2021 年 9 月 6 日

ニュースリリース

Crypto の IoT セキュリティ用量子半導体 IP が PSA Level 2 Ready に認定

IoT 向け量子駆動型サイバー・セキュリティ・スペシャリストの英 Crypto Quantique は、独立系のセキュリティ評価会社である Riscure 社から、同社の QDID 量子半導体 IP が PSA Level 2 Ready（PSA L2R）であると認定されました。

PSA 認定は、グローバルな共同運営によるセキュリティプログラムで、設立メンバー企業には、プロセッサ IP ベンダーの Arm 社をはじめ、チップ、組み込みデバイス、モバイルデバイス分野におけるソフトウェアおよびハードウェアのセキュリティ評価ベンダーである Riscure 社などが含まれます。このプログラムでは、セキュリティが製品開発の障壁になるのを防ぐことを念頭に、コネクテッドデバイスのセキュリティの枠組みが定義されています。

PSA Certified のセキュリティ評価には、チップ、ソフトウェア、RoT コンポーネント、デバイスのセキュリティ資格を認証するためのさまざまな要素があります。PSA Certified Level 2 と PSA Certified Level 3 では、シリコンベンダーが提供する PSA-RoT に焦点を当てています。PSA Certified Level 2 Ready は、PSA-RoT のセキュリティ要件のサブセットを提供する企業向けに構築されています。

Crypto Quantique の半導体ハードウェア IP（QDID）は、標準的な CMOS プロセスで使用される専用の物理困難関数（PUF）です。QDID は、チップの酸化膜を介した電子のランダムな量子トンネリングによって生じるフェムト電流を利用して乱数またはシード層を生成することで、チップベンダーが提供するフル PSA-RoT に対応しています。そのシード層を使って、必要に応じて、無相関でクローン化されていないユニークな ID と暗号鍵を生成します。これらの ID と鍵はデバイス自体で生成され、メモリに保存したり、外部から注入したりする必要がないため、他の技術で生成されたものよりも本質的に安全です。第 2 世代の PUF 技術は、複数の鍵を生成するための最小限のシリコン面積しか必要とせず、セキュアメモリーなどの高価なオンチップペリフェラルも必要としない、圧倒的に経済的な技術です。

PSA Certified Level 2 Ready スキームにより、Crypto Quantique は PSA Certified Level 2 セキュリティ要件のサブセットに関する侵入テストを実施し、チップベンダーに自社の QDID 技術が PSA Certified Level 2 要件の一部を満たしていることを対外的に告知することができました。これにより、お客様は PSA Certified の事前認証を受けて、完全な PSA Certified Level 2 認証に使用できます。

Riscure 社のシニアセールス＆ビジネスデベロップメントマネージャーである Bernie Rietkerken 氏は、次のように述べています。「Crypto Quantique 社のセキュリティに対する意識の高さと、将来の IoT デバイスにおいてより高いセキュリティレベルを実現しようとする意欲を称賛します。Crypto Quantique が、自社のソリューションを評価する独立したラボとして Riscure を選択されたことに感謝しています。チップに組み込むことでチップ固有の値を安全に生成・保存することができる QDID 技術は、PSA 認定レベル 2 レディのステータスを獲得するのに十分な堅牢性を備えていると判断しています」

Crypto Quantique の CEO を務める Shahram Mossayebi は、次のように述べています。「この認定により、当社の量子力学に基づく第 2 世代の PUF 技術が、マイクロコントローラーや特定用途向け半導体、そしてそれらが搭載される IoT デバイスに最高度のセキュリティをもたらすことが証明されました。多くの半導体メーカーがセキュリティの向上に取り組む中で、QDID はパフォーマンスとコストの点で間違いなく先頭に立っていると言えるでしょう」

###

Crypto Quantique について

英国ロンドンに本社を置く Crypto Quantique は、暗号システムのエキスパートである Shahram Mossayebi 博士（CEO）と、複雑な並列コンピューターシステムに関する豊富な経験を持つ半導体設計者の Patrick Camilleri 博士（CTO）が共同で設立した企業です。同社は、世界最高のセキュアなエンドツーエンドの IoT セキュリティ・プラットフォームを開発していますが、その核心にあるのが、世界初の量子力学に基づく半導体ハードウェア IP の QDID です。QDID により、標準の CMOS プロセスによって製造されたデバイス向けに、偽造不可能な一意の暗号鍵が複数生成されます。この暗号鍵は保存する必要がなく、独立して複数の用途にオンデマンドで使用できます。Crypto Quantique の汎用型 IoT セキュリティ・プラットフォーム、QuarkLink の暗号化 API と組み合わせれば、シリコン、デバイス、ソフトウェア、ソリューションプロバイダー間を安全につなぐことが可能です。企業詳細はこちらをご参照ください（www.cryptoquantique.com）。
Crypto Quantique の LinkedIn、 Twitter

メディアのお問い合わせ先
Bob Jones、Crypto Quantique
bjones@cryptoquantique.com
ミアキス・アソシエイツ　本田
honda@miacis.jp