発行日：2020年4月3日

RENESAS TECHNICAL UPDATE

〒135-0061 東京都江東区豊洲 3-2-24 豊洲フォレシア
ルネサス エレクトロニクス株式会社
問合せ窓口 https://www.renesas.com/jp/ja/support/contact/

製品分類	MPU & MCU	発行番号	TN-RX*-A0223A/J	Rev.	第1版
題名	RXファミリ Trusted Secure IP (TSIP) に関する仕様の追加について		情報分類	技術情報	
適用製品	RX72M グループ RX65N グループ、RX651 グループ	対象ロット等 全ロット	関連資料	RX72M グループ ユーザーズマニュアル ハードウェア編 Rev.1.00 (R01UH0804JJ0100) RX65N グループ、RX651 グループ ユーザーズマニュアル ハードウェア編 Rev.2.30 (R01UH0590JJ0230)	

上記適用製品に搭載されている Trusted Secure IP (TSIP) に関し、楕円曲線暗号 (ECC) の仕様を公開いたします。
ECC 公開後の TSIP の仕様は以下のとおりです。

表 1. Trusted Secure IP の仕様 (1 / 2)

項目	内容
アクセス制御	アクセスマネジメント回路 ● プログラムの改ざんや、CPU の暴走等により Trusted Secure IP への異常なアクセスが発生した場合、それ以降のアクセスを受け付けず、Trusted Secure IP からのデータ出力を停止
暗号エンジン	AES：NIST FIPS PUB 197 準拠 ● 鍵長：128 ビット/192 ビット/256 ビット ● データブロック長：128 ビット ● 暗号利用モード ECB, CBC, CTR：NIST SP 800-38A 準拠 CMAC：NIST SP 800-38B 準拠 CCM：NIST SP 800-38C 準拠 GCM：NIST SP 800-38D 準拠 XTS：NIST SP 800-38E 準拠 GCTR ● 実行サイクル数 (注 1) ECB, CBC, CTR, CMAC, GCTR, XTS： 鍵長 128 ビット：PCLKB 11 サイクル、192 ビット：PCLKB 13 サイクル、256 ビット：PCLKB 15 サイクル CCM： 鍵長 128 ビット：PCLKB 22 サイクル、192 ビット：PCLKB 26 サイクル、256 ビット：PCLKB 30 サイクル AES-GCM ● AES-GCTR と GHASH の組み合わせで AES GCM を実現 RSA ● 鍵長：最大 2048 ビット ● データブロック長：最大 2048 ビット ● 実行サイクル数：PCLKB 約 130 万サイクル(CRT を用いた場合) (注 1) TDES ● 鍵長：56 ビット/2 × 56 ビット/3 × 56 ビット ● データブロック長：64 ビット ● 暗号利用モード：ECB, CBC ● 実行サイクル数 (注 1) 56 ビット：PCLKB 16 サイクル、2 × 56 ビット：PCLKB 32 サイクル、3 × 56 ビット：PCLKB 48 サイクル ARC4 ● 鍵長：2048 ビット ● データブロック長：128 ビット ● 実行サイクル数：PCLKB 16 サイクル (注 1)

表 1.　Trusted Secure IP の仕様 (2 / 2)

項目	内容
暗号エンジン	HASH SHA1、SHA224/SHA256/MD5、GHASH に対応 ● データブロック長：512 ビット ● 実行サイクル数 (注 1) SHA1：PCLKB 80 サイクル SHA224/SHA256/MD5：PCLKB 64 サイクル GHASH：PCLKB 9 サイクル ECC ● 鍵長：最大 256 ビット ● データブロック長：256 ビット 鍵の管理 ● 鍵は Trusted Secure IP の内部でのみ有効 ● Trusted Secure IP の外部には鍵生成情報のみを出力 ● 鍵生成情報を Trusted Secure IP に入力することで、鍵が再生成可能 エンディアン ● ビッグエンディアン、リトルエンディアンに対応
乱数生成	32 ビット真正乱数生成回路 ● 32 ビット真正乱数を用いて Trusted Secure IP ライブラリにより 128 ビット、256 ビットの真正乱数を生成可能 ● 生成した 128 ビット、256 ビットの真正乱数を暗号、復号の鍵として使用可能
鍵の不正コピー防止	● MCU 個体固有の ID (ユニーク ID)をアクセスマネジメント回路から専用バス経由でアクセス可能 ● ユニーク ID を鍵生成情報に組み込むことで、本 MCU グループの別の個体への不正コピーを防止可能
スーパバイザモード	● スーパバイザモード信号をアクセスマネジメント回路に接続しており、Trusted Secure IP の制御をスーパバイザモード時に限定することが可能
割り込み要因	11 種類
消費電力低減機能	モジュールストップ状態への遷移が可能

注 1.　Trusted Secure IP ライブラリ呼び出しのオーバヘッドは含みません。

以上