報道発表資料

2021 年 4 月 6 日
凸版印刷株式会社
ISARA Corporation

凸版印刷と ISARA、
IC カードへの耐量子−公開鍵暗号実装に向けて連携

量子セキュアクラウド技術への適用により、安全なアクセス認証・管理を実現

凸版印刷株式会社（本社：東京都文京区、代表取締役社長：麿　秀晴、以下　凸版印刷）と ISARA Corporation（本社：オンタリオ州・カナダ、CEO：Scott Totzke、以下　ISARA）は、IC カードへの耐量子−公開鍵暗号の実装に向けて連携します。

本開発は、耐量子−公開鍵暗号を IC カードへ実装し、IC カードを介したアクセス認証・管理の技術検証を目指すものです。技術検証は、国立研究開発法人情報通信研究機構（NICT）とも連携し、量子セキュアクラウド技術（※1）を搭載したテストベッド H-LINCOS（※2）等で行う予定です。これらを通じて、量子セキュアクラウド技術の利用推進に向けた導入支援、秘匿性の高い電子情報の安全なバックアップやデータ流通のサービス及びソリューションの提供を目指します。

耐量子−公開鍵暗号を実装した IC カード（イメージ図）

■ 本研究の背景

デジタル社会が加速する近年、世界中で様々な個人認証用途で利用される IC カードの重要性が増しています。これらの認証は、IC カードに実装した RSA などに代表される公開鍵暗号を使用しています。しかし、2030 年に実用化が期待されている量子コンピューティング技術により、現在の公開鍵暗号は破られる恐れがあり、セキュリティの強化が課題となっています。そのため、今後は量子コンピューティング技術を用いても破られない公開鍵暗号が求められます。

凸版印刷と ISARA はこれらの課題に対し、これまで培ってきた IC カードのセキュリティ技術や認証技術を用いて、耐量子−公開鍵暗号を実装した IC カードの開発を進めていきます。耐量子−公開鍵暗号の IC カードへの実装と運用は世界でも先進的な試みであり、IC カードを利用するあらゆる環境に大きな影響を与えます。これにより、将来に向けセキュリティを担保し、安全・安心なアクセス認証・管理を実現できる社会となります。

さらに、耐量子−公開鍵暗号を実装した IC カードによるアクセス認証・管理は、世界各国において将来の経済・社会に大きな変革をもたらす革新技術です。そのため、早期に実現し普及させることで、世界の安全・安心な情報流通基盤の構築および維持に貢献します。

従来の IC カードと耐量子−公開鍵暗号を実装した IC カードの違い

■ 具体的な共同研究内容

(1)耐量子−公開鍵暗号のプログラムの開発

耐量子−公開鍵暗号における電子署名の生成と認証のアルゴリズムを実現する、IC カード用のプログラムを開発し、IC カードへの実装と機能検証を行います。

(2)耐量子−公開鍵暗号を実装した IC カードを介したアクセス認証・管理の技術検証

耐量子−公開鍵暗号を実装した IC カードを介したアクセス認証・管理の技術検証を行います。また、量子セキュアクラウド技術への適応性の検証も行います。

■ 2 社の役割

・凸版印刷

IC カードの開発や製造事業を通し、暗号技術、認証技術及び不正アクセス防止技術など、IC カードのセキュリティ技術を培ってきました。このような知見を活かし、凸版印刷は IC カードへの耐量子−公開鍵暗号の実装・適用及び量子セキュアクラウド技術の利用推進に向けた導入支援、秘匿性の高い情報の安全なバックアップやデータ流通サービス、ソリューションの提供など、量子コンピューティング時代における安全・安心な社会の実現に向けて取り組んでいきます。

具体的には、ISARA との共同開発によって耐量子-公開鍵暗号を IC カードに実装し、IC カードを介したアクセス認証・管理を量子セキュアクラウド技術に適用します。

・ISARA

ISARA は、長年にわたるサイバーセキュリティ技術の蓄積をもとに、現在のコンピューティングエコシステムを量子の時代まで守り続ける、アジャイルな暗号技術と耐量子セキュリティソリューション事業の世界的リーダーです。これまでの知見を活かし、ISARA は IC カードに実装する耐量子-公開鍵暗号を用いた認証技術の開発を目指します。

凸版印刷と ISARA は、これまでに培った各々の技術・知見・経験を融合させ、IC カードへの耐量子-公開鍵暗号の実装とアクセス認証・管理技術の確立に向けて連携します。

■ 今後の目標

凸版印刷と ISARA の 2 社は、耐量子-公開鍵暗号を実装した IC カードの開発を推進し、2022 年に耐量子-公開鍵暗号の IC カードへの適用及び認証システムの技術検証を開始します。2025 年に限定的な実用化を、2030 年にサービス化を目指します。

■ 第 1 回 量子コンピューティング EXPO【春】

凸版印刷は 2021 年 4 月 7 日(水)から 9 日(金)に開催される「第 1 回量子コンピューティング EXPO【春】」(会場:東京ビッグサイト)に出展します。凸版印刷ブース(6-12)では本共同研究に関する内容をはじめ、量子コンピューティングに対する凸版印刷の取り組みを紹介します。

※1 量子セキュアクラウド技術

量子暗号技術と秘密分散技術を融合し、データの安全な流通/保管/利活用を可能とするクラウド技術

参考:トッパンプレスリリース 2020 年 10 月 19 日 https://www.toppan.co.jp/news/2020/10/newsrelease_201019.html

※2 H-LINCOS

保健医療用の長期セキュアデータ保管・交換システム(Healthcare long-term integrity and confidentiality protection system)。秘密分散と秘匿通信の技術により、電子カルテデータのセキュアかつ可用性の高いバックアップ、医療機関間での相互利用などを行う保健医療用の長期セキュアデータ保管・交換システム。

参考:NICT プレスリリース 2019 年 12 月 12 日 https://www.nict.go.jp/press/2019/12/12-1.html

＊ 本ニュースリリースに記載された内容は発表日現在のものです。その後予告なしに変更されることがあります。

以 上