Empowering Tomorrow's Automotive Software
www.etas.com

ESCRYPT 耐量子計算機 暗号コンサルティング サービス

量子コンピュータ時代への準備はできていますか？

公開鍵暗号方式は広範囲に使用されていて現在はセキュアなアルゴリズムであっても、量子コンピュータによって破られる可能性があります。量子コンピューティングのブレークスルーまでまだ何年もかかるかもしれませんが、企業は量子セキュアシステムへの移行を早めに準備しておく必要があります。しかし、適切な耐量子計算機アルゴリズム（PQC）の選定と量子セキュアシステムへの移行は簡単ではありません。

セキュアな車両アーキテクチャの開発で実証された専門知識に加え、ETAS は FLOQI（Full lifecycle Post-quantum PKI）プロジェクトのパートナーとして PQC 分野で幅広い経験を積んできました。FLOQI は、自動車用途の耐量子計算機 PKI の開発に特化したドイツ政府主導のプロジェクトです。

課題

近年、量子コンピューティングは大きく進歩しており、今から 10 年～15 年先には今日の公開鍵暗号方式を解読できる最初のコンピュータが登場すると言われています。ライフサイクルの長い製品を保護するために公開鍵暗号を使用している企業は、安全な代替手段を今すぐ探し始める必要があります。

自動車セキュリティへの影響

現在、今後の自動車のセキュリティ対策（ECU の完全保護、SecOC、V2X、アクセス制御など）のほとんどは、量子コンピューティングに対して脆弱な従来の公開鍵暗号方式に依存しています。

特に 自動車メーカーは、攻撃によるサービスの中断を回避し、自動車セキュリティに適用される基準や規制（BSI、UN-R 155 など）に準拠しようとする場合、耐量子暗号ソリューションについて今すぐ検討する必要があります。

推奨する対策

- スケーラブルな量子コンピュータが登場する前に、早期にポスト量子世界に備えましょう。
- 暗号の多様性とマイグレーション（ハイブリッド PQC ソリューションなど）を開発し、すべてのユースケースに適したアルゴリズムを特定しましょう。
- 既存の PQC の専門知識と実装方法をトレーニング、コンサルティング、テスト、ESCRYPT CycurLIB などの製品を通じて利用しましょう。

量子コンピュータ時代のセキュアな未来へ – サービスの概要

経営のガイダンス

- ETAS は量子コンピュータの開発によって発生する問題に対する認識を高めることを目的として、カスタマーワークショップを開催しています。
- ETAS は活動のポイントと優先順位に関する具体的な提言を行い、お客様がタイムラインを確立するお手伝いをします。
- 耐量子計算機アルゴリズムに向けた標準化活動に関する最先端の分析を行います。

特定用途向けの量子セキュアな技術的ソリューション

- ETAS の耐量子計算機暗号エキスパートは、耐量子計算機ソリューションへの移行に必要な変更を特定するために、公開鍵暗号方式を使用する特定のシステム（たとえば、機能または機能単位ブロック）を、固有の要件を考慮して分析します。
- ETAS は、公開鍵基盤（PKI）または鍵管理などに関する移行や移行ソリューションを設計します。

耐量子計算機ソリューションを E/E アーキテクチャに統合

ETAS の PQC エキスパートは、以下の点に関して耐量子計算機アルゴリズムを分析します。

- 鍵や署名サイズ
- 署名のパフォーマンスとアルゴリズムの検証
- メモリ消費
- アルゴリズムのセキュリティに対する信頼性
- ユースケースの要件

ETAS はさまざまなターゲット / ユースケースに適したアルゴリズムを特定するために、配備されている ECU のリソースを使用可能なベンチマークと比較します。また、耐量子計算機セキュリティに必要な変更に関して、隣接する IT システム（PKI、バックエンドなど）の分析を提供します。

ESCRYPT PQC コンサルティングのアドバンテージ

- **コンサルタントとしての実績：**PQC 、自動車セキュリティのエキスパートとしての長年の経験をご活用いただけます。
- **最新の研究動向を熟知：**FLOQI の一員として、ETAS はプロジェクトパートナーとともに、自動車業界のニーズと要件を考慮したセキュアな PKI を定義してきました。
- **最先端：**既存の PQC 実装を使用して、ESCRYPT CycurLIB などの組み込みやバックエンド システムの耐量子セキュリティをテスト、ベンチマークしています。
- **現場で実証済みのソリューション：**実証済みのソリューションを提供し、セキュアなシステムを構築します。

ETAS の製品とソリューションに関するお問い合わせ：
info@etas.com

製品の詳細情報：
www.etas.com/pqc-sonsulting

ETAS/COM-JP/03-2023