カオスを用いた安全な通信

内田　淳史*,**・吉森　茂*

Secure Communication with Chaos

Atsushi UCHIDA and Shigeru YOSHIMORI

Secure communications with chaotic lasers have attracted increasing interests all over the world. We overview recent technologies of secure communications with chaotic lasers. We describe some techniques for message encoding and decoding based on synchronization of chaos. We quantitatively evaluate the degree of security for the techniques of secure communications with chaos. A new approach to secure communications using chaos based on information theoretic security is described.

Key words: secure communication, chaos, laser, security, synchronization, cryptography

高度情報化社会の基盤となる全世界規模の光通信ネットワークはすでに不可欠なインフラストラクチャーとして定着しつつあるが，伝送時における情報セキュリティー問題は，最重要課題であるにもかかわらず現在未解決のままである．従来のセキュリティー通信方式はコンピューターのソフトウェアで作成された暗号コードを用い，その秘匿性は計算量複雑性に起因しているが，これは近年提案されている量子コンピューターや次世代の超高速コンピューターにより原理的に解読可能となる．そこで，従来の手法とは異なる，「原理的に安全な」通信手法の開発は緊急課題であり，その一候補としてレーザーカオスを利用した通信方法が有用であると考えられる．これは送受信レーザー間のカオス同期現象を利用し，カオス的レーザー出力を秘匿通信の搬送波として用いることで，伝送信号を物理的に隠蔽する手法である．

レーザーカオスとは，レーザーの出力や波長が決定論に基づき不規則振動する現象のことである．工学的には，レーザーにおけるノイズ低減の一手法としての研究が古くから行われてきた．近年になり，カオス同期と呼ばれる手法を用いて，2つの離れたシステム間にて同一のカオス波形を共有することが実現可能となった[1]．その後，カオス波形を搬送波として利用した秘匿通信応用が実証され[2-4]，カオス現象を工学分野へ積極的に応用する動きが近年盛んである．カオスの乱雑性，広帯域特性を利用することで，秘匿通信や高帯域スペクトル拡散通信への応用可能性が指摘されている[5]．光通信システムにおいては特に，秘匿通信応用を目指した研究が近年盛んであり，ヨーロッパ共同体プロジェクトも発足している (http://www.imedea.uib.es/project/occult/)．

本稿では，レーザーカオスを用いた秘匿通信応用における現在の状況と今後の課題について概説する．これまでに提案されているレーザーカオスを用いた秘匿通信の概念や方式等について述べ，セキュリティーに関する定量的評価を行う．さらに，コンピューターでは原理的に解読不可能な情報理論的に安全な暗号鍵発生方式についても紹介する．

1. カオス同期

図1に，レーザーカオス通信の概念図を示す．送信側では，カオス搬送波にメッセージを埋め込んで送信する．受信側では，受け取った伝送信号からもとのカオス搬送波を差し引くことでメッセージの復号化が可能となる．ここで

*拓殖大学工学部情報エレクトロニクス学科（〒193-0985 八王子市館町 815-1）　E-mail: a-uchida@es.takushoku-u.ac.jp
**メリーランド大学カレッジパーク校（IREAP, College Park 20742, USA）

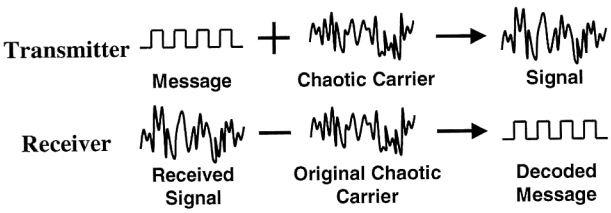

図1　カオス秘匿通信の概念図.

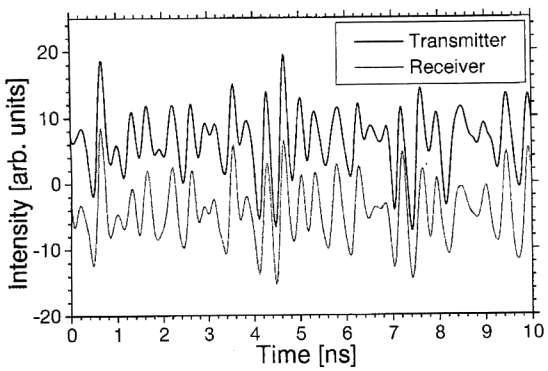

図2　半導体レーザーで発生したカオス同期波形[6].

送・受信間で同一のカオス搬送波を共有することが最も重要であり，これは「カオス同期」と呼ばれる技術により実現可能である.

カオス同期とは，2つの離れたカオスシステムにおいて同一のカオス波形を作成する手法である．カオスの有する初期値鋭敏性により，わずかな初期値の違いがカオスの時系列を大きく変化させるために，異なる2つのカオスシステムにて完全に同一のカオス波形を作成するということは不可能であると従来考えられてきた．しかしながら，結合されたカオスシステムにおいては，注入されたカオス信号に対して受信側が常に安定である条件を満たすことができる．つまり，受信システムの入力波形に対する条件付きリアプノフ指数（conditional Lyapunov exponents）がすべて負である場合，カオスシステム間の同期は実現される[1]．半導体レーザーにおけるカオス同期の例を図2に示す[6].

カオス同期の必要条件として，2つのシステム間のパラメーター値をすべて一致させることが重要である．カオスのダイナミクスはパラメーター値に強く依存しているため，システム間のパラメーター値が同一であるほど，カオス同期の実現は容易となる．この「パラメーター偏差に対するカオス同期許容幅」は，カオス通信の秘匿性を議論するうえで重要な指標である．パラメーター偏差に対するカオス同期許容幅が小さいほど，盗聴者はカオス同期を達成するのが困難となり，システムの秘匿性は向上するといえる（第4章参照）.

レーザーにおいては，カオス振動する複数のレーザーを

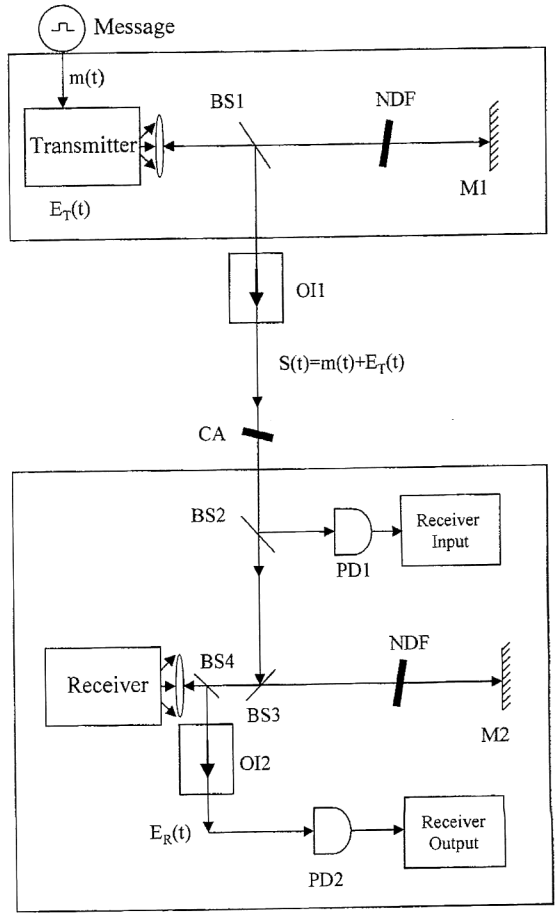

図3　半導体レーザーを用いたchaotic masking方式．BS：ビームスプリッター，PD：受光器，OI：光アイソレーター，M：ミラー，NDF：可変減光器，CA：減光器[15].

結合し，すべてのパラメーター値をできるだけ一致させることでカオス同期の実現が可能となる．これまでに，気体レーザー[7]，固体レーザー[8,9]，ファイバーレーザー[10]，および半導体レーザー[11-13]の，ほぼすべての種類のレーザーシステムにおいてカオス同期の報告がなされている.

2.　カオス秘匿通信方式

現在までに提案されているレーザーカオス秘匿通信方式は，大きく3つに分類される[14]．chaotic masking，chaotic modulation，およびchaos shift keyingと呼ばれる方式である.

chaotic masking法は，カオス搬送波に外部変調を加えてメッセージを隠蔽する手法である．半導体レーザーを用いたchaotic masking方式を図3に示す[15]．外部鏡を有する半導体レーザーにおいてカオスを発生させ，送信側にて半導体レーザーの注入電流を変調することでメッセージを埋め込む．受信側では，カオスとメッセージを含む伝送信号を分割し，一方はフォトダイオードへ，もう一方は送信

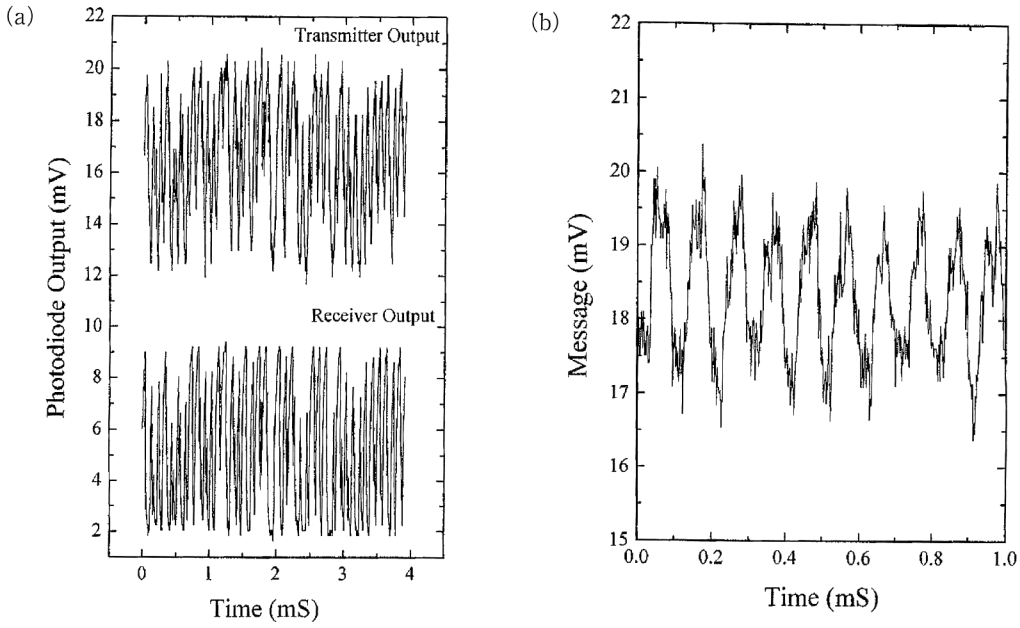

図4 (a) メッセージを含むカオス送信波形と受信側でのカオス同期波形，(b) 復元されたメッセージ波形（正弦波）[15]．

レーザーと同一パラメーター値を有する半導体レーザーへ注入する．受信側の半導体レーザーでは，カオス同期現象を利用して，もとのカオス搬送波のみを再現することが可能となる．この同期信号を別のフォトダイオードで検出し，メッセージを含む伝送信号からカオス同期信号を差し引くことで，もとのメッセージ信号を復元できる．図4(a)に，メッセージを含むカオス送信信号および受信側のカオス同期信号を示す．カオス搬送波にメッセージ信号が隠蔽されており，メッセージ信号は観測されない．しかしながら，この2つの波形の差信号を計算することで，図4(b)に示すような復号化信号（正弦波）が得られる．

chaotic masking 法では，カオスとメッセージを含む伝送信号を受信レーザーへ注入した場合に，なぜカオス信号のみを再現できるのか，という点が不明瞭である．これは，摂動に対するカオスアトラクターの安定性として解釈する報告[2]，またレーザー共振器の小信号に対する応答特性として解釈する報告[16]がなされている．いずれにせよ，chaotic masking を用いる際には，カオス信号の振幅に比べてメッセージ信号の振幅を十分に小さくする必要がある．

chaotic modulation 法は，初のレーザーカオス通信実証実験で用いられた手法であり[3,4]，その原理も明瞭である．メッセージをカオスダイナミクスの内部で変調するという点が重要であり，これが chaotic masking との大きな違いである．つまり，メッセージを用いてカオス自身を変調し，カオスのダイナミクスを変化させる．本手法は，時間遅延を有するレーザーカオスシステムに適用され，時間遅延ループ内で変調を加えている．図5では，ファイバーレーザーのループ内でメッセージを加えており[17]，メッセージ信号はファイバー増幅器へフィードバックされ，カオスダイナミクスを大きく変化させる．メッセージで変調されたカオス信号は，伝送信号として受信側へ送信される．受信側では，同一パラメーターを有するファイバー増幅器を用いてカオス同期を達成し，メッセージの復元が可能となる．

図6に chaotic modulation 法の実験結果を示す[17]．図6 (a) のカオス送信信号をみる限り，もとのメッセージは不明である．しかしながら，受信側で得られた図6 (b) の同期信号と送信信号との商を計算することで，メッセージの復号化が可能となる．図6 (c) では，メッセージであるディジタル信号列が回復している．

chaos shift keying 法は，2種類のカオス状態を送信側で作成し，それぞれディジタルビットに割り当てる方式であり，カオスを用いたディジタル信号伝送方式である．レーザーパラメーターのひとつをわずかに変化させると，カオス波形自身も変化する．パラメーターの変化により2つのカオス状態を作成し，それぞれディジタル信号の0，1に対応させ，送信したいビット列に応じてどちらか一方のカオス波形を送信する．受信側では2つのレーザーを用意し，それぞれ受信側の2つのカオス状態に対応するパラメーター値に設定する．受信側のどちらのレーザーがカオス同期するかに応じて，伝送されたディジタル信号を判別する方式である．chaos shift keying 法をさらに簡潔にしたのが，chaotic on-off keying と呼ばれる手法である．これは，受

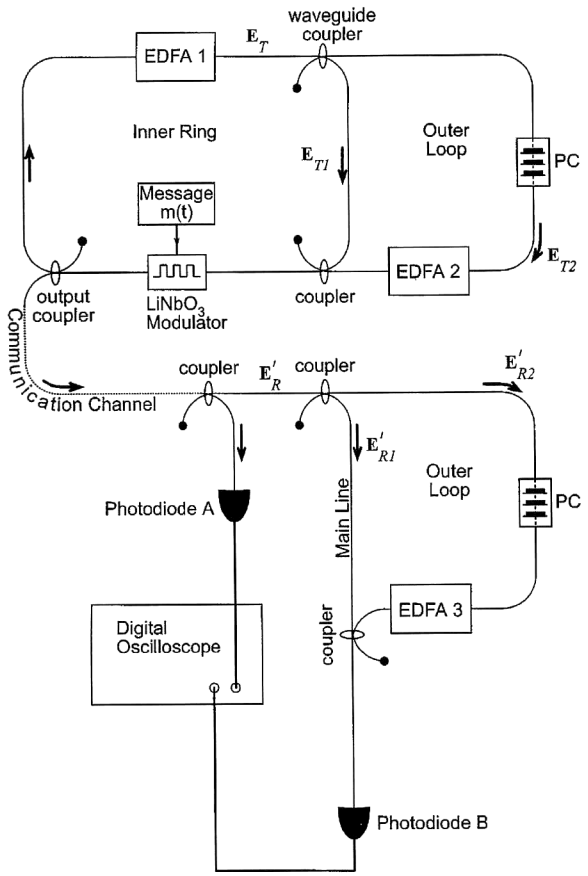

図5　ファイバーレーザーを用いたchaotic modulation方式．EDFA：エルビウム添加ファイバー増幅器，PC：偏光制御板[17]．

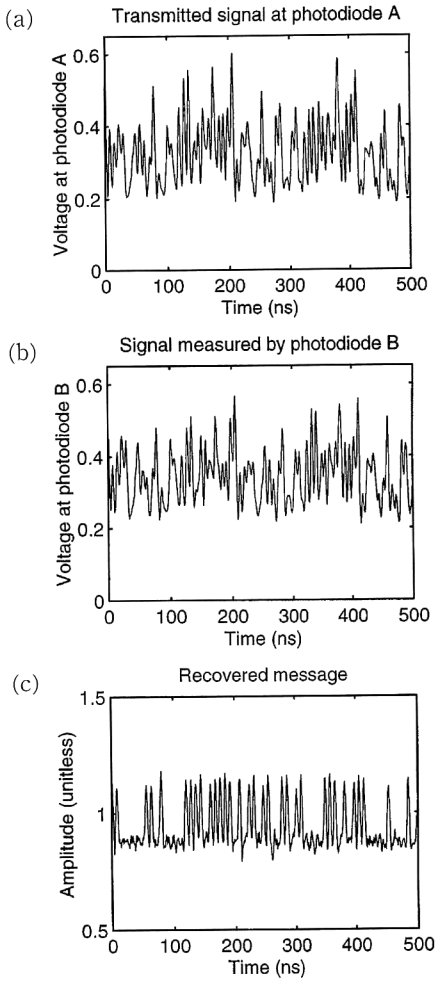

図6　(a) メッセージを含むカオス送信波形，(b) 受信側でのカオス同期波形，(c) (a)と(b)の波形の商，ディジタルメッセージ成分が復元されている[17]．

信側のレーザーを1つにし，カオス同期の達成の有無によりディジタル信号を判定する手法である．送受信間でカオス同期しているときは0，同期していないときは1と判定できる．マイクロチップレーザー[18]および光電気混合回路[19]において，本手法に基づく通信実験が実証されている．

これらの3手法を比較すると，原理的にメッセージの回復が保障され，メッセージの大きさや形式に対する制限のないchaotic modulation法が，汎用性の高いすぐれた方式である．chaotic modulation法が最も誤差特性にすぐれていることも，実験的に実証されている[14]．

3.　カオス通信の高速化および多重化

従来の光通信と同様に，レーザーカオス通信においても，通信の高速化が盛んに行われている．TangとLiuらは，光電気フィードバックを利用した半導体レーザーカオスにおいて，前章に述べた3種類の符号化・復号化方式を用いて，2.5 Gb/sの通信速度を実現した[14]．大坪らは，戻り光を有する半導体レーザーにてカオスを発生させ，chaotic masking法によりカオスに正弦波を重畳して1.5 GHzでメッセージの符号化・復号化を行った[20]．数値計算においては，戻り光を有する半導体レーザーで発生するカオスを用いて，20 Gb/sにおいてもメッセージ伝送が可能であることが示された[21]．

カオス通信を高速化する際に問題となるのが，カオスの帯域幅である．通常，カオススペクトルの帯域幅はレーザーの緩和発振周波数オーダーで決定されるため[22]，半導体レーザーの場合では数GHzが限度である．そこで，光注入法を用いた半導体レーザーカオスの帯域増大方式も近年提案されている[23,24]．

また，搬送波として利用するカオス波形が直交性を有している場合，カオス信号をスペクトル拡散符号として用いた多重通信が実現可能である[25]．複数のカオス搬送波を用いることで，複数の独立なメッセージを1つの伝送チャネルで送信することができる．しかしながら，一般的にはカオス波形が直交している条件を満たすことは困難である．そこで，近年，カオス多重同期という技術が提案されてい

る[26]．これは，複数のカオス搬送波を混合して1つの伝送チャネルで送信し，カオス同期法を用いて受信側でカオス波形を分離する手法である．送・受信システムにおいて対応するカオスシステム間ではパラメーター値を一致させ，対応しないシステム間では異なるパラメーター値を用いることで，カオス同期特性を利用することにより，混合されたカオス波形からカオスの分離が可能となる．

これまでに，複数のカオス波形を用いた多重通信が数値計算[27]および実験[28]により実証されている．しかしながら，これらはいずれも異なる波長において複数のカオス波形を作成し，メッセージを送受信している．したがって，前述のようなカオスの特性を利用した多重化というよりも，波長多重通信にカオスをサブキャリヤーとして用いている方式である．カオスの直交性や多重同期特性を利用した多重通信方式の提案・実証は，今後の課題であろう．

4. セキュリティー

カオス通信，特に秘匿通信への応用の際に最も重要となるのが，セキュリティーの定量的評価である．これまで数多くのレーザーカオス通信に関する論文が出版されているにもかかわらず，セキュリティー問題を定量的に議論している文献は驚くほど少ない[29]．これは，カオス秘匿通信においては，システム自体を非公開にするというハードウェア依存型セキュリティーを仮定しているため，システムを公開することが大前提となる暗号学的な意味でのセキュリティーを評価することが困難であるからであろう．カオス通信の研究が開始された当初は，カオスは乱雑であるがゆえに高いセキュリティーを有する，という表現が文献中に多々みられたが，これは必ずしも正しくない．セキュリティーの定義を行いシステムを定量的に評価することが，カオスの秘匿通信応用に関して非常に重要な課題である．

カオス通信におけるセキュリティーは，カオス同期特性で評価できる[30]．正規ユーザー以外の盗聴者が所有するレーザーにおいても，カオス同期が達成された場合，盗聴が可能となり安全性は失われる．カオス同期達成の「鍵」となるのが，送・受信間ですべてのシステムパラメーター値を一致させることである．ここで，従来の暗号学の手法と同様に，レーザーシステムは公開されており，すべてのシステムパラメーターの値が秘密鍵であると仮定しよう．レーザーの可変パラメーターが n 個存在し，パラメーター偏差に対するカオス同期の許容幅の平均値が $m\%$ であるとする．この許容幅とは，例えば1つのパラメーター値を100% 変化させたとき，$m\%$ の変化以内ではカオス同期が維持できるということである．盗聴者は，パラメーター値をスキャンしてすべてのパラメーター値を検索することで鍵の推定が可能であり，それに要する回数は，$(100/m)^n$ と定量的に見積もれる．例えば $m=50\%$ と仮定すると，n 個の可変パラメーターを有するシステムに対する安全性は，n ビットの秘密鍵の全数探索と同じ労力が必要になる．$m=6.25\%$ とすると組み合わせは $16^n=2^{4n}$ となり，128 ビットの秘密鍵と同等の秘匿性を有するためには，$n=32$ 個の可変パラメーターが必要になる．このように，可変パラメーターの個数を増加させること，またパラメーター偏差に対する同期許容幅を小さくすることにより，盗聴者に対してカオス同期を困難とさせ，秘匿性を向上させることが可能となる[30]．

カオス通信におけるセキュリティーの別の評価方法としては，カオス時間波形の特徴からシステムパラメーター値を推測する方法があげられる[31]．カオス時間波形は完全乱数ではなく，何らかのシステムの物理的特徴を内包しているため，その特徴を利用してレーザーのパラメーター値を推定することが可能となる．時間遅延を有するレーザーカオス波形の場合，時間波形の自己相関を計算することで遅延時間を推定でき，すべてのパラメーター値を探索しなくても遅延時間を求められる．このような攻撃法は，暗号学における，線形探索や差分探索のような暗号列の特徴を利用して最適な解読を行うという攻撃方法に類似している．カオスが内包する物理的特性に着目した攻撃方法を提案していくことで，秘匿性の定量化および強化が今後実現されるであろう．例えば，上述の攻撃を避けるために，時間遅延を変調することで自己相関関数をデルタ関数に近づける方法も提案されている[32]．

5. カオス通信の新潮流

前章までに述べたカオス通信方式はいずれも，カオス同期を利用する方式であった．セキュリティーを向上させるためには同期許容幅を減少させればよいが，その場合カオス同期が不安定化するため，カオス同期の安定性とセキュリティーには常にトレードオフの関係がある．そこで近年，カオス同期を利用しない新たな秘匿通信方式が提案されている[33]．これは情報理論的に安全な暗号鍵発生方式と呼ばれ，メッセージの秘匿化に必要な秘密暗号鍵の発生方式であり，カオス同期を用いた通信方式とは本質的に異なる．情報理論的安全性とは，盗聴者の情報が限定されているという仮定に基づき，確率論で暗号鍵の安全性を保障するものである．

以下に，その概念を示す[33](図7参照)．正規ユーザーのアリスとボブが，盗聴者のイブに対して安全な暗号鍵を共

有することを考える．公開チャネル上に暗号生成用のランダム波形が伝送され，アリスとボブは独立にこのランダム波形をサンプリングする．ここで重要なのは，アリスもボブもイブも「すべての」ランダム波形を取得することは不可能であるという仮定である．物理的に発生させた超高速なランダム波形を用いることにより，測定器のサンプリング速度の制限や測定器内のメモリー容量の制限によって，この仮定が満たされる．一例として，高速振動する半導体レーザーカオスをランダム波形発生用デバイスとして用いることができる（図7）．アリスとボブは全ランダム波形列の一部分のサンプルをそれぞれ所有しているが，サンプリング終了後にどのサンプルを所有したかの情報を公開チャネル上で交換し合う（例えば，取得したランダム波形の前半部分をお互いに公開する）．もしもアリスとボブが同一のサンプルを共有していることが確認されれば，そのサンプルの後半部分（非公開）から秘密暗号鍵を作成することが可能となる．ここでイブも同様に，アリスとボブがどのサンプルを共有しているのかを盗聴できるが，いかなるユーザーもすべてのサンプルを取得できないという仮定のため，アリスとボブが共有しているサンプルをイブまでもが所有していない可能性がある．つまり，アリスとボブがあるサンプルを共有している確率に対して，そのサンプルをイブまでもが所有している確率をはるかに小さく設定することで，情報理論的に秘匿性が保障される．さらに，1回のセッションで生成された共有鍵を複数組み合わせて1つの鍵を作成することで，イブに対する鍵の強度を指数関数的に向上させることが可能となる[33]．

本手法の利点として，計算量的安全性（computational security）の弱点である，将来の計算能力の向上による暗号解読の恐れが完全にないこと，およびシステムにおけるセキュリティーの制御・評価が定量的に可能であること，があげられる．本手法は，非常に新規性に溢れる画期的なカオス暗号鍵発生方式であり，次世代の暗号技術となりうるポテンシャルを秘めている．

本稿では，レーザーカオスを用いた秘匿通信応用に関する研究を紹介してきた．カオス同期に基づく通信方式では，セキュリティーと同期安定性のトレードオフが常に存在するがゆえに，高いセキュリティーを得るのは困難であろう．一方で，第5章で提案した情報理論的に安全な暗号鍵発生方式はセキュリティーの定量化が可能であり，カオスを単純な乱数発生器として用いるがゆえにその工学的実装も容易なため，今後の有望なセキュリティー方式といえる．

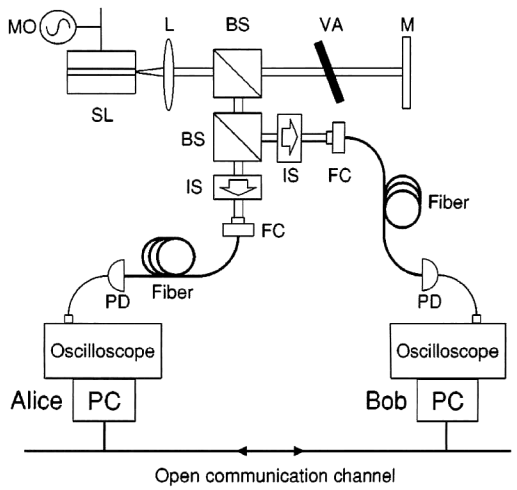

図7　半導体レーザーカオスを用いた情報理論的に安全な暗号鍵発生方式．BS：ビームスプリッター，FC：ファイバーカップラー，IS：光アイソレーター，L：レンズ，M：ミラー，MO：トリガー用変調，PC：コンピューター，PD：受光器，SL：半導体レーザー，VA：可変減光器[33]．

また，カオス通信研究における別の問題意識として，カオスのようなノイズ的アナログ信号伝送下で，情報を正しく送受信することは可能なのか，ということがあげられる．これは本質的に，アナログ情報処理を強いられる生体内での電気信号伝達や脳内でのニューラルネットワーク内での通信における重要な課題である．このように単に光秘匿通信への直接応用という意味合いだけでなくとも，カオス通信研究の意義は大いにあり，本研究で培われた知識や技術を他の物理・化学・生物分野へと横断的に移植することで，予測しえなかった新たな応用が芽生えるかもしれない．

カオスの通信応用に関して大変有意義なディスカッションをしてくださった大坪順次先生，吉村和之博士，Dr. Peter Davis, Dr. Yun Liu, Prof. Rajarshi Roy, Dr. Fabien Rogister, Prof. Jordi García-Ojalvo に感謝いたします．また，日本学術振興会海外特別研究員制度のご支援に感謝いたします．

文　献

1) L. M. Pecora and T. L. Carroll: "Synchronization in chaotic systems," Phys. Rev. Lett., **64** (1990) 821-824.
2) K. M. Cuomo and A. V. Oppenheim: "Circuit implementation of synchronized chaos with applications to communications," Phys. Rev. Lett., **71** (1993) 65-68.
3) G. D. VanWiggeren and R. Roy: "Communication with chaotic lasers," Science, **279** (1998) 1198-1200.
4) J. P. Goedgebuer, L. Larger and H. Porte: "Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode," Phys. Rev. Lett., **80** (1998) 2249-2252.

5) M. P. Kennedy, R. Rovatti and G. Setti: *Chaotic Electronics in Telecommunications* (CRC Press, Boca Raton, 2000).
6) I. Fischer, Y. Liu and P. Davis: "Synchronization of chaotic semiconductor laser dynamics on subnanosecond time scales and its potential for chaos communication," Phys. Rev. A, **62** (2000) 011801(R).
7) T. Sugawara, M. Tachikawa, T. Tsukamoto and T. Shimizu: "Observation of synchronization in laser chaos," Phys. Rev. Lett., **72** (1994) 3502-3505.
8) K. Otsuka, R. Kawai, S.-L. Hwong, J.-Y. Ko and J.-L. Chern: "Synchronization of mutually coupled self-mixing modulated lasers," Phys. Rev. Lett., **84** (2000) 3049-3052.
9) A. Uchida, T. Ogawa, M. Shinozuka and F. Kannari: "Accuracy of chaos synchronization in Nd : YVO_4 microchip lasers," Phys. Rev. E, **62** (2000) 1960-1971.
10) Y. Imai, H. Murakawa and T. Imoto: "Chaos synchronization characteristics in erbium-doped fiber laser systems," Opt. Commun., **217** (2003) 415-420.
11) J. Ohtsubo: "Chaotic dynamics in semiconductor lasers with optical feedback," *Progress in Optics, 44*, ed. E. Wolf (Elsevier, Amsterdam, 2002) pp. 1-84.
12) A. Murakami and J. Ohtsubo: "Synchronization of feedback-induced chaos in semiconductor lasers by optical injection," Phys. Rev. A, **65** (2002) 033826.
13) Y. Liu, Y. Takiguchi, P. Davis, S. Saito and J. M. Liu: "Experimental observation of complete chaos synchronization in semiconductor lasers," Appl. Phys. Lett., **80** (2002) 4306-4308.
14) J. M. Liu, H. F. Chen and S. Tang: "Synchronized chaotic optical communications at high bit rates," IEEE J. Quantum Electron., **38** (2002) 1184-1196.
15) S. Sivaprakasam and K. A. Shore: "Message encoding and decoding using chaotic external-cavity diode lasers," IEEE J. Quantum Electron., **36** (2000) 35-39.
16) A. Uchida, Y. Liu and P. Davis: "Characteristics of chaotic masking in synchronized semiconductor lasers," IEEE J. Quantum Electron., **39** (2003) 963-970.
17) G. D. VanWiggeren and R. Roy: "Communication with optical chaotic waveforms," Phys. Rev. Lett., **81** (1998) 3547-3550.
18) A. Uchida, S. Yoshimori, M. Shinozuka, T. Ogawa and F. Kannari: "Chaotic on-off keying for secure communications," Opt. Lett., **26** (2001) 866-868.
19) J.-B. Cuenot, L. Larger, J.-P. Goedgebuer and W. T. Rhodes: "Chaos shift keying with an optoelectronic encryption system using chaos in wavelength," IEEE J. Quantum Electron., **37** (2001) 849-855.
20) K. Kusumoto and J. Ohtsubo: "1.5-GHz message transmission based on synchronization of chaos in semiconductor lasers," Opt. Lett., **27** (2002) 989-991.
21) D. Kanakidis, A. Argyris and D. Syvridis: "Performance characterization of high-bit-rate optical chaos communication systems in a back-to-back configuration," IEEE J. Quantum Electron., **21** (2003) 750-758.
22) J. Mørk, B. Tromborg and J. Mark: "Chaos in semiconductor lasers with optical feedback: Theory and experiment," IEEE J. Quantum Electron., **28** (1992) 93-108.
23) Y. Takiguchi, K. Ohyagi and J. Ohtsubo: "Bandwidth-enhanced chaos synchronization in strongly injection-locked semiconductor lasers with optical feedback," Opt. Lett., **28** (2003) 319-321.
24) A. Uchida, T. Heil, Y. Liu, P. Davis and T. Aida: "High-frequency broad-band signal generation using a semiconductor laser with a chaotic optical injection," IEEE J. Quantum Electron., **39** (2003) 1462-1467.
25) K. Yoshimura: "Multichannel digital communications by the synchronization of globally coupled chaotic systems," Phys. Rev. E, **60** (1999) 1648-1657.
26) Y. Liu and P. Davis: "Dual synchronization of chaos," Phys. Rev. E, **61** (2000) R2176-R2179.
27) J. K. White and J. V. Moloney: "Multichannel communication using an infinite dimensional spatiotemporal chaotic system," Phys. Rev. A, **59** (1999) 2422-2426.
28) J. Paul, S. Sivaprakasam and K. A. Shore: "Dual-channel chaotic optical communications using external-cavity semiconductor lasers," J. Opt. Soc. Am. B, **21** (2004) 514-521.
29) F. Dachselt and W. Schwarz: "Chaos and cryptography," IEEE Trans. Circuits Syst. I, **48** (2001) 1498-1509.
30) K. Yoshimura: "Secure communications using cascaded chaotic optical rings," Int. J. Bifurcation Chaos, **14** (2004) 1105-1113.
31) J. B. Geddes, K. M. Short and K. Black: "Extraction of signals from chaotic laser data," Phys. Rev. Lett., **83** (1999) 5389-5392.
32) W.-H. Kye, M. Choi, M.-W. Kim, S.-Y. Lee, S. Rim, C.-M. Kim and Y.-J. Park: "Synchronization of delayed systems in the presence of delay time modulation," Phys. Lett. A, **322** (2004) 338-343.
33) A. Uchida, P. Davis and S. Itaya: "Generation of information theoretic secure keys using a chaotic semiconductor laser," Appl. Phys. Lett., **83** (2003) 3213-3215.

(2004年3月25日受理)