-2 || May-Aug || Year-2024 || pp. 1-24**

# *Contact-less integrity verification of microelectronics ssing near- field EM analysis*

**[*1]Manu H. M, [2]Yella Ajay Kumar Reddy**

[*1]Associate Professor, Department of Electronics and Communication Engineering, Dayananda Sagar Academy of Technology and Management, Bengaluru, Karnataka, India
[2]UG Student, Department of Electronics and Communication Engineering, Dayananda Sagar Academy of Technology and Management, Bengaluru, Karnataka, India

[*]*Corresponding Author: Manu H. M*
*Email: ajayreddy15.y@gmail.com*

## Abstract:

The development of a contact-less integrity verification system for microelectronics using near- field electromagnetic (EM) analysis. The system is designed to insert digital signatures into hardware or software targets and then detect them without physical contact. The system consists of two main components: a transmitter and a receiver. The transmitter generates digital signatures using a linear-feedback shift register (LFSR) circuit and emits them as near-field EM signals. The receiver uses a probe and a high-speed oscilloscope to sense the EM signals and detect the digital signatures.

This also includes the protection against EM interference, error correction mechanisms, and experimental results related to the logic utilization, memory usage, and speed of EM signature generation. Additionally, it provides information about the researchers involved in the project, their affiliations, and their research interests.

It's a novel methodology for authenticating hardware and software at different stages of their supply chains. It enables the secure transmission of information from an IC without physical contact and can be applied to various applications such as reading a physical unclonable function (PUF) output signature, authenticating hardware or software cores within embedded systems, and securely transmitting other types of information from an IC.

## Keywords:

Near-field electromagnetic emission, hardware integrity verification, FPGA fabric, system on chip, linear-feedback shift register, counterfeit electronics.

## 1. Introduction:

The relentless march of miniaturization and complexity in modern electronics has yielded remarkable advancements. However, this progress comes with a hidden vulnerability: the growing threat posed by counterfeit and substandard microelectronic components. These malicious actors infiltrate the intricate supply chain, jeopardizing the integrity of entire systems. The consequences can be far-reaching, encompassing intellectual property (IP) theft, system malfunctions, and even catastrophic safety hazards.

Traditionally, safeguarding against these threats has relied on meticulous physical testing of components. These methods, although crucial, are often time-consuming, require specialized equipment, and can even render the component unusable after testing. This creates a bottleneck in the verification process, hindering efficiency and practicality.

A novel technique for verifying the integrity of microelectronics using near-field electromagnetic (EM) analysis. This method offers a non-contact approach, eliminating the need for physical testing and streamlining the verification process.

Understanding the Risks: Counterfeits and their Destructive Impact.

The global electronics market is a vast and complex network. Components often change hands multiple times before reaching the final product. This intricate web creates opportunities for counterfeiters to introduce malicious components that mimic the functionality of legitimate ones.

These counterfeits can be difficult to detect and pose a multitude of risks:

- IP Theft: Counterfeit components may lack the robust security features present in genuine ones, exposing sensitive design information and functionalities to unauthorized access. This can lead to the theft of valuable intellectual property, crippling innovation and impacting a company's competitive edge.
- Functionality Issues: Counterfeits may not meet the performance specifications of the original components. This can lead to system malfunctions, reduced lifespan, and unexpected behavior. In critical applications, such as medical devices or aerospace systems, these malfunctions can have dire consequences.
- Safety Hazards: Substandard components may fail to meet safety regulations, potentially causing overheating, fires, or even catastrophic system failures. Imagine the devastating consequences of a counterfeit component causing a fire in an aircraft or a malfunction in

a medical device during a critical procedure.

Currently, several methods exist for verifying the integrity of microelectronics. However, these methods come with their own set of limitations:

- Functional Testing: This method verifies if the component performs its intended function as specified. While crucial, it may not reveal underlying security vulnerabilities or potential for future failures. Think of it as testing a car's engine – it might start and run, but it won't reveal hidden rust or faulty brakes.
- Microscopic Inspection: This technique involves visually examining the component's physical structure for signs of tampering or deviations from the original design. While helpful in identifying crude counterfeits, it may not be effective for more sophisticated forgeries that mimic the genuine component's appearance almost flawlessly.
- Destructive Testing: This method involves physically breaking down the component to analyze its internal structure and materials composition. While providing detailed information, it destroys the component and is not suitable for high-volume verification or situations where preserving the component is crucial. It's like dissecting a frog to understand its anatomy – informative, but not a viable method for studying a living population.

These traditional methods are often time-consuming, require specialized equipment and expertise, and can render the component unusable after testing. Furthermore, they may not be readily applicable to complex systems with multiple components, creating logistical challenges.

A New Dawn: Contact-Less Verification with Near-Field EM Analysis

A novel approach that overcomes these limitations: contact-less integrity verification using near-field EM analysis. This method leverages the inherent electromagnetic emissions that all electronic components generate during operation. These emissions, though often unintentional, carry information about the component's internal functionality and design. They act as a unique fingerprint, whispering secrets about the component's authenticity.

The proposed technique involves two key steps:

Secure Information Embedding: A unique identifier or signature is embedded within the target microelectronic component. This can be achieved through hardware modifications for logic circuits or software modifications for microprocessors or Systems-on-Chip (SoCs). This

signature serves as the verification key for the specific component.

Near-Field EM Analysis: A specialized near-field probe is used to analyze the electromagnetic emissions generated by the component during operation. These emissions are processed to extract the embedded signature information.

By comparing the extracted signature with the expected value for the genuine component, the integrity of the microelectronic component can be verified without any physical contact. Imagine using a special scanner to read a hidden code embedded within the component's emissions.

## 2. Background and motivation:

The background and motivation are centered on the need for secure information transmission and probing methods to verify the integrity of digital integrated circuits (ICs) based on their electromagnetic (EM) near-field emissions. The proposed methodology aims to protect systems against counterfeit components and has been tested on both high-level instructions executed by microprocessors or Systems-on-Chip (serving as examples of software), and also logic circuits within FPGA fabrics and ASICs (serving as examples of hardware). And also highlights the need to maintain the integrity of electronic components used in diverse sectors and the threats posed by counterfeit and substandard microelectronic components in the modern supply chain. Additionally, it focuses the limitations of current mainstream hardware or software authenticating methods and the need for non-contact authentication systems for hardware and software verification.

## 3. Methodology:

### 3.1 EM signal generation:

EM signal generation involves creating electromagnetic waves for various applications such as communication, radar, and imaging. The process begins with designing the signal's characteristics, including frequency range, modulation scheme, and power level. Oscillators, like crystal or LC oscillators, generate the carrier wave at the desired frequency, ensuring stability and accuracy. Modulation techniques, such as AM, FM, or digital modulation, imprint information onto the carrier wave, encoding data for transmission. Amplification boosts the signal's power to appropriate levels for transmission, employing RF amplifiers while maintaining

Fidelity and spectral purity. Filtering and conditioning remove unwanted noise and harmonics, ensuring compliance with regulatory standards. Antenna coupling connects the amplified signal to an antenna, optimizing radiation efficiency and coverage.

Monitoring circuits measure signal parameters like power level and modulation depth, employing feedback loops for dynamic adjustments. Testing and calibration validate system performance through laboratory and field tests, ensuring reliability and accuracy.

EM signal generation encompasses a systematic process involving signal design, carrier wave generation, modulation, amplification, and conditioning, antenna coupling, monitoring, and testing. Each step contributes to creating reliable and efficient electromagnetic signals tailored to specific communication needs.

### 3.1.1. Authentication information generation:

The process described involves the generation of authentication information unique to each integrated circuit (IC) to ensure integrity verification and security. This is achieved using pseudo-random number generation (PRNG) circuits, implemented either through hardware logic gates or software functions, depending on whether it's for hardware or software authentication.

The PRNG circuits are designed to create a multitude of unique and unpredictable electrical signals containing digital signature information. This uniqueness and unpredictability are crucial to thwart potential attacks, ensuring that the generated authentication information cannot be easily intercepted or replicated by attackers. By incorporating these PRNG circuits into ICs, the aim is to enable the authentication of hardware or software components, especially when deployed in large quantities. This authentication mechanism helps prevent counterfeiting of hardware or software, safeguarding against unauthorized access and tampering.

Once the unique digital signatures are generated, they can be emitted from the IC in the form of electromagnetic (EM) emissions. This means that the authentication information can be transmitted wirelessly, making it suitable for various applications where physical connections may not be feasible or secure. Overall, this approach provides a robust method for generating authentication information that enhances the security and integrity of ICs, thereby mitigating risks associated with unauthorized access, interception, and counterfeiting. For Example, Secure Access Key Fobs, in a corporate setting employees use access key fobs to gain entry to secure areas within the office premises. These key fobs contain embedded integrated circuits (ICs) with built-in pseudo-random number generation (PRNG) circuits. The PRNG circuits are designed using hardware logic gates to generate unique digital signatures for each key fob. When an

employee presents their access key fob to the card reader at a secure entrance, the reader wirelessly communicates with the key fob's IC. The IC emits the unique digital signature as electromagnetic emissions, which the reader captures and verifies in real- time to authenticate the access key fob. This authentication process ensures that only authorized personnel can gain entry to restricted areas, enhancing overall security. Additionally, the use of wireless communication streamlines the authentication process, providing convenience to employees while reducing the risk of interception by potential intruders.

## 3.2. Security improvement using inter-chip variations:

Inter-chip variations in the context of contact-less integrity verification of microelectronics using Near-field electromagnetic (EM) analysis offer a sophisticated means to enhance security. At the core of this approach lies the exploitation of inherent differences in physical characteristics between individual integrated circuits (ICs), stemming from variations in manufacturing processes such as lithography, doping, and material composition. These variations result in subtle differences in IC behavior, including electromagnetic emissions, which can be leveraged for security purposes.

In the realm of anti-counterfeiting measures, inter-chip variations offer an effective means to distinguish genuine devices from counterfeit ones. Manufacturers can establish reference profiles based on the electromagnetic signatures of authentic ICs and use near-field EM analysis to compare these signatures against those of suspected counterfeit devices. Deviations from expected patterns can indicate potential counterfeiting attempts, enabling timely detection and mitigation of counterfeit products. Moreover, inter-chip variations can serve as indicators of tampering or physical alterations to ICs. By continuously monitoring the electromagnetic emissions of ICs using near-field EM analysis, deviations from baseline characteristics can signal unauthorized access or tampering attempts. This enables proactive security measures, such as triggering alarms or disabling compromised devices, to mitigate potential security breaches.

In the example of secure access key fobs, each key fob contains an embedded integrated circuit (IC) with inherent inter-chip variations stemming from manufacturing processes. These variations result in subtle differences in the electromagnetic emissions of each key fob, which can be probed and analyzed using near-field EM analysis. By leveraging these variations, unique identifiers or fingerprints can be extracted from the electromagnetic signatures of individual key fobs. During the authentication process at secure entrances, the card reader communicates wirelessly with the key fob's IC and captures its electromagnetic emissions. Through near-field EM analysis, the reader extracts the unique identifier from the electromagnetic signature,

enabling contact-less authentication of the key fob based on its intrinsic characteristics. This approach enhances security by reducing reliance on external credentials or tokens, mitigating the risk of unauthorized access through cloning or replication of access cards.

## 3.3 Error correction mechanism:

Even when the proposed magnetic field emissions used for hardware and software authentication are detected with high SNR, it is still possible for external interference to generate bit errors while constructing the digital signature. Potential interference sources include 1) other logic circuits operated in the FPGA fabric, and 2) software functions running on the HPS. Thus, an error correction mechanism is needed to detect or correct potential bit errors. For example, here we use a Hamming code that can detect and correct 1-bit errors.

A Hamming code encodes the input data with parity bits (or redundant bits) inserted at certain positions, namely those which are powers of 2 (i.e., positions 1, 2, 4, 8, 16, 32,) to generate a final Hamming-encoded vector. The total number of parity bits is determined by the expression:

$$2N \geq n + N + 1 \qquad (1)$$

Where N is the number of parity bits and n is the length of the input data. For a 32-bit digital signature, a minimum of 6 parity bits are required to detect and correct single-bit errors. Since each parity bit Px governs different data bits Dx, parity bits P1, P2, P4, P8, P16 and P16 at positions 1, 2, 4, 8, 16 and 32 of the final (32, 26) Hamming vector can be computed using Eqn. (2), where D1 ~ D32 are the data bits of a 32-bit signature. Errors in the data bits can then be detected as mismatches between the parity bit values of the original and the reconstructed digital signatures, respectively. Also, a single-bit error can be corrected through the syndrome decoding method.

$P1 = D1 \oplus D2 \oplus D4 \oplus D5 \oplus D7 \oplus D9 \oplus D11 \oplus D12 \oplus D14 \oplus D16 \oplus D18 \oplus D20 \oplus D22 \oplus D24 \oplus D26 \oplus D27 \oplus D29 \oplus D31,$

$P2 = D1 \oplus D3 \oplus D4 \oplus D6 \oplus D7 \oplus D10 \oplus D11 \oplus D13 \oplus D14 \oplus D17 \oplus D18 \oplus D21 \oplus D22 \oplus D25 \oplus D26 \oplus D28 \oplus D29 \oplus D32,$

$P4 = D2 \oplus D3 \oplus D4 \oplus D8 \oplus D9 \oplus D10 \oplus D11 \oplus D15 \oplus D16 \oplus D17 \oplus D18 \oplus D23 \oplus D24 \oplus D25 \oplus D26 \oplus D30 \oplus D31 \oplus D32,$

$P8 = D5 \oplus D6 \oplus D7 \oplus D8 \oplus D9 \oplus D10 \oplus D11 \oplus D19 \oplus D20 \oplus D21 \oplus D22 \oplus D23 \oplus$

D24 ⊕ D25 ⊕D26,

P16 = D12 ⊕ D13 ⊕ D14 ⊕ D15 ⊕ D16 ⊕ D17 ⊕ D18 ⊕ D19 ⊕ D20 ⊕ D21 ⊕ D22 ⊕ D23 ⊕ D24 ⊕ D25 ⊕ D26, P32 = D27 ⊕ D28 ⊕ D29 ⊕ D30 ⊕ D31 ⊕ D32.

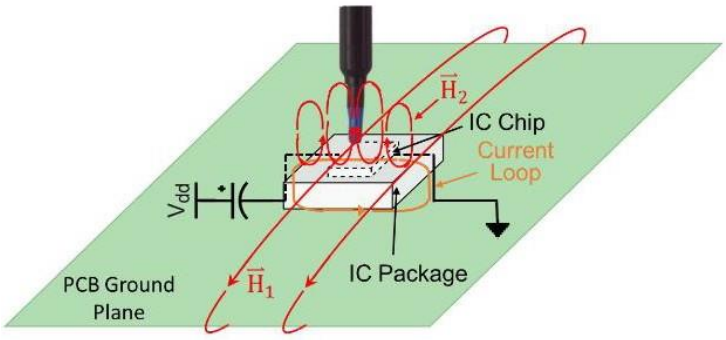


***Figure. 1: Mechanism of near-field magnetic emissions from an IC***

## 4. EM signal sensing:

EM signal sensing involves the detection, acquisition, analysis, interpretation, and decision-making based on electromagnetic (EM) signals emitted by electronic devices or systems. It begins with the detection of EM radiation using specialized sensors or antennas, followed by signal acquisition using receivers or spectrum analyzers. The acquired signals undergo analysis to extract useful information like frequency, amplitude, and modulation. This analyzed data is then interpreted to derive insights or make decisions, such as optimizing wireless communication or identifying threats in radar systems. EM signal sensing finds applications in wireless communication, radar systems, electronic warfare, remote sensing, and medical imaging, playing a vital role in various domains by enabling the detection, analysis, and utilization of EM radiation for diverse applications.

### 4.1. Near-field em emissions from ics:

The transmission of encoded signature information from an integrated circuit (IC) through electromagnetic (EM) emissions, focusing specifically on magnetic field emissions due to their typically higher signal-to-noise ratio (SNR) compared to electric field emissions. This superiority arises from two key factors: lower ambient noise for magnetic fields and the limited influence of non-magnetic materials on magnetic fields. In contrast, dielectric materials, which are prevalent in everyday objects, strongly affect electric fields. In the context of non-contact probing, the research focuses on capturing magnetic field emissions from embedded authentication systems after IC assembly on a printed circuit board (PCB). These emissions

primarily include near-field emissions from internal circuitry, conductive emissions from PCB traces, and direct emissions from bond wires within the IC package. However, the primary emphasis is on near-field emissions due to challenges in probing PCB traces and the high frequency of direct emissions, which can distort embedded signatures.

Near-field magnetic emissions from an IC involve two main components: 1) field 2*H*2 generated by transient current loops across the internal IC and 2) field 1*H*1 formed around the ground plane of the PCB. The strength of 2*H*2, localized within approximately 10 mm above the IC package surface, surpasses 1*H*1 and serves as the primary source of near-field emissions detected by a magnetic field probe. The proposed system employs a near-field magnetic probe and broadband pre-amplifier to capture these emissions, enabling the recovery of digital signatures for hardware and software authentication. By leveraging near-field magnetic emissions from ICs, the research aims to develop a non-contact method for capturing encoded signature information, which is crucial for hardware and software authentication. This approach is particularly valuable for applications where PCB traces are inaccessible or where high-frequency direct emissions pose challenges for accurate signature recovery.

The process of modeling near-field electromagnetic (EM) emissions from an integrated circuit (IC) involved simulating a rectangular current loop placed on a two-layer printed circuit board (PCB) with an FR4 dielectric layer in between. The loop, with its ground pin connected to the bottom copper layer via a via, carried a current of 150 μA.

Using an EM field solver (COMSOL Multiphysics), the quasistatic magnetic field surrounding the loop was simulated, revealing that the magnetic field strength was highest along the traces on the PCB plane, where the current flowed.

The amplitude of the magnetic field emissions was visualized as a color map, indicating the distribution across the PCB plane. Additionally, the field amplitude at the center of the loop was plotted against the distance from the PCB plane, showing a symmetrical decay above and below the plane. The theoretical approximation of the magnetic field followed the behavior of a circular loop with the same area, with the on-axis field decreasing proportionally to the inverse of the cube of the distance from the loop's characteristic size. Moreover, the study examined the maximum distance at which magnetic field emissions could be reliably detected, considering factors such as measurement noise, signal-to-noise ratio (SNR), magnetic probe sensitivity, and pre-amplifier gain. The graph depicting the relationship between the maximum sensing distance and the current applied to the trace loop showed rapid growth for currents below 20 mA before saturating at around 12.5 mm. However, in real-world scenarios, the emitted field amplitude is

typically weaker due to shielding provided by additional on-chip metal layers, limiting the useful sensing distance to approximately 10 mm.

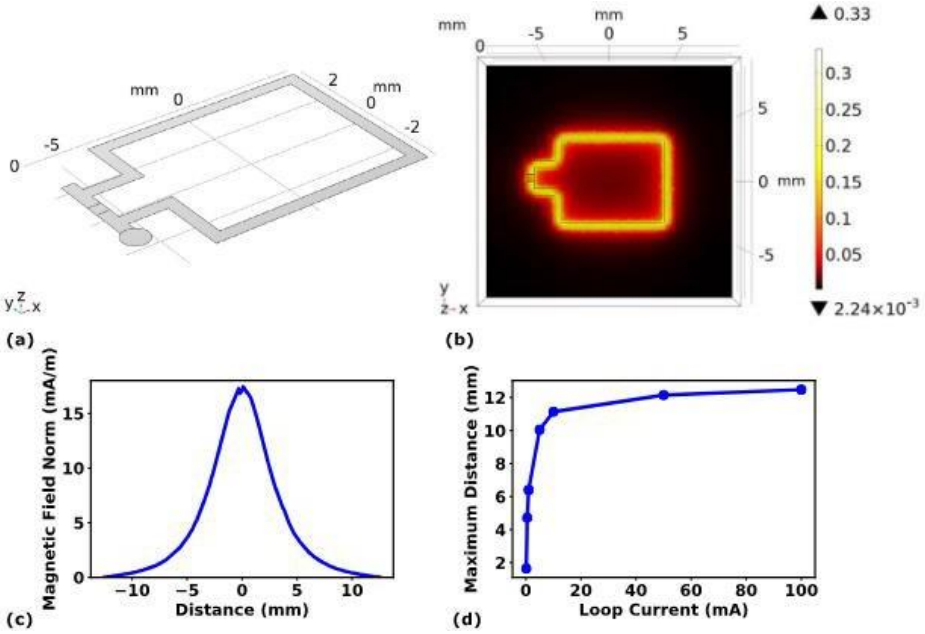


***Figure. 2:***

Fig. 2: Simulation results of quasistatic magnetic field emitted from a 150 μA current loop on a PCB. (a) 3D model of a trace loop on a 2-layer PCB. (b) Color map of the magnetic flux density (in T) across the PCB plane. (c) Magnetic field amplitude (in mA/m) versus distance from the PCB plane, as measured along a line through the center of the loop. (d) Maximum distance for reliable detection of magnetic field emission as a function of loop current.

The field amplitude at the center of the loop is plotted in Fig. 2(c) as a function of distance from the PCB plane, d. This figure shows that the magnetic flux density is maximal on the plane containing the loop but decays symmetrically with d both above and below this plane.

Theoretically, the field may be approximated by that of a circular loop with the same area, A. Using Ampere's law, the resulting on-axis field is given by,

$$H_z(d) = \frac{\sqrt{\pi}}{2}\frac{AI}{(\pi d^2 + A)^{3/2}}, \quad (3)$$

Where I denote the current and the loop is assumed to lie in the XY-plane. Eqn. (3) shows that Hz decreases ∝ 1/d3 for distances larger than the characteristic size of the loop, √A/π. This dependence limits the maximum sensing distance of the proposed non-contact authentication method. In addition, we studied the maximum distance at which magnetic field emissions from the loop are detectable as a function of I, the loop current. The amplitude of the minimally detectable magnetic field emission signal was calculated as about 0.134 A/m based on the following conditions: 1) measurement noise floor of 0.34 mV; 2) a minimum SNR of 2.5 dB

for robust signal detection (50% probability of detection at a false alarm rate of 3.2% in Gaussian noise); 3) a magnetic probe sensitivity of 3 m Vm/A at a frequency of 2.5 MHz; and 4) a pre- amplifier gain of 30 db. Fig. 3(d) shows a graph of the maximum distance required to reliably detect the magnetic field emissions as a function of the current applied to the trace loop. The graph shows that the maximum sensing distance grows rapidly for currents < 20 mA before saturating at ∼12.5 mm. In reality, the emitted field amplitude is typically weaker than in the simulation model due to the shielding provided by additional on-chip metal layers, thus limiting the useful sensing distance to ∼10 mm.

## 4.2. Accurate detection of embedded signatures:

Accurate detection of embedded signature information relies on maximizing the signal-to-noise ratio (SNR) of the measured magnetic field emission signal, which can be achieved through two main methods. The first method involves optimizing the on-chip source to increase the strength of the magnetic field (*H*). This can be achieved, for instance, by enhancing the self-inductance of interconnects within gate arrays mapped to an FPGA fabric through careful routing and layout constraints during the floor-planning stage. Conversely, the second method relies on employing signal processing techniques, such as low-pass filtering, to attenuate high-frequency noise in the sensed signal, thereby increasing the SNR.

An additional signal processing technique employed for SNR enhancement is matched filtering, known for its optimal accuracy in detecting known signals (minimal false error rate, *Pfa*, for a given probability of detection, (*Pd*) in white Gaussian noise. This technique can also be extended to situations where the noise is non-white by adding a whitening filter before the matched filter. Specifically, in the context of the integrity verification system, the known signal of interest (i.e., the embedded digital signature or template) is denoted by $s(t)$, while the noisy received data is represented by $r(t) = s(t) + n(t)$, where $n(t)$ is additive white noise. The impulse response of the corresponding matched filter, $hM(t)$, is defined as

$$HM(t) = s*(t0 - t), \quad (4)$$

Where $*$ denotes complex conjugation and $t0$ is the time at which peak output SNR is achieved. The output of the matched filter, $Sout(t)$, is obtained through convolution of $r(t)$ with $hM(t)$, resulting in

$$Sout = r(t) * hM(t) = s(t) * s*(t0 - t) + n(t) * s*(t0 - t). \quad (5)$$

The first term represents the desired signal, while the second term corresponds to the filtered noise. Notably, the convolution operation is equivalent to cross-correlation, requiring $O(N2)$

operations for a length-N signal vector. Alternatively, matched filtering can be performed in the frequency domain, where the convolution becomes a multiplication, significantly reducing the computational complexity to $O(N\log(N))$ operations due to the efficiency of the fast Fourier transform (FFT).

The improvement in SNR achieved through matched filtering depends on the bandwidth-time product ($B\times Tp$) of the known signal or template $s(t)$. For instance, for a pulse-like template of length $Tp$ and amplitude $A$, the waveform is "compressed" to a duration approximately $1/B$, where $B$ is its bandwidth (referred to as pulse compression in radar systems). The amplitude of the compressed pulse ($'A'$) conserves signal energy and is determined by $A'=ABTp$. Since the noise is uncorrelated with $hM(t)$, its root mean square (rms) amplitude remains unaffected by the matched filter, resulting in an output SNR improvement factor of $BTp$. The integrity verification system utilizes pseudorandom bit streams as the signals of interest (i.e., the embedded signatures), characterized by $Tp=nbit/fclk$ and $B\approx 1/fclk$, where $fclk$ denotes the clock frequency and $nbit$ is the signature length. Consequently, such waveforms exhibit a bandwidth-time product ($B\times Tp$) approximately equal to $nbit$. Therefore, the improvement in SNR provided by matched filtering is directly proportional to the length of the signature ($nbit$). Consequently, with a fixed sensing distance $d$, matched filtering enables a reduction in the amplitude of the on- chip field source by a factor of $nbit$ while preserving SNR. Alternatively, considering that field amplitude decreases proportional to $1/d3$, matched filtering can also be utilized to increase the maximum usable sensing distance by a factor of 33 $nbit$ when the field source remains constant.

## 4.3. Protection against em interference (EMI):

Several approaches to both i) protect a target IC against external EMI attacks, and ii) also prevent the target IC from generating its own EMI. These methods can be classified into two categories based on circuit design at the EM transmitter (i.e., the target IC) and signal processing at the EM receiver. Some EMI removal or prevention methods are implemented at the FPGA or SoC level using logic circuits or software instructions, respectively. For example, resistance to external EMI attacks on the hardware authentication system can be improved by using differential signalling both within the FPGA fabric and for the I/O pins. Most FPGA families feature built-in modules for converting single-ended I/O to differential protocols such as low-voltage differential signalling (LVDS) or current-mode logic (CML). Such differential signals are robust to common-mode noise, i.e., noise that appears with the same polarity at both the non-inverting and inverting input terminals of a differential amplifier, as shown in Fig. 4.

Another method for improving resistance to EMI or EM-based attacks on an FPGA fabric is to copy the target circuit to different regions of the IC.

As a result, this technique can help protect against localized EMI that affects only a subset of these copies. However, this method is ineffective against attacks that affect the entire chip.

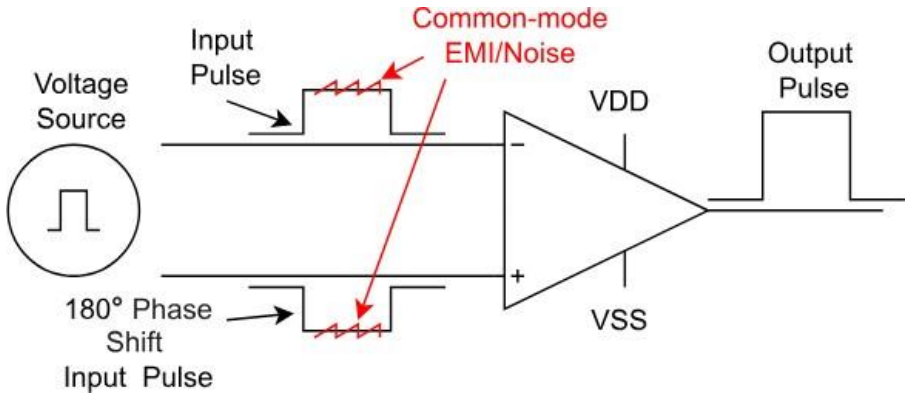


***Figure. 3: The concept of using differential signaling to reduce the impact of common-mode noise, such as external EMI***

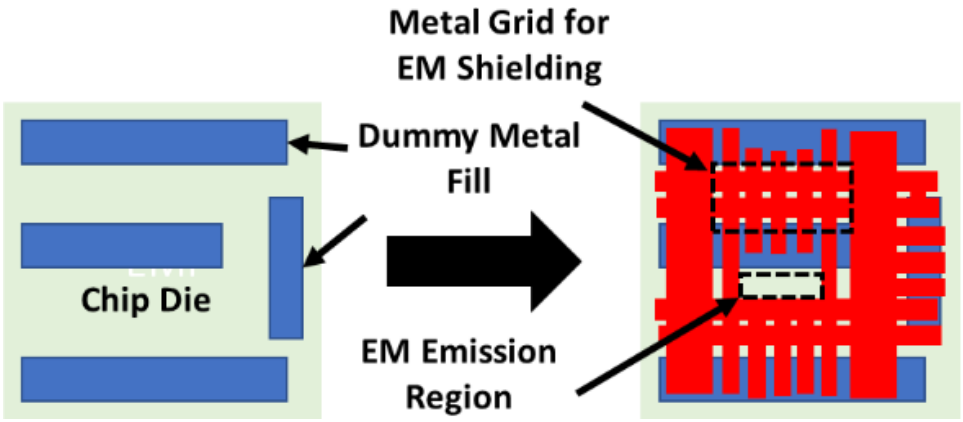


***Figure. 4: Summary of the design flow for fabricating EM-shielding layers using dummy metal fills***

ASICs offer designers additional options for eliminating and/or tailoring EMI. In particular, ASICs can include custom on-chip metallization patterns that are optimized to block external EMI but still allow for EM emissions of the desired electrical signals. For example, unconnected ‘‘dummy’’ metal fills, which are typically used to planarize the chip surface, can be reconfigured to serve as an EMI shielding layer. Specifically, EMI shielding regions are formed by connecting squares of the (normally floating) dummy metals together to form metal grids with hole dimensions much smaller than the EMI wavelength, thus blocking external EMI. On the other hand, fill blocking layers are used to remove dummy metals from regions where desired EM emissions take place. The resulting design flow is summarized in Fig. 4. At the receiver end, signal processing methods can be used to minimize noise and EMI within the

signals recorded by the data acquisition (DAQ) system. Out-of-band EMI can be removed by using a band-pass filter, while in-band noise can be minimized by using a matched filter. As discussed in the previous section, a matched filter enhances signal components that match the selected template while suppressing unmatched components such as those due to EMI.

## 5. Hardware and software integrit verification systems:

In the realm of hardware and software integrity verification systems, Fig. 5 illustrates the intricacies of securely transferring information to and from an integrated circuit (IC) through near-field emissions. The process begins with the selection of a security-critical signal, denoted as S, which could represent a digital watermark or signature. This signal is then associated with a pseudo-random number generator (PRNG) seed value. The PRNG, implemented either in hardware through logic gates within FPGA fabric or ASIC, or in software via high-level instructions within an HPS (Hard Processor System), generates an electrical signature signal, SE, corresponding to the chosen security signal S. To enhance data integrity, an error correction code is applied to SE, followed by encryption using a cipher function, C, with a designated key, K. The resultant encrypted electrical signal undergoes serialization and conversion into an electromagnetic (EM) signal, primarily magnetic, denoted as SEM, in a bit-wise manner by an EM transmitter.

For authorized parties seeking to verify integrity, a near-field magnetic probe serves as the EM receiver. This receiver has the capability to detect the emitted magnetic field signal, SEM, and subsequently recover the signature information using a matched filter. These steps encapsulate the comprehensive process involved in ensuring the integrity of hardware and software through non-contact means.

### 5.1. FPGA fabric-based system:

The proposed hardware integrity verification system is realized on an FPGA fabric, incorporating both a pseudo-random number generator (PRNG) circuit for generating digital signatures and near-field emission and sensing capabilities. The system architecture, depicted in Fig. 6, comprises two primary modules: a transmitter and a receiver. The transmitter module consists of a file system, a Hard Processor System (HPS), and the FPGA fabric. The file system stores pairs of signature values and their corresponding seed values, generated offline by the PRNG circuit. The HPS receives an intended digital signature value from a user input, searches for a match in the signature list, and outputs the corresponding seed value to the PRNG in the FPGA fabric.

This PRNG generates the final magnetic field emission signature based on the provided seed value.

On the other hand, the receiver module integrates a magnetic field probe with a high-speed oscilloscope (DAQ system) for measuring magnetic field emission signals. Real-time signal averaging is performed during each signature period to enhance the Signal-to-Noise Ratio (SNR). The signature detection module further improves the SNR by implementing a low-pass filter to minimize out-of-band noise and using matched filtering to detect the signature waveform. Within the FPGA fabric, modules for random number generation, error correction, and parallel-in to serial-out conversion are implemented. The PRNG circuit can be a Linear Feedback Shift Register (LFSR) generating a high-entropy digital signature, followed by error correction using a Hamming code. The encoded bitstream is serialized, encrypted, and written into different registers to strengthen the magnetic field emissions. To optimize field strength, layout and routing within the FPGA fabric are designed to maximize interconnect inductance. Clocking of sequential logic blocks is done by either an off-chip stable clock or an on-chip ring Oscillator (RO) to introduce chip-specific EM signal patterns. During normal operation, a synchronization sequence embedded within the emitted magnetic field replaces the wired trigger signal used in experimental procedures.

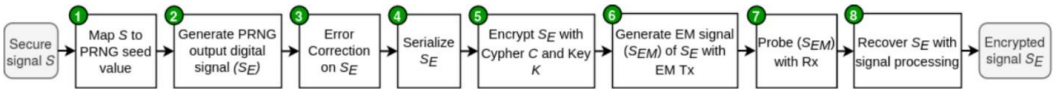


***Figure. 5: Flow chart of secure information generation and detection through the proposed hardware/software integrity verification system***

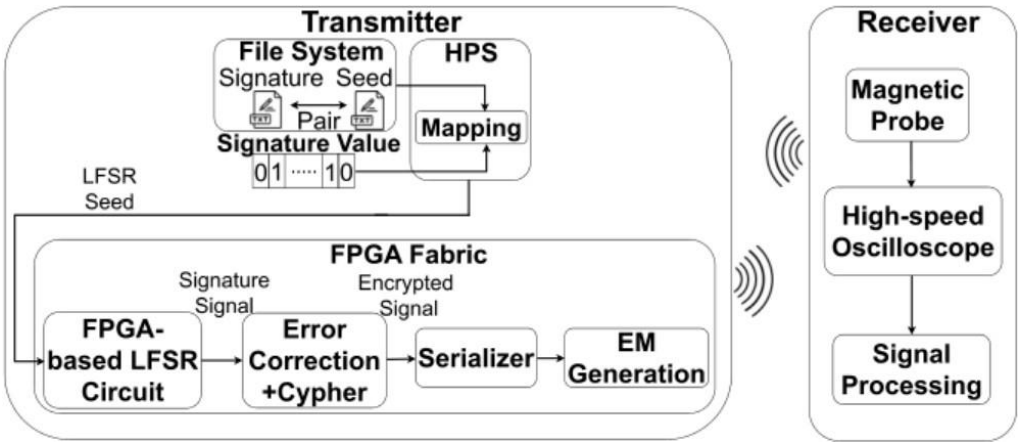


***Figure. 6: System architecture of FPGA-based hardware integrity verification using H-field emissions for secure information generation and sensing***

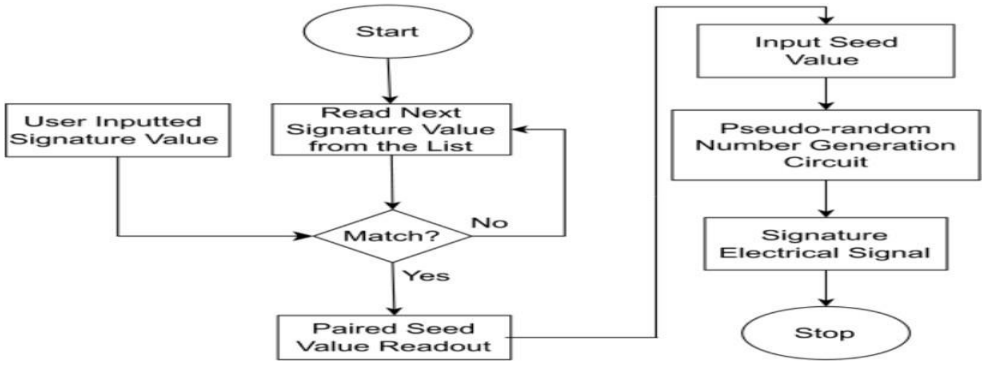


***Figure. 7: Flow chart of mapping an input signature value S, to the electrical output of a PRNG (step 1-2) from Fig 5***

## 5.2. Acid-based system:

The hardware integrity verification system described in the previous section can be readily extended to ASICs by replacing the FPGA fabric with custom logic. Standard cell placement and routing on ASICs is highly customizable, thus allowing 1) the SNR of the EM emission signals to be more easily optimized during the design phase; and 2) dummy metallization patterns to be customized for EM shielding purposes. The hardware integrity verification system described in the previous section can be readily extended to ASICs by replacing the FPGA fabric with custom logic. Standard cell placement and routing on ASICs is highly customizable, thus allowing 1) the SNR of the EM emission signals to be more easily optimized during the design phase; and 2) dummy metallization patterns to be customized for EM shielding purposes.

## 5.3. HPS-based system:

The extension of the proposed integrity verification approach to software running on an embedded Hard Processor System (HPS) broadens its applicability to systems where only software-based processing is available, such as computers or embedded processors. The architecture of the software authentication system, depicted in Fig. 9, mirrors that of the hardware authentication system, with all functions executed on the HPS through software instructions. In this setup, the same mapping procedure is implemented in the HPS to find the seed value corresponding to a Linear Feedback Shift Register (LFSR) signature input. Signature and seed pairs are stored in the file system, which is booted from an external memory dedicated to the System-on-Chip (SoC). The receiver and signal detection algorithm remain identical to those used in the hardware authentication system.

The functions of the Pseudo-Random Number Generator (PRNG) and error correction are now

performed using processor instructions in a high-level programming language. The PRNG utilizes a software function that recursively runs an LFSR to generate periodic multiple-bit digital signatures specified by user input. Error correction employs the same Hamming code algorithm for error detection and correction. To initiate periodic measurements, a GPIO pin configured as a processor-based trigger signal is utilized. During actual operation, this trigger pin can be replaced by an embedded synchronization sequence. Strong magnetic field emissions, crucial for maximizing the received Signal-to-Noise Ratio (SNR), are generated by processor instructions. For instance, writing a word into a HPS register in the SoC produces robust emissions. This observation is leveraged to maximize amplitude modulation of the magnetic field due to the embedded signature.

The modulation process for each signal period involves reading the encrypted signature signal, controlling the GPIO pin to output a trigger signal, sequentially examining each bit of the signature, setting or clearing the LED bit in the GPIO register address based on the bit value, and applying time delays to differentiate between logic '1' and '0' emissions. After examining all signature bits, the modulation process concludes, and the trigger signal is disabled until the next signal period, with further modulation achieved through additional time delays.

The modulation process for each signal period involves reading the encrypted signature signal, controlling the GPIO pin to output a trigger signal, sequentially examining each bit of the signature, setting or clearing the LED bit in the GPIO register address based on the bit value, and applying time delays to differentiate between logic '1' and '0' emissions. After examining all signature bits, the modulation process concludes, and the trigger signal is disabled until the next signal period, with further modulation achieved through additional time delays.

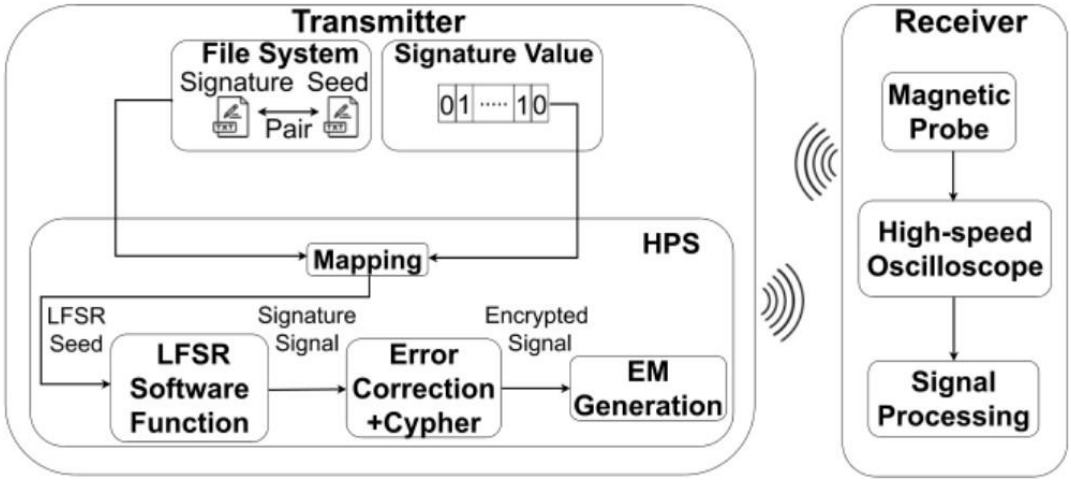

***Figure. 8: System architecture of HPS-based software integrity verification using $\vec{H}$-field emissions for secure information generation and sensing***

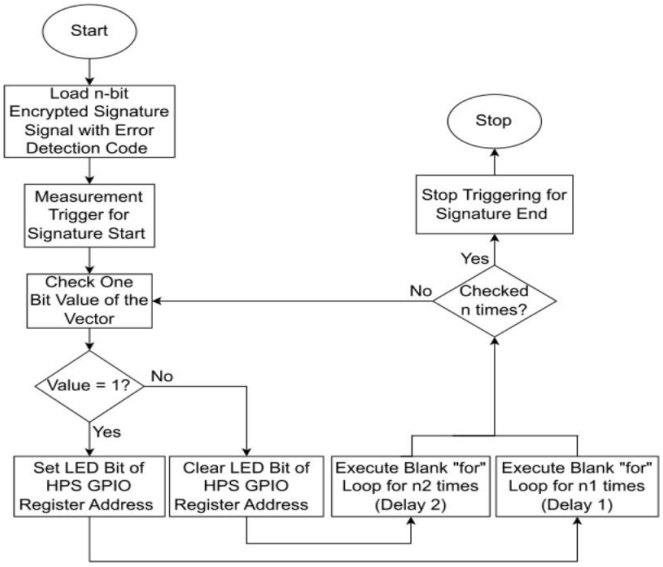


***Figure. 9: Flow chart of generating an EM signal in the HPS instance for EM-based integrity verification (step 6 of Fig. 5)***

## 6. Applications:

Contact-less integrity verification of microelectronics using near-field Electromagnetic (EM) analysis has numerous applications across various industries and domains. Some key applications include:

### 6.1. Hardware security:

Ensuring the integrity and authenticity of hardware components, such as integrated circuits (ICs), microcontrollers, and Field-Programmable Gate Arrays (FPGAs), is critical in sectors like aerospace, defense, and telecommunications. Near-field EM analysis provides a non-invasive method to verify the authenticity of these components and detect any unauthorized modifications or tampering.

### 6.2. Supply chain security:

Verifying the integrity of electronic components throughout the supply chain is essential to prevent counterfeit or compromised hardware from entering critical systems. Near-field EM analysis enables rapid screening of components to validate their authenticity and integrity, thereby enhancing supply chain security.

### 6.3. Embedded systems:

Embedded systems are prevalent in various applications, including automotive, industrial

control, and medical devices. Ensuring the integrity of embedded systems is crucial for safety and reliability. Near-field EM analysis can be employed to verify the integrity of firmware, configuration data, and cryptographic keys stored in embedded systems.

## 6.4. Critical infrastructure protection:

Critical infrastructure, such as power grids, transportation systems, and financial networks, relies heavily on electronic components and systems. Detecting and mitigating potential threats, such as hardware Trojans or malicious implants, is vital for protecting these critical assets. Near-field EM analysis provides a proactive approach to identify and address security vulnerabilities in electronic systems.

## 6.5. IoT Security:

With the proliferation of Internet of Things (IoT) devices, ensuring the security and trustworthiness of connected devices is paramount. Near-field EM analysis offers a means to verify the integrity of IoT devices and detect any unauthorized modifications or malicious activities, safeguarding against potential cyber threats.

## 6.6. Medical device security:

Medical devices, including implantable devices and diagnostic equipment, rely on electronic components for functionality and data processing. Ensuring the integrity and security of these devices is essential to prevent unauthorized access or tampering, which could compromise patient safety. Near-field EM analysis can be used to validate the integrity of electronic components and firmware in medical devices.

## 6.7. Aviation and automotive security:

Aircraft and automotive systems incorporate numerous electronic components and systems critical for operation and safety. Detecting and mitigating potential security threats, such as hardware tampering or malicious modifications, is essential to ensure the reliability and safety of these systems. Near-field EM analysis offers a non-intrusive method to assess the integrity of electronic components and identify any anomalies or vulnerabilities.

# 7. Conclusion and future work:

The non-contact integrity verification systems presented in this study offer innovative solutions for ensuring the security and reliability of electronic components and systems. These systems,

implemented in both hardware and software, enable seamless integration of digital signatures into target ICs and facilitate secure detection without physical contact. The conclusion and future work of this research are summarized as follows:

The innovative approach employed in these systems addresses a critical need for robust integrity verification mechanisms in electronic devices and systems. By allowing digital signatures to be inserted and detected without physical contact, these systems offer a convenient and efficient solution for ensuring the authenticity of electronic components. This approach represents a significant departure from traditional methods, which often rely on physical inspection or direct contact-based authentication techniques. Furthermore, the versatility of these systems enables their application across various levels of electronic systems, from individual chips to entire PCBs and system-level components. This broad applicability ensures that the integrity verification needs of diverse electronic devices and systems can be addressed effectively. Whether used in consumer electronics, industrial machinery, or critical infrastructure systems, these systems offer a reliable means of ensuring the security and reliability of electronic components and systems. Privacy preservation is another key aspect of these systems, as they enable the secure transfer of sensitive information while maintaining the confidentiality of the data being transmitted. This feature is particularly important in applications where privacy and data security are paramount concerns, such as in healthcare, finance, and government sectors. By providing a secure and reliable means of transmitting sensitive information, these systems can help organizations comply with stringent data protection regulations and safeguard against unauthorized access or tampering. The robust security measures incorporated into these systems ensure their resilience against potential attacks or vulnerabilities. Leveraging encryption mechanisms, programmable PRNGs, and error correction algorithms, the systems are designed to withstand various security threats and maintain the integrity of the authentication process. By implementing these advanced security measures, these systems offer a high level of assurance to users and organizations seeking to protect their electronic assets from malicious actors or unauthorized access. In terms of performance, these systems demonstrate rapid generation of unique pseudo- random digital signatures and achieve high sensitivity in detecting emitted H-field emissions. This high performance is critical for ensuring the efficiency and effectiveness of the integrity verification process, particularly in high-speed electronic systems or applications where real- time authentication is required. By delivering robust performance capabilities, these systems meet the stringent requirements of modern electronic devices and systems, thereby enhancing their overall security and reliability.

Looking ahead, future work will focus on enhancing the security, performance, and applicability of these non-contact integrity verification systems. Efforts will include implementing additional security measures to protect against electromagnetic interference (EMI) attacks, optimizing system performance to enhance efficiency and accuracy, and validating the systems in real-world applications across various industries. By continuing to innovate and improve upon these systems, researchers aim to establish them as indispensable tools for ensuring the security and integrity of electronic components and systems in the digital age.

## 8. References:

(1) M. M. Ahmed, D. Hely, N. Barbot, R. Siragusa, E. Perret, M. Bernier, and F. Garet, ‘‘Radiated electromagnetic emission for integrated circuit authentication,’’ IEEE Microw. Wireless Compon. Lett., vol. 27, no. 11, pp. 1028–1030, Nov. 2017.

(2) M. M. Ahmed, E. Perret, D. Hely, R. Siragusa, and N. Barbot, ‘‘Guided electromagnetic wave technique for IC authentication,’’ Sensors, vol. 20, no. 7, p. 2041, Apr. 2020.

(3) P. Karthigaikumar and K. Baskaran, ‘‘An ASIC implementation of a low power robust invisible watermarking processor,’’ J. Syst. Archit., vol. 57, no. 4, pp. 404–411, Apr. 2011.

(4) B. Min and V. Varadharajan, ‘‘Rethinking software component security: Software component level integrity and cross verification,’’ Comput. J., vol. 59, no. 11, pp. 1735–1748, Nov. 2016.

(5) M. Aydos, T. Yantk, and C. K. Koc, ‘‘A high-speed ECC-based wireless authentication on an ARM microprocessor,’’ in Proc. 16th Annu. Comput. Secur. Appl. Conf. (ACSAC), 2000, pp. 401–409.

(6) C. Vaughan, ‘‘Xbox security issues and forensic recovery methodology (utilising Linux),’’ Digit. Invest. vol. 1, no. 3, pp. 165–172, Sep. 2004.

(7) M. Tehranipoor, U. Guin, and D. Forte, Counterfeit Integrated Circuits: Detection and Avoidance. Cham, Switzerland: Springer, 2015. Available: https://books.google.com/books?id=2yqkBgAAQBAJ

(8) . Bhunia and M. Tehranipoor, Hardware Security: A Hands-on Learning Approach. San Mateo, CA, USA: Morgan Kaufmann, 2018.

(9) J. K. Brotz, R. W. Hymel, R. J. Punnoose, T. Mannos, N. Grant, and N. Evans, ‘‘FPGA authentication methods,’’ US Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2017-5214R and 653370, May 2017.

(10) F.Bache, C. Plump, J. Wloka, T. Güneysu, and R. Drechsler, ‘‘Evaluation of (power) side-channels in cryptographic implementations,’’ Inf. Technol., vol. 61, no. 1, pp. 15–28, Feb. 2019.

(11) M. Nagata, D. Fujimoto, N. Miura, N. Homma, Y.-I. Hayashi, and K. Sakiyama, ‘‘Protecting cryptographic integrated circuits with side-channel information,’’ IEICE Electron. Exp., vol. 14, no. 2, Jan. 2017, Art. No. 20162005.

(12) G. Keramidas, A. Antonopoulos, D. N. Serpanos, and S. Kaxiras, ‘‘Non deterministic caches: A simple and effective defense against side channel attacks,’’ Design Autom. Embedded Syst., vol. 12, no. 3, pp. 221–230, Sep. 2008.

(13) G. T. Becker, M. Kasper, A. Moradi, and C. Paar, ‘‘Side-channel based watermarks for integrated circuits,’’ in Proc. IEEE Int. Symp. Hardware- Oriented Secur. Trust (HOST), Jun. 2010, pp. 30–35.

(14) L. Lin, M. Kasper, T. Güneysu, C. Paar, and W. Burleson, ‘‘Trojan side-channels: Lightweight hardware trojans through side-channel engineering,’’ in Cryptographic Hardware and Embedded Systems—CHES, C. Clavier and K. Gaj, Eds. Berlin, Germany: Springer, 2009, pp. 382–395.

(15) W. Liang, B. Liao, J. Long, Y. Jiang, and L. Peng, ‘‘Study on PUF based secure protection for IC design,’’ Microprocessors Microsystems, vol. 45, pp. 56–66, Aug. 2016.

(16) J. Zhang and G. Qu, ‘‘Recent attacks and defenses on FPGA-based says,’’ ACM Trans. Reconfigurable Technol. Syst., vol. 12, no. 3, pp. 1–24, Aug. 2019.

(17) G. E. Suh, D. Clarke, B. Gassend, M. V. Dijk, and S. Devadas, ‘‘Efficient memory integrity verification and encryption for secure processors,’’ in Proc. 36th Annu. IEEE/ACM Int. Symp. Microarchitecture. Washington, DC, USA: IEEE Computer Society, Dec. 2003, pp. 339–350.

(18) X. Li, Q. Wen, W. Li, H. Zhang, and Z. Jin, ‘‘Secure privacy-preserving bio-metric authentication scheme for telecare medicine information systems,’’ J. Med. Syst., vol. 38, no. 11, p. 139, Nov. 2014.

(19) A. Clark, E. Dawson, J. Fuller, J. Golic, H. Lee, W. Millan, S. Moon, and L. Simpson,

''The LILI-II keystream, generator,'' in Information Security and Privacy (Lecture Notes In Computer Science), vol. 2384, L. Batten and J. Seberry, Eds. Melbourne, QC, Australia: Deakin University, Jul. 2002, pp. 25–39.

(20) S. Bhunia and M. Tehranipoor, Hardware Security: A Hands-on Learning Approach. Amsterdam, the Netherlands: Elsevier Science, 2018.

(21) U. Jetzek, Galois Fields, Linear Feedback Shift Registers and Their Applications. Munich, Germany: Carl Hanser Verlag GmbH & Company KG, 2018.

(22) R. W. Hamming, ''Error detecting and error correcting codes,'' Bell Syst. Tech. J., vol. 29, no. 2, pp. 147–160, Apr. 1950.

(23) B. Deutschmann, H. Pitsch, and G. Langer, ''near field measurements to predict the electromagnetic emission of integrated circuits,'' in Proc. Int. Workshop Electromagn. Compat. Integr. Circuits, 2005, pp. 27–32.

(24) V. Pano, I. Tekin, Y. Liu, K. R. Dandekar, and B. Taskin, ''TSV-based antenna for on-chip wireless communication,'' IET Microw., Antennas Propag., vol. 14, no. 4, pp. 302–307, Mar. 2020.

(25) P. P. Ray, ''Intelligent ingestibles: Future of Internet of Body,'' IEEE Internet Comput., vol. 24, no. 5, pp. 19–27, Sep. 2020.

(26) Z. Martinasek, V. Zeman, P. Sysel, and K. Trasy, ''near electromagnetic field measurement of microprocessor,'' Przeglad Elektrotechniczny, vol. 89, pp. 203–207, Jan. 2013.

(27) A. Inan, R. Said, and S. Umran, Engineering Electromagnetics and Waves, Global Edition (Law Express Questions & Answers). London, U.K.: Pearson Education, 2015. [Online]. Available: https://books.google.com/books?id=19w4CQAAQBAJ.

(28) I.A. Aref, N. A. Ahmed, F. Rodriguez-Salazar, and K. Elgaid, ''RTL-level modeling of an 8B/10B encoder–decoder using SystemC,'' in Proc. 5t IFIP Int. Conf. Wireless Opt. Commun. Netw. (WOCN), May 2008, pp. 1–4.