集積ナノフォトニクスに基づく耐タンパ光論理回路

塩見 準[1,a)]　木次 修也[2]　董 博語[1]　小野寺 秀俊[1]　新家 昭彦[3,4]　納富 雅也[3,4]

概要：本稿では，集積ナノフォトニクスに基づき，電磁的サイドチャネル攻撃に耐性を示す光論理回路の実現手法を提案する．まず，光の位相変調に基づき論理演算する光回路設計手法を提案する．論理値に応じて光信号の位相のみを変調して論理演算を行うことで，回路中を伝搬する光の強度情報を変調することなく論理回路を設計できる．この結果，光素子や導波路から漏れ出す近接場光を通して論理状態を盗聴することが原理上困難になる．また，光位相変調器を制御する電気端子より漏えいする電磁波を限りなくゼロにする回路実装方式を提案する．提案実装方式を施すことで，従来型 CMOS 回路と同等以上の動作速度を保ちながら，CMOS 論理ゲート 1 個と比較して，電気制御端子 1 個で生じる電流時間変化量 ($\mathrm{d}i/\mathrm{d}t$) を 300 倍以上削減可能であることを示し，攻撃者が使用する磁界プローブに生じる起電力を限りなくゼロにできることを示す．

1. 序論

将来の情報化社会では，ヒトやモノに多種多様な IoT (Internet of Things) デバイスが取り付けられ，各デバイスより生成・通信される無数のデータを高効率に解析し，リアルタイムに実世界にフィードバックする基盤技術が求められる．現在では車車間・路車間通信に基づく自動運転技術や，ファクトリオートメーションなど，人命やプライバシーにかかわる情報を高効率に通信・処理する事例が実用化されつつある．この普及の根底には，個々のデバイスで暗号通信や個体認証などを処理する，暗号処理技術の普及が欠かせない．

暗号 LSI の内部情報を，物理的な手段で不正に観測するサイドチャネル攻撃 (Side-Channel Attack: SCA) は，近年の暗号処理回路に対する脅威として認知されている．SCA は，暗号 LSI の処理時間，消費電流や電磁波情報などの情報をリアルタイムに測定・操作し，暗号鍵情報を代表とした機密情報を逆算する攻撃手法である．Kocher らにより提案された，単純電力解析や差分電力解析 [1] が最も有名な攻撃手法であり，その拡張や対策が幅広く研究されている．本稿では特に，暗号 LSI から漏えいする電磁波に基づく SCA である，EMA (ElectroMagnetic Analysis) [2] に注目する．EMA は暗号 LSI に対する受動的な SCA の一種であり，安価な電磁プローブを用いることで，暗号 LSI より漏えいする電磁波強度パターンから機密情報を逆算できる．また，小口径電磁プローブを用いることで，暗号 LSI 内の局所的な漏えい電磁波を取得できる [3]．EMA は，安価かつ局所的に SCA を行える脅威として認識されている．

本稿は，EMA および，侵襲攻撃に対して耐タンパ性を示す光論理回路の構成手法を提案する．シリコンフォトニクスや集積ナノフォトニクスの登場により，チップ上でコヒーレント光を変調・制御できるようになった．この結果，光の低遅延性を活用し，CMOS 集積回路では実現できない超低遅延光演算回路の研究が活発化している．従来の光コンピューティング手法 [4–7] では，光の振幅情報を基に論理演算を行っている．他方，本稿では，位相変調に基づく論理演算手法を提案する．導波路中を通過する光信号の位相情報のみを変調し，論理演算を行うことで，光集積回路内を伝搬する光の強度情報を変調せずに論理演算を行える．この結果，光信号の有無のみから光集積回路の内部状態の取得することを困難にする．この結果，光集積回路中の電磁波情報から SCA を行うことを原理上困難にする．

本章の残りの構成は以下の通りである．第 2 章でまず，光集積回路の耐タンパ性に対するポテンシャルを述べ，本稿の成果を述べる．次に関連研究を述べる．第 3 章で耐タンパ光論理回路の設計手法を述べる．第 4 章で提案手法の性能評価を行う．第 5 章で回路実装方式に関して議論した後，第 6 章で結論を述べる．

2. 背景

2.1 動機

図 1 に示す方向性結合器に基づく論理回路を例に，本稿

[1] 京都大学大学院情報学研究科
[2] 京都大学工学部電気電子工学科
[3] NTT ナノフォトニクスセンタ
[4] NTT 物性科学基礎研究所
[a)] shiomi-jun@i.kyoto-u.ac.jp

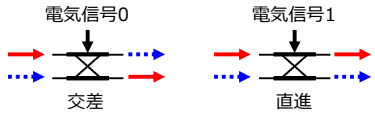

図 1　方向性結合器の定義.

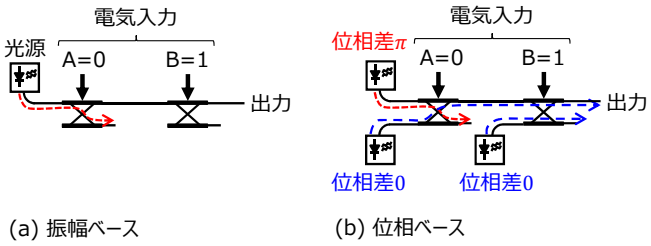

図 2　方向性結合器に基づく AND 回路.

の動機を示す．本稿で示す方向性結合器は，入力信号が 0 のときに入力光信号が交差して進み，1 のときに直進するよう設計される．ただし，光信号が交差する場合，光信号の位相が $\pi/2$ だけシフトすることに注意．方向性結合器に基づく AND 回路の例を図 2 (a) に示す．入力電気信号がすべて 1 の時のみ出力信号に光信号を出力し，この結果出力光の有無を検出することで AND 演算を行える．図 2 (a) の回路は振幅変調に基づく光論理回路である．したがって，入力信号値に応じて光信号の強度分布が切り替わっており，結果として SCA への脆弱性へ繋がる．例えばパッケージを開封・研磨し，導波路周辺へしみ出す近接場光をプロービングすることで，AND 回路内の論理情報を検知することが原理上可能である．

光は波動特性を示すため，様々な物理特性に論理値を割り当てることが可能である．次に，位相変調に基づく AND 回路を図 2 (b) に示す．位相変調に基づく論理回路では，基準光と比較した際の，コヒーレント光の位相差で論理値を定義する．例えば本稿では，位相差ゼロを論理値 0, 位相差 π を論理値 1 と定義する．図 2 (b) の回路では，入力信号値がすべて 1 の時のみ，位相差 π の信号を出力する．このため出力光の位相差を測定することで，論理演算結果を判定できる．なお，光信号が方向性結合器を交差する場合，位相が $\pi/2$ だけ変化するため，位相シフト分を逆算して光源を用意するか，方向性結合器の出力部分に位相シフタを接続する必要があることに注意．本回路は図 2 (a) に示した論理回路ほぼ同じ構成をとるが，任意の入力値に対し，すべての導波路および光素子内を光信号が常に通過している点が異なる．特に，光素子による光信号の減衰が無視できる程度まで小さい場合，導波路周辺をプロービングしても，得られる強度情報は入力データパターンに依存せず常に一定で，位相検波を行わない限り，内部状態を逆算することが困難である．本稿ではこの性質に注目し，耐タンパ性を示す光論理回路の設計手法を提案する．

2.2　関連研究と本稿の成果

EMA に基づく SCA の脅威は様々な論文で報告されている．例えば，入力データパターンに依存して変化するスタンダードセルの電流消費パターンが電磁マイクロプローブで測定可能であることを述べている [3]．EMA に基づく SCA に対する対策手法としては，例えば論理ゲートレベルの対策として WDDL などの手法が提案されている [8]．相補的に論理ゲートを稼働させることで，入力データパターンに依存せず常に一定の電力消費を行い，結果として漏えい電磁波の強度を平滑化する．回路レベルの対策としては，電磁プローブの接近を検知し，SCA を事前に検知するセンサデバイスの提案も行われている [9]．しかしながら，電荷の充放電に基づき論理演算を行う従来の CMOS 回路では，セルレベルで注目すると，入力データパターンに依存した電磁波が論理セルから物理的に漏えいする．本稿では，既存の CMOS 技術と異なり，光素子単体から漏えいする電磁波の強度を，理想的には変えることなく論理演算を行い，SCA に原理的に困難にする光論理回路設計手法を提案する．

光集積回路設計技術を耐タンパコンピューティングに適用する研究は，[10] で行われている．[10] では，ナノフォトニクスにおいて，近接場光相互作用によりナノ領域を移動する光信号より散逸するエネルギー，すなわち論理演算の際に光回路が消費するエネルギーが極めて小さく，攻撃者が観測することは極めて困難であるため，ナノフォトニクスに基づく光システムの耐タンパ性が極めて高いことを指摘している．しかし，光信号そのものをプロービングされた際の耐タンパ化技術や，具体的な論理回路設計手法は提案されていない．また，従来の光論理回路設計技術は，光信号の有無を検知して論理演算しており [4–7]，従来の光コンピューティング技術をそのまま適用しても，導波路のプロービングといった侵襲攻撃による論理情報の取得を避けられない．本稿ではこれらの問題に対応するため，以下を提案する．

- 光の位相変調に基づく耐タンパコンピューティング手法を提案する．位相変調に基づく論理演算により，光信号の伝搬経路を変えることなく論理演算を行えるようになり，光信号の有無の検出だけでは内部状態の観測自体が困難になる．
- 位相変調器の最も現実的な実装方式である，電気制御型光素子の電気制御端子から漏えいする電磁波を，マッハツェンダ変調器 (Mach-Zehnder Modulator: MZM) を用いて，限りなくゼロにする回路実装方式を提案する．提案実装方式を施すことで，従来型 CMOS 回路と同等以上の動作速度を保ちながら，CMOS 論理ゲート 1 個と比較して，電気制御端子 1 個で生じる電流時間変化量 ($\frac{di}{dt}$) を 300 倍以上削減可能であることを示し，攻撃者が使用する磁界プローブに生じる起電力を

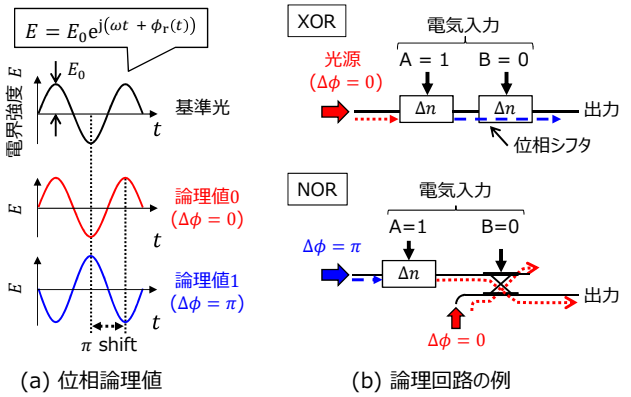

図 3　位相変調に基づく論理演算.

限りなくゼロにできることを示す.

3. 位相変調に基づく耐タンパコンピューティング

3.1 位相変調に基づく論理演算回路

本稿では，次式の位相変調に基づき論理演算を行う:

$$E \propto E_0 e^{j(\omega t + \phi_r(t) + \Delta\phi)}. \quad (1)$$

ここで，E は光の電界強度，E_0 はその振幅，ω は光の角振動数，t は時間である．$\phi_r(t)$ は，時間的にランダムに変調された位相シフト量である．光信号の位相に $\phi_r(t)$ を付加することで，位相検波に基づく SCA を困難にする．次に，$\Delta\phi$ のコンセプトを図 3 (a) に示す．光信号の論理値に応じて，位相を $\Delta\phi$ だけ変調する．本稿では，$\Delta\phi = 0$ を論理値 0, $\Delta\phi = \pi$ を論理値 1 と定義する．位相に基づく論理回路の例として，XOR 回路と NOR 回路の例を図 3 (b) に示す．位相シフタは，入力電圧に応じて屈折率を変えて光路長を制御する回路である．本稿では，入力電圧が 0 のときに位相変化なしとし，入力電圧が 1 のときに位相が π シフトするよう設計する．図 3 (b) 上部の回路では，2 つの入力信号のどちらか一方のみが 1 の場合，出力光の位相が π となり，出力光を観測することで，XOR 演算結果を観測できる．図 3 (b) 下部の回路では，入力信号がすべて 0 の場合のみ，出力光の位相が π となり，NOR 演算を行える．図 3 (b) の回路で重要な点は，すべての導波路と光素子において，入力データに依存しない，一定強度の光信号が通過する点である．したがって，導波路中の光信号強度から，内部状態を推定することが困難である．

回路の全体構成を図 4 に示す．図の “論理回路” は図 3 (b) の部分に相当する．光源の直後に位相変調器を配置して，“ランダム電圧” と書かれた部分で $\phi_r(t)$ に対応する位相オフセットを基準光に与える．電気制御入力の位相シフタや方向性結合器を用いて “論理回路” の部分で組み合わせ回路を設計する．“ホモダイン検波回路” にて基準光に基づき演算結果を検波し，電圧信号を生成する．“ホモダイン検波回路” を図 5 を用いて述べる．本稿では，[11] で述べられ

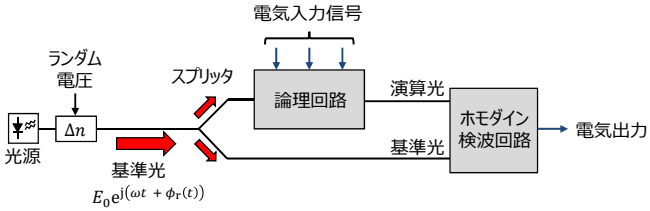

図 4　全体構成の概略図.

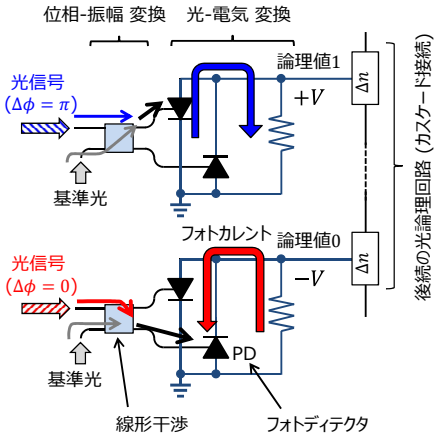

図 5　ホモダイン検波回路.

ている，光電変換器の構成をホモダイン検波回路として利用する．まず，論理値を持った入力光と基準光が線形干渉した光信号が 2 つのフォトディテクタ (PD) から出力される．この結果，入力光信号の位相に応じて，線形干渉の結果が変化し，光が入射する PD が変化する．この結果フォトカレントの流れる向きが逆になり，位相差に応じて出力電圧が変化する．フォトディテクタとして，[12] で提案されている低容量オンチップフォトディテクタの使用を想定する．図 5 右側に示すように “ホモダイン検波回路” の出力信号を次段の光素子に接続することで，論理ゲートをカスケード接続できる．図 3 (b) に示した NOR は完全系をなすため，カスケード接続により任意の組み合わせ回路を実現できる．フォトカレントの流れる向きが論理値に応じて切り替わるため，フォトカレントより漏えいする電磁波は入力データ依存となり，EMA に基づく SCA の対象となる．本稿では次節にて，この漏えい電磁波に対する回路的対策を述べる．

3.2 漏えい電磁波を限りなくゼロにする光電変換回路

まず，図 6 に示す，CMOS インバータを対象に，電磁的情報漏えいの発生メカニズムを述べる．CMOS 集積回路において，論理ゲートの出力値が切り替わる際に，負荷容量を充放電するために急峻な電流 i が発生する．i の時間変動により，集積回路周辺の周囲の磁束 Φ が時間的に変化し，レンツの法則により磁束の時間変化が EMA 攻撃者の磁界プローブに起電力 V を生じさせる [2]．電流 i の変動パターンは入力データに依存しており，磁束 Φ の時間変

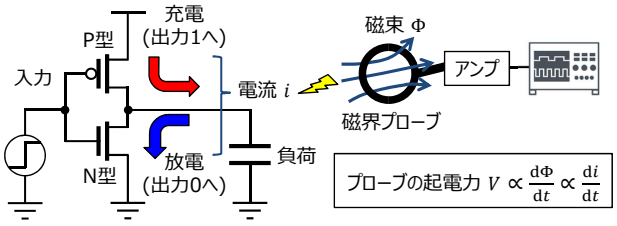

図 6　電磁プローブを通した電磁的情報漏えい.

化が SCA の対象となる．同期式 CMOS 回路を使用する場合，クロックエッジと共にフリップフロップと，その後続の論理ゲートが一斉に稼働するため，CMOS 回路において，たとえば単純にクロック周波数を遅くするだけなどの対策では起電力 V を削減することは困難である．

以上の議論から，図 5 のホモダイン検波回路に生じるフォトカレント i_{oe} の瞬時変化 ($\frac{di_{\mathrm{oe}}}{dt}$) を最小化することが重要である．本稿では，この課題を解決するため，マッハツェンダ変調器 (Mach-Zehnder Modulator: MZM) に基づく光電変換制御方式を提案する．本稿では，図 7 に示すようにスプリッタ，位相シフタ，コンバイナで構成された MZM を使用する．出力信号の強度が位相シフト量の正弦曲線に従う．本稿では，$-\pi/2$ から $\pi/2$ シフトの部分を利用し，$-\pi/2$ シフトの際にオフ，$\pi/2$ シフトの際にオンとなるスイッチとして MZM を利用する．位相シフト量を連続的に変調することで，出力信号強度を連続的に制御できる．図 8 に，MZM を用いたホモダイン検波回路の制御方式を示す．各クロックサイクル T にて，“set”，“reset”のタイミングを用意し，“valid”のタイミングで論理値を取得する．フォトカレント i_{oe} の時間変化量 $\frac{di_{\mathrm{oe}}}{dt}$ は T を大きくすることでゼロに収束し，EMA 攻撃者の磁界プローブに生じる起電力 V が，T の増大とともに小さくなる．

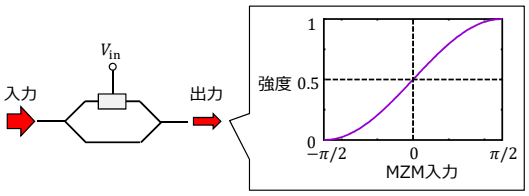

図 7　MZM による振幅変調.

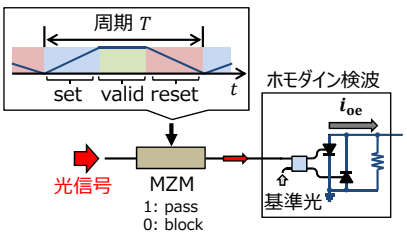

図 8　MZM に基づくフォトカレントの調節.

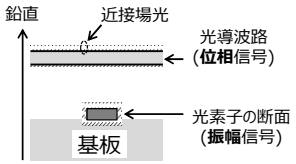

図 9　多層配線構造.

3.3　光フリップフロップに基づく順序回路設計

集積ナノフォトニクス技術を用いることで，光フリップフロップを実装できる．[13] において，ナノフォトニック共振器を用いた全光フリップフロップが提案されている．当該全光フリップフロップは，データ信号，クロック信号に対応する光信号の有無に基づきフリップフロップとして稼働する．位相変調された論理信号を，図 5 の “位相-振幅変換”にて振幅信号に変換することで原理上実装可能であるが，詳細な実装方式は今後の検討課題である．光フリップフロップや，図 5 の PD 直前の光信号は，振幅変調に基づき動作する．耐タンパ性を高めるために，図 9 のような多層配線構造が考えられる．振幅信号を取り扱う光素子の，近接場光により結合しない程度に離れた上層に位相信号を取り扱う導波路を配置する．攻撃者が下層配線の信号を盗聴するためには，上層配線を研磨等で破壊する必要があり，回路が誤動作し攻撃を検知できる．なお，このような多層配線構造はシリコンフォトニクス [14] などで実現可能な技術であるが，詳細な実装や耐タンパ性の評価は今後の検討課題である．

4.　光集積回路の耐タンパ性の評価

4.1　セットアップ

本章では，前章で述べたフォトカレント制御回路 (図 8) に示したフォトカレント調節回路に生じるフォトカレントの瞬時変化量を評価する．[11,12] で述べられたフォトディテクタの性能に基づき，光–電流変換効率を 1 A/W とする．フォトディテクタの受光可能な最小のパワーを 10 μW と仮定する．すなわち，図 8 の回路において，i_{oe} は ± 10 μA の間の値を取り得る．MZM は理想的な正弦曲線特性を有すると仮定し，10 μW の光信号が MZM に入力した状況を仮定する．図 8 の T のうち，“valid”の期間を 150 ps に固定し，T を変更して $\frac{di_{\mathrm{oe}}}{dt}$ の最大値を評価する．なお，フォトディテクタの寄生容量を 0.6 fF, 負荷容量を 1 fF，出力抵抗を 20 kΩ と仮定する [11] と，“valid”の期間で，最大値出力電圧の 95%以上の応答を実現できる．上記パラメータの下，光電混載回路シミュレータにて i_{oe} の時間変化を評価する．

他方，CMOS 集積回路に基づく比較対象として，商用 65 nm プロセスで設計された駆動力 1X の，十分長いファンアウト 1 インバータチェインの瞬時消費電流を評価する．各インバータセルとして，ポストレイアウトのネットリス

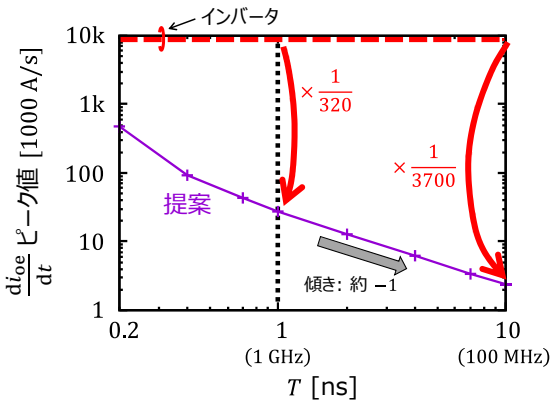

図 10　フォトカレントの瞬時変化量最大値と T の対応.

トを使用し，トランジスタレベル回路シミュレーションにより，消費電流の瞬時変化 $\frac{\mathrm{d}i}{\mathrm{d}t}$ の最大値を評価する．電源電圧を 1.0 V に設定する．

4.2　光電変換回路の耐タンパ性評価

図 10 に，フォトカレントの瞬時変化量の評価結果を示す．縦軸は $\frac{\mathrm{d}i_{\mathrm{oe}}}{\mathrm{d}t}$ の最大値，横軸は T である．赤色の破線は，1.0 V で動作するインバータチェインの消費電流の瞬時変化 $\frac{\mathrm{d}i}{\mathrm{d}t}$ の最大値である．なお，インバータチェインの $\frac{\mathrm{d}i}{\mathrm{d}t}$ の最大値は，インバータチェインが十分に長ければ，段数に依存せず一定になる．提案方式では，$\frac{\mathrm{d}i_{\mathrm{oe}}}{\mathrm{d}t}$ のピーク値が，T に反比例して減少する．インバータのピーク値を CMOS 論理ゲート 1 個を代表する値として $\frac{\mathrm{d}i_{\mathrm{oe}}}{\mathrm{d}t}$ と比較すると，集積回路のクロック周期の典型値である 1 ns, 10 ns において，それぞれ 320 分の 1, および 3700 分の 1 まで小さくできる．原理上は，T を十分大きくすることで，フォトカレントの瞬時変化を限りなく 0 に削減できる．3.2 節の議論により，$\frac{\mathrm{d}i_{\mathrm{oe}}}{\mathrm{d}t}$ の減少とともに，攻撃者の磁界プローブに誘導される起電力 V も限りなくゼロになる．

5.　議論

5.1　組み合わせ回路の実装手法

3.1 節にて，NOR ゲートをカスケード接続することで任意の組み合わせ回路を設計できることを示した．ただし，クリティカルパス中の光電変換の回数が論理の大規模化にしたがって増大する．図 8 に示した MZM を取り除いた場合の，光電変換に必要な遅延はおよそ 25 ps 程度と見積もられる [11]．一方で，光信号が位相シフタや方向性結合器を伝搬する遅延はデバイス長に依存し，本稿では 1 ps 程度と仮定する．したがって，クリティカルパス上の光電変換回数が増大すると，正確な論理演算を行うためには “valid” の期間を増大する必要があり，結果として，固定された周期 T の下では $\frac{\mathrm{d}i_{\mathrm{oe}}}{\mathrm{d}t}$ のピーク値が増大する．

図 2 に示した AND 回路は 2 入力であるが，直列接続する方向性結合器の数を増やすことで，途中に光電変換を加

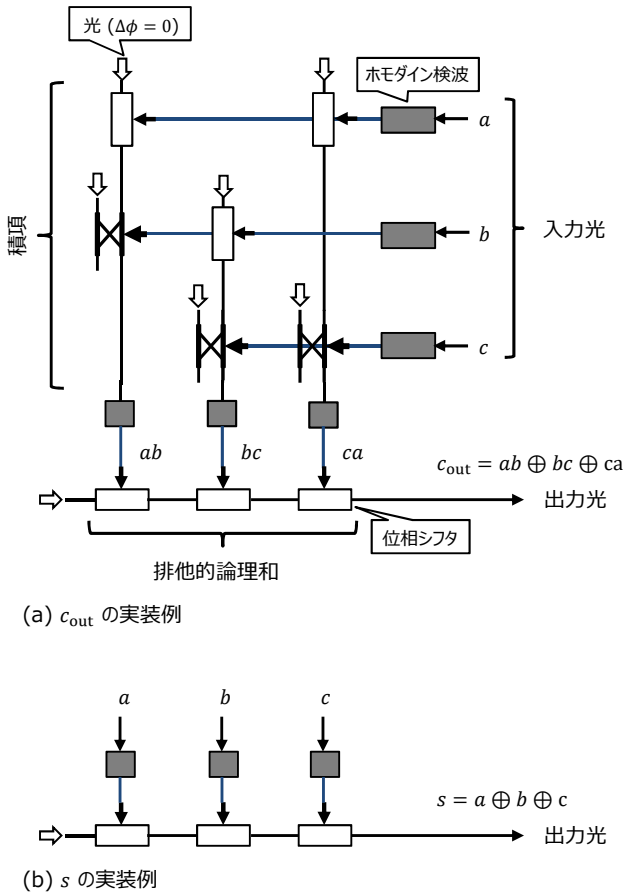

図 11　Exclusive-Sums-of-Products (ESOPs) に基づく全加算器の実装例.

えることなく多入力 AND を実装できる．しかし，入力数の増大とともに光源の個数を増やす必要があり，消費電力の増大に繋がる．他方，図 3 (b) に示した XOR 回路では，位相シフタを直列接続することで，光源を導入することなく多入力化できる．以上の事実を考慮し，XOR 演算を積極的に使用した設計例として，[6] などで検討されている Exclusive-Sums-of-Products (ESOPs) の利用などが考えられる．ESOPs では AND 演算された積項を XOR 演算で足し合わせることで論理演算を行う．ESOPs はリード-マラー標準形 (Algebraic Normal Form: ANF) を包含しており，任意の組み合わせ回路を実装できる．位相に基づく ESOPs の実装例を図 11 に示す．図 11 では，3 つの入力 a, b, c を持ち，2 つの出力 c_{out}, s を持つ全加算器である．図 11 (a) は，c_{out} の実装例である．入力光がホモダイン検波回路にて電気信号に変換され，位相シフタと方向性結合器からなるアレイに電気信号が供給される．当該アレイ部分で積項が計算される．積項結果を基に，図 11 の下部の位相シフタにて排他的論理和が計算される，出力光を観測することで，ESOPs を計算できる．図 11 (b) の s では積項が発生しないため，位相シフタのみが実装されている．クリティカルパス上の光電変換の個数は 2 以下である．

5.2 信号タッピングに対する耐タンパ性

提案回路の脆弱性として，集積イオンビーム (FIB) などでチップに穴を開け，タッピング用配線を作成し，信号タッピングによりホモダイン検波回路の出力電圧を読み取る可能性が考えられる．商用のアクティブプローブの容量は数 pF のオーダであり，フォトディテクタの容量成分より 100 倍以上大きい．したがって，プロービングを行われると回路がタイミング故障を起こし，攻撃を検知できる．

6. 結論

本稿では，光集積回路技術に基づき，耐タンパ性を示す論理回路設計手法を議論した．位相変調に基づき論理演算を行うことで，光集積回路内を伝搬する光信号の強度変調を行わずに演算を行え，光信号の有無のみから光集積回路の内部状態の取得を困難にする．また，マッハツェンダ変調器に基づき，光論理回路の電気制御端子より漏えいする電磁波を，限りなくゼロにする光電変換回路を述べた．光電混載回路シミュレータに基づく解析の結果，従来の CMOS 集積回路と同等の動作速度を保ちながら，CMOS インバータの消費電流の瞬時変化量と比較して，フォトカレントの瞬時変化量を 300 倍以上削減できることを示した．本稿では，位相変調に基づき，原理上論理回路を設計できることを示した．耐タンパ性の詳細な解析や，回路実装方式に対する詳細なフィージビリティスタディなどが今後の重要な課題である．位相シフタに生じる位相ノイズや，光素子で生じる減衰が入力電圧依存の場合における耐タンパ性の評価なども今後の重要課題である．

謝辞

本研究の一部は，科学技術振興機構の戦略的創造研究推進事業「新たな光機能や光物性の発現・利活用を基軸とする次世代フォトニクスの基盤技術」(JPMJCR15N4) の助成により行われた．本研究一部は，東京大学大規模集積システム設計教育研究センターを通し，シノプシス株式会社，日本ケイデンス株式会社，メンター株式会社の協力で行われた．

参考文献

[1] P. C. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” in *Annual International Cryptology Conference on Advances in Cryptology*, ser. CRYPTO ’99. Berlin, Heidelberg: Springer-Verlag, 1999, p. 388397.

[2] K. Gandolfi, C. Mourtel, and F. Olivier, “Electromagnetic analysis: Concrete results,” in *Cryptographic Hardware and Embedded Systems — CHES 2001*, Ç. K. Koç, D. Naccache, and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 251–261.

[3] T. Sugawara, D. Suzuki, M. Saeki, M. Shiozaki, and T. Fujino, “On measurable side-channel leaks inside asic design primitives,” in *Cryptographic Hardware and Embedded Systems – CHES 2013*, 2013, pp. 159–178.

[4] J. Hardy and J. Shamir, “Optics Inspired Logic Architecture,” *Opt. Express*, vol. 15, no. 1, pp. 150–165, Jan 2007.

[5] Q. Xu and R. Soref, “Reconfigurable optical directed-logic circuits using microresonator-based optical switches,” *Opt. Express*, vol. 19, no. 6, pp. 5244–5259, Mar 2011.

[6] C. Condrat, P. Kalla, and S. Blair, “Logic Synthesis for Integrated Optics,” in *Great Lakes Symposium on Great Lakes Symposium on VLSI*, ser. GLSVLSI ’11, 2011, pp. 13–18.

[7] Z. Zhao, D. Liu, Z. Ying, B. Xu, C. Feng, R. T. Chen, and D. Z. Pan, “Exploiting Wavelength Division Multiplexing for Optical Logic Synthesis,” in *Design, Automation Test in Europe Conference*, Mar 2019, pp. 1567–1570.

[8] K. Tiri, D. Hwang, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, “Prototype IC with WDDL and Differential Routing DPA Resistance Assessment,” in *Proceedings of the 7th International Conference on Cryptographic Hardware and Embedded Systems*, ser. CHES’05. Berlin, Heidelberg: Springer-Verlag, 2005, p. 354365.

[9] N. Homma, Y.-i. Hayashi, N. Miura, D. Fujimoto, D. Tanaka, M. Nagata, and T. Aoki, “Em attack is non-invasive? - design methodology and validity verification of em attack sensor,” in *Cryptographic Hardware and Embedded Systems – CHES 2014*, L. Batina and M. Robshaw, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 1–16.

[10] M. Naruse, H. Hori, K. Kobayashi, and M. Ohtsu, “Tamper resistance in optical excitation transfer based on optical near-field interactions,” *Opt. Lett.*, vol. 32, no. 12, pp. 1761–1763, Jun 2007.

[11] K. Nozaki, S. Matsuo, T. Fujii, K. Takeda, A. Shinya, E. Kuramochi, and M. Notomi, “Femtofarad optoelectronic integration demonstrating energy-saving signal conversion and nonlinear functions,” in *Nature Photonics*, vol. 13, Jul 2019, pp. 454–459.

[12] K. Nozaki, S. Matsuo, T. Fujii, K. Takeda, M. Ono, A. Shakoor, E. Kuramochi, and M. Notomi, “Photonic-crystal nano-photodetector with ultrasmall capacitance for on-chip light-to-voltage conversion without an amplifier,” *Optica*, vol. 3, no. 5, pp. 483–492, May 2016.

[13] A. Shinya, S. Mitsugi, T. Tanabe, M. Notomi, I. Yokohama, H. Takara, and S. Kawanishi, “All-optical flip-flop circuit composed of coupled two-port resonant tunneling filter in two-dimensional photonic crystal slab,” *Opt. Express*, vol. 14, no. 3, pp. 1230–1235, Feb 2006.

[14] W. D. Sacher, J. C. Mikkelsen, Y. Huang, J. C. C. Mak, Z. Yong, X. Luo, Y. Li, P. Dumais, J. Jiang, D. Goodwill, E. Bernier, P. G. Lo, and J. K. S. Poon, “Monolithically integrated multilayer silicon nitride-on-silicon waveguide platforms for 3-d photonic circuits and devices,” *Proceedings of the IEEE*, vol. 106, no. 12, pp. 2232–2245, 2018.