life.augmented

STM32MP13

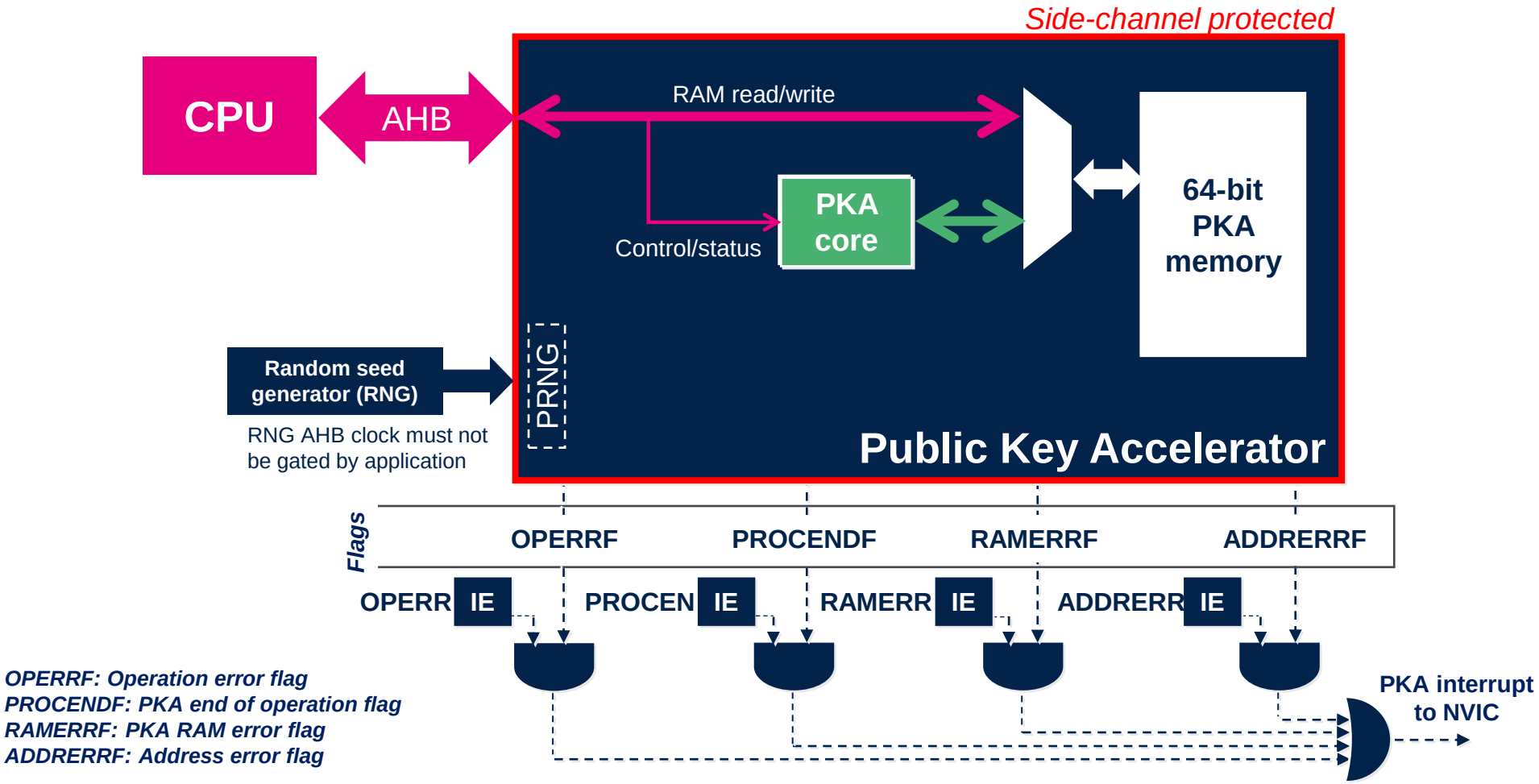
Public key accelerator

Revision 1.0

PKA feature list

- Acceleration of asymmetric cryptography, up to 4160 bits for RSA/DH and 640 bits for elliptic curves
  - Used in NIST FIPS186-4, RSA PKCS#1, ANSI X9.62, IETF RFC5639 (Brainpool), Chinese SM2 and SEC2 curves.
- Side channel protection for operations manipulating secrets
  - RSA / DSA private modular exponentiation
  - ECC scalar multiplication, signature generation
- Operations not manipulating secrets are also supported
  - RSA / DSA public modular exponentiation and its faster CRT (Chinese Remainder Theorem) version
  - ECDSA signature verification
  - ECC point on curve check, complete addition, double base ladder & projective to affine
  - Arithmetic and modular operations like addition, subtraction, multiplication, comparison, reduction…

PKA peripheral block diagram



PKA processing time (STM32MP13@650MHz)

- Modular exponentiation operation (in milliseconds) (DPA resistant)

	Exponent length (in bits)	Modulus length (in bits)		
		1024	2048	3072
public	**3**	0.3	0.9	1.2
private	**1024**	11, 6.5 or 2.3 (CRT)	-	-
	2048	-	66, 43 or 13 (CRT)	-
	3072	-	-	200, 136 or 40 (CRT)

- Other operations in ms (DPA resistant)

Note: CRT is Chinese Remainder Theorem optimization

	Modulus length (in bits)			
	256	384	512	521
ECC scalar multiplication	4.6	11	22.5	30
ECDSA signature	4	9.5	18	22.5
ECDSA verification	4.6	11	22	27

life.augmented

Thank you

life.augmented