光論理ゲートで構成する暗号回路技術

近年，ナノフォトニクス技術の進展により小型の光素子の実現が可能になり，光論理ゲートの研究開発がさかんに行われています．私たちは，IOWN（Innovative Optical and Wireless Network）の構成要素であるオールフォトニクス・ネットワークにおける光情報通信および光コンピューティング上でのデータの暗号化・認証などに用いるため，光論理ゲートで構成する暗号回路の研究を行っています．本稿では，標準暗号の1つであるAESの暗号回路を光論理ゲートで構成する方法を紹介します．

高橋 順子[†1]　千田 浩司[†1]
山越 公洋[†1]　北 翔太[†2]
新家 昭彦[†2]

NTT社会情報研究所[†1]
NTT物性科学基礎研究所[†2]

オールフォトニクス・ネットワーク情報処理基盤における光演算

オールフォトニクス・ネットワーク（APN）の情報処理基盤では，通信ネットワーク・通信基盤から端末デバイスに至るまで光技術を導入することにより，低消費電力，高品質・大容量および低遅延の情報処理の実現をめざしています．従来のネットワーク機器でのデータ処理および端末デバイスでの演算は電子回路で行われていますが，APN情報処理基盤ではそれらに光技術を用いることにより，処理や演算の性能を向上させることを想定しています．光技術の1つに，光論理ゲートで構成され，論理演算等が可能な光回路があります．光回路は，例えば，深層学習の分野における学習アルゴリズムの演算に利用されており，低遅延・低消費電力な演算が可能と示されています[(1)]．

光暗号回路技術

APN情報処理基盤では，コンピューティングの性能向上のためにさまざまな専用ハードウェアが光回路で実現されます．そのため，APN情報処理基盤の安全性を担保するために必要な暗号専用ハードウェアも光回路で実装し，暗号演算が全体の性能のボトルネックとならないように遅延や消費電力を抑えた回路にすることが望ましいと考えます．そこで私たちは，光信号により暗号・認証の演算が可能な光暗号回路を研究しています．本章では，標準暗号の1つであるAdvanced Encryption Standard（AES）を光回路で実現する方法を紹介します．

■AESの暗号方式

AESは，128ビットブロック長のブロック暗号であり，鍵長は128，192，256ビットから選択することができます[(2)]．ステートと呼ばれる中間値の128ビットを8ビットずつ区切って4×4行列で表現し，暗号化の基本構造であるラウンド関数を繰り返し演算して暗号文を出力します．ラウンド関数は，非線形演算であるSubBytes，線形演算であるShiftRows，MixColumns，およびステートと鍵との加算であるAddRoundKeyから構成されます．本章では，AESの主要な演算であるSubBytesとMixColumnsに着目し，それらを光回路で実現する方法を紹介します．

■光論理ゲートで実装するSubBytes

SubBytesは，8ビットごとに仕様で定められたS-boxテーブルに基づいた変換を行います．S-boxテーブルは，8ビット入出力の非線形変換です．ある8ビットの入力値に対して，テーブルを参照することにより，8ビットの出力値が得られます．例えば，入力値0xf0に対するS-boxの出力は0x8cとなります（入出力の値は16進数で表しています）．

このようなテーブルに基づいた変換は，光論理ゲートの一種であるマッハ・ツェンダー干渉型光スイッチ（MZIスイッチ）を用いて実装することができます．MZIスイッチは，**図1**(a)に示すように，光カプラと位相シフタから構成され，位相シフタが埋め込まれ

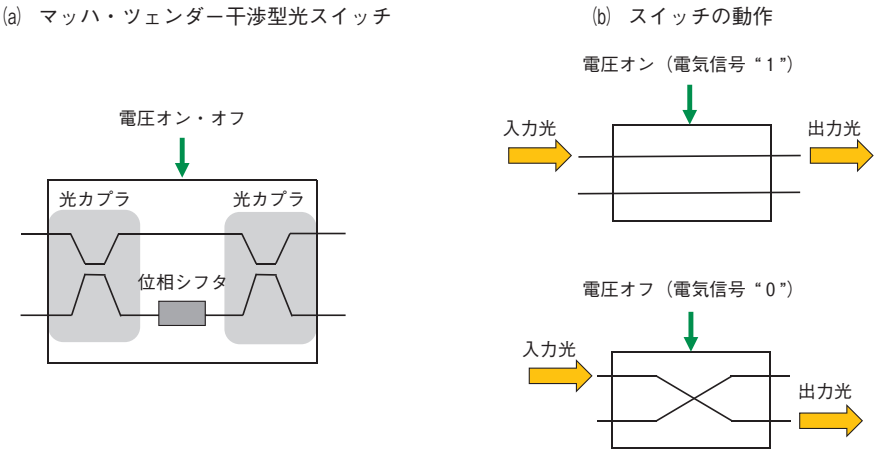


図1　マッハ・ツェンダー干渉型光スイッチ（MZIスイッチ）とその動作

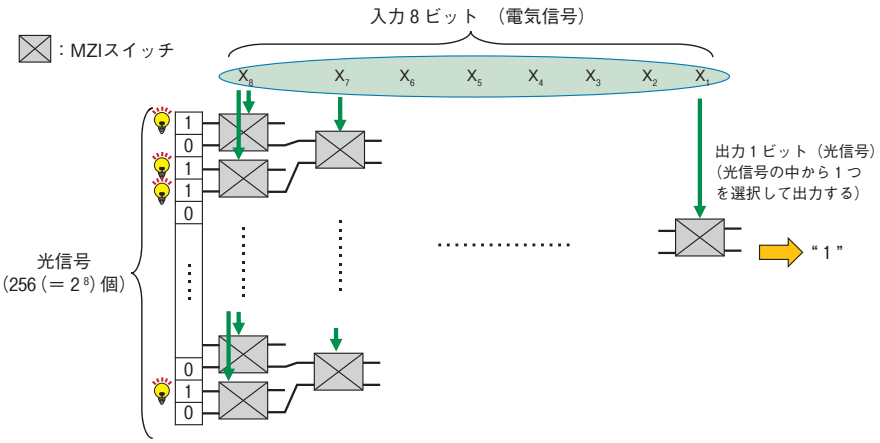


図2　MZIスイッチによるテーブル変換の実装方法

た経路に電圧を加えるか否かによって光導波路の屈折率の変化を起こすことにより，2つの経路の位相差を変更します．このことにより，MZIは光の経路を切り替えるスイッチとして動作します．例えば図1(b)では，上側の経路に光が入力され，位相シフタが埋め込まれた経路に電圧を加える場合は（電気信号のビット“1”に相当）光信号は直進した経路（上側）から出力され，電圧を加えない場合は（電気信号のビット“0”に相当）光信号はクロスした経路（下側）から出力されます．

私たちは，テーブル変換の入力ビット数に応じた数のMZIスイッチを接続して経路を切り替えることにより（**図2**），入力8ビットに対して1ビットの光信号を出力するテーブル変換の実装方法を考案しました．図2において，単一の光源を分岐した256個（＝2^8個）の光を用意し，点灯（光信号のビット“1”に相当）または消灯（光信号のビット“0”に相当）と設定します．このとき，8ビットの入力（x_1, x_2, ・・・, x_8）に応じて経路を選択しながら光がMZIを通過し，最終的に1つの光信号が選択され，出力されます．このように，MZIを用いて8ビットの入力に対して1ビットの光信号を出力するテーブル変換を実現することが可能です．

前述のように複数のMZIスイッチを接続し，256個の光信号を適切に設定することで，S-boxテーブルを構成することができます．MZIの入力（電気信号）にS-boxテーブルの入力を設定し，光信号にS-boxテーブルの出力を設定します．例えば，S-boxテーブルの各256個の値の最下位ビットを光信号に設定しておけば，入力8ビット（x_1, x_2, ・・・, x_8）に対してS-boxテーブルの出力の最下位1ビットを得ることができます．同様に，S-boxテーブルの出力の各々nビット目（n＝1, . . . , 7）を光信号に設定しておけば，8ビットの入力に対するS-boxテーブルの出力のnビット目を得ることができます．

8ビット分のS-boxテーブルの出力を得るためには，上記演算処理を時系列的に8回繰り返す方法や図2の回路を8個並列に実装する方法もありますが，光の場合は波長を8波長に多重化し，波長ごとにS-boxテーブルのnビット目を導出することにより，図2の1つの回路で8ビット分を演算することも可能です．

■光論理ゲートで実装するMixColumns

MixColumnsは，**図3**(a)に示すように，定数行列とステートの乗算で定義されています（X，Yは8ビット）．行列式を計算すると，出力の各8ビットは図3(b)の式①のように表すことができます（図3(b)ではY_1のみを示

(a)

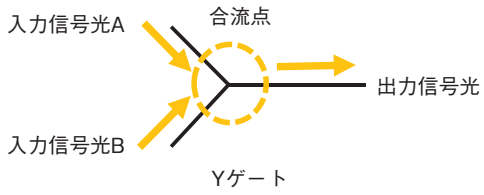
出力　　定数行列　　ステート

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix}$$

(b)　$Y_1 = \{02\} \cdot X_1 \oplus \{03\} \cdot X_2 \oplus X_3 \oplus X_4$　…①

（※）⊕：排他的論理和（XOR）
・：乗算

図 3　AES の MixColumns 構成



ケース＼信号光	入力信号光A	入力信号光B	出力信号光	出力ビット値
①	—	—	—	0
②	—			1
③		—		1
④			—	0

図 4　Y ゲートを用いた XOR 演算

しています）．さらに，乗算を計算すると，式①は 5 ビットの XOR 演算（入力 5 ビット・出力 1 ビットの XOR 演算）5 つと，7 ビットの XOR 演算（入力 7 ビット・出力 1 ビットの XOR 演算）3 つを用いて表すことができます[2]．ここでは，例として，7 ビットの XOR 演算を光論理ゲートで構成する方法を紹介します．同様に，5 ビットの XOR 演算も構成可能です．

XOR 演算が可能な光演算素子として Y ゲートがあります[3]．Y ゲートは，2 つの入力信号光が合流する点で信号を重ね合わせます．光信号が振幅と位相を持つ「波」である性質を利用することで XOR 演算や OR 演算を実現でき，電気による論理ゲートに比べて約 300 倍の高速な演算が可能です[3]．

Y ゲートによる XOR 演算の原理を**図 4** に示します．図 4 のように，位相差が 180° で振幅の大きさが同等の 2 つの信号光（入力信号光 A と入力信号光 B）を入力とします．図 4 の「−」は入力信号光の振幅が 0 の状態，つまり信号光がない状態を示します．この 2 つの信号光を Y ゲートへ入力し，出力光の振幅の大きさを判定します．例えば，図 4 のケース④の場合，2 つの入力信号光の振幅が同等で位相差が 180° であるため，信号が打ち消し合い，振幅が 0 となります．このようにして，振幅が 0 の状態をビット“0”，振幅の大きさが入力信号光と同程度である状態をビット“1”に対応付けると，図 4 の出力信号光のビット値に示すように XOR の論理演算を行うことが可能となります．このように 2 つの入力信号光の位相差を 180° にするといった入力光に対する制約をつけることで，Y ゲートを用いて XOR 演算が可能なことが示されています．

ここで，7 ビットの XOR 演算を行う際には複数の Y ゲートをつなげて演算しますが，XOR 演算の演算結果を次の XOR 演算の入力とする場合は，各 Y ゲートの 2 つの入力信号光の位相差は演算結果に依存し，必ずしも 180° になるとは限りません〔例えば，4 ビットの XOR 演算（a⊕b⊕c⊕d）を行う際に，a，b との XOR 演算結果と c，d との XOR 演算結果とが共にケース②の出力となり，その結果を XOR 演算する場合など〕．よって，各 Y ゲートの 2 入力信号光の位相差を演算結果に応じて変更するといった操作が必要

であり，この操作による遅延や消費電力が増加してしまいます．

そこで私たちは，演算途中の位相の変換を不要とするために，Yゲートの入力の光信号を同位相として演算し，演算の最後にしきい値処理により出力結果を補正する方法を考案しました．**図5**にその概要を示します．本手法は，Yゲートの重ね合わせと光検出器内でのしきい値処理により構成されます．Yゲートの重ね合わせでは，合計7つのYゲートを利用して，光の振幅を足し合わせていきます〔入力数が7であるため，8番目は振幅“0”の光（消灯）とします〕．しきい値処理では，入力光（x_1，x_2，x_3，x_4，x_5，x_6，x_7）の中で光の振幅が0でない信号の数が多いほど，出力光の振幅が大きくなるため，それを検出し，出力のビットを判定します．具体的には，出力光の検出なし（消灯），または入力光の振幅の偶数倍（2倍，4倍，6倍）の振幅を検出した場合は出力結果をビット“0”，入力光の振幅の奇数倍（1倍，3倍，5倍，7倍）を検出した場合は出力結果をビット“1”と判定します．前述の実装方法により，Yゲートの演算度に入力光の位相を変換する必要なく，XOR演算を行うことが可能になります．本演算方法により，Yゲートの出力の処理を7回（Yゲートの出力の数）から1回（しきい値処理時のみ）に削減することが可能です．

図3(b)の式①から計算される7ビットのXOR演算および5ビットのXOR演算を図5に示す演算方法に対応させると，Y_1の1ビット分を計算することができます．Y_1（8ビット分）を計算するには，SubBytesの演算と同様に，時系列的に演算する，複数の演算回路を用いる，または，1つの演算回路で波長の多重化により演算を行うという実装方法が可能です．

今後の展開

私たちは，光論理ゲートを利用するAES暗号回路の構成方法を考案しました．今後，APN情報処理基盤の安全性を確保するために，さまざまな暗号方式による演算や認証などのセキュリティ技術を光回路で実装する光セキュリティアクセラレータが必要になってきます．このアクセラレータは，**図6**に示すAPN情報処理基盤を支えるアーキテクチャである光ディスアグリゲーテッドコンピューティング[4]の構成要素の1つになると考えていま

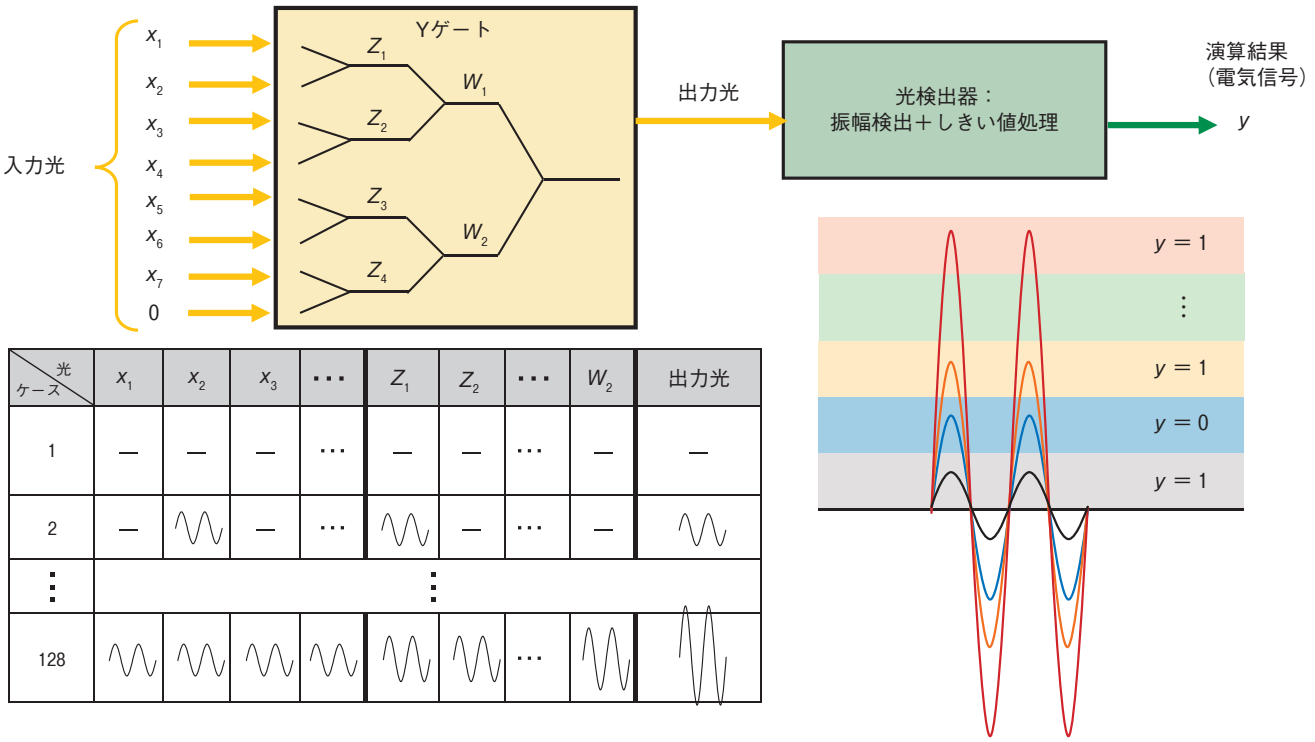
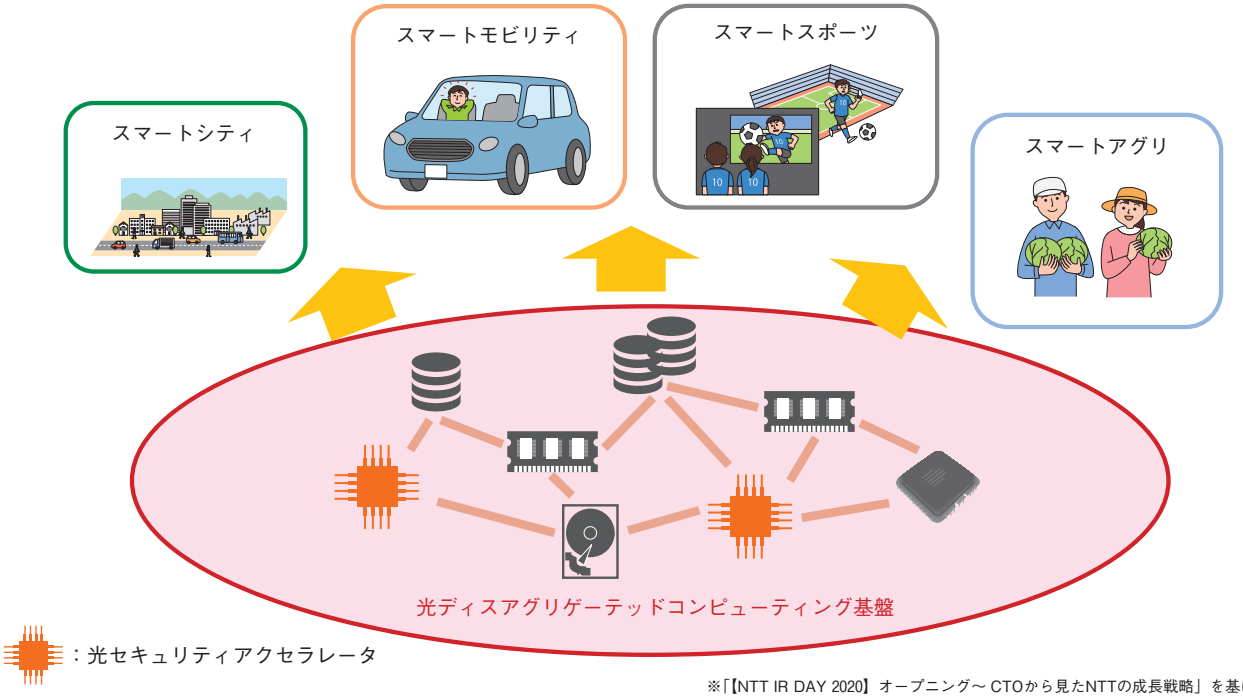


図5　7ビット入力・1ビット出力のXOR演算の実装方法



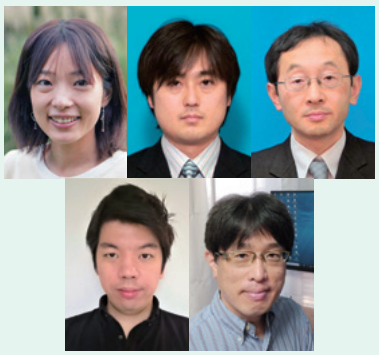
※「【NTT IR DAY 2020】オープニング～CTOから見たNTTの成長戦略」を基に図を作成.

図6　光セキュリティアクセラレータを搭載したAPN情報処理基盤

す．従来，CPU・メモリ等の各種デバイスは各サーバ内に閉じていましたが，光ディスアグリゲーテッドコンピューティングは，それらを高速光ネットワークで接続し，分散させることにより，ラック・データセンタスケールのコンピュータとして扱うという新しいアーキテクチャです．光セキュリティアクセラレータは，安全な光ディスアグリゲーテッドコンピューティング基盤およびそれによる安全なスマートサービスの提供につながると考えています．今後も，低遅延・低消費電力の光セキュリティアクセラレータの実現のために，私たちは光の特性を活かした新たな暗号・認証の実装方式の研究を引き続き行っていきます．このことにより，安全なIOWNの実現に貢献していきます．

■参考文献

(1) J. Peng, Y. Alkabani, S. Sun, V. J. Sorger, and T. El-Ghazawi：“DNNARA：A Deep Neural Network Accelerator using Residue,” ICPP 2020, No. 61, pp. 1-11, Edmonton, Canada, August 2020.
(2) NIST：“Announcing the ADVANCED ENCRYPTION STANDARD (AES),” Federal Information Processing Standards Publication 197, 2001.
(3) S. Kita, K. Nozaki, K. Takata, A. Shinya, and M. Notomi：“Ultrashort low-loss Ψ gates for linear optical logic on Si photonics platform,” Communications Physics, Vol. 3, No. 33, pp.1-8, 2020.
(4) 岡田・木原・岡崎：“IOWNを支えるディスアグリゲーテッドコンピューティング,” NTT技術ジャーナル，Vol. 33, No. 5, pp. 40-44, 2021.



（上段左から）高橋　順子/ 千田　浩司/ 山越　公洋
（下段左から）北　翔太/ 新家　昭彦

光技術で暗号回路を実現するというチャレンジングな研究テーマに取り組んでいます．今後も，安全な新しい光コンピューティング基盤の実現をめざして，研究を進めていきます．

◆問い合わせ先
NTT社会情報研究所
企画担当
E-mail　solab＠hco.ntt.co.jp