ELectronics EXpress

LETTER

IEICE Electronics Express, Vol.15, No.8, 1–6

Data deletion method for security improvement of Flash memories

Ruishan Xin[1,2], **Mao Ye**[1,2a)], **Jia Wang**[1,2], **Kai Hu**[1,2], **and Yiqiang Zhao**[1,2]

[1] *School of Microelectronics, Tianjin University, Tianjin 300072, China*

[2] *Tianjin Key Laboratory of Imaging and Sensing Microelectronic Technology, Tianjin 300072, China*

a) *mao_ye@tju.edu.cn*

Abstract: For Flash memories, data remanence can cause differences in threshold voltage among the erased cells. By detecting such differences, already-erased data can be recovered. To decrease the differences, a secure deletion method of data is investigated in this paper. The effects of erase-erase (EE) operation and erase-program (EP) operation on threshold voltage are studied in theory. Based on the floating-gate device model, the optimal overwriting sequence, EPEPE, is obtained by simulation. This sequence can reduce the difference to 0.1 mV in threshold voltage among the erased Flash cells, which equals to that caused by one floating-gate electron.

Keywords: Flash memory cells, data remanence, floating gate, threshold voltage, secure deletion method, overwriting sequence

Classification: Circuits and modules for storage

References

[1] C. C. Chung, *et al.*: "A high-performance wear-leveling algorithm for flash memory system," IEICE Electron. Express **9** (2012) 1874 (DOI: 10.1587/elex.9.1874).

[2] J. W. Park, *et al.*: "Sub-grouped superblock management for high-performance flash storages," IEICE Electron. Express **6** (2009) 297 (DOI: 10.1587/elex.6.297).

[3] J. Wang, *et al.*: "A study of residual characteristics in floating gate transistors," Sci. China Inf. Sci. **61** (2018) 069402 (DOI: 10.1007/s11432-017-9145-2).

[4] P. Gutmann: "Data remanence in semiconductor devices," Conference on Usenix Security Symposium (2001) 4.

[5] S. Skorobogatov: "Data remanence in flash memory devices," Conference on Cryptographic Hardware and Embedded Systems (2005) 339.

[6] C. Friederich: in *Inside NAND Flash Memories*, ed. R. Micheloni (Springer, Netherlands, 2010) 55.

[7] P. Pavan, *et al.*: "Floating gate devices: Operation and compact modeling," IEEE Circuits Devices Mag. **22** (2006) 33 (DOI: 10.1109/MCD.2006.1708380).

[8] S. Yamada, *et al.*: "Degradation mechanism of flash EEPROM programming after program/erase cycles," Electron Devices Meeting (1993) 23 (DOI: 10.1109/IEDM.1993.347407).

DOI: 10.1587/elex.15.20180152
Received February 6, 2018
Accepted March 14, 2018
Publicized April 4, 2018
Copyedited April 25, 2018

[9] Atlas user's manual: Silvaco International Software (2010).
[10] S. S. Chung, *et al.*: "A Spice-compatible flash EEPROM model feasible for transient and program/erase cycling endurance simulation," Electron Devices Meeting (1999) 179 (DOI: 10.1109/IEDM.1999.823874).

1 Introduction

With the development of microelectronics technology, the manufacturing cost of memories is becoming lower and lower. The solid state memories are edging out the disk memories and wildly used in mobile communications, smart home systems and so on. Due to high speed, low power consumption and mass memory capacity, Flash memories turn into the most popular parts of solid-state memories [1, 2].

However, data remanence seriously threatens the security of Flash memory [3]. Data remanence is the phenomenon that electrons in floating gate are not moved entirely during common erase operation. As a result of diversity on number of residual electrons, the threshold voltages of floating-gate cells will have differences. By detecting such differences, attackers can recover the already-erased data. Research proves that the cells without program/erase operation and the cells with one program/erase operation can be distinguished [4]. Experiments show that the difference in threshold voltage is approximately 0.5 V between the above-mentioned cells [5]. Hence, the threshold voltage is an easy target for attackers to implement data recovery. By drawing artificial pads conducting into terminals of floating gate via focused ion beam modification, attackers can detect the threshold voltage directly. Therefore, a secure deletion method of data based on erase-program cycles is proposed in this paper. This method reduces the differences in threshold voltage among the erased cells, preventing the unauthorized data recovery and enhancing the security of Flash memories.

2 Data remanence in Flash memories

Data are stored in Flash memories in form of electric charges. Floating gate is the basic structure for storing charges. The operations on floating-gate cells include program and erase [6]. In program operation, electrons get into floating gate due to the effect of channel hot-electron injection. In erase operation, as a result of the Fowler-Nordheim (FN) tunneling, electrons are moved from floating gate to source diffusion.

The model of floating-gate threshold voltage [7] is

$$V_{th} = K - \frac{Q_{FG}}{Q_{CG}}, \tag{1}$$

where K is a constant. Q_{FG} is the quantity of electric charge in floating gate. C_{CG} is the capacitance between control gate and floating gate. Q_{FG} is the product of the quantity of electric charge of a single electron and the number of electrons. The former is a negative constant. Thus, the larger the number of electrons is, the smaller Q_{FG} is. V_{th} is inversely proportional to Q_{FG}. The threshold voltage have obvious differences, which are 6 V commonly [8], between the floating-gate cells storing 0 and those storing 1.

DOI: 10.1587/elex.15.20180152
Received February 6, 2018
Accepted March 14, 2018
Publicized April 4, 2018
Copyedited April 25, 2018

Normally, the erase operation is executed only once to clean data. However, the electrons will not be moved entirely. A spot of electrons will remain in floating gate. The number of residual electrons in each floating gate is various, so the threshold voltages of these cells are different. By distinguishing the differences in threshold voltage, erased data could be recovered.

Sergei Skorobogatov makes an experiment on floating-gate cells [5]. He performs erase operation continuously on the cells storing 0 and the cells storing 1, respectively. The difference tendency of threshold voltage is shown in Fig. 1. Even though the erase operation is executed 100 times, the differences in threshold voltage between the programmed cells and the previously erased cells still obviously exist. Thus, duplication of erase operation is not a secure and efficient method to protect key data.

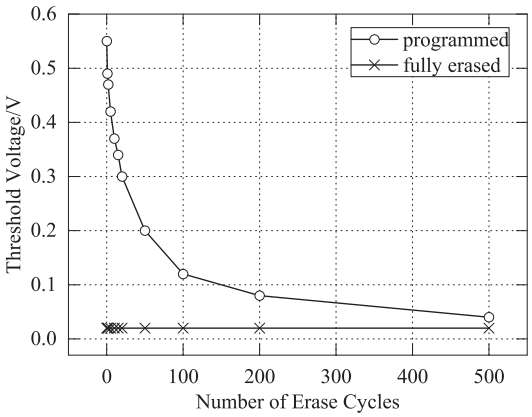

Fig. 1. Variation tendency of threshold voltage during erase cycles

3 Secure deletion method

Based on standard 180 nm Flash process, the device model of floating-gate transistor is achieved on the platform of the device simulator TCAD. The p-type Si substrate has the boron concentration of $1 \times 10^{12}\,\mathrm{cm}^{-3}$. The thickness of tunneling oxide is 10 nm. The thickness of floating gate formed by a phosphorus-doped polysilicon layer is 150 nm. The phosphorus concentration is $6 \times 10^{14}\,\mathrm{cm}^{-3}$. The program operation utilizes the Luck-Electron Hot Carrier Injection model and the Impact Ionization model. The erase operation utilizes the FN tunneling model. The threshold voltage is defined as the control-gate voltage when the drain current is 1 μA/μm under the condition of 1 V drain-to-source voltage. Based on the device model, the study on different overwriting operations is implemented.

3.1 Overwriting operation

Here we define that P represents the program operation and E represents the erase operation. According to the programming principles of Flash memories, before a program operation, an erase operation must be executed first. Thus, the overwriting operation can be classified into two categories: erase-program (EP) operation and erase-erase (EE) operation. In erase-program operation, erase operation is executed

DOI: 10.1587/elex.15.20180152
Received February 6, 2018
Accepted March 14, 2018
Publicized April 4, 2018
Copyedited April 25, 2018

first, and then program operation. In erase-erase operation, erase operation will be executed twice.

Aim at the EP operation, we make some preliminary definitions. $Q(0)$ is the absolute value of Q_{FG} after an E operation when the cell previously stores 0. $Q'(0)$ is the absolute value of Q_{FG} after an EP operation when the previous stored datum is 0. $\Delta Q(0)$ is the absolute difference of Q_{FG} during the P operation in an EP operation when the previous stored datum is 0. $Q(1)$, $Q'(1)$ and $\Delta Q(1)$ are similar to $Q(0)$, $Q'(0)$ and $\Delta Q(0)$, respectively, but the cell previously stores 1.

According to Fig. 1, after an E operation, the threshold voltage of the cell storing 0 is larger than that of the cell storing 1. Therefore,

$$Q(0) > Q(1). \tag{2}$$

The model of injection current [9] in a P operation is

$$I_{inj} = \iint P_n(x, y)|\vec{J_n}(x, y)|dxdy, \tag{3}$$

where $\vec{J_n}(x, y)$ is the current density at the position (x, y) of the channel. For a certain position, the current density is fixed. $P_n(x, y)$ is the probability that an electron is injected into floating gate from channel. In a P operation, the longitudinal electric field of the cell storing 0 is smaller than that of the cell storing 1. Thus, the P_n of the cell storing 0 is also smaller than that of the cell storing 1, resulting in that the injection current of the cell storing 0 is smaller than that of the cell storing 1.

The model of floating-gate charge [10] is

$$(Q_{FG})_n = (Q_{FG})_{n-1} + I_{inj}\Delta t, \tag{4}$$

where $(Q_{FG})_n$ is the quantity of electric charge in floating gate after n operations of program or erase, and n is variable. Δt is the execution time of the operation. From Eq. (4), we get

$$\Delta Q_n = (Q_{FG})_n - (Q_{FG})_{n-1} = I_{inj}\Delta t, \tag{5}$$

where ΔQ_n is the difference of quantity of electric charge in floating gate during the n time operation. ΔQ_n is proportional to the injection current. Because the injection current of the cell storing 0 is smaller than that of the cell storing 1, ΔQ_n of the cell storing 0 is also smaller than that of the cell storing 1. Thus,

$$\Delta Q(0) < \Delta Q(1). \tag{6}$$

And then we can get

$$\begin{aligned} Q'(0) - Q'(1) &= [Q(0) + \Delta Q(0)] - [Q(1) + \Delta Q(1)] \\ &= [Q(0) - Q(1)] - [\Delta Q(1) - \Delta Q(0)] \\ &< Q(0) - Q(1). \end{aligned} \tag{7}$$

From Eq. (7), after EP operation, the differences in quantity of electric charge decrease, leading to the reduction of differences in threshold voltage. Likewise, the differences in threshold voltage also decrease after EE operation, but the reduction is discrepant from that of EP operation. One hundred simulations of EP and EE operation are implemented based on the device model on TCAD platform. The results are illustrated in Fig. 2. The horizontal ordinate is the order number of the

DOI: 10.1587/elex.15.20180152
Received February 6, 2018
Accepted March 14, 2018
Publicized April 4, 2018
Copyedited April 25, 2018

results. The longitudinal ordinate is the difference in threshold voltage. From Fig. 2, no matter what the stored data are, the differences after EE operation are greater than 0.5 V, while the differences are smaller than 0.4 V after EP operation. Thus, the EP operation is more efficient to reduce the differences in threshold voltage. During the P operation in an EP operation, the quantity of electrons injected into floating gate is approximately 5500, which is close to the limit. Hence, the P operation makes the difference of threshold voltage smaller.

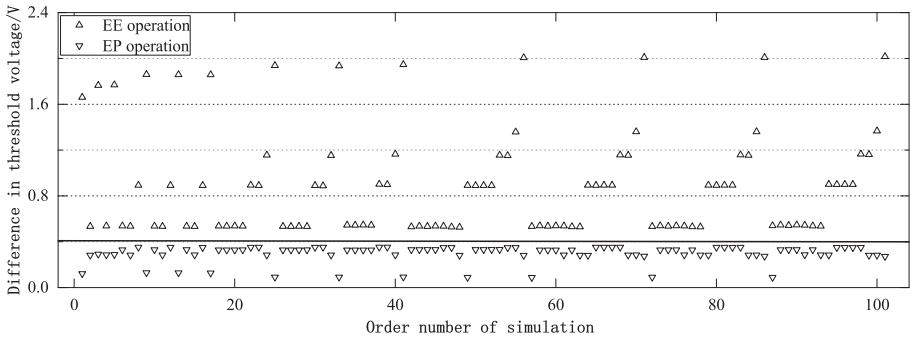

Fig. 2. Difference in threshold voltage after EE operation and EP operation

3.2 Secure overwriting sequence

The floating-gate cells need to have the same threshold voltage after utilizing this secure deletion method no matter what the previous stored data are. From Eq. (1), if two cells have the same threshold voltage, they must have equal quantity of electric charge. Ideally, the minimum difference in threshold voltage is caused by one electron in floating gate. Then we get

$$\Delta V_{th} = \frac{V_{th}(x) - V_{th}(0)}{N(x)}, \tag{8}$$

where ΔV_{th} is the difference in threshold voltage caused by one electron, $V_{th}(0)$ is the initial threshold voltage without any operation, $V_{th}(x)$ is the threshold voltage after x operations, and $N(x)$ is the number of electrons in floating gate after x operations.

Simulations based on the device model are implemented to obtain ΔV_{th}. Table I shows the simulation results of threshold voltages and number of electrons. The number of electrons in floating gate is obtained from the quantity of electric charge through mathematical computation. To keep high accuracy, the number of electrons is not converted to integer. From Table I, the minimum difference in threshold voltage is 1.5 mV.

Table I. Threshold voltages and floating-gate electrons

Threshold voltage/V	Number of electrons	ΔV_{th}/mV
1.04031	0	/
9.12783	5399.870162	1.5
3.16394	1417.827715	1.5

DOI: 10.1587/elex.15.20180152
Received February 6, 2018
Accepted March 14, 2018
Publicized April 4, 2018
Copyedited April 25, 2018

To achieve the optimal overwriting sequence, the effects of several different EP cycles are studied by simulations. Based on the device model, these EP cycles are executed in the floating-gate cells storing different data. Several differences are obtained. The maximum of differences is utilized to evaluate the worst case of effects for each overwriting sequence in Table II. The difference in threshold voltage is up to 9.14016 V without overwriting operation. The more times the EP cycles are executed, the lower the difference in threshold voltage is. If the acceptable value of difference in threshold voltage is 0.01 V, only EPEP overwriting sequence needs to be executed. To achieve the minimum difference 1.5 mV, the overwriting sequence, EPEPE, needs to be implemented. From Fig. 1, after one hundred erase cycles, the difference is still large than 0.1 V. But after the overwriting sequence EPEPE, the difference is only 0.1 mV. Therefore, the effect of proposed overwriting sequence is more significant.

Table II. Effects of overwriting sequence

Overwriting sequence	Maximum difference in threshold voltage/V
None	9.14016
E	2.49853
EP	0.35302
EPE	0.01340
EPEP	0.00301
EPEPE	0.00010

4 Conclusion

To improve the security of Flash memories, a deletion method of data is proposed in this paper. The EP cycles are recommended as the overwriting sequence, which can make the differences smaller in threshold voltage between the cells previously storing 0 and those storing 1. According to the simulation results, the EPEPE is the optimal overwriting sequence to make the differences minimum. Utilizing this sequence, all the floating-gate cells previously storing different data will have extraordinarily similar threshold voltages after overwriting operation, making data recovery difficult.

Acknowledgments

This work was supported by National Natural Science Foundation of China (Grant No. 61376032) and Tianjin Science and Technology Project of China (Grant No. 15ZCZDGX00180).

DOI: 10.1587/elex.15.20180152
Received February 6, 2018
Accepted March 14, 2018
Publicized April 4, 2018
Copyedited April 25, 2018