# NeuroHammer: Inducing Bit-Flips in Memristive Crossbar Memories

Felix Staudigl*, Hazem Al Indari*, Daniel Schön‡, Dominik Sisejkovic*,
Farhad Merchant*, Jan Moritz Joseph* Vikas Rana† Stephan Menzel‡, Rainer Leupers*
* *Institute for Communication Technologies and Embedded Systems, RWTH Aachen University, Germany*
† *Peter Grünberg Institut (PGI-10) Forschungszentrum Juelich GmbH, Juelich, Germany*
‡ *Peter Grünberg Institut (PGI-7) Forschungszentrum Juelich GmbH, Juelich, Germany*
{staudigl, alindari, sisejkovic, merchantf, joseph, leupers}@ice.rwth-aachen.de
{st.menzel, schoen, v.rana}@fz-juelich.de



***Abstract*—Emerging non-volatile memory (NVM) technologies offer unique advantages in energy efficiency, latency, and features such as computing-in-memory. Consequently, emerging NVM technologies are considered an ideal substrate for computation and storage in future-generation neuromorphic platforms. These technologies need to be evaluated for fundamental reliability and security issues. In this paper, we present *NeuroHammer*, a security threat in ReRAM crossbars caused by thermal crosstalk between memory cells. We demonstrate that bit-flips can be deliberately induced in ReRAM devices in a crossbar by systematically writing adjacent memory cells. A simulation flow is developed to evaluate NeuroHammer and the impact of physical parameters on the effectiveness of the attack. Finally, we discuss the security implications in the context of possible attack scenarios.**

***Index Terms*—ReRAM, memristor, hardware security, thermal crosstalk, reliability, neuromorphic computing**

## I. Introduction

Emerging non-volatile memory (NVM) technologies offer promising features that give them an advantage over classical RAM technologies. These advantages are density, low leakage power, and computing-in-memory (CIM) capabilities [1]. Specifically, CIM capabilities help alleviate the von Neumann bottleneck by significantly reducing data movements [2].

Reliability and disturbance errors in contemporary solid-state storage technologies, like dynamic random access memory (DRAM), have emerged due to a technology push resulting in high memory densities [3], [4]. These disturbance errors can form security vulnerabilities like RowHammer, compromising user information through privilege escalation, as demonstrated in Google's Project Zero [5], or denial of service in clouds [6].

Similar disturbance errors have been reported in phase-change memory, which suffers from thermal crosstalk in technology nodes below $20\,\mathrm{nm}$ [7]. Cai et al. [8] discuss thermal crosstalk in ReRAM structures and their impact on the reliability of neuromorphic systems. These disturbance errors can cause an unintended malfunction in memory cells. The authors in [9] discuss the impact of the filament temperature on the switching kinetics of ReRAM cells. In this paper, we combine the reported thermal crosstalk in dense memristive crossbars with the temperature impact on the switching kinetics to define an attack that intentionally causes malfunctions.

This work was funded by the Federal Ministry of Education and Research (BMBF, Germany) in the project NEUROTEC II (Project Nos. 16ME0398K and 16ME0399).

**Contributions:** We introduce *NeuroHammer*, a security attack on emerging NVMs, which deliberately causes bit-flips. To the best of our knowledge, this paper provides the first investigation of undesired bit-flips in emerging NVMs in the context of a security attack. The major contributions are as follows. (1) A security threat based on disturbance errors in ReRAM structures through thermal crosstalk observed during the writing process of memory cells. (2) A simulation methodology for the characterization of NeuroHammer using state-of-the-art crossbar models. (3) A discussion on NeuroHammer-induced security threats based on the provided characterization.

## II. Background

**RowHammer:** In 2014, Kim et al. [4] reported the impact of disturbance errors on DRAMs. The DRAM memory cell consists of a capacitor connected to a transistor. The capacitor's charge decreases with the scaling down of the DRAM process technology. Consequently, the memory cell is more susceptible to disturbance errors based on electromagnetic inference. The RowHammer attack uses this phenomenon to deliberately flip certain bits in DRAM memories by hammering/reading particular rows. The consciously triggered bit-flips violate a fundamental concept of secure and reliable computing systems: memory isolation, which ensures strict separation of application memory to mitigate malicious changes in its internal state.

**ReRAM**: Redox-based resistive memories (ReRAMs) are an emerging class of non-volatile memories, which store binary information in terms of resistances, i.e., the *low resistive state* (LRS) and the *high resistive state* (HRS). ReRAMs typically consist of a simple metal/insulator/metal structure, enabling a high integration density. Depending on the ionic defect type, one can distinguish between valence change memories (VCM) and electrochemical metallization cells (ECM) [10]. VCM cells rely on the motion of oxygen defects in the insulating oxide material. ECM cells are based on the migration of (typically) Ag or Cu cationic defects, which were injected from the chemically active electrode consisting of Ag or Cu. The most studied ReRAMs are filamentary VCM cells in which oxygen defects form very small conducting filamentary regions. This enables high scalability down to a few nm [11] and fast switching speed down to 50 ps [12] at moderate switching voltages. This fast switching speed is achieved by local Joule heating, which accelerates the ion migration exponentially [13].

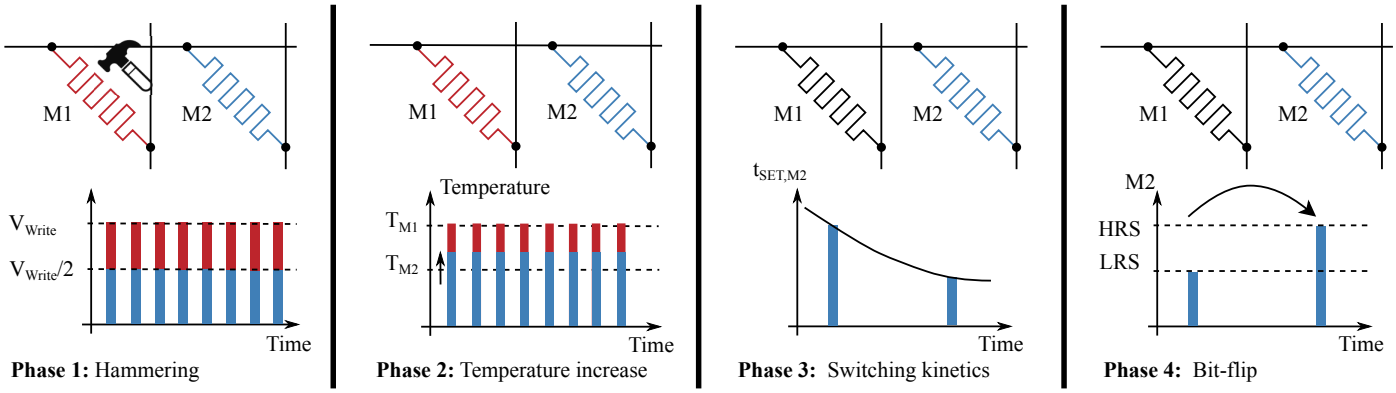



Fig. 1: Working principle of NeuroHammer.

## III. Mechanics of NeuroHammer

Von Witzleben et al. [9] investigated the impact of the temperature on the switching kinetics of redox-based ReRAM cells, concluding that the switching time depends significantly on the temperature of the filament. The proposed attack uses this phenomenon to deliberately induce bit-flips in ReRAM crossbar memories. In the following, we define a *pulse* as a rectangular electrical pulse with a fixed amplitude of $V_{\text{SET}} = 1.05\text{V}$ and a given pulse length. The pulse length is defined by the duration in which the signal is active. The attack is divided into four distinct phases, as illustrated in Fig. 1:

*1) Hammering:* The NeuroHammer attack hammers a single memory cell to trigger a bit-flip. In Fig. 1, the red (blue) cell symbolizes the attacked (target) cell. The red cell should be initially switched to LRS to maximize the resulting current flowing through the cell. The $V/2$ scheme is used to apply constant stress to the blue cell, which equals $V_{\text{SET}}/2$ of the voltage pulse applied to the red cell.

*2) Temperature increase:* The recurring voltage pulses applied on the red cell result in a current through the device, and hence, a temporary temperature increase of the filament. As a result, the temperature of the blue cell increases due to thermal coupling. In addition, the $V/2$ scheme applies a respective voltage pulse ($V_{\text{SET}}/2$) to the blue cell, which simultaneously leads to a temperature increase in the filament.

*3) Switching kinetics:* The increased temperature of the blue cell changes the switching kinetics of the ReRAM device. Consequently, the ReRAM device is more susceptible to pulses, which have either a larger amplitude or a longer pulse length.

*4) Bit-flip:* At this point, the blue cell gradually switches its internal state based on the changed switching kinetics and the constantly applied $V/2$ voltage pulses. These pulses would typically not be sufficient to switch the state of the blue cell. However, considering the thermal coupling effects of dense crossbar structures, the target cell is susceptible to pulses with even lower amplitudes. Eventually, the blue cell switches its internal state and a bit-flip occurs.

## IV. Simulation Methodology

To verify the attack presented in Chapter III, a simulation framework was developed based on the simulator COMSOL Multiphysics [14] and the circuit simulator Cadence Virtuoso [15]. Initially, the crossbar simulation aims to simulate the thermal crosstalk, based on which we extract thermal crosstalk coefficients, which are called *alpha values*. These values serve as input for the circuit simulation to enable the framework to simulate thermal coupling in dense ReRAM crossbar structure.

### A. Crossbar Simulation

Fig. 2b illustrates the basic structure of the simulation model, which consists of a memristive crossbar array of electrodes on a $Si/SiO_2$ substrate. To calculate the temperature of the adjacent cells which surround the target cell, the static heat transfer equation and the current continuity equation are solved for the temperature $T$ and the potential $\phi$, shown in Equation 1 and 2.

$$-\nabla \cdot (\kappa \nabla T) = \mathbf{j} \cdot \mathbf{E} \tag{1}$$

$$\nabla \cdot \mathbf{j} = -\nabla \cdot (\sigma \nabla \phi) = 0 \tag{2}$$

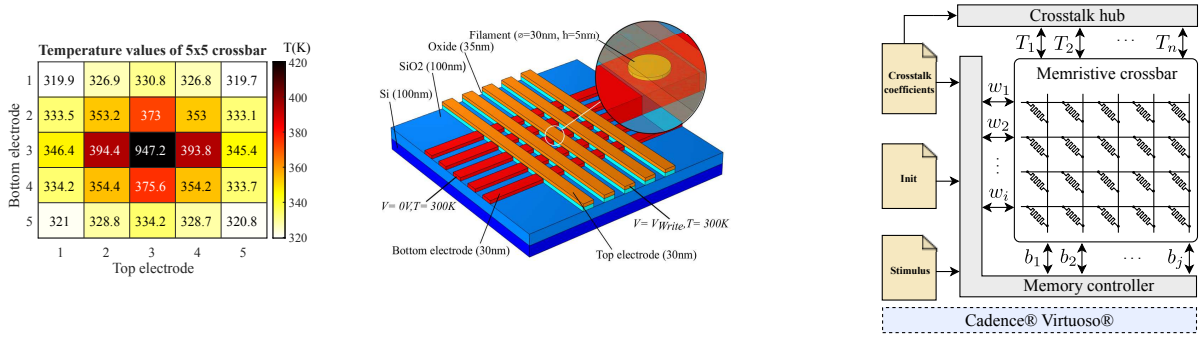
Here, $\kappa$ denotes the thermal conductivity, $\sigma$ the electric conductivity, $\mathbf{j}$ the local current density, and $\mathbf{E}$ the electric field. The electric conductivity and thus also the thermal conductivity (see Wiedemann–Franz law) of the filament is adjusted so that a certain current flows through the device. All other surfaces are thermally and electrically insulated.

To determine the alpha values of a geometry with specific materials for a temperature prediction of the adjacent cells, a variation of the dissipated power in the selected cell is required. Through a voltage sweep of $V_{\text{SET}}$, a temperature matrix which contains the temperature of each cell can be extracted from every simulation (see Fig. 2a). The thermal resistance $R_{\text{th}}$ of the selected cell can then be determined as a fit parameter of a linear regression of the respective temperature $T(P_{\text{LRS}})$ and dissipated power $P_{\text{LRS}} = V_{\text{SET}} \cdot I$ (Equation 3). With further linear regression for every neighboring cell, the alpha values can be determined (Equation 4).

$$T(P_{\text{LRS}}) = T_0 + R_{\text{th}} \cdot P_{\text{LRS}} \tag{3}$$

$$T_{ij}(P_{\text{LRS}}) = T_0 + R_{th} \cdot P_{\text{LRS}} \cdot \alpha_{ij} \tag{4}$$

Here, $T_{ij}(P_{\text{LRS}})$ denotes the temperature of the cell $i, j$ depending on the dissipated power $P_{\text{LRS}}$ and $\alpha_{ij}$, the alpha value of the cell $i, j$.




(a) (b) (c)

Fig. 2: Simulation methodology: (a) the thermal coupling in a 5x5 memristive crossbar, (b) low-level simulation setup and its boundary conditions, and (c) circuit-level simulation setup and its internal components.

### *B. Circuit Simulation*

The circuit-level simulation and its internal modules are illustrated in Fig. 2c. The framework consists of three major parts: memristive crossbar, memory controller, and the crosstalk hub. The platform can be parameterized based on configuration files and the standard graphical user interface (GUI) of the Cadence Virtuoso tool. The remainder of this section describes the modules of the framework in detail.

**Memory controller:** In general, crossbar structures are interfaced over their rows (word lines) and columns (bit lines). The memory controller is responsible for generating and driving the respective pulse for a certain input line of the crossbar. The stimuli file stores the explicit characteristics, i.e. pulse length, duty cycle, and amplitude of each input pulse, while the init file holds the initial state of every ReRAM cell.

**Crosstalk hub:** The hub calculates the temperature increase of a ReRAM cell due to thermal coupling with all surrounding cells. The temperature is calculated based on the alpha values extracted from the crossbar simulation (Section IV-A) and the filament temperatures of the adjacent cells:

$$T_{\text{in}}(\boldsymbol{\alpha}, \mathbf{T}) = \sum_{\substack{0<i<m \\ 0<j<n}} \alpha_{ij} T_{ij,\text{out}}, \tag{5}$$

where $i, j \in \mathbb{N}$ indicate the row and column of the crossbar excluding the attacked cell itself, $m, n \in \mathbb{N}$ indicate the number of rows and columns, and $T_{\text{in}}$ the additional temperature based on the thermal crosstalk.

**Memristive crossbar:** The passive 5x5 memristive crossbar array represents the central part of the simulation framework in which the instantiated memristive devices connect the bit lines to the respective word lines. The JART VCM v1b model employed in this study was developed for filamentary switching VCM cells and fitted to a nanocrossbar Pt/$HfO_2$/$TiO_x$/Ti device [16]–[18]. The dissipated power $P_{\text{d}}$ in the cell increases the local temperature $T$ according to

$$T = R_{\text{th,eff}} \cdot P_d + T_0, \tag{6}$$

where $T_0$ is the ambient temperature and $R_{\text{th,eff}}$ is the effective thermal resistance (in K/W), describing the heat dissipation to the immediate cell surrounding and the thermal properties of the materials. The complete equation system and the used parameters can be found in [17]. It should be noted that the "deterministic" model version is used here.

The original model was adjusted to enable the memristive model to exchange parameters with the simulation framework. Thus, we introduced two interface variables to communicate the temperature values to the crosstalk hub, and receive the additional temperature generated from the adjacent cells.

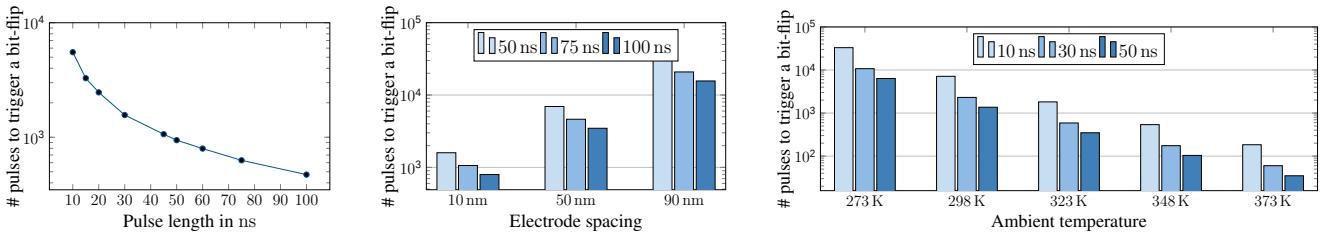
## V. Results

In this section, we verify the proposed NeuroHammer attack and demonstrate the flexibility of our simulation framework. Each experiment uses a simple attack pattern in which we attack the cell in the middle of the crossbar.

**Pulse length:** The simulation uses a crossbar with an electrode spacing of $50\,\text{nm}$, assuming an ambient temperature of $300\,\text{K}$. The controllers select the attacked cell by applying $V$ and $GND$. All remaining inputs are supplied with $V/2$ to minimize the sneak-path currents. Hence, the bit-flip can only occur in the blue cells based on the voltage drop of $V/2$ compared to the remaining cells, which experience no voltage drop. The results show that the number of required pulses to trigger the error decreases with the pulse length (Fig. 3a).

**Electrode spacing:** The second experiment concerns the electrode spacing of the crossbar memory structure. The analysis uses an ambient temperature of $300\,\text{K}$. The spacing of the electrode is defined by the distance between the electrodes of two adjacent cells. Fig. 3b illustrates the simulation results of the electrode spacing ranging from $10\,\text{nm}$ to $90\,\text{nm}$, which indicate that the closer the cells are placed, the more vulnerable they are in terms of disturbance errors. Accordingly, we assume that disturbance errors become a serious problem for dense crossbar memory structures, the more the technology node advances.

**Ambient temperature:** Next, we investigated the effects of the ambient temperature on the occurrence of disturbance errors. Fig. 3c shows the results that use an electrode spacing of $50\,\text{nm}$. The results indicate a strong impact of the ambient temperature on the number of pulses required to trigger a bit-flip.




(a) (b) (c)

Fig. 3: Simulation results of the circuit-level simulation framework: (a) impact of the pulse length, (b) impact of the electrode spacing, (c) impact of the ambient temperature, (d) impact of different attack patterns, and (e-h) overview of attack patterns.

## VI. Security Implications

Several RowHammer-inspired attack scenarios have been presented to threaten both embedded systems and desktop computers. This section illustrates possible attack scenarios in which NeuroHammer can be exploited. Both attacks utilize disturbance errors in dense memory structures, which are deliberately caused by repeatedly hammering certain memory cells. Based on the similarities between both attacks, we briefly describe a common attack scenario using RowHammer to discuss, ultimately, the reuse of attack scenarios for NeuroHammer.

Seaborn et al. [5] demonstrated gaining kernel privileges through the DRAM RowHammer bug on a typical laptop. Two requirements enable the attack. First, the adversary has to find the correct address mapping between the physical and virtual memory space to hammer the correct cells. Second, the cache of the system would typically mitigate frequent activation of the same memory location. The authors used the flush instruction to constantly flush the cache, enabling the adversary to frequently activate the same memory location. Ultimately, the attacker gains kernel access to the whole physical memory through a normal process execution on an x86-64 machine by hammering a page table entry to point to an attacker-owned page table.

Considering its advantages, ReRAM has the potential to replace DRAM in modern computing systems. Thus, the mentioned attack scenario is transferable to NeuroHammer. Hereby, the access patterns must be adjusted to match the physical characteristics of the thermal crosstalk in memristive crossbar memories. In general, any attack proven to work with RowHammer could additionally work with NeuroHammer. However, the application domain of DRAM and ReRAM does not completely overlap. Hence, the proposed attack poses a supplementary threat to emerging neuromorphic-based systems, such as neuromorphic machine-learning accelerators.

## VII. Conclusion

This work introduced NeuroHammer, a security threat to emerging non-volatile memories based on thermal crosstalk in dense crossbar structures. We developed a simulation framework to investigate the impact of physical parameters on the effectiveness of the attack. The results show that the NeuroHammer attack deliberately induces bit-flips in memristive crossbar structures. Finally, we discussed the security implications of NeuroHammer by analyzing attack scenarios of the related RowHammer attack. In future work, we plan to verify the existence of the NeuroHammer attack on physical crossbars and explore countermeasures to mitigate the security threat.

With this work, we demonstrated that the fundamental security implication of disturbance errors still persists even in emerging neuromorphic technologies. As neuromorphic hardware has the potential to become a key component of modern computing systems, evaluating its basic security aspects is essential to providing a stepping stone to building secure next-generation devices.

## References


[1] C. D. Schuman *et al.*, "A survey of neuromorphic computing and neural networks in hardware," *CoRR*, vol. abs/1705.06963, 2017.

[2] F. Staudigl *et al.*, "A survey of neuromorphic computing-in-memory: Architectures, simulators and security," *IEEE Design & Test*, 2021.

[3] O. Mutlu *et al.*, "RowHammer: A retrospective," *IEEE TCAD*, vol. 39, no. 8, pp. 1555–1571, 2020.

[4] Y. Kim *et al.*, "Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors," in *2014 ACM/IEEE ISCA*. IEEE, jun 2014.

[5] M. Seaborn *et al.*, "Exploiting the DRAM Rowhammer bug to gain kernel privileges," *Black Hat*, vol. 15, p. 71, 2015.

[6] L. Cojocar *et al.*, "Are we susceptible to Rowhammer? an end-to-end methodology for cloud providers," *CoRR*, vol. abs/2003.04498, 2020.

[7] L. Jiang *et al.*, "Mitigating write disturbance in super-dense phase change memories," in *2014 44th Annual IEEE/IFIP DSN*. IEEE, jun 2014.

[8] Y. Cai *et al.*, "Technology-array-algorithm co-optimization of RRAM for storage and neuromorphic computing: Device non-idealities and thermal cross-talk10.1109/dsn.2014.32," in *2020 IEEE IEDM*. IEEE, dec 2020.

[9] M. von Witzleben *et al.*, "Investigation of the impact of high temperatures on the switching kinetics of redox-based resistive switching cells using a high-speed nanoheater," *Advanced Electronic Materials*, vol. 3, no. 12, nov 2017.

[10] R. Waser *et al.*, "Redox-based resistive switching memories - nanoionic mechanisms, prospects, and challenges," *Adv. Mater.*, vol. 21, no. 25-26, pp. 2632–2663, 2009.

[11] S. Pi *et al.*, "Memristor crossbar arrays with 6-nm half-pitch and 2-nm critical dimension," *Nat. Nanotechnol.*, vol. 14, no. 1, pp. 35–39, 2019.

[12] M. von Witzleben *et al.*, "Study of the SET switching event of VCM-based memories on a picosecond timescale," *J. Appl. Phys.*, vol. 127, no. 20, p. 204501, 2020.

[13] S. Menzel *et al.*, "Origin of the ultra-nonlinear switching kinetics in oxide-based resistive switches," *Adv. Funct. Mater.*, vol. 21, no. 23, pp. 4487–4492, 2011.

[14] "Comsol Multiphysics," COMSOL Group, accessed: 2021-09-14. [Online]. Available: https://www.comsol.com/comsol-multiphysics

[15] "Virtuoso System Design platform," Cadence Design Systems, Inc., accessed: 2021-09-14. [Online]. Available: https://www.cadence.com

[16] F. Cüppers *et al.*, "Exploiting the switching dynamics of HfO2-based ReRAM devices for reliable analog memristive behavior," *APL Materials*, vol. 7, no. 9, p. 091105, sep 2019.

[17] C. Bengel *et al.*, "Variability-aware modeling of filamentary oxide based bipolar resistive switching cells using SPICE level compact models," *TCAS 1*, vol. 67, no. 12, pp. 4618–4630, 2020.

[18] S. Menzel, "Juelich Aachen resistive switching tools (JART)," Tech. Rep., 2019. [Online]. Available: http://www.emrl.de/Jart.html