Ultra-fast Data Sanitization of Sram by Back-biasing to Resist a Cold Boot Attack

Seong-Joo Han
Korea Advanced Institute of Science and Technology
Joon-Kyu Han
Korea Advanced Institute of Science and Technology
Gyeong-Jun Yun
Korea Advanced Institute of Science and Technology
Mun-Woo Lee
Korea Advanced Institute of Science and Technology
Ji-Man Yu
Korea Advanced Institute of Science and Technology
Yang-Kyu Choi (ykchoi@ee.kaist.ac.kr)
Korea Advanced Institute of Science and Technology

Research Article

Keywords: Back-bias, cold boot attack, data sanitization, security, SRAM

Posted Date: May 10th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-493322/v1

Version of Record: A version of this preprint was published at Scientific Reports on January 7th, 2022.
See the published version at https://doi.org/10.1038/s41598-021-03994-2.

Ultra-fast Data Sanitization of SRAM by Back-biasing to Resist a Cold Boot Attack

Seong-Joo Han[1†], Joon-Kyu Han[1†], Gyeong-Jun Yun[1], Mun-Woo Lee[1], Ji-Man Yu[1], and Yang-Kyu Choi[1,a)]

† These authors equally contributed to this work

[1]School of Electrical Engineering, Korea Advanced Institute of Science and Technology, (KAIST) 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea

a) Authors to whom correspondence should be addressed.

Email addresses: ykchoi@ee.kaist.ac.kr

Abstract

Although SRAM is a well established type of volatile memory, data remanence has been observed at low temperature even for a power-off state, and thus it is vulnerable to a physical cold boot attack. To address this, an ultra-fast data sanitization method within 5 ns is demonstrated with physics-based simulations for avoidance of the cold boot attack to SRAM. Back-bias, which can control device parameters of CMOS, such as threshold voltage and leakage current, was utilized for the ultra-fast data sanitization. It is applicable to temporary erasing with data recoverability against a low-level attack as well as permanent erasing with data irrecoverability against a high-level attack.

Keywords: Back-bias, cold boot attack, data sanitization, security, SRAM

Introduction

Static random access memory (SRAM), which is a type of volatile memory, is widely used for temporary storage of encryption keys and secret data in security systems[1-3]. It is commonly believed that stored data in SRAM are lost immediately and instantly when power is removed, and this is the main reason why SRAM is considered a secured memory device for high-level security applications. However, data remanence at low temperature was reported in power-off SRAM[4, 5]. Recently, studies on a cold boot attack to SRAM have been reported[6, 7]. If the time of data remanence is prolonged at low temperature, encryption keys and secret data can be decoded *via* a cold boot attack by a hacker. A method for fast erasing in SRAM is therefore necessary against the cold boot attack. A few approaches were demonstrated to prevent SRAM data from being decoded by the physical cold boot attack by use of additional circuitry including an erase transistor, storage capacitor, and charge pump. However, they sacrificed layout efficiency and increased hardware cost[8, 9]. In addition, long time of 0.2 μs was needed for data erasing.

In this work, an ultra-fast data sanitization of SRAM within 5 ns is demonstrated by use of forward back-biasing against the cold boot attack. Back-bias applied to a body of a metal-oxide-semiconductor field-effect transistor (MOSFET) is utilized to delete stored data *via* intentional distortion of the latch state between two inverters of a SRAM cell, which also encloses two n-channel pass-gate MOSFETs.

These two inverters are cross-coupled to sustain the latch state stably as long as power is supplied. An inverter is composed of a complementary metal-oxide-semiconductor (CMOS), *i.e.*, a pull-down n-channel MOSFET abbreviated NMOS and a pull-up p-channel MOSFET abbreviated PMOS. In the proposed data sanitization, two types of data erasing are available. One is temporary erasing by symmetric application of back-bias to two p-channel MOSFETs in each inverter. The other is permanent erasing by asymmetric application of back-bias to a

PMOS in one inverter and to an NMOS in the other inverter. In the former case, data recovery is allowed after a low-level threat attempt by hacking. In the latter case, data recovery is impossible after an attempt of a high-level threat by hacking. Temporary erasing partially disturbs data reading by application of the symmetric forward back-bias during an attack and then the partially distorted data are recoverable after the cessation of the hacking attempt. In contrast, permanent erasing completely deletes remnant data by application of the asymmetric forward back-bias against the critical hacking attempt and thereafter the erased data are irrecoverable. This approach with the aid of the back-biasing does not demand additional circuitry because back-biasing is commonly used for tuning CMOS characteristics, such as threshold voltage (V_T) or leakage current (I_{OFF})[10-12]. The data sanitization mechanism is analyzed for both the permanent erasing and the temporary erasing with physics-based device simulations. The results show that the proposed back-bias scheme can provide immunity against a cold boot attack at low temperature.

Simulation Methodology

For the simulations of a SRAM cell, MOSFETs with a high-*k* gate dielectric and a metal gate for a 32 nm technology node were modeled with the aid of a SILVACO ATLAS TCAD simulator [13]. The detailed parameters of the NMOS were set by referring to [14]. Thereafter those of the PMOS were regenerated as a counter-part of the NMOS. Based on the device-level simulations, a conventional cell of six transistor-SRAM (6T-SRAM) was constructed using ATLAS mixed-mode TCAD simulations to confirm the behaviors of the SRAM data sanitization by forward back-biasing. It is well known that the 6T-SRAM is composed of two pull-up PMOS, two pull-down NMOS, and two pass-gate NMOS.

In detail, the gate length (L_G), the gate width (W_G), and the equivalent oxide thickness (*EOT*) of the gate dielectric are 45 nm, 1 μm and 1.53 nm, respectively. The doping concentration of

the source (N_{source}), drain (N_{drain}), and substrate (N_{sub}) was set as 1×10^{20} cm^{-3}, 1×10^{20} cm^{-3}, and 3×10^{18} cm^{-3}, respectively. The dopant polarity for the PMOS was opposite to that for the NMOS. Various physical models, such as Schockley-Read-Hall (SRH), bandgap narrowing (BGN), Fermi-Dirac (FERMI), non-local band-to-band tunneling (BTBT), trap-assisted tunneling (TAT), and Cryogenic (CRYO) were used for accurate physics-based simulations. As a result, transfer characteristics (I_D-V_G) of the NMOS and PMOS modulated by forward back-bias (V_{BS}) were obtained, as shown in Figure 1(a) and (b). Note that the forward V_{BS} of the NMOS is 1 V and the forward V_{BS} of the PMOS is -1 V. This bias mode is opposite to that of the conventional back-bias scheme that usually relies on a reverse mode. Under the forward back-biasing, both NMOS and PMOS were turned on regardless of V_G. Figure 1(a) and (b) also show that the I_D-V_G characteristics of the NMOS and the PMOS were influenced by temperature (T). As T is lowered, the subthreshold slope (SS) becomes steeper and the off-state current (I_{OFF}), referred to as leakage current, tends to be decreased. When a cold boot attack was attempted at 173 K, remnant data were read even at a power-off state owing to the improved SS and suppressed I_{OFF} [6], [7]. It is inferred that the cold boot attack can be avoided by intentionally heating up the SRAM far above room temperature when the hacking attempt is sensed. However, it is practically difficult to apply heat to the SRAM. Moreover, this approach is not effective because the shift of V_T by temperature change, expressed as dV_T/dT, is very small. It was found that dV_T/dT was 0.94 mV/K for the NMOS and -0.72 mV/K for the PMOS from Figure 1 (a) and (b). These values are comparable to the experimental data reported in [15], [16]. As an example, ΔT ($=T_{high} - T_{300K}$) of 426 K is required to make a ΔV_T of 0.4 V that can distort the I_D-V_G. This means that high temperature (T_{high}) of 726 K is needed to induce the ΔV_T of 0.4 V solely by temperature at room temperature. Such high temperature can provoke serious damage to the package of a SRAM chip or a PCB board owing to melting. In contrast, a ΔV_T of 0.4 V is achievable by the back-bias of below 0.8 V. This reveals that the

forward back-biasing is more effective than increment of temperature to avoid the cold boot attack.

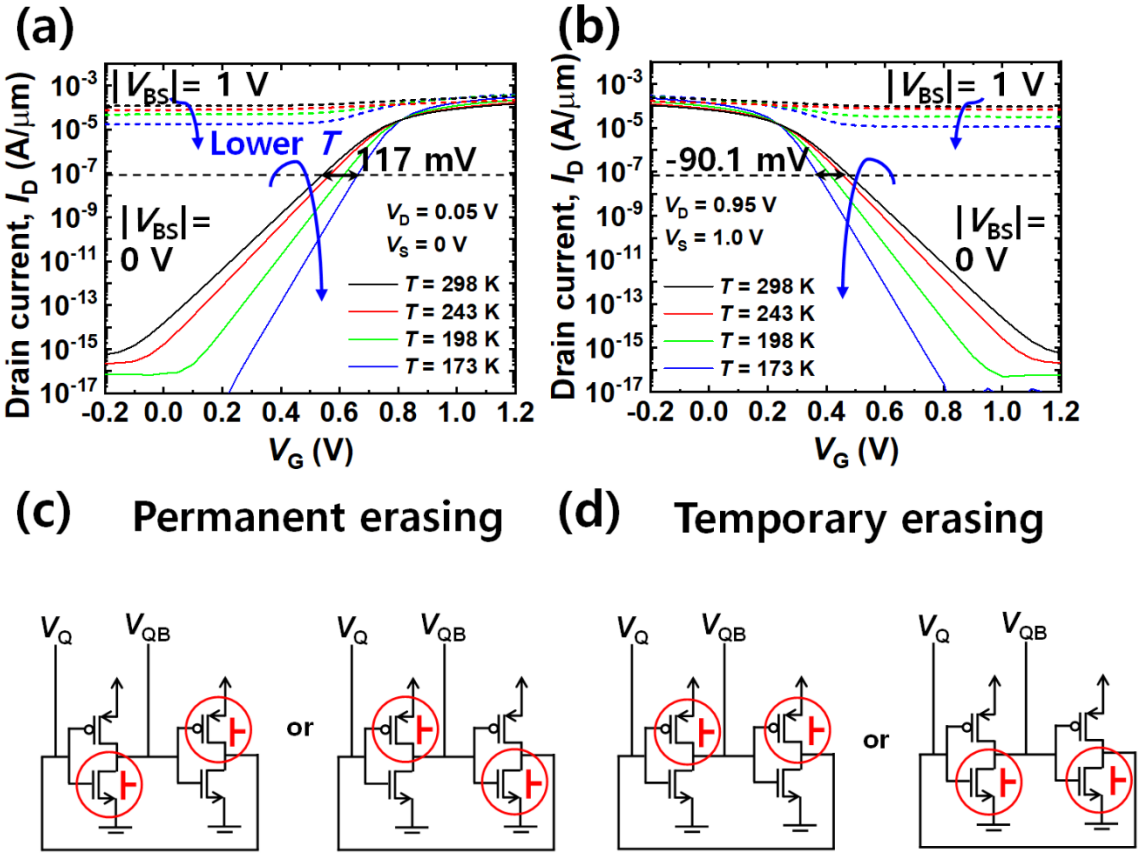


Figure 1. Transfer characteristics (I_D-V_G) and back-bias ($|V_{BS}|$) schemes in a SRAM cell. (a) Plot of I_D-V_G in NMOS. (b) Plot of I_D-V_G in PMOS. (c) Schematic of asymmetric back-biasing for permanent erasing. (d) Schematic of symmetric back-biasing for temporary erasing.

Using the modeled CMOS, a SRAM cell was designed to examine the feasibility of data sanitization by forward back- biasing. The behaviors of the SRAM sanitization were verified using a SILVACO ATLAS mixed-mode TCAD simulation. The supply voltage (V_{DD}) for SRAM operation was set to 1 V. For permanent erasing, asymmetric forward back-bias was applied to the NMOS of the left inverter and the PMOS of the right inverter or *vice versa*, as depicted in Figure 1(c). Note that the magnitude of the forward back-bias is the same for the NMOS and the PMOS, whereas they have opposite voltage polarity. In this case, the initial data

state can be reset to '0' or '1'. For temporary erasing, symmetric forward back-bias was applied to the PMOS of both inverters or the NMOS of both inverters, as depicted in Figure 1(d). In this case, the latch state locked in both inverters can be distorted when initially off-state PMOSs or NMOSs are turned on not by gate bias but by the applied back-bias, as shown in Figure 1(a) and (b).

Results and Discussion

A. Permanent Erasing

Figure 2 shows the results of permanent erasing by use of forward back-biasing at room temperature. Figure 2(a) and (b) show the bit line voltage (V_Q) and bit bar line voltage (V_{QB}) when '0' was stored initially. Note that V_Q and V_{QB} have contrasted voltage levels for the same data state. For example, V_Q and V_{QB} have 0 V and 1 V for the data state '0', respectively. V_Q and V_{QB} are changed by the applied forward back-bias ($|V_{BS}|$). When positive V_{BS} was forwardly applied to the NMOS of the left inverter and negative V_{BS} was forwardly applied to the PMOS of the right inverter with the same magnitude of more than 0.9 V (Figure 1(c)), the initial V_Q of 0 V was changed to 1 V and the initial V_{QB} of 1 V was changed to 0 V. Therefore, the initial '0' was pulled up to a final '1'. Figure 2(c) and (d) show V_Q and V_{QB} when '1' was stored initially. With the same forward back-biasing, as shown in Figure 2(a) and (b), V_Q was maintained as 1 V and V_{QB} also remained at 0 V. Hence the initial '1' was sustained as final '1'. As a consequence, stored data were reset to '1' *en bloc*, regardless of the initial data state. Figure 3 (a) and (b) show simplified data diagrams and corresponding circuits for the permanent erasing. The erased states to '1' were sustained even after the back-biasing was removed, as shown in Figure 3(a). In contrast, '0' and '1' were reset to '0' *en bloc*, as another permanent erasing when the forward back-bias was applied to the PMOS of the left inverter and the NMOS of the right inverter, as shown in Figure 3(b).

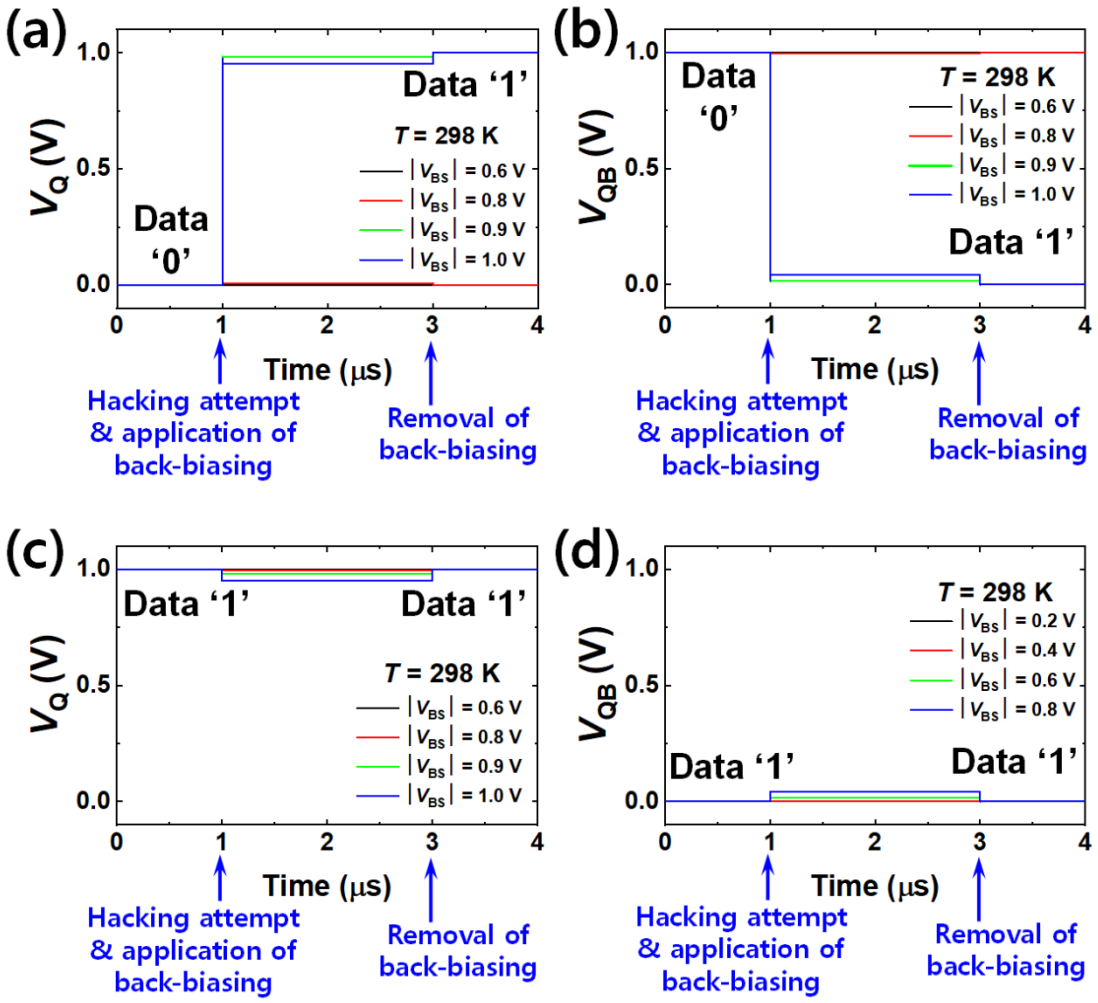


Figure 2. Permanent erasing characteristics at room temperature (298 K). (a) Bit line voltage (V_Q) for various $|V_{BS}|$ with transition from '0' to '1'. (b) Bit bar line voltage (V_{QB}) for various $|V_{BS}|$ with transition from '0' to '1'. (c) V_Q for various $|V_{BS}|$ with stay from '1' to '1'. (d) V_{QB} for various $|V_{BS}|$ with stay from '1' to '1'.

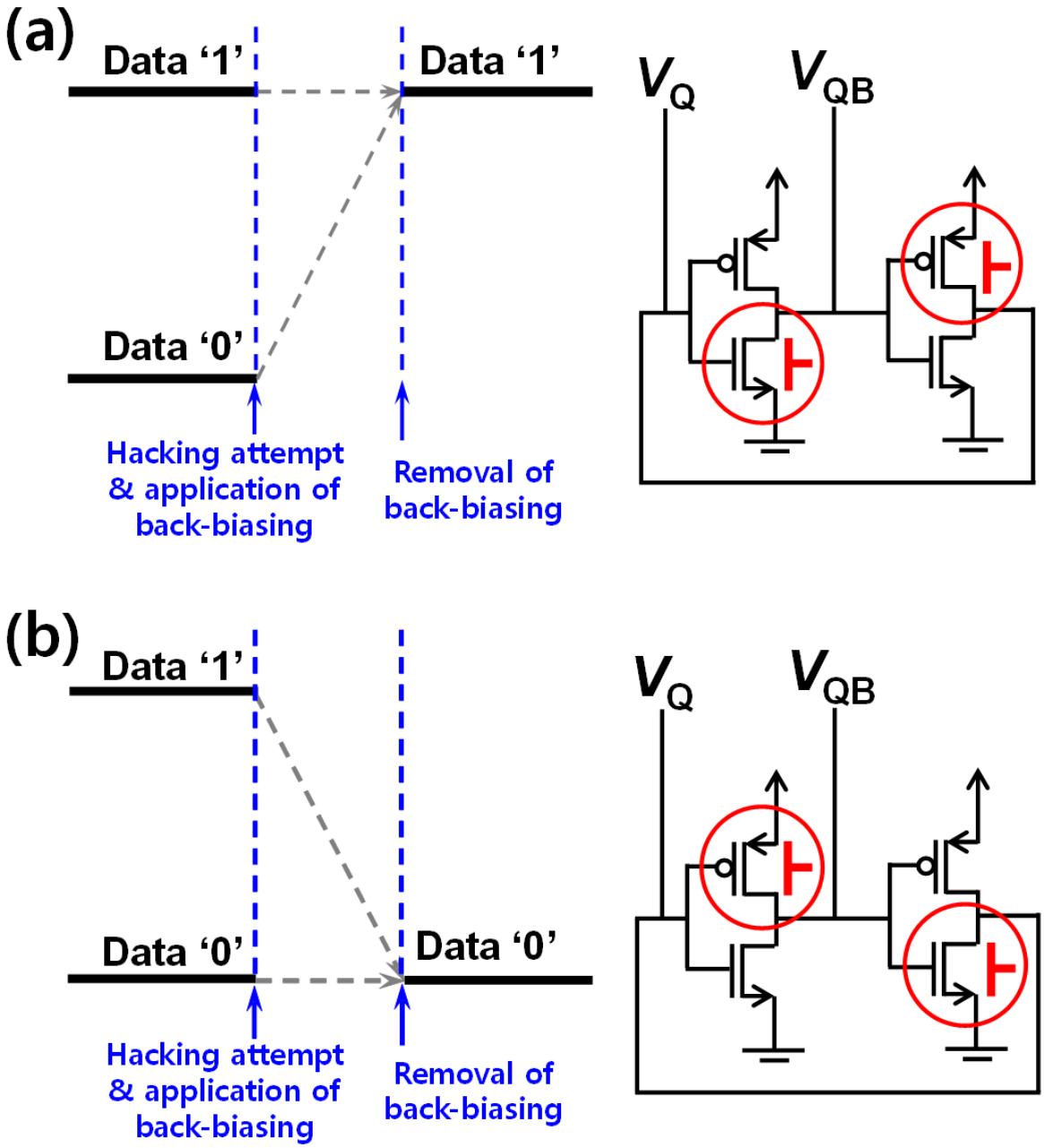
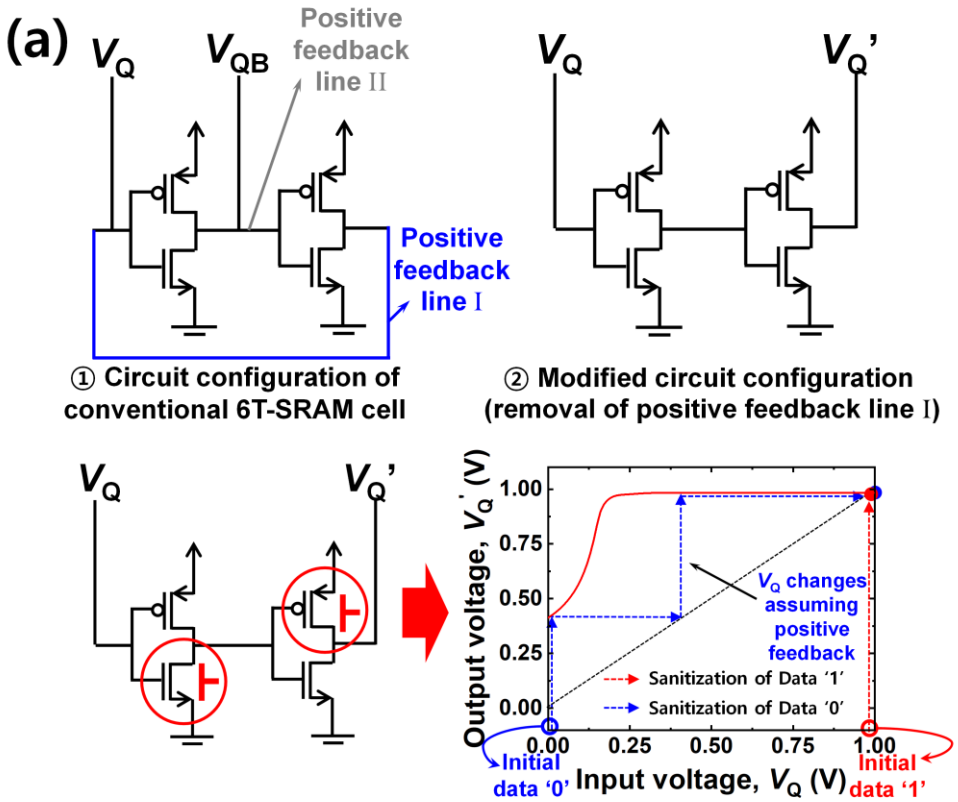


Figure 3. Simplified data diagram with the asymmetric forward back-biasing scheme for permanent erasing. (a) All the data are reset to '1'. (b) All the data are reset to '0'. Whether all the data were reset to '1' or '0' is determined according to the asymmetric forward back-biasing scheme.

A body terminal in a MOSFET can serve as a secondary gate (pseudo-gate), while an actual gate terminal can operate as a primary gate. Herein when an initially off-state MOSFET in an

inverter was turned on by the applied back-bias, the latch state in the cross-coupled inverters was notably distorted. Figure 4 explains how the latch state is distorted and thereby data are permanently erased to state '1'. The configuration of a 6T-SRAM cell was intentionally modified to analyze the distortion of the latch state. Figure 4(a) and (b) show the modified circuit configuration and its input-output voltage transfer curve (VTC) with the back-biasing. Two positive feedback lines, I and II, are separately removed from the conventional 6T-SRAM cell. Thereafter, forward back-bias was applied to the modified cell in order to extract the distorted VTC of V_Q and V_{QB}. V_Q' and V_{QB}' were defined as the output voltage through two inverters that receive input V_Q and V_{QB}, respectively. In the case where positive feedback line I is removed, shown in Figure 4(a), the blue rectilinear dashed-line in the VTC graph shows how V_Q is changed, when data '0' was initially stored in the modified VTC graph. The initial V_Q of 0 V (data '0') was pulled up to 1 V (data '1') by the removal of positive feedback line I. The red vertical dashed-line in the VTC graph shows how V_Q is changed, when data '1' was initially stored. The initial V_Q of 1 V (data '1') was maintained by the removal of positive feedback line I. Therefore, the permanent data erasing can proceed by making both data '0' and '1' into '1'. In the case of removing positive feedback line II, shown in Figure 4(b), the blue rectilinear dashed-line in the VTC graph shows how V_{QB} is changed, when data '0' was initially stored. The initial V_{QB} of 1 V (data '0') was pulled down to 0 V (data '1') by the removal of positive feedback line II. The red vertical dashed-line in the VTC graph shows how V_{QB} is changed, when data '1' was initially stored. The initial V_{QB} of 0 V (data '1') was maintained by removing positive feedback line II. Therefore, the permanent data erasing can also proceed by making both data '0' and '1' into '1'. While the other permanent data erasing shown in Figure 3(b) is not explained, it similarly works as described above. In this case, all the data of '0' and '1' can be reset to '0'.


(a)
V_Q
V_{QB}
Positive feedback line II
Positive feedback line I
V_Q
V_Q'
① Circuit configuration of conventional 6T-SRAM cell
② Modified circuit configuration (removal of positive feedback line I)
V_Q
V_Q'
③ Modified circuit configuration with back-biasing
Output voltage, V_Q' (V)
1.00
0.75
0.50
0.25
0.00
V_Q changes assuming positive feedback
Sanitization of Data '1'
Sanitization of Data '0'
0.00
0.25
0.50
0.75
1.00
Initial data '0'
Input voltage, V_Q (V)
Initial data '1'
Input-output VTC of modified circuit with back-biasing

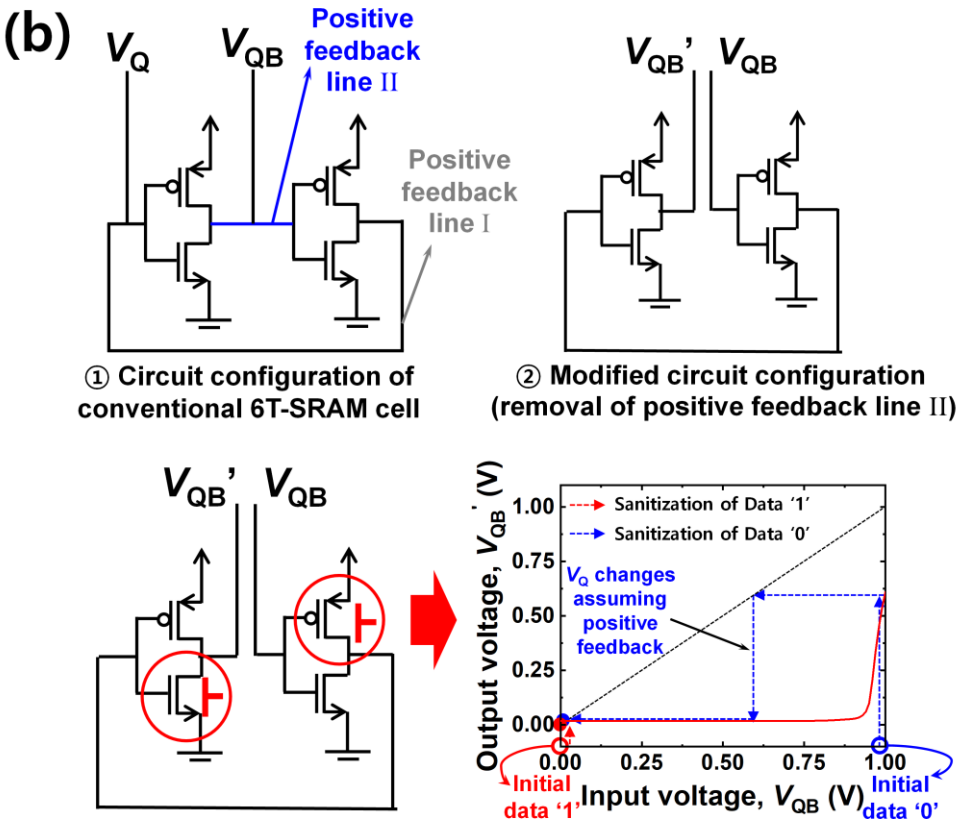

(b)
V_Q
V_{QB}
Positive feedback line II
Positive feedback line I
V_{QB}'
V_{QB}
① Circuit configuration of conventional 6T-SRAM cell
② Modified circuit configuration (removal of positive feedback line II)
V_{QB}'
V_{QB}
③ Modified circuit configuration with back-biasing
Output voltage, V_{QB}' (V)
1.00
0.75
0.50
0.25
0.00
Sanitization of Data '1'
Sanitization of Data '0'
V_Q changes assuming positive feedback
0.00
0.25
0.50
0.75
1.00
Initial data '1'
Input voltage, V_{QB} (V)
Initial data '0'
Input-output VTC of modified circuit with back-biasing

Figure 4. Modified configuration of a 6T-SRAM cell with its corresponding input-output voltage transfer curve (VTC) by asymmetric forward back-biasing for permanent erasing to state '1'. (a) Circuit diagrams with two conventional positive feedback lines (I & II) and without positive feedback line I and the VTC in terms of bit line voltage (V_Q) to show distorted latch in SRAM. The initial V_Q of 0 V (data '0') and 1 V (data '1') were changed to 1 V (data '1'). (b) Circuit diagrams with two conventional positive feedback lines (I & II) and without positive feedback line II and the VTC in terms of bit bar line voltage (V_{QB}) to show distorted latch in SRAM. The initial V_{QB} values of 1 V (data '0') and 0 V (data '1') were changed to 0 V (data '1'). All the data are reset to '1'.

In order to resist a cold boot attack, the proposed data erasing by forward back-biasing must be available in a low temperature environment. Therefore, it was confirmed that permanent data erasing was achievable at low temperatures down to 173 K [6], [7]. The abovementioned cryogenic (CRYO) model was used for accurate physics-based low temperature simulations. Figure 5(a) and (b) show V_Q and V_{QB} when data '0' was initially stored, and Figure 5(c) and (d) exhibit V_Q and V_{QB} when data '1' was initially stored for various temperatures ranging from 173 K to 298 K. The data was reset to '1' by the forward back-biasing even at T of 173 K. This is because ΔT (=T_{room} - T_{low}) of 125 K (=298 K – 173 K) makes a small positive ΔV_T of 0.12 V and ΔV_{BS} (=$V_{BS,GND}$ - $V_{BS,FWD}$) of -1 V (=0 V – 1 V) induces a large negative ΔV_T of 0.66 V in an NMOS; *i.e.*, the V_T change by the forward back-biasing overwhelms the V_T change by the temperature.

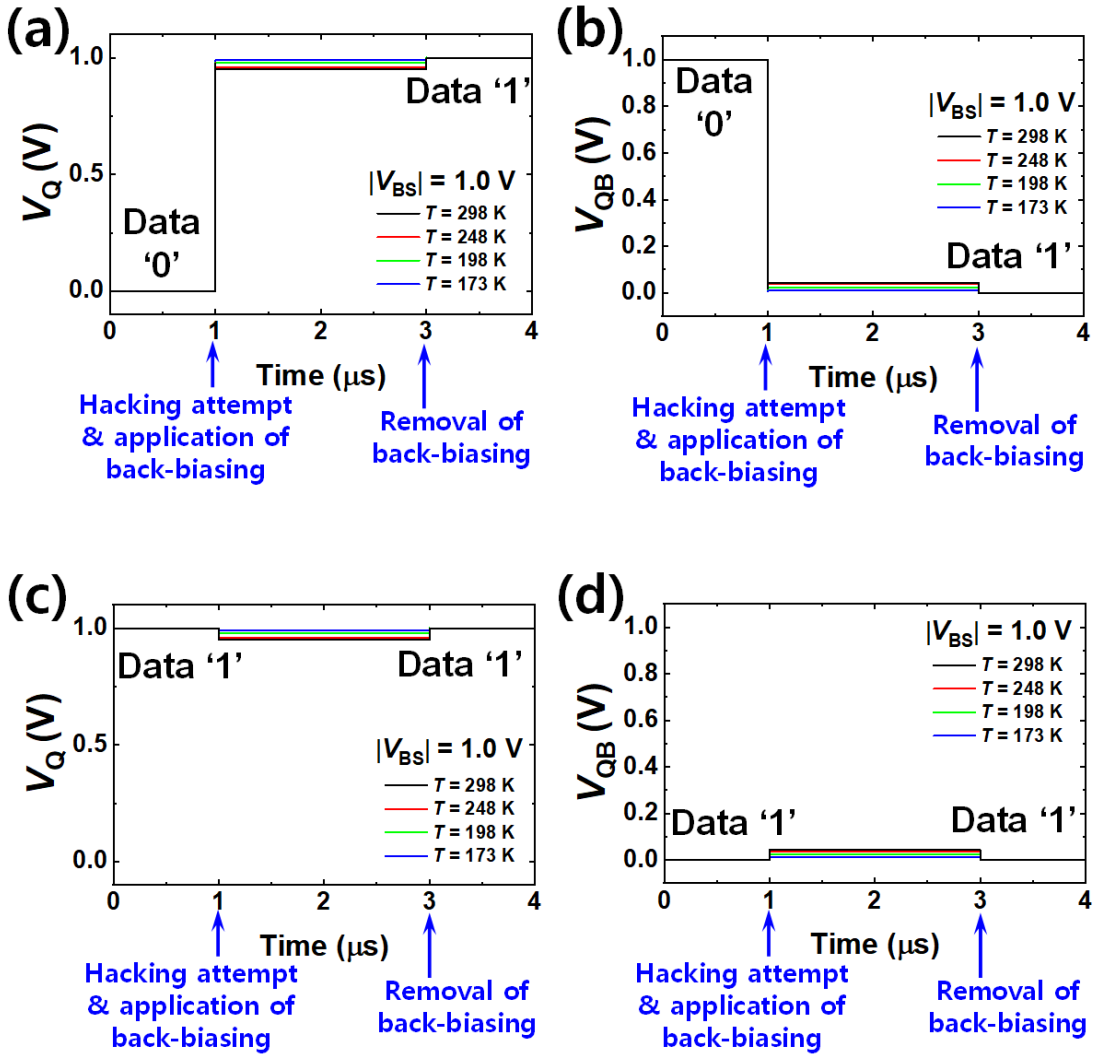


Figure 5. Temperature-invariant data distortion by permanent erasing with $|V_{BS}|$ of 1 V. (a) and (b) are for when the initial data was '0'. (c) and (d) are for when the initial data was '1'. (a) Distorted V_Q from '0' to '1' for various T. (b) Distorted V_{QB} from '0' to '1' for various T. Data '0' was changed to data '1' regardless of T. (c) Distorted V_Q with stay of '1' for various T. (d) Distorted V_{QB} with stay of '1' for various T. Data '1' was maintained regardless of T. All the data were reset to '1'-state after the permanent erasing even at low T against the cold boot attack.

Figure 6(a) shows how the erasing time varies according to the load capacitance (C_L) connected to each inverter. The erasing time is increased by prolonged RC delay, as C_L is

increased. Nonetheless, ultra-fast data sanitization within 5 ns was confirmed even for a C_L of 1 pF, which is larger than a nominal C_L below 100 fF [17] at the 32 nm node. Note that the erasing time can be further shortened by increment of $|V_{BS}|$. Figure 6(b) shows the erasing time influenced by C_L for various temperatures. Ultra-fast erasing within 5 ns is also achievable even at 173 K (Supplementary Figure S1(a)). This implies that the proposed bask-biasing scheme can resist the cold boot attack.

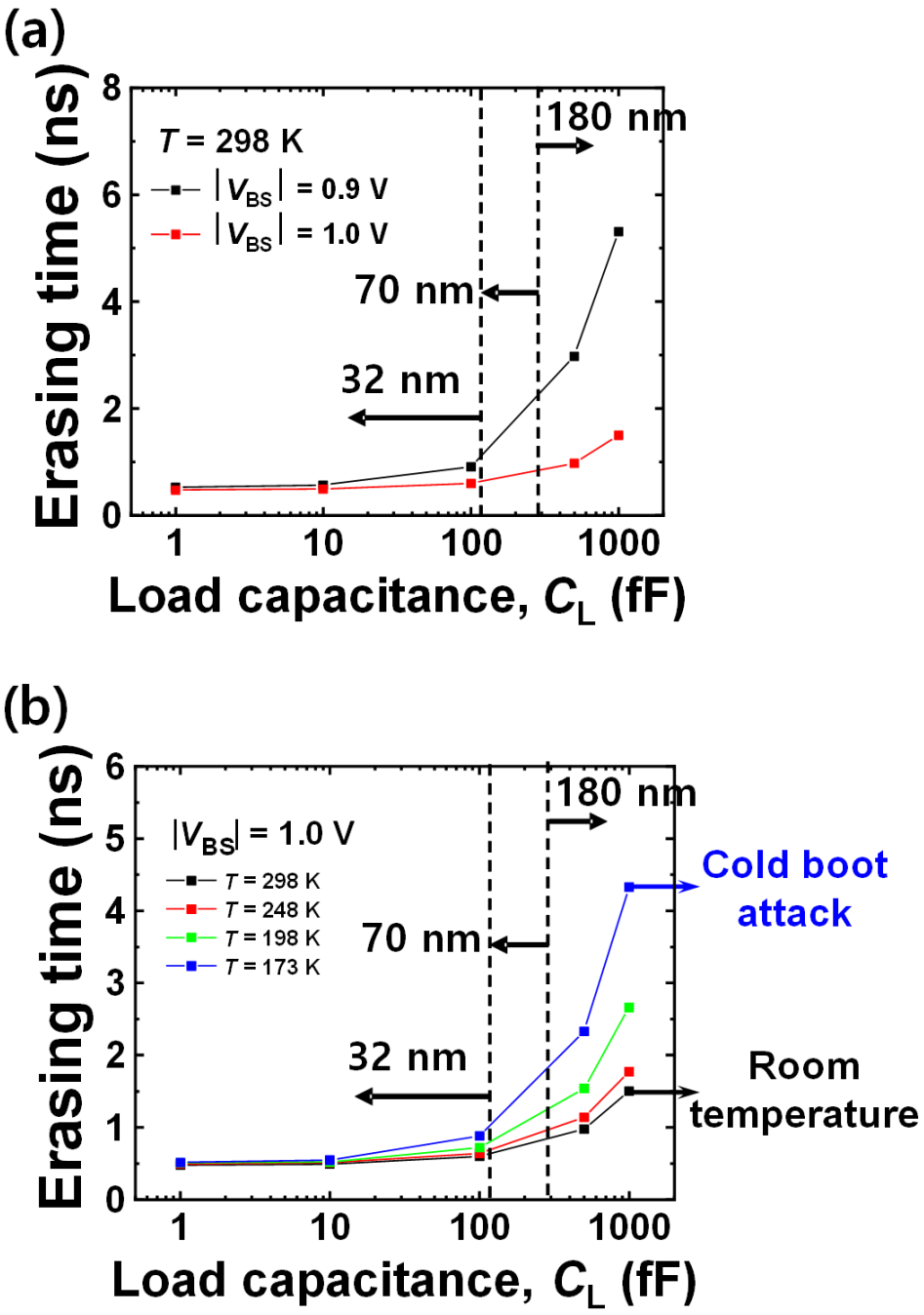


Figure 6. Erasing time versus load capacitance for various technology nodes: 32 nm, 70 nm and 180 nm. (a) Erasing time as a function of load capacitance (C_L) for various $|V_{BS}|$ at room temperature (T = 298 K). (b) Erasing time as a function of C_L for various T at $|V_{BS}|$ = 1.0 V. Ultra-fast data sanitization within 5 ns was possible regardless of T even for a C_L of 1 pF.

Meanwhile, if $|V_{BS}|$ is larger than the built-in potential (~0.8 V) of the p-n junction at the source and drain, a forward junction current ($I_{j,FWD}$) is flown [18]. From the simulation, $I_{j,FWD}$ values of 0.29 mA and 2.13 mA were flown for $|V_{BS}|$ of 0.9 V and 1 V, respectively. Accordingly, power consumption for the permanent erasing was extracted as 0.58 mW and 4.26 mW for the $|V_{BS}|$ of 0.9 V and 1 V, respectively. However, the energy consumption for the permanent erasing could be reduced to an order of pJ. This is because shorter time than 5 ns is sufficient to delete the data in the ultra-fast sanitization.

B. Temporary Erasing

Figure 7 shows the results of the temporary erasing with forward back-biasing at room temperature. Figure 7(a) and (b) show V_Q and V_{QB} when '0' and '1' were respectively stored. They were modulated by the applied V_{BS}. When negative V_{BS} (*i.e.*, forward back-biasing) applied to both PFETs in two inverters was increased, the voltage margin (V_{margin}) between V_Q and V_{QB} was narrowed. Note that the minimal V_{margin} for normal reading operation in SRAM is 0.25 V to distinguish '0' and '1' [19]. From the simulation, the corresponding value was 0.22 V at a $|V_{BS}|$ of 0.93 V. Thus, the latched data state in the SRAM cell is seriously distorted to the point of being illegible because its V_{margin} is smaller than 0.25 V. Figure 7(c) shows a simplified data diagram of the temporary erasing. When V_{margin} is small enough to be indistinguishable, a hacker cannot read the data. On the other hand, unreadable data by temporary erasing can be promptly recovered to their original states by removing the back-bias after the threat of the

attack has disappeared. Figure 7(d) shows the erasing time of the temporary erasing, which was affected by C_L. The data sanitization could be accomplished within 15 ns, which is sufficiently fast. The slight difference between temporary erasing time and permanent erasing time is attributed to the different back-bias scheme. Recall that symmetric back-biasing was applied for the temporary erasing and asymmetric back-biasing was applied for the permanent erasing. This results in a dissimilar *RC* delay affecting the time to distort the stored data in SRAM.

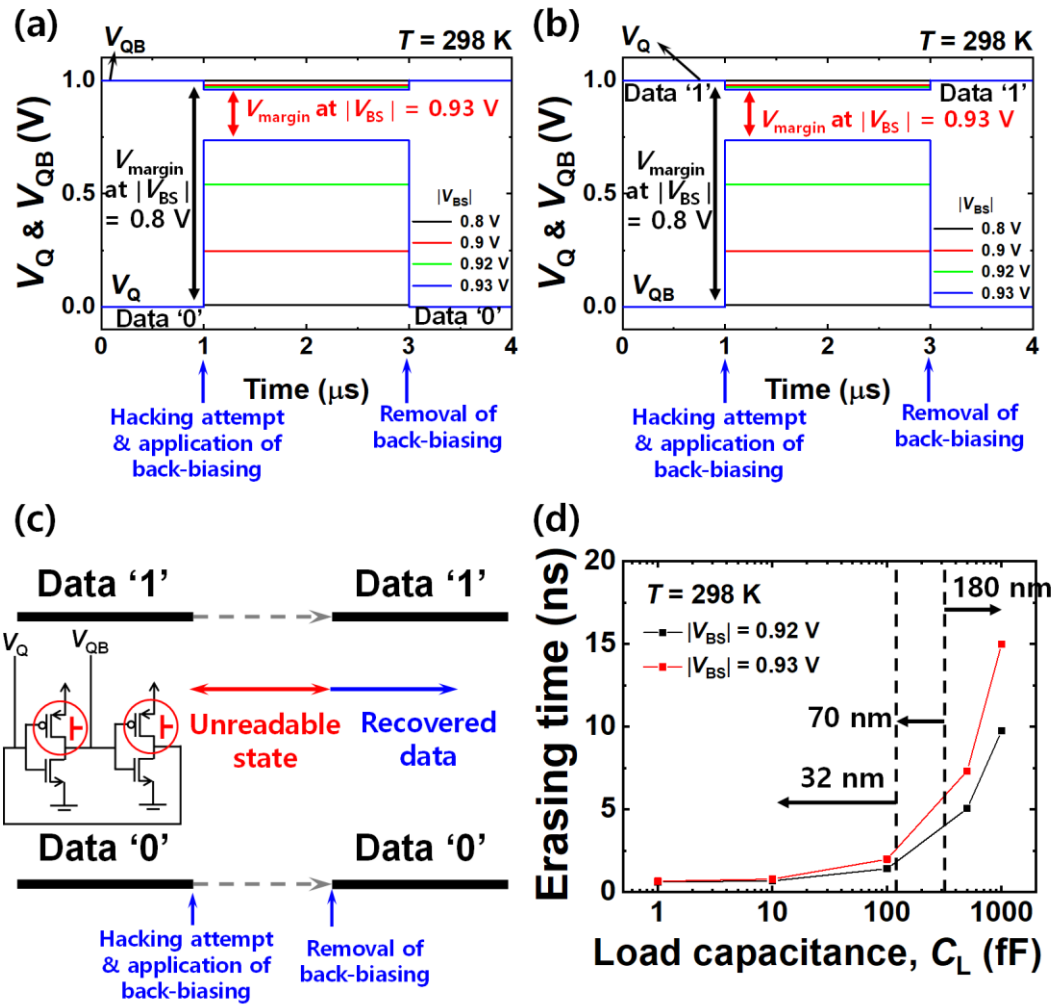


Figure 7. (Temporary erasing) Bit line voltage (V_Q) and bit bar line voltage (V_{QB}) depending on the $|V_{BS}|$ at T = 298 K, when the initial data was (a) '0' and (b) '1'. V_{margin} reduction was achieved by applied $|V_{BS}|$. (c) Simplified data diagram with the asymmetric forward back-biasing scheme for temporary erasing. (d) Erasing time versus load capacitances for various technology nodes: 32 nm, 70 nm and 180 nm.

Like the permanent erasing by the aforementioned asymmetric back-biasing, the temporary erasing can also partially disturb the latch state by symmetric back-biasing. However, the level of the disturbance in the temporary erasing is small compared with that in the case of permanent erasing. Figure 8 shows how much the latch state is disturbed by the temporary erasing and thereby data become temporarily unreadable. Figure 8(a) and (b) show the modified circuit configuration and its input-output VTC with the back-biasing. Being done at Figure 4, two positive feedback lines I and II were also individually removed from the conventional 6T-SRAM cell, as depicted in each circuit diagram of Figure 8. Thereafter, forward back-bias was applied to the modified SRAM cell in order to extract the distorted VTC of V_Q and V_{QB}. V_Q' and V_{QB}' were defined as the output voltage through the modified cross-coupled inverters that receive input V_Q and V_{QB}, respectively. Referring to the VTC graph from Figure 8(a), the blue rectilinear dashed-line shows how much V_Q is changed, when data '0' was initially stored. The initial V_Q of 0 V (data '0') was pulled up to 0.73 V by removing positive feedback line I. The red vertical dashed-line in the VTC graph shows how V_Q is changed, when data '1' was initially stored. The initial V_Q of 1 V (data '1') was pulled down to 0.95 V by the removed positive feedback line I. Likewise, referring to the VTC graph in Figure 8(b), the blue vertical dashed-line shows how much V_{QB} is changed, when data '0' was initially stored. The initial V_{QB} of 1 V (data '0') was pulled down to 0.95 V by removal of positive feedback line II. The red rectilinear dashed-line in the VTC graph shows how much V_{QB} is changed, when data '1' was initially stored. The initial V_{QB} of 0 V (data '1') was pulled up to 0.73 V by removal of positive feedback line II. Therefore, V_{margin} becomes 0.22 V (=0.95 V - 0.73 V) for both temporary erasing of data '0' and '1'. Herein V_Q of 0.73 V and V_{QB} of 0.95 V (or *vice versa*) are too ambiguous to be classified as one of a binary data state: 0 V and 1 V. Moreover, the temporarily disturbed V_Q and V_{QB} by the abovementioned pulled-up or pulled-down operation could be recovered to their initial states by removal of the back-biasing, because the final order of V_Q >

V_{QB} or $V_Q < V_{QB}$ inherited from their initial order was not reversed.

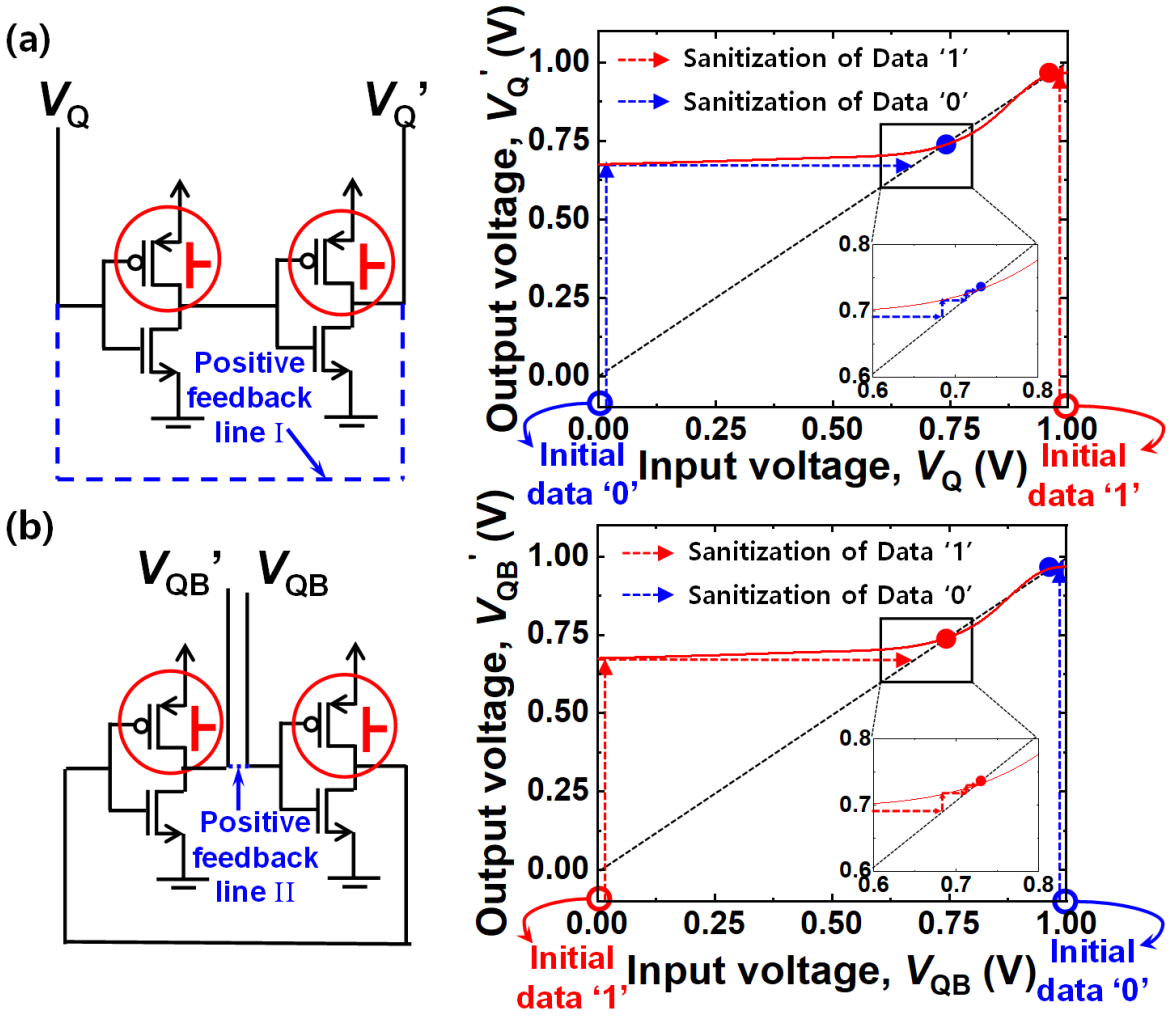


Figure 8. Modified configuration of a 6T-SRAM cell with its corresponding input-output voltage transfer curve (VTC) by symmetric forward back-biasing for temporary erasing. (a) Circuit diagram without positive feedback line I and its VTC in terms of bit line voltage (V_Q) to show partially distorted latch. The initial V_Q values of 0 V (data '0') and 1 V (data '1') were changed to 0.73 V and 0.95 V, respectively. (b) Circuit diagram without positive feedback line II and its VTC in terms of bit bar line voltage (V_{QB}) to show partially distorted latch. The initial V_{QB} values of 1 V (data '0') and 0 V (data '1') were changed to 0.95 V and 0.73 V, respectively. V_{margin} of 0.22 V is achieved for both temporary erasing of data '0' and '1'.

The temporary erasing at low temperature was also investigated with simulations to confirm whether it can resist the cold boot attack. Figure 9(a) and (b) show V_Q and V_{QB} depending on the temperature, when a $|V_{BS}|$ of 0.93 V was applied. This is the condition where the temporary erasing worked at room temperature. As the temperature was decreased to 173 K, V_{margin} was notably widened to nearly 1V again. Thus, data sanitization by the temporary erasing could not be accomplished. This vulnerability to low temperature can be mitigated by increasing $|V_{BS}|$. Figure 9(c) and (d) show V_Q and V_{QB} as a function of $|V_{BS}|$ at 173 K. As $|V_{BS}|$ was increased, V_{margin} narrowed. Temporary erasing time within 5 ns was also achievable even at 173 K (Supplementary Figure S1(b)). Conclusively, it is confirmed that the temporary erasing as well as the permanent erasing can resist the cold boot attack by the forward back-biasing.

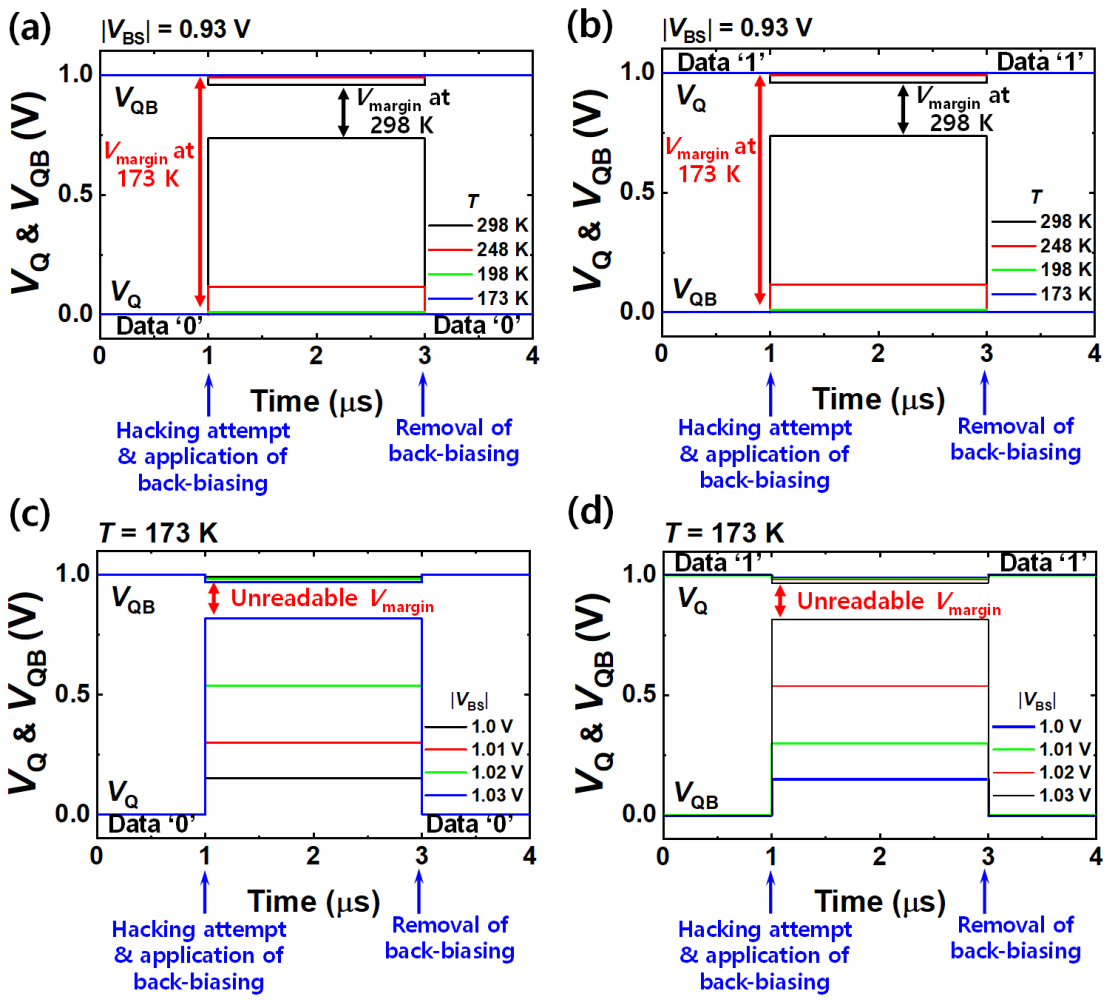


Figure 9. Temperature-variant partial data distortion by temporary erasing for various $|V_{BS}|$. (a) V_Q and V_{QB} for various temperatures at $|V_{BS}|$ of 0.93 V, when the initial data was '0'. (b) V_Q and V_{QB} for various temperatures at $|V_{BS}|$ of 0.93 V, when the initial data was '1'. At 173 K, widened V_{margin} (close to 1 V) under $|V_{BS}|$ of 0.93 V is vulnerable to a hacking attempt. (c) V_Q and V_{QB} for various $|V_{BS}|$ at 173 K, when the initial data was '0'. (d) V_Q and V_{QB} for various $|V_{BS}|$ at 173 K, when the initial data was '1'. Temporary erasing is possible even at low temperature by further increment of $|V_{BS}|$.

It should be noted that the proposing data sanitization requires a new layout scheme in order to separately apply the back-bias. Supplementary Figure S2(a) shows a conventional layout of high-density 6T-SRAM. According to the conventional 6T-SRAM layout, two pull-up (PU) PFETs share the same N-type well so that it is impossible to provide different back-bias for each PU PFET. In order to provide back-bias to only one of the PU PFET, the layout innovation is required. Supplementary Figure S2(b) shows a possible layout innovation to realize individual back-biasing by using two N-type wells, which are separated by a slim P-type well. In addition, as shown in Supplementary Figure S2(a), pull-down (PD) NFET and pass-gate (PG) NFET share the same P-type well. Therefore, if the back-bias is applied to the P-type well, the back-bias will influence on the PG and PD NFET together because they are located in the same well. One of the solutions is to apply negative voltage to the GND node rather than to apply positive voltage to the P-type well for the back-biasing. More specifically, if the GND is divided to GND1 and GND2 as shown in the Supplementary Figure S2(b), two PD NFETs can be biased individually. The cross-sections of conventional layout of high-density 6T-SRAM and possible layout innovation to realize proposed data sanitization scheme are shown in Supplementary Figure S3.

Conclusion

For a security system, ultra-fast data sanitization for SRAM was demonstrated with forward back-biasing, which did not require any extra circuit. The simulation study confirmed that this strategy could resist the cold boot attack. The latch states in SRAM were distorted by the forward back-biasing in order to reset data or make data unreadable against hacking. The level of the distortion was modulated by various back-biasing schemes. Symmetric back-biasing to two PMOS supported recoverable temporary erasing. Furthermore, asymmetric back-biasing to the PMOS in one inverter and to the NMOS in the other inverter facilitated irrecoverable permanent erasing. According to the level of the hacking threat, either permanent erasing or temporary erasing can be chosen by an end user. Based on the physics-based ATLAS device simulations, the possibility of data sanitization at low temperature down to 173 K in order to resist a cold boot attack was confirmed.

References

1 P. Gutmann, "Secure Deletion of Data from Magnetic and Solid-State Memory," *Proc. Sixth USENIX Security Symp.*, 1996.

2 K. Xiao, M. T. Rahman, D. Forte, Y. Huang, M. Su, and M. Tehranipoor, "Bit selection algorithm suitable for high-volume production of SRAM-PUF," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, pp. 101–106, May 2014. DOI: 10.1109/HST.2014.6855578.

3 A. Garg and T. T. Kim, "Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect," in *Proc. 2014 IEEE Int. Symp. Circuits and Systems*, pp. 1941–1944, June 2014. DOI: 10.1109/ISCAS.2014.6865541.

4 S. Skorobogatov, “Low temperature data remanence in static RAM”, Technical report UCAM-CL-TR-536, University of Cambridge Computer Laboratory, June 2002.

5 J. Hui-fang, Z. Xiao-bo, J. Xin-zhang, Y. Xue-ying, and Z. Zheng-yu, “The Characteristic Study of Data Remanence of SRAM,” *Research & Progress of SSE*, vol. 26, no. 4, pp. 536, 2006.

6 N. Anagnostopoulos, S. Katzenbeisser, M. Rosenstihl, A. Schaller, S. Gabmeyer, and T. Arul, “Low-temperature data remanence attacks against intrinsic SRAM PUFs,” in *Proc. Euromicro Conf. Digit. Syst. Des. (DSD)*, pp. 581–585, Aug. 2018. DOI: 10.1109/DSD.2018.00102.

7 N. Anagnostopoulos, T. Arul, M. Rosenstihl, A. Schaller, S. Gabmeyer, and S. Katzenbeisser, “Attacking SRAM PUFs using very-low-temperature data remanence,” *Microproc. Microsyst*. pp. 102864, Nov. 2019. DOI: 10.1016/j.micpro.2019.102864.

8 K. Wenjing, Y. Kai, Y. Guoyi, and Z. Xuecheng, “Novel Security Strategies for SRAM in Powered off State to Resist Physical Attack”, in *Proceedings of the International Symposium on Integrated Circuits*, pp. 298-301, 2009.

9 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. DOI: 10.1088/1674-4926/30/9/095010.

10 M.-J. Chen, J.-S. Ho, T.-H. Huang, C.-H. Yang, Y.-N. Jou, and T. Wu, “Back-gate forward bias method for low-voltage CMOS digital circuits,” *IEEE Trans. Electron Devices*, vol. 43, no. 6, pp. 904–910, Jun. 1996. DOI: 10.1109/16.502122.

11 M. Togo, T. Fukai, Y. Nakahara, S. Koyama, M. Makabe, E. Hasegawa, M. Nagase, T. Matsuda, K. Sakamoto, S. Fujiwara, Y. Goto, T. Yamamoto, T. Mogami, M. Ikeda, Y. Yamagata, and K. Imai, "Power aware 65 nm node CMOS technology using variable V_{DD} and back-bias control with reliability consideration for back-bias mode," in *Dig. Tech. Papers Symp. VLSI Technol.*, pp. 88–89, 2004. DOI: 10.1109/VLSIT.2004.1345409.

12 A. Keshavarzi, S. Ma, S. Narendra, B. Bloechel, K. Mistry, T. Ghani, S. Borkar, and V. De, "Effectiveness of reverse body bias for leakage control in scaled dual V_t CMOS ICs," in *Proc. Int. Symp. Low Power Electron*. pp. 207–212, Dec. 2001.

13 *Atlas User's Manual: Device Simulation Software*, Silvaco Int., Santa Clara, CA, USA, 2008.

14 S. Hanson, M. Seok, D. Sylvester, and D. Blaauw, "Nanometer device scaling in sub-threshold logic and SRAM," *IEEE Trans. Electron Devices*, vol. 55, no. 1, pp. 175–185, Jan. 2008. DOI: 0.1109/TED.2007.911033.

15 A. Becker, F. Jazaeri, and C. Enz, "Cryogenic MOSFET Threshold Voltage Model," in *Proc. 49th Eur. Solid-State Device Res. Conf. (ESSDERC)*, pp. 94–97, Sep. 2019, DOI: 10.1109/ESSDERC.2019.8901806.

16 R. M. Incandela, L. Song, H. A. R. Homulle, F. Sebastiano, E. Charbon, and A. Vladimirescu, "Nanometer CMOS characterization and compact modeling at deep-cryogenic temperatures," in *Proc. 47th Eur. Solid-State Device Res. Conf. (ESSDERC)*, pp. 58–61, Sep. 2017, DOI: 10.1109/ESSDERC.2017.8066591.

17 K. Kim, H. Mahmoodi, and K. Roy, "A Low-Power SRAM Using Bit-Line Charge-Recycling," in *Proc. Int. Symp. Low-Power Electron. Design*, pp. 446–459, Aug. 27, **DOI:** 10.1109/JSSC.2007.914294.

18 G.-B. Lee, C.-K. Kim, J.-Y. Park, T. Bang, H. Bae, S.-Y. Kim, S.-W. Ryu, and Y.-K. Choi, "A novel technique for curing hot-carrier-induced damage by utilizing the forward current of the PN-junction in a MOSFET," *IEEE Electron Device Lett.*, vol. 38, no. 8, pp. 1012–1014, Aug. 2017. DOI: 10.1109/LED.2017.2718583.

19 B. Zhai, S. Hanson, D. Blaauw, and D. Sylvester, "A variation-tolerant sub-200 mV 6-T subthreshold SRAM," *IEEE J. Solid-State Circuits*, vol. 43, no. 10, pp. 2338–2347, Oct. 2008. DOI: 10.1109/JSSC.2008.2001903.

Acknowledgements

This work was supported by the National Research Foundation (NRF) of Republic of Korea (2018R1A2A3075302, 2019M3F3A1A03079603, and 2020M3F3A2A01082592), and in part by IC Design Education Center (EDA Tool and MPW). S. -J. Han, J. -K. Han, G. –J. Yun, M. –W. Lee, J. -M. Yu and Y. -K. Choi are with the School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), 291 Daehak-ro, Daejeon 34141, Republic of Korea. (Seong-Joo Han and Joon-Kyu Han contributed equally to the manuscript.) (Corresponding author: Y.-K. Choi, e-mail: ykchoi@ee.kaist.ac.kr)

Author contributions

S.-J. Han and J.-K. Han equally contributed to this work. Y.-K. Choi conceived, supervised, and led the project. S.-J. Han, J.-K. Han and Y.-K. Choi designed the experiments and found a mechanism of the proposing SRAM data sanitization technique. G.-J Yun set up a cryogenic TCAD simulation, and M.-W Lee optimized the simulation environments. J.-M. Yu supported finding references related to security device including SRAM. S.-J. Han and J.-K. Han conducted the TCAD simulation and wrote the manuscript. All the authors interpreted data, contributed reviewing the manuscript, and approved the final version of the article.

Additional information

Supplementary information accompanies this paper at http://www.nature.com/

Scientificreports

Competing financial interests: The authors declare no competing interests.

Figures

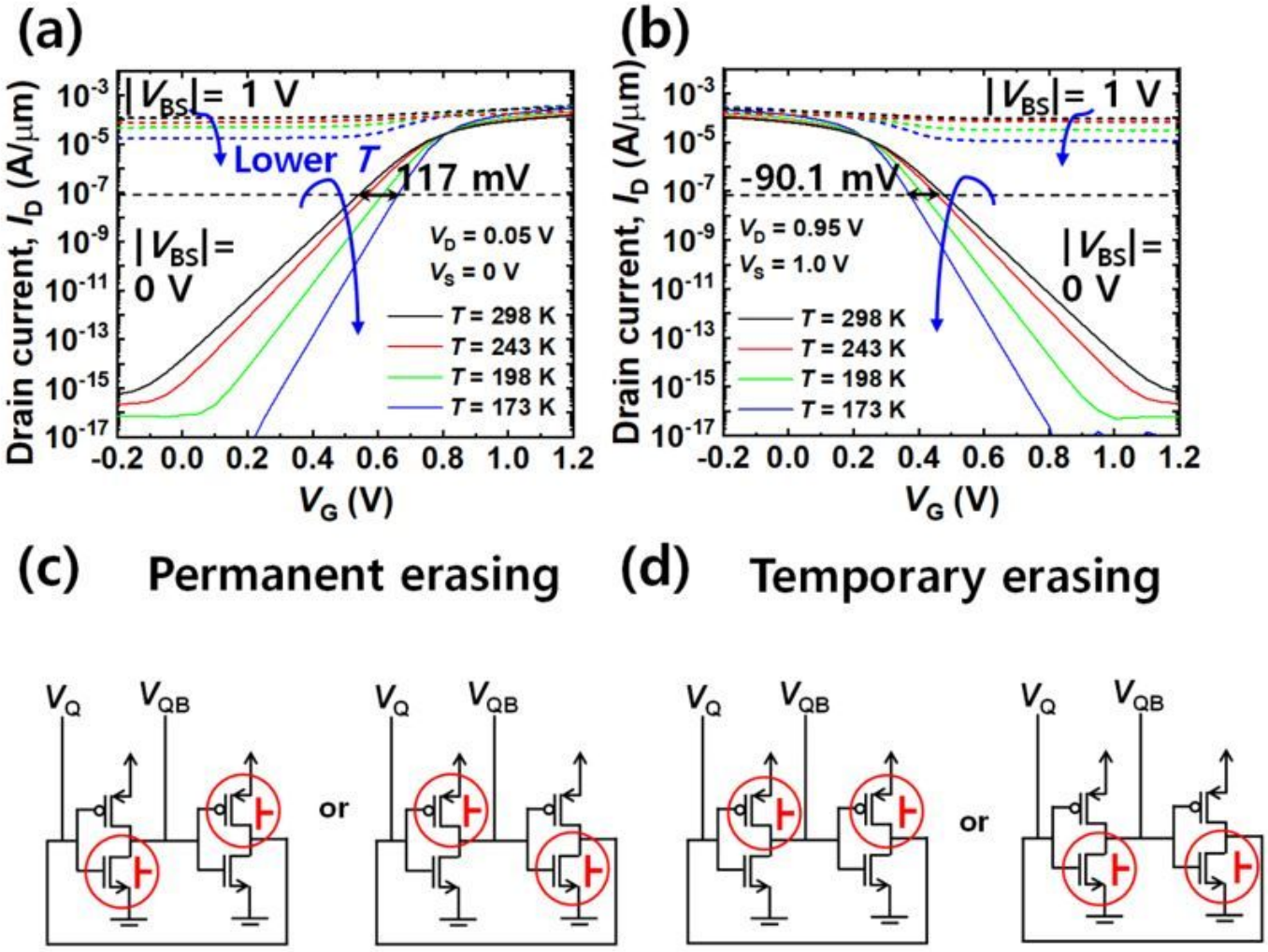


Figure 1

Transfer characteristics (ID-VG) and back-bias (|VBS|) schemes in a SRAM cell. (a) Plot of ID-VG in NMOS. (b) Plot of ID-VG in PMOS. (c) Schematic of asymmetric back-biasing for permanent erasing. (d) Schematic of symmetric back-biasing for temporary erasing.

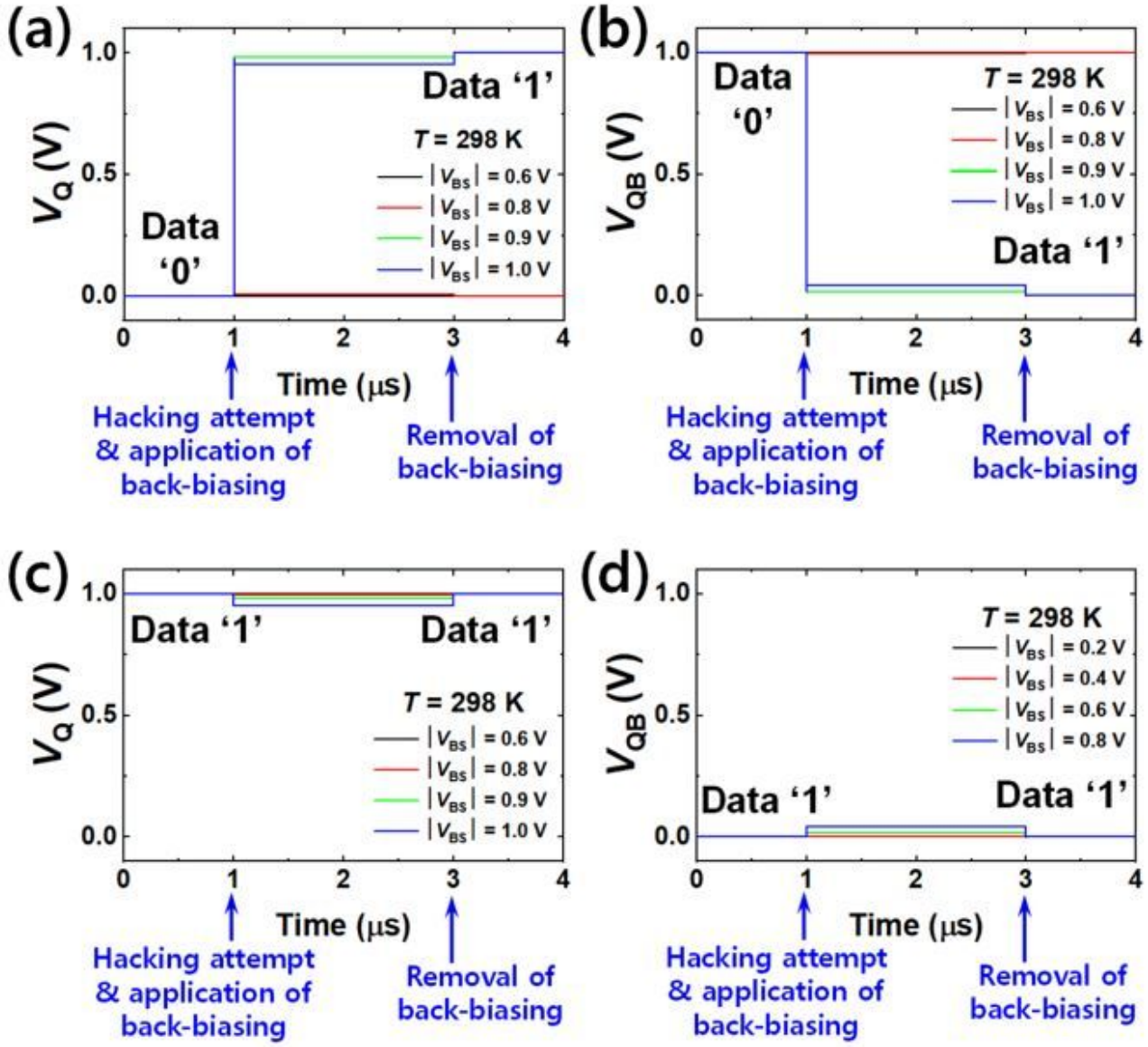


Figure 2

Permanent erasing characteristics at room temperature (298 K). (a) Bit line voltage (VQ) for various |VBS| with transition from '0' to '1'. (b) Bit bar line voltage (VQB) for various |VBS| with transition from '0' to '1'. (c) VQ for various |VBS| with stay from '1' to '1'. (d) VQB for various |VBS| with stay from '1' to '1'.

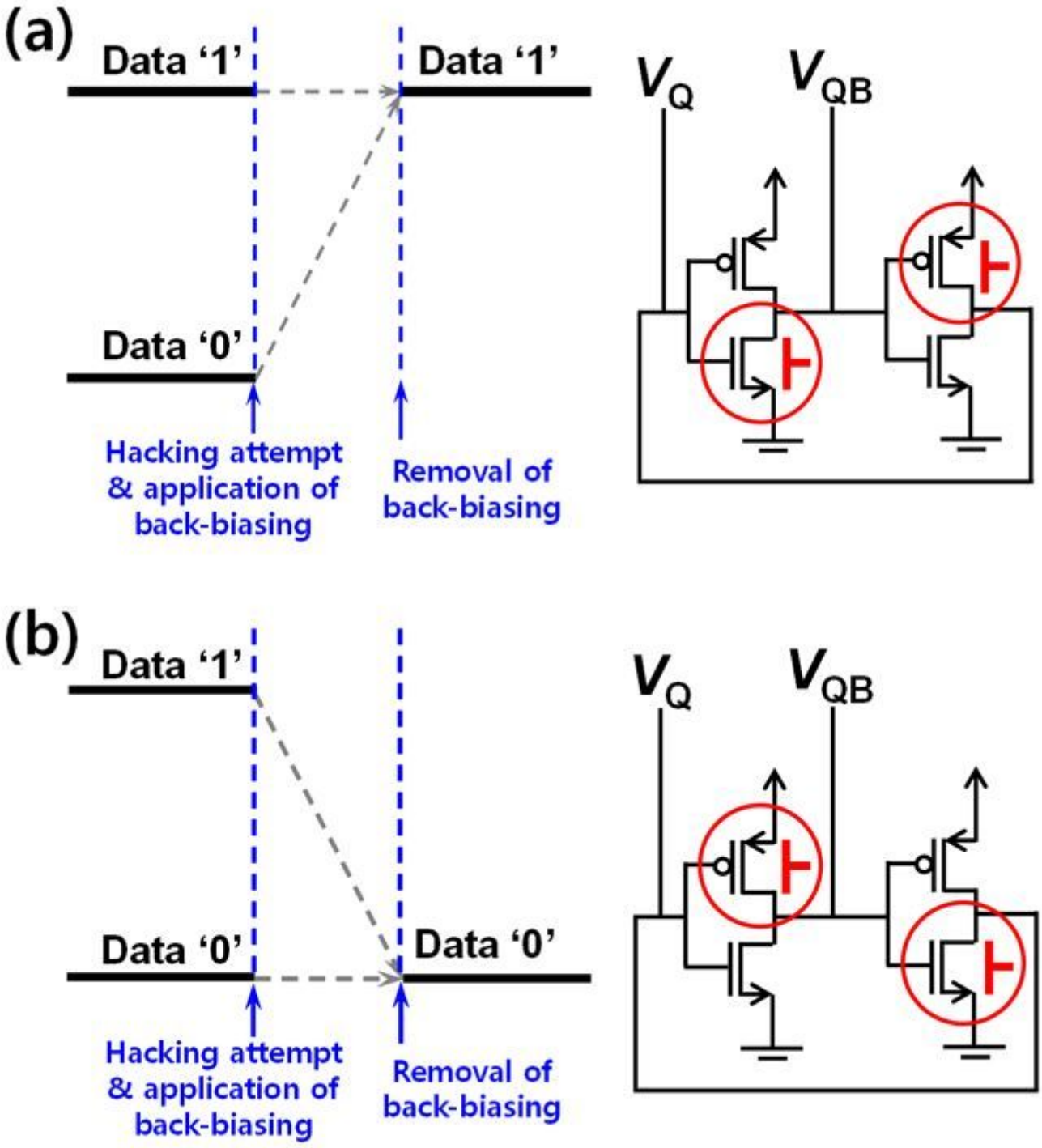


Figure 3

Simplified data diagram with the asymmetric forward back-biasing scheme for permanent erasing. (a) All the data are reset to '1'. (b) All the data are reset to '0'. Whether all the data were reset to '1' or '0' is determined according to the asymmetric forward back-biasing scheme.

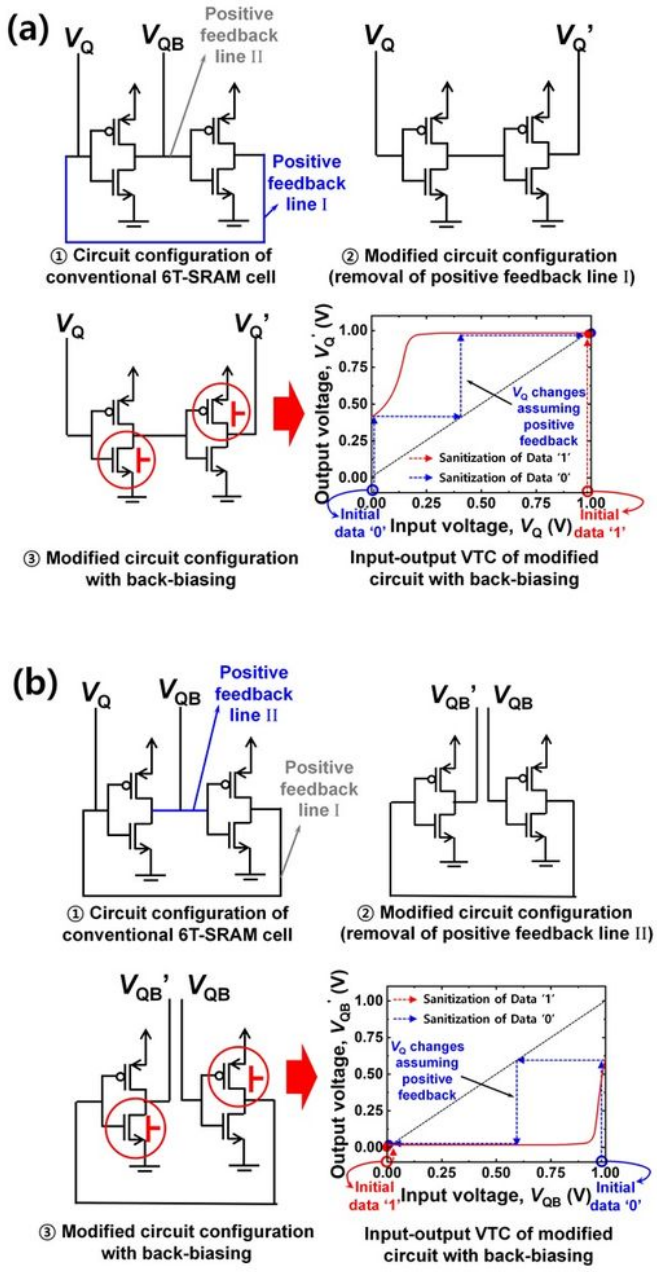


Figure 4

Modified configuration of a 6T-SRAM cell with its corresponding input-output voltage transfer curve (VTC) by asymmetric forward back-biasing for permanent erasing to state '1'. (a) Circuit diagrams with two conventional positive feedback lines (I & II) and without positive feedback line I and the VTC in terms of bit line voltage (VQ) to show distorted latch in SRAM. The initial VQ of 0 V (data '0') and 1 V (data '1') were changed to 1 V (data '1'). (b) Circuit diagrams with two conventional positive feedback lines (I & II)

and without positive feedback line II and the VTC in terms of bit bar line voltage (VQB) to show distorted latch in SRAM. The initial VQB values of 1 V (data ‘0’) and 0 V (data ‘1’) were changed to 0 V (data ‘1’). All the data are reset to ‘1’.

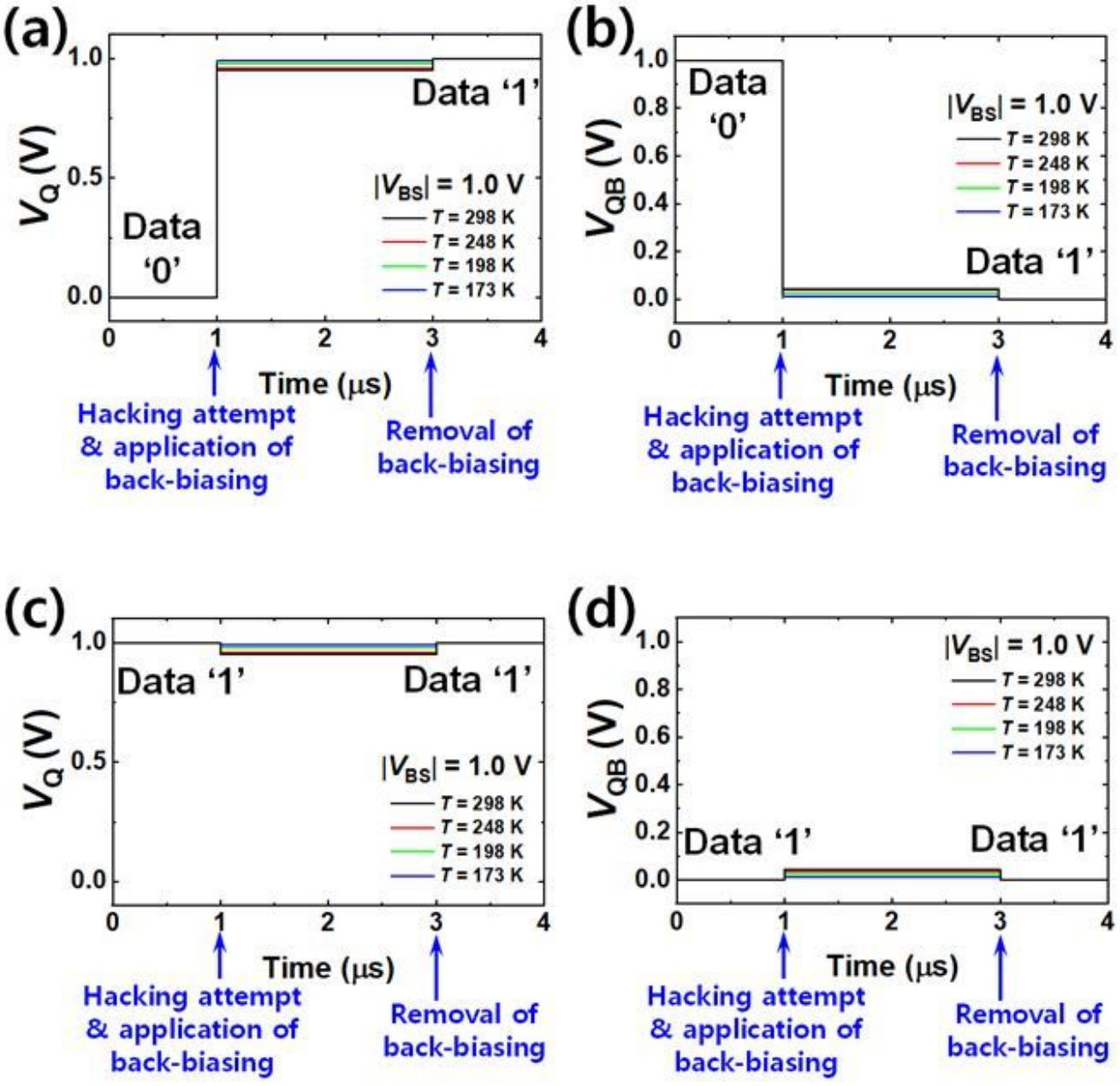


Figure 5

Temperature-invariant data distortion by permanent erasing with |VBS| of 1 V. (a) and (b) are for when the initial data was ‘0’. (c) and (d) are for when the initial data was ‘1’. (a) Distorted VQ from ‘0’ to ‘1’ for various T. (b) Distorted VQB from ‘0’ to ‘1’ for various T. Data ‘0’ was changed to data ‘1’ regardless of T. (c) Distorted VQ with stay of ‘1’ for various T. (d) Distorted VQB with stay of ‘1’ for various T. Data ‘1’ was maintained regardless of T. All the data were reset to ‘1’-state after the permanent erasing even at low T against the cold boot attack.

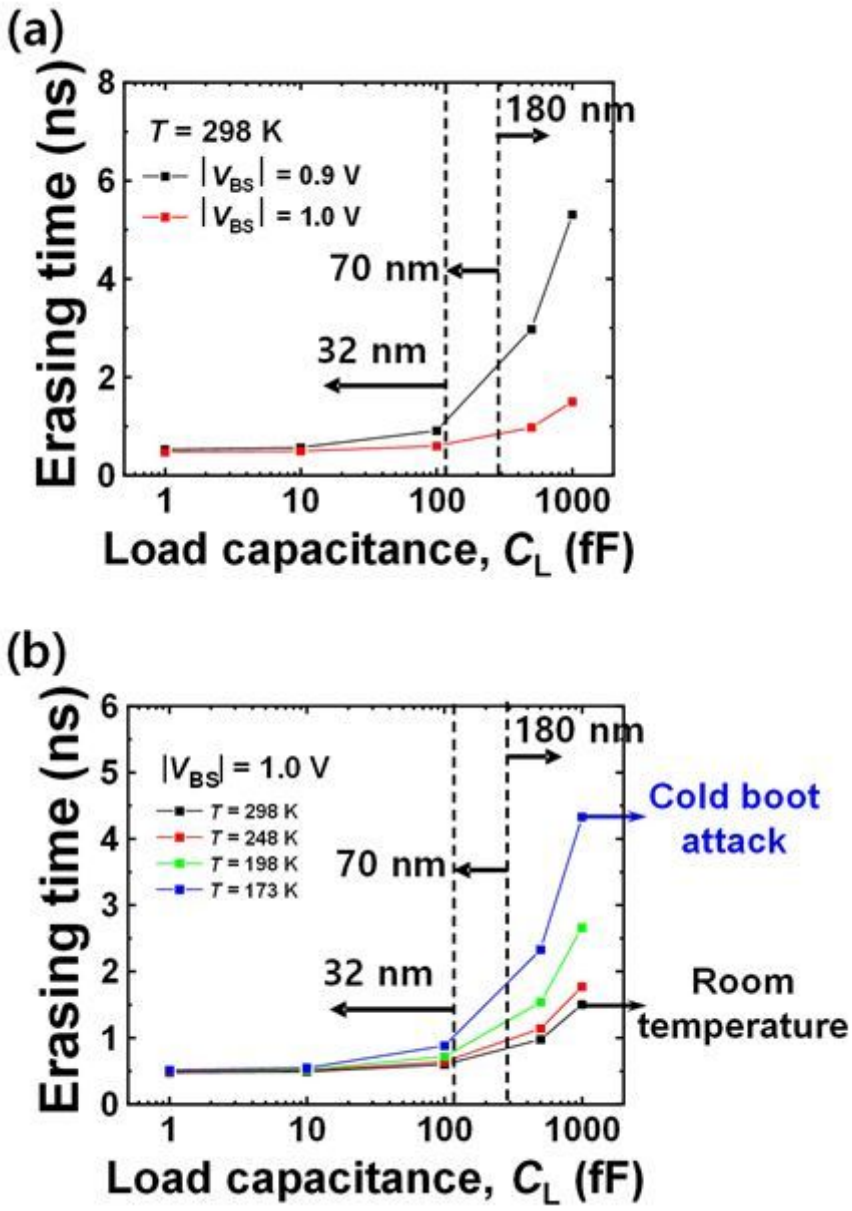


Figure 6

Erasing time versus load capacitance for various technology nodes: 32 nm, 70 nm and 180 nm. (a) Erasing time as a function of load capacitance (CL) for various |VBS| at room temperature (T = 298 K). (b) Erasing time as a function of CL for various T at |VBS| = 1.0 V. Ultra-fast data sanitization within 5 ns was possible regardless of T even for a CL of 1 pF.

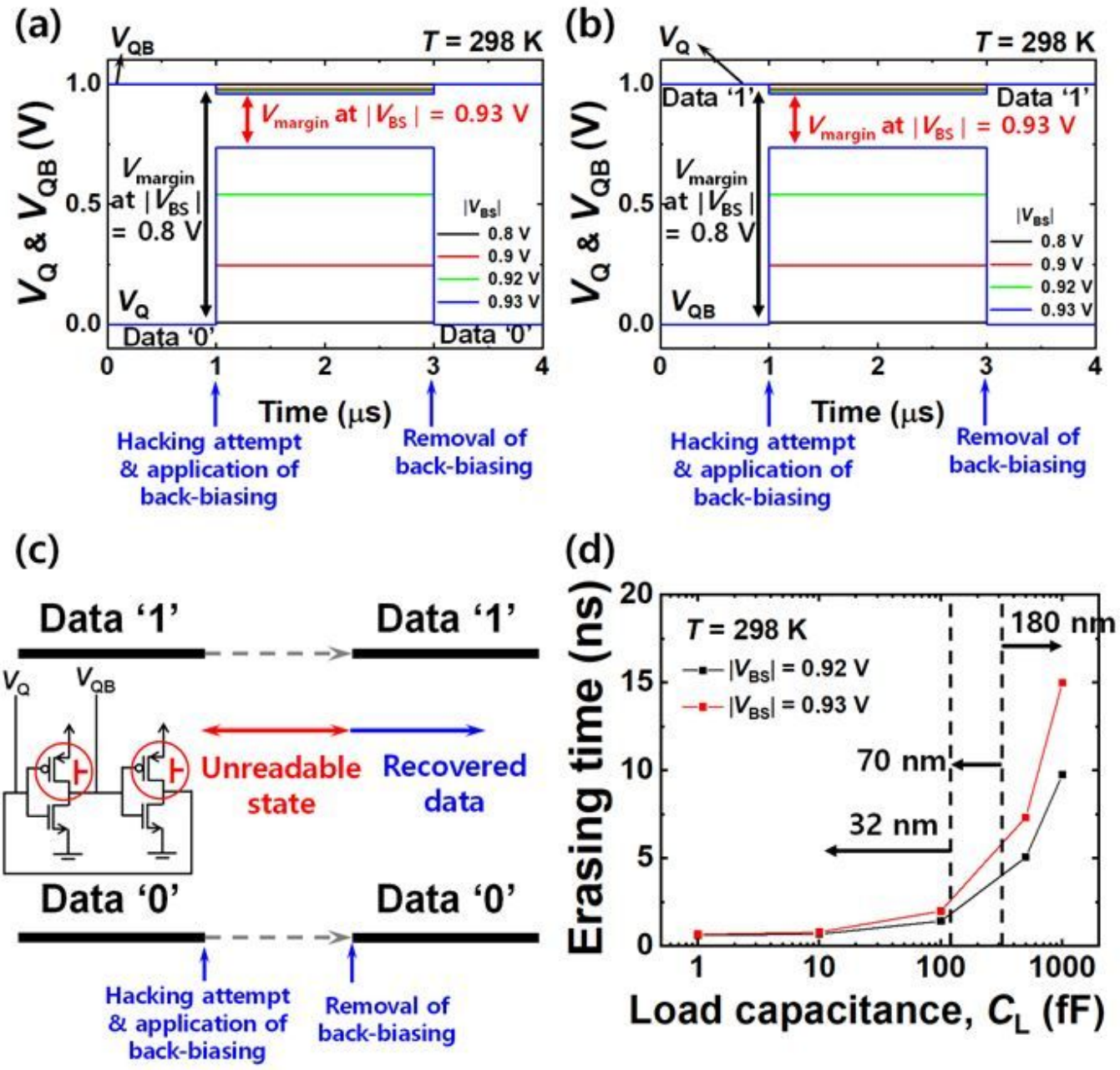


Figure 7

(Temporary erasing) Bit line voltage (VQ) and bit bar line voltage (VQB) depending on the |VBS| at T = 298 K, when the initial data was (a) '0' and (b) '1'. Vmargin reduction was achieved by applied |VBS|. (c) Simplified data diagram with the asymmetric forward back-biasing scheme for temporary erasing. (d) Erasing time versus load capacitances for various technology nodes: 32 nm, 70 nm and 180 nm.

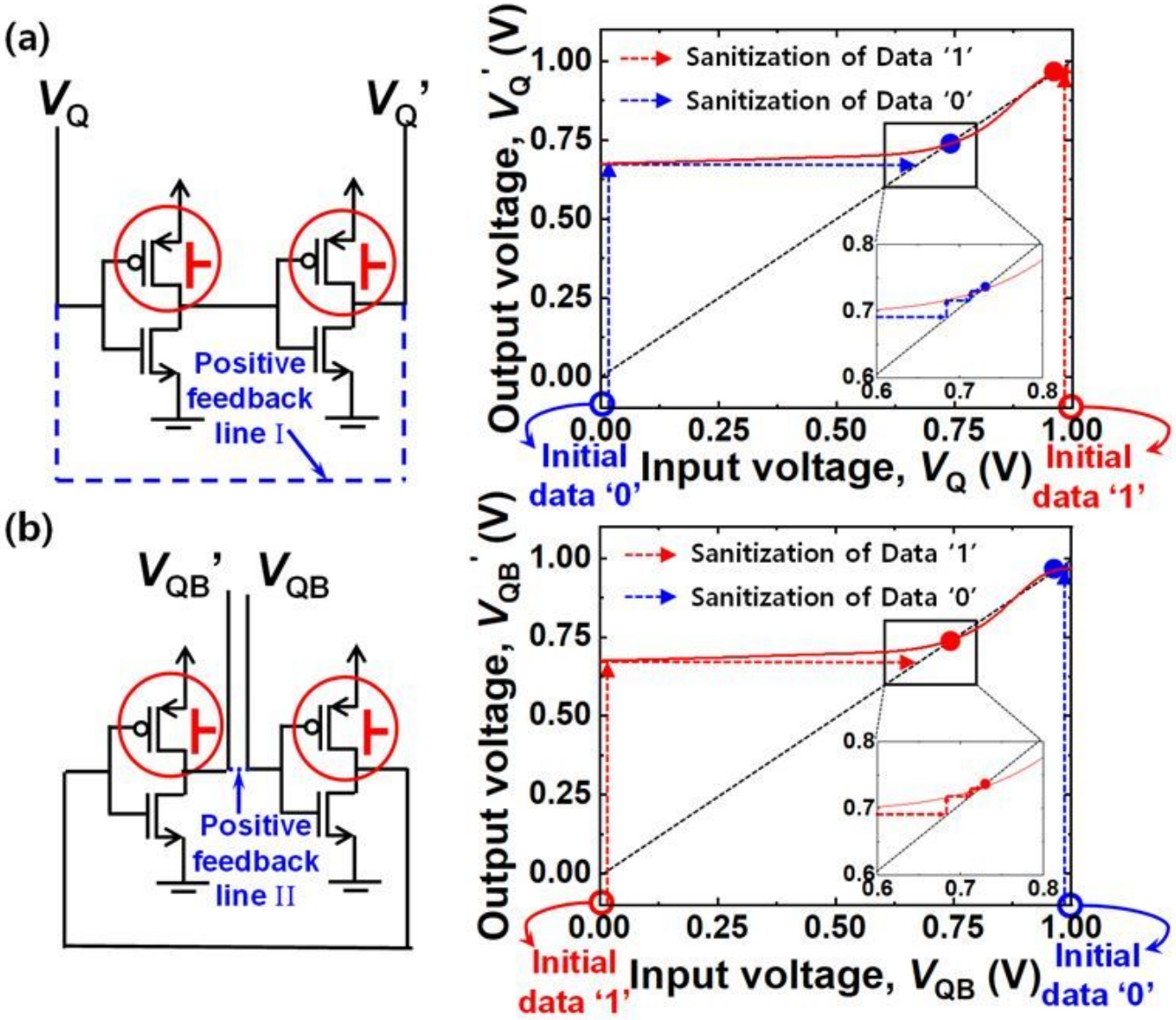


Figure 8

Modified configuration of a 6T-SRAM cell with its corresponding input-output voltage transfer curve (VTC) by symmetric forward back-biasing for temporary erasing. (a) Circuit diagram without positive feedback line I and its VTC in terms of bit line voltage (VQ) to show partially distorted latch. The initial VQ values of 0 V (data '0') and 1 V (data '1') were changed to 0.73 V and 0.95 V, respectively. (b) Circuit diagram without positive feedback line II and its VTC in terms of bit bar line voltage (VQB) to show partially distorted latch. The initial VQB values of 1 V (data '0') and 0 V (data '1') were changed to 0.95 V and 0.73 V, respectively. Vmargin of 0.22 V is achieved for both temporary erasing of data '0' and '1'.

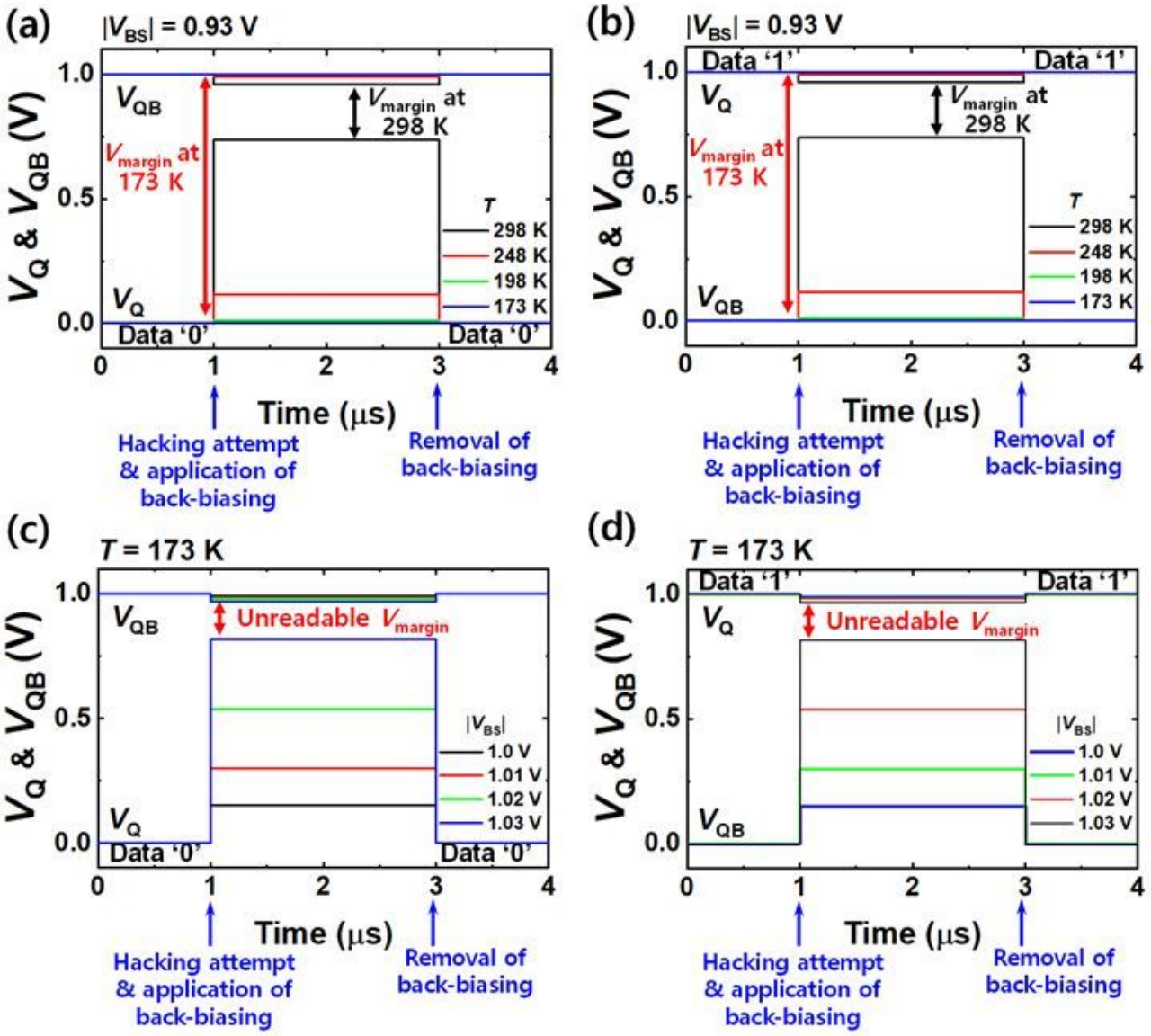


Figure 9

Temperature-variant partial data distortion by temporary erasing for various |VBS|. (a) VQ and VQB for various temperatures at |VBS| of 0.93 V, when the initial data was '0'. (b) VQ and VQB for various temperatures at |VBS| of 0.93 V, when the initial data was '1'. At 173 K, widened Vmargin (close to 1 V) under |VBS| of 0.93 V is vulnerable to a hacking attempt. (c) VQ and VQB for various |VBS| at 173 K, when the initial data was '0'. (d) VQ and VQB for various |VBS| at 173 K, when the initial data was '1'. Temporary erasing is possible even at low temperature by further increment of |VBS|.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- Supplementaryinformation.docx