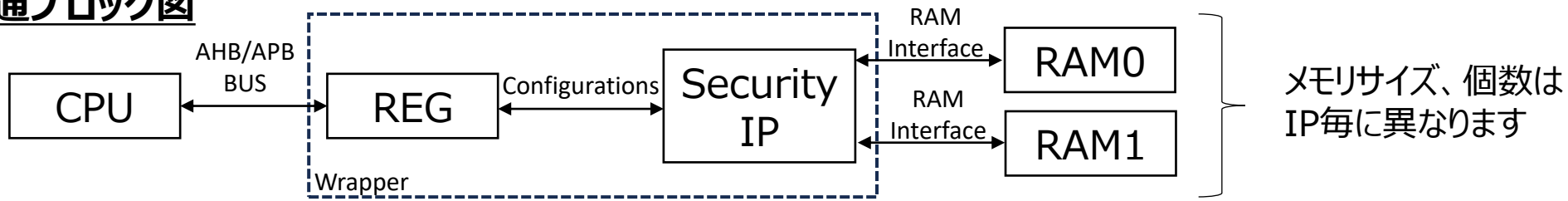
Security IP

- AES：ハードウェア実装、FIPS PUB 197 準拠

			AES-Speed	AES-Standard	AES-Secure
共通鍵暗号	128/192/256bit	ECB	●	●	●
		CBC	●	●	●
		CTR	●		
外部システム要件	BUS I/F: AHB/APB		●	●	●
	同期クロック入力		●	●	●
	非同期リセット、同期リセット解除		●	●	●
	メモリサイズ		なし	128b*32w*1	128b*32w*2
	乱数要件(乱数はクロックサイクル毎に異なる)				●

共通ブロック図

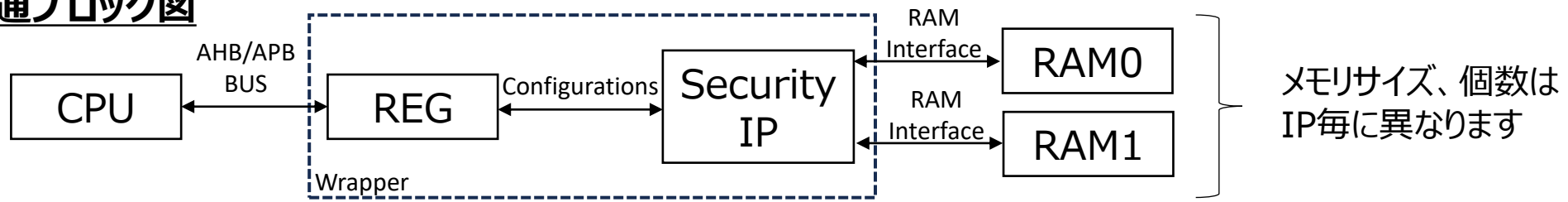


Security IP

- DES：ハードウェア実装、FIPS-46-3 準拠

			DES-Speed	DES-Standard	DES-Secure
共通鍵暗号	64bit	ECB	●	●	●
		CBC	●	●	●
外部システム要件	BUS I/F: AHB/APB		●	●	●
	同期クロック入力		●	●	●
	非同期リセット、同期リセット解除		●	●	●
	メモリサイズ		なし	128b*32w*2	128b*32w*2
補足				標準	保護機能強化

共通ブロック図

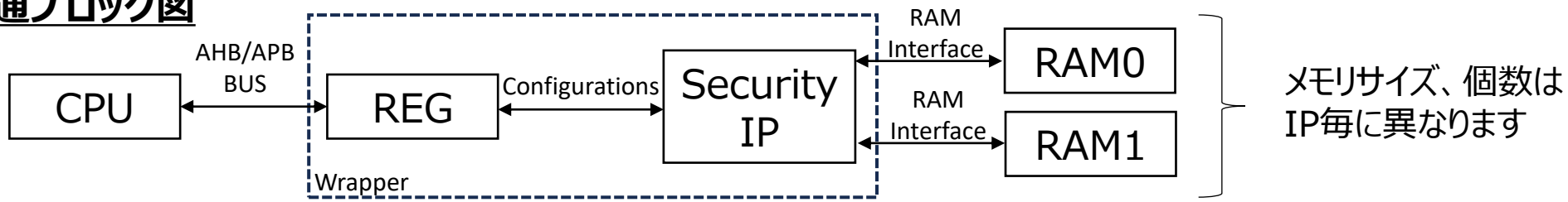


Security IP

- SHA：ハードウェア実装、FIPS PUB 180-3 準拠

		SHA-Speed	SHA512-Standard	SHA256-Standard	SHA256-Secure
ハッシュ関数	SHA1	●		●	●
	SHA224	●		●	●
	SHA256	●		●	●
	SHA384	●	●		
	SHA512	●	●		
	SM3	●		●	
	MD5	●		●	
外部システム要件	BUS I/F: AHB/APB	●	●	●	●
	同期クロック入力	●	●	●	●
	非同期リセット、同期リセット解除	●	●	●	●
	メモリサイズ		128b*32w*2	128b*32w*2	128b*32w*2
補足				標準	保護機能強化

共通ブロック図



Security IP

- SM4：ハードウェア実装、GM/T 0002-2012 “SM4 Block Cipher Algorithm” 準拠

			SM4-Speed	SM4-Nano	SM4-Standard (Single RAM)	SM4-Standard (Dual RAM)	SM4-Secure
共通鍵暗号	128bit	ECB	●	●	●	●	●
		CBC	●	●	●	●	●
外部システム要件	BUS I/F: AHB/APB		●	●	●	●	●
	同期クロック入力		●	●	●	●	●
	非同期リセット、同期リセット解除		●	●	●	●	●
	メモリサイズ		なし	64b*32w*1	128b*32w*1	128b*32w*2	128b*32w*2
補足				小面積	標準	標準	保護機能強化

共通ブロック図