URL https://journal.ntt.co.jp/article/25306
DOI https://doi.org/10.60249/24031301

NTT社会情報研究所
特別研究員
高橋順子 Junko Takahashi

光情報処理基盤の安全を支える「光論理ゲートで構成する光暗号回路技術」

NTTが推進する6G（第6世代移動通信システム）/IOWN（Innovative Optical and Wireless Network）時代では，光技術を駆使した次世代通信ネットワークが実現されます．しかしそこで問題になっているのが暗号化の技術です．たとえ光回路が実現されたとしても，暗号演算が現在のままでは遅延や無駄な電力消費が発生してしまい，光技術のメリットを十分に活かすことができません．NTTではこの課題を解決するため，従来電子で行われていた暗号演算の複雑な処理を光に置き換えようとする研究に取り組んでいます．今回は，IOWN時代に対応した「光演算手法」を考案して「光暗号回路」を実装した高橋順子特別研究員にお話を伺い，光暗号技術研究の現在と未来の見通しについて語っていただきました．

◆PROFILE：2004年早稲田大学理工学部物理学科卒業．2006年同大学大学院理工学研究科物理学及応用物理学専攻修士課程修了．同年，日本電信電話株式会社入社．2012年電気通信大学情報理工学研究科博士課程修了．博士（工学）．専門はハードウェアセキュリティ．これまでサイドチャネル攻撃対策技術，自動車セキュリティ技術，組み込みセキュリティ技術の研究に従事．現在はNTT社会情報研究所にて光暗号回路の研究に従事．産業技術総合研究所サイバーフィジカルセキュリティ研究センター客員研究員．電子情報通信学会会員．情報処理学会会員．2023年より特別研究員．

革新的な暗号技術で，APNの安全性を実現

■はじめに，「光論理ゲートで構成する光暗号回路技術」とはどのような技術でしょうか．

私が研究している「光論理ゲートで構成する光暗号回路技術」とは，従来は電子で行われていた暗号演算を光で実現する技術です．この研究を開始したきっかけは，2019～2020年ごろに当時NTTがIOWN（Innovative Optical and Wireless Network）構想を大々的に提唱したことにあります．IOWNの鍵となっている光技術を，私自身がそれまで携わっていた暗号やセキュリティ技術の研究に活用することで，暗号技術をはじめとした革新的なセキュリティ技術を創出できないかと考えたのが本研究テーマの始まりです．

従来では暗号演算のような複雑な処理は電子で行うことが常識でした．一方，IOWNでは，サーバなどのコンピューティング環境やあらゆる電子機器を光技術によるデバイスに置き換えて光ネットワークで結ぶことで，低遅延・低消費電力などの実現をめざしています．演算処理を光技術で実現する中で，もし暗号演算だけが電子回路で実装されていれば，光電変換のために大きなオーバヘッド（負荷）がかかってしまうため，コンピューティング環境全体での演算性能が下がってしまいます．そこで新しく研究を開始したのが「光論理ゲートで構成する光暗号回路技術」です．暗号演算も，IOWN構想におけるオールフォトニクス・ネットワーク（APN: All-Photonics Network）の中で，光を使って実装することによって，さらなる低遅延・低消費電力の演算を実現し，環境負荷を低減させることができると考え，光回路を用いた暗号回路の作製・研究を開始しました（**図1**）．

■実際にご研究を進める中で，どのような点に苦労されましたか．

研究を開始した当初は，単純に既存の光演算素子を組み合わせて実装すればよいと考えており，電子回路の回路設計・作製と同等の期間で容易に実現できると想定していました．しかし実際に研究を進める中で，理論とは異なるさまざまな物性的課題があることが判明したのです．まず暗号演算を行うために必要な光演算素子は，世界中でもまだ発展段階で，現在利用可能な光演算素子にも利用方法の制限がありました．

本来暗号を光回路で実現するためには，暗号処理を複数の論理演算で構成する必要があります．しかし現在利用可能な光演算素子には，複数の論理演算を行うことができないなどの制限があったのです．また遅延や消費電力といった性能面でもまだ発展段階で，APNが掲げる数値目標には到底届かないという現状があり

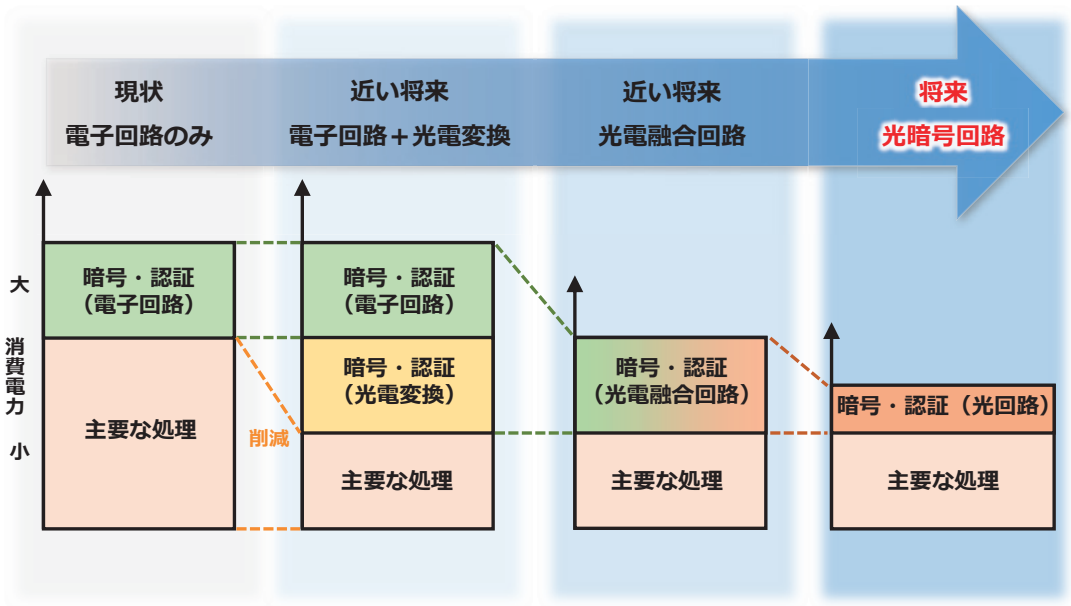

図1　光を用いた暗号回路の研究概要

ます．そのため本研究では，演算に制限がある光演算素子を用いて既存の複雑な暗号関数をどのように構成するか，というところが難しい点でした．加えて暗号演算を行うために必要なメモリやレジスタといった周辺回路も，まだ光技術で実現されていないため電子回路で実現する必要がありました．そのため低遅延・低消費電力実現に向けて，光回路と周辺回路の組合せをどのように行えば最大のパフォーマンスを発揮できるのかというところに非常に苦労しました．

また光デバイス作製上の課題として，設計図・回路チップ・周辺回路の作製といった工程をすべて行うのに1年単位といった非常に長い時間が必要になってしまう点も，研究を開始するまで予想していなかった大きな障壁でした．このため，短期間で製造が可能な素子を見極めて，その中で良い性能を導き出す必要があります．また回路チップは一度作製したら修正を行って後戻りすることができないため，どのように回路を構成してどういった方法で製造するかを慎重に見極めなければいけません．さらに性能の良い光演算素子を使うと全体的な回路規模が大きくなってしまう傾向があるため，これをどのように抑えるかが大きな課題でした．

■現在までのご研究の成果を教えてください．

現在までの研究では，one-hotエンコーディングという手法を用いて，暗号演算の主要な関数である非線形関数を実現する演算手法を考案しました．具体的には4ビット入出力のテーブル変換を行う関数を対象に，シリコンフォトニクス技術を基にした光暗号回路を作製しています．このone-hotエンコーディング手法では，基本的に光配線を基にして演算を行っています．光配線は電子回路とは異なり配線抵抗がないため，低遅延の演算が可能です．また通常の暗号演算ではビット（「0」または「1」）の表現を用いて演算を行いますが，one-hotエンコーディング手法を利用するためにはビット表現を16進数の表現（16通りの表現）に変換する必要があります．この変換にマッハツェンダ光変調器という，光演算素子の中でも比較的実装が容易なものを用いて，さらにその光変調器と光配線を組み合わせることで，暗号の非線形関数の光回路チップを世界で初めて実装しました．

加えて光回路チップの演算動作を検証するために，光回路チップと電気部分を組み合わせた光デバイスを作製し，非線形関数が本当に正しく演算できているのかを確認しています．この光デバイスは，光変調器を制御する電気信号（非線形関数の入力信号）が入力された後，数10ピコセカンドという非常に低遅延で演算することが可能という特長を持ち，APNの目標に大きく貢献していると考えています．

研究と関係がないようにみえる場所にこそ，「光」が射している

■これからのご研究の展望を教えてください．

これまでに研究開発した回路では入力が電気信号で出力が光信号のため，光電融合回路となっています．しかし現在ではより低遅延・低消費電力の演算をめざし，論理演算が可能なYゲートやΨゲートという光演算素子を用いて，入出力が光信号の非線形関数を実現する新たな光回路チップを作製中です．この光回路も正しく演算ができることを実験で確認しており，APNの未来に向けて着実に歩を進めていることを実感できています．

今後の展望としては，2030年代にハードウェアリソース分散を行う「光ディスアグリゲーテッドコンピューティング基盤」が確立される際に，光暗号演算回路を実装して，新たな通信基盤を誰もが安全に利用できるコンピューティング環境の実現をめざしています（**図2**）．目標数値としては，従来の電気的な暗号演算回路と比較して「遅延は1000分の1」「消費電力は100分の1」で動作可能な回路作製を掲げて日々研究に取り組んでいます．さらに将来的には，地上のコンピューティング環境だけでなく宇宙でのコンピューティング環境（宇宙統合コンピューティング・ネットワーク）で利用可能な光暗号回路を作製し，新時代の通信基盤に貢献する大きな技術に発展させていきたいと考えています．

私が取り組むこの研究は前例がなく，研究を開始した当初の周囲からの反応は「そんな魔法のようなことができるのか」と懐疑的な反応ばかりでした．確かに研究を開始した2019年ごろには，やはりネットワーク部分だけが光通信と思っている方が大半で，一部演算は光で実現されていたものの発展途上の段階でした．そのような状況でもともとデジタル回路に設計されていた暗号回路を光に置き換えることに疑問を持つのは当然です．しかし初めて光を用いて暗号演算を実証して発表したとき，多くの方の好意的な反応をいただき，「今まで不可能だと思われた常識を少しでも変えることができた」と嬉しかったことを覚えています．現在は，暗号回路をすべて光で演算することはかなっていませんが，これからも徐々に光回路の可能性を示していくことで，より多くの方に納得いただける研究に取り組んでいきたいと思っています．

■NTT研究所にはどのような印象をお持ちでしょうか．

私が所属するNTT社会情報研究所は，基礎的な暗号技術だけではなく，ネットワーク・IoTシステムに対するサイバー攻撃対策技術や，秘密計算技術・AIセキュリティといったデータ保護技術などのセキュリティに関する研究，さらにはWell-beingといった人々の幸福をめざした研究や法制度・倫理に関する研究など，

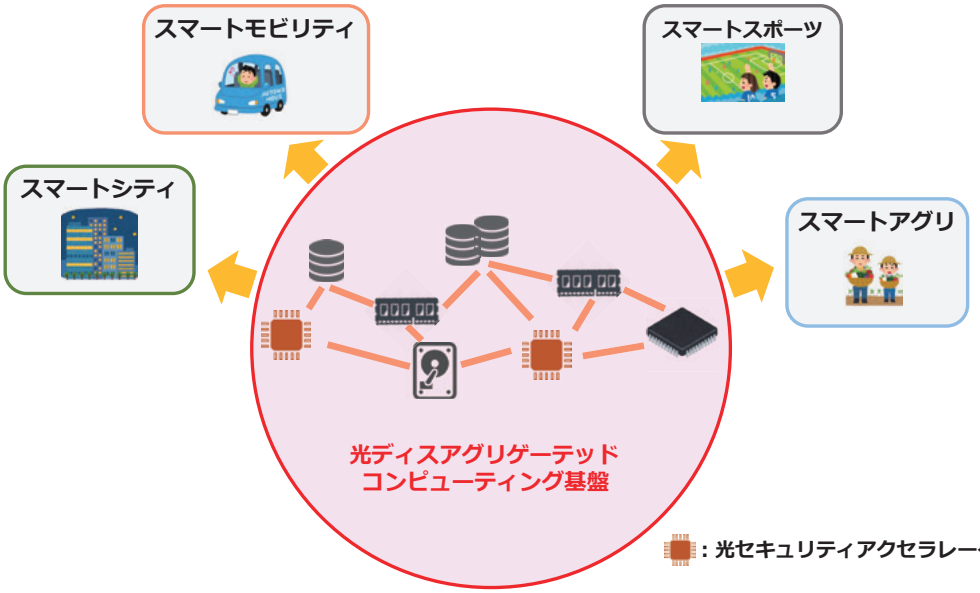

図2　描く未来：安心安全・低遅延・低消費電力のコンピューティング基盤に貢献

社会システムに関する幅広い研究テーマを扱っています．私自身は本研究を開始する前に暗号技術に関する研究とは離れて６年間ほどサイバー攻撃対策技術の研究に従事していました．このようにNTTでは社会システムに関するさまざまな研究テーマに携わることができ，私のように暗号関連の研究テーマを実施した後にサイバーセキュリティの研究に携わり，再び暗号関連の研究へ戻るなど，研究テーマを行き来することが可能なのびのびとした風土が醸成されており，多分野に興味のある研究者にとっては非常に魅力的な環境だと感じています．

またさまざまな研究テーマを扱っているNTT社会情報研究所では，研究を進める中で自身の専門外の問題に当たった際にも，身近な研究者に簡単に相談できるという強みがあると感じています．私は以前，研究を進める中で法律や倫理に関する問題に当たり，解釈を検討しなければいけない場面に直面したことがあります．当然専門外の内容だったため非常に困ったのですが，そのとき所属研究所に法律や倫理に関する研究テーマを扱う研究者が身近にいたためすぐに相談・解決することができ，円滑に自身の研究を進めることができました．このように自身の研究範囲外の問題が出てきた際にすぐに解決する手段があるのもNTTの強みであり，スピード感を持って研究を進められる環境はとてもありがたいものだと感じています．

■最後に研究者・学生・ビジネスパートナーの方々へ向けてメッセージをお願いします．

一般的に研究業務というと，論文執筆・学会発表・特許執筆やビジネス化に向けた開発が主な仕事であると考えられるかと思います．しかし私は，研究を進めるうえで発生する研究以外の業務の地道なプロセスも，すべて自ら実施することを入社してからずっと大切にしています．例えば数年前に自動車のサイバー攻撃対策技術を実施していたころ，自動車に特有の機能をセキュリティの観点から評価するために，特定の年代に製造された，ある運転に関する機能が付いた自動車の入手が必要でした．新車としてはすでに販売されていない車種であったことから，日本全国の中古業者に自らアクセスしてようやくの思いで見つけた中古業者に，自分たちで出向いて交渉と手続きを行いました．そしてその後はもちろん自動車の日々のメンテナンスも自分たちで実施しました．またそういった研究を行ううえで必要な関連装置も自ら選定して，日本国内で唯一設置された場所へ出向いて見学し，設置業者への交渉や社内での設備工事に関する手続きも含めて設置に必要なことを自分たちですべて行ったこともあります．

確かにこのようなプロセスは，一見すると直接的に研究業務と関係ないようにもみえます．しかし自分で汗をかき，すべてに取り組もうとすることで，その業界の裏や全体像がみえてくることがあるかと思います．特に自身の研究分野などとは異なる業界の研究分野へ飛び込む際には，その業界の裏にある黙示的な「常識」や「作法」を知る必要もあり，それを知っているだけで他分野の方との交流がスムーズに進むこともしばしば起こります．そのため私は研究を行ううえでいつも「最大限できることはすべて取り組む」ことを実施して研究を進めています．

現在取り組んでいる光論理ゲートを用いた光暗号回路の研究は，暗号の理論的検討をはじめ，光回路チップの設計・作製，光回路チップと電気回路による光デバイスの作製，周辺回路の作製，回路チップの原理検証を行うための環境構築，といったたくさんのプロセスが必要で，すべてを自らの手により取り組むこともできないので，本当に多くの方に携わっていただきながら研究を進めています．理論からデバイスまで多くの専門家がそろうNTT研究所は，これからも自分の考え・思いを具現化できる環境が整っていてとても心強いです．そういった環境で，これから１人でも多くの研究者・学生・ビジネスパートナーの方々と一緒に，IOWN時代の安全な情報基盤を構成する基礎となる技術を提供していきたいと思っています．もしこれを読んでご興味のある方がいらっしゃれば，ぜひ共に手を取って新しい未来に向けて一緒に挑戦していきましょう．

（今回はリモートにてインタビューを実施しました）