CamSkyGate: Camouflaged Skyrmion Gates for Protecting ICs

Yuqiao Zhang, Chunli Tang, Peng Li and Ujjwal Guin
Department of Electrical and Computer Engineering
Auburn University, Auburn, Alabama, USA
{yuqiao.zhang,ctz0036,pzl0047,ujjwal.guin}@auburn.edu

ABSTRACT

Magnetic skyrmion has the potential to become one of the candidates for emerging technologies due to its ultra-high integration density and ultra-low energy. Skyrmion is a magnetic pattern created by transverse current injection in the ferromagnetic (FM) layer. A skyrmion can be generated by localized spin-polarized current and behaves like a stable pseudoparticle. Different logic gates have been proposed, where the presence or absence of a single skyrmion is represented as binary logic 1 or logic 0, respectively. In this paper, we propose novel camouflaged logic gate designs to prevent an adversary from extracting the original netlist. The proposal uses differential doping to block the propagation of the skyrmions to realize the camouflaged gates. To the best of our knowledge, we are the first to propose camouflaged skyrmion gates to prevent an adversary from performing reverse engineering. We demonstrate the functionality of different camouflaged gates using the **mumax^3** micromagnetic simulator. We have also evaluated the security of the proposed camouflaged designs using SAT attacks. We show that the same security from the traditional CMOS-based camouflaged circuits can be retained.

CCS CONCEPTS

• **Hardware** → **Spintronics and magnetic technologies**; • **Security and privacy** → **Hardware attacks and countermeasures**; **Hardware attacks and countermeasures**.

KEYWORDS

Skyrmion-based logic, IC camouflaging, reverse engineering, VCMA effect, doping, SAT-based attack.

ACM Reference Format:
Yuqiao Zhang, Chunli Tang, Peng Li and Ujjwal Guin . 2022. CamSkyGate: Camouflaged Skyrmion Gates for Protecting ICs. In *Proceedings of Design Automation Conference (DAC'22).* ACM, San Francisco, CA, USA, 6 pages. https://doi.org/10.1145/3489517.3530528

1 INTRODUCTION

Integrated circuits (IC) with CMOS technology are approaching the limit of quantum-mechanical boundaries with increased power dissipation and process variation [6]. With the urgent requirement for developing an alternative solution, spintronic devices offer a feasible choice for post-Moore devices, and magnetic skyrmion offers an ideal platform for implementing various designs [9]. Over the past years, different types of skyrmion-based logic gates have been proposed. The effects of skyrmion movement such as skyrmion Hall effect [15, 35], skyrmion-edge repulsion [13], and spin-orbit torque-induced motion [14, 34] are exploited to implement logic functions. With the advantages of minimal power consumption and small device size, the skyrmion-based circuit becomes a competitive candidate beyond traditional CMOS technology. However, the security aspects of the skyrmion designs are yet to be explored.

Reverse engineering (RE) of ICs is commonly used in the semiconductor industry to perform failure analysis, defect identification, and verify intellectual property (IP) infringement [29, 30]. Unfortunately, the same RE can be exploited by an adversary to reconstruct the gate-level netlist from a chip [21]. As a result, an adversary can clone an entire chip or pirate the extracted netlist. Note that a cloned chip may also be maliciously modified with a hardware Trojan, which can be exploited while the chip is in the field.

IC camouflaging can be an effective technique to prevent RE so that an adversary cannot extract the inner details of a circuit. In camouflaging, the layout of a gate can be designed in such a way that multiple gates can be mapped to the same layout. Over the years, researchers have proposed different solutions for IC camouflaging. Rajendran et al. [22] proposed camouflaging by creating standard cells with "dummy contact". Erbagci et al. [8] proposed to camouflage a gate based on the utilization of transistors with different threshold voltages. These threshold voltage-defined logic gates are one-time programmed as different functions but with an identical layout. Yasin et al. [33] proposed an IC camouflaging scheme by toggling the output for one minterm of the perturbed function, and a separate camouflaged block is exploited to restore the perturbed minterm. Li et al. demonstrated two camouflaging strategies (low-overhead camouflaging cell generation and AND-tree camouflaging) to realize exponentially increased security levels with a cost of linearly increasing performance overhead [17]. Shakya et al. [24] proposed to add always-on or always-off transistors by doping modification and dummy contacts. As a result, the physical layout of the camouflaged cells is identical to normal logic gates.

Boolean Satisfiability (SAT)-based attack [26] originally proposed to break logic locking [23] can be used to break IC camouflaging very effectively. The attack needs preprocessing of the camouflaged design to convert to a locked design with a secret key. For example, a camouflaged gate, which can be of AND, OR, NAND, or NOR gate, needs to be replaced with four gates and a 4-to-1 multiplexer with two selection inputs. These section inputs are treated as the secret key. An SAT solver will calculate the Distinguishing Input Patterns (DIPs) and help eliminate the wrong keys. When the correct key is recovered, all the multiplexers will be replaced with the

DAC'22, July 10-14 2022, San Francisco, CA, USA

ACM ISBN 978-1-4503-9142-9/22/07…$15.00
https://doi.org/10.1145/3489517.3530528

corresponding logic gate. Thus, a secure camouflaging scheme must be SAT-resilient. The covert gate design proposed in [24] can prevent SAT attacks for CMOS designs. However, no solution has been proposed so far for spintronic devices, such as magnetic skyrmions-based circuits. The contributions of this paper are as follows:

(1) We propose novel **CamSkyGate**, **Cam**ouflaged **Sky**rmion-based logic **Gate**s, for protecting ICs against RE. A camouflaged gate can be configured between AND and OR, and OR and buffer (BUF). A complex camouflaged gate that can be configured between a two-input AND with a dummy input, two-input OR with a dummy input, 2-to-1 MUX, and a BUF with two dummy inputs, are also proposed. We present the layout for these different gates and perform micromagnetic simulations to verify the functionality of these gates. ***To the best of our knowledge, we are the first to propose camouflaged skyrmion logic gates.***
(2) Unlike the CMOS counterparts, the skyrmion-based gates that we propose are non-volatile, compact, and do not require extra components for camouflaging. The camouflaging can be realized by doping selected regions with different magnetic anisotropy.
(3) We evaluate the security of our proposed design against the SAT attack. The experiment results show that our proposed design has a similar security level compared with the existing CMOS-based IC camouflaging scheme [24].

The rest of the paper is organized as follows. Section 2 introduces the background of magnetic skyrmions, VCMA effect, and doping effect on skyrmion movements. Section 3 introduces our proposed CamSkyGate for circuit camouflaging with micromagnetic simulations. Security analysis is carried out in Section 4. Finally, Section 5 concludes the paper.

2 BACKGROUND

Before introducing our proposed designs, we will introduce some basic concepts of background in this section.

2.1 Skyrmion Nucleation and Detection

Skyrmion is a magnetic texture protected by topology and behaves as a stable pseudoparticle. In logic device applications, a nanotrack with heavy metal (HM) and ferromagnetic (FM)/perpendicular magnetic anisotropy (PMA) bilayer is usually used to house a skyrmion. Meanwhile, a magnetic tunnel junction (MTJ) is fabricated on top of the nanotrack for the nucleation of skyrmions [36]. In the nucleation process, a local spin-polarized current follows through MTJ and flips part of the magnetization in the PMA layer, which can form a skyrmion if adequate Dzyaloshinskii–Moriya Interaction (DMI) is present in the nanotrack [16, 18]. The skyrmion detection can also be realized through a readout MTJ. The tunneling magnetoresistance (TMR) can be dictated by the skyrmion appearance. The presence (absence) of skyrmion underneath the MTJ corresponds to a high (low) TMR value, which can represent logic 1 and logic 0, respectively [1]. The output signal can cascade directly to the gate inputs, and be synchronized through VCMA (see Section 2.3).

2.2 Skyrmion Movement

Skyrmion moves through a structure called nanotrack, made of an FM layer and an HM layer [5]. The HM layer has a sidewall-like structure that wraps the FM layer at the bottom and on two sides. The skyrmion stays at the FM/HM interface. The sidewall wrapping structure eliminates the transverse motion of the skyrmion caused by the skyrmion Hall effect, allowing only linear motion. In order to drive the skyrmion in the nanotrack, a continuous electric current J is required in the HM layer. Due to the spin Hall effect, J generates a spin current J_s in the FM layer. At the FM/HM interface, the spin current applies a spin-orbit torque on the skyrmion, driving it along the y-axis, while the Hall effect tends to move the skyrmion transversely along the x-axis. The dynamics of a skyrmion is governed by the Landau–Lifshitz– Gilbert–Slonczewski (LLG) equation:

$$\frac{dm}{dt} = -|\gamma| m \times H_{eff} + \alpha (m \times \frac{dm}{dt}) + \tau_{SOT} \tag{1}$$

where m is the normalized magnetization M/M_s. M stands for magnetization, M_s is the saturation magnetization and H_{eff} is the effective magnetic field associated with magnetocrystalline anisotropic energy and the DMI energy. Further, γ is gyromagnetic ratio, α is damping coefficient, and τ_{SOT} represents the spin-orbit torque determined by multiple parts: a gyromagnetic ratio, effective field spin polarization rate, permeability of vacuum, driving current density, and the thickness of magnetic film.

The skyrmion inside nanotrack is driven by a current flowing in the HM layer via spin orbit torque (SOT). The forces on the micromagnetic skyrmion can be modeled by Thiele equation [28]:

$$G \times v - \alpha D + F_{SOT} - \nabla V = 0 \tag{2}$$

The first term describes the Magnus force, which G presents the gyromagnetic coupling vector, and v is the skyrmion velocity. Dissipative force is represented by multiplication of damping coefficient α and the dissipative tensor D. The third term represents the driving force F_{SOT} generated by the spin Hall effect. The last term shows the resultant force on the skyrmion, and V presents the confining potential due to boundaries, process impurities, and other textures.

2.3 VCMA Effect

Skyrmion synchronization is a critical requirement when considering the functionality of a scalable skyrmion system. As the skyrmion gates work based on the skyrmion-skyrmion interaction, it is necessary that different skyrmions arrive at the inputs at the same time. In other words, the skyrmions need to be held at the inputs of the gates. The authors in [31] proposed a Voltage-Controlled Magnetic Anisotropy (VCMA) based synchronizer at the input of the gate so that skyrmions cannot enter inside the nanotrack. A clock notch [37, 38] can also be placed instead of a VCMA to synchronize the skyrmion movement. We adopt this VCMA to control the skyrmion movement as it provides better controllability.

To vary the uniaxial anisotropy of a magnetic material, the VCMA technique can be exploited by providing an applied electric field. Once a voltage is applied to cross the ferromagnetic nanotrack, the electron density will be changed which will change the perpendicular magnetic anisotropy in turn. It is noticed that the changed anisotropy is predominantly linear to the applied voltage, and the equation can be concluded as follows:

$$K_{\mu v} = K_{\mu} + \zeta E_b \tag{3}$$

where $K_{\mu v}$ is the resultant anisotropy in the affected region, and K_{μ} presents the value of original anistropy. The electric field is present by E_b, and ζ is the coefficient of the VCMA effect. When enough positive voltage is given, the skyrmions will be stopped at the affected region. When no electrical field is applied, the skyrmions will move in the nanotrack normally.

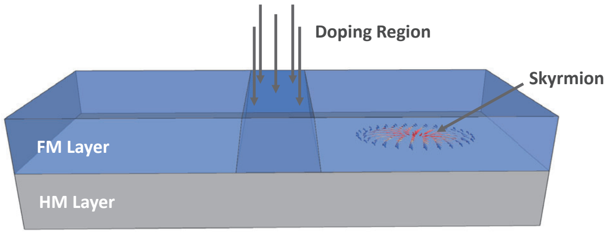

Figure 1: An abstract view of doping process at the FM layer.

2.4 Doping Effect

Selective doping can be used to modulate magnetic anisotropy in a local area in magnetic thin films. When the magnetic anisotropy is significantly different from the rest of the thin film, the skyrmion propagation can be blocked. A common method to realize selective doping is ion implantation [3, 12, 18, 19]. It emits an energetic ion beam to dope foreign ions (e.g., Ga^+ or Ar^+) to a magnetic thin film. Thus, it is vastly used to modulate the anisotropy of magnetic thin films. In the past, it has facilitated the fabrication of bit patterned media for magnetic recording, and fabrication of nanomagnetic logic systems [3, 11]. In the devices we have proposed in this article, ion implantation is a viable technique to realize doping in a local region to control skyrmion propagation, which is shown in Figure 1. Note that doping is a non-reversible process and will modify the magnetic anisotropy permanently. However, the magnetic anisotropy in the VCMA region can be tuned by applying a different voltage.

2.5 Simulation Parameters

The micro-magnetic simulations are performed using **mumax^3** tool, which is a GPU-based accelerated program that can analyze the dynamic behavior of skyrmions. The movement of a skyrmion in the track is modeled based on Equation 2 where the electrical current in the HM layer drives the skyrmion. Parameters used in simulation are: Gilbert damping factor $\alpha = 0.3$, non adiabatic STT factor $\beta = 0.1$, exchange stiffness $A_{\text{ex}} = 1.5 \times 10^{-13}$ J/m, perpendicular magnetic anisotropy $K_{\text{u}} = 6 \times 10^5$ J/m^3, saturation magnetization $M_{\text{s}} = 5.8 \times 10^5$ A/m, and DMI constant $D = 3 \times 10^3$ J/m^2. Mesh sizes are 1 nm × 1 nm × 0.4 nm, along X, Y, and Z axes. In our proposed CamSkyGate designs, we create differential doped regions, where the heavily doped region blocks the propagation of a skyrmion, and the lightly doped region does not affect the skyrmion movement (see the details in Section 3). We simulate the heavily doped region with parameter $1.2 \times K_{\text{u}}$ and lightly doped region with $1.1 \times K_{\text{u}}$. The study from Se Young Park et al. [20] showed the modulation of magnetic anisotropy by the changing of chemical potential. Therefore, the K_{u} can be modulated using the doping method. The choice of these parameters allows the realization of the camouflaged gate.

3 PROPOSED CAMSKYGATE DESIGN

This section introduces the designs for our proposed camouflaged gates. As IC camouflaging aims to protect threats from reverse engineering, we start describing this section with the adversarial model.

3.1 Adversarial Model

The secure logic camouflaging relies upon the fact that an adversary cannot determine the actual gate-level netlist from the camouflaged design. In the attack model, we treat the foundry as trusted, and no attack is to be performed at the manufacturing site like prior camouflaging schemes. The adversary can be any entity other than the foundry that has the capability of performing RE.

- Camouflaged gate-level netlist reconstruction: The adversary can acquire a working chip from the market and has the capability to obtain Scanning Electron Microscopy (SEM) images by delayering the chip. The camouflaged netlist can be constructed from these SEM images.
- Internal scan access: The adversary has access to the scan design so that it can perform SAT attack [26]. One can also assume that the adversary can not access the internal scan chains and launch a sequential SAT attack. However, if we show the camouflaged design is secure against SAT, then automatically, it will be secure against sequential SAT attacks. As a result, we assume that the adversary has scan access.

3.2 CamSkyGate Design Principles

The camouflaged skyrmion gates operate based on the skyrmion-skyrmion interaction, similar to the traditional skyrmion gates. The additional modification that leads to the camouflaging is from different doping regions that look the same as the other regions. This section introduces the primary design principles to build a CamSkyGate.

(1) *Skyrmion Motion Control:* The skyrmion motion can be controlled by applying doping at different regions of the nanotrack. The perpendicular magnetic anisotropy of the doping region can be changed so that it affects the motion of the skyrmions. The doping region blocks the skyrmion to move into the annihilation region of the nanotrack.

(2) *Topological Indistinguishability*: The CamSkyGate uses the selective differential doping technique to implement different logic functions from the same layout. While doping has a strong influence on the skyrmion propagation, SEM cannot distinguish regions with different doping concentrations if they are designed properly, as demonstrated by Frank et al. [10]. The results showed that regions with different doping levels with selected doping concentrations have little effect on the contrast of the SEM images. Thus, the different doping regions of CamSkyGate cannot be identified by performing RE and only identical layouts will be recovered.

(3) *Annihilation of Redundant Skyrmions*: The layout of camouflaged gates is designed in such a way so that more than two gate functionalities can be obtained simultaneously. For example, the AND and OR gates can use the same layout depending on the doping regions (see Figure 2). It is thus necessary to annihilate one or more skyrmions from the nanotrack; otherwise, multiple skyrmions will arrive at the gate output.

In the following, we will present different simple and complex designs of CamSkyGates.

3.3 Simple camouflaged gates

Figure 2 shows two simple camouflaged cell designs with two inputs (X_1 and X_2) and one output (Y). Figure 2.a shows the layout of a camouflaged cell to implement AND and OR functions. Two VCMA regions at the input of the gate are placed to synchronize the motion of the skyrmions at each nanotrack. Two doping regions, denoted as A and B, highlighted in black and white stripes, are selected for

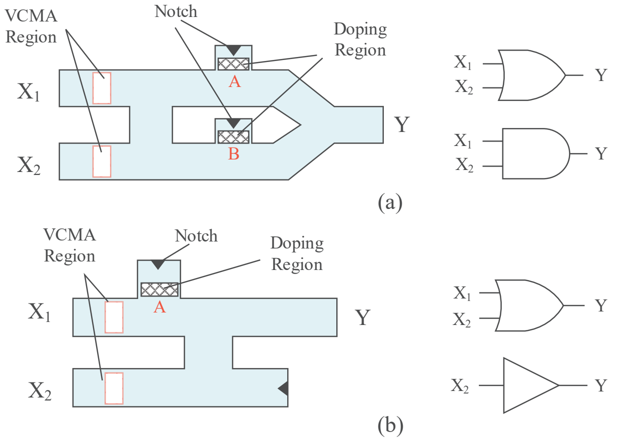

Figure 2: Simple camouflaged skyrmion gates. (a) AND and OR CamSkyGate. (b) OR and BUF CamSkyGate.

doping to determine the function of the cell. When region A is heavily doped with gallium (Ga$^+$) ions, its magnetic anisotropy changes, thus, region A can block a skyrmion from entering the notch region in the top nanotrack. Region B will be lightly doped. The layout will result in the OR function. When region B is heavily doped with gallium ions, it will prevent the skyrmion on the bottom track to enter the annihilation region, and region A will be lightly doped. At this point, the cell will behave as an AND gate. We propose to use differential doping to make the two regions same under SEM images [10]. One region is heavily doped to prevent the skyrmion motion and the other region is lightly doped so that it does not impact the skyrmion propagation. The heavily and lightly doped regions result in $1.2 \times K_u$ and $1.1 \times K_u$, respectively. The layouts of these gates are perfectly symmetrical, and it is infeasible for an adversary to determine the functionality using image analysis.

Figure 2.b illustrates the overall structure of the camouflaged cell for an OR gate and a BUF. Unlike the AND/OR CamSkyGate, one doping region is sufficient for determining the OR and BUF functions. When region A is doped to achieve $1.2 \times K_u$, the OR function will be realized as the skyrmion on the upper track cannot enter the annihilation region. In the case the region is lightly doped to obtain $1.1 \times K_u$, the skyrmion on the top nanotrack will pass the doping region and be annihilated at the notch. This makes input X_1 redundant, and it becomes a dummy connection. Due to the absence of a skyrmion at the upper nanotrack, a skyrmion at input X_2 will reach the output Y. As a result, a BUF will be realized.

Figure 3 shows the simulation results of different simple CamSkyGates. We use the GPU-based accelerated **mumax^3** tool to simulate all the gates. Note that logic 1 and logic 0 are realized using the presence and absence of a skyrmion, respectively. The simulations for all the inputs with logic 0 are redundant as there are no skyrmions in any of the nanotracks of a gate. In the figure, the motion trajectory of a specific skyrmion is illustrated by arrows. Figure 3.a and Figure 3.b show the simulation results for OR/AND CamSkyGate with different input combinations. For input $X_1X_2 = 01$, the skyrmion from the lower track moves to the upper track and reaches the output (Figure 3.b) while it gets destroyed at the annihilation region (Figure 3.b). Note that region A (see Figure 2.a) in the upper nanotrack is heavily doped while region B is lightly doped for an OR gate and vice versa for an AND gate, the skyrmion at the upper nanotrack can pass successfully reach to the output for an OR gate while it is destroyed at the annihilation region for an AND gate. Similar analysis can be done for other input combinations. Figures 3.c and 3.d shows the simulation results BUF and OR functions. When region A is lightly doped, the skyrmion on the upper nanotrack moves to the annihilation region and gets destroyed. This results in the input X_1 being redundant, and a BUF is realized. Region A is heavily doped for an OR gate, and no skyrmion can enter into the annihilation region. One can find all the simulation videos for each CamSkyGate with all input combinations in [25].

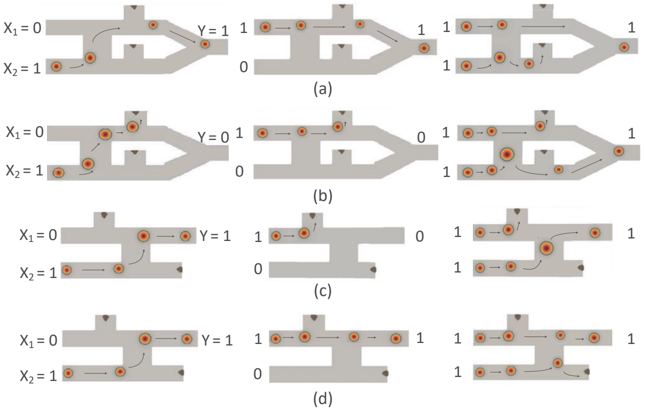

Figure 3: Simulation results for different simple CamSkyGates. (a) OR gate, (b) AND gate, (c) BUF, and (d) OR gate.

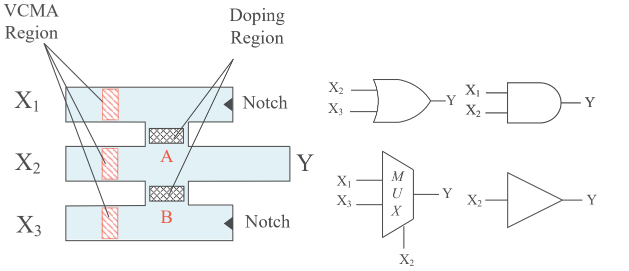

Figure 4: Complex CamSkyGate design with different functions between OR, AND, MUX, and BUF.

3.4 Complex camouflaged gate

Besides the simple CamSkyGate designs with two inputs, we have also proposed a complex CamSkyGate design with multiple inputs and is shown in Figure 4. The layout for a two-input OR gate, two-input AND, 2-to-1 MUX, and a BUF is shown in Figure 4. The doping regions, A and B, are highlighted as black and white stripes like before. Region A is inserted between the upper two nanotracks while B is located between the lower two nanotracks. When A is heavily doped and B is lightly doped, it will block the movement of skyrmions from the lower nanotracks to the upper one. Therefore, X_2 and X_3 will determine the gate functionality, and X_1 becomes the dummy input. If A is lightly doped and B is processed with heavy doping, the lower nanotrack will be blocked and a AND gate can be implemented. X_1 and X_2 are the inputs and determine the functionality while X_3 is the dummy input. When both regions A and B are lightly doped, the skyrmions from all the nanotracks will interact, and a 2-to-1 MUX function will be obtained, where X_2 becomes the selector input and X_1 and X_3 are the inputs. When there

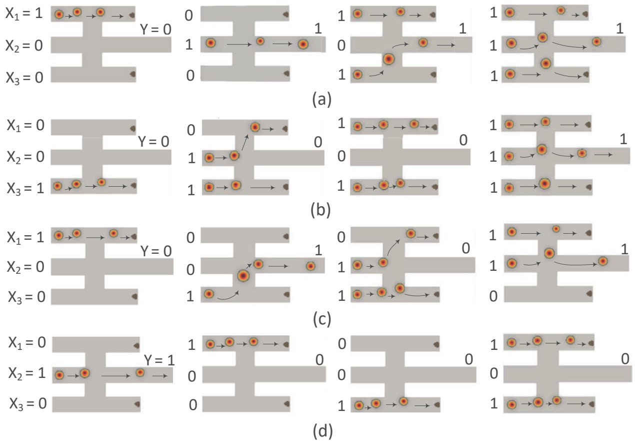

Figure 5: Simulation result examples for different complex gate designs. (a) Two-input OR gate, (b) Two-input AND gate, (c) 2-to-1 MUX, and (d) BUF.

is a skyrmion present at X_2 input (i.e., X_2 is at logic 1), the output Y will be decided by input X_1, otherwise by input X_3. In the case of A and B are all heavily doped, There is no interaction between each nanotrack and the CamSkyGate can realize the function of a simple buffer in which X_2 is the input. Both X_1 and X_3 will be the dummy inputs in this layout of CamSkyGate.

Figure 5 shows the simulation results for the complex CamSkyGate presented in Figure 4 which implements four different functions. Figure 5.a shows the simulation for a two-input OR gate. As X_1 input is a dummy connection, it will have no impact on the gate functionality. The input pattern $X_1X_2X_3 = [100]$ results $Y = 0$ which validates the effect of X_1 on Y. All other combinations $X_2X_3 = [10, 01, 11]$ results $Y = 1$. Figure 5.b shows the simulation for a two-input AND gate with X_3 as a dummy input. We apply $X_3 = 1$ to verify that it has no impact on Y. All three input pattern $X_1X_2 = [00, 01, 10]$ results $Y = 0$ and one input $X_1X_2 = [11]$ makes $Y = 1$ which validates the AND function. The simulations for 2-to-1 MUX are illustrated in Figure 5.c. When the selection input $X_2 = 0$, it selects $Y = X_3$ otherwise, $Y = X_1$. As a result, $Y = 0$ when $X_1X_2X_3 = [100, 011]$ and $Y = 1$ when $X_1X_2X_3 = [001, 110]$. Finally, Figure 5.d shows the simulation for a buffer X_1 and X_3 as dummy inputs. The output $Y1$ becomes logic 1, when input X_2 is logic 1.

4 SECURITY ANALYSIS

This section evaluates the security of our proposed design against the SAT attack [26]. We also provide a detailed comparison with the existing CMOS-based camouflaging to show the effectiveness of our proposed CamSkyGate design for emerging circuit camouflaging.

4.1 SAT-based attack on camouflaged circuits

The SAT attack is an effective way to determine the logic function of a camouflaged gate. An adversary needs to perform reverse engineering to obtain the gate-level netlist. As the logic function of each CamSkyGate is unknown, it needs to convert the camouflaged gate with its key-based equivalent [7]. For example, the simple AND/OR CamSkyGate, shown in Figure 2.a, can be replaced with a MUX where the key bit at the selector input selects one of the two gate combinations. Similarly, the complex CamSkyGate, shown in Figure 4, can be replaced with a MUX, where two key bits at the selector input select one of the four gate combinations. An adversary can reconstruct a key-based netlist from the camouflaged circuit and apply the SAT attack to determine the key. Once the value of the key is determined, he/she can identify all the camouflaged gates and construct the original gate-level netlist.

Since the function of our designed camouflaged skyrmion cell cannot be determined by RE or imaging processing, the attacker needs to replace all the CamSkyGates with the MUX-based selection networks. Table 1 shows the SAT attack resistance evaluation for different circuits using our proposed CamSkyGate camouflaging scheme. Five benchmark circuits from ISCAS'85 [4] and two circuits from EPFL suite [2] are selected to test the effectiveness and listed in Column 1. Column 2 represents the gate count for each benchmark circuit. To perform the SAT attack, we camouflage each benchmark circuit by placing complex CamSkyGate and simple CamSkyGate with a ratio of 1:2 and replacing them with the corresponding MUX structure for performing the SAT attack. Since the complex CamSkyGate requires two selection bits for the selection network while the simple design requires one, the exact key space size is identical for both complex and simple CamSkyGates. We perform the SAT attack using the code provided in [27] and compare the performance with the results provided in [24] (Regular Camouflaging and Covert Gate Camouflaging in Table 1). Timeout for the attack was also set to 12 hours, which is in line with the prior work [24, 27, 32]. For each camouflaging scheme, we have shown the size of the key (Columns 3, 6, and 9), the attack time (Columns 4, 7, and 10), and the number of iterations to launch the attack (Columns 5, 8, and 11). Since the longer key value will lead to higher overall search space for the SAT solver, the run time of the SAT attack will also be increased. In the security evaluation, we determine the unit of run time is in hours which is the same as the unit of covert gate camouflaging evaluation presented in [24], while the evaluation on regular camouflaging provided in [24] is on the scale of seconds. The camouflaging scheme presented here and in [24] can not provide security for the c1908 benchmark circuit due to its small size. The SAT attack becomes ineffective for all the remaining benchmarks (i.e., a timeout that is over 12 hours). As a result, it can be concluded that our proposed CamSkyGate design could provide the same level of security compared with the CMOS-based camouflaging scheme [24], which indicates the feasibility of protecting the IP privacy of the skyrmion-based circuit.

5 CONCLUSION

In this paper, we have proposed several novel skyrmion-based camouflaged gates denoted as CamSkyGate to protect a design from reverse engineering. We use differential doping at the different regions of a camouflaged layout to implement different logic functions. Doping can change the physical parameters and control the skyrmion motion. A lightly doped region lets the skyrmion pass through the nanotrack, whereas the heavily doped region blocks its propagation. Different gate functionality can be obtained in a single layout by placing these heavily and lightly doped regions to control skyrmion-skyrmion interaction. As it is infeasible to distinguish these heavily and lightly doped regions, the functionality of a CamSkyGate cannot be determined using SEM imaging which is commonly used for reverse engineering. The functionality of each

Table 1: Comparison of SAT attack resiliency.

Benchmark	Gate Count	Regular Camouflaging [24]			Covert Gate Camouflaging [24]			Proposed Camouflaging		
		5% of NAND/NOR/XOR			NAND + NOR + AND + OR			AND+OR+MUX+BUF		
		|K|	Attack Time (s)	# iterations	|K|	Attack Time (hrs)	# iterations	|K|	Attack Time (hrs)	# iterations
c1908	880	34	0.55	7	811	3.25	235	756	3.44	217
c2670	1193	26	0.65	11	1514	Timeout	2127	1040	Timeout	430
c3540	1669	28	0.68	11	2088	Timeout	28	1488	Timeout	180
c5315	2307	46	3.58	25	3379	Timeout	24	1774	Timeout	305
c7552	3512	106	4.07	27	4454	Timeout	52	2000	Timeout	87
arbiter	11839	1182	3815	855	23678	Timeout	82	4000	Timeout	3490
voter	13758	1078	Timeout	33	21560	Timeout	51	4000	Timeout	67

CamSkyGate is simulated using the **mumax^3** simulation tool. To further launch the attack and recover the full functionality of the entire circuit, the adversary is required to synthesize the skyrmion-based circuit into a gate-level netlist and construct a MUX-based network for each camouflaged cell. The SAT-based security evaluation shows that our proposed design can provide the same level of protection similar to the traditional CMOS-based camouflaging.

ACKNOWLEDGMENTS

This material is based on research sponsored by Air Force Research Lab (AFRL) under agreement number AF-FA8650-19-1-1707. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of AFRL.

REFERENCES

[1] [n.d.]. Perpendicular reading of single confined magnetic skyrmions. 6 ([n. d.]).

[2] L. Amarú, P. Gaillardon, and G. De Micheli. 2015. The EPFL combinational benchmark suite. In *Proceedings of the International Workshop on Logic & Synthesis (IWLS)*.

[3] S. Breitkreutz, G. Ziemys, I. Eichwald, J. Kiermaier, G. Csaba, W. Porod, D. Schmitt-Landsiedel, and M. Becherer. 2013. Domain wall gate for magnetic logic and memory applications with perpendicular anisotropy. In *IEEE International Electron Devices Meeting*. 22–4.

[4] D. Bryan. 1985. The ISCAS'85 benchmark circuits and netlist format. *North Carolina State University* 25 (1985), 39.

[5] M. Chauwin, X. Hu, F. Garcia-Sanchez, N. Betrabet, A. Paler, C. Moutafis, and J S. Friedman. 2019. Skyrmion logic system for large-scale reversible computation. *Physical Review Applied* 12, 6 (2019), 064053.

[6] T. Chen. 2006. Overcoming research challenges for CMOS scaling: Industry directions. In *International Conference on Solid-State and Integrated Circuit Technology Proceedings*. 4–7.

[7] M. El Massad, S. Garg, and M. V. Tripunitara. 2015. Integrated Circuit (IC) Decamouflaging: Reverse Engineering Camouflaged ICs within Minutes.. In *NDSS*. 1–14.

[8] B. Erbagci, C. Erbagci, N. E. C. Akkaya, and K. Mai. 2016. A secure camouflaged threshold voltage defined logic family. In *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 229–235.

[9] A. Fert, V. Cros, and J. Sampaio. 2013. Skyrmions on the track. *Nature nanotechnology* 8, 3 (2013), 152–156.

[10] L. Frank, M. Hovorka, MM. El-Gomati, I. Müllerová, F. Mika, and E. Mikmeková. 2020. Acquisition of the dopant contrast in semiconductors with slow electrons. *Journal of Electron Spectroscopy and Related Phenomena* 241 (2020), 146836.

[11] N. Gaur, S. Kundu, SN. Piramanayagam, SL. Maurer, HK. Tan, SK. Wong, SE. Steen, H. Yang, and CS. Bhatia. 2013. Lateral displacement induced disorder in L1 0-FePt nanostructures by ion-implantation. *Scientific reports* 3, 1 (2013), 1–7.

[12] M. Gavagnin, H. D. Wanzenboeck, S. Wachter, M. M. Shawrav, A. Persson, K. Gunnarsson, P. Svedlindh, M. Stoger-Pollach, and E. Bertagnolli. 2014. Free-standing magnetic nanopillars for 3D nanomagnet logic. *ACS applied materials & interfaces* 6, 22 (2014), 20254–20260.

[13] J. Iwasaki, M. Mochizuki, and N. Nagaosa. 2013. Current-induced skyrmion dynamics in constricted geometries. *Nature nanotechnology* 8, 10 (2013), 742–747.

[14] W. Jiang, P. Upadhyaya, W. Zhang, G. Yu, M B. Jungfleisch, F. Y Fradin, J. E Pearson, Y. Tserkovnyak, K. L Wang, O. Heinonen, et al. 2015. Blowing magnetic skyrmion bubbles. *Science* 349, 6245 (2015), 283–286.

[15] W. Jiang, X. Zhang, G. Yu, W. Zhang, X. Wang, M B. Jungfleisch, J. E Pearson, X. Cheng, O. Heinonen, K. L Wang, et al. 2017. Direct observation of the skyrmion Hall effect. *Nature Physics* 13, 2 (2017), 162–169.

[16] W. Kang, Y. Huang, X. Zhang, Y. Zhou, and W. Zhao. 2016. Skyrmion-Electronics: An Overview and Outlook. *Proc. IEEE* 104, 10 (2016), 2040–2061.

[17] M. Li, K. Shamsi, T. Meade, Z. Zhao, B. Yu, Y. Jin, and D. Z Pan. 2017. Provably secure camouflaging strategy for IC protection. *IEEE transactions on computer-aided design of integrated circuits and systems* 38, 8 (2017), 1399–1412.

[18] S. Luo and L. You. 2021. Skyrmion devices for memory and logic applications. *APL Materials* 9, 5 (2021), 050901.

[19] J. McCord, I. Mönch, J. Fassbender, A. Gerber, and E. Quandt. 2009. Local setting of magnetic anisotropy in amorphous films by Co ion implantation. *Journal of Physics D: Applied Physics* 42, 5 (2009), 055006.

[20] S. Y. Park, D. S. Kim, Y. Liu, J. Hwang, et al. 2020. Controlling the Magnetic Anisotropy of the van der Waals Ferromagnet Fe3GeTe2 through Hole Doping. *Nano Letters* 20, 1 (2020), 95–100.

[21] S. E Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor. 2016. A survey on chip to system reverse engineering. *ACM journal on emerging technologies in computing systems (JETC)* 13, 1 (2016), 1–34.

[22] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri. 2013. Security analysis of integrated circuit camouflaging. In *Proceedings of the ACM SIGSAC conference on Computer & communications security*. 709–720.

[23] J. A Roy, F. Koushanfar, and I. L Markov. 2010. Ending piracy of integrated circuits. *Computer* 43, 10 (2010), 30–38.

[24] B. Shakya, H. Shen, M. Tehranipoor, and D. Forte. 2019. Covert gates: Protecting integrated circuits with undetectable camouflaging. *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019), 86–118.

[25] CamSkyGate Skyrmion Simulations. 2021. https://github.com/2660039863/CamSkyGate_DAC.

[26] P. Subramanyan, S. Ray, and S. Malik. 2015. Evaluating the security of logic encryption algorithms. In *International Symposium on Hardware Oriented Security and Trust*. 137–143.

[27] P. Subramanyan, S. Ray, and S. Malik. 2015. Evaluating the security of logic encryption algorithms. In *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 137–143.

[28] A.A. Thiele. 1973. Steady-state motion of magnetic domains. *Physical Review Letters* 30, 6 (1973), 230.

[29] R. Torrance and D. James. 2007. Reverse engineering in the semiconductor industry. In *IEEE Custom Integrated Circuits Conference*. 429–436.

[30] R. Torrance and D. James. 2011. The state-of-the-art in semiconductor reverse engineering. In *Proceedings of the Design Automation Conference*. 333–338.

[31] Benjamin W Walker, Can Cui, Felipe Garcia-Sanchez, Jean Anne C Incorvia, Xuan Hu, and Joseph S Friedman. 2021. Skyrmion logic clocked via voltage-controlled magnetic anisotropy. *Applied Physics Letters* 118, 19 (2021), 192404.

[32] Y. Xie and A. Srivastava. 2016. Mitigating SAT attack on logic locking. In *International conference on cryptographic hardware and embedded systems*. 127–146.

[33] M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran. 2016. CamoPerturb: Secure IC camouflaging for minterm protection. In *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. 1–8.

[34] G. Yu, P. Upadhyaya, X. Li, W. Li, S. K. Kim, Y. Fan, K. L Wong, Y. Tserkovnyak, P. K. Amiri, and K. L Wang. 2016. Room-temperature creation and spin–orbit torque manipulation of skyrmions in thin films with engineered asymmetry. *Nano letters* 16, 3 (2016), 1981–1988.

[35] J. Zang, M. Mostovoy, J. H. Han, and N. Nagaosa. 2011. Dynamics of skyrmion crystals in metallic thin films. *Physical review letters* 107, 13 (2011), 136804.

[36] X. Zhang, Y. Zhou, M. Ezawa, G.P. Zhao, and W. Zhao. 2015. Magnetic skyrmion transistor: skyrmion motion in a voltage-gated nanotrack. *Scientific reports* 5, 1 (2015), 1–8.

[37] Z. Zhou, U. Guin, P. Li, and V. D Agrawal. 2021. Defect Characterization and Testing of Skyrmion-Based Logic Circuits. In *VLSI Test Symposium (VTS)*. 1–7.

[38] Z. Zhou, U. Guin, P. Li, and V. D Agrawal. 2022. Fault Modeling and Test Generation for Technology-Specific Defects of Skyrmion Logic Circuits. In *VLSI Test Symposium (VTS)*. 1–7.