半導体レーザーのランダム現象を用いた超高速物理乱数生成と相関乱数秘密鍵配送

内田　淳史[*1]・吉村　和之[*2]・村 松　純[*2]
デイビス ピーター[*2, *3]・原山　卓久[*4]・砂 田　哲[*5]

Fast Physical Random Number Generation and Secure Key Distribution with Random Phenomenon in Semiconductor Lasers

Atsushi UCHIDA[*1], Kazuyuki YOSHIMURA[*2], Jun MURAMATSU[*2], Peter DAVIS[*2, *3], Takahisa HARAYAMA[*4] and Satoshi SUNADA[*5]

We overview recent progress on use of semiconductor lasers for fast physical random-number generation and secure key distribution. We describe techniques for improvement of generation speed of random number generators using chaotic semiconductor lasers, and their miniaturization. We also report on secure key distribution based on information-theoretic security with synchronized semiconductor lasers.

Key words: chaos, semiconductor laser, information security, random number generation, secure key distribution, physical randomness, correlated randomness

高度情報化社会における情報セキュリティーや，自然予測分野および設計工学における大規模数値シミュレーションには，乱数とよばれるランダムな数列が必要不可欠である．インターネットや携帯電話における情報セキュリティーの信頼性は，ランダムな数列である乱数に強く依存している．例えばインターネット商取引においては，電子情報の秘匿化，本人認証，ディジタル署名などに乱数が利用されており，乱数の予測不可能性，非再現性，統計的均一性が情報セキュリティー上きわめて重要な特性となる．特に，暗号技術の中で乱数を利用する部分として，鍵生成が挙げられる．乱数のランダム性が低い場合，盗聴者による鍵の推定が容易になり，鍵の秘匿性に依存した暗号システムの安全性の脅威に直結する．

現在多く用いられている乱数は擬似乱数とよばれ，コンピューターを用いて決定論的に生成される．それゆえに盗聴者が乱数の初期値（シード）を推定することで乱数の予測が可能になるという致命的欠点を有している．これを改善するために，物理乱数とよばれる自然現象を利用した乱数生成方式が近年注目を浴びており，電子回路の熱雑音等を用いて実装されている．物理乱数は雑音を用いているがゆえにランダム性が高いという優れた特性を有しているものの，従来の方式では生成速度が遅いのが欠点であり，その生成速度は最大でも 1 Gb/s 程度にとどまっている[1]．

本課題を解決するために，半導体レーザーカオスを用いた超高速物理乱数生成器が近年注目されている．2008 年に 1.7 Gb/s での乱数生成が初めて実験実証されて以来[2,3]，本分野は急速な進展をみせている．半導体レーザーの高速性とカオスのランダム性を組み合わせることで，1〜400 Gb/s の生成速度を有する超高速物理乱数生成器の実現方法がこれまでに報告されている[2–5]．さらに乱数生成器の

[*1] 埼玉大学大学院理工学研究科数理電子情報部門（〒338–8570 さいたま市桜区下大久保 255）　E-mail: auchida@mail.saitama-u.ac.jp
[*2] NTT コミュニケーション科学基礎研究所（〒619–0237 京都府相楽郡精華町光台 2–4）
[*3] (株)テレコグニックス（〒606–8314 京都市左京区吉田下大路町 58–13）
[*4] 早稲田大学理工学術院先進理工学部応用物理学科（〒169–8555 東京都新宿区大久保 3–4–1）
[*5] 金沢大学理工研究域機械工学系（〒920–1192 金沢市角間町）

小型化を目指した光集積回路や乱数生成モジュールも提案されている[6–8]．そこで本稿の前半部では，半導体レーザーカオスを用いた超高速物理乱数生成方式について概説する．本テーマに関する解説論文等はすでに出版されているが[9–12]，本稿では特に乱数生成の高速化と小型化に関する近年の進展について述べる．

ところで，2人のユーザーが秘匿通信を実現するためには，事前に秘密情報（秘密鍵）を共有している必要がある．秘密鍵配送とは，あらかじめ秘密鍵を共有していない2人のユーザーがこれを共有するための技術である．秘密鍵配送の安全性概念として，2つの異なる概念が知られている．そのひとつは，計算量的な仮定に基づく安全性であり，現在一般に使われている公開鍵暗号がこのタイプに属する．もうひとつは，無限の計算能力を有する盗聴者を想定した場合にも秘密情報の解読が不可能なタイプの安全性概念であり，情報理論的安全性とよばれている．後者の実現には，計算能力の限界に代わる仮定が導入される．

物理的な原理や性質に基づいて情報理論的安全性を備えた鍵配送を実装する試みが，近年盛んになされている．そのような試みの中で，量子暗号[13]は特によく知られている．これは量子力学的原理に基づく方式であり，究極の安全性を実現する観点からは重要な方式である．しかしながら，信号光の中継が困難なため，通信距離が最大でも100 km程度に制限される．そこで，通信距離の制約を取り除き汎用性を高める観点より，古典的な光学現象を利用した鍵配送方式が提案されている[14,15]．

情報理論分野においては，2人のユーザーが相関のある乱数源を利用可能な場合に，公開通信路上での情報交換により，第三者に対し完全に秘密の情報（秘密鍵）をユーザー間で共有可能であることが知られている[16]．自然界には，現在の観測技術では，その付随する物理量を完全に観測することが著しく困難な対象が存在する．そのような観測に関する物理的制約を，“bounded observability”とよぶ[17]．典型的な例のひとつとして，時間的に高速かつランダムに位相と振幅が変動するような広帯域光が挙げられる．最近，広帯域ランダム光の完全観測困難性とレーザー同期現象を利用する相関乱数源の実装法が提案されている[18,19]．そこで本稿の後半部では，この相関乱数源の実装法と，それを用いた秘密鍵配送方式について解説を行う．

1. 半導体レーザーカオスを用いた超高速物理乱数生成

1.1 物理乱数生成器の構成

物理乱数生成器は，ランダム信号生成源としての「前処理部」と，ディジタル信号処理を用いた乱数抽出部の「後処理部」に大別される．構成図の一例を図1に示す．前処理においては，戻り光を有する半導体レーザーを用いてカオス的振動出力を生成させる．これは半導体レーザーの外部に鏡を設置し，自分自身の微弱な戻り光によりレーザー出力が不安定化する現象である[11,12]．レーザーの緩和発振周波数と外部共振周波数との非線形相互作用により，数GHz以上のカオス的振動光出力が観測される．また1.2節で述べるように，高速化のために2つの半導体レーザーを一方向に結合することで，カオスの帯域拡大を実現できる．さらに，1つのカオス信号を分割し，一方に時間遅延を導入することで，相関の低い複数のカオス信号を用いることも可能となる．これらのカオス光信号を光検出器により電気信号へと変換する．前処理においてカオス光信号の代わりに，量子状態の不確定性に基づくゆらぎや自然放出光ノイズを用いる方法も提案されている[9–11]．カオス信号を用いる利点としては，その高速性と可制御性にある．カオスの周波数帯域は半導体レーザーの緩和発振周波数により決定されるため，乱数生成源として用いた場合の最大生成速度の制御や設計が可能となる．

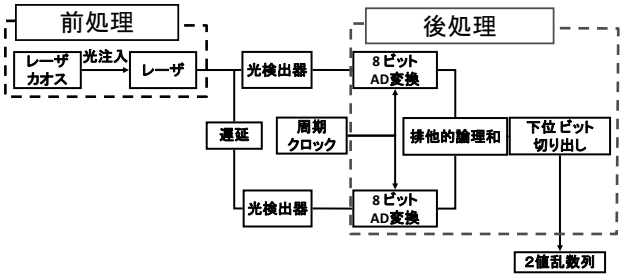

図1　物理乱数生成器の構成例．

次に後処理においては，得られた電気信号に対して周期クロックでサンプリングと閾値処理を行い，閾値の上下に応じて1または0へと変換する．また，AD（analog to digital）変換器を用いて複数ビット列へ変換することで，より多くのビットを抽出することも可能である．さらに乱数のランダム性（二値乱数の0, 1の出現確率の偏り等）の向上のために，排他的論理和などの論理演算や下位ビット切り出し処理を行うことで，最終的な二値乱数列を出力する．得られた乱数に対しては，統計乱数検定を用いてランダム性の評価を行う．

戻り光を有する半導体レーザーのカオス時間波形は量子ゆらぎを含む微小ノイズの影響を受けて変化するため，サンプリング間隔が十分に長ければ（例えば1 ns以上），得られたビット列は確率的となる．このサンプリング間隔が長いほどビット列の相関は小さくなり，ビット列の予測は困難となる．さらにカオスの周波数スペクトルが白色ノイ

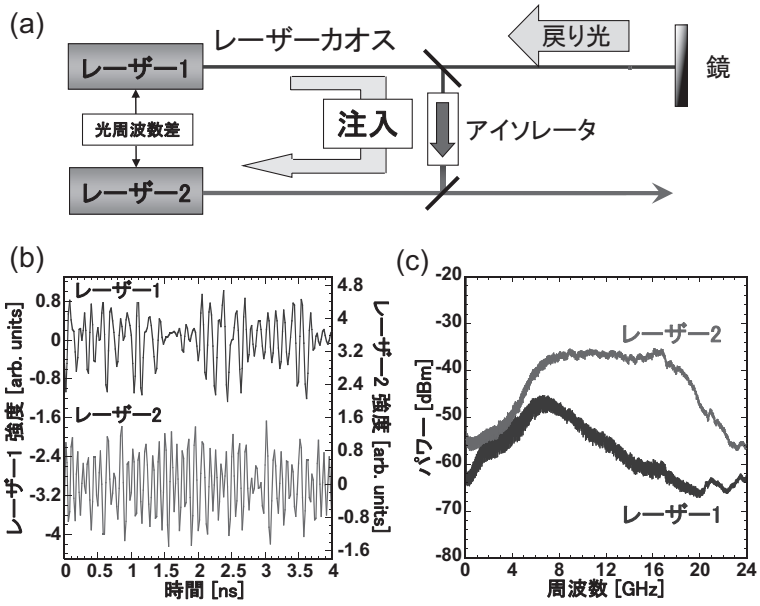

図2　前処理部における帯域拡大カオスの発生方法．(a) 構成図，(b) 半導体レーザー1と2の時間波形，(c) 半導体レーザー1と2のRFスペクトル．

ズのような連続スペクトルに近いほど，ビット列の統計的な偏りは少なくなる．後処理は決定論的なディジタル処理であるため原理的な確率性を増加させないが，統計的な偏りを減少させることは可能であり，ビット列の統計的な解析のみから純粋な乱数との区別は難しくなるといえる．

多くの研究において前処理や後処理の高速化および小型化が達成されており，以下にその方式について述べる．

1.2　高　速　化

乱数生成速度の向上のために，前処理および後処理において高速化が達成されている．前処理での高速化の一例として，一方向結合された半導体レーザーによる帯域拡大カオスの生成が挙げられる[4]．構成図を図2 (a) に示す．2つの分布帰還型半導体レーザー（波長1548 nm）を用意し，それぞれレーザー1およびレーザー2とよぶ．レーザー1に外部鏡を設け，戻り光を付加してカオスを発生させる．レーザー1のカオス光を一方向にレーザー2に注入し，2つのレーザーの光周波数差を10〜20 GHzの範囲で固定する．このとき，光周波数差に対応する変調成分がレーザー2の出力に出現し，レーザー2の緩和発振周波数と非線形相互作用することにより，レーザー2の出力が帯域拡大されたカオスとなる．このときのレーザー1で発生させたカオスと，光注入により帯域が拡大されたレーザー2のカオスの時間波形とRF (radio frequency) スペクトルを図2 (b) および2 (c) に示す．レーザー1, 2の出力時間波形はともにカオス的な振動であるが，レーザー2の振動のほうがレーザー1よりも高速であることがわかる．また，RFスペクトルを比較すると，9.5 GHzから16.1 GHzに周波数帯域が拡大されている（ここで周波数帯域とは，DC成分から全パワーの80% を含む最大周波数と定義）．また，レーザー1のRFスペクトルと比較して，レーザー2のRFスペクトルはピークの高低差が小さく，平坦なスペクトルとなっている．このような平坦なRFスペクトルは，物理乱数生成に適しているといえる．

図3　乱数生成用後処理の一例（ビット列逆順方式）．

さらに，後処理による高速化手法の一例を図3に示す[5]．本手法は大きく3つのステップに分けられる．はじめに，カオス信号とその時間遅延信号の2つの信号を2チャネルのオシロスコープを用いて，8ビット振幅量子化

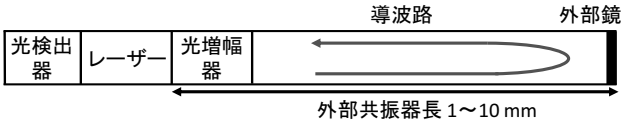

図 4　乱数源のための戻り光を有する半導体レーザーの光集積回路の構成図.

によりサンプリングする．ここで，それぞれの信号を Ch1, Ch2 とよぶことにする．次に，時間遅延された信号（Ch2）に対して，サンプリング点ごとにビット列を最上位ビットが最下位ビットになるように逆順に並べ替える（図 3 のステップ 2 参照）．ここで 8 ビットを逆順に並べ替えた遅延信号を $Ch2^R$ とよぶ．さらに，Ch1 と $Ch2^R$ に対してサンプリング点ごとに排他的論理和演算（同じビットなら 0，異なるビットなら 1 に変換）を行い，得られたビット列を上位ビットから乱数として出力する．レーザーカオス波形の出現頻度（確率分布）は正規分布から多少歪んでいるために，AD 変換された 8 ビットのうち，上位ビットの 1 の出現確率が下位ビットよりも高いことが知られている．そのため，本処理を加えることにより，最終的に生成される乱数のランダム性が改善される[5]．従来提案されている多くの乱数生成方式では，逆順に並べ替えずに 8 ビット乱数列の下位ビットを切り出すという処理を行っているが，その場合，捨てた上位ビットの分だけ乱数生成速度が低下する[4]．一方で提案手法では 8 ビットすべてを乱数として使用することが可能であり，有用な後処理方式といえる．本方式を用いてこれまでに 400 Gb/s（＝ 8 ビット×50 Giga-Sample/s）の生成速度での乱数生成に成功している[5]．

1.3　小　型　化

物理乱数生成器の小型化のため，ランダム信号生成用の光集積回路がこれまでに開発されている[6–8]．その概念図を図 4 に示す．光集積回路は，光検出器，分布帰還型半導体レーザー，光増幅器，導波路，外部鏡から構成される．レーザーから発振した光が導波路を通り外部鏡で反射され，戻り光として再びレーザーに注入されることによりカオスが発生する．このとき，光増幅器への注入電流を変化させると戻り光量が変化する．レーザー端面から外部鏡までの距離は 1〜10 mm の範囲で固定されており，これが外部共振器長に対応する．レーザーへの注入電流と戻り光量を変化させると時間ダイナミクスが変化するため，これらのパラメーター値を調整してカオス状態を探索する．

前処理としての光集積回路の効果を示すために，1 ビット AD 変換と排他的論理和演算方式を用いてできるだけ簡潔な後処理を行い，乱数生成を行った．レーザーカオス波形とその時間遅延波形を同時刻にサンプリングし，閾値を設けて 1 ビット AD 変換を行った．ここで時間遅延は，追加した 1 m の同軸ケーブル 1 本分に対応する 4.6 ns と設定した．1 ビット AD 変換により得られたビットに対して，排他的論理和演算を行うことで乱数を生成した．その結果，外部共振器長が 4 mm の光集積回路において，最大生成速度が 5.56 Gb/s での乱数生成に成功している[8]．

2.　レーザー同期による相関乱数列生成と秘密鍵配送

2.1　秘密鍵配送方式

本節では，2 人のユーザーに対し，相関乱数列を利用して秘密鍵を配送する方法について述べる．文献 18 で提案されている秘密鍵配送システムの構成図を図 5 に示す．2 人の正規ユーザーを Alice, Bob とし，Alice と Bob は同一の光学的スクランブラー（例えば光散乱物質やカオス生成用レーザーなど）を有しているとする．スクランブラーの構造自体に秘密はなく，かつ，盗聴者 Eve も同一のスクランブラーを入手可能であると仮定する．スクランブラーは可変パラメーター v を備えるとする（例えばレーザーの注入

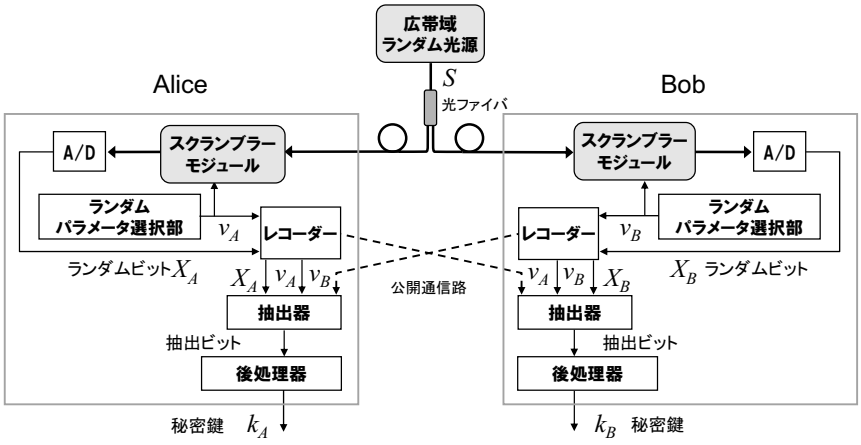

図 5　相関乱数秘密鍵配送方式の説明図.

電流や光位相など)．一般には，v は複数のパラメーターからなるパラメーターベクトルである．パラメーター v は，離散的で異なる M 個の値のいずれかを取るものとする．広帯域ランダム光源では光 S が生成され，S は光ファイバーを介して各ユーザーに配信される．Alice と Bob はそれぞれ，独立かつランダムに選択された値 v_A, v_B にスクランブラーのパラメーター値を設定し，配信された光 S をおのおののスクランブラーに注入する．スクランブラーは，注入光 S とパラメーター値 v に依存した出力光を生成する．ここで，スクランブラーは次のような入出力特性を備えていると仮定する．

(1) 2 個のスクランブラーに同一の広帯域ランダム光が注入されるとき，それらのパラメーター値 v, v' が一致している場合には各スクランブラーからの出力光強度の波形は一致する

(2) パラメーター値が不一致の場合には，出力光強度の波形は無相関となる

Alice と Bob は，それぞれ，スクランブラーの出力光強度を同時にサンプルし，その値を AD 変換器で二値化してビット X_A, X_B を生成する．Alice と Bob は，それぞれのレコーダーに，パラメーター値と生成されたビットの組 (v_A, X_A), (v_B, X_B) を保存する．以上が 1 回のビット生成操作の手順である．

非再帰的な時間変動をする広帯域ランダム光 S が，連続的に配信される状況を想定する．Alice と Bob は，毎回，ランダムかつ独立にパラメーター値を選択し，スクランブラーに S を注入した後，出力光を同時にサンプリングしてビットを生成する．この操作を多数回繰り返すことにより，パラメーター値と生成ビットの組 $(v_{A,i}, X_{A,i})$, $(v_{B,i}, X_{B,i})$, $i = 1, 2, \cdots, n$ を生成しレコーダーに保存する．$\{X_{A,i}\}$ と $\{X_{B,i}\}$ が相関乱数列である．

Alice と Bob は，彼等が生成したビット列から以下の手順により互いに一致している部分を抽出する．まず，公開通信路を介して，彼等がビット生成に利用したパラメーター値 $\{v_{A,i}\}$, $\{v_{B,i}\}$, $i = 1, 2, \cdots, n$ の情報を交換する（図 5 の破線）．次にパラメーター値が一致する，すなわち $v_{A,i} = v_{B,i}$ である番号 i に対するビット $X_{A,i}$, $X_{B,i}$ のみを保持し，他の生成ビットを破棄する．先に仮定したスクランブラー入出力特性により，抽出操作後に保持されるビットは Alice と Bob の間で一致する．

最後に，保持されている共通ビット列に対し，後処理器において秘密増幅プロトコル（privacy amplification）[20] を施すことにより共通の秘密鍵 $k_A = k_B$ を生成する．一般には，盗聴者 Eve が，Alice と Bob が抽出操作後に保持する共通ビット列に関して，いくらかの情報を持っている可能性がある．秘密増幅プロトコルは，そのような状況下で，Eve が全く推定することができない秘密鍵 $k_A = k_B$，すなわち，それに関して Eve が持ちうる情報量がゼロであるような秘密鍵を生成するためのプロトコルである．

2.2 提案方式の安全性

提案方式の安全性に関する議論を行う．まず，盗聴者 Eve に関して以下を仮定する．

(a) Eve は正規ユーザーに配信されるものと全く同一の広帯域ランダム光 S を利用できる

(b) Eve は公開通信路を介して Alice と Bob が交換する情報をすべて知ることができる

(a) に関しては，例えば，多数のスクランブラーを用意して，それらに S を注入し出力光を調べるようなことが許される．一方で，S の波形を変化させる，または，公開通信路上の情報を改ざんするなどの能動的な攻撃は，ここでは考えないものとする．任意の受動的な攻撃に対し，Alice と Bob が抽出操作後に保持している共通ビット列を Eve が全く誤りなく完全に推定できない場合，そしてその場合に限り，Alice と Bob は Eve に対して完全に秘密の鍵を生成できることが数学的に証明されている[17]．したがって，安全性を確保するためには，物理的な制約を利用して，Eve による Alice と Bob の共通ビット列の完全推定が，事実上不可能になるようにすればよい．

以下の物理的制約が満たされるようにした場合，Eve による共通ビット列の完全推定を防ぐことができる．

(i) 共通ランダム光 S として，非常に帯域が広く，その位相と振幅のランダムな高速時間変動を現在の技術では完全には観測できない光を利用する．これにより，正規ユーザーと盗聴者を含めて，誰も S の時間変動を完全には観測・記録できないようにする．

(ii) Eve が同時に動作させることが可能なスクランブラーの最大数 M_E が $M_E < M$ となるように，パラメーターが取り得る値の総数 M を設定する．

Alice と Bob が公開通信路を介してパラメーターに関する情報を交換した後の時点で，Eve がランダム光 S を再現できる場合を想定する．この場合 Eve は，再現された S を，Alice, Bob が用いたパラメーター値に設定した 1 個のスクランブラーに入力して，その出力値より Alice, Bob のビット値を知ることができてしまう．(i) により，この可能性を排除することができる．よって，Eve が，互いに異なるパラメーター値に設定された M_E 個 ($M_E < M$) のスクランブラーを用意し，Alice, Bob がビット生成を行うのと同じ時点でそれらにランダム光 S を注入し，出力光およ

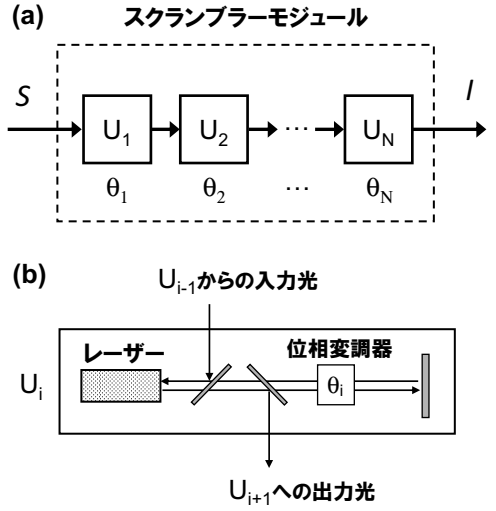

図6　スクランブラーの実装法．(a) 一方向結合ユニットによるモジュール構成，(b) 戻り光位相 θ_i を制御する位相変調器を備える半導体レーザーによるユニット構成．

び生成ビットを観測・記録する状況を考える．(ii) により，ランダム光 S が配信された時点で，M 通りのすべての可能なパラメーター値に対する出力光および生成ビットを観測・記録することはできない．したがって，Alice と Bob のパラメーター値が偶然一致し，一方で，その値が Eve が用いた M_E 個のパラメーター値に含まれないような場合が，必然的にゼロでない確率で生じる．このような Alice と Bob のパラメーター値が一致し，かつ，Eve のパラメーター値は異なる場合に，Alice と Bob が共有する1ビットの情報に関して Eve が得られる情報量（もしくはその上界値）を I_E で表す．特性 (2) により，Eve のスクランブラーからの出力光波形は Alice, Bob のそれとは無相関であるため，$I_E < 1$ と期待される（理想的には $I_E = 0$）．

鍵生成レート R は，最終的に秘密鍵 k_A, k_B として得られるビット数の最初に生成するビット数 n に対する比として定義される．提案方式の鍵生成レートは次式で与えられる[18]．

$$R = \frac{1}{M}\left(1-\frac{M_E}{M}\right)\cdot(1-I_E) \qquad (1)$$

ここで，$1/M$ は Alice と Bob のパラメーター値が一致する確率であり，$1-M_E/M$ はその値が Eve の用いる M_E 個のパラメーター値に含まれない確率である．Alice と Bob は，少なくともレート R までは，安全な秘密鍵を生成できることが保証される．理想的には $I_E = 0$ であるが，実際には，スクランブラーの入出力特性の不完全性等の理由により，$I_E > 0$ の場合が起こりうる．式 (2) は，そのような場合でも $I_E < 1$ である限り，すなわち，Eve が Alice と Bob の共有ビットを“完全”に推定できない限り，生成レート R は減少するものの依然 $R > 0$ であり，安全な鍵生成が可能であることを示している．これは，提案方式の重要な特性である．

2.3　半導体レーザーカオスの同期現象を用いた実装法と実験結果

図6 (a) はスクランブラーモジュールの構成図である．1個のモジュールは，一方向結合された N 個の半導体レーザーで構成される（個々のレーザー装置をユニットとよぶ）．各ユニット U_i は可変パラメーター θ_i を備え，その組 $v = (\theta_1, \theta_2, \cdots, \theta_N)$ がスクランブラーモジュールの可変パラメーターを与える．各 θ_i は，0 または π のいずれかの値を取る．図6 (b) はユニットの構造を示している．各ユニットは，位相制御器を備えた外部共振器を有する半導体レーザーで構成される．位相制御器で戻り光に加えられる位相シフト量をパラメーター θ_i とする．モジュール内では，ユニット U_i の出力光がユニット U_{i+1} への入力光となるように結合される．したがって，ランダム光 S を注入した場合，すべての位相シフトパラメーター θ_i が最終的なモジュール出力光に影響を及ぼす．

2つの同一な戻り光半導体レーザーに共通ランダム光が注入される場合，それらの間に同期現象が生じることが近年明らかにされている[21,22]．上述のスクランブラー実装法は，この同期現象に基づいている．2つのスクランブラーモジュールに同じランダム光が注入される場合を考える．すべての対応するユニットのパラメーター θ_i が一致するとき，モジュール出力光波形は同期現象により一致する．一方，対応するユニット間で1つでもパラメーターの不一致があれば，不一致ユニットより下段では光信号が両モジュール間で異なってくるため出力光相関は小さくなる．

ユニット数 N を十分大きくすることで条件 (ii) を満たすことができる．パラメーター $v = (\theta_1, \theta_2, \cdots, \theta_N)$ が取りうる値の総数 M は，ユニット段数 N に関して指数関数的に増大する．各 θ_i の取り得る値は $0, \pi$ の2通りなので，$M = 2^N$ で与えられる．よって，ある程度大きな N に対しては事実上 $M_E < M$ が実現される．非常に大きな M_E を実現可能な強力な盗聴者を想定した場合には，それに応じた大きな M を設定することが必要である．式 (1) に従えば，その場合，R は非常に小さな値となる．したがって，実用的な鍵生成レートを得るためには，抽出操作前の実時間ビット生成レートとして大きな値を達成する必要がある．半導体レーザーは応答速度が速いことが特徴であり，前節で述べたように，半導体レーザーを用いた非常に高速なランダムビット生成が実験的に実証されている．この点より，半導体レーザーによるスクランブラー実装は有望と

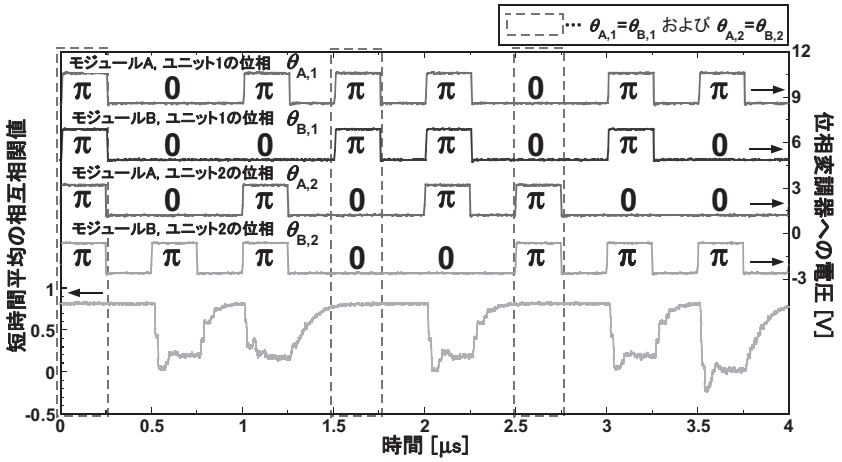

図7　実験結果．ランダム変調された各レーザーユニット戻り光位相の時系列（RZ format），およびモジュールA, Bの出力光強度波形の短時間平均の相互相関値（最下段の時系列）．戻り光位相が一致（$\theta_{A,1}=\theta_{B,1}$および$\theta_{A,2}=\theta_{B,2}$）した時間フレームを破線で囲んである．

思われる．

秘密鍵配送の実現可能性を示すために行った実証実験を紹介する[19]．最小限のモジュール構成として2段レーザー系（$N=2$）を用いた．共通ランダム光は，一定出力の分布帰還型半導体レーザー光（波長1548 nm）にランダム位相変調（帯域約1.5 GHz）を加えて生成し，それを光源から各モジュールへ60 kmの光ファイバー，およびファイバー増幅器を介して配信した．つまりAliceとBobの間の距離は120 kmである．Alice, Bobのモジュールをそれぞれ A, Bで表し，ユニットを1, 2で番号付ける．図7は，2つのモジュール出力光の短時間平均を取った相関値の時間に対するグラフである．各ユニットの位相変調パラメーター（0またはπ）は，2 MHzでランダム変調した．それらのグラフも併せて示してある．図7の結果より，対応するパラメーターが1, 2段目ユニットともに一致するとき（$\theta_{A,1}=\theta_{B,1}$および$\theta_{A,2}=\theta_{B,2}$）出力相関が高く，それ以外の場合に相関が小さいことがわかる．すなわち，前述の特性（1），（2）が実現されていることが確認できる．実験で得られたモジュール出力光を二値化して相関ビット列を生成した場合，$M=2^2=4$，$M_E=2$に対して鍵生成レート$R=0.032$が得られた[19]．ランダム変調周波数2 MHzを考慮すると，最終的な鍵生成レートは64 kb/s（$=2\ \text{MHz}\times 0.032$）となった[19]．この実験結果は，相関乱数秘密鍵配送方式が原理的に実現可能であり，有望な方式であることを示している．

本稿では，半導体レーザーカオスを用いた超高速物理乱数生成および相関乱数秘密鍵配送方式について概説した．前半では，物理乱数生成器の高速化手法や，光集積回路を用いた物理乱数生成器の小型化について述べた．また後半では，半導体レーザーの同期現象を利用した情報理論的に安全な秘密鍵配送方式について概説した．このように，半導体レーザーにおけるランダム現象には，超高速物理乱数生成器や新たな情報セキュリティー技術への応用や技術革新が期待できる．

文　　献

1）田村義保，小野寺徹，中畑昌也，清水隆邦：“日本における物理乱数発生装置の現状”，日本統計学会誌，**35**（2006）201–212.
2）A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura and P. Davis: “Fast physical random bit generation with chaotic semiconductor lasers,” Nat. Photonics, **2**（2008）728–732.
3）I. Reidler, Y. Aviad, M. Rosenbluh and I. Kanter: “Ultrahigh-speed random number generation based on a chaotic semiconductor laser,” Phys. Rev. Lett., **103**（2009）024102.
4）K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama and P. Davis: “Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers,” Opt. Express, **18**（2010）5512–5524.
5）Y. Akizawa, T. Yamazaki, A. Uchida, T. Harayama, S. Sunada, K. Arai, K. Yoshimura and P. Davis: “Fast random number generation with bandwidth-enhanced chaotic semiconductor lasers at 8×50 Gb/s,” IEEE Photon. Technol. Lett., **24**（2012）1042–1044.
6）A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris and D. Syvridis: “Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit,” Opt. Express, **18**（2010）18763–18768.
7）T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki and A. Uchida: “Fast nondeterministic random-bit generation using on-chip chaos lasers,” Phys. Rev. A, **83**（2011）031803（R）.
8）R. Takahashi, Y. Akizawa, T. Yamazaki, A. Uchida, T. Harayama, K. Tsuzuki, S. Sunada, K. Yoshimura, K. Arai and P. Davis: “Random number generation with a photonic integrated

circuit for fast chaos generation," *Proc. of 2012 International Symposium on Nonlinear Theory and Its Applications (NOLTA)*, 1 (2012) pp. 138–141.
9) 内田淳史："光のランダム現象を応用した超高速物理乱数生成器の研究開発の最新動向"，レーザー研究，**39** (2011) 508–514.
10) 内田淳史："セキュリティネットワークを支える物理乱数生成技術［Ⅲ］—レーザーカオスを用いた超高速物理乱数生成器の最新動向—"，電子情報通信学会誌，**95** (2012) 74–80.
11) A. Uchida: *Optical Communication with Chaotic Lasers: Applications of Nonlinear Dynamics and Synchronization* (Wiley-VCH, Weinheim, 2012) pp. 445–509.
12) J. Ohtsubo: *Semiconductor Lasers: Stability, Instability and Chaos,* 3rd ed. (Springer, Berlin, 2013) pp. 509–535.
13) C. H. Bennett and G. Brassard: "Quantum cryptography: Public key distribution and coin tossing," *Proc. of the IEEE International Conference on Computers, Systems & Signal Processing* (Institute of Electrical and Electronics Engineers, Bangalore, India, 1984) pp. 175–179.
14) J. Scheuer and A. Yariv: "Giant Fiber Lasers: A new paradigm for secure key distribution," Phys. Rev. Lett., **97** (2006) 140502.
15) R. Vicente, C. R. Mirasso and I. Fischer: "Simultaneous bidirectional message transmission in a chaos-based communication scheme," Opt. Lett., **32** (2007) 403–405.
16) U. M. Maurer: "Secret key agreement by public discussion from common information," IEEE Trans. Inf. Theory, **IT-39** (1993) 733–742.
17) J. Muramatsu, K. Yoshimura and P. Davis: "Information theoretic security based on bounded observability," Lect. Notes Comput. Sci., **5973** (2010) 128–139.
18) K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida and A. Uchida: "Secure key distribution using correlated randomness in lasers driven by common random light," Phys. Rev. Lett., **108** (2012) 070602.
19) H. Koizumi, S. Morikatsu, H. Aida, T. Nozawa, I. Kakesu, A. Uchida, K. Yoshimura, J. Muramatsu and P. Davis: "Information-theoretic secure key distribution based on common random-signal induced synchronization in unidirectionally-coupled cascades of semiconductor lasers," Opt. Express, **21** (2013) 17869–17893.
20) C. H. Bennett, G. Brassard, C. Crepeau and U. M. Maurer: "Generalized privacy amplification," IEEE Trans. Inf. Theory, **IT-41** (1995) 1915–1923.
21) I. Oowada, H. Ariizumi, M. Li, S. Yoshimori, A. Uchida, K. Yoshimura and P. Davis: "Synchronization by injection of common chaotic signal in semiconductor lasers with optical feedback," Opt. Express, **17** (2009) 10025–10034.
22) H. Aida, M. Arahata, H. Okumura, H. Koizumi, A. Uchida, K. Yoshimura, J. Muramatsu and P. Davis: "Experiment on synchronization of semiconductor lasers by common injection of constant-amplitude random-phase light," Opt. Express, **20** (2012) 11813–11829.

(2013 年 12 月 10 日受理)