

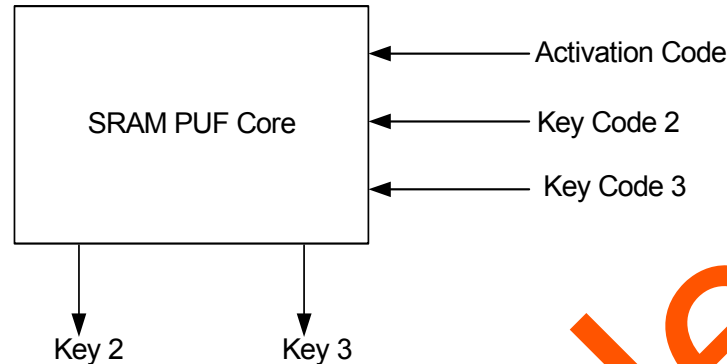




## Key Reconstruction

The keys have to be reconstructed because they are not stored in the memory. To reconstruct the keys, activation code and key codes are required as shown in [Figure 1](#).

SRAM PUF core reconstructs the original intrinsic or extrinsic keys.



**Figure 1 • Key Reconstruction**

This application note also provides the design example to access the following SRAM-PUF services. For more information on SRAM-PUF services, refer to the "SRAM-PUF Services" section on [page 4](#).

- Create User AC (Activation Code)
- Delete User AC
- Get Number of KC (Key Code)
- Create User KC for an Intrinsic Key
- Create User KC for an Extrinsic Key
- Export all KC
- Import all KC
- Delete User KC
- Fetch a User PUF Key
- Get a PUF Seed

## System Controller Block in SmartFusion2 Device

The SRAM PUF services provide access to the system controller's PUF core. SRAM PUF core block is accessed through the communication block (COMM\_BLK).

There are two COMM\_BLK instances located in:

- Microcontroller subsystem (MSS)
- System Controller

The COMM\_BLK consists of an APB interface, eight byte transmit FIFO, and eight byte receive FIFO. The COMM\_BLK provides a bi-directional message passing facility between the MSS and the system controller.

The PUF system services are initiated using the COMM\_BLK in the MSS, which can be read or written by any master on the AMBA® high performance bus (AHB) matrix; typically either the Cortex-M3 processor or a design in the FPGA fabric (also known as a fabric master).

The system controller receives the command through the COMM\_BLK in the system controller. On completion of the requested service, the system controller returns a status message through the COMM\_BLK. The responses generated are based on the selected command.



































