# Amnesiac Memory: A Self-Destructive Polymorphic Mechanism Against Cold Boot Data Remanence Attack

Tasnuva Farheen[1], Sourav Roy[1], Andrew Cannon[1], Jia Di[3], Shahin Tajik[2], 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 Engineering and Computer Science, University of Arkansas

## ABSTRACT

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 cold boot attacks. Cold boot attack is based on remanence effect of memories, which says that memory contents do not disappear immediately after power is cut; they fade gradually over time, which can be significantly prolonged at low temperatures. This effect can be exploited by rebooting a running machine and reading what is left in memory. This paper proposes a self-destructive latch extending to amnesiac register, protecting sensitive data when temperature goes to freezing conditions. Our proposed latch senses the temperature drop required during such attacks and reacts instantaneously by entering a forbidden data state, erasing registers stored data. The design uses a NULL convention logic (NCL)-based polymorphic NOR/NAND gate, which changes its functionality with temperature. Our results show that latch and register are stable across process variation, corresponding to attack with 99% and 80% confidence. Even for the 20% where data is not destroyed, in 9.5% of cases data flips its state, making reliable extraction difficult for an attacker. The polymorphic mechanism is straightforward to implement due to its easy implementation, and temperature threshold for self-destructive behavior is easily programmed using only one gate voltage.

## KEYWORDS

Hardware security, Cold boot attack, Data remanence, Polymorphic latch, Self-destructive countermeasure, Polymorphic register.

## 1 INTRODUCTION

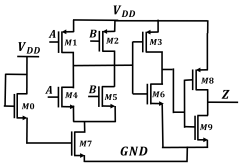
Data security and privacy are paramount in today's digital age. The volatile memory of computing systems plays a vital role in data security. Attackers who gain access to caches, latches, registers, or scan flip flops in a hostile environment can compromise their security by deploying attacks; one such attack is a cold boot data remanence attack. Despite the widespread belief that values stored in volatile memories are instantly lost when power is cut, they gradually fade away over time. Cold boot attacks can use this property to prolong the remanence effect by cooling down or freezing before the attack [22]. The first practical attack based on the remanence effect is described in [7], showing that the RAM data can be recovered, keeping it at $-50^0$C. One past study showed that DRAM data could persist for a full week without refresh when cooled with liquid nitrogen [7]. Also, in numerous kinds of boot scenarios, such as preboot execution environment (PXE), USB, extensible firmware interface (EFI), and iPods, the RAM data can be retrieved in seconds [20]. It is also shown that the secret key of AES and RSA can be retrieved through the recovered RAM data, which means that it is possible to regain secret information even though some data is lost [7, 15]. In addition, [1] has demonstrated that manipulating cryptographic keys generated by SRAM PUFs takes advantage of data remanence effects due to low temperatures. Since these cold boot data remanence attacks pose a significant threat, with the growing use of advanced techniques in hardware attacks, new methods are needed to protect sensitive on-chip data.

A number of potential countermeasures have been developed over the years. Some of them are based on hardware changes that require high additional manufacturing costs and, therefore, are impractical [7, 11, 28]. Defining a specific power-off time could be used to mitigate data remanence [4, 5, 9]; however, [1] shows that this time would have to differ based on the ambient temperature and the device would need to be constantly aware of its on-off state and of time. Sensors are also proposed to detect low temperature and power-off conditions and then trigger the complete destruction of the IC substrate or zeroization of all sensitive data [16, 25]. However, these sensors are separate from the volatile storage elements under attack and, therefore, can be disabled or isolated from the response mechanisms. Most notably, zeroization can be disabled by lowering the CPU/SoC supply voltage to the brownout level where on-chip registers still maintain their contents and thus are susceptible to data exfiltration [18, 23]. Sensors and zeroization mechanisms can also be disabled by physically editing circuits using focused ion beam (FIB) systems [8, 26] before probing.

In this paper, we design a novel self-destructive polymorphic latch and register to protect sensitive data from temperature manipulation. Our approach offers sense and react mechanism at the same time; as a result, it requires no extra circuitry or fabrication steps for reaction mechanisms like other countermeasures and possesses acceptable overhead PPA. On top of that, it has an instantaneous, local response under freezing conditions.

**Contributions.**Main contributions in the paper are summarized:

- We propose a self-destructive polymorphic latch extending to the amnesiac register, protecting sensitive data from cold boot data remanence attacks. This polymorphic mechanism obfuscates sensitive bits by entering a "forbidden" data state when an attack's environmental conditions are fulfilled. In this paper, our latch and register respond to temperature manipulation, protecting the data in a self-destructive manner.
- We apply the state-of-the-art polymorphic circuit design methodology (NCL-based) along with the body biasing effect to create a temperature-controlled NOR/NAND gate. We show that the temperature by which the gate's function changes from NOR to NAND is easily tunable through a gate voltage to fit different




| A | B | Z(NAND) | Z(NOR) |
|---|---|---|---|
| 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 |

**Figure 1: Polymorphic threshold gate, with gating NMOS transistors M0 and M7 [2]. NAND is considered a Boolean subset of NOR, as it outputs a logic 0 under stricter logical conditions (yellow) than NOR.**

attack scenarios. To our knowledge, this is first time temperature has been used to control NCL-based polymorphic gates.

- We generate power, performance, and area of polymorphic latch and register. Later, we compare them to a standard NOR-based latch and register in same technology node.
- We use simulations to verify the reliability of the polymorphic latch and register across process variation. Worst-case performance characteristics are also measured.

## 2 BACKGROUND

**Standard and NCL-based Polymorphic Gates** Polymorphic gates are logic circuits that change their functionality in response to factors such as voltage, temperature, and light. They were first introduced by NASA's Jet Propulsion Laboratory in 2001 [24]. Since the original proposal, polymorphic logic has been implemented in CMOS processes with multiple functions [19]. These original polymorphic gates are often designed by using genetic algorithms to size transistors so that the output behavior of the gate changes with a design variable, but this is challenging, time-consuming, and difficult to port in different technology nodes.

The polymorphic NOR/NAND gate used in our proposed approach utilizes more recent techniques demonstrated in [2]. In this publication, researchers developed *supply voltage-controlled polymorphic circuits* for use with asynchronous null-convention logic (NCL) circuits. 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, NAND is considered a Boolean subset of NOR. The truth table illustrates this idea in Fig. 1. 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. Add two "gating" NMOS transistors, M0 and M7 in Fig. 1 – one in threshold drop configuration; that is, it drives the gate of the other, which gates the connection between the PDN and ground. The supply voltage can be changed to select voltage at which the gate shows polymorphic behavior, i.e., changes behavior from NOR to NAND and vice versa.

## 3 THREAT MODEL

A cold boot data remanence attack requires physical access to the target chip. After getting access, the attacker drops the chip's temperature in running condition, which can be accomplished by spraying compressed nitrogen over the chip. In the next step, a cold rebooting is performed, where the attacker forces the power to shut down for a few seconds and then back on. The steps can also be reversed, where the attacker stops the power first, cools the chip to frozen condition, and then back on the power. Though the attack mechanism is the same, some additional attack steps might be needed depending on the device under attack. For example:

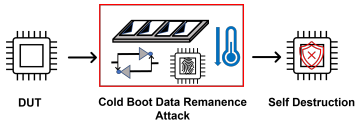



**Figure 2: (left) Cold boot data remanence attack by bringing the memories to freezing cold temperatures before powering off; (right) Desired self-destruction of on-chip data.**

**Cache** In case of cold boot attacks on cache, CPU runs some software of interest, sensitive data is stored in cache; power is suddenly cut off, and immediately afterward, system is booted up with an ad-hoc fake program making a backup copy of memory in DRAM. The attack effect can also be boosted by power or EM radiation [17].
**Scan Chain** Also, for test consideration, a register containing a key or other asset may be a part of a scan chain and hence, its contents may be scanned out via cold boot attack [27].
**RAM** Cold boot attacks often may target RAM; in that case, even full disk encryption schemes with a trusted platform module (TPM) installed are ineffective against this attack.

In all cases, cooling the temperature causes the data remanence effect in memory while it is supposed to erase away. The attacker can use a specialized tool or software to extract the volatile memory contents in power-rebooting conditions, effectively copying the data stored in the memory and/or register file. The attacker can then analyze data to retrieve sensitive information like encryption keys, passwords, or other confidential data in memory. Thus, it is crucial to have a comprehensive, reliable sense-and-response solution that can *detect the necessary step of attack, lowering the temperature in freezing conditions* and can *destroy the data* as a defensive mechanism shown in Fig. 2.

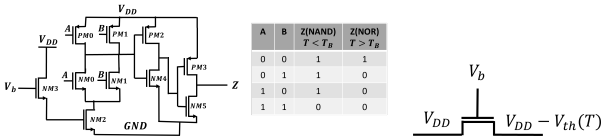
## 4 PROPOSED POLYMORPHIC DESIGN

In this paper, we design a self-destructive, temperature-controlled polymorphic latch and extend it to a polymorphic register to protect sensitive data from data remanence attacks whereby data is instantaneously erased based on a user-specified temperature condition.
**Conceptual Overview** The key principle for the design of our polymorphic gates is the NMOS transistor threshold effect due to temperature. An NMOS transistor with its drain connected to the supply voltage and the gate connected to a gate voltage $V_b$ passes a degraded signal; thereby, the voltage at the source is dropped by its threshold voltage controlled by temperature. The relationship of threshold voltage with temperature can be described using the following equation [13]:

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

Here, in Equation (1), an expression for threshold voltage thermal co-efficient is given where $V_{th}$ is the threshold voltage, $T$ is temperature, $\Phi_{ms}$ is polysilicon-silicon work function, $\Phi_F$ is Fermi potential, $t_{OX}$ is gate oxide thickness, $\varepsilon$ 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 slope of the threshold voltage thermal co-efficient is negative, which means threshold voltage decreases as temperature increases. The source voltage also depends on the gate voltage according to the Equation (2):

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




| A | B | Z(NAND) $T < T_B$ | Z(NOR) $T > T_B$ |
|---|---|---|---|
| 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 |

(a) (b)

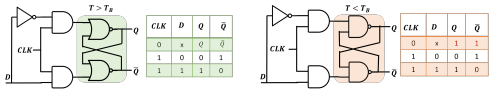
**Figure 3: (a) Polymorphic NOR/NAND gate functioning as NOR for $T$ greater than $T_B$, and as NAND for $T$ less than $T_B$. $V_b$ is applied voltage controlling temperature threshold $T_B$. (b)NFET threshold effect due to temperature. $V_b$ is the variable gate voltage, which can be adjusted depending on the desired temperature threshold in our polymorphic gates.**

Here, $V_S$ is the source voltage, drain voltage is the supply voltage, $V_{DD}$, $I_D$ is the current through the transistor, $\mu_n$ is the electron mobility, $C_{OX}$ is the oxide capacitance, $W$ and $L$ are width and length of the transistor. The current $I_D$ is a function of gate voltage which is also 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 $V_S$, thus increasing temperature threshold for polymorphism $T_B$.

Figure 3 (b) illustrates the NMOS transistor threshold effect considering constant gate voltage $V_b$. At fixed $V_b$, low threshold voltage at high temperature causes degradation at source voltage; however, this degradation does not impede circuit operation- driving another NMOS transistor to be completely turned on and working as a pass transistor. However, if temperature is at freezing level,i.e., lower than threshold, $T_B$, resulting high threshold voltage causes the gating transistor to be partially on. $V_b$ can be altered to choose suitable $T_B$ for any specific application. This principle can be used to select function of polymorphic gate. At high temperatures above $T_B$, the low threshold drop causes the pull-down network to be active, selecting the built-in functionality, whereas at low temperatures below $T_B$, the high threshold drop forces the pull-down portion to be significantly weakened, causing the function to be changed.

**Multi-Threshold Null Convention Logic** The polymorphic circuits also use multi-threshold null convention logic (MTNCL). 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 [29]. 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 [2]. Nevertheless, proposed polymorphic latch protects data by self-destruction in both synchronous and asynchronous circuits.

**Gate Biasing Effect**Any temperature-sensitive polymorphic circuit can be designed using the above design principles and gate biasing effect. As an example, we have constructed an NCL-based polymorphic NOR-NAND gate. The pull-up network for the polymorphic gate in Fig. 3. Gate biasing effect of the transistor $NM3$ is used to control the threshold for polymorphism. The drain voltage of $NM3$ is fixed at supply voltage and gate voltage is fixed at a biasing voltage. Thus the gate biasing and threshold voltage drop is




| CLK | D | Q | $\bar{Q}$ |
|---|---|---|---|
| 0 | x | Q | $\bar{Q}$ |
| 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 |

| CLK | D | Q | $\bar{Q}$ |
|---|---|---|---|
| 0 | x | 1 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 |

(a) (b)

**Figure 4: Polymorphic NOR/NAND D-latch and truth tables for (a) normal operation and (b) temperature freezing condition. When $T$ is lowered below freezing temperature, $T_B$, the polymorphic gates change from NOR behavior (green) to NAND (orange) and the latch enters the forbidden state (red).**

dependent on temperature. Under normal operating temperatures, the threshold voltage drop of $NM3$ is low enough to turn on $NM2$ allowing the PDN to dominate so that the polymorphic gate behaves like NOR gate. Under freezing temperatures, the threshold drop increases enough to turn off the transistor $NM2$ disconnecting the pull-down network, thus, the polymorphic gate behaves like NAND gate. When the polymorphic gate changes to NAND behavior, the polymorphic latch enters forbidden state destroying the data.

## 4.1 Polymorphic Latch and Register Design

**Polymorphic Latch** The polymorphic nature of latch is derived from the behavior of a latch constructed with NOR gates versus that of a latch constructed with NAND gates. A normal NOR-based D-latch, shown in Figure 4(a), operates with the ability to hold data when the clock signal ($CLK$) is low (0). On the other hand, when the clock is high (1), it will set (reset) $Q$ if $D = 1$ ($D = 0$). However, if the same latch is constructed with NAND gates, the latch enters a forbidden state when $CLK$ is 0. This is illustrated by the red row in the truth table of Figure 4(b). Regardless of $D$, the outputs $Q$ and $\overline{Q}$ both output a logic 1, due to the NAND gates both having a low input when $CLK = 0$. This state, with $Q$ and $\overline{Q}$ equal, does not represent valid data and effectively destroys any previous data contained in latch. Depending on the temperature, this polymorphic latch behavior can be controlled. By constructing a latch with polymorphic NOR/NAND gates, the latch can function normally at room temperature where the polymorphic gate operates as a NOR gate. But enters a forbidden state when the temperature goes to freezing temperature, operating as a polymorphic NAND gate. Since lowering the temperature is a prerequisite of the cold boot data remanence attack explained in Section 3, our proposed latch can effectively destroy data when the temperature drops below the threshold $T_b$ set by a designer. *It is to be noted that, during cold boot attack, the system clock is not typically frozen and CLK will be low eventually and latched data will be destroyed. If the attacker also freezes the system clock to facilitate data recovery, an additional polymorphic gate can be implemented that forces the system clock to logic low under attack conditions similar to [3].*

**Polymorphic Register** The extension of the polymorphic latch design to a register is formed by two polymorphic latches connected in series. The clock is inverted and fed to the second (slave) latch of the register. All the four NOR gates used in the register are replaced with polymorphic NOR-NAND gates as nature as shown in Fig. 3. Similar to the latch, the polymorphic register operates as usual through NOR behavior of the polymorphic NOR-NAND gates under normal operating temperatures and enters forbidden state through NAND behavior of the polymorphic NOR-NAND gates used in the register. To be more specific, either first (master) latch

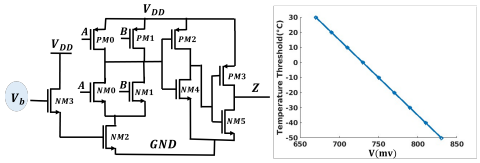
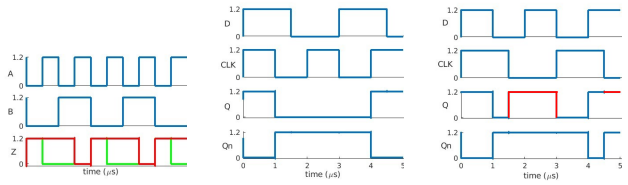



**Figure 5: Polymorphic temperature threshold as a function of gate biasing voltage $V_b$.**




(a) (b) (c)

**Figure 6: Simulation results of (a) polymorphic NOR/NAND gate: (green), at $0^0$C, output signal ($Z$) is true only for the NOR of both input signals ($A$, $B$); (red), at $-40^0$C, output signal ($Z$) is true only for the NAND of both input signals. Polymorphic latch behavior: (b) at $0^0$CC, $D$ is latched to $Q$ and the inverse to $\overline{Q}$ ($Qn$) when $CLK$ is high; (c) at $-40^0$C, $Q$ and $\overline{Q}$ ($Qn$) both enter logical high state when $CLK$ is 0. This is invalid data and shows the latch entering a forbidden state (red).**

or slave latch will be in hold mode where its input $CLK$ or $\overline{CLK}$ is equal to 0. At low temp latch in hold state destroys its data.

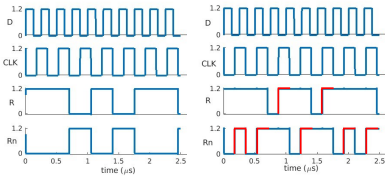
**Adjusting Self-destruction Temperature Threshold:** The temperature threshold at which the NOR-NAND gate changes behavior from NOR to NAND gate can be adjusted by changing the gate voltage $V_b$ of transistor $NM3$ as shown in Fig. 5. As the gate voltage increases the temperature threshold at which polymorphism (destruction) occurs gets lower.

## 5 RESULTS AND DISCUSSION

Cadence Virtuoso ADE simulation environment is used as simulation environment, technology node used is 45nm. Cadence Virtuoso ADE XL simulation is used to perform Monte Carlo analysis for assessing method's reliability.

**NOR/NAND Gate:** The behavior of the NOR-NAND polymorphic gate is shown in Fig. 6(a). When the temperature is at $0^0$C or above, the polymorphic gate behaves as a NOR gate which means output $Z$ is true only for the NOR of inputs $A$ and $B$. In this condition, the operating temperature is above the temperature threshold for polymorphism. At temperature $-40^0$C which is below the polymorphism temperature threshold, the polymorphic gate behaves as a NAND gate which means output $Z$ is true only for the NAND of inputs $A$ and $B$. The temperature of $-40^0$C is chosen as representative temperature of attack for simulation as successful cold boot attack was demonstrated at a temperature of $-50^0$C [7].

**Latch:** The latch behavior containing two NOR-NAND polymorphic gates as shown in Fig. 6. When the temperature is at $0^0$C or above at which the polymorphic gates act as NOR gates, the latch operates normally and data $D$ is latched at output $Q$ and $Q_n$ successfully where $Q_n$ is inverted version of $Q$. At temperature of $-40^0$C which is below the polymorphism temperature threshold, the polymorphic gates behave as NAND gates and the latch enters forbidden state when clock is logic low. Both $Q$ and $Q_n$ enters same




(a) (b)

**Figure 7: Simulation of polymorphic Register behavior: (a) at $0^0$C, $D$ is latched to $R$ and the inverse to $R$, $\overline{R}$ ($Rn$) when $CLK$ is high; (b) at $-40^0$C, $R$ and $\overline{R}$ ($Rn$) both enter logical high state at $CLK$ transition. This is invalid data and shows the register entering a forbidden state (red).**

logic (logic high) when clock goes low signifying that the latch enters forbidden state, i.e., the latched data is destroyed.

**Register:** The register output is shown in Fig. 7 at temperatures $0^0$C and $-40^0$C . At $0^0$C, register is able to store data successfully for all clock transitions. From the waveform, it is evident that the register behaves as a negative edge-triggered flip-flop. At each negative edge of the clock $CLK$, the output $R$ assumes the value of the input $D$. $R_n$ is the inverted version of $R$ as seen from the waveform at $0^0$C. At $-40^0$C, the register output $R$ and its inverted counterpart $R_n$ both enters the similar logic value at clock transitions as seen in the waveform. This is an invalid state, i.e., stored data in the register is destroyed. The output $R$ also switches randomly irrespective of the negative edge of the clock $CLK$. As a result, if attacker tries to carry out cold boot data remanence attack at temperature of about $-40^0$C, randomness in both outputs $R$ and $R_n$ will ensure destruction of sensitive data.

**Power, Performance and Area Overhead:** Layout is performed for both the polymorphic latch and polymorphic register. Parasitic extraction is then performed to extract resistances and capacitance from device nets. Power, performance, and area (PPA) results are then obtained using ADE simulation against extracted design in Cadence Virtuoso. These results are compared to that of a standard NOR-based latch as shown in Table 1.

**Area:** Area is compared by physical dimensions of cell layout.

**CLK2Q and D2Q Delay:** Clock-to-$Q$ and clock-to-$\overline{Q}$ timings are obtained by analyzing the propagation delay from a falling clock edge to valid data being latched to the output. $D$-to-$Q$ and $D$-to-$\overline{Q}$ timings are similarly obtained by measuring the time for data to be latched to the output when the clock is held high and the D input changes. $D$-to-$Q$ timings cannot be extracted for register, as register output only updates with clock transitions.

**Setup and Hold Time** is measured by determining the earliest that data can arrive relative to a falling clock edge and still be propagated to $Q$ within 5% of nominal delay. In the case of the latches, this nominal delay is the $D$-to-$Q$ delay. In the case of the register, this nominal delay is the clock-to-$Q$ delay.Hold Time is measured by determining how long data that arrives near the minimum setup time must be held after the falling clock edge to be properly latched.

**Power:** Power measurements are collected by running transient simulations up to 10 μs, with the latches and register alternating between states in which new data is clocked and states in which no input transitions are activated. Minimum static power refers to the minimum measured power consumption during this simulation.

**Table 1: Power, performance, and area (PPA) comparison.**

| Parameters | NOR Latch | Polymorphic Latch | Polymorphic Register |
|---|---|---|---|
| Area | 7.8 $\mu m^2$ | 34.1 $\mu m^2$ | 66.1 $\mu m^2$ |
| $CLK2Q$ delay (rise/fall) | 170 ps / 95 ps | 315 ps / 248 ps | 402 ps / 327 ps |
| $CLK2\overline{Q}$ delay (rise/fall) | 177 ps / 90 ps | 321 ps / 241 ps | 420 ps / 310 ps |
| $D2Q$ delay (rise/fall) | 171 ps / 117 ps | 335 ps / 261 ps | N/A |
| $D2\overline{Q}$ delay (rise/fall) | 200 ps / 95 ps | 333 ps / 252 ps | N/A |
| Setup Time | 79 ps | 162 ps | 298 ps |
| Hold Time | 4 ps | 19 ps | -83 ps |
| Minimum Static Power | 32 pW | 105 pW | 59 uW |
| Average Power | 904 nW | 33 uW | 61 uW |
| Peak Power | 73 uW | 174 uW | 246 uW |

**Table 2: Reliability analysis with Monte Carlo simulation.**

| Temp. | NOR Latch | Polymorphic Latch | Polymorphic Register |
|---|---|---|---|
| $-40^0$C | 100% data retention | 99% data erasure | 79.75% data erasure, 9.5% data flipped |
| $27^0$C | 100% data retention | 97.5% data retention | 98.25% data retention |

Average power refers to the power consumption when the device experiences switching activity similar to that shown in Figure 6. Peak power consumption is the highest recorded power value observed during switching in simulation. All PPA measurements are simulated under nominal conditions at $27^0$C and 1.2V operation. As discussed previously, the polymorphic temperature is chosen to be $-40^0$C. To implement this, the bias voltage is set to 795mV. *Note that although overhead of polymorphic latch and register are high, they need only be used to replace latches and registers in design which are expected to carry sensitive assets.*

**Effects of Process Variation:** Monte Carlo simulation with 400 simulation points is performed to analyze the effects of process variation and transistor mismatch on the reliability of the latch and register. The passing condition is retention of previously latched data at the end of transient simulation. Results are illustrated in Table 2. Monte Carlo simulation is performed for two temperature points:−40, and $27^0$C.

## 6 RELATED WORK

In case of cold boot attacks, sensitive data stored in DRAM, SRAM or Register encryption key stored in memory is divulged to attacker. In an attempt to keep the encryption keys out of RAM, countermeasures such as TRESOR [14], Loop-Amnesia [21] use register-based key storage. However, an attacker can attack those registers as well where the proposed polymorphic register can now ensure security. Cache instead of DRAM or SRAM can also be used [6] to store encryption keys. Hardware and software based full memory encryption can be employed to protect against cold boot attacks but comes with complexity and performance overhead. Also test and debug become troublesome. Moreover, full memory encryption key kept in tamper-resistant hardware can also be hacked into as shown in [10]. Another countermeasure can be secure erasure of memory or secure writing of random data on memory on power-interruption such as power-off [12]. Unfortunately, such countermeasures are operating system (OS) specific. For DRAM, they can also be circumvented by attacker by removing the memory from motherboard and placing it in another motherboard prepared for attack. The data remanence timekeepers TARDIS and cusTARD presented in [9] can be used as remanence detectors and separate response mechanisms can be designed to protect SRAM from cold boot attack. Compared to aforementioned countermeasures, our one requires smaller PPA overhead with integrated sense and response mechanism.

## 7 CONCLUSION AND FUTURE WORK

In this work, we have proposed polymorphic latch and register designs that destroy data when the chip is intentionally chilled, such as in cold boot data remanence attacks. Our countermeasure does not require any extra fabrication steps and can destroy data upon attack within a few nanoseconds. The incorporation of detection and response mechanisms in the same memory element makes this countermeasure versatile and makes it difficult for the attacker to remove without disturbing the functionality of memory elements in the chip. Similar to latches and registers, in the future, we plan to extend our countermeasure to SRAM memory by developing and incorporating polymorphic inverters using the same methodology. We also plan to mitigate the effect of process variation on the design by introducing a calibration mechanism.

## REFERENCES

[1] et al. Anagnostopoulos. [n. d.]. Low-temperature data remanence attacks against intrinsic SRAM PUFs. In *2018 21st Euromicro Conference on Digital System Design.*
[2] et al. Bernard. [n. d.]. Design of Asynchronous Polymorphic Logic Gates for Hardware Security. In *IEEE High Performance Extreme Computing Conference.*
[3] Cannon. [n. d.]. Protection Against Physical Attacks Through Self-Destructive Polymorphic Latch. In *IEEE/ACM 2023 ICCAD.*
[4] et al. Claes. [n. d.]. Comparison of SRAM and FF PUF in 65nm technology. In *Information Security Technology for Applications.*
[5] et al. Eiroa. [n. d.]. Reducing bit flipping problems in SRAM physical unclonable functions for chip identification. In *2012 19th IEEE International Conference on Electronics, Circuits, and Systems.*
[6] et al. Guan. [n. d.]. Copker: A Cryptographic Engine Against Cold-Boot Attacks. *IEEE Transactions on Dependable and Secure Computing* ([n. d.]).
[7] et al. Halderman. 2009. Lest we remember: cold-boot attacks on encryption keys. *Commun. ACM* (2009).
[8] et al. Helfmeier. [n. d.]. Breaking and entering through the silicon. In *Proceedings of the 2013 ACM SIGSAC.*
[9] et al. Hester. [n. d.]. Persistent clocks for batteryless sensing devices. *ACM Transactions on Embedded Computing Systems* ([n. d.]).
[10] Andrew Huang. [n. d.]. Keeping Secrets in Hardware: The Microsoft Xbox™ Case Study. In *Workshop on Cryptographic Hardware and Embedded Systems.*
[11] et al. Kai. [n. d.]. Security strategy of powered-off SRAM for resisting physical attack to data remanence. *Journal of Semiconductors* ([n. d.]).
[12] ST Microelectronics. [n. d.]. Protection against cold boot attacks. https://tails.net/doc/advancedtopics/coldbootattacks/index.en.html.
[13] ST Microelectronics. 2006. Design of asynchronous. https://www.st.com/resource/en/application_note/.
[14] et al. Müller. [n. d.]. TRESOR Runs Encryption Securely Outside RAM. In *USENIX.*
[15] et al. Müller. 2012. Forensic Recovery of Scrambled Telephones. (2012).
[16] et al. Nagata. [n. d.]. On-chip physical attack protection circuits for hardware security. In *2019 IEEE Custom Integrated Circuits Conference.*
[17] et al. Neagu. [n. d.]. Defending cache memory against cold-boot attacks boosted by power or EM radiation analysis. *Microelectronics Journal* ([n. d.]).
[18] et al. Nedospasov. [n. d.]. Invasive PUF analysis. In *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography.*
[19] et al. Nevoral. [n. d.]. CMOS gates with second function. In *2018 IEEE Computer Society Annual Symposium on VLSI.*
[20] et al. Pan. 2018. Nvcool: When non-volatile caches meet cold boot attacks. In *2018 IEEE 36th International Conference on Computer Design.*
[21] Patrick Simmons. [n. d.]. Security through amnesia: a software-based solution to the cold boot attack on disk encryption. In *Asia-Pacific Computer Systems.*
[22] Sergei Skorobogatov. 2002. *Low temperature data remanence in static RAM.* Technical Report.
[23] et al. Srivastava. [n. d.]. An efficient memory zeroization technique under side-channel attacks. In *2019 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems.*
[24] et al. Stoica. [n. d.]. Polymorphic electronics. In *Evolvable Systems: From Biology to Hardware: 4th International Conference, ICES.*
[25] et al. Tada. [n. d.]. Design and concept proof of an inductive impulse self-destructor in sense-and-react countermeasure against physical attacks. *Japanese Journal of Applied Physics* ([n. d.]).
[26] et al. Wang. [n. d.]. Probing attacks on integrated circuits: Challenges and research opportunities. *IEEE Design & Test* ([n. d.]).
[27] et al. Wu. [n. d.]. A dynamic-key secure scan structure against scan-based side channel and memory cold boot attacks. In *2018 IEEE 27th Asian Test Symposium.*
[28] et al. Zhang. [n. d.]. Optimizating emerging nonvolatile memories for dual-mode applications: Data storage and key generator. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* ([n. d.]).
[29] et al. Zhou. [n. d.]. MTNCL: An Ultra-Low Power Asynchronous Circuit Design Methodology. In *Journal of Low Power Electronics and Applications.*