Calibratable Polymorphic Temperature Sensor for Detecting Fault Injection and Side-channel Attacks

Tasnuva Farheen[1], Sourav Roy[1], Jia Di[3], Shahin Tajik[2], and Domenic Forte[1]
[1]Department of Electrical and Computer Engineering, University of Florida
[2]Department of Electrical and Computer Engineering, Worcester Polytechnic Institute
[3]Department of Electrical and Computer Engineering, University of Arkansas

***Abstract*—Security of a computing system can be compromised by physical attacks against the hardware. Side-channel attacks involve the observation of integrated circuit (IC) or system behavior to extract assets such as cryptographic keys. Fault injection attacks involve the manipulation of underlying circuits to provoke erroneous operations that lead to the escalation of privilege or leakage of secret information. Some side-channel and fault injection attacks force circuits to work at temperatures out of operating range. Several countermeasures have been proposed to detect temperature change. However, they do not perform well in wide temperature fluctuations, have a large overhead area, or introduce other reliability concerns. This paper proposes a calibratable Null Convention Logic-based (NCL) polymorphic sensor that changes its functionality with temperature and can sense whether the temperature goes below or above a carefully designed application-specific threshold. It can be used with a wide range of process technologies without requiring significant modification. Low area overhead, low power consumption, configurable nature, and easy integration make it ideal for ICs. Our results show that this sensor can work at various temperature ranges with reliable operation with $\pm 1^0 C$ confidence, $8\ \mu m^2$ area and $19.2\ \mu W$ power overhead, which is approximately $40x$ less overhead compared to alternative techniques.**

***Index Terms*—Polymorphic Temperature Sensor, Fault Injection Attack, Side Channel Attacks, Polymorphism, Calibratable Sensor, Polymorphic Circuit**

I. Introduction

Embedded electronic devices are essential components of networked systems requiring strong cryptography to maintain data confidentiality and integrity. Despite such cryptographic primitives, the security of deployed devices can still be compromised by attackers, who gain access to them in hostile environments and launch physical attacks. Physical attacks pose a severe threat to the hardware implementation of any computing system. The most powerful tools in the arsenal of physical attacks are fault injection and side-channel attacks. Moreover, the advent of sophisticated temperature-based fault injection and side-channel attacks have added another dimension, unveiling the vulnerabilities posed by temperature variations on integrated circuits (ICs) and electronic devices [1]. Heating fault attacks [2] and temperature-assisted side-channel attacks [3] represent two distinct yet interrelated facets of exploiting temperature-induced weaknesses in hardware security. These attacks leverage the manipulation of temperatures to induce faults, trigger malfunctions, or extract sensitive information, like parts of the internal memory and cryptographic key from targeted devices [4], [5].

Many attacks have been performed over the years using this temperature effect. As reported in [4], high-temperature fault attacks were investigated, observing memory errors after hours of extensive heating. The uses of spotlight clip-on lamps to induce errors into memory have been described in [5] as well. Also, clock glitch attacks performed on microcontrollers at ambient temperatures of 100°C or higher cause more faults, making the attacks easier in practice [6]. There have also been reports of temperature-stressed data remanence attacks [1], where the content in SRAM could be read after stressing the device for long hours at high temperatures. Using memory collisions in dual-port SRAM, an attack was reported in [7] that exploited remote temperature faults in FPGA. The growing concern over temperature-assisted hardware attacks makes tamper-resistant countermeasures for protecting these sensitive data imperative.

A number of countermeasures have been developed to address temperature-based exploits. One approach is the use of temperature-dependent polymorphic circuits as temperature sensors. They are designed to exhibit

multiple behaviors or functionalities based on specific operating conditions. These circuits can dynamically adapt their functionality or configuration in response to changing environmental factors such as temperature, voltage, or other parameters. An evolutionary algorithm is often used to design these circuits, which is most often cartesian genetic programming [8], [9]. However, one of these designs' most prominent bottlenecks is the inefficiency in transistor sizing [10], [11]. Each polymorphic gate must be individually evolved for the current application, and the creation of polymorphic gates in this way discourages the development of design guidelines to minimize overheads. Moreover, it is time-consuming and highly technology-dependent. Another common approach is the ring oscillator (RO) based temperature sensor. These sensors work by exploiting the dependence of the propagation delay of an RO on temperature [12]. The output frequency of the RO changes with temperature due to variations in the propagation delay of each inverter. This variation in frequency can be used to estimate the chip's temperature. However, this implementation has enormous area penalties. There are also several temperature sensors based on the relationship of voltage with temperature. However, the area and power consumed by the pn-junctions used in these sensors are not attractive for on-chip applications, and the performance of ΔVd-based sensors appears to be seriously degraded in fine feature processes because of degradations in the performance of the parasitic vertical pnp transistor [13], [14], [15], [16].

This paper proposes an NCL-based polymorphic temperature sensor to address all these challenges. Null Convention Logic (NCL) is a logic style for designing low-power, high-performance digital circuits. Due to its unique characteristics, including reduced power consumption, simplicity, low area overhead, and technology Independence, it is explored here to design a temperature sensor. The proposed sensor can detect temperature variations exploited by side-channel and fault injection attacks. The basic circuitry of an NCL-based temperature sensor consists of complimentary logic in pull-up and pull-down networks and an NMOS transistor threshold drop effect. Compared to other temperature sensor designs, our NCL-based polymorphic temperature sensors have several advantages:

- They have a low area overhead and can be easily integrated into existing circuits.
- It is calibratable, working at various temperature ranges, even in the face of process variations, with reliable operation.

Contributions. Our main contributions in this paper are summarized as follows:

- We propose a temperature sensor that can detect the temperature variation due to temperature-based physical and remote attacks.
- We apply the state-of-the-art polymorphic circuit design methodology (NCL-based) along with the body biasing effect to create a temperature-controlled polymorphic gate. We show that the temperature by which the gate's function changes is easily tunable through a gate voltage to fit different attack scenarios.
- We propose a calibration circuit to enable the sensor to work in a wide temperature range.
- To assess the reliability of the sensor, we analyze the effect of process variation on it performing Monte Carlo simulation.
- We perform simulation analysis to verify our sensor's efficacy and report our sensor's reliable operation with $\pm 1^0 C$ confidence.

II. Background

A. Attack Vectors

In this section, we describe potential attacks that leverage the effect of temperature.

1) Fault Injection Attack: Fault injection attack due to heating involves deliberately inducing localized temperature alterations in a targeted hardware component to compromise its functionality or security measures. By subjecting a specific area of the hardware to excessive heat, attackers aim to create faults or vulnerabilities that can be exploited to undermine the device's security. This attack leverages the susceptibility of hardware elements to malfunctions or altered behavior when exposed to elevated temperatures. The induced heat can disrupt the normal functioning of the hardware, potentially causing bit flips, altered logic operations, or revealing sensitive information stored within the device. High-temperature fault attacks have been investigated in [4], observing memory errors after hours of extensive heating at around 75°C. Similar results have been reported in [5], where errors were induced into memories using a 50 W spotlight clip-on lamp. By heating an IBM JVM to 100°C, they were able to inject faults with a probability of 71.4% before their machine crashed. It is also reported in [6] that clock glitch attacks performed on a microcontroller at an ambient temperature of 100°C or higher induce more faults, making the fault attacks easier to perform

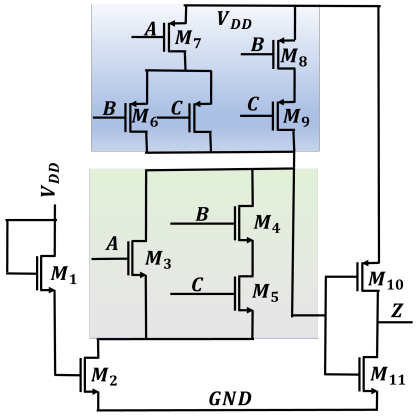


Fig. 1: Polymorphic threshold gate, with gating NMOS transistors M1 and driving M2 transistor [17] corresponding to Boolean function $AB + BC + CA$ (blue) at low voltage and $A + BC$ (green) at high voltage.

in practice. In [7], a remote temperature fault attack in FPGA was reported that relied on memory collisions in dual-port SRAM. The collisions cause the temperature to gradually go beyond 85°C, potentially creating faults resulting in a denial of service and privilege escalation.

2) Data Remanence Attack: Volatile memories, like registers and SRAM, are integral parts of any CPU or system-on-chip (SoC). They store a variety of on-chip sensitive assets, such as cryptographic keys, intermediate cipher computations, passwords, obfuscation keys, and hardware security primitive outputs. Although such data should be erased as soon as the power is off, it can be susceptible to burn-in-stress data remanence effects. In this attack, the attacker exposes the device to extensive temperature for several hours to accelerate aging effects. Consequently, residual data remains in the volatile memories, enabling the attacker to access and extract its contents successfully. It has been reported in [1] that they were able to read the content of SRAM memories after stressing the device for 36 hrs at 100°C.

3) Temperature Assisted Side-channel Attacks: Temperature-assisted side-channel attacks exploit the correlation between a device's behavior and changes in temperature. These attacks involve monitoring the device's response to varying temperatures, revealing variations in power consumption, electromagnetic emissions, or execution time. For instance, as the temperature fluctuates, the power consumption of a device might exhibit distinct patterns. Adversaries can measure these variations to infer the device's specific operations or extract cryptographic keys. Similarly, changes in execution time or electromagnetic radiation due to temperature alterations can divulge valuable insights into the device's internal processes. In [18], it is shown that increasing the temperature of the hardware to around 50°C-70°C caused undesirable leakage of masked cipher implementations.

B. Design of Polymorphic Circuits

Polymorphic Circuits are logic circuits that perform two or more different functions under varying operating conditions. These varying conditions may encompass voltage, temperature, or light. The first polymorphic circuits were introduced by NASA's Jet Propulsion Laboratory in 2001 [9]. Since the original proposal, polymorphic logic has been implemented in CMOS processes with multiple functions [19]. These original polymorphic gates are often designed using genetic algorithms to size transistors so that the output behavior of the gate changes with a design variable. However, each transistor in a polymorphic gate necessitates a tailored evolutionary process aligned with its specific application, thereby impeding the establishment of design paradigms aimed at minimizing complexities. Furthermore, this process is time-consuming and difficult to port to different technology nodes in practice.

A new polymorphic gate design approach has been proposed in [17]. In this publication, researchers developed supply voltage-controlled technology-independent polymorphic circuits for use with asynchronous null-convention logic (NCL) circuits. The polymorphic TH23-TH23W2 gate shown in Fig. 1, utilizes this technique. Here, the TH23 gate has a threshold value of two and three total inputs. In order for the output to be asserted, at least two of the three inputs must be asserted. Whereas a TH23w2 gate has a threshold of two as well as three total inputs but, input A is assigned a weight of two. In this case, asserting input A would be enough to satisfy the threshold of two alone. The design process is summarized as follows:

- Select two logic functions, where the low-voltage function is a Boolean subset of the high-voltage function. For example, TH23w2 is considered a Boolean subset of TH23. The TH23-TH23w2 polymorphic gate performs the built-in functions of a TH23 NCL gate and a TH23w2 NCL gate. A TH23 gate corresponds to the Boolean function AB+AC+BC and a TH23w2 gate corresponds to the function A+BC.
- The high-voltage function is selected as the less specific Boolean equation. In the case of our later design, this is the A+BC functionality. The low-voltage function is the more specific Boolean equa-

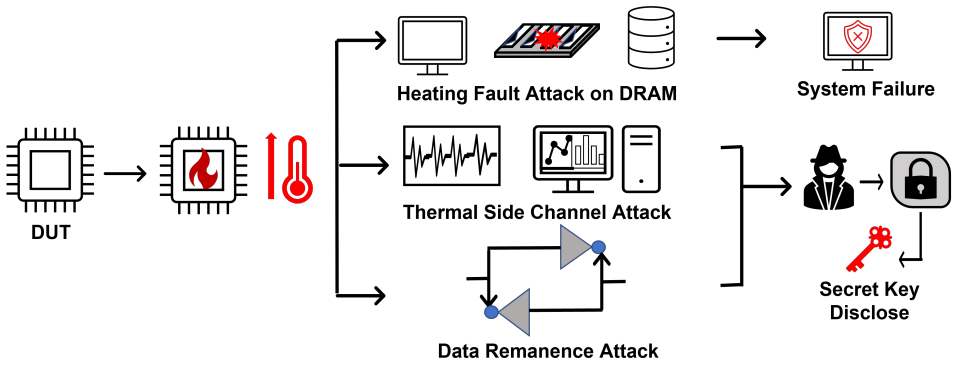


Fig. 2: Temperature assisted Fault Injection, Side-channel and data remanence attacks on the chip via the control of temperature

tion, which is the AB+BC+CA functionality in our design.

- Construct a logic gate with the pull-down network (PDN) of the high-voltage function connected to the pull-up network (PUN) of the low-voltage function. The PDN transistors are sized to be five times larger than the PUN.
- Add two "gating" NMOS transistors – one in threshold drop configuration; that is, it drives the gate of the other, which gates the connection between the pull-down network and ground. These transistors are sized to select the voltage at which the gate exhibits polymorphic behavior, i.e., changes from AB+BC+CA functionality to AB+BC and vice versa.

An example polymorphic threshold gate from [17], shown in Figure 1, demonstrates such a polymorphic structure. In the example, the PUN is that of a threshold three-of-two gate, whereas the PDN is that of a threshold one gate with high biasing. The transistors M1 and M2 are the threshold drop and gating NMOS transistors, respectively. The gating NMOS transistors connect the dominant pull-down network to the ground at high voltages, allowing the high-voltage function to dominate. At low voltages, the gating transistors are turned off, and the pull-down network is disconnected from the ground. The pull-up network is then able to drive the output functionality.

III. Threat Model

Temperature-based attacks can be active or passive. In our threat model, we have considered both cases as depicted in Fig. 2. An active heating temperature side-channel attack is a sophisticated method that actively manipulates a device's temperature to exploit vulnerabilities and extract sensitive information. Attackers first identify the DUT, such as a cryptographic system, and then monitor its behavior under varying temperature conditions. This involves analyzing the device's response to changes in temperature and observing fluctuations in power consumption, electromagnetic radiation, or execution time. The attackers then actively manipulate the temperature of the device. They use external tools or methods to raise the temperature intentionally. This manipulation aims to induce specific responses or vulnerabilities in the device, such as altering its behavior or disclosing the secret key. During active heating, attackers closely monitor the device's behavior for any variations induced by the temperature changes. They analyze these variations to extract sensitive information, such as cryptographic keys or other confidential data processed by the device. Correlation of the observed side-channel information, like power consumption patterns or electromagnetic emissions, with the manipulated temperature changes helps the attacker in this attempt. Attackers may iteratively refine their heating strategies and monitoring techniques to extract more precise or valuable information. This process involves adjusting the temperature ranges, observing subtler variations, and optimizing the extraction of sensitive data. In [18], increasing the temperature of the hardware to around 50°C-70°C caused undesirable leakage of masking implementation.

In a heating fault attack, an attacker intentionally elevates the temperature of the device to induce fault errors that compromise the security. By raising the temperature beyond specified operational limits, attackers aim to cause faults that can be exploited for unauthorized access or to extract sensitive information. The exposure of ICs to extreme temperature causes multiple-bit errors in DRAM memory and disrupts the read/write threshold setting in non-volatile memory, as shown in [20]. A notable proof-of-concept in [5] showcased that in-

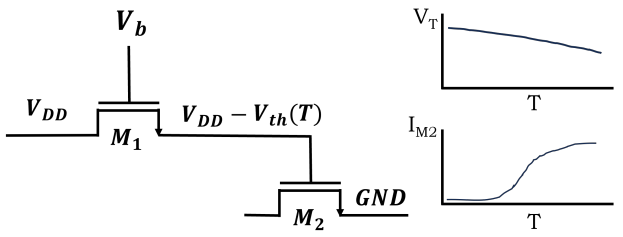


Fig. 3: NFET threshold effect due to temperature. V_b is the variable gate voltage, which can be adjusted depending on the desired temperature threshold in our polymorphic gates.

creasing the temperature of DRAM to 100°C, achieved using a 50W light bulb, triggered up to 10 flipped bits within a 32-bit word with a 71.4% likelihood. Exploiting these temperature-induced bit errors, they successfully bypassed Java type system defenses, uncovering vulnerabilities in two widely-used commercial Java virtual machine implementations. These incidents demonstrate that heating attacks, classified as severe Fault Injection Attacks (FIAs), can potentially inflict lasting damage on ICs if exposure surpasses specified operational limits [2]. The rapid increase in the likelihood of faults with temperatures beyond 60°C is also reported in [21].

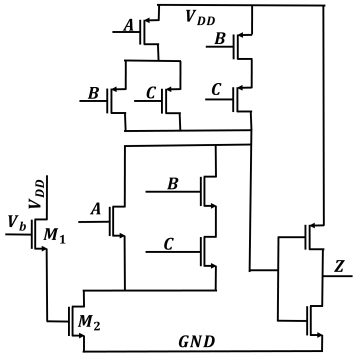
A fault attack can also occur by a remote attack where, due to the attack, the temperature of the device rises, resulting in a fault. In [7], a remote temperature fault attack in FPGA has been reported using memory collision. Due to this attack effect, the temperature gradually goes beyond 85°C, potentially creating faults resulting in a denial of service attack.

To mitigate the threats mentioned above, it is imperative to deploy temperature sensors to monitor temperature variations and detect these attacks. In this regard, our paper proposed an NCL-based temperature sensor that can detect temperature variations due to attack. We have taken 60°C as the deployed temperature in all the attacks is above this threshold.

IV. Proposed Thermally Sensitive Polymorphic Logic Design

A. Conceptual Overview

The key principle for designing our polymorphic gates which is temperature dependent, is to utilize the NMOS gating transistor's threshold effect due to temperature. Instead of connecting $M1$ in threshold drop configuration, we connect its drain to the supply voltage and connect the gate to a bias voltage V_b which is kept constant above the threshold voltage of the transistor as shown in Fig.4. In such configuration, the voltage at the source of $M1$



A	B	C	Z(AB+AC+BC) $T < T_B$	Z(A+BC) $T > T_B$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	0	1
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Fig. 4: NCL polymorphic gate used for temperature sensor. For a particular set of inputs A logic high and B and C logic low, this gate shows polymorphism at a threshold temperature T_B which can be controlled using gate voltage and transistor sizing.

is dropped by its threshold voltage which is dependent on temperature. The relationship of threshold voltage with temperature can be described using the following equation [22]:

$$\frac{\partial V_{th}}{\partial T} = \frac{\Phi_{ms}}{T} + 2\frac{\Phi_F}{T} + t_{OX}\frac{\sqrt{\varepsilon_s q N_a}}{\varepsilon_{OX}\sqrt{\Phi_F}}\frac{\partial \Phi_F}{\partial T} - 6\frac{K}{q} - 2\frac{E_{go}}{qT} \tag{1}$$

Here, an expression for threshold voltage thermal co-efficient is given where V_{th} is the threshold voltage, T is temperature, Φ_{ms} is polysilicon-silicon work function, Φ_F is Fermi potential, t_{OX} is gate oxide thickness, ε is permittivity, N_a is acceptor concentration, q is charge of electron, K is Boltzman constant and E_{go} is temperature independent portion of band-gap energy. The threshold voltage thermal co-efficient slope is negative, which means threshold voltage decreases as temperature increases.

The source voltage also depends on the gate voltage according to the Equation (2):

$$V_S \approx V_{DD} - V_{th} - \sqrt{\frac{2I_D}{\mu_n C_{OX}\frac{W}{L}}} \tag{2}$$

Here, V_S is the source voltage, drain voltage is the supply voltage (V_{DD}), I_D is the current through the transistor, μ_n is the electron mobility, C_{OX} is the oxide capacitance, and W and L are width and length of the transistor. The current I_D is a function of gate voltage which is also the bias voltage, V_b. As V_b increases I_D increases and source voltage V_S decreases. Lower gate voltage, V_b leads to higher V_S. In our thermally sensitive polymorphic gates, this allows the temperature threshold for polymorphism (T_B) to be set by the chip designer as described in more detail below.

Figure 3 illustrates the NMOS transistor threshold

effect which applies to the transistor $M1$ considering constant gate voltage V_b. At fixed V_b, the low threshold voltage at high temperatures above T_B causes degradation at source voltage; however, this degradation is not high enough to impede circuit operation as a pass transistor- driving another NMOS transistor, $M2$, to be completely turned on. In such configuration both the PUN and PDN are active. However, if the temperature decreases lower than threshold, T_B, it results in high threshold voltage causing the gating transistor to be partially on. V_b can be altered to choose suitable T_B for any specific application. At temperatures above T_B, the lower threshold drop causes the pull-down network to be active, selecting the built-in functionality, whereas at temperatures below T_B, the comparatively higher threshold drop forces the pull-down portion to be significantly weakened, causing the function to be changed.

B. Multi-Threshold Null Convention Logic

The polymorphic circuits also use multi-threshold null convention logic (MTNCL). MTNCL is typically used to implement asynchronous logic circuits. Null convention logic (NCL) is an extension to Boolean logic used for asynchronous digital logic circuits where null and intermediate are additional values along with logic high and low giving rise to a four-valued logic. Incorporation of multi-threshold CMOS circuits into the NCL logic gives rise to MTNCL. MTNCL uses dual-rail encoding to represent valid data of 0 and 1 [23]. This preserves the principle of quasi-delay-insensitivity provided by NCL, under which a clock is not needed to synchronize data changes in a pipeline. MTNCL allows lower area overhead and simpler timing analysis while designing polymorphic gates as asynchronous circuits [17].

C. Gate Biasing Effect

Any temperature-sensitive polymorphic circuit can be designed using above design principles and gate biasing effect. We have constructed an example NCL-based polymorphic TH23w2-TH23 gate. The PUN for the polymorphic gate in Fig. 4 is that of the PUN of a 3-input TH23w2 gate consisting of five PMOS devices. The PDN is a 3-input TH23 gate with three NMOS devices. Two gating transistors are connected to the PDN.

The gate biasing effect of the transistor $M1$ is used to control the threshold for polymorphism. The drain voltage of $M1$ is fixed at supply voltage, and gate voltage is fixed at a biasing voltage, V_b. Thus the gate biasing and threshold voltage drop are dependent on temperature. Under temperatures lower than T_B, the threshold voltage drop of $M1$ is low enough to turn on $M2$ allowing the PDN to dominate so that the polymorphic gate behaves like TH23 gate. Under temperatures above T_B, the threshold drop increases enough to turn off or weaken the transistor $M2$, disconnecting the pull-down network, thus, the polymorphic gate behaves like TH23w2 gate.

TABLE I: Transistor sizing for Th23-TH23w2 polymorphic gate.

Transistors	Width (nm)	Length (nm)
M1, M2	1800	45
Calibration Transistors	2000	45
Pull Down NMOS Transistor	2000	45
Pull Up PMOS Transistors	120	45

V. Proposed Sensor

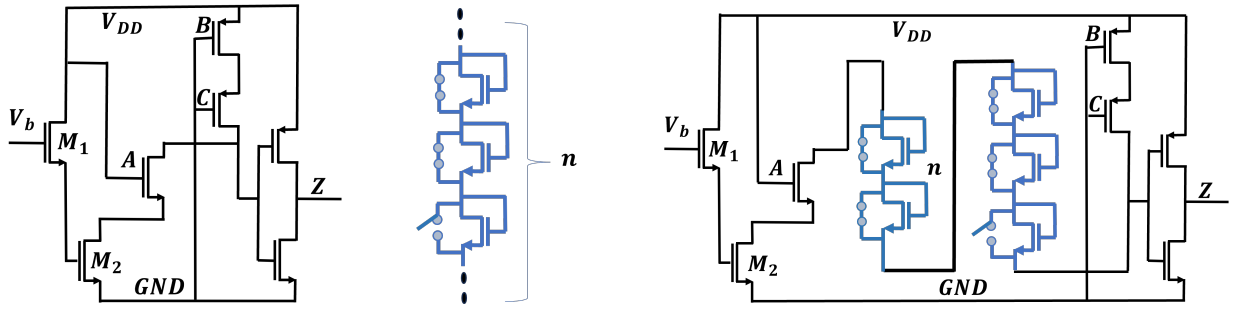
To detect the temperature variation to deploy side-channel and fault injection attacks, we design an NCL-based polymorphic temperature sensor based on the concept described in Section IV-A.

A. Architectural Diagram and Basic Operation

The circuit from Fig. 4 operates as a temperature sensor only for a fixed set of inputs which is $A = 1, B = 0$ and $C = 0$. If input A is connected with supply voltage and inputs B and C are connected to ground then the sensor can be reduced to the circuit shown in Fig. 5(a). In this configuration the sensor output Z is purely dependent on temperature threshold T_B. If the operating temperature is above T_B, the sensor outputs logic high and if the temperature is below T_B, the sensor outputs logic low. The transistor sizes used are provided in Table I.

B. Process Variation Effect

The polymorphism threshold of NCL polymorphic gates depend on the gate voltage of the control transistors used for gate biasing also the aspect ratio of those transistors. The aspect ratio of PUN and PDN also contribute to the polymorphism threshold but the impact of control transistor's sizing outweighs the sizing of PUN and PDN transistors. Due to process variation aspect ratio of control transistors may vary and it may have significant effect on the polymorphism threshold as well. For security critical applications, it is imperative that sensor operate at intended polymorphism threshold irrespective of the process variation and as a result calibration mechanism is needed for that.



(a) (b) (c)

Fig. 5: (a) Sensor circuit after simplification from Fig. 4 by forcing input A to logic high and inputs B and C to logic low. (b) Calibration Circuit consisting of n calibratable NMOS transistors with control switches in parallel. (c) Calibration circuit integrated with sensor circuit.

1) Calibration Circuit: The calibration circuit to compensate for process variation consists of n number of NMOS transistors connected in series with control switches connected in parallel to each transistor. The switches can be used to short the corresponding transistor. The NMOS transistors contribute to the PDN. The more transistors are turned on the stronger the PDN becomes and it requires larger threshold drop due to temperature in the control transistor to disconnect the PDN. The overall effect is the upward shift of the polymorphism temperature threshold. If each transistor contributes to δt change in temperature threshold and in the base design if $n/2$ NMOS switches are turned on, the calibratable temperature range is from $T_B - (n/2)\delta t$ to $T_B + (n/2)\delta t$, where T_B is the threshold temperature for polymorphism in the base design without considering process variation. Process variation within this range can be compensated using the calibration circuitry.

The range can be increased by increasing the number of calibration transistors (n) at the cost of increased area overhead. δt depends on aspect ratio of calibration NMOS transistors and can be fine tuned depending on the intended application. The calibration circuitry is shown in Fig. 5(b) and calibration circuitry integrated with sensor circuitry is shown in Fig. 5(c).

C. Sensor Configurability

The threshold temperature T_B can be controlled using the gate voltage V_b shown in Fig. 4. The mechanism is explained in Section IV-A. The gate voltage V_b can be supplied by a dedicated low dropout regulator (LDO) with proper reference voltage V_{ref}, so that intended application specific temperature threshold, T_B can be obtained. The advantage of using dedicated LDO is that the gate voltage V_b will be constant irrespective of the temperature variation which ensures that T_B remains fixed even under temperature fluctuation. By controlling the reference voltage to the LDO we can configure the gate voltage V_b and threshold T_B. Then using the calibration circuit we can fine tune the threshold. With the combination of V_b and calibration circuitry it is possible to cover a range of temperatures, large enough to encompass all the applications described in Sections II and III.

D. Methods to Mitigate False Positives

During usage of the device, temperature may rise even when there is no malicious attempt is going on. There is a possibility that due to this rise in temperature, it may go beyond the set threshold, T_B and raise the flag denoting temperature-assisted side channel or fault injection attack is taking place. The response mechanism can be designed in such a way that in the condition of false positive, functionality does not suffer but specially designed countermeasure gets activated that prevents attacker from successfully carrying out side-channel or fault injection attacks. One such countermeasure may be activation of power hungry circuitry that will generate extra power overhead that will mask the side channel so that it is difficult for attacker to get relevant information to steal assets. An example of power hungry circuitry may be a network of ring oscillator (RO) [12] implemented in the redundant silicon space or around security critical silicon space. Such RO network remain dormant under temperature threshold of T_B. Once the temperature goes above T_B whether it is due to malicious attack or temperature rise due to usage, the polymorphic sensor raises a flag and activates the RO network. The objective of the RO network is to create additional power signature that masks the switching activity of security critical blocks such as cryptographic core. The disadvantage of using RO as countermeasure is high area and power

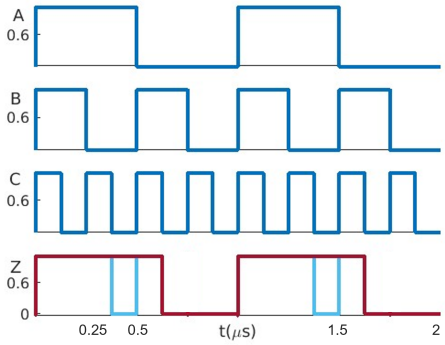


Fig. 6: Polymorphic functionality at normal temperature (Z in blue) and when temperature above 60°C (Z in red).

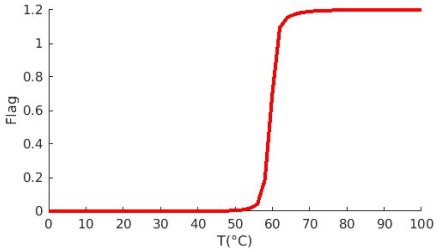


Fig. 7: Flag raises when the temperature is above 60°C.

overhead. The flag of temperature sensor can be used to activate clock-jitter circuitry [24], shuffling [25] or dual rail logic [26] based countermeasure. Such countermeasures may introduce delay and reduce the throughput of the system beside additional area overhead. Another countermeasure that can be used is masking [27] along with the temperature sensor to limit attacker capability to extract secret asset exploiting vulnerable conditions. The temperature sensor can also be used in combination with other sensors such as voltage monitoring sensors [28], electromagnetic sensors [29], TDC based delay sensors [30] etc. to detect malicious intrusion with high confidence and reduce false positives.

E. Methods to Mitigate False Negatives

The impact of temperature effects resulting from various attack methods can differ, presenting either local or global implications. Local effects often necessitate deploying multiple sensors strategically to counter false negatives. In this regard, the distribution of temperature sensors across a chip involves considering several factors, such as anticipated temperature fluctuations during regular operations or potential attacks, the chip's dimensions, its thermal characteristics, and heat dissipation within the circuit. So, it is important to follow some guidelines to mitigate false negatives:

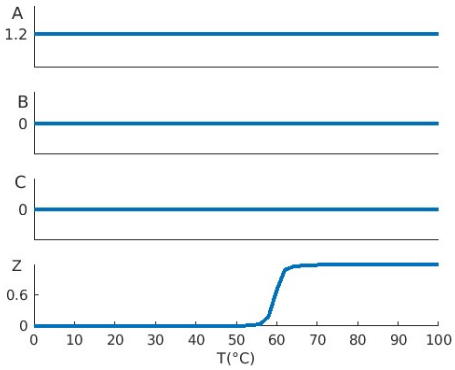


Fig. 8: Sensor output Z changes when temperature goes above 60°C.

a) Placing sensors near areas of high heat dissipation: Areas of the chip that generate a lot of heat will be more susceptible to temperature changes. Hence, it is important to place sensors near these areas to detect any temperature changes accurately.

b) Placing sensors in areas with high spatial variability: Temperature variations can occur at different spatial scales, so it is important to distribute sensors in areas where temperature changes may be more localized or concentrated.

c) Placing sensors in areas critical to system operation: Areas of the chip critical to system operation may be more vulnerable to temperature-based attacks. Hence, it is important to distribute sensors in these areas to quickly detect any faults or anomalies.

d) Using redundancy: Multiple sensors can help improve coverage and reduce the risk of missed temperature changes. By placing sensors in different areas of the chip, redundancy can help to ensure that any temperature changes are detected, even if some sensors fail or are compromised.

e) Sensor placement optimization through simulation: Computer simulations can help identify areas of the chip most vulnerable to temperature changes and optimize the sensors' placement to provide the best coverage.

Overall, distributing temperature sensors on a chip to get the best coverage requires careful consideration of the specific characteristics of the chip. Several algorithms [31], [32] proposed in the literature for sensor placement can be used to optimize our polymorphic temperature sensor placement. By following these guidelines, it is possible to improve the security and reliability of electronic systems.

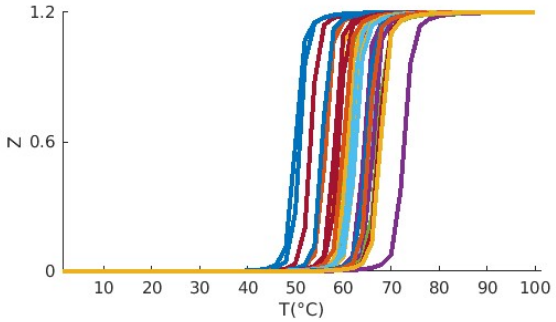


Fig. 9: Monte Carlo simulation to simulate process variation with 6 calibration transistor 'ON' and rest 'OFF'; threshold temperature for polymorphism varies between 50^0C and 72^0C.

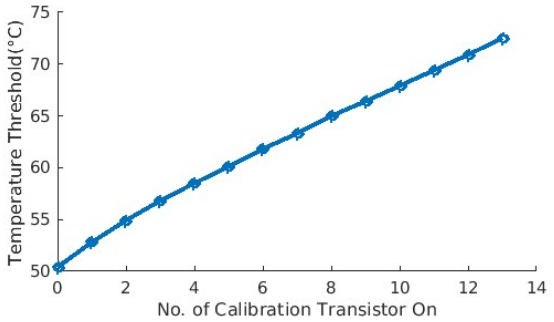


Fig. 10: Effect of calibration transistors on temperature threshold, T_B for polymorphism at constant gate voltage, V_b of $600mV$.

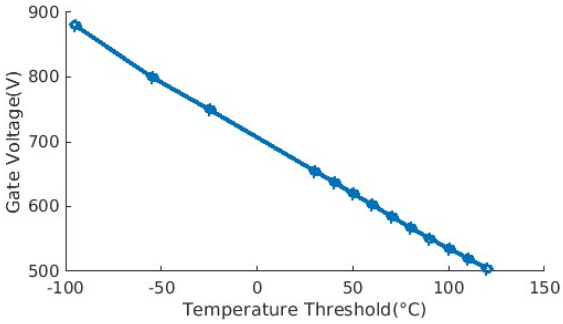


Fig. 11: Gate voltage at various temperature thresholds.

VI. Simulation Results and Discussion

A. Simulation Setup

Cadence Virtuoso ADE simulation environment is used as the simulation environment, and the technology node used in most experiments is 45nm. The supply voltage is set at $1.2V$ and intended temperature threshold is set at 60^0C as a proof of concept. Cadence Virtuoso ADE XL simulation environment is used to perform Monte Carlo analysis for assessing sensor reliability.

B. Simulation Results and Discussion

At first, we have implemented the sensor circuit shown in Fig. 4 with gate voltage V_b fixed at $600mV$. Then we varied the three inputs A, B and C to find out for which set of inputs polymorphism can be observed. We observed that for $A = 1.2V$ and $B = C = 0V$, there is polymorphism in sensor output Z which is shown in Fig. 6. The temperature at which polymorphism occurs is about 60^0C as shown in Fig. 7.

Next, we connected input A to $1.2V$ supply voltage and inputs B and C to ground to implement the sensor circuit shown in Fig. 5(a). We denote the output Z of the sensor as $Flag$. Below 60^0C the sensor outputs 0 and above 60^0C sensor outputs $1.2V$. In other words the $Flag$ is raised when the temperature goes above 60^0C as shown in Fig. 8.

C. Process Variation and Calibration

To simulate process variation we used Monte Carlo simulation with 300 simulations and to compensate the effect of process variation we implemented calibration circuitry as shown in Fig. 5(c). At first, to observe the effect of process variation we implemented the circuit in Fig. 5(c) using the aspect ratio reported in Tab. I with $n = 13$, i.e., 13 calibration transistors. In this implementation, we kept 6 calibration transistors to be 'ON' and rest of the calibration transistors to be 'OFF' to offer calibration capability both direction of T_B. The gate voltage V_b is kept fixed at $600mV$. Using this setup, the temperature threshold T_B is about 62^0C. After the Monte Carlo simulation we observed that, the temperature threshold, T_B varies between 50^0C and 72^0C as shown in Fig. 9.

By turning the calibration transistors 'ON' or 'OFF' we can achieve the intended threshold of 62^0C even considering process variation. Fig. 10 shows how the polymorphism threshold changes if calibration transistors are turned 'ON' incrementally. It is evident that intended threshold of 62^0C can be achieved even at the worst cases of process variation with a confidence of $\pm 1^0C$. The intended threshold, T_B can be controlled by changing the gate voltage V_b as shown in Fig. 11. After setting up the intended threshold, T_B using the appropriate V_b, calibration circuitry can be used to make sure process variation does not affect the intended threshold.

D. Limitations

Although process variations have been handled through calibration, NCL-based temperature sensors have some other limitations as well. Specifically, improvements are necessary for high-precision temperature measurement applications as large number of polymor-

TABLE II: Comparison between previous studies and our work regarding process, performance/power/area (PPA) overhead and working temperature range. 'NR' stands for not reported.

Source	Process	Area (μm^2)	Power (μW)	Error (°C)	Range (°C)
Genetic Algorithm Based Polymorphic Circuit [8]	0.7 μm	571300	Not Reported (NR)	NR	[27–125]
BJT Based Sensor [13]	32 nm	10800	3780	$\pm 1.5^0C$	[40–80]
Band Gap Reference Based Sensor [14]	90 nm	460	25	1^0C	[50–125]
Voltage Calibrated Temperature Sensor [15]	0.16 μm	80000	6.8	$\pm 0.15^0C$	[-55–125]
RO Based Sensor [12]	0.35 μm	NR	NR	NR	NR
Threshold Voltage Based Sensor [16]	0.18 μm	328.6	1.026 (1% duty cycle)	$\pm 0.21^0C$	[-20–100]
This work	45 nm	8	19.2	$\pm 1^0C$	[-95–120]

phic temperature sensors are needed to measure temperature accurately over a large range. Our sensor is more suitable for point temperature sensing applications where only a few sensors are enough for reliable operation.

VII. Related Work

Various temperature sensors have been proposed in the literature, offering distinct advantages and limitations. Genetic algorithm-based polymorphic circuits offer the advantage of inherently built-in features at various operating conditions that can be used as a sensor [8]. However, the inefficient, time-consuming transistor sizing with high overhead make it an unsuitable one. There are also several temperature sensors based on the relationship of voltage with temperature. However, the area and power consumed by the pn-junctions used in these sensors are not attractive for on-chip applications, and the performance of ΔVd-based sensors appears to be seriously degraded in fine feature processes because of degradations in the performance of the parasitic vertical pnp transistor [13], [14], [15], [16]. There are also ring oscillator-based temperature sensors that work by exploiting the dependence of propagation delay on temperature [12]. This implementation has huge area penalties as well as dynamic power consumption .

A performance comparison between the proposed sensor and other temperature sensors has been made in Table II. The polymorphic sensor designed in this work has a low area, low power overhead, and wide temperature range.

VIII. Conclusion and Future Work

Non-invasive physical or remote attacks that can be carried out by utilizing temperature variation can be hard to detect as it does not leave any traces of the attack. Temperature based sensors to detect such temperature-assisted side channel or fault injection attacks are unheard of. Our attempt to address this issue is to utilize the temperature-based polymorphism observed in polymorphic NCL gates. Although traditional polymorphic NCL gates operate with variation of supply voltage, we repurposed this technique to design a novel temperature sensor that changes behavior with temperature. We used simulation to validate the practicality of a temperature sensor to detect temperature-based side channel and fault injection attacks and improved its reliability with the inclusion of calibration circuitry that ensures reliable sensor operation under process variation. In future, we plan to implement temperature based NCL polymorphic sensors in FPGA to validate the usefulness and effectiveness of such sensors in embedded setting.

References

[1] M. Hutter and J.-M. Schmidt, "The temperature side channel and heating fault attacks," in *Smart Card Research and Advanced Applications: 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013. Revised Selected Papers 12*. Springer, 2014, pp. 219–235.

[2] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proceedings of the IEEE*, vol. 100, no. 11, pp. 3056–3076, 2012.

[3] J. Brouchier, T. Kean, C. Marsh, and D. Naccache, "Temperature attacks," *IEEE Security & Privacy*, vol. 7, no. 2, pp. 79–82, 2009.

[4] J.-J. Quisquater and D. Samyde, "Eddy current for magnetic analysis with active sensor," in *Proceedings of eSMART*, vol. 2002, 2002.

[5] S. Govindavajhala and A. W. Appel, "Using memory errors to attack a virtual machine," in *2003 Symposium on Security and Privacy, 2003.* IEEE, 2003, pp. 154–165.

[6] T. Korak, M. Hutter, B. Ege, and L. Batina, "Clock glitch attacks in the presence of heating," in *2014 Workshop on Fault Diagnosis and Tolerance in Cryptography*, 2014, pp. 104–114.

[7] M. M. Alam, S. Tajik, F. Ganji, M. Tehranipoor, and D. Forte, "Ram-jam: Remote temperature and voltage fault attack on fpgas using memory collisions," in *2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 2019, p. 48.

[8] R. Ruzicka, V. Simek, and L. Sekanina, "Behavior of cmos polymorphic circuits in high temperature environment," in *14th IEEE International Symposium on Design and Diagnostics of Electronic Circuits and Systems*. IEEE, 2011, pp. 447–452.

[9] A. Stoica, R. Zebulum, and D. Keymeulen, "Polymorphic electronics," in *Evolvable Systems: From Biology to Hardware: 4th International Conference, ICES 2001 Tokyo, Japan, October 3–5, 2001 Proceedings 4*. Springer, 2001, pp. 291–302.

[10] A. Stoica, R. Zebulum, D. Keymeulen, J. Lohn, and D. Clancy, "On polymorphic circuits and their design using evolutionary algorithms," 2002.

[11] A. Stoica, R. Zebulum, X. Guo, D. Keymeulen, M. Ferguson, and V. Duong, "Taking evolutionary circuit design from experimentation to implementation: Some useful techniques and a silicon demonstration," *IEE Proceedings-Computers and Digital Techniques*, vol. 151, no. 4, pp. 295–300, 2004.

[12] S. Suman and B. Singh, "Ring oscillator based cmos temperature sensor design," *International Journal of Scientific & Technology Research*, vol. 1, no. 4, pp. 76–81, 2012.

[13] J. Shor, K. Luria, and D. Zilberman, "Ratiometric bjt-based thermal sensor in 32nm and 22nm technologies," in *2012 IEEE International Solid-State Circuits Conference*. IEEE, 2012, pp. 210–212.

[14] M. Sasaki, M. Ikeda, and K. Asada, "A temperature sensor with an inaccuracy of -1/+0.8°c using 90-nm 1-v cmos for online thermal monitoring of vlsi circuits," *IEEE Transactions on Semiconductor Manufacturing*, vol. 21, no. 2, pp. 201–208, 2008.

[15] K. Souri, Y. Chae, and K. A. Makinwa, "A cmos temperature sensor with a voltage-calibrated inaccuracy of 0.15 from -55 to 125°c," *IEEE journal of solid-state circuits*, vol. 48, no. 1, pp. 292–301, 2012.

[16] S. Microelectronics, "A CMOS on-chip Temperature Sensor with -0.21°C/0.17°C inaccuracy from -20°C to 100°C ," https://www.academia.edu/105000873, 2013, IEEE International Symposium on Circuits and Systems(ISCAS).

[17] C. Bernard, W. Bryant, R. Becker, and J. Di, "Design of asynchronous polymorphic logic gates for hardware security," in *2021 IEEE High Performance Extreme Computing Conference (HPEC)*. IEEE, 2021, pp. 1–5.

[18] T. De Cnudde, M. Ender, and A. Moradi, "Hardware masking, revisited," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 123–148, 2018.

[19] J. Nevoral, R. Ruzicka, and V. Simek, "Cmos gates with second function," in *2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2018, pp. 82–87.

[20] C. H. Kim and J.-J. Quisquater, "Faults, injection methods, and fault attacks," *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 544–545, 2007.

[21] R. Kumar, P. Jovanovic, and I. Polian, "Precise fault-injections using voltage and temperature manipulation for differential cryptanalysis," *2014 IEEE 20th International On-Line Testing Symposium (IOLTS)*, pp. 43–48, 2014.

[22] S. Microelectronics, "BWorld Robot Control Software," https://www.st.com/resource/en/application_note/, 2006, Online; accessed 10-October-2023.

[23] L. Zhou, R. Parameswaran, F. Parsan, S. Smith, and J. Di, "Multi-threshold null convention logic (mtncl): An ultra-low power asynchronous circuit design methodology," in *Journal of Low Power Electronics and Applications*. MDPI, 2015, pp. 81–100.

[24] A. G. Bayrak, N. Velickovic, F. Regazzoni, D. Novo, P. Brisk, and P. Ienne, "An eda-friendly protection scheme against side-channel attacks," *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 410–415, 2013. [Online]. Available: https://api.semanticscholar.org/CorpusID:2204079

[25] N. Veyrat-Charvillon, M. Medwed, S. Kerckhof, and F.-X. Standaert, "Shuffling against side-channel attacks: A comprehensive study with cautionary note," in *Advances in Cryptology – ASIACRYPT 2012*, X. Wang and K. Sako, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 740–757.

[26] Z. Chen and Y. Zhou, "Dual-rail random switching logic: A countermeasure to reduce side channel leakage," in *Cryptographic Hardware and Embedded Systems - CHES 2006*, L. Goubin and M. Matsui, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 242–254.

[27] T. D. Cnudde, M. Ender, and A. Moradi, "Hardware masking, revisited," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2018, pp. 123–148, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:46939231

[28] T. Farheen, S. Roy, S. Tajik, and D. Forte, "A twofold clock and voltage-based detection method for laser logic state imaging attack," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 31, no. 1, pp. 65–78, 2023.

[29] G. K. A. Oswald, A. T. Richardson, and N. J. Kerry, "Electromagnetic sensor system," Jun. 25 2002, uS Patent 6,411,250.

[30] C.-C. Chen, P. Chen, A.-W. Liu, W.-F. Lu, and Y.-C. Chang, "An accurate cmos delay-line-based smart temperature sensor for low-power low-cost systems," *Measurement Science and Technology*, vol. 17, no. 4, p. 840, 2006.

[31] R. Mukherjee and S. O. Memik, "Systematic temperature sensor allocation and placement for microprocessors," in *Proceedings of the 43rd annual Design Automation Conference*, 2006, pp. 542–547.

[32] M. Arnesano, G. Revel, and F. Seri, "A tool for the optimal sensor placement to optimize temperature monitoring in large sports spaces," *Automation in Construction*, vol. 68, pp. 223–234, 2016.