4.2.9 UICR — User information configuration registers

The user information configuration registers (UICR) are non-volatile memory (NVM) registers that configure user specific settings and values for emulated one-time programmable (OTP).

All UICR registers have a RW1 protection, which means that they can be read multiple times, but written only once when UICR has been erased by the Erase All operation.

For information on writing registers, see RRAMC — Resistive random access memory controller on page 47 and Memory on page 13.

Notice that all access port protection registers are duplicated into PROTECT0/PROTECT1. For optimal security, set both registers set to "random" values different from the Unprotected value. For ERASEPROTECT, set both PROTECT0/PROTECT1 registers to the Protected value.

4.2.9.1 Registers

Instances

Instance	Domain	Base address	TrustZone			Split access	Description
			Map	Att	DMA		
UICR	GLOBAL	0x00FFD000	HF	S	NA	No	User information configuration

Register overview

Register	Offset	TZ	Description
APPROTECT[n].PROTECT0	0x000		Access port protection
APPROTECT[n].PROTECT1	0x01C		Access port protection
SECUREAPPROTECT[n].PROTECT0	0x020		Access port protection
SECUREAPPROTECT[n].PROTECT1	0x03C		Access port protection register
AUXAPPROTECT[n].PROTECT0	0x040		Access port protection
AUXAPPROTECT[n].PROTECT1	0x05C		Access port protection register
ERASEPROTECT[n].PROTECT0	0x60		Erase protection
ERASEPROTECT[n].PROTECT1	0x7C		Erase protection
BOOTCONF	0x080		Immutable boot region configuration.
USER.ROT.PUBKEY[n].DIGEST[o]	0x200		First 256 bits of SHA2-512 digest over RoT public key generation [n].
USER.ROT.PUBKEY[n].REVOKE[o]	0x220		Revocation status for RoT public key generation [n].
USER.ROT.AUTHOPKEY[n].DIGEST[o]	0x2B0		First 256 bits of SHA2-512 digest over RoT authenticated operation public key generation [n].
USER.ROT.AUTHOPKEY[n].REVOKE[o]	0x2D0		Revocation status for RoT authenticated operation public key generation [n].
OTP[n]	0x500		One time programmable memory

4.2.9.1.1 APPROTECT[n] (n=0..0)

Access Port Protection Registers

4.2.9.1.1.1 APPROTECT[n].PROTECT0 (n=0..0)

Address offset: 0x000 + (n × 0x20)

Access port protection

Any other value than Unprotected will lock TAMPC PROTECT.DOMAIN signal protectors.