Using 2.7V – 3.6V CryptoMemory® Devices in 5V Designs

1. Introduction

The new generation of CryptoMemory® devices, identifiable by the "CA" in their catalog base name as in AT88SC0104CA, operates within the voltage range of 2.7V – 3.6V but are fully backward compatible with older generation CryptoMemory devices that operate within the voltage range of 2.7V – 5.5V. Narrowing of the operating voltage range is a security improvement to keep with low voltage design trends. Acknowledging the fact that not every application is suited for low voltage operation, the new generation CryptoMemory devices were designed to be 5V tolerant such that with minor adaptations, they can operate within 5V applications without compromise to security. This application note describes how to adapt the 2.7V – 3.6V CryptoMemory devices to operate in 5V applications.

2. Improved Security with 2.7V – 3.6V Narrow V_{CC} Range

CryptoMemory devices possess countermeasures against a wide variety of physical and systematic security attack methods in order to assure the confidentiality and integrity of keys and sensitive content resident within them. One of such countermeasures is that against attacks on the device's supply voltage, V_{CC}. CryptoMemory deploys this countermeasure by defining a narrow operating range for V_{CC} and employs voltage tamper monitoring circuits to limit operation only within this range. A narrower operating voltage range offers better security because it leaves little room for voltage attacks. The narrower 2.7V – 3.6V operation range in the new generation CryptoMemory is therefore a security improvement over the 2.7V – 5.5V wider range of older generation devices.

3. CryptoMemory Signal Pins Remain 5V Tolerant

Narrowing of the V_{CC} operating range for the new generation CryptoMemory devices is purely for security improvement. The device remains capable of operating in 5V application environments without risk of physical destruction. As such the signal pins (SDA and SCL) are capable of operating over the full voltage range of 0V – 5.5V as with all generations of CryptoMemory devices. They are 5V tolerant and require no special conditioning for connection to microcontrollers. The 2.7V – 3.6V voltage constraint therefore applies only to V_{CC}.

4. Designing the 2.7V – 3.6V CryptoMemory into 5V Applications

The only requirement for designing the new generation CryptoMemory into a 5V application is to make sure the V_{CC} of the CryptoMemory device is within 2.7V – 3.6V. Connect the signal pins as you would with any 5V CryptoMemory device. The following figure illustrates this setup.

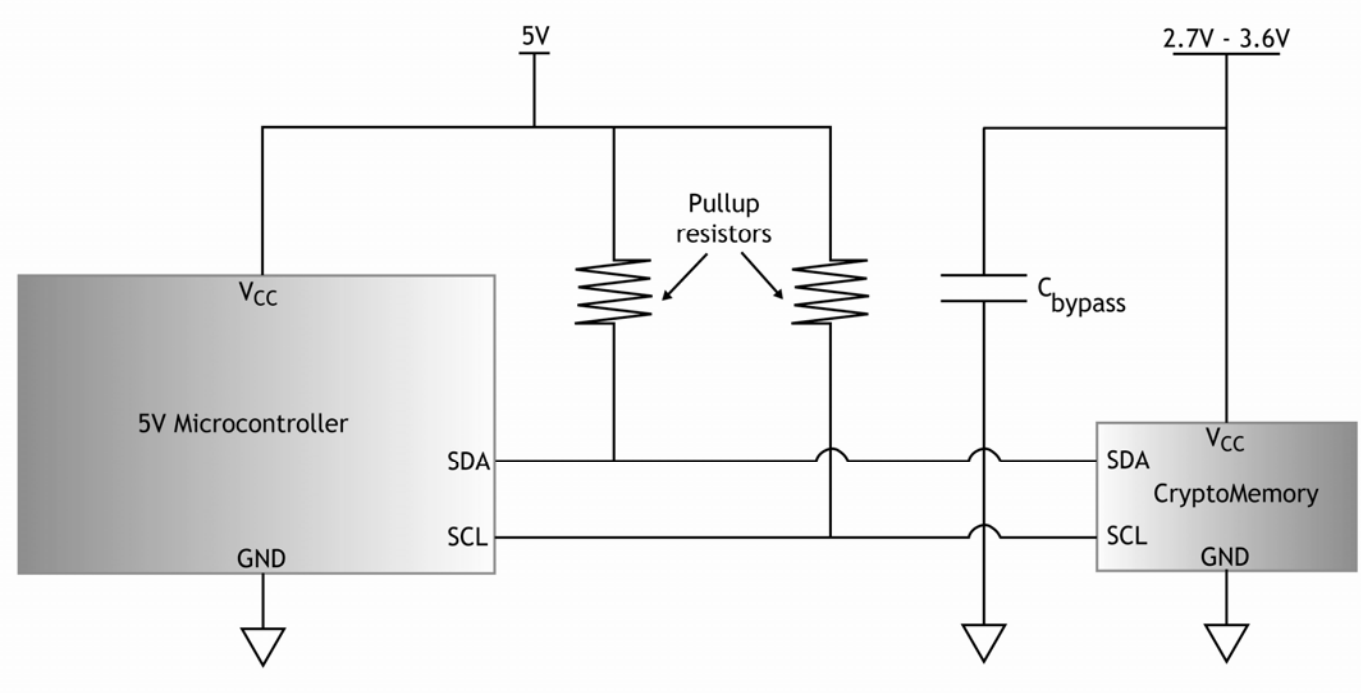
Using 2.7V – 3.6V CryptoMemory Devices in 5V Designs

AT88SC0104CA
AT88SC0204CA
AT88SC0404CA
AT88SC0808CA

Application Note

8661A–CryptoMemory–4/09

Figure 1. 2.7V - 3.6V CryptoMemory in a 5V system



5. Circuit Examples

Many circuit techniques for stepping down a 5V voltage source to 3V exist. While these techniques have different advantages and disadvantages, their proper application to CryptoMemory only require that the output voltage remain fairly stable and that they deliver sufficient current to satisfy CryptoMemory device's loading requirements.

The voltage step-down circuit should deliver a fairly stable output voltage to the CryptoMemory device's V_{CC} pin. The output voltage may vary but should not exceed the bounds of 2.7V and 3.6V. Variations close to these bounds run the risk of triggering V_{CC} tamper monitors within the CryptoMemory device.

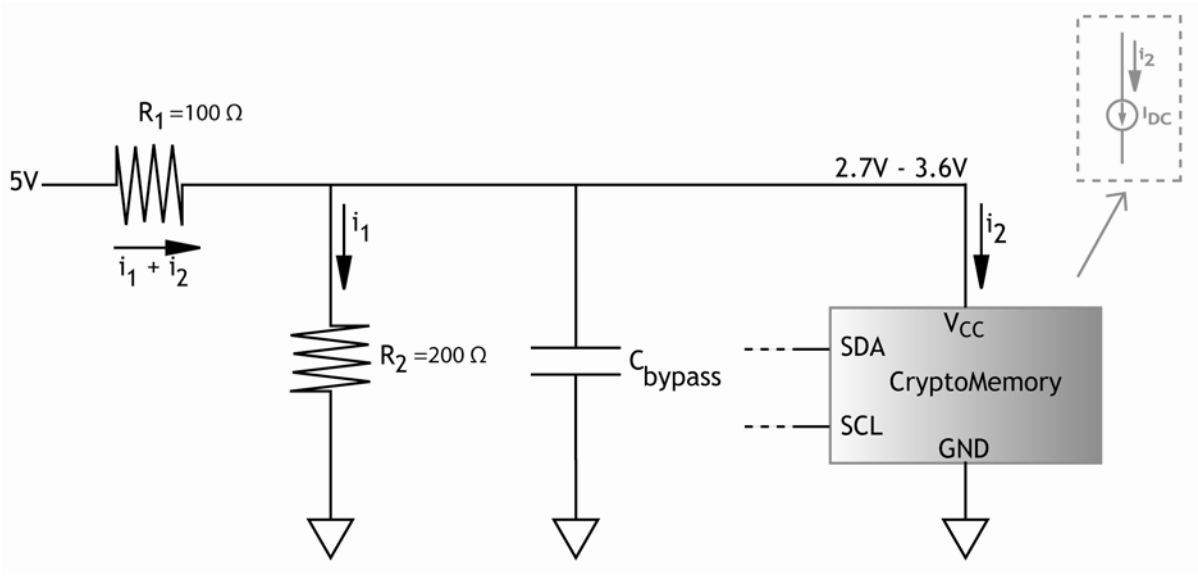
The voltage step-down circuit should also deliver sufficient current to satisfy the CryptoMemory device's requirements. Loading by the CryptoMemory devices varies depending on the internal operation in progress such as EEPROM read, write, or erase cycles. The maximum current, however, shall never exceed 5mA. To guarantee sufficient current supply, it is therefore recommended that the voltage step-down circuit network be capable of delivering 5mA of current to CryptoMemory.

The proceeding sections show examples of viable circuit techniques applicable to stepping down a 5V board supply to satisfy the CryptoMemory device's V_{CC} requirements. Connections to the microcontroller remain the same as in Figure 1, and have been removed in subsequent illustrations for clarity. Just as for 5V CryptoMemory devices, the application is expected to have bypass capacitors on the CryptoMemory device's V_{CC}. Typical values are 1uF and 10nF connected in parallel from V_{CC} to ground. Depending on the design, a single bypass capacitor with a value between 10nF to 1uF might suffice.

5.1. Example: Using a Voltage Divider Resistor Network

A couple of resistors in a simple voltage divider network can step down the board voltage to meet the CryptoMemory device requirements. Figure 2 illustrates such a network.

Figure 2. Voltage divider resistor network where CryptoMemory can be modeled as a constant current load.



Values for R1 and R2 can be determined from the following set of equations:

R_1 must be low enough to allow the max supply current to flow to the CryptoMemory device. Therefore, the selection of R_1 is governed by (1).

$$R_1 \leq \frac{5V - V_{CC}}{I_1 + 5mA} \qquad (1)$$

Where 5mA is the specified maximum current CryptoMemory can ever draw.

And 5V is assumed to be the operating voltage of the board design.

Next, R_1 and R_2 must maintain a given ratio for the appropriate voltage division. This ratio, provided in (2) is solvable by applying the constraints imposed by the V_{CC} voltage limits as follows:

$$V_{CC} = \frac{R_2}{R_1 + R_2}\left[5V - I_2 R_1\right]_{I_2 = 5mA, V_{CC} \geq 2.7V}^{I_2 = 100uA, V_{CC} \leq 3.6V}$$

or

$$R_2 = R_1\left[\frac{V_{CC}}{5V - R_1 I_2 - V_{CC}}\right]_{I_2 = 5mA,\ V_{CC} \geq 2.7V,\ Lower\ Bound}^{I_2 = 100uA,\ V_{CC} \leq 3.6V,\ Upper\ Bound}$$

Hence

$$\frac{R_1}{R_2} \geq 0.46 \qquad (2)$$

Therefore (1) governs the current budget for CryptoMemory and (1) determines the voltage division ratio. In short, choose R1 and R2 such that

$$0.46R_2 \leq R_1 \leq \frac{5V - V_{CC}}{I_1 + 5mA}$$

Example
We find that values of R_1 =100Ω, and R_2 = 200 Ω work suitably well and will keep V_{CC} within the range of 2.7V – 3.6V irrespective of the amount of current drawn by CryptoMemory.

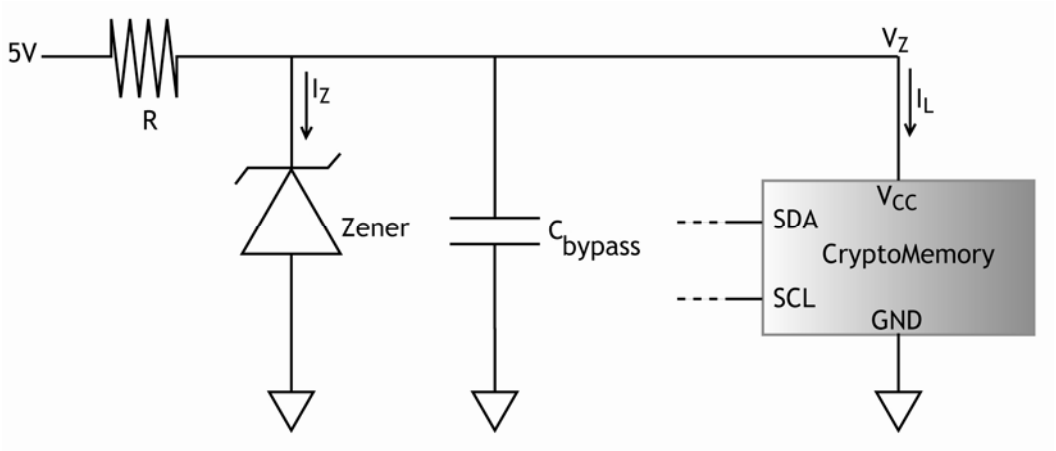
This technique is probably the easiest, cheapest, and most versatile due to the wide availability of resistors with various resistance values. However, it may offer the least precision due to varying tolerances on commercially available resistors and the resistors may sink high current in standby. If adopting this technique, we recommend 10% or better quality resistors in order to minimize tolerance variability and variability due to environmental factors like temperature. Also pay attention to the power rating of the resistors to make sure they can handle the I_1 and I_2 without damage.

5.2. Example: Using a Zener Diode

A zener diode offers a more precise way than the voltage divider network to generate a constant voltage output for the CryptoMemory device's V_{CC}. The output voltage from the zener network will remain constant even with variable loading by the CryptoMemory device from its internal operations.

To design a step-down circuit using a zener diode, choose a commercially available zener diode with a reverse breakdown voltage rating around 3V and a load current capacity no less than 5mA. Figure 3 illustrates the zener voltage regulator network.

Figure 3. Zener diode voltage limiter



The next step is to decide on the appropriate value of R to keep the zener diode in reverse breakdown mode. Solve for R from the equation:

$$R = \frac{5 - V_Z}{I_Z - I_L} \quad (3)$$

Where:

- It is assumed the system is operating at 5V otherwise change 5 to the actual system voltage
- V_Z is the reverse breakdown voltage rating which we want to be close to 3V (i.e. within 2.7V – 3.6V range)
- I_L is the desired amount of current to budget for CryptoMemory operations, preferably up to 5mA
- I_Z is the zener current normally reported in the zener diode device specification

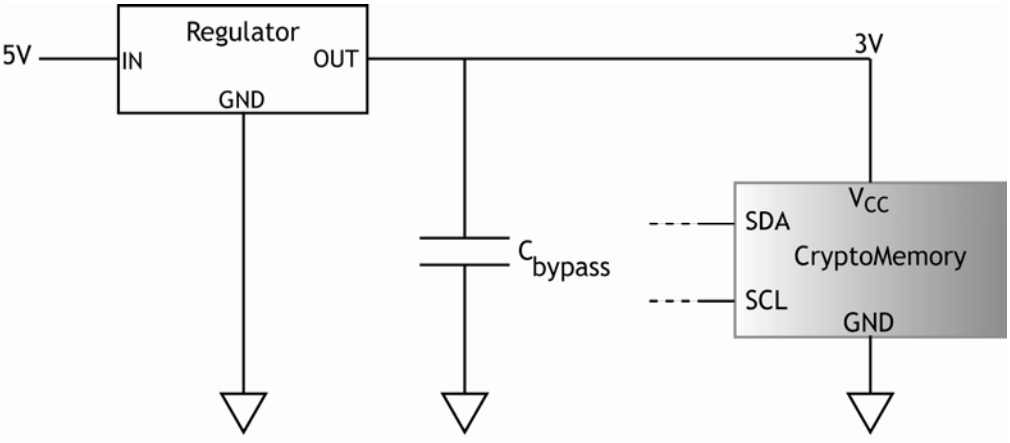
While zener diodes offer more precise and less environmentally sensitive alternative to resistors, one still has to watch out for a couple of things: R must be small enough so that enough current goes through the zener diode to keep it in reverse breakdown mode, and large enough to limit the current from destroying the diode. Just as in the case for the resistor network, the current sink in standby is also of concern. In essence, careful thought must go into the selection of the resistor R. It should be of high quality with minimal variance from changes in environmental parameters like temperature.

If using a ZMM5227BDITR zener diode for example, choose a nominal value for R = 280 Ω for a constant voltage of 3.3V.

5.3. Example: Using a Voltage Regulator IC

A sure way to assure the CryptoMemory device's V_{CC} remains within the operation range is to use a linear voltage regulator IC. The regulator will take the board voltage input and supply a constant voltage around 3V to the CryptoMemory device. Figure 4 illustrates the step-down circuit using a voltage regulator.

Figure 4. Using a voltage regulator



The advantage of using a voltage regulator is that it provides a constant voltage with better internal compensation for environmental changes. It may also be the case that the 5V in the system derives from a higher supply voltage using a regulator that already has a 3V output option. Should this be the case then the solution is to simply connect the 3V output of the regulator to the CryptoMemory device's V_{CC} pin. If the situation permits, then using a voltage regulator is our best recommendation. An example of a linear regulator is LM1117MP-3.3CT for a 3.3V regulated output.

6. Conclusion

While the new generation 2.7V – 3.6V CryptoMemory offers tighter security limits on its operating voltage, it remains fully backward compatible with older generation 2.7V – 5.5V CryptoMemory devices. The signal pins are 5V tolerant and require no additional conditioning to operate in 5V applications just like the older generation devices. To avoid triggering voltage security tampers in the new CryptoMemory devices, V_{CC} must remain within the specified operating limits. This application note explores various techniques for complying with these limits within 5V applications.

7. Revision History

Doc. Rev.	Date	Comments
8661A	4/2009	Initial document release

Headquarters

Atmel Corporation
2325 Orchard Parkway
San Jose, CA 95131
USA
Tel: 1(408) 441-0311
Fax: 1(408) 487-2600

International

Atmel Asia
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimshatsui
East Kowloon
Hong Kong
Tel: (852) 2721-9778
Fax: (852) 2722-1369

Atmel Europe
Le Krebs
8, Rue Jean-Pierre Timbaud
BP 309
78054 Saint-Quentin-en-
Yvelines Cedex
France
Tel: (33) 1-30-60-70-00
Fax: (33) 1-30-60-71-11

Atmel Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
Tel: (81) 3-3523-3551
Fax: (81) 3-3523-7581

Product Contact

Web Site
www.atmel.com

Technical Support
CryptoMemory@atmel.com

Sales Contact
www.atmel.com/contacts

Literature Requests
www.atmel.com/literature