ICH

SPYRUS Security to the Edge™

2009/11/19

Rosetta Micro Series II

ワンチップＨＳＭ

現在再度注目を浴びているＰＫＩのＨＳＭのワンチップ化に成功ししました。
Rosetta Micro Series II チップ型ＨＳＭは５ｍｍＸ６ｍｍのチップに SuiteB を超える暗号アルゴリズム群を内蔵しています。FIPS140-2 Level 2, Level 3 に対応できる機能を備え、米国政府規定の”Unclassified, Classified, TOP SECRET”情報暗号化の鍵長規定に対応しています。
カスタム製品、大量生産の内蔵セキュリティ・アプリケーションに最適です。

高度なセキュリティ設計

Rosetta MicroはInfineon SLE66CX642Pセキュリティコントローラと SPYCOS (Spyrus Cryptographic Operating System)の組合せで稼動します。このチップはCommon Criteria EAL5+によりドイツ政府にも認定されています。この構成はSpyrus社のスマートカード、USBメモリー・トークンに使用されており実績があります。また、このチップは現在FIPS140-2 Level ３の認証中で、内蔵されたセット上でのFIPS認定の要求に応じるためです。

Rosetta Microはアクティブ、パッシブ両方の攻撃にも耐えるように設計されております。ランダムメモリーレイアウトにより物理的攻撃にも対応します。タイミング分析、シンプル・ディファレンシャル・パワー分析、ディファレンシャル・フォルト分析によるサイド・チャンネル攻撃に対してハードウェアとカウンター・アルゴリズムで応じます。ＰＣ暗号化ソフトウェアに問題を起こすブランチ予測分析による攻撃に対しても非常に強固です。

Rosetta Microの内容を探ったり、支配しようとする攻撃が行われた場合EEPROM内にある証明書や、セキュリティ・パラメータ、鍵、変数などや、RAM上にあるデータも全て消去します。ただし、状態表示インジケータ（ランプ、電圧、グリッチ・センサー）などが反応した場合はRAMを消去しチップをリセットします。この場合はEEPROMにある情報は消去されません。揮発性RAMに一時的に置いた暗号化された秘密鍵やセキュリティ・パラメータは使用後直ちに消去されます。セキュリティのためPINはこのチップ上には保存されません。10回以上の不正PIN入力でPIN予測攻撃とみなし鍵の消去が行われます。

KK ICH　3-5-17-408 Nishigotanda, Shinagawa, Tokyo 141-0031 Japan
Phone　+81-50-3735-0211
https://www.ich-one.com

Rosetta Microは真のハードウェア・ランダム数発生を行い、この数を使用しSPYCOSはHigh-Entropy Deterministic Random Bit Generator (NIST SP 800-90)に植えつけて、ECC P-521 やAES-256鍵長を超える要求に対応します。また、高度なプロービング・タイプ攻撃に対して、ユーザーがログオフし電源が切れている間に備えEEPROMの内容を暗号化します。

Spyrus社は現在、特許申請中の"K out of N split knowledge technique"を提供し、一時復号化された鍵、鍵リカバリー、アプリケーションのマルチ・パーティアクセスを可能にし、認証されたホストやデバイスにデータの数学的アプローチの保管セキュリティを提供し、特定のコンピュータに限りデバイスの使用を許可することが出来ます。
Spyrus社は高度で低コストのセキュリティ・プロセッサーを十年以上にわたり提供してきました。この経験はインタグレータやOEMユーザーに直ぐに提供できるパッケージに反映されています。また、特殊なコマンドを追加したり、チップそのものの正当性を確認するクローニング防止機能を追加できるなどのRosetta Microの特注も受け賜っています。

SuiteBを超えたRosetta Microの暗号機能

RSAや3DES、SHA-1のような既存のアプリケーションに使用される暗号アルゴリズムや、米国NSAの全SuiteBのみならず、より高度な暗号アルゴリズムがRosetta Microではサポートされています。もちろんPKIに基づく証明書に基づくカード・ログオンやメールの署名、暗号化、WEB証明などにも使用されます。サポートされているアルゴリズムのリストをご参照ください。

先進の特長

- 鍵、デジタルＩＤ、データなどのハードウェアによる保護
- 商業的製品では最強の暗号アルゴリズムと鍵の強度
- 内蔵アプリケーションには最適なハイ・パフォーマンスと低電力
- 8012インストラクションとISO7816インターフェースで幅広いアプリケーションサポート
- 32KBのEEPROMでX.509証明書とデータ保管
- ハードウェア・メモリー管理と保護デバイス
- 先進の高度エントロピーランダム数発生で鍵の生成
- 生体認証を含む多要素認証対応
- 機体毎のシリアル番号とモジュール毎の、トークン毎の鍵ペアーによりクローニング防止
- 同種のRosetta Microのあるシステムからのアクセス防止（タンパー防止と、リアクション）
- 設計はFIPS140-2 Level4以上の要求に対応可能
- Microsoft CryotpAPI、Cryptographic API, Next Generation完全互換API提供(Windows Vista, PKCS#11対応)
- カスタム・ライブラリー、ドライバー、OS対応可能
- 特注で産業用、MIL-SPECバージョン出荷可能

KK ICH　3-5-17-408 Nishigotanda, Shinagawa, Tokyo 141-0031 Japan
Phone　+81-50-3735-0211
https://www.ich-one.com

技術仕様

SPYCOS ソフトウェア

セキュリティ・ポリシー適用機能

Cryptographic and Access Control Listがアプリケーション間のファイアウォールを形成

Anti-tearing Memory File Managerがファイル転送中の抜差しにファイルを保護

カーネル上でのEEPROMダイナミック・メモリーアロケーション

アプリケーション間の暗号ファイアウォール

ハードウェア・アクセラレーション：RSA, ECC, 鍵ペアー3DES

生体認証のPrecise™アルゴリズム

OATHアルゴリズムでワンタイム・パスワード生成

ICモジュール

Infineon SLE66CX642P 16-bit processor

64K EEPROM, 206K ROM, 5052 RAM

1100-bit Advanced Cryptographic Engine

112-bit/192-bit DDES & ECC GF(2n) Accelerator

最低10年間のデータ保持

最低 500,000 write/erase サイクル（25º C)

高セキュリティ部品配置、 レイアウト・スクランブル

ROHS 対応

使用条件

動作温度　-15℃ - +55℃

保存条件　-20℃ - +65℃

消費電力　<6 mA @3.3VDC, <10mA@5VDC

MIL/JEDEC	**試験結果（合格）**
高温保存	MIL-STD-883 Method 1008
温度サイクル	MIL-STD-883 Method 101 Condition C
対湿度	JEDEC JESD22-A101-B
	JEDEC JESD22 A113-E

KK ICH　3-5-17-408 Nishigotanda, Shinagawa, Tokyo 141-0031 Japan
Phone　+81-50-3735-0211
https://www.ich-one.com

規格対応

ANSI X9.31 RSA Key Generation

FIPS PUB 46 Data Encryption Standard

FIPS PUB 180-2 Secure Hash Algorithm Standard

FIPS PUB 186-2 Digital Signature Standard

FIPS PUB 197 Advanced Encryption Standard

SP 800-38A Block Modes of Operation

SP 800-56A Key Establishment Guidelines

SP 800-90 Deterministic Random Bit Generators

セキュリティ規格

ICC certified EAL 5+

FIPS 140-2 Level からLevel 4,アプリケーションにより対応

対応暗号アルゴリズム

Elliptic Curve Cryptography using the NIST curves in GF(p) (P-256, P-384, P-521*)

ECDH and ECMQV Key Establishment per SP 800-56A (all seven modes)

ECDSA Digital Signature Algorithm

Concatenation KDF per SP 800-56A

RSA 1024/2048 Digital Signature Algorithm

RSA-1024/2048 key exchange

DSA 1024 Digital Signature Algorithm

RSA-1024/2048 key exchange

DES, two & three-key triple DES with ECB, CBC

AES 128/192/256 with ECB, CBC

SHA-1 and SHA-224/256/384/512* Secure

Hash Algorithms with HMAC support

OATH HMAC-based One Time Password

(HOTP) algorithm

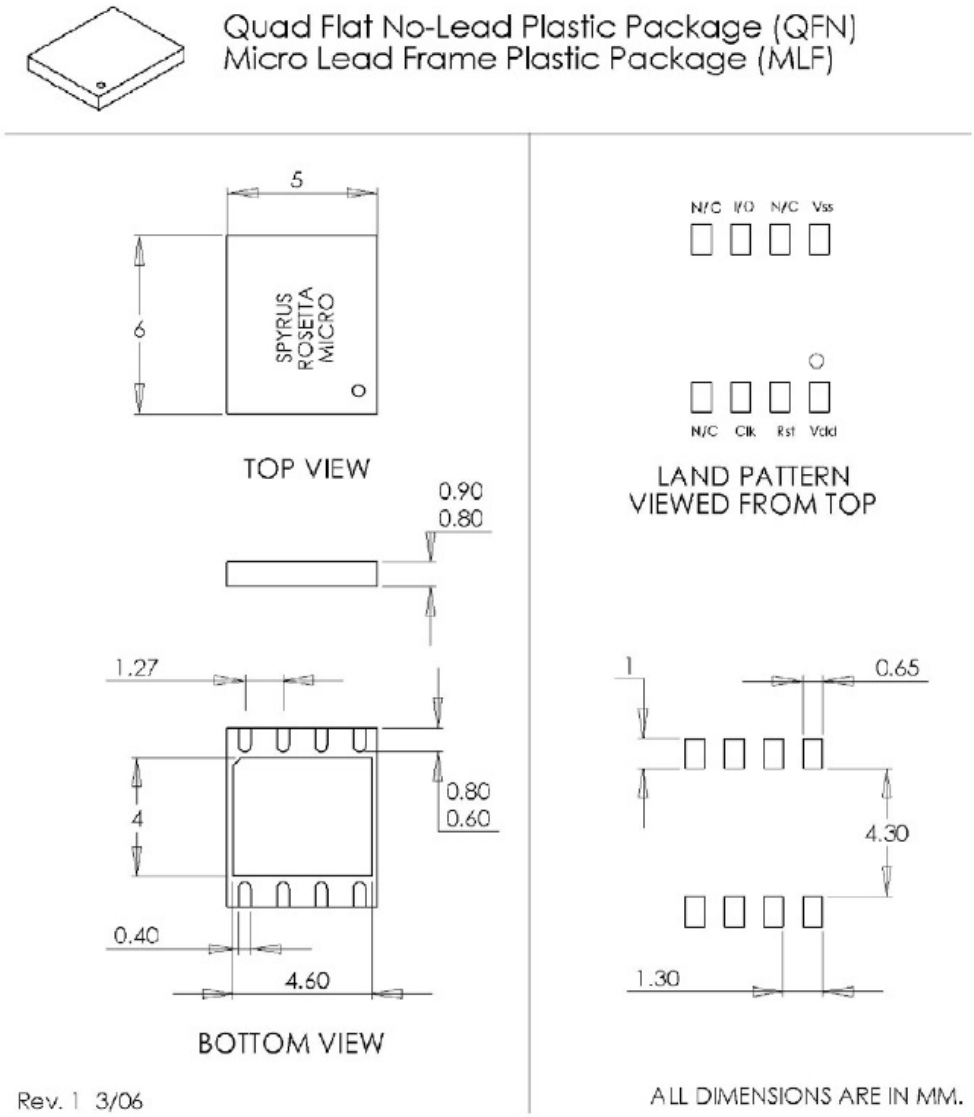
*はSuiteB仕様を超えているアルゴリズム

KK ICH 3-5-17-408 Nishigotanda, Shinagawa, Tokyo 141-0031 Japan
Phone +81-50-3735-0211
https://www.ich-one.com

ICH

SPYRUS Security to the Edge™

機械的仕様及び半田付情報



KK ICH 3-5-17-408 Nishigotanda, Shinagawa, Tokyo 141-0031 Japan
Phone +81-50-3735-0211
https://www.ich-one.com