CYATB108LD

8-Mbit (1024 K × 8) Anti-Tamper Memory

Features

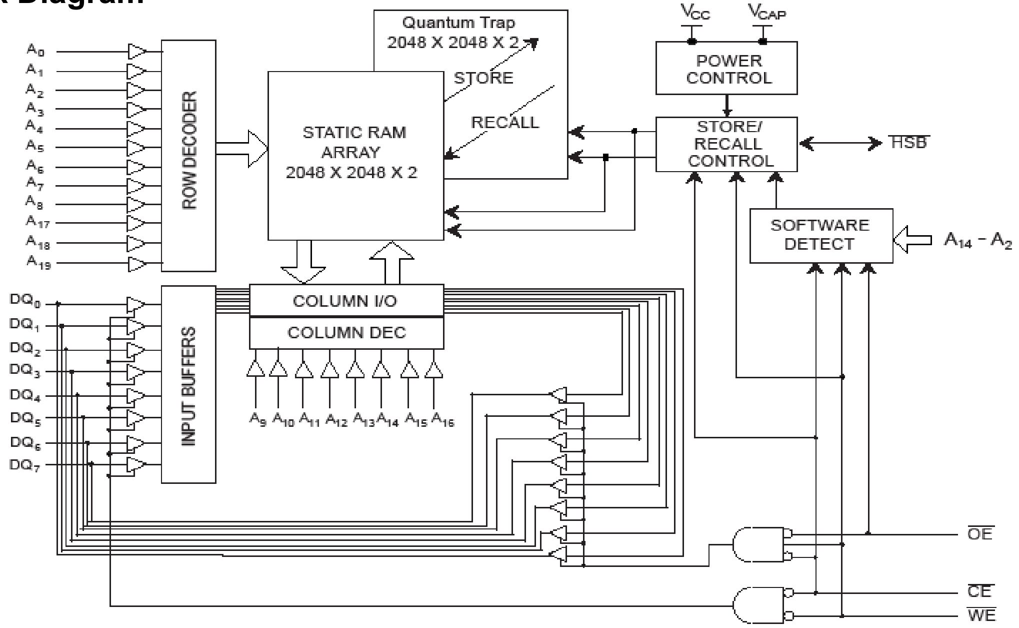
- 45 ns access time
- Internally organized as 1024 K × 8
- Tamper protection [1]
  - Password protection against unauthorized access at power-up
  - Data destruction initiated automatically on password failure or initiated by user
- Hands off automatic STORE on power-down with only a small capacitor
- STORE to QuantumTrap nonvolatile elements initiated by software, or AutoStore on power-down
- RECALL to SRAM initiated by software or power-up
- Infinite read, write, and RECALL cycles
- 1 million STORE cycles to QuantumTrap
- 20 year data retention
- Single 3 V +20%, –10% operation
- Industrial temperature
- 44-pin thin small-outline package (TSOP) Type-II package
- Pb-free and Restriction of Hazardous Substances (RoHS) compliant

Functional Description

The Cypress CYATB108LD is a fast static RAM, with a nonvolatile element in each memory cell. The memory is organized as 1024 Kbytes of 8 bits each. The embedded nonvolatile elements incorporate QuantumTrap technology, producing the world's most reliable nonvolatile memory. The SRAM provides infinite read and write cycles, while independent nonvolatile data resides in the highly reliable QuantumTrap cell. Data transfers from the SRAM to the nonvolatile elements (the STORE operation) takes place automatically at power-down. On power-up, data is restored to the SRAM (the RECALL operation) from the nonvolatile memory. Both the STORE and RECALL operations are also available under software control.

CYATB108LD is password protected from unauthorized access at power-up. Destruction option is available for user in case of tampering. Change Tamper Timeout, Password Disable/Enable, Change Password, Destruction Option and Destruction Disable/Enable operations are available under software control.

Logic Block Diagram



Note

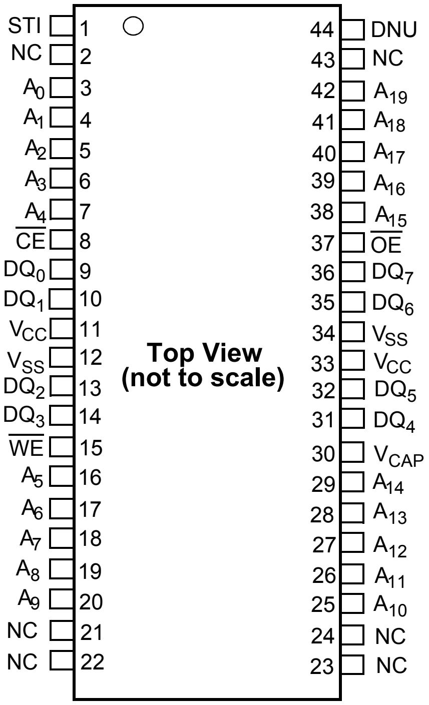
[1] The CYATB108Lx part is capable of different destruction options, but only data destruction option, CYATB108LD is available at this time. More extreme options will be available in the future. Please contact Cypress for further information.

Contents

Pinout

Figure 1. Pin Diagram – 44-pin TSOP II

(× 8)



Pin Definitions

Pin Name	I/O Type	Description
A_0–A_{19}	Input	**Address inputs**. Used to select one of the 1,048,576 bytes of the Anti-Tamper Memory.
DQ_0–DQ_7	Input/output	**Bidirectional data I/O lines**. Used as input or output lines depending on operation.
$\overline{\text{WE}}$	Input	**Write Enable input, Active LOW**. When selected LOW, data on the I/O pins is written to the specific address location.
$\overline{\text{CE}}$	Input	**Chip Enable input, Active LOW**. When LOW, selects the chip. When HIGH, deselects the chip.
$\overline{\text{OE}}$	Input	**Output Enable, Active LOW**. The active LOW $\overline{\text{OE}}$ input enables the data output buffers during read cycles. I/O pins are tristated on deasserting $\overline{\text{OE}}$ HIGH.
V_{SS}	Ground	**Ground for the device**. Must be connected to the ground of the system.
V_{CC}	Power supply	**Power supply inputs to the device**.
STI	Output	**Status Indicator**: It provides the status of Anti-Tamper operations.
V_{CAP}	Power supply	**AutoStore capacitor**. Supplies power to the Anti-Tamper Memory during power loss to store data from SRAM to nonvolatile elements.
NC	No connect	**No connect**. This pin is not connected to the die.
DNU	Do not use	**Do not use**: This pin has to be left floating to ensure proper operation.

Device Operation

The CYATB108LD Anti-Tamper Memory is made up of two functional components paired in the same physical cell. They are a SRAM memory cell and a nonvolatile QuantumTrap cell. The SRAM memory cell operates as a standard fast static RAM. Data in the SRAM is transferred to the nonvolatile cell (the STORE operation), or from the nonvolatile cell to the SRAM (the RECALL operation). Using this unique architecture, all cells are stored and recalled in parallel. During the STORE and RECALL operations, SRAM read and write operations are inhibited. The CYATB108LD supports infinite reads and writes similar to a typical SRAM. In addition, it provides infinite RECALL operations from the nonvolatile cells and up to one million STORE operations. See Truth Table For SRAM Operations on page 30 for a complete description of read and write modes.

SRAM Read

The CYATB108LD performs a read cycle when $\overline{\text{CE}}$ and $\overline{\text{OE}}$ are LOW and $\overline{\text{WE}}$ is HIGH. The address specified on pins A_{0-19} determines which of the 1,048,576 data bytes are accessed. When the read is initiated by an address transition, the outputs are valid after a delay of t_{AA} (read cycle 1). If the read is initiated by $\overline{\text{CE}}$ or $\overline{\text{OE}}$, the outputs are valid at t_{ACE} or at t_{DOE}, whichever is later (read cycle 2). The data output repeatedly responds to address changes within the t_{AA} access time without the need for transitions on any control input pins. This remains valid until another address change or until $\overline{\text{CE}}$ or $\overline{\text{OE}}$ is brought HIGH, or $\overline{\text{WE}}$ is brought LOW.

SRAM Write

A write cycle is performed when $\overline{\text{CE}}$ and $\overline{\text{WE}}$ are LOW. The address inputs must be stable before entering the write cycle and must remain stable until $\overline{\text{CE}}$ or $\overline{\text{WE}}$ goes HIGH at the end of the cycle. The data on the common I/O pins DQ_{0-15} are written into the memory if the data is valid t_{SD} before the end of a $\overline{\text{WE}}$ controlled write or before the end of an $\overline{\text{CE}}$ controlled write. Keep $\overline{\text{OE}}$ HIGH during the entire write cycle to avoid data bus contention on common I/O lines. If $\overline{\text{OE}}$ is left LOW, internal circuitry turns off the output buffers t_{HZWE} after $\overline{\text{WE}}$ goes LOW.

AutoStore Operation

The CYATB108LD stores data to the Anti-Tamper Memory using one of the following two storage operations: Software STORE activated by an address sequence; AutoStore on device power down. The AutoStore operation is a unique feature of QuantumTrap technology and is enabled by default on the CYATB108LD.

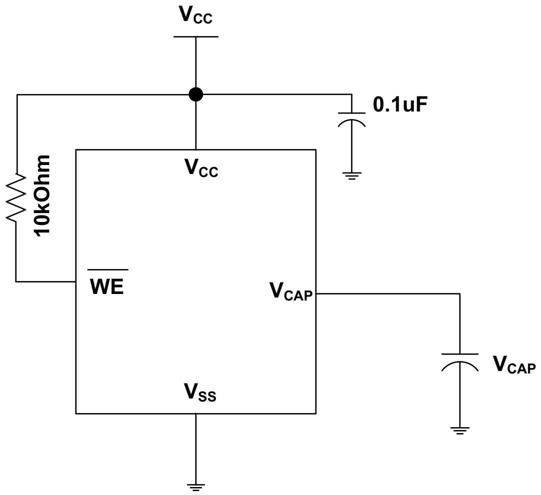
During a normal operation, the device draws current from V_{CC} to charge a capacitor connected to the V_{CAP} pin. This stored charge is used by the chip to perform a single STORE operation. If the voltage on the V_{CC} pin drops below V_{SWITCH}, the part automatically disconnects the V_{CAP} pin from V_{CC}. A STORE operation is initiated with power provided by the V_{CAP} capacitor.

Note Errata: AutoStore Disable feature does not work in the device and hence V_{CAP} should always be connected. For more information, see Errata on page 34. In case V_{CAP} is not connected, the device attempts an AutoStore operation without sufficient charge to complete the Store. This will corrupt the data stored in Anti-Tamper Memory.

Figure 2 shows the proper connection of the storage capacitor (V_{CAP}) for automatic STORE operation. Refer to DC Electrical Characteristics on page 20 for the size of V_{CAP}. The voltage on the V_{CAP} pin is driven to V_{CC} by a regulator on the chip. A pull-up should be placed on $\overline{\text{WE}}$ to hold it inactive during power up. This pull-up is effective only if the $\overline{\text{WE}}$ signal is tristate during power up. Many MPUs tristate their controls on power up. This should be verified when using the pull-up. When the Anti-Tamper Memory comes out of power-on-recall, the MPU must be active or the $\overline{\text{WE}}$ held inactive until the MPU comes out of reset.

To reduce unnecessary nonvolatile STOREs, AutoStore and Hardware STORE operations are ignored unless at least one write operation has taken place since the most recent STORE or RECALL cycle. Software initiated STORE cycles are performed regardless of whether a write operation has taken place.

Figure 2. AutoStore Mode



Hardware RECALL (Power Up)

During power up or after any low power condition ($V_{CC} < V_{SWITCH}$), an internal RECALL request is latched. When V_{CC} again exceeds the sense voltage of V_{SWITCH}, a RECALL cycle is automatically initiated and takes $t_{HRECALL}$ to complete.

Software STORE

Transfer data from the SRAM to the nonvolatile memory with a software address sequence. The CYATB108LD Software STORE cycle is initiated by executing sequential $\overline{\text{CE}}$ controlled read cycles from six specific address locations in exact order. During the STORE cycle an erase of the previous nonvolatile data is first performed, followed by a program of the nonvolatile elements. After a STORE cycle is initiated, further input and output are disabled until the cycle is completed.

Because a sequence of READs from specific addresses is used for STORE initiation, it is important that no other read or write accesses intervene in the sequence, or the sequence is aborted and no STORE or RECALL takes place.

To initiate the Software STORE cycle, the following sequence of CE or OE controlled read operations (with WE kept HIGH) must be performed:

1. Read Address 0x4E38 Valid READ
2. Read Address 0xB1C7 Valid READ
3. Read Address 0x83E0 Valid READ
4. Read Address 0x7C1F Valid READ
5. Read Address 0x703F Valid READ
6. Read Address 0x8FC0 Initiate STORE cycle

After the sixth address in the sequence is entered, the STORE cycle commences and the chip is disabled. After the t_{STORE} cycle time is fulfilled, the SRAM is activated again for the read and write operation.

Software RECALL

Transfer the data from the nonvolatile memory to the SRAM with a software address sequence. A Software RECALL cycle is initiated with a sequence of read operations in a manner similar to the Software STORE initiation. To initiate the RECALL cycle, the following sequence of CE or OE controlled read operations (with WE kept HIGH) must be performed:

1. Read Address 0x4E38 Valid READ
2. Read Address 0xB1C7 Valid READ
3. Read Address 0x83E0 Valid READ
4. Read Address 0x7C1F Valid READ
5. Read Address 0x703F Valid READ
6. Read Address 0x4C63 Initiate RECALL Cycle

Internally, RECALL is a two-step procedure. First, the SRAM data is cleared; then, the nonvolatile information is transferred into the SRAM cells. After the t_{RECALL} cycle time, the SRAM is again ready for read and write operations. The RECALL operation does not alter the data in the nonvolatile elements.

Tamper Protect

The CYATB108LD is password protected from unauthorized access at power-up. User has to enter the password (factory default password is 0x5555555555) followed by End Password Entry soft sequence within a timeout period (factory default timeout period is 25.5 sec) to complete the boot up process.

After the initial power-up, user has the following Anti-Tamper feature options.

- Change Tamper Timeout
- Password Disable/Enable
- Change Password
- Destruction Option
- Destruction Disable/Enable

The Tamper Protect soft sequence must precede Anti-Tamper feature soft sequences.

To initiate the Tamper Protect cycle, the following sequence of CE or OE controlled read operations (with WE kept HIGH) must be performed:

1. Read Address 0x4E38 Valid READ
2. Read Address 0xB1C7 Valid READ
3. Read Address 0x83E0 Valid READ
4. Read Address 0x7C1F Valid READ
5. Read Address 0x703F Valid READ
6. Read Address 0x4F42 Initiate Tamper Protect Cycle

After the sixth address in the sequence is entered, the Tamper Protect cycle commences and STI pin will toggle indicating the readiness for Anti-Tamper feature soft sequences.

After the Tamper Protect cycle is initiated, the user must initiate the follow on Anti-Tamper feature soft sequence within a tamper timeout (t_{TT}) period. If the user does not enter an Anti-Tamper feature soft sequence command within the tamper timeout period, the device will lock up. The user can cancel the Tamper Protect sequence and not execute any Anti-Tamper feature soft sequence by entering the current password and sending End Password Entry soft sequence within tamper timeout.

If power fails during Anti-Tamper feature soft sequence (Change Tamper Timeout/ Password Disable/ Password Enable/ Change Password/ Destruction Disable/ Destruction Enable, except data destruction soft sequence), autoStore will not be initiated. User is expected to store the data using software STORE before initiating Tamper Protect cycle for any of the above sequences. User is also expected to ensure that V_{CC} power does not fail or use V_{CAP} when using any of the above features.

The following sections describe password entry at power-up, End Password Entry soft sequence and the Anti-Tamper feature soft sequences.

Password Entry

At power-up, the CYATB108LD will toggle the STI pin to acknowledge that it is waiting for the password. The user must write the 5-byte password in to FFFF1–FFFF5 memory locations and initiate the End Password Entry soft sequence to signal that the password is entered. This needs to be done within tamper timeout duration.

Note: The part comes from the factory with password set to 0x5555555555 and the tamper timeout set to 25.5 seconds.

End Password Entry

After the password is entered within timeout duration, the user has to execute End Password Entry soft sequence.

To initiate the End Password Entry cycle, the following sequence of CE or OE controlled read operations (with WE kept HIGH) must be performed:

1. Read Address 0x4E38 Valid READ
2. Read Address 0xB1C7 Valid READ
3. Read Address 0x83E0 Valid READ
4. Read Address 0x7C1F Valid READ
5. Read Address 0x703F Valid READ
6. Read Address 0x3394 Valid READ
7. Read Address 0x4C42 Initiate End Password Entry Cycle

After entering the End Password Entry cycle, the part then checks if entered password is valid. If the correct password is entered within the allowed time the part will toggle the STI pin again to indicate that it received the correct password and will continue with the power up. FFFF1–FFFF5 memory locations will be filled with 1's after password authentication.

If the STI pin does not toggle within t_{ACK} time from the End Password Entry cycle, then the password entered is invalid. In that case, user should attempt to enter the correct password within the tamper timeout period.

Note: STI pin toggle (If any) is not valid during password entry and is valid only after End Password Entry soft sequence is initiated.

If the entered password is incorrect, user will have 3 attempts to enter the correct password. If the user can not enter the password within the tamper timeout (t_{TT}) or exceeds the attempt count the CYATB108LD will execute Data Destruction option as per the factory default setting and lock up the device. If destruction option is disabled by the user, the device will not execute destruction option and will only lock up the device. The user must power cycle the device and enter the password again to use it.

Change Tamper Timeout

Tamper Timeout can be changed by sending the Change Tamper Timeout soft sequence. The minimum password entry time is 100 ms and it can be changed up to maximum of 25.5 s in steps of 100 ms by writing into memory location 0xFFFF1.

The user executes the Change Tamper Timeout process by sending Tamper Protect soft sequence followed by Change Tamper Timeout soft sequence.

After the Tamper Protect soft sequence, to initiate the Change Tamper Timeout cycle, the following sequence of $\overline{\text{CE}}$ or $\overline{\text{OE}}$ controlled read operations (with $\overline{\text{WE}}$ kept HIGH) must be performed:

1. Read Address 0x4E38 Valid READ
2. Read Address 0xB1C7 Valid READ
3. Read Address 0x83E0 Valid READ
4. Read Address 0x7C1F Valid READ
5. Read Address 0x703F Valid READ
6. Read Address 0x3394 Valid READ
7. Read Address 0x8842 Initiate Change Tamper Timeout Cycle

After the seventh address in the sequence is entered, the STI pin will toggle acknowledging acceptance of Change Tamper Timeout soft sequence. The device then takes t_{STORE} time to process the tamper timeout change. After the t_{STORE} cycle time, the SRAM is activated again for the read and write operation.

The Change Tamper Timeout steps are given below,

1. Write time count between 0x01 to 0xFF into memory location 0xFFFF1. Time count has a resolution of 100 ms. A time count of 0x00 is invalid and tamper timeout will be set to max.

Example: Time count of 0x20 will set tamper timeout to 32 × 100 ms = 3.2 s.

2. Execute Change Tamper Timeout soft sequence

Note: The part comes from the factory with the default time set to 25.5 s (maximum), which is the time count value of 0xFF.

Password Disable/Enable

The Password feature can be disabled by the user if it is not required. When the password is disabled, on the next power up the part will be ready for read/write operation without the password entry.

Note: Password Disable/Enable is applicable for requirement of password at power-up only. Irrespective of Password Disable/Enable status, user need to enter the password for Change Password cycle and to cancel Tamper Protect sequences.

The Password Entry is disabled by initiating a Password Disable soft sequence to avoid password entry at power up to access memory.

The user executes the Password Disable process by sending Tamper Protect soft sequence followed by Password Disable soft sequence.

After the Tamper Protect soft sequence, to initiate the Password Disable sequence, the following sequence of $\overline{\text{CE}}$ or $\overline{\text{OE}}$ controlled read operations (with $\overline{\text{WE}}$ kept HIGH) must be performed:

1. Read address 0x4E38 Valid READ
2. Read address 0xB1C7 Valid READ
3. Read address 0x83E0 Valid READ
4. Read address 0x7C1F Valid READ
5. Read address 0x703F Valid READ
6. Read address 0x3394 Valid READ
7. Read address 0x8E4B Initiate Password Disable

After the seventh address in the sequence is entered, the STI pin will toggle acknowledging acceptance of Password Disable soft sequence. The device then takes t_{STORE} time to process the Password Disable. After the t_{STORE} cycle time, the SRAM is activated again for the read and write operation.

The Password is re-enabled by initiating an Password Enable sequence. The user executes the Password Enable process by sending Tamper Protect soft sequence followed by Password Enable soft sequence.

After the Tamper Protect soft sequence, to initiate the Password Enable sequence, the following sequence of $\overline{\text{CE}}$ or $\overline{\text{OE}}$ controlled read operations (with $\overline{\text{WE}}$ kept HIGH) must be performed:

1. Read address 0x4E38 Valid READ
2. Read address 0xB1C7 Valid READ
3. Read address 0x83E0 Valid READ
4. Read address 0x7C1F Valid READ
5. Read address 0x703F Valid READ
6. Read address 0x3394 Valid READ
7. Read address 0x4FC3 Initiate Password Enable

After the seventh address in the sequence is entered, the STI pin will toggle acknowledging acceptance of Password Enable soft sequence. The device then takes t_{STORE} time to process the Password Enable. After the t_{STORE} cycle time, the SRAM is activated again for the read and write operation.

Note: The part comes from the factory with password enabled.

Change Password

The user can change the password anytime after a successful boot-up. The old password and the new password (2 times) should be entered to change the password. The old password must be written at 0xFFFF1–0xFFFF5 memory locations. The new password must be written at 0xFFFF6–0xFFFFA and again at 0xFFFFB–0xFFFFF memory locations. The allowed time to change the password is the same as the tamper timeout. 3 attempts are allowed to change the old password.

The new password cannot be the same as the last 2 passwords (current and previous password). It also needs that all five bytes have at least one bit changed from the last 2 passwords.

The user executes the Change Password process by sending Tamper Protect soft sequence followed by Change Password soft sequence.

After the Tamper Protect soft sequence, to initiate the Change Password sequence, the following sequence of $\overline{\text{CE}}$ or $\overline{\text{OE}}$ controlled read operations (with $\overline{\text{WE}}$ kept HIGH) must be performed:

1. Read Address 0x4E38 Valid READ
2. Read Address 0xB1C7 Valid READ
3. Read Address 0x83E0 Valid READ
4. Read Address 0x7C1F Valid READ
5. Read Address 0x703F Valid READ
6. Read Address 0x3394 Valid READ
7. Read Address 0x89C5 Initiate Change Password Cycle

The Change Password steps are given below,

1. Send “Tamper Protect” Soft Sequence
2. Write the old password into address: FFFF1 to FFFF5
3. Write the new password into memory locations FFFF6 to FFFFA and again into FFFFB to FFFFF
4. Send “Change Password” Soft Sequence

After entering Change Password cycle, the part then checks the password immediately. If the correct password is entered the part will toggle STI pin acknowledging acceptance of Change Password soft sequence within t_{ACK}. The device then takes t_{STORE} time to process the changed password. After the t_{STORE} cycle time, the SRAM is activated again for the read and write operation.

Memory location (0xFFFF1–0xFFFFF) that the user uses to enter the password will be filled with all 1’s.

If the STI pin does not toggle within t_{ACK} time, then the password entered does not satisfy the valid password criteria. In that case, user should attempt again with the valid password criteria within the tamper timeout period.

If all attempts to change the password fail or time allowed elapsed without a successful password, the device will lock up. The user must power cycle the device and enter the password again to use it.

The user can cancel the password change request by entering the current password and sending End Password Entry soft sequence. The current password will be retained and the password address memory location (0xFFFF1–0xFFFFF) will be filled with all 1’s.

Note: The part comes from the factory with password set to 5555555555h.

Destruction Option

Data Destruction feature is available in the CYATB108LD part. The Data Destruction option will destroy the nonvolatile and SRAM data, but the device will continue to function after power cycle.

Whenever the user detects tampering, the user can execute destruction option by sending soft sequence. The soft sequence that execute Data Destruction option will destroy the data.

The user executes the Data Destruction process by sending Tamper Protect soft sequence followed by Data Destruction soft sequence.

After the Tamper Protect soft sequence, to initiate the Data Destruction cycle, the following sequence of $\overline{\text{CE}}$ or $\overline{\text{OE}}$ controlled read operations (with $\overline{\text{WE}}$ kept HIGH) must be performed:

1. Read Address 0x4E38 Valid READ
2. Read Address 0xB1C7 Valid READ
3. Read Address 0x83E0 Valid READ
4. Read Address 0x7C1F Valid READ
5. Read Address 0x703F Valid READ
6. Read Address 0x3394 Valid READ
7. Read Address 0x8B49 Initiate Data Destruction Cycle

After the seventh address in the sequence is entered, the STI pin will toggle acknowledging acceptance of Data Destruction soft sequence. The device then takes t_{SSDD} time to destroy the data. After the t_{SSDD} cycle time, the device will lock up.

Note: AutoStore Enable and AutoStore Disable bit is destroyed by the execution of data destruction and will be set to default (which is AutoStore enable) on the next power-up.

Destruction Disable/Enable

If Data Destruction on a password failure or a tamper timeout is not desired, the user has the option to disable the destruction option.

The Destruction option is disabled by initiating an Destruction Disable soft sequence to avoid self destruction if wrong password is entered three times or if the password is not entered in the allowed time (t_{TT}) at power up.

The user executes the Destruction Disable process by sending Tamper Protect soft sequence followed by Destruction Disable soft sequence.

After the Tamper Protect soft sequence, to initiate the Destruction Disable cycle, the following sequence of $\overline{CE}$ or $\overline{OE}$ controlled read operations (with $\overline{WE}$ kept HIGH) must be performed:

1. Read address 0x4E38 Valid READ
2. Read address 0xB1C7 Valid READ
3. Read address 0x83E0 Valid READ
4. Read address 0x7C1F Valid READ
5. Read address 0x703F Valid READ
6. Read Address 0x3394 Valid READ
7. Read address 0x8D4D Initiate Destruction Disable

After the seventh address in the sequence is entered, the STI pin will toggle acknowledging acceptance of Destruction Disable soft sequence. The device then takes t_{STORE} time to process the Destruction Disable. After the t_{STORE} cycle time, the SRAM is activated again for the read and write operation.

If user enters the wrong password three times or if the password is not entered in the allowed time at power up in Destruction Disable mode, the device will only lock up without destroying the data. The user must power cycle the device and enter the password again to use it. The Destruction is re-enabled by initiating the Destruction Enable sequence.

The user executes the Destruction Enable process by sending Tamper Protect soft sequence followed by Destruction Enable soft sequence.

After the Tamper Protect soft sequence, to initiate the Destruction Enable cycle, the following sequence of $\overline{CE}$ or $\overline{OE}$ controlled read operations (with $\overline{WE}$ kept HIGH) must be performed:

1. Read address 0x4E38 Valid READ
2. Read address 0xB1C7 Valid READ
3. Read address 0x83E0 Valid READ
4. Read address 0x7C1F Valid READ
5. Read address 0x703F Valid READ
6. Read Address 0x3394 Valid READ
7. Read address 0x4DC3 Initiate Destruction Enable

After the seventh address in the sequence is entered, the Destruction Enable cycle commences and STI pin will toggle indicating successful Destruction Enable option.

Note: The part comes from the factory with destruction enabled.

Figure 3. Power-up Sequence

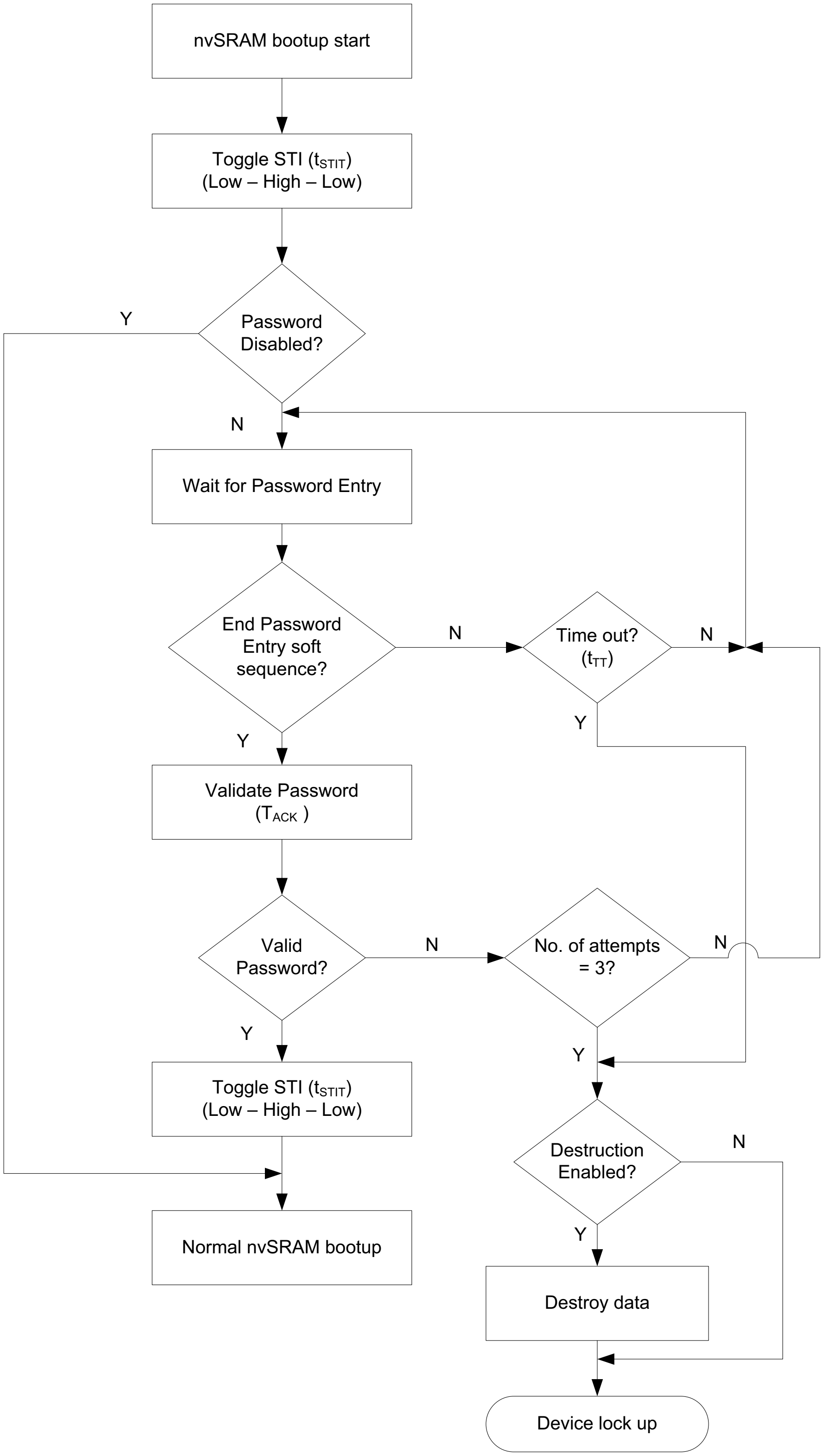


Figure 4. Change Tamper Timeout

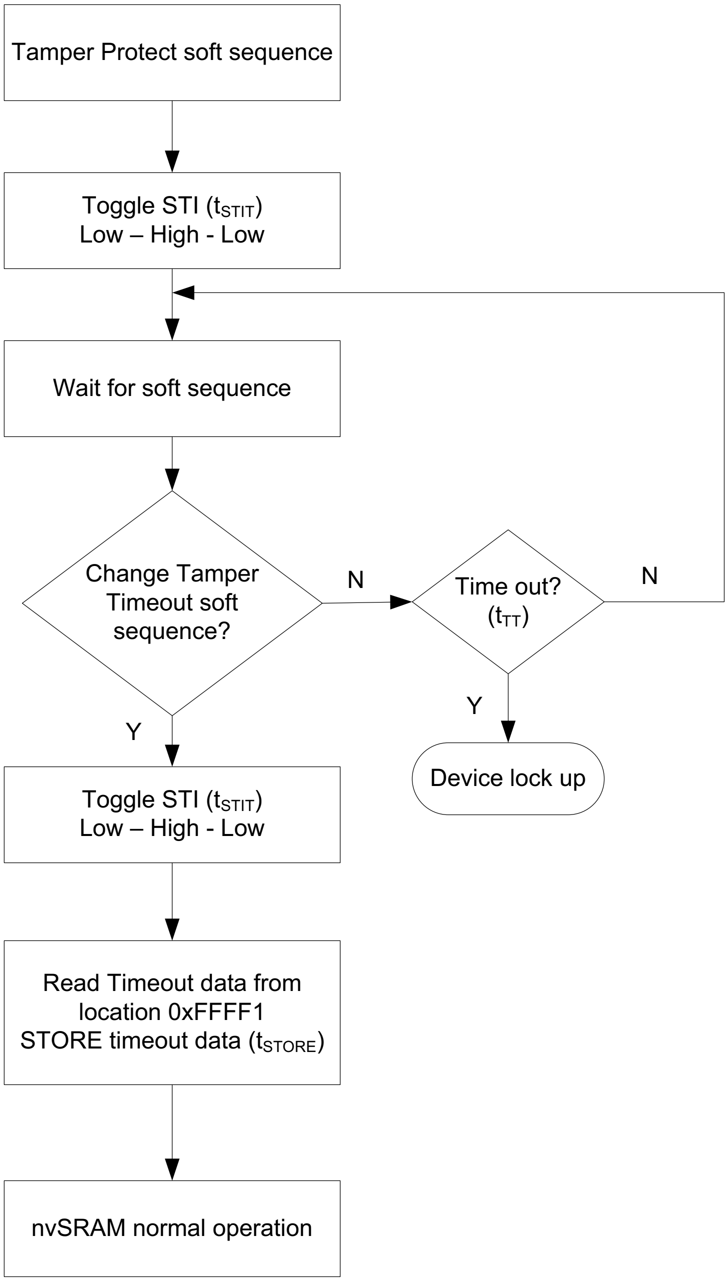


Figure 5. Password Disable/Enable

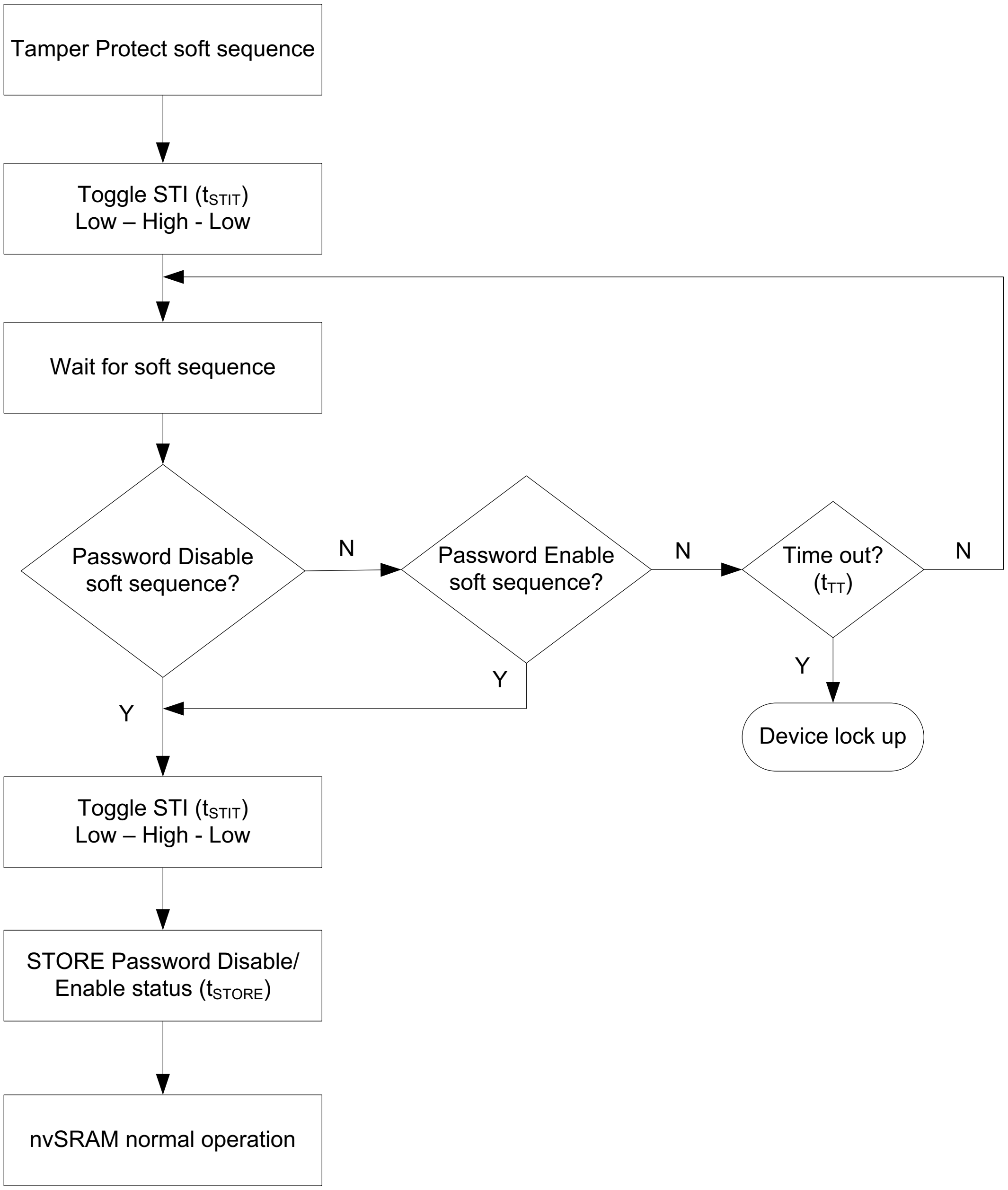

Tamper Protect soft sequence
Toggle STI (t_{STIT}) Low – High - Low
Wait for soft sequence
Password Disable soft sequence?
N
Password Enable soft sequence?
N
Time out? (t_{TT})
N
Y
Y
Y
Device lock up
Toggle STI (t_{STIT}) Low – High - Low
STORE Password Disable/ Enable status (t_{STORE})
nvSRAM normal operation

Figure 6. Change Password

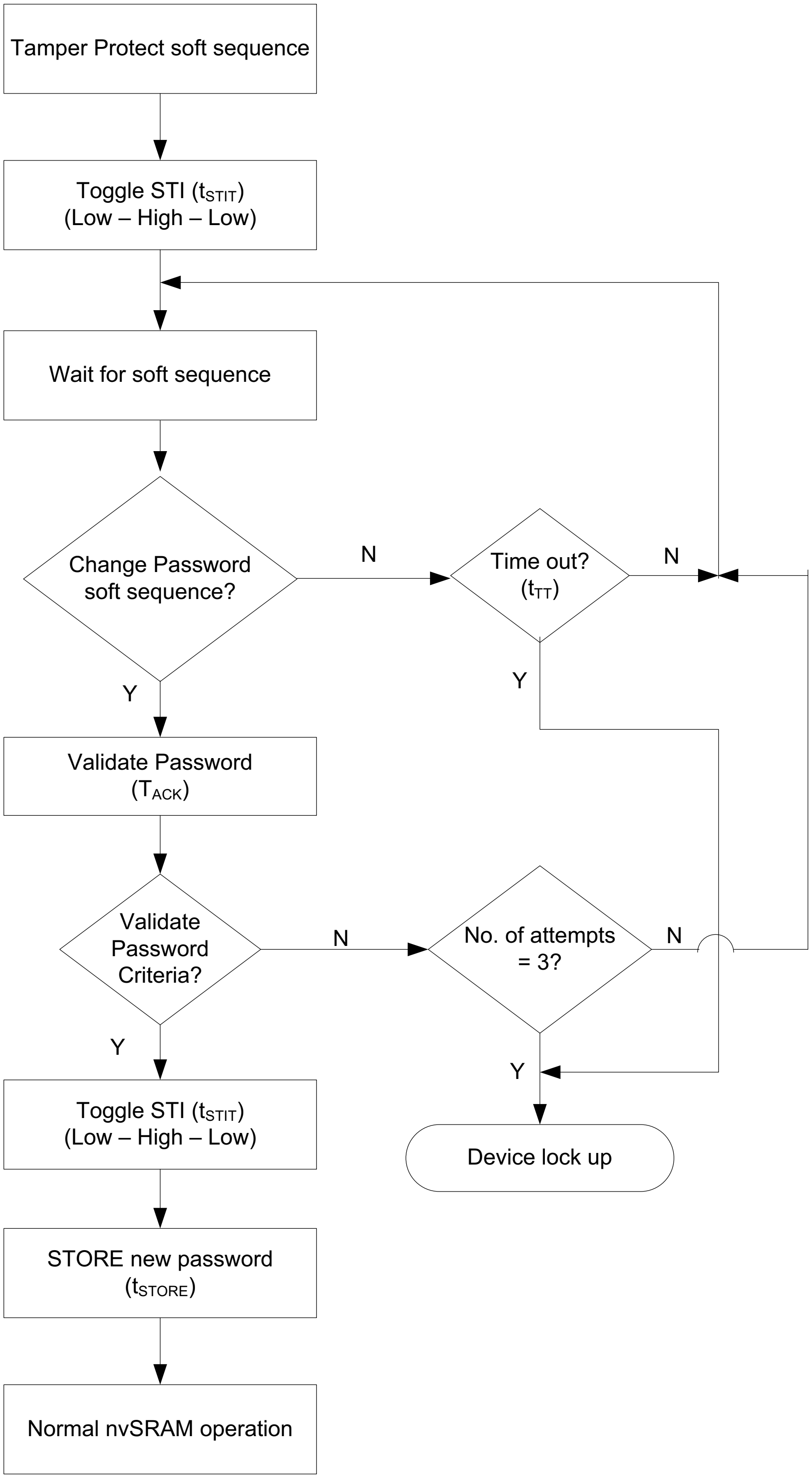

Tamper Protect soft sequence
Toggle STI (t_{STIT}) (Low – High – Low)
Wait for soft sequence
Change Password soft sequence?
N
Time out? (t_{TT})
N
Y
Y
Validate Password (T_{ACK})
Validate Password Criteria?
N
No. of attempts = 3?
N
Y
Y
Toggle STI (t_{STIT}) (Low – High – Low)
Device lock up
STORE new password (t_{STORE})
Normal nvSRAM operation

Figure 7. Destruction Option

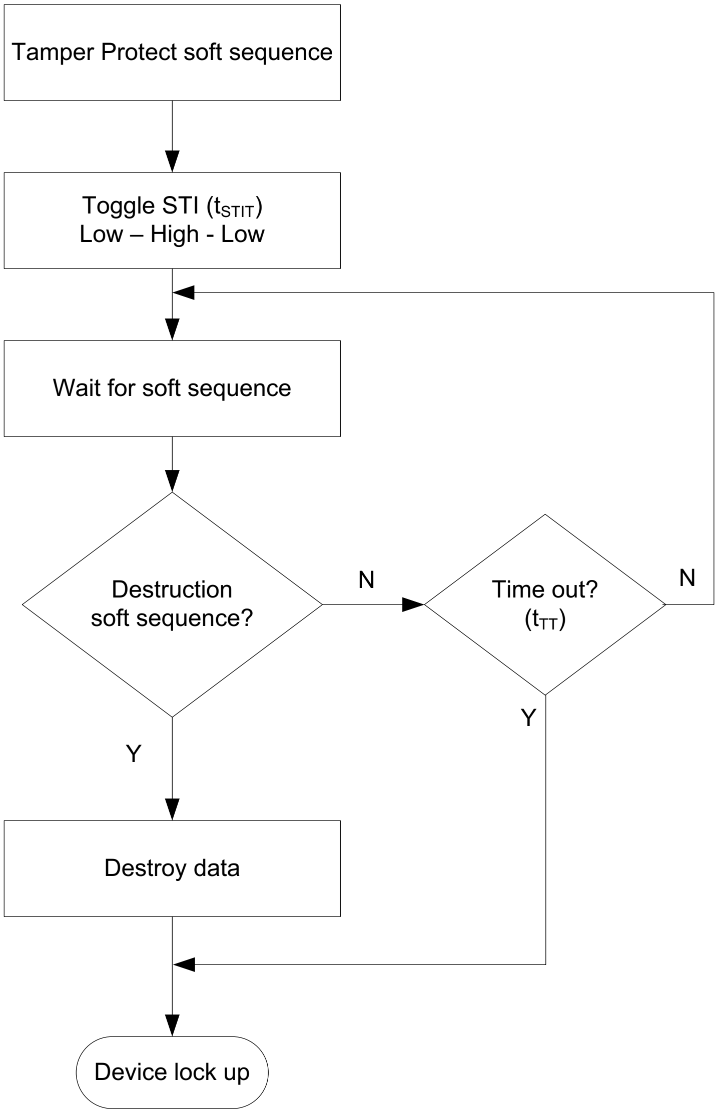


Figure 8. Destruction Disable/Enable

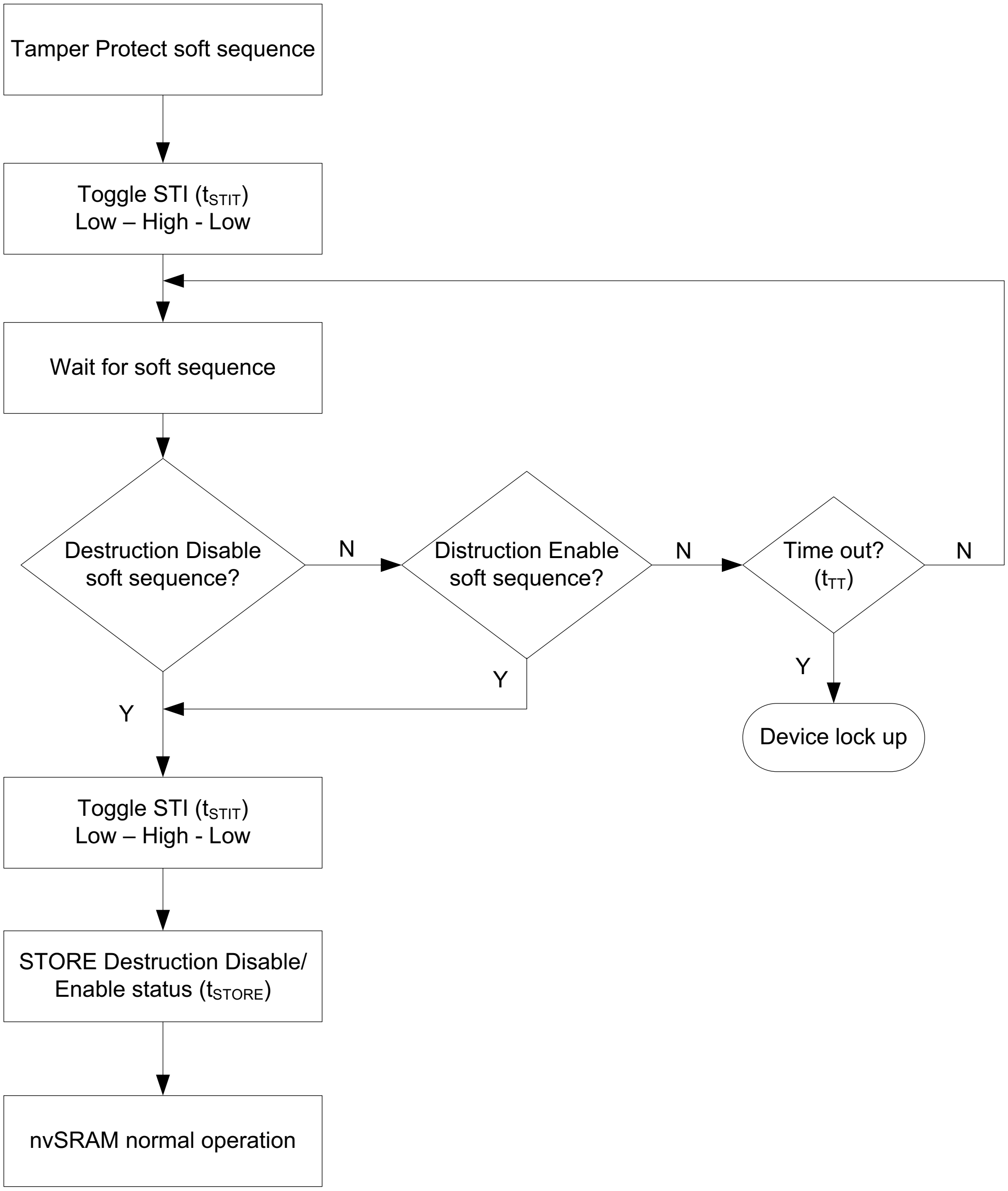

Tamper Protect soft sequence
Toggle STI (t_{STIT}) Low – High - Low
Wait for soft sequence
Destruction Disable soft sequence?
N
Distruction Enable soft sequence?
N
Time out? (t_{TT})
N
Y
Y
Y
Device lock up
Toggle STI (t_{STIT}) Low – High - Low
STORE Destruction Disable/ Enable status (t_{STORE})
nvSRAM normal operation

Figure 9. Tamper Protect Exit Sequence

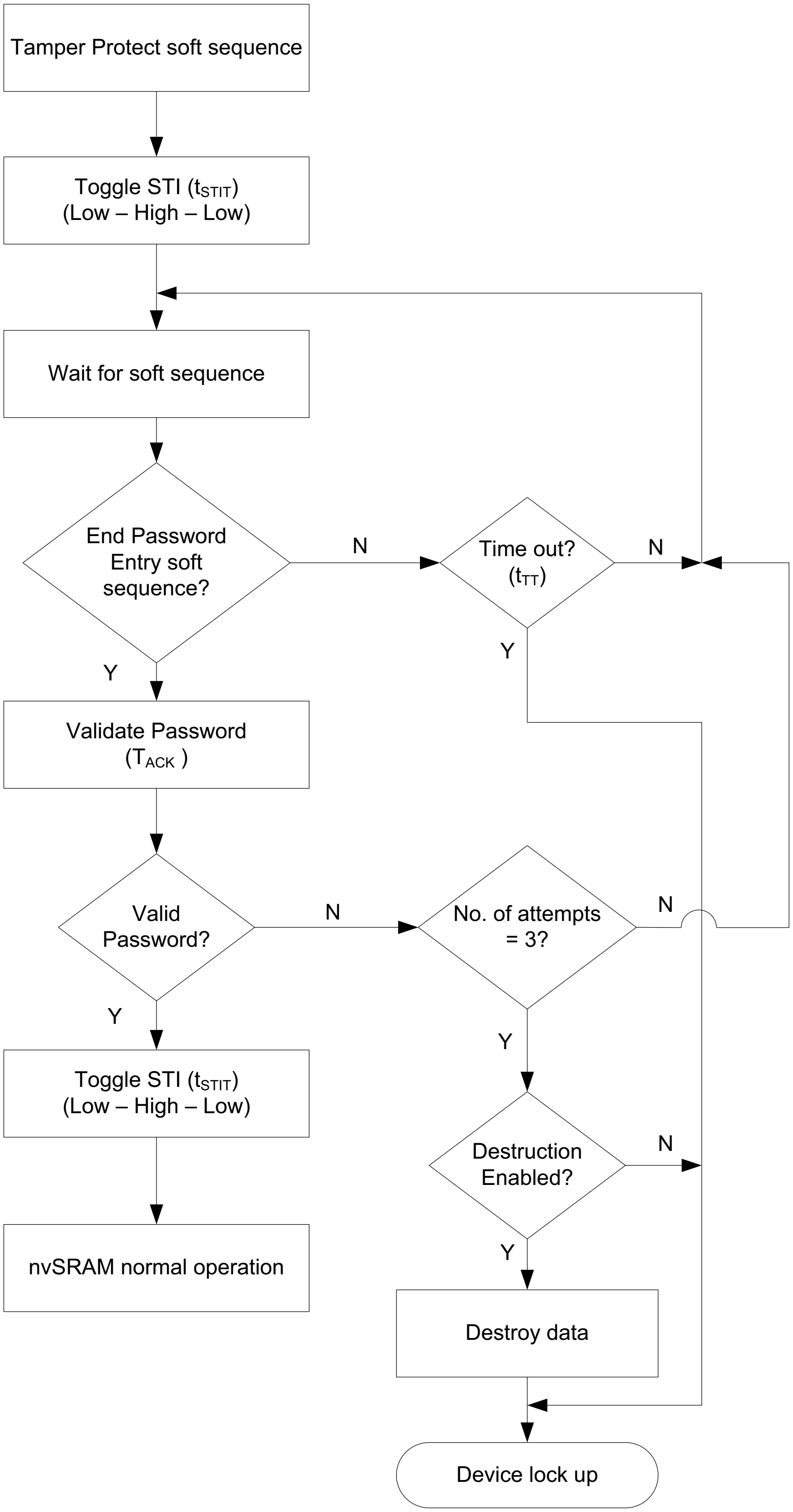


Table 1. Mode Selection

$\overline{CE}$	$\overline{WE}$	$\overline{OE}$	A_{15}–A_0[2]	Mode	I/O	Power
H	X	X	X	Not Selected	Output High Z	Standby
L	H	L	X	Read SRAM	Output Data	Active
L	L	X	X	Write SRAM	Input Data	Active
L	H	L	0x4E38 0xB1C7 0x83E0 0x7C1F 0x703F 0x8B45	Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM AutoStore Disable	Output Data Output Data Output Data Output Data Output Data Output Data	Active[3]
L	H	L	0x4E38 0xB1C7 0x83E0 0x7C1F 0x703F 0x4B46	Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM AutoStore Enable	Output Data Output Data Output Data Output Data Output Data Output Data	Active[3]
L	H	L	0x4E38 0xB1C7 0x83E0 0x7C1F 0x703F 0x8FC0	Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Nonvolatile STORE	Output Data Output Data Output Data Output Data Output Data Output High Z	Active I_{CC2}[3]
L	H	L	0x4E38 0xB1C7 0x83E0 0x7C1F 0x703F 0x4C63	Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Nonvolatile RECALL	Output Data Output Data Output Data Output Data Output Data Output High Z	Active[3]
L	H	L	0x4E38 0xB1C7 0x83E0 0x7C1F 0x703F 0x4F42	Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Initiate Tamper Protect	Output Data Output Data Output Data Output Data Output Data Output High Z	Active[3]

Notes

[2] While there are 20 address lines on the CYATB108LD, only the 13 address lines (A_{14}–A_2) are used to control software modes. Rest of the address lines are don't care.

[3] The soft sequence consecutive address locations must be in the order listed.

Table 2. Tamper Protect Mode Selection

$\overline{CE}$	$\overline{WE}$	$\overline{OE}$	A_{15}–A_0[4]	Mode	I/O	Power
L	H	L	0x4E38 0xB1C7 0x83E0 0x7C1F 0x703F 0x3394 0x4C42	Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM End Password Entry	Output Data Output Data Output Data Output Data Output Data Output Data Output High Z	Active[5]
L	H	L	0x4E38 0xB1C7 0x83E0 0x7C1F 0x703F 0x3394 0x8842	Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Change Tamper Timeout	Output Data Output Data Output Data Output Data Output Data Output Data Output High Z	Active[5]
L	H	L	0x4E38 0xB1C7 0x83E0 0x7C1F 0x703F 0x3394 0x8E4B	Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Password Disable	Output Data Output Data Output Data Output Data Output Data Output Data Output High Z	Active[5]
L	H	L	0x4E38 0xB1C7 0x83E0 0x7C1F 0x703F 0x3394 0x4FC3	Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Password Enable	Output Data Output Data Output Data Output Data Output Data Output Data Output High Z	Active[5]
L	H	L	0x4E38 0xB1C7 0x83E0 0x7C1F 0x703F 0x3394 0x89C5	Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Change Password	Output Data Output Data Output Data Output Data Output Data Output Data Output High Z	Active[5]
L	H	L	0x4E38 0xB1C7 0x83E0 0x7C1F 0x703F 0x3394 0x8B49	Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Data destruction	Output Data Output Data Output Data Output Data Output Data Output Data Output High Z	Active[5]

Notes

[4] While there are 20 address lines on the CYATB108LD, only the 13 address lines (A_{14}–A_2) are used to control software modes. Rest of the address lines are don't care.

[5] The soft sequence consecutive address locations must be in the order listed.

Table 2. Tamper Protect Mode Selection (continued)

$\overline{CE}$	$\overline{WE}$	$\overline{OE}$	A_{15}–A_0[4]	Mode	I/O	Power
L	H	L	0x4E38 0xB1C7 0x83E0 0x7C1F 0x703F 0x3394 0x8D4D	Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Destruction Disable	Output Data Output Data Output Data Output Data Output Data Output Data Output High Z	Active[6]
L	H	L	0x4E38 0xB1C7 0x83E0 0x7C1F 0x703F 0x3394 0x4DC3	Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Read SRAM Destruction Enable	Output Data Output Data Output Data Output Data Output Data Output Data Output High Z	Active[6]

Note

[6] The soft sequence consecutive address locations must be in the order listed.

Preventing AutoStore

The AutoStore function is disabled by initiating an AutoStore disable sequence. A sequence of read operations is performed in a manner similar to the Software STORE initiation. To initiate the AutoStore disable sequence, the following sequence of $\overline{CE}$ controlled read operations must be performed:

1. Read address 0x4E38 Valid READ
2. Read address 0xB1C7 Valid READ
3. Read address 0x83E0 Valid READ
4. Read address 0x7C1F Valid READ
5. Read address 0x703F Valid READ
6. Read address 0x8B45 AutoStore Disable

Note Errata: AutoStore Disable feature does not work in the device. For more information, see Errata on page 34.

The AutoStore is re-enabled by initiating an AutoStore enable sequence. A sequence of read operations is performed in a manner similar to the Software RECALL initiation. To initiate the AutoStore enable sequence, the following sequence of $\overline{CE}$ or $\overline{OE}$ controlled read operations must be performed:

1. Read address 0x4E38 Valid READ
2. Read address 0xB1C7 Valid READ
3. Read address 0x83E0 Valid READ
4. Read address 0x7C1F Valid READ
5. Read address 0x703F Valid READ
6. Read address 0x4B46 AutoStore Enable

If the AutoStore function is disabled or re-enabled, a manual STORE operation (Hardware or Software) must be issued to save the AutoStore state through subsequent power-down cycles. The part comes from the factory with AutoStore enabled and 0x00 written in all cells.

Note: AutoStore Enable and AutoStore Disable bit is destroyed by the execution of data destruction and will be set to default on the next power-up.

Data Protection

The CYATB108LD protects data from corruption during low voltage conditions by inhibiting all externally initiated STORE and write operations. The low voltage condition is detected when $V_{CC} \le V_{SWITCH}$. If the CYATB108LD is in a write mode (Both $\overline{CE}$ and $\overline{WE}$ are LOW) at power-up, after a RECALL or STORE, the write is inhibited until the SRAM is enabled. This protects against inadvertent writes during power-up or brown out conditions.

Maximum Ratings

Exceeding maximum ratings may shorten the useful life of the device. User guidelines are not tested.

Storage temperature .... –65 °C to +150 °C

Maximum accumulated storage time

At 150 °C ambient temperature 1000h

At 85 °C ambient temperature .... 20 Years

Ambient temperature with power applied .... –55 °C to +150 °C

Supply voltage on V_{CC} relative to V_{SS}............–0.5 V to 4.1 V

Voltage applied to outputs in high Z state ....–0.5 V to V_{CC} + 0.5 V

Input voltage ....–0.5 V to V_{CC} + 0.5 V

Transient voltage (< 20 ns) on any pin to ground potential ....–2.0 V to V_{CC} + 2.0 V

Package power dissipation capability (T_A = 25 °C) .... .1.0 W

Surface mount Pb soldering temperature (3 seconds) .... +260 °C

DC output current (1 output at a time, 1 s duration).................................. 15 mA

Static discharge voltage (per MIL-STD-883, Method 3015) ....> 2001 V

Latch-up current ....> 200 mA

Operating Range

Range	Ambient Temperature	V_{CC}
Industrial	–40 °C to +85 °C	2.7 V to 3.6 V

DC Electrical Characteristics

Over the Operating Range

Parameter	Description	Test Conditions	Min	Typ [7]	Max	Unit
V_{CC}	Power supply	–	2.7	3.0	3.6	V
I_{CC1}	Average V_{CC} current	t_{RC} = 45 ns Values obtained without output loads (I_{OUT} = 0 mA)	–	–	57	mA
I_{CC2}	Average V_{CC} current during STORE	All inputs don’t care, V_{CC} = Max Average current for duration t_{STORE}	–	–	20	mA
I_{CC3}	Average V_{CC} current at t_{RC} = 200 ns, $V_{CC(Typ)}$, 25 °C	All inputs cycling at CMOS levels. Values obtained without output loads (I_{OUT} = 0 mA).	–	40	–	mA
I_{CC4}	Average V_{CAP} current during AutoStore cycle	All inputs don’t care. Average current for duration t_{STORE}	–	–	10	mA
I_{SB}	V_{CC} standby current	$\overline{CE} \geq (V_{CC} - 0.2\ V)$. $V_{IN} \leq 0.2\ V$ or $\geq (V_{CC} - 0.2\ V)$. Standby current level after nonvolatile cycle is complete. Inputs are static. f = 0 MHz.	–	–	10	mA
I_{IX}	Input leakage current	V_{CC} = Max, $V_{SS} \leq V_{IN} \leq V_{CC}$	–2	–	+2	µA
I_{OZ}	Off-state output leakage current	V_{CC} = Max, $V_{SS} \leq V_{OUT} \leq V_{CC}$, $\overline{CE}$ or $\overline{OE} \geq V_{IH}$ or $\overline{WE} \leq V_{IL}$	–2	–	+2	µA
V_{IH}	Input HIGH voltage	–	2.0	–	V_{CC} + 0.5	V
V_{IL}	Input LOW voltage	–	V_{ss} – 0.5	–	0.8	V
V_{OH}	Output HIGH voltage	I_{OUT} = –2 mA	2.4	–	–	V
V_{OL}	Output LOW voltage	I_{OUT} = 4 mA	–	–	0.4	V
V_{CAP}[8]	Storage capacitor	Between V_{CAP} pin and V_{SS}, 5 V rated	122	150	360	µF

Notes

7. Typical values are at 25 °C, $V_{CC} = V_{CC(Typ)}$. Not 100% tested.
8. Min V_{CAP} value guarantees that there is a sufficient charge available to complete a successful AutoStore operation. Max V_{CAP} value guarantees that the capacitor on V_{CAP} is charged to a minimum voltage during a Power-Up RECALL cycle so that an immediate power-down cycle can complete a successful AutoStore. Therefore it is always recommended to use a capacitor within the specified min and max limits. Refer application note AN43593 for more details on V_{CAP} options.

Data Retention and Endurance

Over the Operating Range

Parameter	Description	Min	Unit
$DATA_R$	Data retention	20	Years
NV_C	Nonvolatile STORE operations	1,000	K

Capacitance

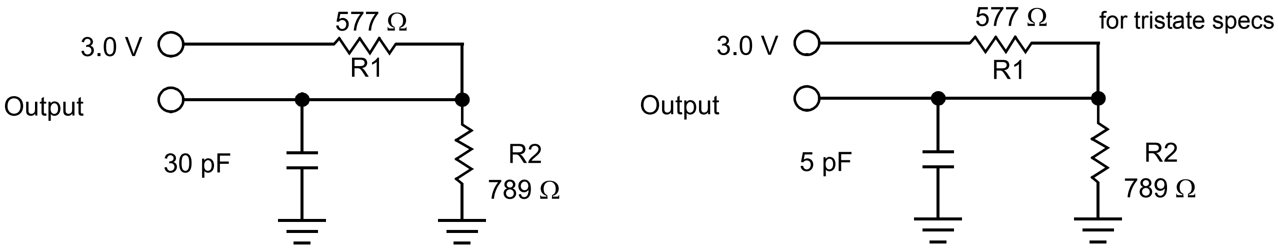
Parameter [9]	Description	Test Conditions	Max	Unit
C_{IN}	Input capacitance	T_A = 25 °C, f = 1 MHz, $V_{CC} = V_{CC(Typ)}$	14	pF
C_{OUT}	Output capacitance		14	pF

Thermal Resistance

Parameter [9]	Description	Test Conditions	44-pin TSOP II	Unit
θ_{JA}	Thermal resistance (junction to ambient)	Test conditions follow standard test methods and procedures for measuring thermal impedance, in accordance with EIA/JESD51.	31.11	°C/W
θ_{JC}	Thermal resistance (junction to case)		5.56	°C/W

AC Test Loads

Figure 10. AC Test Loads



AC Test Conditions

Input pulse levels ....0 V to 3 V

Input rise and fall times (10%–90%) .... ≤ 3 ns

Input and output timing reference levels .... 1.5 V

Note

[9] These parameters are guaranteed by design but not tested.

AC Switching Characteristics

Over the Operating Range

Parameters [10]		Description	45 ns		Unit
Cypress Parameter	Alt Parameter		Min	Max	
SRAM Read Cycle					
t_{ACE}	t_{ACS}	Chip enable access time	–	45	ns
t_{RC}[11]	t_{RC}	Read cycle time	45	–	ns
t_{AA}[12]	t_{AA}	Address access time	–	45	ns
t_{DOE}	t_{OE}	Output enable to data valid	–	20	ns
t_{OHA}[12]	t_{OH}	Output hold after address change	3	–	ns
t_{LZCE}[13, 14]	t_{LZ}	Chip enable to output active	3	–	ns
t_{HZCE}[13, 14]	t_{HZ}	Chip disable to output inactive	–	15	ns
t_{LZOE}[13, 14]	t_{OLZ}	Output enable to output active	0	–	ns
t_{HZOE}[13, 14]	t_{OHZ}	Output disable to output inactive	–	15	ns
t_{PU}[13]	t_{PA}	Chip enable to power active	0	–	ns
t_{PD}[13]	t_{PS}	Chip disable to power standby	–	45	ns
t_{DBE}	–	Byte enable to data valid	–	20	ns
t_{LZBE}[13]	–	Byte enable to output active	0	–	ns
t_{HZBE}[13]	–	Byte disable to output inactive	–	15	ns
SRAM Write Cycle					
t_{WC}	t_{WC}	Write cycle time	45	–	ns
t_{PWE}	t_{WP}	Write pulse width	30	–	ns
t_{SCE}	t_{CW}	Chip enable to end of write	30	–	ns
t_{SD}	t_{DW}	Data setup to end of write	15	–	ns
t_{HD}	t_{DH}	Data hold after end of write	0	–	ns
t_{AW}	t_{AW}	Address setup to end of write	30	–	ns
t_{SA}	t_{AS}	Address setup to start of write	0	–	ns
t_{HA}	t_{WR}	Address hold after end of write	0	–	ns
t_{HZWE}[13, 14, 15]	t_{WZ}	Write enable to output disable	–	15	ns
t_{LZWE}[13, 14]	t_{OW}	Output active after end of write	3	–	ns
t_{BW}	–	Byte enable to end of write	30	–	ns

Notes

[10] Test conditions assume signal transition time of 3 ns or less, timing reference levels of $V_{CC}/2$, input pulse levels of 0 to $V_{CC(typ)}$, and output loading of the specified I_{OL}/I_{OH} and load capacitance shown in Figure 10 on page 21.

[11] WE must be HIGH during SRAM read cycles.

[12] Device is continuously selected with CE and OE LOW.

[13] These parameters are guaranteed by design but not tested.

[14] Measured ±200 mV from steady state output voltage.

[15] If WE is LOW when CE goes LOW, the outputs remain in the high impedance state.

Switching Waveforms

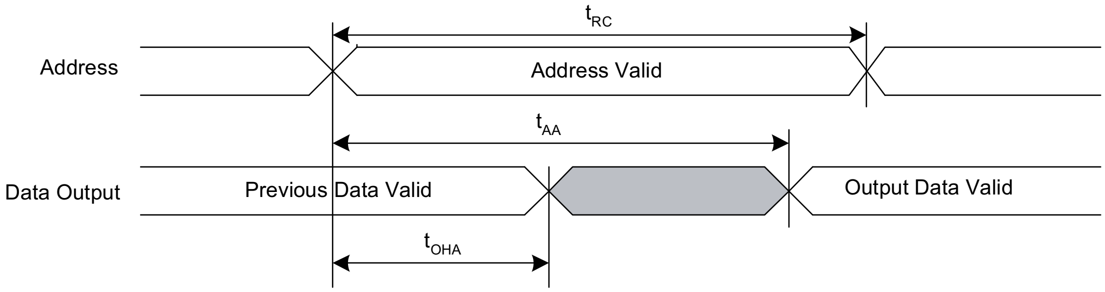


Figure 11. SRAM Read Cycle #1: Address Controlled [16, 17]

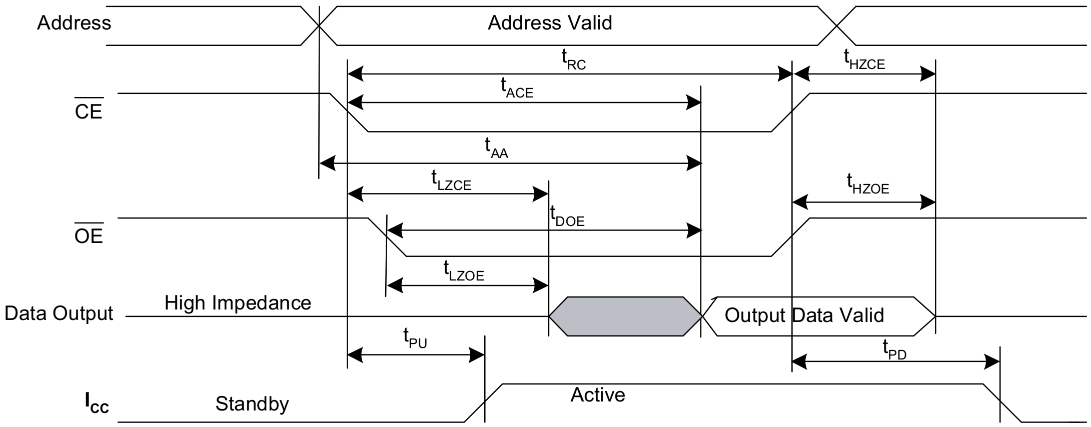


Figure 12. SRAM Read Cycle #2: CE and OE Controlled [16]

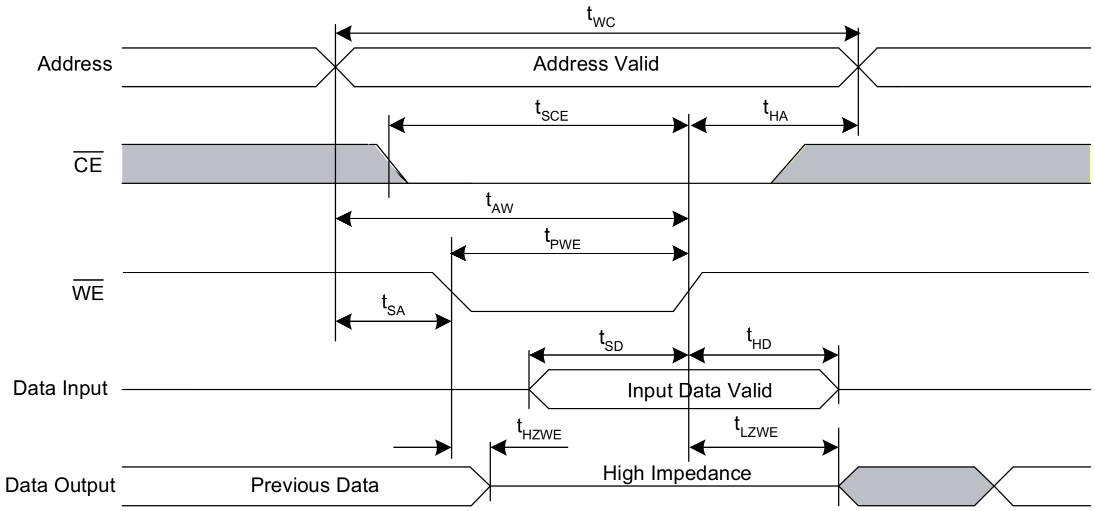


Figure 13. SRAM Write Cycle #1: WE Controlled [18, 19]

Notes

16. WE must be HIGH during SRAM read cycles.
17. Device is continuously selected with CE and OE LOW.
18. If WE is LOW when CE goes LOW, the outputs remain in the high impedance state.
19. CE or WE must be ≥V_{IH} during address transitions.

Switching Waveforms (continued)

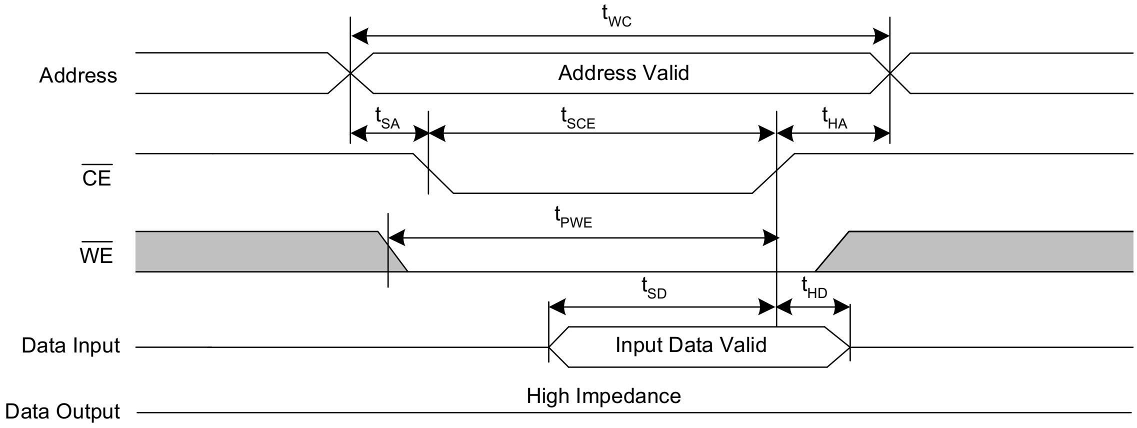


Figure 14. SRAM Write Cycle #2: $\overline{CE}$ Controlled [20, 21]

Notes

[20] If $\overline{WE}$ is LOW when $\overline{CE}$ goes LOW, the outputs remain in the high impedance state.

[21] $\overline{CE}$ or $\overline{WE}$ must be $\geq V_{IH}$ during address transitions.

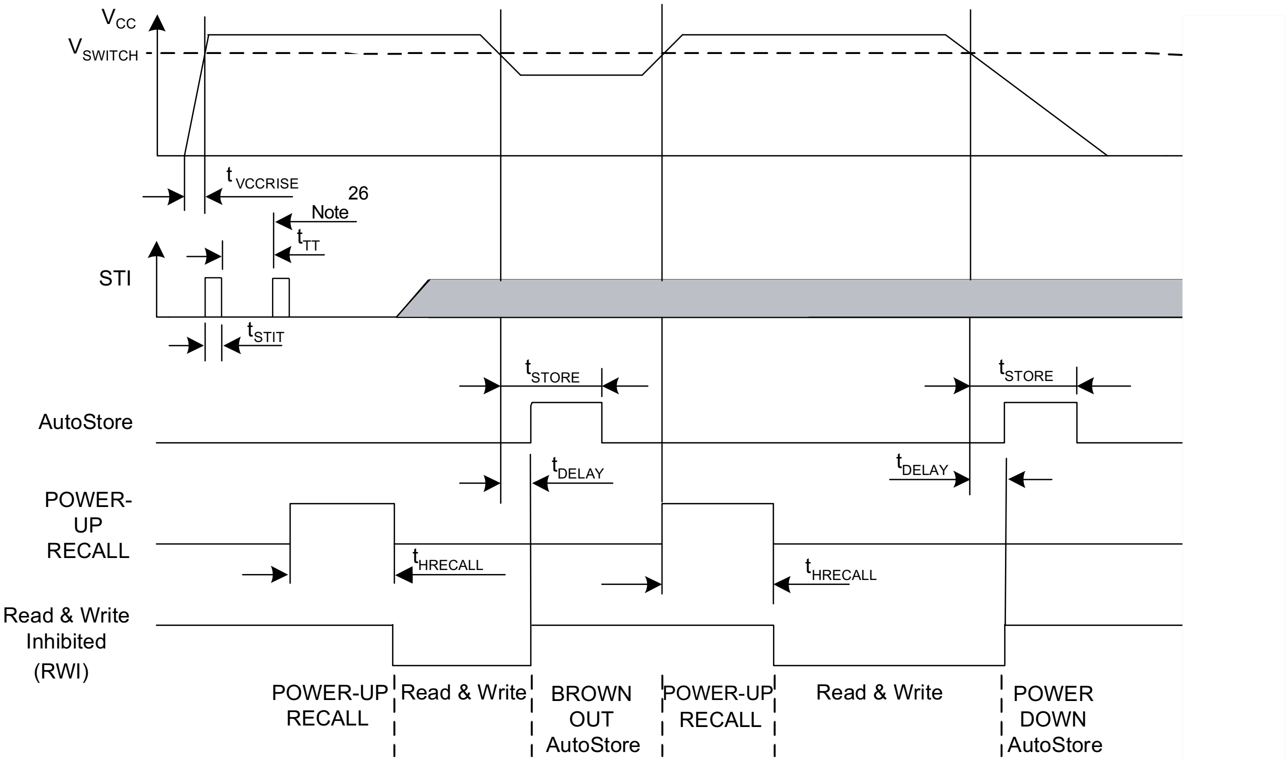
AutoStore/Power-up RECALL

Over the Operating Range

Parameter	Description	45 ns		Unit
		Min	Max	
$t_{HRECALL}$[22]	Power-up RECALL duration	–	20	ms
t_{STORE} [23]	STORE cycle duration	–	8	ms
t_{DELAY} [24]	Time allowed to complete SRAM write cycle	–	25	ns
V_{SWITCH}	Low voltage trigger level	–	2.65	V
$t_{VCCRISE}$[25]	V_{CC} rise time	150	–	µs
t_{STIT}	STI toggle time	25	75	µs
t_{TT}[26, 27]	Tamper timeout time	0.1	25.5	sec

Switching Waveforms - AutoStore/Power-up RECALL

Figure 15. AutoStore or Power-up RECALL [28]



Notes

[22] $t_{HRECALL}$ starts from the time V_{CC} rises above V_{SWITCH}.

[23] If an SRAM write has not taken place since the last nonvolatile cycle, no AutoStore or Hardware Store takes place.

[24] On a AutoStore initiation, SRAM write operation continues to be enabled for time t_{DELAY}.

[25] These parameters are guaranteed by design but not tested.

[26] If the valid password is not entered in the required time (t_{TT}) or exceed the attempt count, the device will execute destruction option at power-up according to the factory settings.

[27] t_{TT} will have a +/- 25% variation across temperature.

[28] Read and Write cycles are ignored during STORE, RECALL, and while V_{CC} is below V_{SWITCH}.

Software Controlled STORE/RECALL Cycle

Over the Operating Range

Parameter [29, 30]	Description	45 ns		Unit
		Min	Max	
t_{RC}	STORE/RECALL initiation cycle time	45	–	ns
t_{SA}	Address setup time	0	–	ns
t_{CW}	Clock pulse width	30	–	ns
t_{HA}	Address hold time	0	–	ns
t_{RECALL}	RECALL duration	–	200	µs
t_{SS} [31, 32]	Soft sequence processing time	–	100	µs

Switching Waveforms - Software Controlled STORE/RECALL Cycle

Figure 16. $\overline{CE}$ and $\overline{OE}$ Controlled Software STORE/RECALL Cycle [30]

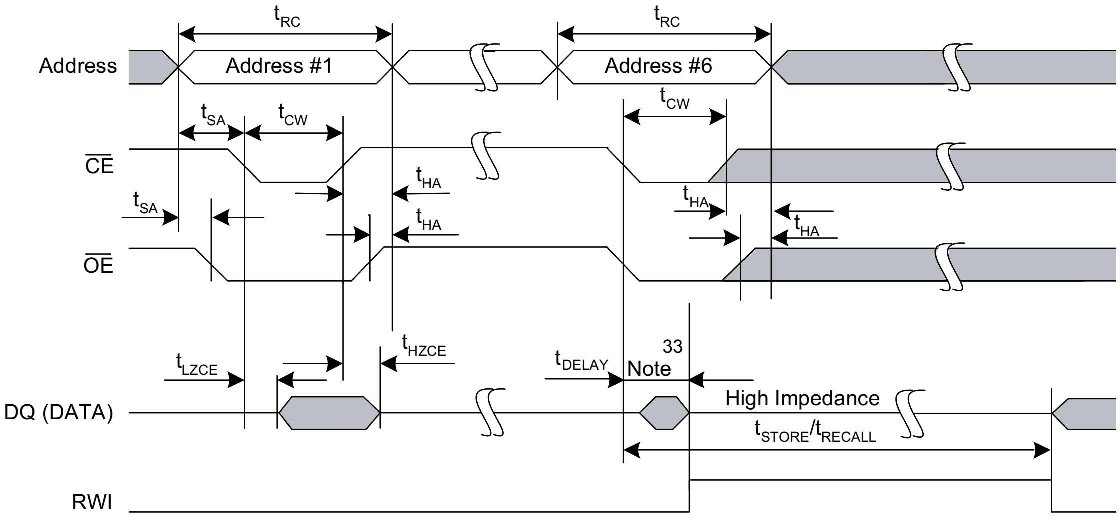
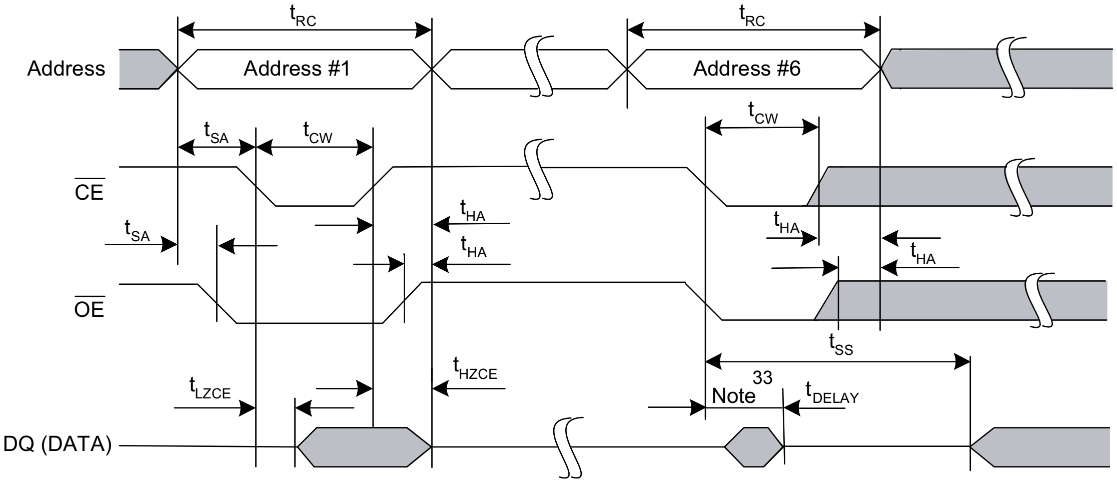


Figure 17. Autostore Enable/Disable Cycle



Notes

[29] The software sequence is clocked with $\overline{CE}$ controlled or $\overline{OE}$ controlled reads.

[30] The six consecutive addresses must be read in the order. WE must be HIGH during all six consecutive cycles.

[31] This is the amount of time it takes to take action on a soft sequence command. Vcc power must remain HIGH to effectively register command.

[32] Commands such as STORE and RECALL lock out I/O until operation is complete which further increases this time. See the specific command.

[33] DQ output data at the sixth read may be invalid since the output is disabled at t_{DELAY} time.

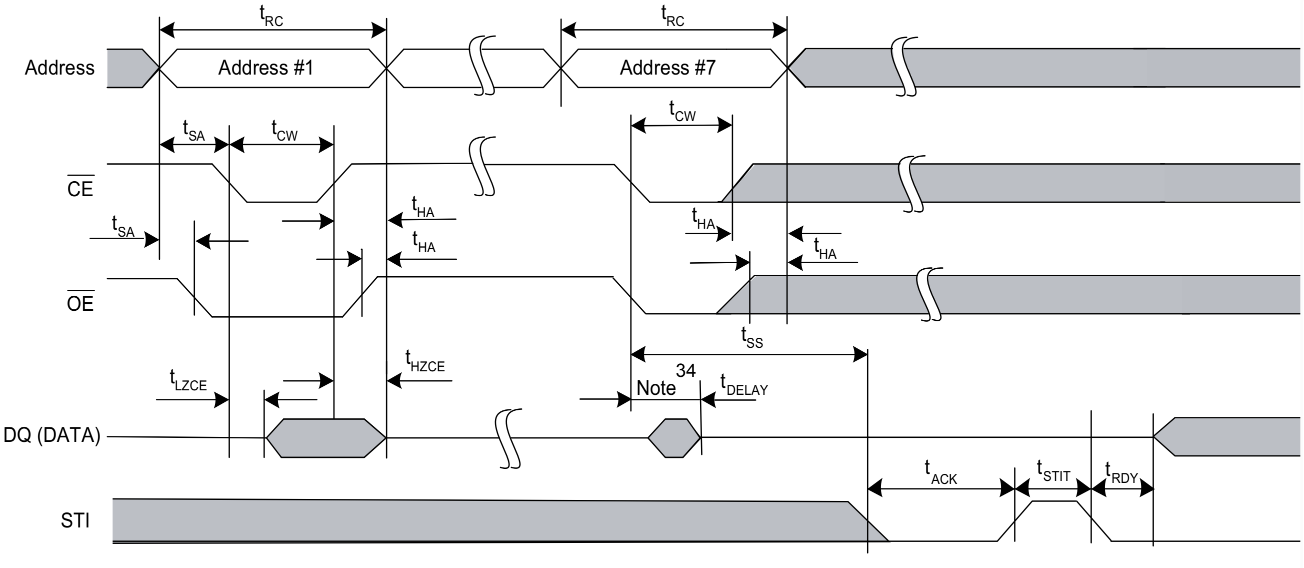
Tamper Protect Cycle

Over the Operating Range

Parameter	Description	45 ns		Unit
		Min	Max	
t_{ACK}	End of Password Entry cycle/Anti-Tamper feature cycle to STI toggle	–	575	µs
t_{RDY}	End of Password Entry cycle - STI toggle LOW to device ready	–	500	µs
t_{TPCT}	Tamper Protect Cycle entry time	–	1	ms
t_{SSDD}	End of data destruction soft sequence to actual destruction	–	8	ms
t_{PUDD}	End of password time out to actual data destruction	–	8	ms

Switching Waveforms - Tamper Protect Cycle

Figure 18. End Password Entry Cycle



Note

[34] DQ output data at the sixth read may be invalid since the output is disabled at t_{DELAY} time.

Switching Waveforms - Tamper Protect Cycle (continued)

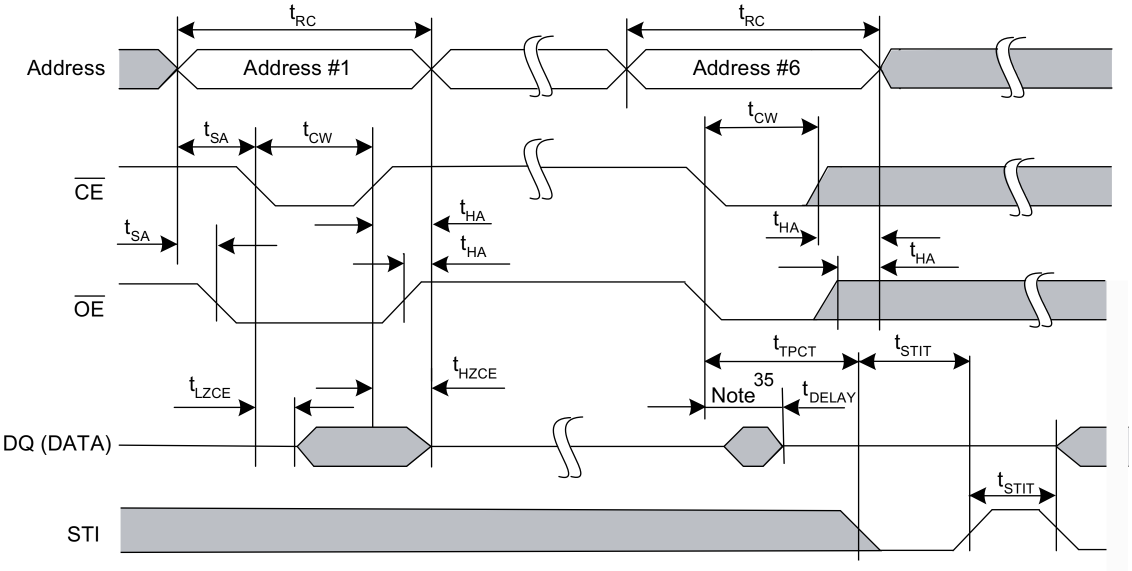
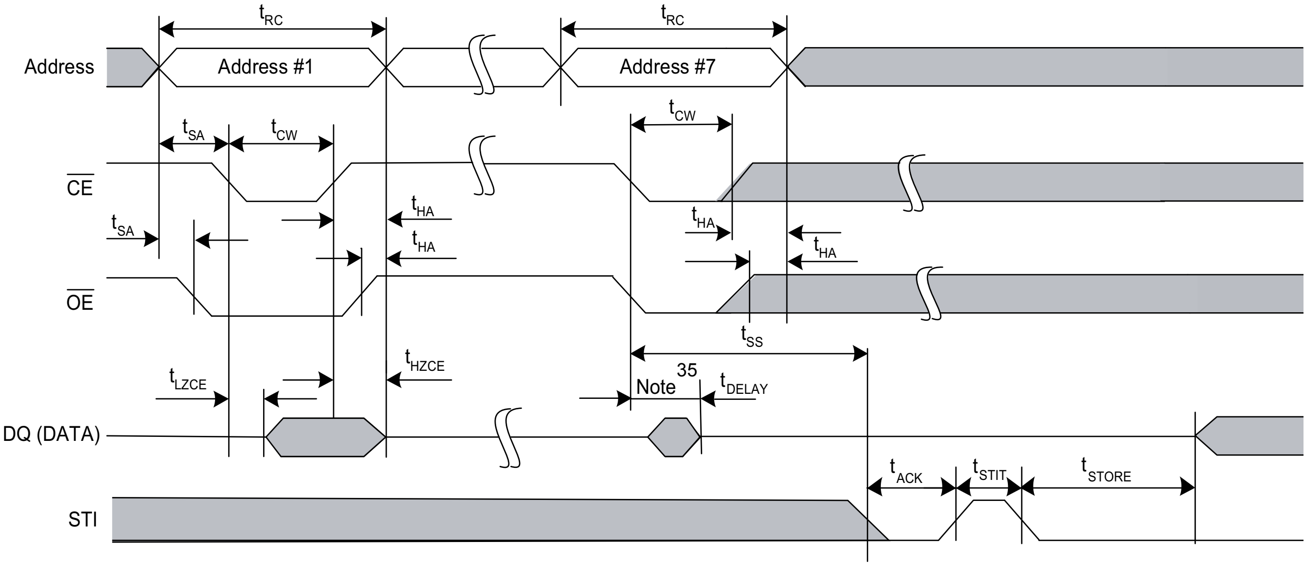


Figure 19. Tamper Protect Cycle

Figure 20. Change Tamper Timeout, Password Disable/Enable, Change password, Destruction Disable/Enable Cycle



Note

35. DQ output data at the sixth read may be invalid since the output is disabled at t_{DELAY} time.

Switching Waveforms - Tamper Protect Cycle (continued)

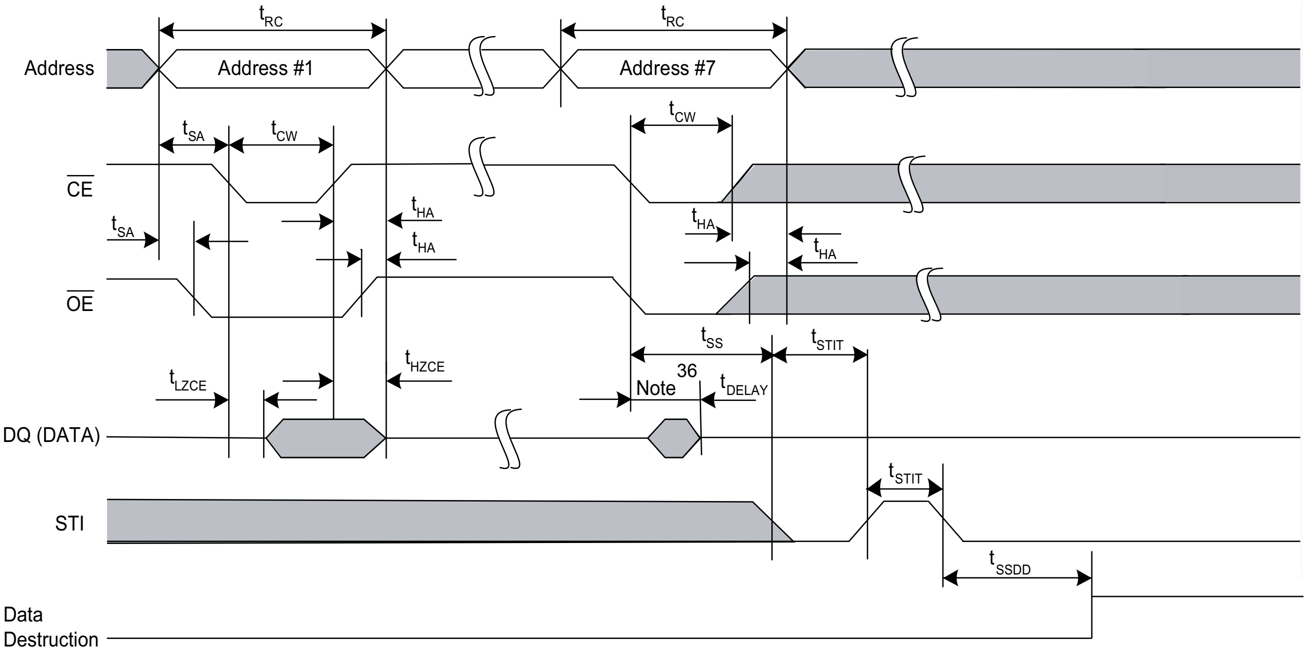
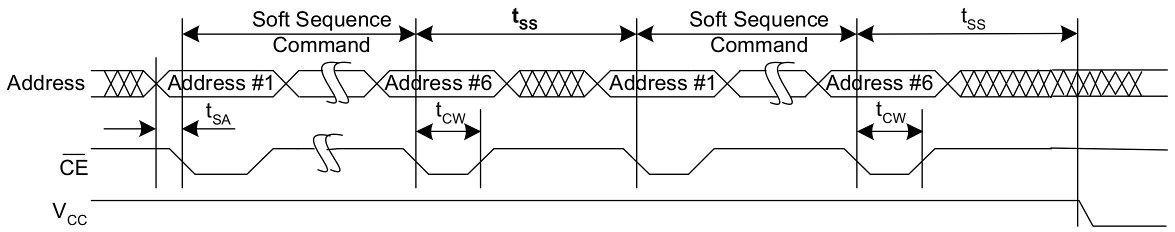


Figure 21. Data Destruction Cycle

Figure 22. Soft Sequence Processing [37, 38]



Notes

[36] DQ output data at the sixth read may be invalid since the output is disabled at t_{DELAY} time.
[37] This is the amount of time it takes to take action on a soft sequence command. V_{CC} power must remain HIGH to effectively register command.
[38] Commands such as STORE and RECALL lock out I/O until operation is complete which further increases this time. See the specific command.

Truth Table For SRAM Operations

For × 8 Configuration

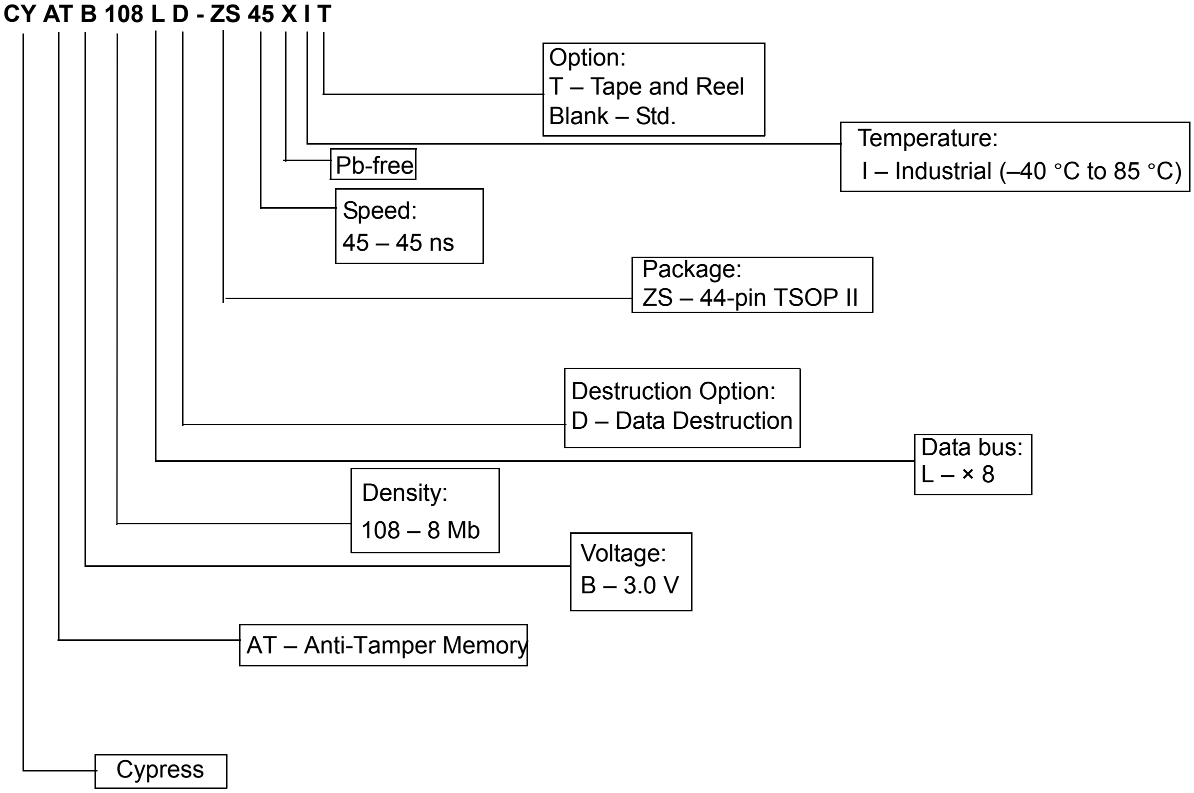
$\overline{CE}$	$\overline{WE}$	$\overline{OE}$	Inputs/Outputs	Mode	Power
H	X	X	High Z	Deselect/power-down	Standby
L	H	L	Data-out (DQ_0–DQ_7);	Read	Active
L	H	H	High Z	Output disabled	Active
L	L	X	Data-in (DQ_0–DQ_7);	Write	Active

Ordering Information

Speed (ns)	Ordering Code	Package Diagram	Package Type	Operating Range
45	CYATB108LD-ZS45XI	51-85087	44-pin TSOP II	Industrial
	CYATB108LD-ZS45XIT			

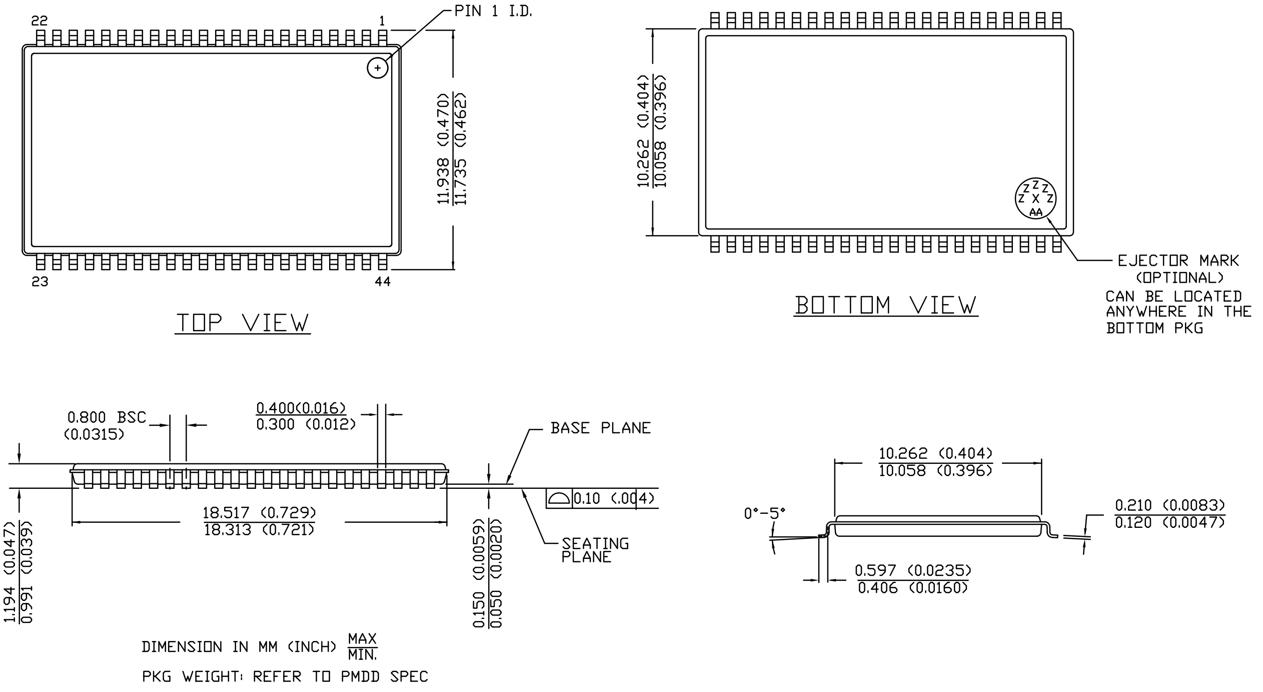
The Cypress Anti-Tamper Memory can be customized to meet your application needs. Please contact antitamper@cypress.com for ordering details.

Ordering Code Definitions



Package Diagram

Figure 23. 44-pin TSOP Z44-II Package Outline, 51-85087



51-85087 *E

Acronyms

Acronym	Description
$\overline{CE}$	chip enable
CMOS	complementary metal oxide semiconductor
EIA	electronic industries alliance
I/O	input/output
nvSRAM	non-volatile static random access memory
$\overline{OE}$	output enable
RoHS	restriction of hazardous substances
RWI	read and write inhibited
SRAM	static random access memory
TSOP	thin small outline package
$\overline{WE}$	write enable

Document Conventions

Units of Measure

Symbol	Unit of Measure
°C	degree Celsius
MHz	megahertz
µA	microampere
µF	microfarad
µs	microsecond
mA	milliampere
ms	millisecond
ns	nanosecond
%	percent
pF	picofarad
V	volt
Ω	ohm
W	watt

Errata

This section describes the errata for the 8 Mb (2048 K × 8) nvSRAM product families. Details include errata trigger conditions, scope of impact, available workarounds, and silicon revision applicability.

Contact your local Cypress Sales Representative if you have questions. You can also send your related queries directly to nvSRAM@cypress.com.

Part Numbers Affected

Part Number	Device Characteristics
CYATB108LD	1024 K × 8, Asynchronous Interface nvSRAM in 44 TSOP-II package option

8Mb (1024 K × 8) nvSRAM Qualification Status

Production parts.

8Mb (1024 K × 8) nvSRAM Errata Summary

The following table defines the errata applicability to available CYATB108LD device.

Items	Part Number	Silicon Revision	Fix Status
1. AutoStore Disable feature does not work correctly	CYATB108LD	Rev 0	None. This issue is applicable to all 8Mb nvSRAM parts in production

1. AutoStore Disable feature does not work correctly

- **Problem Definition**

  The AutoStore Disable soft sequence disables the AutoStore feature in nvSRAMs. The AutoStore Disable feature is used in applications where data written in the SRAM is not required to be saved automatically on power loss. The 8Mb nvSRAM executes the nonvolatile Store automatically in half the memory (4Mb) even after the AutoStore feature is disabled. The reason is as follows:

  The 8Mb nvSRAM uses two dice stack of 4Mb with $\overline{\text{HSB}}$ pin of each die are tied together. Each nvSRAM die in the stacked-die monitors the V_{CC} power independently. When the device V_{CC} fails, the die which detects the V_{CC} dropping below V_{SWITCH} first, internally triggers the power down interrupt and drives its $\overline{\text{HSB}}$ output low. Since the $\overline{\text{HSB}}$ is a bidirectional pin, the low $\overline{\text{HSB}}$ output driven by one die is detected as $\overline{\text{HSB}}$ input by the other die. Therefore, low on the $\overline{\text{HSB}}$ input of other die internally triggers hardware Store and executes unintended nonvolatile Store even though AutoStore was disabled by AutoStore Disable soft sequence.

- **Parameters Affected**

  None.

- **Trigger Condition(S)**

  Device V_{CC} power down with nvSRAM AutoStore disable.

- **Scope of Impact**

  It can corrupt the data in half of the memory by overwriting the existing data in its nonvolatile memory with unintended data.

- **Workaround**

  None. AutoStore disable feature should not be used in 8Mb nvSRAMs.

- **Fix Status**

  This issue is applicable to all 8Mb nvSRAM parts in production and will continue serving with errata. There is no plan to fix this issue in the existing parts in production.

Document History Page

Document Title: CYATB108LD, 8-Mbit (1024 K × 8) Anti-Tamper Memory
Document Number: 001-65351

Rev.	ECN No.	Orig. of Change	Submission Date	Description of Change
**	3100066	GVCH	12/02/10	New datasheet
*A	3292228	GVCH	08/30/11	Datasheet status changed from “Advance” to “Preliminary” Removed functional and physical destruction related information Updated Logic Block Diagram Updated Pinout (Updated Figure 1 ($\overline{\text{HSB}}$ pin is made as DNU and defined pin 1 as STI pin). Updated Pin Definitions (Removed $\overline{\text{HSB}}$ pin definition and Added STI pin definition, removed HSB pin related information). Updated Device Operation (Updated Tamper Protect (changed location from FFFF0–FFFF4 to FFFF1–FFFF5, replaced the sub-section Password Entry Time is by Change Tamper Timeout and memory location changed from FFFFF to FFFF1 in the same section, updated Change Password (updated memory location), added sub-sections Password Disable/Enable and Destruction Disable/Enable), updated Table 1 and added Table 2, added more clarity to Figure 3, Figure 4, Figure 6 and Figure 7, added Figure 5, Figure 8 and Figure 9). Updated DC Electrical Characteristics (Added Note 8 and referred the same note in V_{CAP} parameter). Updated AC Switching Characteristics (Added Note 10 and referred the same note in parameters column). Updated AutoStore/Power-up RECALL (Added t_{STIT} parameter and its details, removed t_{HSBT} parameter and its details, T_{PT} parameter naming convention is changed to t_{TT}, updated Figure 15). Updated Software Controlled STORE/RECALL Cycle (Updated Note 26). Updated Tamper Protect Cycle (Table).
*B	3420760	GVCH	12/13/2011	Updated Tamper Protect (Updated description, updated sub sections Change Tamper Timeout (Updated description), Updated sub sections Destruction Option (Added Note at the end)). Updated Preventing AutoStore (Added Note at the end). Updated AutoStore/Power-up RECALL (Changed minimum value of t_{STIT} parameter from blank to 25 μs, changed maximum value of t_{STIT} parameter from 55 μs to 75 μs, changed maximum value of t_{TT} parameter from 25.6 sec to 25.5 sec, added Note 27 and referred the same in t_{TT} parameter). Updated Tamper Protect Cycle (Changed minimum value of t_{ACK} parameter from 100 μs to blank, added t_{RDY} parameter and its details, added t_{TPCT} parameter and its details). Updated Switching Waveforms - Tamper Protect Cycle (Updated Figure 18, Figure 19, Figure 21, added Note 36 and referred the same in Figure 21).
*C	3532419	GVCH	02/22/2012	Changed status from Preliminary to Final.
*D	4612154	GVCH	01/23/2015	Updated Package Diagram: spec 51-85087 – Changed revision from *D to *E. Added Errata. Updated to new template. Completing Sunset Review.

Sales, Solutions, and Legal Information

Worldwide Sales and Design Support

Cypress maintains a worldwide network of offices, solution centers, manufacturer's representatives, and distributors. To find the office closest to you, visit us at Cypress Locations.

Products

Automotive	cypress.com/go/automotive
Clocks & Buffers	cypress.com/go/clocks
Interface	cypress.com/go/interface
Lighting & Power Control	cypress.com/go/powerpsoc
Memory	cypress.com/go/memory
PSoC	cypress.com/go/psoc
Touch Sensing	cypress.com/go/touch
USB Controllers	cypress.com/go/USB
Wireless/RF	cypress.com/go/wireless

PSoC® Solutions

psoc.cypress.com/solutions

PSoC 1 | PSoC 3 | PSoC 4 | PSoC 5LP

Cypress Developer Community

Community | Forums | Blogs | Video | Training

Technical Support

cypress.com/go/support

Disclaimer: CYPRESS MAKES NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Cypress reserves the right to make changes without further notice to the materials described herein. Cypress does not assume any liability arising out of the application or use of any product or circuit described herein. Cypress does not authorize its products for use as critical components in life-support systems where a malfunction or failure may reasonably be expected to result in significant injury to the user. The inclusion of Cypress' product in a life-support systems application implies that the manufacturer assumes all risk of such use and in doing so indemnifies Cypress against all charges.