OPEN

Ultra-fast data sanitization of SRAM by back-biasing to resist a cold boot attack

Seong-Joo Han^{1,2}, Joon-Kyu Han^{1,2}, Gyeong-Jun Yun¹, Mun-Woo Lee¹, Ji-Man Yu¹ & Yang-Kyu Choi¹✉

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.

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 μ s 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. Therefore, the user can reuse the previous data with temporal erasing, whereas one cannot do them with permanent erasing when the hacker's attack is finished. 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.

¹School of Electrical Engineering, Korea Advanced Institute of Science and Technology, (KAIST) 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea. ²These authors contributed equally: Seong-Joo Han and Joon-Kyu Han. ✉email: ykchoi@ee.kaist.ac.kr

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.

Methods

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 simulator¹³. The detailed parameters of the NMOS were set by referring to¹⁴. 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 (6 T-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 6 T-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 in the device level simulations with single MOSFET. The doping concentration of the source (N_{source}), drain (N_{drain}), and substrate (N_{sub}) was set as $1 \times 10^{20} \text{ cm}^{-3}$, $1 \times 10^{20} \text{ cm}^{-3}$, and $3 \times 10^{18} \text{ cm}^{-3}$, respectively. The dopant polarity for the PMOS was opposite to that for the NMOS. Various physical models, such as Shockley-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 Fig. 1a 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 1a 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 Fig. 1a and b. These values are comparable to the experimental data reported in^{15,16}. As an example, $\Delta T (= T_{\text{high}} - T_{300\text{K}})$ 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 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'.

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 6 T-SRAM was composed of two pull-up PMOS, two pull-down NMOS, and two pass-gate NMOS. The word-line (V_{WL}) voltage of the pass-gate MOSFETs was low for turning them off and isolating the storage node (SN) and bit-lines (BLs). The W_G of the MOSFET comprising the SRAM cell was set as 80 nm referring to¹⁷. 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 Fig. 1c. 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 Fig. 1d. 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 Fig. 1a and b.

Results

Permanent erasing. Figure 2 shows the results of permanent erasing by use of forward back-biasing at room temperature. Figure 2a 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 (Fig. 1c), 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 2c and d show V_Q and V_{QB} when '1' was stored initially. With the same forward back-biasing, as shown in Fig. 2a 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

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.

state. Figure 3a 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 Fig. 3a. 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 Fig. 3b.

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 6 T-SRAM cell was intentionally modified to analyze the distortion of the latch state. Figure 4a 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 6 T-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 Fig. 4a, 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 Fig. 4b, 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 Fig. 3b is not explained, it similarly works as described above. In this case, all the data of '0' and '1' can be reset to '0'.

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 5a and b show V_Q and V_{QB} when data '0' was initially stored, and Fig. 5c and d exhibit V_Q and V_{QB} when data '1' was initially stored for various temperatures ranging from 173 to 298 K. The data was reset to '1' by the forward back-biasing even at T of 173 K. This is because ΔT ($= T_{\text{room}} - T_{\text{low}}$) of 125 K ($= 298 \text{ K} - 173 \text{ K}$) makes a small positive ΔV_T of 0.12 V and ΔV_{BS} ($= V_{BS, \text{GND}} - V_{BS, \text{FWD}}$) of -1 V ($= 0 \text{ V} - 1 \text{ V}$) 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.

Supplementary Fig. S1a shows how the erasing time varies according to the load capacitance (C_L) connected to each inverter in a SRAM cell. It corresponds to bit-line capacitance, which tends to be decreased as a technology

Figure 4. Modified configuration of a 6 T-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’.

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.

node is advanced. Referring to¹⁶, C_L is 117 fF at a 70 nm technology node. The erasing time is increased by prolonged RC delay, as C_L is increased. Therefore, the erasing time can be increased with larger C_L in larger array architecture. However, as the technology node advances, fast data sanitization is possible due to reduced C_L . For example, the ultra-fast data sanitization within 5 ns is feasible for C_L of 1 pF, which is larger than nominal C_L below 100 fF¹⁸ at the 32 nm node. It is worth noting that the erasing time can be further shortened by increment

Figure 6. (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.

of $|V_{BS}|$. Supplementary Fig. S1b 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 Fig. S2a). This implies that the proposed back-biasing scheme can resist the cold boot attack.

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 flown¹⁸. 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.

Temporary erasing. Figure 6 shows the results of the temporary erasing with forward back-biasing at room temperature. Figure 6a 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 6c 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 6d 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.

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 7 shows how much the latch state is disturbed by the temporary erasing and thereby data become temporarily unreadable. Figure 7a and b show the modified circuit configuration and its input–output VTC with the back-biasing. Being done at Fig. 4, two positive feedback lines I and II were also individually removed from the conventional 6 T-SRAM cell, as depicted in each circuit diagram of Fig. 7. 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 Fig. 7a, 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 Fig. 7b,

Figure 7. Modified configuration of a 6 T-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 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 ($= 0.95 - 0.73$ 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.

The temporary erasing at low temperature was also investigated with simulations to confirm whether it can resist the cold boot attack. Figure 8a 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 1 V 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 8c 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 Fig. S2b). 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.

It should be noted that the proposing data sanitization requires a new layout scheme in order to separately apply the back-bias. Supplementary Fig. S3a shows a conventional layout of high-density 6 T-SRAM. According to the conventional 6 T-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 Fig. S3b 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 Fig. S3a, 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 Fig. S3b, two PD NFETs can be biased individually. The cross-sections of conventional layout of high-density 6 T-SRAM and possible layout innovation to realize proposed data sanitization scheme are shown in Supplementary Fig. S4. In a layout point of view, a concern to the proposed SRAM cell to allow the back-biasing is a slim p-type well that has a width in a range of 80 nm, which is close to a lithographic limit in a 32 nm technology node. Supplementary Fig. S5 compares a footprint area between a conventional layout and the proposed layout in a 6 T-SRAM cell. According to²¹, the area of SRAM cell in the 32 nm technology is $0.74 \mu\text{m} \times 0.27 \mu\text{m}$. Therefore, the area of the proposed SRAM cell is expected to be increased to 10.8% compared with the conventional one owing to an additional 80 nm well width. The well-proximity effect (WPE) may provoke an V_T shift in a proposed cell transistor. But, it is simply compensated

Figure 8. 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 $|V_{BS}|$.

	Cell type	Sanitization type	Number of transistors	Normalized cell size
–	Conventional 6 T-SRAM	–	6	1
²¹	8 T-SRAM	Power-cut	8	1.81
²²	8 T-SRAM	Feedback-cut	8	1.41
²³	7 T-SRAM	Voltage equalizing	7	1.78
This work	6 T-SRAM	Back-biasing	6	1.1

Table 1. Comparison of various implementations for SRAM sanitization.

for an invariant noise margin by employment of channel V_T implantation, which has commonly used in CMOS fabrication. Table 1 shows the area comparison among various implementations for SRAM sanitization^{22–24}. Each implementation has a different cell size according to a sanitization type. Note that the proposed approach has the smallest number of transistors with the reduced normalized cell size.

To generate the back-bias, a controller should detect whether the SRAM is under attack. Supplementary Fig. S6 shows a strategy to detect the cold boot attack, which will be served as a trigger to enable the data sanitization. As soon as the cold boot attack is attempted by lowering temperature of a SRAM chip to a cryogenic level, such threatening should be detected prior to actual hacking. Herein, a CMOS temperature-to-pulse generator can be used to sense the lowering of ambient temperature, as shown in Supplementary Fig. S7. A delay time is induced between two transmission lines when the ambient temperature is changed, and a XOR gate generates

pulses according to the mismatch in the two lines²⁵. By connecting the output of the CMOS temperature-to-pulse generator to a back-bias terminal, the data in the SRAM cell can be instantly erased when a rapid cooling is attempted by liquid nitrogen. In this way, the back-bias for SRAM data sanitization can be applied automatically.

Discussion

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. In the meanwhile, the direct demonstration of the sanitization with a fully fabricated SRAM chip is planned for the justification of actual security hardware in future.

Data availability

Scientific Reports requires the inclusion of a data availability statement with all submitted manuscripts, as this journal requires authors to make available materials, data, and associated protocols to readers.

Received: 4 May 2021; Accepted: 6 December 2021

Published online: 07 January 2022

References

- Gutmann, P. Secure deletion of data from magnetic and solid-state memory. *Proc. Sixth USENIX Security Symp.*, 1996.
- Xiao, K. *et al.* Bit selection algorithm suitable for high-volume production of SRAM-PUF. *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)* <https://doi.org/10.1109/HST.2014.6855578> (2014).
- Garg, A. & Kim, T. T. Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect. *Proc. IEEE Int Symp Circuits Syst.* <https://doi.org/10.1109/ISCAS.2014.6865541> (2014).
- S. Skorobogatov, "Low temperature data remanence in static RAM", Technical report UCAM-CL-TR-536, University of Cambridge Computer Laboratory, June 2002.
- Hui-fang, J., Xiao-bo, Z., Xin-zhang, J., Xue-ying, Y. & Zheng-yu, Z. The characteristic study of data remanence of SRAM. *Res. Prog. SSE* **26**(4), 536 (2006).
- Anagnostopoulos, N. *et al.* Low-temperature data remanence attacks against intrinsic SRAM PUFs. *Proc. Euromicro Conf. Digit. Syst. Des. (DSD)* **581**, 585. <https://doi.org/10.1109/DSD.2018.00102> (2018).
- Anagnostopoulos, N. *et al.* Attacking SRAM PUFs using very-low-temperature data remanence. *Microproc. Microsyst.* <https://doi.org/10.1016/j.micpro.2019.102864> (2019).
- Wenjing, K., Kai, Y., Guoyi, Y., Xuecheng, Z., 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.
- Yu, K., Zou, X., Yu, G. & Wang, W. Security strategy of powered-off SRAM for resisting physical attack to data remanence. *J. Semicond.* **30**(9), 1–5. <https://doi.org/10.1088/1674-4926/30/9/095010> (2009).
- Chen, M.-J. *et al.* Back-gate forward bias method for low-voltage CMOS digital circuits. *IEEE Trans. Electron Devices* **43**(6), 904–910. <https://doi.org/10.1109/16.502122> (1996).
- Togo, M. *et al.* Power aware 65 nm node CMOS technology using variable V_{DD} and back-bias control with reliability consideration for back-bias mode. *Dig. Tech. Papers Symp. VLSI Technol.* <https://doi.org/10.1109/VLSIT.2004.1345409> (2004).
- 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, 2001.
- Atlas User's Manual: Device Simulation Software, Silvaco Int., Santa Clara, CA, USA, 2008.
- Hanson, S., Seok, M., Sylvester, D. & Blaauw, D. Nanometer device scaling in sub-threshold logic and SRAM. *IEEE Trans. Electron Devices* **55**(1), 175–185. <https://doi.org/10.1109/IEDM.2007.911033> (2008).
- Becker, A., Jazaeri, F., and Enz, C., Cryogenic MOSFET threshold voltage model. in *Proc. 49th Eur. Solid-State Device Res. Conf. (ESSDERC)*, pp. 94–97, 2019. <https://doi.org/10.1109/ESSDERC.2019.8901806>.
- Incandela, R. M., Song, L., Homulle, H. A. R., Sebastiano, F., Charbon, E., and Vladimirescu, A., 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. <https://doi.org/10.1109/ESSDERC.2017.8066591>.
- Fried, D. M. *et al.*, Aggressively scaled (0.143 μm^2) 6T-SRAM cell for the 32 nm node and beyond. in *IEDM Tech. Dig.*, 2004, pp. 261–264. <https://doi.org/10.1109/IEDM.2004.1419127>.
- Kim, K., Mahmoodi, H., and Roy, K., A low-power sram using bit-line charge-recycling. in *Proc. Int. Symp. Low-Power Electron. Design*, pp. 446–459, Aug. 27. <https://doi.org/10.1109/JSSC.2007.914294>.
- Lee, G.-B. *et al.* A novel technique for curing hot-carrier-induced damage by utilizing the forward current of the PN-junction in a MOSFET. *IEEE Electron Dev. Lett.* **38**(8), 1012–1014. <https://doi.org/10.1109/LED.2017.2718583> (2017).
- Zhai, B., Hanson, S., Blaauw, D. & Sylvester, D. A variation-tolerant sub-200 mV 6-T subthreshold SRAM. *IEEE J. Solid-State Circuits* **43**(10), 2338–2347. <https://doi.org/10.1109/JSSC.2008.2001903> (2008).
- Chang, L., Fried, D. M., Hergenrother, J., Sleight, J. W., Dennard, R. H., Montoye, R., Sekaric, L., McNab, S. J., Topol, A. W., Adams, C. D., Guarini, K. W., and Haensch, W., Stable SRAM cell design for the 32 nm node and beyond. in *Proc. IEEE Symp. VLSI Circuits*, 2005, pp. 128–129. <https://doi.org/10.1109/2005.1469239>.
- Konur, E. *et al.* Power analysis resistant SRAM. *World Automation Congress IEEE* <https://doi.org/10.1109/WAC.2006.375932> (2006).
- Rozić, V. *et al.* Design solutions for securing SRAM cell against power analysis. *Hardware Orient. Secur. Trust HOST IEEE Int. Symp.* <https://doi.org/10.1109/HST.2012.6224331> (2012).
- Giterman, R., Keren, O. & Fish, A. A 7T security oriented SRAM bitcell. *IEEE Trans. Circuits Syst. II Exp. Briefs* **66**(8), 1396–1400. <https://doi.org/10.1109/TCSII.2018.2886175> (2019).
- Chen, P., Chen, C., Tsai, C. & Lu, W. A time-to-digital-converter-based CMOS smart temperature sensor. *IEEE J. Solid-State Circuits* **40**(8), 1642–1648. <https://doi.org/10.1109/JSSC.2005.852041> (2005).

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). This work was also supported by the BK-21 FOUR program through National Research Foundation of Korea (NRF) under Ministry of Education. 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.

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.

Funding

National Research Foundation of Korea, 2018R1A2A3075302, 2018R1A2A3075302, 2018R1A2A3075302, 2018R1A2A3075302, 2018R1A2A3075302, 2018R1A2A3075302, IC Design Education Center.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary Information The online version contains supplementary material available at <https://doi.org/10.1038/s41598-021-03994-2>.

Correspondence and requests for materials should be addressed to Y.-K.C.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2022