［研究助成（A）］

時間拡散暗号鍵生成と全光鍵配合を連携した高速・広帯域光暗号化技術の研究

Research on high-speed and wideband optical encryption technology with time-spreading encryption key generation and all-optical key combination

2191007

研究代表者　香川大学　創造工学部　講　師　小　玉　崇　宏

［研究の目的］

データセンタ周辺における光通信ネットワークでは，高秘匿なIoTデータのやり取りを実現するために，セキュアな光ファイバ通信システムの構築が求められる。将来のデータセンタ間光通信ネットワークでは，空間多重技術が導入されることで，盗聴者が光ノードやリンクなどにおいて空間的に光が漏れる箇所から信号を直接検出しやすくなり，物理的なセキュリティ攻撃の対象になることが懸念される。そのような背景から，エンド・ツー・エンドにおける物理層のデータ暗号に対する重要性について光通信分野でも認識されつつある。

光通信システムで既に市販化されているトランシーバ内の暗号化技術として，機密性を破るために膨大な計算処理時間を要するブロック暗号高度暗号化標準（AES）アルゴリズムが広く採用されている。ただし，AESアルゴリズムなどのビット単位の暗号化はビットレートの速度で処理されるため，暗号化と復号化の回路処理速度は，シンボルレートとシンボルの多値数が増大するにつれて線形的に増加する。

M値位相偏移変調（PSK）信号のシンボル単位の暗号化は，多値レベルのシンボル数に依存することなくシンボルレートのみに依存するため，ビット単位の暗号化に比べて遅い処理速度で暗号化を実現できるといった特長がある。

当研究室では，今後の高シンボルレート化に対応していくため，デジタルーアナログ変換器（DAC）とアナログーデジタル変換器（ADC）の通常の仕様を維持するユニフォームコンステレーションマスキング（UCM）を提案している。デジタルUCMは，同相直交変調器（IQM）で生成される前に予め暗号鍵のバイナリデータを基に位相シフトを行い，標準的なコンスタレーション形式を維持する単純なシンボル暗号化であり特長もあるが，次の2つの課題をもつ。(1) 各シンボルに含まれる暗号鍵ビット数が少ない，(2) 暗号化できる場所が送信ノードもしくは電気変換を伴う中継ノードに限定される。最近では，光信号処理によって2つの課題を同時に解決するため，高非線形デバイスにより非線形効果の1種である相互位相変調（XPM）を発生させて，位相を最大でπ［rad］シフトさせるアナログ的なUCMを備えた光BPSK信号の原理検証実験を行った。アナログUCMは市販の波長変換器と同様に光中継器を対象とした光ファイバ非線形光学効果を用いたアプリケーションの一つとなり得る。しかし，XPMによる位相回転量の増大に伴うポンプ光電力の増加だけでなく，自己位相変調（SPM）または誘導ブリルアン散乱（SBS）も同時に発生するため，位相シフト量とそれに伴う信号品

質劣化の観点で，アナログ UCM は BPSK 方式への適用に留まっていた。

今回，アナログ UCM とデジタル UCM を組み合わせたハイブリッド UCM 方式を提案する。この方式では，デジタル UCM 方式およびアナログ UCM 方式のように単体で用いる場合と比較して，シンボルに含まれるデータビット対する暗号鍵ビットの割合を増大できる。更に，低電力化と高秘匿化の 2 つの観点で，提案手法に対して 2 つの追加のアプローチについて検討した。1 点目は，アナログ UCM 自体の低消費電力化と非所望の非線形効果の抑圧を同時に実現するため，XPM を使用した $\pi/2$ 位相シフト UCM とバイナリ強度変調暗号化キーを適用した。また，2 点目は，非ゼロ復帰信号に対し判定点以外での情報をマスク化するため，暗号鍵ビットに相当する信号に対しフィルタによる帯域制限を行うことで，シンボル間で鍵情報を時間領域で拡散する時間拡散暗号鍵を適用した。提案するシステムの実現可能性を確認するために，1 つのシンボルに 2 つのデータビットと 2 つの暗号化キービットを含む 4 レベル PSK（QPSK）信号のハイブリッド UCM について初期段階での実験を行った。

［研究の内容，成果］

図 1 に，デジタル領域とアナログ領域のハイブリッド処理による UCM-QPSK システムの原理を示す。光送信器側では，シリアルデータ列が 2 ビットごとにセグメント化され，シンボルマッパによって 1 つのシンボルがマッピングされた後，デジタル UCM として動作するデジタルエンコーダによって暗号化される。光中継器のアナログエンコーダでは，XPM によって小さな光位相シフトを発生させる。バイナリデータで構成される暗号鍵ビット列は，鍵長のビット列が周期的に現れる。

受信器側では，ハイブリッド UCM により暗号化された受信シンボルがデジタルデコーダに

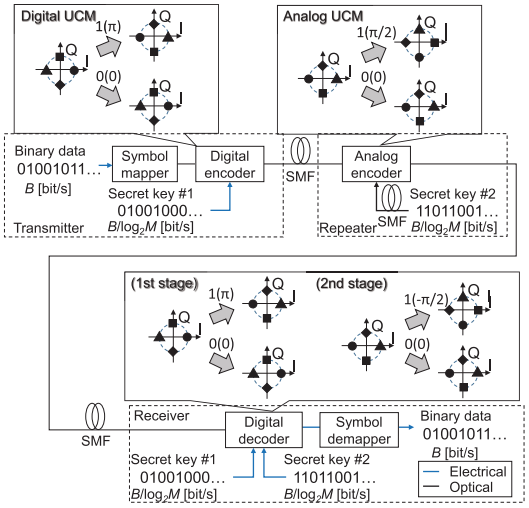

図 1　提案方式の構成

よって復号化される。デジタルデコーダでは，デジタルエンコーダおよびアナログエンコーダとは逆の位相シフト規則を適用する。NRZ 信号を対象とした場合，送信器側でデジタル UCM により暗号化された信号と光中継器でアナログ UCM を行うタイミングは非同期でも問題ないが，受信時のアナログデジタル変換器でサンプリングするタイミングは信号品質に影響を及ぼすため，受信器側でデジタル UCM とアナログ UCM の同期タイミングに関する情報は，予めパイロット信号などを用いて受信器側で認識しておく必要がある。今回の実験では，受信器側において送信器側と中継器側の暗号化のタイミングを事前に知っていることを前提とする。デジタルデコーダからの出力シンボルは 2 ビットに変換され，元のビット列が復元される。ハイブリッド UCM を適用した QPSK 信号が理想的に正しい暗号鍵でエンコードおよびデコードされる場合，ビット誤り率（BER）特性はデジタル UCM を使用する QPSK に近くなる。一方で，ハイブリッド UCM を適用した QPSK 信号が誤った暗号鍵でデコードした場合やデコードしなかった場合，信号に対する雑音量に関係なく BER 特性は約 0.5 になる。

図 1 に，QPSK 方式のハイブリッド UCM の動作原理を示す。送信器と中継器では，暗号鍵ビットが「1」の場合，位相シフト量はデジタ

ルエンコーダの「π」，アナログエンコーダの「$\pi/2$」である。暗号鍵ビットが「0」の場合，シンボルの位相はシフトしない。受信器では，復号鍵ビットが「1」の場合，第 1 段デジタルデコーダの位相シフト量は「π」，第 2 段デジタルデコーダの「$-\pi/2$」，シンボル位相は復号鍵ビットが「0」の場合，第 1 段および第 2 段ともに送信器側と同様にシンボルの位相シフトはない。

図 2 に，ハイブリッド UCM を用いた 10 GSymbol/s M-PSK システムの実験系を示す。純粋なデジタル UCM とハイブリッド UCM の特性を比較する実験を行った。原理確認実験として，任意波形発生器（AWG）とデジタルストレージオシロスコープ（DSO）でデジタルエンコーダとデジタルデコーダをエミュレートした。AWG と DSO のサンプリングレートはそれぞれ 10 GSa/s と 20 GSa/s となる。光中継器では，暗号鍵のシリアルなバイナリデータ列が強度変調器（IM）によって変調される。LD は，1545 nm の中心波長で CW を生成する。図 2 に示すように，CW 光は IM に入力された後，オンオフキーイング（OOK）信号に変調される。OOK 信号によって生成される SPM と SBS の量を監視するため，光サーキュレータ，光カプラ，および光スペクトラムアナライザ（OSA）を高非線形ファイバ（HNLF）の前後に配置した。HNLF で暗号化鍵ビットが「1」の場合，暗号化エンコーダで各シンボルの XPM による位相変化を「$\pi/2$」発生させる。一方で，HNLF で暗号鍵ビットが「0」の場合，XPM によるシンボル位相変化は発生させない。ここでは，28 個の疑似ランダムビット系列を 256 ビットとして使用する。

送信器では，シリアルバイナリデータが 2 ビット単位で分割され，シンボルマッパーでシンボルの 1 つにマッピングする。各シンボルの位相はデジタルエンコーダによって位相シフトされ，IQM によって変調される。単一の波長可変レーザーダイオード（LD）は，1 nm の帯域幅で 1550 nm の中心波長で連続波（CW）を生成する。CW 光は IQM に入力された後，デジタル UCM で QPSK 信号に変調される。

図 3 に，受信電力の関数としての受信信号の実験的な BER を示す。ここでは，QPSK 信号の場合のパフォーマンスをデジタル UCM およびハイブリッド UCM と比較した。図 3 に示すように，受信電力が −33 dBm の場合のデジタル UCM とハイブリッド UCM のコンスタレーションは，正確に 4 ポイントに収束しているため，アナログ暗号化強度に問題がないことを確認できる。デジタル UCM とハイブリッド UCM の誤り訂正限界である BER$=3.4\times10^{-3}$ 時点の電力ペナルティは，SBS のような非所望非線形光学効果の影響により 3.5 dB で発生した。デジタル UCM およびハイブリッド UCM 信号が間違った復号鍵でデコードされた場合またはデコードされなかった場合，雑音量

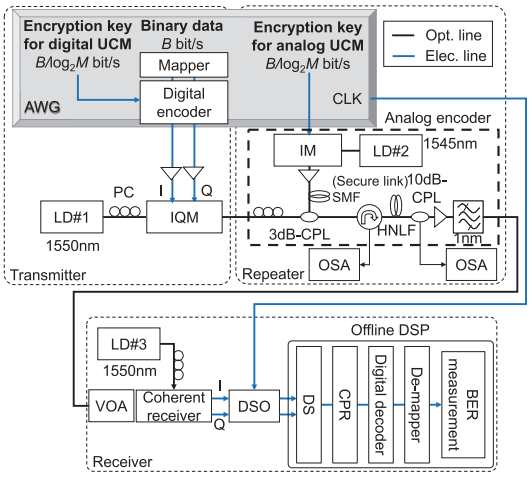

図 2　実験系

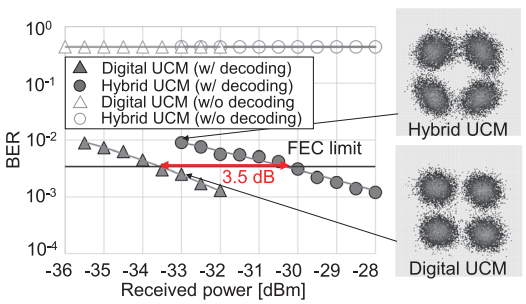

図 3　BER 特性

に関係なく BER 特性は 0.5 となる。

［今後の研究の方向，課題］

今回は，QPSK 信号に対して弱拡散暗号鍵の適用について検討したが，今後は更に高多値度な変調信号に対する適用について検討していきたいと考える。

［成果の発表，論文等］

国際会議投稿予定