Area-efficient and low stand-by power 1k-byte transmission-gate-based non-imprinting high-speed erase (TNIHE) SRAM

Ho, Weng-Geng; Ne, Kyaw Zwa Lwin; Prashanth Srinivas, Nagarajan; Chong, Kwen-Siong; Kim, Tony Tae-Hyoung; Gwee, Bah Hwee

2016

Ho, W.-G., Ne, K. Z. L., Prashanth Srinivas, N., Chong, K.-S., Kim, T. T.-H., & Gwee, B. H. (2016). Area-efficient and low stand-by power 1k-byte transmission-gate-based non-imprinting high-speed erase (TNIHE) SRAM. 2016 IEEE International Symposium on Circuits and Systems (ISCAS), 698-701.

<https://hdl.handle.net/10356/83999>

<https://doi.org/10.1109/ISCAS.2016.7527336>

© 2016 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<http://dx.doi.org/10.1109/ISCAS.2016.7527336>].

Downloaded on 26 Apr 2023 17:15:56 SGT

Area-Efficient and Low Stand-By Power 1K-Byte Transmission-Gate-Based Non-Imprinting High-Speed Erase (TNIHE) SRAM

Weng-Geng Ho*, Kyaw Zwa Lwin Ne, N. Prashanth Srinivas, Kwen-Siong Chong, Tony Tae-Hyoung Kim and Bah-Hwee Gwee
School of Electrical and Electronic Engineering,
Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798
Email: *wggho@ntu.edu.sg

Abstract—We propose a novel 15-T Transmission-gate-based Non-Imprinting High-speed Erase (TNIHE) SRAM cell with emphases on low area overhead and low stand-by power attributes for highly secured data storage applications. We benchmark our proposed 15-T TNIHE SRAM cell against the reported 22-T Non-Imprinting High-speed Erase (NIHE) SRAM cell, and demonstrated three key features of reducing 7 transistors. First, we adopt the transmission gates (as opposed the cross-couple inverters) in the slave circuitry, saving 4 transistors. Second, we eliminate a transistor which uses to reset the slave circuitry, hence saving 1 transistor. Third, we apply the global inverse transistors (as opposed to the local inverse transistors) in the read/write circuit for each SRAM cell, hence further reduce 2 more transistors. As a result, our proposed TNIHE SRAM cell @ 65nm CMOS features ~17% smaller layout area. We design a 1k-byte memory based on the proposed TNIHE SRAM cells. On the basis of simulations, we show that our 1k-byte SRAM memory features overall ~13% smaller area, and dissipates on average, ~30% lower stand-by power than the reported NIHE counterpart.

I. INTRODUCTION

SRAM is one of the most important building blocks for digital systems. In many security applications, confidential data (including passwords) are stored in the SRAM. Unfortunately, unauthorized hackers can retrieve the SRAM information based on the data imprint effect [1] on the SRAM even though when the power supply has been turned off. The data imprint effect is essentially the imprinted marks introduced or the associated degraded transistor characteristic on SRAM cells when these cells are biased unevenly over a long period of time. The hackers are hence possibly to reveal the data information through various means such as supply voltage aging, temperature freezing, power analysis attack, microscopy de-layer scanning etc [2].

A possible solution to prevent SRAM cells from data-imprinting is to regularly swap, shift or alter the confidential data to either various locations (within the same SRAM array) or other (separate) memory such that the strength of the data imprint becomes insignificant [3],[4]. Nonetheless, the hardware and power cost of these approaches could be large, limiting their practicability for power-critical applications. Another preferable solution is to realize a toggling Non-Imprinting High-speed Erase (NIHE) memory, where each SRAM cell therein has a master circuit and a slave circuit [5], [6]. The master and slave circuits keep swapping the stored data locally (instead of globally) from each other in a way that the storage nodes keep alternating. Consequently, the average voltage-stress on each node will almost be the same, hence minimizes the data imprint in each node.

The high-speed erase feature further enhances the memory security from an improper or unauthorized access [7], [8]. Particularly, the SRAM cell is actively being monitored according to the functionality of the system and the associated operating conditions. If an impending attack is detected (or deemed) under an ‘abnormal’ scenario and in response to the attack, the stored memory content can be erased in-situ, minimizing the risk of data leaking.

However, to feature the non-imprinting and high-speed erase mechanisms, the reported NIHE 22-T SRAM cell [5], [9] occupies a comparatively larger area overhead. The large overhead also leads to high power dissipation (with significant amount of leakage power). For non-imprinting function (as defined as stand-by mode in the reported article), the high stand-by power dissipation becomes worse due to the periodically data toggling, affecting the practicality of the memory for power-critical applications.

In this paper, we propose 15-T Transmission-gate-based Non-Imprinting High-speed Erase (TNIHE) SRAM cell with low overhead and low stand-by power. We achieve these attributes in our proposed TNIHE cell by simplifying the overall transistor configuration with three main features. First, we propose to adopt two transmission gates to replace the usual 8-transistor cross-coupled inverter for the slave circuit, hence saving 4 transistors. Second, with the new slave circuit, we employ only 1 reset transistor, instead of usual 2 transistors, for the high-speed erase. Third, we apply global inverse transistors to access the cell in two different states for every SRAM column; in contrast to the conventional approach of using local inverse transistors for every single cell, hence saving another 2 transistors. In overall, our proposed TNIHE cell features ~17% smaller area (@ 65nm CMOS) than the reported NIHE cell [5]. We further design an 1k-byte SRAM memory based on the proposed TNIHE cells, and benchmark it against the reported NIHE counterpart. Our proposed 1k-byte TNIHE SRAM memory features ~13% smaller area, and dissipates on average, ~30% lower stand-by power than the reported NIHE counterpart.

This paper is organized as follows. Section II reviews the reported 22-T NIHE cell and its non-imprinting feature. Section III presents the proposed TNIHE SRAM memory with the proposed TNIHE cell, SRAM interface structure and operations. Section VI presents the simulation results and finally, conclusions are drawn in Section V.

II. REVIEW OF REPORTED NIHE SRAM

We first review the reported 22-T NIHE cell [5] and its non-imprinting feature. Fig. 1 depicts the schematic of the reported NIHE cell, which comprises a master circuit, a slave circuit, a reset circuit and a read/write circuit. The master circuit inverts the data s/sb to q/qb . The slave circuit copies the data q/qb to s/sb . The reset circuit erases the data q/qb quickly when T_RST is triggered. The read/write circuit access q/qb to write in or read out the data.

Fig. 1: Reported NIHE Cell Schematic

We will now study the data imprint effect in the SRAM. In a typical conventional SRAM, the cell nodes q and qb store data value '1' ($q = '1'$ and $qb = '0'$) or '0' ($q = '0'$ and $qb = '1'$). The data imprint occurs when the data is stored over a long period of time as the cells are biased unevenly. The voltage-stress on the nodes q and qb is largely different since their values are constant and contrast to each other.

In contrast, the NIHE cell consists of master and slave circuits, which constantly swapping the stored data between nodes q/qb and s/sb . It is noted that the nodes are toggling between '0' and '1' value periodically. As a result, the average voltage-stress on each node will almost be the same, hence the difference of the effect due to the data imprint could be negligible.

However, in the reported NIHE cell, the slave circuit, which is similar to the master circuit, uses a pair of cross-coupled inverters and pull-down transistors to swap the s/sb . Since the data is also stored in s/sb , the cell has to embed an additional reset transistor to quick erase the slave circuit when T_RST is triggered. Furthermore, to read/write the q/qb in two different states, two additional inverse transistors are embedded in the read/write circuit as compared to the conventional 6-T SRAM cell. For example, $BL = q$ and $BLB = qb$ when $WL = '1'$. $BL = qb$ and $BLB = q$ when $WLB = '1'$.

III. PROPOSED TNIHE SRAM

A. Proposed TNIHE Cell

We now elaborate the proposed 15-T TNIHE cell schematic, as depicted in Fig. 2(a). The proposed TNIHE cell comprises a master circuit, two slave circuits, a reset circuit and a read/write circuit. Their individual functionalities are exactly the same as those circuits in the reported NIHE cell. The slave circuit 1 and 2, are basically the transmission gates, copy the data q/qb to s/sb .

The proposed 15-T TNIHE cell is implemented in the layout as depicted in Fig. 2(b). The cell layout follows the industrial practice where all the poly and metal layers are drawn in parallel to each other, to minimize the cell area. The interface signals are drawn in the metal layers extended from top to bottom of the layout, to ease the cell placement in the SRAM array. In short, the cell layout occupies $5.7\mu\text{m}^2$.

Fig. 2: Proposed TNIHE Cell (a) Schematic and (b) Layout

There are several features in our proposed 15-T TNIHE cell over the reported 22-T TNIHE cell. First, the combination of cross-coupled inverters with pull-down transistors in the slave circuit are replaced with transmission gates, saving 4 transistors. Second, the reset transistor to erase the slave circuit is eliminated, reducing 1 transistor. Third, the global inverse transistors are used for every SRAM column to access the cell in two different states, hence the local inverse transistors in the read/write circuit for every single cell can be eliminated, saving 2 transistors. In total, 7 transistors are reduced in the proposed TNIHE cell.

Table I compares the characteristics of the proposed TNIHE cell against the reported NIHE cell. Read and write noise margins are used to characterize the data stability of the cell for read and write operation, respectively. Read delay is measured as the delay from WL asserted until BL/BLB de-asserted. Write Delay is measured as the delay from WL asserted until q/qb asserted. Read and write active power are the average power dissipated by cell during read and write operation, respectively. Cell area is the layout area occupied by one cell.

From the table I, we remark the followings. First, the noise margin, delay and active power for the read and write operations remain unchanged when comparing the reported 22-T NIHE cell with the proposed 15-T TNIHE cell. This

implies that although the transistor count is reduced, it does not compromise the data stability and figure-of-merits. Second, the proposed TNIHE cell is more area-efficient, 17% smaller area than the reported NIHE cell, due to the reduced transistor count.

TABLE I
CHARACTERISTICS OF PROPOSED TNIHE AND REPORTED NIHE CELLS

SRAM Cell	Reported 22-T NIHE [5]	Proposed 15-T TNIHE
Read Noise Margin (mV)	220	
Write Noise Margin (mV)	488	
Read Delay (ns)	0.6	
Write Delay (ns)	0.5	
Read Active Power (nW)	41.4	
Write Active Power (nW)	32.8	
Cell Area (μm^2)	6.9	5.7 (17%)

B. Interface Structure

We now implement the proposed TNIHE cell into the SRAM structure. Fig. 3 depicts the block diagram of the proposed 1k-byte TNIHE SRAM, which comprises a TNIHE SRAM array + peripherals (i.e. Memory), and a TNIHE controller. The Memory receives 10-bit address input $A[9:0]$, 8-bit data input $D[7:0]$, chip-enable CEN and write-enable WEN control signals, clock signal CLK to generate 8-bit data output $Q[7:0]$. The TNIHE controller comprises a clock divider and a state machine. The clock divider accepts CLK to generate a slower data toggling frequency for master circuit MT_CLK and slave circuit ST_CLK respectively, to the Memory. The state machine generates and periodically changes the state between ‘even’ and ‘odd’ of the controller in the Memory.

Fig. 3: Block Diagram of Proposed 1k-byte TNIHE SRAM

Fig. 4 depicts the Memory architecture, which comprises TNIHE SRAM array, row decoder, column decoder, R/W circuit, input driver and sense amplifier with the output driver. The TNIHE SRAM array distributes the TNIHE cells into 128 row $\times$ 8 column $\times$ 8-bit with bit-conditioning circuit to pre-charge bit-line BL/BLB . The row decoder receives $A[6:0]$ to trigger 128-bit word-line WL signals to determine the accessed row. The column decoder receives $A[9:7]$ to determine the accessed column. R/W circuit receives CEN and WEN to trigger write signal WR to write in data, or read signal RD to read out data. Input driver write in $D[7:0]$ to SRAM array through BL/BLB . Sense amplifier with output driver amplifies and reads out data from SRAM array to $Q[7:0]$ through BL/BLB .

Fig. 4: Architecture of 1k-byte TNIHE SRAM Array + Peripherals (Memory)

C. SRAM Operations

The operation modes of the proposed TNIHE SRAM depend on the SRAM control signals CEN , WEN and T_RST , as tabulates in Table II. When T_RST is ‘1’, the mode is reset and there is no operation in the TNIHE SRAM.

When T_RST is ‘0’, the mode is active, stand-by or idle. In active mode, there are two operations, namely write and read. The write operation requires both CEN and WEN to be ‘0’. The read operation requires $CEN = ‘0’$ and $WEN = ‘1’$. In stand-by mode, the TNIHE SRAM is running data toggling operation with $CEN = ‘1’$ and $WEN = ‘0’$. In idle mode, the TNIHE SRAM is waiting with $CEN = ‘1’$ and $WEN = ‘1’$, and ready for next operation.

TABLE II
PROPOSED TNIHE SRAM OPERATION MODES

Operation Modes	CEN	WEN	T_RST
Reset	X	X	1
Active	0	0	0
	0	1	0
Stand-By	1	0	0
Idle	1	1	0

Fig. 5 depicts the timing diagram of TNIHE SRAM in the stand-by operation, where the cell in nodes q/qb and s/sb are toggling between ‘true’ and ‘inverted’ data alternately, depends on MT_CLK and ST_CLK . The state T_STATE is either ‘even’ or ‘odd’, depends on the q/qb value (‘true’ or ‘inverted’) in the cell. Hence, in order to read/write the correct data in two different states, the additional inverse transistors are to be added globally into input driver and output driver. For example during the read operation, $Q = BL$ when T_STATE is ‘even’, and $Q = BLB$ when T_STATE is ‘odd’. During the write operation, $BL = D$ when T_STATE is ‘even’, and $BLB = D$ when T_STATE is ‘odd’.

Fig. 5: Timing Diagram for Stand-By Operation

IV. SIMULATION RESULTS

We design and implement the 1k-byte SRAM based on the proposed TNIHE cell using Global Foundries 65nm CMOS technology process. Fig. 6 depicts the layout of the proposed 1k-byte TNIHE SRAM, which occupies $\sim 79,000\mu\text{m}^2$ area.

Fig. 6: Layout of Proposed 1k-byte TNIHE SRAM

The proposed TNIHE SRAM is benchmarked against the reported NIHE counterpart, as tabulated in Table III. From the table, we remark the followings. First, both the SRAMs are organized in the same array structure 128 row $\times$ 8 column $\times$ 8-bit and clocked at the frequency of 100MHz. Second, the proposed TNIHE SRAM occupies 13% smaller area than the reported counterpart, due to the smaller area contributed by the proposed TNIHE cell. Third, both proposed TNIHE and reported NIHE SRAM features the same memory access time, erase time, active power, and dissipates insignificant $\sim 2\%$ higher stand-by power, implying that the performance of the SRAM is not compromised when the area is reduced.

TABLE III

SIMULATION RESULTS OF 1K-BYTE SRAM BASED ON PROPOSED TNIHE AND REPORTED NIHE@65NM CMOS, 1.2V

1k-byte SRAM	Reported NIHE [5]	Proposed TNIHE
Memory Organization	128 row $\times$ 8 column $\times$ 8-bit	
Clock Frequency (MHz)	100	
Memory Access Time (ns)	5.4	
Erase Time (ns)	0.4	
Active Power ($\mu\text{W}/\text{MHz}$)	3.2	
Idle Power (μW)	2.76	2.81 (-2%)
Area (μm^2)	$\sim 90,000$	$\sim 79,000$ (13%)

Fig. 7 depicts the stand-by power dissipation based on different data toggling frequency during the non-imprinting operation. We remark the followings. First, when the toggling frequency reduces, the stand-by power dissipation decreases accordingly. This is because the switching power reduces due to the slower switching activity. Second, the proposed TNIHE SRAM dissipates $\sim 30\%$ lower stand-by power than the reported counterpart. This is due to the lower dissipated current in the proposed TNIHE cell.

Fig. 7: Stand-By Power Dissipation versus Data Toggling Frequency during Non-Imprinting Operation

V. CONCLUSIONS

We have proposed an area-efficient TNIHE SRAM with reduced stand-by power dissipation. In terms of SRAM cell, our proposed TNIHE features $\sim 17\%$ smaller layout area than the reported NIHE. In terms of 1k-byte SRAM design based on 65nm CMOS process, our proposed TNIHE features $\sim 13\%$ smaller area, and dissipates on average, $\sim 30\%$ lower stand-by power than the reported NIHE design, during the non-imprinting operation.

REFERENCES

- [1] S. Skorobogatov, *Low Temperature Data Remanence in Static RAM*, Technical Report, Computer Laboratory, University of Cambridge, Jun. 2002.
- [2] S. H. Weingart, "Physical security devices for computer subsystems: a survey of attacks and defences," *Proc. Second International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pp. 302-317, 2000.
- [3] S. M. Trimberger, "System and method of detecting and reversing data imprinting in memory," *US Patent No. 8,359,447 B1*, Jan. 2013.
- [4] C. U. Buscaglia et al., "Protection of secure electronic modules against attacks," *US Patent No. 7,953,987 B2*, 31 May 2011.
- [5] R. M. Backus, C. F. Duffey, A. C. Well and S. V. Joshi, "Non-imprinting memory with high speed erase," *US Patent No. 7,525,836 B2*, Apr. 2009.
- [6] B. B. Pedersen and D. A. Reese, "Systems and methods for preventing data remanence in memory systems," *US Patent Application Publication No. US2012/0274353 A1*, Nov. 2012.
- [7] K. Yu, X. Zou, G. Yu, and W. Wang, "Security strategy of powered-off SRAM for resisting physical attack to data remanence," *Journal of Semiconductors*, vol. 30, no. 9, pp. 1-5, Sep. 2009.
- [8] M. M. Furusawa and C. T. Nguyen, "High-assurance processor active memory content protection," *US Patent Application Publication No. US2006/0023486 A1*, Feb. 2006.
- [9] W.-G. Ho, K.-S. Chong, B.-H. Gwee, J. S. Chang and K. Z. L. Ne, "A dynamic-voltage-scaling 1kbyte $\times$ 8-bit non-imprinting Master-Slave SRAM with high speed erase for low-power operation," *International Symposium on Integrated Circuits, ISIC*, Singapore, pp. 320-323, Dec. 2014.
- [10] N. H. E. Weste and D. Harris, *CMOS VLSI Design: A System Perspective*, Pearson/Addison-Wesley, 2005.