偏りのない全光学式乱数生成器

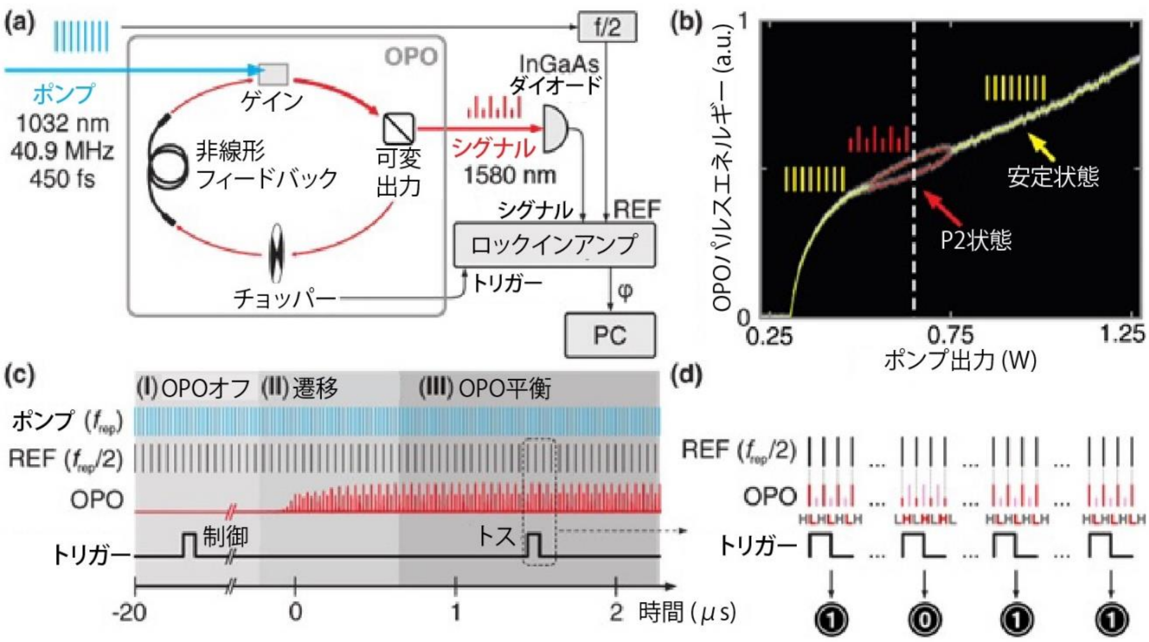
Tobias Steinle,[1,2,†] Johannes N. Greiner,[2,3] Jörg Wrachtrup,[2,3,4] Harald Giessen,[1,2] and Ilja Gerhardt[2,3,4,*]
[1]University of Stuttgart, 4th Physics Institute and Research Center SCoPE, Pfaffenwaldring 57, 70569 Stuttgart, Germany
[2]Center for Integrated Quantum Science and Technology, IQST, Pfaffenwaldring 57, 70569 Stuttgart, Germany
[3]University of Stuttgart, 3rd Physics Institute and Research Center SCoPE, Pfaffenwaldring 57, 70569 Stuttgart, Germany
[4]Max Planck Institute for Solid State Research, Heisenbergstraße 1, 70569 Stuttgart, Germany
(Received 13 June 2017; revised manuscript received 8 August 2017; published 30 November 2017)

ランダムビットの生成は、現代の情報科学において非常に重要です。暗号セキュリティは、生成に物理的なプロセスを必要とする乱数に基づいています。これは通常、ハードウェア乱数生成器によって実行されます。これらは、実験バイアス、システム内のメモリ、およびその他の技術的な微妙な問題など、エントロピー推定の信頼性を低下させる多くの問題を引き起こすことがよくあります。さらに、生成された結果は、そのような偽の効果を「解決」するために後処理する必要があります。ここでは、光パラメトリック発振器の双安定出力に基づく、純粋に光学的なランダム性生成器を紹介します。検出器のノイズは役割を果たさず、後処理は最小限に抑えられます。双安定状態に入ると、最初に結果として生じる出力位相は真空変動に依存します。その後、位相は厳密にロックされ、ポンプレーザーから得られるパルス列に対して適切に決定できます。これにより、あいまいさのない出力が得られ、確実に検出され、バイナリ結果に関連付けられます。結果として生じるランダムビットストリームは、完全なコイントスに似ており、関連するすべてのランダム性基準を満たします。生成されたバイナリ結果のランダムな性質は、結果として得られる条件付きエントロピーの分析によってさらに確認されます。

DOI: 10.1103/PhysRevX.7.041050 Subject Areas: Optics

* Corresponding author.
i.gerhardt@fkf.mpg.de

† Present address: ICFO—Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain.



I. 導入

ギャンブルや統計に興味がない人でも、乱数は日常生活で非常に重要です[1]。乱数の最も重要な用途は強力な暗号化であり、現代の通信、送金、機密情報の保管を保護しています。暗号化されたデータのロックを解除するために使用される暗号化キーは、離散対数問題や素因数分解などの数学的に難しい問題によって保護されています。基礎となるキーは乱数に基づいています。最近示されたように、現代の暗号化に対する最も効率的な攻撃ベクトルの 1 つは弱い乱数の提供であり[2,3]、キー空間を数学的確率のほんの一部にまで削減します。N ビットの現代の暗号化キーを想定すると、キー空間は 2^N の可能性になります。N が大きいと、ブルートフォース復号化プロセスに長い時間がかかります。このようなキーが乱数ジェネレーターの $n \ll N$ の可能な結果のみに基づいている場合、データの復号化は数秒の問題になる可能性があります。

コンピュータ時代において、最初に思い浮かぶアイデアは、コンピュータベースの乱数生成器です。残念ながら、このような生成器は一般的に再帰関係に基づいて定義され、一見ランダムなビットの（部分的に非常に長い）サイクルしか生成できません[4,5]。そのため、ハードウェアベースの乱数生成器が過去に提案されました。初期のハードウェア乱数生成器はサイコロ[1]または単にコインでした[6]。どちらの生成器も、科学者以外の人々にもよく知られています。数学的に言えば、コイン投げは、少なくともコインが端に落ちない場合は、サンプル空間 $\Omega=\{\mathbf{0},\mathbf{1}\}$ のベルヌーイ試行です[7]。公平なコインは、バイアスを示さず、端に落ちることができず、メモリを持たず、確率 $p(\mathbf{0})=p(\mathbf{1})=1/2$ を示すモデルシステムとして定義されます。このシステムは文献で十分に説明されています[6,8–10]。いくつかの要件を満たす必要がある古典的な乱数ビット生成器[11]に加えて、最近では量子効果の本質的に予測不可能な性質を利用して乱数を生成する量子乱数生成器が開発されています[12–19]。

将来のアプリケーションでは、速度、漏れ、熱の発生、配線の点で光子が実用的な利点を持つため、電気回路は最終的に完全に光デバイスのみに置き換えられる可能性があります。そのため、ランダムプロセスが特定の検出器の実装に依存しない「全光」ランダム性生成を紹介します。具体的な例としては、光パラメトリック発振器(OPO)、縮退発振器があり、以前このタスクに使用されていました[20–22]。2 つのジェネレーターの相対位相により、2 つの状態の結果が生成されますが、2 つの位相安定化 OPO などの実験的な取り組みが必要です。文献で概説されているように、OPO の出力位相は量子プロセスに基づいており、これは別の形式の量子ランダム性生成を表しています[22–28]。OPO による乱数生成には、光ジェネレーターの速度、等エネルギー双安定性、および復調器ベースのあいまいさのない測定原理など、いくつかの利点があります。「曖昧さのない」とは、測定装置の技術的な問題により混同されることのない、2 つ（またはそれ以上）の明確な結果を持つ測定を指します。単一光子検出器による量子ランダム性生成では、デッドタイム、電気的ジッタ、検出効率の変動などにより、このような曖昧さが発生する可能性があります[29]。

ここでは、ランダム性生成のために周期倍加光パラメトリック発振器に実装された双安定構成の使用を紹介します。私たちの知る限り、これは現在までに文献で報告された OPO における周期-2(P2)状態の初めての実験的利用です。簡略化されたモデルを図 1 に示します。関係する双安定は等エネルギーかつ等確率です。可能な結果は 2 つだけであり、バイアスは観察されません。ランダム性生成には、バイナリ結果のストリームを直接使用でき、追加のバイアス除去やビット抽出は必要ありません。結果を、公平なコイントスの予測結果と比較してテストします。論文の最後では、ジェネレーターから生成されるビットの有限サンプルのサイズに対する最も保守的な境界である最小エントロピーを計算します。

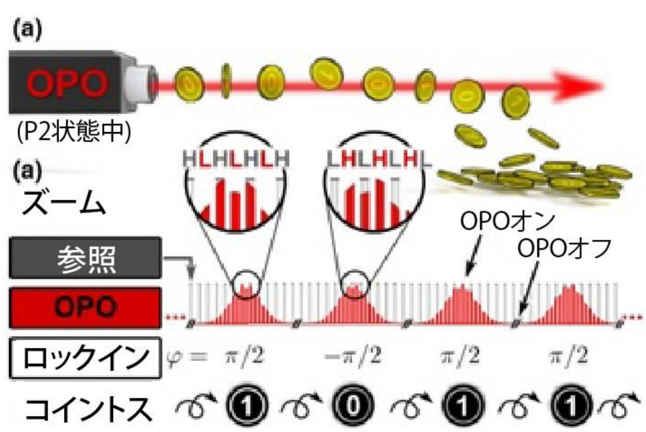


図 1.全光ランダム性発生器の動作原理。(a)光パラメータ発振器(OPO)の出力は、2 つの異なる出力状態を明確に生成します。両方の出力は等エネルギーかつ等確率で、OPO の過渡振動に基づいています。コイントスに匹敵する出力ビットに結果を関連付けます。(b)検出は、ポンプレーザーによって供給される外部基準クロックに対する位相測定(φ)によって実行されます。H と L は、周期-2 状態(P2 と名付けられる)で動作する OPO の異なるパルスエネルギー出力を示します。

II. 実験計画

自作のファイバーフィードバック OPO[30,31]は、モードロックされた 450fs、1032nmYb:KGW 発振器によって励起されます[図 2(a)]。ゲイン要素は、周期分極反転リチウムニオブ酸結晶です。繰り返し率はレーザーによって定義され、40.9MHz になります。OPO キャビティの長さは、可動ミラーによってこれと一致します。OPO キャビティの一部はシングルモードフィードバックファイバーで構成されており、可変出力カプラーと組み合わせることで、有効なキャビティ内非線形性を制御できます。出力信号は、逆バイアスされた InGaAs フォトダイオード(浜松ホトニクス)で検出されます。信号は、オシロスコープでリアルタイムに監視されます[図 2(c)]。または、信号をロックインアンプに送り、さらに分析します。

ポンプパワーが変化すると、OPO は周期倍増として識別できるバイモーダルな動作を示します[32–36]。発振閾値を超えると、OPO は定常状態で動作し[図 2(b)の黄色のトレース]、モード同期レーザーで知られているように、出力パルス列とそれに続く同じパルスが生成されます。ポンプパワーをさらに増加させると、システムはいわゆる周期‒2 状態に入り、異なるパルスエネルギー、ピークパワー、およびスペクトル特性を持つ交互パルスを出力します。この動作は、スペクトル選択ゲインと非線形フィードバックの相互作用に起因します[37]。OPO の同期ポンピングの結果、これらのパルスはポンプ周波数と時間的に揃います。

ポンプ周波数(この場合は 40.9MHz)が電子的に 2 で割られると、P2 状態のパルス列は、この派生した参照信号に対して定義された位相を持ちます。OPO がオンになると、この位相は同位相になるか、50%の確率で位相がずれます。この位相差 π は、さまざまな復調技術を使用して明確に測定できます。簡単で便利な方法は、検出された信号と参照の相対乗算です。簡単な市販のソリューションは、相対位相 φ に直接アクセスできるロックインアンプによる検出です。ここでは、Zurich Instruments のロックインアンプ(UHFLI)を使用します。位相を決定するための測定時間は 1μs です。

乱数生成では、OPO は光チョッパーによってオン/オフにされます。光チョッパーは、キャビティの振動を抑制できるように設置されています。図 2(c)は、ジェネレーターで 1 ビットを生成するシーケンスを示しています。測定信号(赤)は、ポンプレーザーの繰り返し周波数(f_{rep})の半分に相当する参照信号(REF)に対して測定されます。この測定は、1 つのチョッパーサイクルで 2 回実行されます。OPO がオフのときは制御信号として、OPO が P2 状態のときは実行中の発振器の信号として、つまり投げられて着地したコインとして測定されます。制御測定は、2 回の連続した測定で、ある結果から次の結果に誤った情報が伝わらないことを確認するために実行されます。オン状態での 4 回の連続した測定のシーケンスを図 2(d)に示します。H と L は、それぞれ P2 状態の OPO の 2 つの交互の高および低パルスエネルギー出力を示します。

測定結果は、MATLAB(Matlab,Inc.)スクリプトによって包括的なデータセットに保存され、測定されたすべての位相が保存されます。これらは、直接位相として分析することも、ビット結果として処理することもできます。

振動する OPO の測定位相は、本質的に 2 つの測定結果、すなわち−π/2 と π/2 を示します。単純なしきい値によって、測定値はバイナリ結果に選択されます。ゼロ位相を超える値は結果 **1** に関連付けられ、ゼロ未満の値には値 **0** が割り当てられます。同様に、これらの結果は、P2 状態の 2 つの可能な安定構成、L**H**L**H**…(0)または **H**L**H**L…(1)であり、順序はポンプ周波数の半分の基準信号によって固定されます[図 2(d)を参照]。上記の説明で、太字の文字は、OPO からのパルスが基準パルス列と一致していないことを示します。これは、図 1 または 2 の(赤色の)文字に対応します。測定結果はヒストグラムにプロットされ、推定値の周りに非常に狭い分布を示します[図 3(b)を参照]。

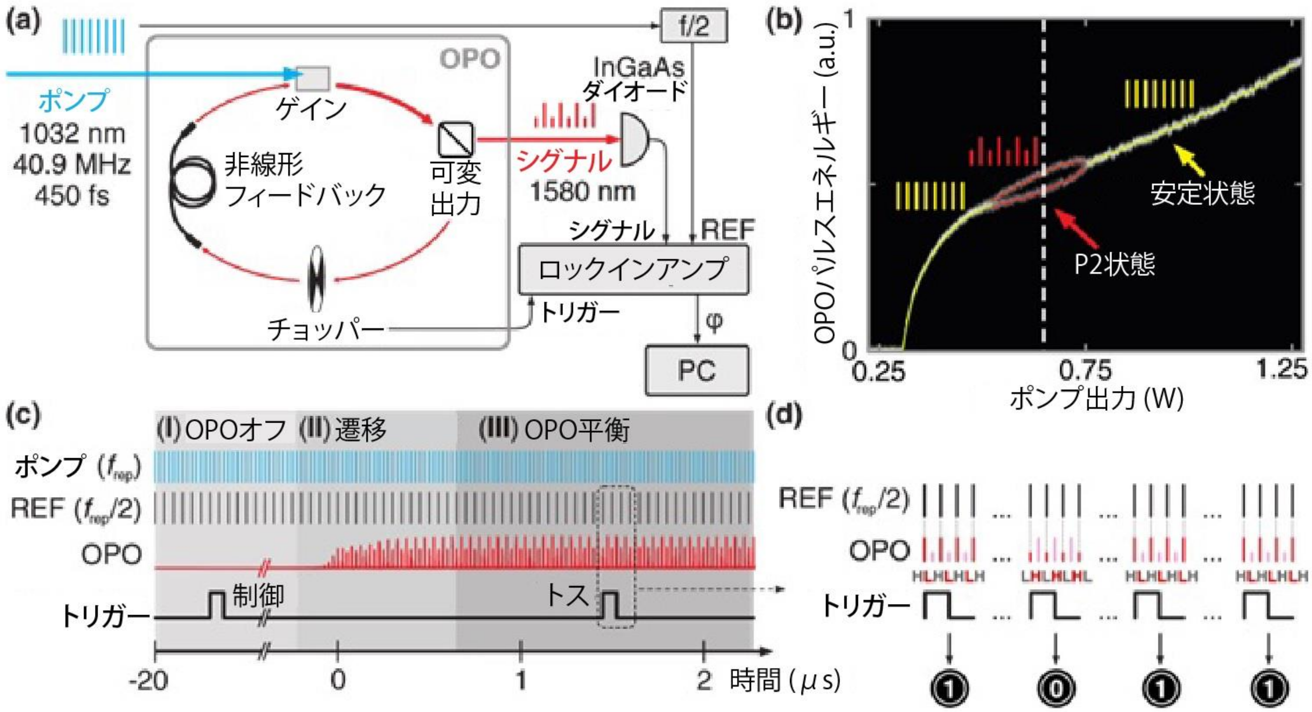


図 2.ランダム性生成の実験的スキーム。(a)光パラメトリック発振器の実験的実装。(b)出力依存の出力パルスエネルギー。2 つの異なる出力パルス列オプションは、等エネルギーであることに注意してください。(c)チョッパー周波数で周期的な測定遷移スキーム。トリガーパルスは、OPO がブロックされたとき(制御)と P2 状態に達したとき(トス)の 2 つの測定を定義します。基準周波数は 40.9MHz/2 で、ポンプレーザーと周波数分周器によって供給されます。(d)測定結果を最終ビットとして解釈します。

III. ランダム性の期限

文献では、OPO 始動時の過渡過程におけるランダム性要素が量子効果に由来することが確立されています。量子効果には、ゲイン要素の真空変動やキャビティ損失などが含まれます[22–28]。振動の蓄積における主要な量子過程は、非線形ゲイン結晶のポンピングによって引き起こされる自発的なダウンコンバージョン過程における単一光子の生成である[22,27,28]。これらの過程が P2 状態の形成にどの程度寄与するかは現在調査中です。ランダム性生成の文脈では、特に周期倍加アトラクターはカオスアトラクターではないことに注意することが重要です[38,39]。これは、補足資料[40]で詳細に説明されているように、周期倍加とカオスが 1 つの非線形システムで発生する可能性があるにもかかわらずです。

ポンプパワーの小さな変動に対する一次ランダム性プロセスの独立性は、重要な特徴です。この特殊性を証明するために、人工的に固定された追加のシードを使用して、過渡プロセスの数値パルス伝播シミュレーション(RPPhotonics の RPProPulse)を実行します。これにより、測定結果に π の位相変化を引き起こすには、±1%を超える相対強度変化が必要であることが示されます。ただし、10kHz から 20MHz まで積分された測定された相対強度ノイズ[41]は± 0.0215%であり、ランダム性生成の関連する要因としては約 50 倍低すぎます。

さらに、後続の測定結果の独立性も重要であり、これは以下の観測ビットで論じられています。したがって、追加実験ではビット間の待機時間が 1000 分の 1 に短縮されます。これは、OPO を拡張キャビティ構成で動作させて実行され、4 つの独立したパルスがキャビティ内で同時に振動します。後続の測定では、1 回のチョッパーサイクル内で 4 ビットが読み取られます。これにより、連続するビットの比較に関連する時間スケールが 100μs から 100ns に短縮され、機械的振動、チョッパージッター、熱効果、およびポンプ強度ノイズの影響が排除されます。ただし、上記の技術的効果のいずれかがランダム性を引き起こす場合は、交互のビットを測定しません(補足資料[40]を参照)。これらの調査は、量子効果がシステムにおけるランダム性の大きな原因であることを示しています。

このプロセスによって生成されるランダム性をさらに定量化するために、次のセクションでは、測定された位相とそのバイナリ表現を多数の結果に対して分析します。

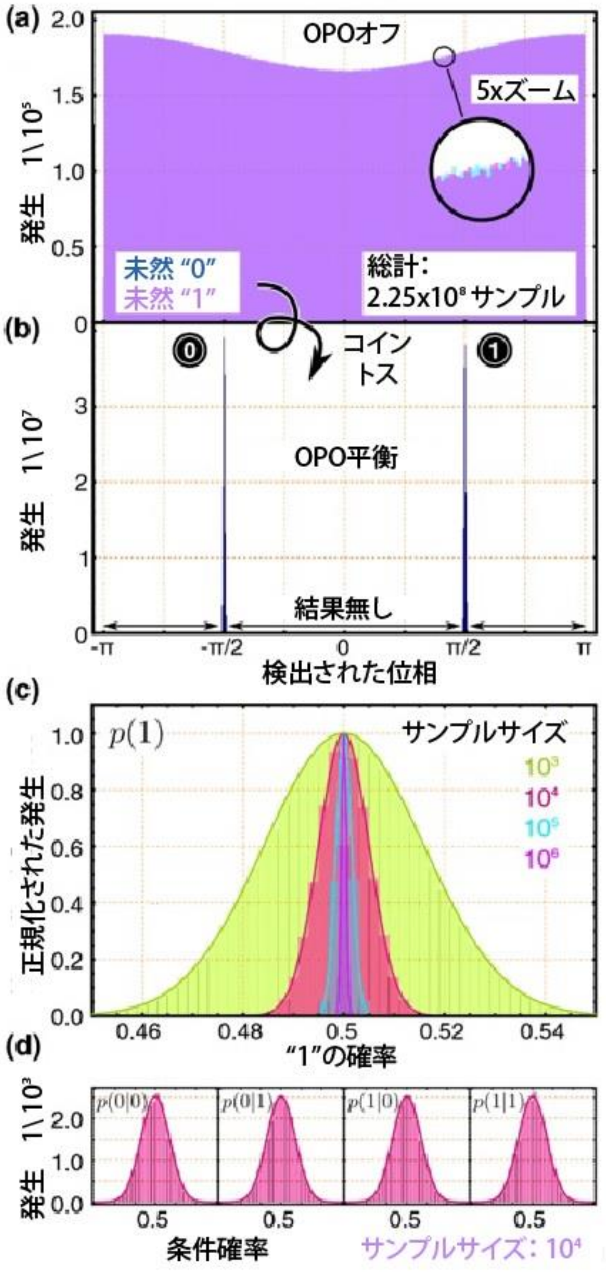


図 3.生のビットの分析。(a)OPO がオフのときの測定結果。基本的に、すべての異なる位相が小さなバイアスでランダムに測定されます。(b)OPO が P2 状態で平衡化された後の測定結果。(c)異なるサンプルサイズ N で結果として 1 が見つかる確率。実線は予測結果であり、近似ではないことに注意してください。(d)タプル結果のさまざまなオプションの条件付き確率。範囲は p_{cond}=0.47 から 0.53 です。これらの確率は、以下のエントロピー推定に関連する重要な数値です。上記すべての合計サンプルサイズは、2.25×10^8 測定です。

IV. 生のビットから最終ビットまで

取得したデータの最初の分析は、オフ状態の OPO の測定位相 φ に関するものです。図 3(a)は、実行中の OPO の各測定の直前のロックインの生の位相出力のヒストグラムを示しています。出力の数値は、それぞれ 0 または 1 が先行する結果に分割されています。明らかに、両方のデータセットは非常に類似しており、後続の結果に特に優先順位はありません。小さなバイアス(波状の曲線)は、ロックインアンプに到達するスプリアス信号に基づいており、両方の位相結果に対して対称的です。

過渡時間が経過した後、2 回目の測定で最終状態(OPO オン)が決定されます。前述のように、これはロックインアンプによって分析され、イベントのヒストグラムが生成されます。両方の可能な結果は、それぞれ-π/2 と π/2 を中心としています。それらの分布は、位相を測定するための実験的不確実性によって決定されます。これは、スプリアス位相情報、結晶内の自発的なダウンコンバージョン、サンプリングおよび測定時間、および信号内の残留(位相)ノイズによって生じます。決定された結果の幅(1σ)は 0.0023rad になります。言い換えると、2 つの結果が混同されている可能性を除いて、結果は 400 以上の標準偏差で分離されています。このようなあいまいさのない測定は、たとえばダークカウント[12、29、42]のために、光子カウントに基づくジェネレーターでは実現できません。

約 1 日の間に、$2\times2.25\times10^8$ 回の測定が行われます。ここで、たとえば技術的なノイズ[43]によって引き起こされる実験結果の偏りや不均衡の可能性を分析します。このノイズは追加の測定結果を生み出し、情報理論的には、ジェネレーターの過渡的プロセスにおけるランダム性につながります。分析では、ビットストリームを長さ N の部分文字列に分割し、結果 1 の実験的確率を決定します。分布は、サンプルサイズ N に関係なく、0.5 を中心としています。分析により、分布の幅が $\sigma_{\mathrm{single}}=\sqrt{Np(1-p)}/N$ として再確認されます。データはフィッティングされていませんが、理論曲線が測定データとともに描かれていることに注意してください。

測定結果のバランスは、コイントスがバランスが取れていることを示す一つの指標に過ぎません。もうひとつの重要な指標は条件付き確率で、これは後続の結果が発振器の以前の状態の何らかの記憶を含むかどうかを示します。これについては、図 3(a)と 3(b)の分析によって最初の指標が与えられますが、それでも平衡 OPO における後続の測定結果の独立性

を証明するものではありません。前の結果 **0** の後に結果 **1** を得る条件付き確率は $p(\mathbf{1}|\mathbf{0})$ と表され、ゼロを条件とする 1 の確率として読み取られます。これは p(x|y)=p(x∧y)/p(y)と定義され、その分布の理論的予測 $\sigma_{\mathrm{cond}}=1/\sqrt{2N}$ とともに図 3(c)に示されています。高次のビット間相関も考慮した自己相関分析は、補足資料[40]に記載されています。ここでも、予想される動作が再確認され、システム内にメモリがないことが明らかになりました。

いわゆる乱数テストの使用は非常に一般的です。テスト *ent*、*NIST* テストスイート[44]、*die-harder* スイート、または最も包括的な *TestU01* スイート[45]が一般的に知られています。多くの人々は、このようなテストがビット列がランダムかどうかを示すことができると今でも信じています。しかし、それらは、乱数ビットジェネレーターの実装に重大な欠陥が発生しなかったことを証明することしかできません。さらに、これらのテストのほとんどはアルゴリズム情報理論に基づいており、物理プロセスによって生成された乱数ではなく、アルゴリズムによって生成された疑似乱数をテストするように設計されています[46]。したがって、特定のビット列がすべてのテストに合格したという主張は、入力のランダム性を証明するものではありません。π の 2 進展開などの非ランダムで予測可能な数は、これらのテストをすべて完璧に合格します。予想どおり、提示したジェネレーターはすべてのセットテストに合格し、*NIST* スイートのサンプル出力は補足資料[40]に記載されています。

説明した乱数テストのサブセットは、異なるビットパターンとデータセット内でのそれらの出現の分析です。このアプローチは、乱数テストに関する初期の議論で検討されてきました[4]。今日では、他の著者は乱数テストに情報理論的言語を使用することを提案しています[46]。この文脈では、一般化 Fibonacci 数列[8]と密接に関連する Feller[6]によるコイン投げ定数は、公平なコインを n 回投げたシーケンスで長さ k が **1** または **0** のシーケンスが発生しないイベントの漸近確率 p(n, k)を記述します。Feller の定数には、次の特性があります。

$$\lim_{n\to\infty} p(n,k)\alpha_k^{n+1} = \beta k \tag{1}$$

表 I は、長さ N=400 ビットのジェネレーターの部分文字列の分析を示しています。この小さな数は、高次のパラメータ(k>5)に関連付けられた確率の値がゼロにならないように選択されています。実験的に決定された値は 3 番目の列に示されており、10^{-4} のオーダーの相対偏差は、記録されたビット 2.25×10^8 の平方根(ショットノイズ)に対応します。コイン投げ定数の計算値は、提供されたランダムビットシーケンスの想定される動作と非常によく一致しています。

表 I.フェラーのコイン投げ定数。定数は、ランダムビットセットで特定の 1 のシーケンスが発生しない確率に関連しています。ここで、サンプルサイズは N=400 です。コイン投げ定数 α の理想値は、実験データから抽出された値と比較されます。相対的な変化は、(α ideal－α extracted)/ α ideal として計算されます。相対的な不確実性は、取得されたデータセットの有限の長さによって決まります。

k	α_{ideal}	$\alpha_{\mathrm{extracted}}$	相対的変化
2	1.236 067 98		
3	1.087 378 03		
4	1.037 580 13	1.036 763 54	7.87010735×10^{-4}
5	1.017 320 78	1.017 314 06	6.61125775×10^{-6}
6	1.008 276 52	1.008 279 33	-2.78877013×10^{-6}
7	1.004 034 11	1.004 037 01	-2.88459780×10^{-6}
8	1.001 988 36	1.001 985 88	2.47363715×10^{-6}
9	1.000 986 24	1.000 985 84	4.01117501×10^{-7}
10	1.000 490 92	1.000 491 82	-8.99357769×10^{-7}
11	1.000 244 86	1.000 246 24	-1.38152744×10^{-6}
12	1.000 122 26	1.000 123 58	-1.31441456×10^{-6}
13	1.000 061 09	1.000 061 63	-5.40416736×10^{-7}
14	1.000 030 53	1.000 030 25	2.79986856×10^{-7}
15	1.000 015 26	1.000 015 22	4.33916550×10^{-8}

コイントス定数は条件付き確率よりも高次のタプルを解析するため、この点ではすべての可能なバイナリ文字列の辞書式出現を解析する数学的なボレル正規性テスト[4]に似ています。このようなテストは、Calude らによって、いくつかのハードウェアベースの乱数生成器をテストするために実装されました[47]。

後続の測定結果セットの確率に関する上記の分析は、理想的なコイントスの挙動を強調しています。各ビットをひとつの隣接ビットとペアにして測定結果を処理し、以前とは異なりタプルの重複を許可しないと、興味深い効果が発生します。すべてのタプル順列(**00**、**01**、**10**、**11**)が等確率であることがわかりましたが、2 つの同等の結果間の「距離」である待機時間は、ビット変更(**01**、**10**)とビット同等の結果(**00**、**11**)で異なります。ビット反転を含むタプルの場合、予測される待機時間は 4 回連続して投げる

ことです。一方、**00** または **11** のダブルシーケンスの場合、予測される待機時間は 6 回連続して投げることです。これは現在のデータセットで検証され、それぞれ 3.99976 と 5.99784 という値を決定します。繰り返しになりますが、約 10^{-4} の相対的不確実性はデータセットの長さに対応しており、測定結果にそれ以上のメモリストレージがないことが証明され、予測された動作が再確認されます。

要約すると、P2 状態のオン線形フィードバック OPO を使用した、提示された全光ランダム性ジェネレーターの測定された生のビットは、完全なベルヌーイ試行のものと測定可能な方法では違いがないという結論に達しました。これは、連続した測定結果の独立性、2 つの確率のバランス、および完全なコイントスの予想される結果に似たさらなるテストによって示されます。その後、必要な後処理を最小限に抑えることができます。このような後処理は、有限サイズ効果のため、公平な(完全な)コイントスの物理的な実装に一般的に必要になります。次に、生のビットストリームのエントロピー分析に移ります。

V. エントロピー推定

上記のすべての尺度は、生のビットが完全なランダムビットのソースとして使用できることを示唆していますが、これまでのところ、実験装置の出力に関する重要な情報理論的尺度である生成されたエントロピーを無視しています。以下に概説するように、ランダム性ジェネレーターにとって重要な品質の数値は、出力ビットあたりの達成可能なエントロピーです。理想的には、各ビットは完全な唯一のエントロピーを持ちます。つまり、生成された各ビットは独立した光学コイントスとして使用でき、公正なコインの出力に似ています。ただし、ビットの有限部分を分析する場合、すべての **1** と **0** が均等にバランスされている場合にのみ、これを証明できます。本質的に、望ましくない(ただし統計的に許容される)バイアスが存在する可能性があります。この場合、決定されたエントロピーは 1 未満になります。長さが有限であるため、提示されたデータセットの場合、これが当てはまる可能性が最も高くなります。エントロピーを計算する最初の単純なアプローチは、ビットストリームのバランスを分析し、次のように定義される無条件シャノンエントロピーによって与えられます。

$$H_{Sh} = \sum_y p(y) I(p(y)) = -\sum_y p(y) log2 p(y) \qquad (2)$$

ここで、p(y)は、それぞれ完全なビットシーケンスで **0** または **1** を取得する単一の確率です。ただし、これは測定結果の依存性やメモリ効果を考慮していません。たとえば、交互シーケンス **101010**…は、完全にランダムな、つまり完全に順序付けされていないシーケンスと同じエントロピーになります。したがって、条件付きエントロピーが考慮され、システム内のメモリ（またはその欠如）が説明されます。これは次のように定義されます。

$$H_{Sh}(X|Y) = \sum_y p(y) H_{Sh}(X|Y = y)$$

$$= -\sum_y p(y) \sum_x p(y) log2 p(x|y) (3)$$

条件付きエントロピーの計算の詳細については、補足資料[40]を参照してください。明確にするために、イベント y と x は「i 番目のビットが **0(1)**」および「$(i+1)$番目のビットが **0(1)**」と定義されます。大文字の Y と X は、すべてのビットのイベントの統一されたセットです。したがって、エントロピーの概念は、出力データの頻度分析に関連していますが、事前に推定することもできます。シャノンエントロピーとは異なり、最小エントロピー($H\infty$と表記)は、乱数ジェネレーターの使用可能なエントロピーの最も保守的な境界です。これは、x に対する(条件付き)確率 p(x|y)を最大化します。この不均衡と最大化効果は、図 3(c)と 3(d)に示されています。サンプルサイズ N が大きいほど、分布の幅が狭くなり、エントロピーの量が一般的に大きくなることがわかります。最小エントロピーは次のように定義されます。

$$H_{Sh}(X|Y) = -\log_2[\textstyle\sum_y p(y) max\{p(x|y)\}] \qquad (4)$$

上記のエントロピー定義は、実験的に生成されたデータセットに対して簡単に計算できます。この結果、スカラーエントロピー値が生成されますが、これは解釈する必要があります。優れたジェネレーターの場合、結果の数値は通常 1 に近くなります。エントロピーがどの程度「完璧」で、1 にどの程度近いかは、次の 3 つの要素によって決まります。(a)ジェネレーターの品質、(b)分析されたビットストリームのサイズ(ここでは分析されたビットの数を N と表記)、(c)どの特定のデータセットを分析するか。結論として、有限ビット文字列のエントロピーを計算すると

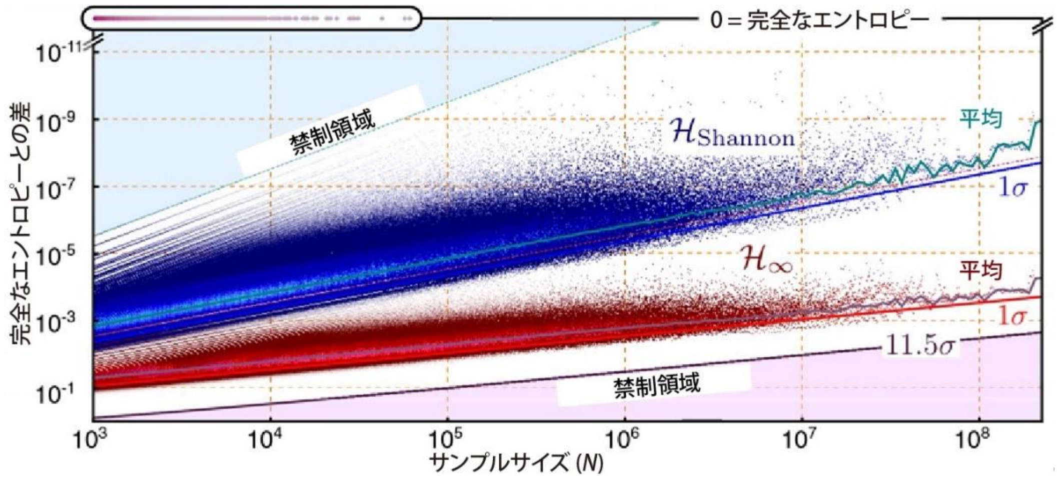


図 4.生成されたビットストリームの最終エントロピー。サンプルサイズ(N)に対するシャノンエントロピー(青)と最小エントロピー(赤)のエントロピー(H)の 1 に対する差を示します。実験データから得られた点の密度が高く色が明るいほど、特定の値の結果が多いことを意味します。最良のケースは、グラフ上部の対数スケールのカットオフ後に表示されるように、差が 0 になることです。$N<10^5$ の場合、この「完全な」エントロピーを持つシーケンスが引き続き観測され、個別の点として表示されます。特定の 1 つのビットが反転すると、エントロピーは 1 未満に減少します。その後、グラフ内で 1 のエントロピーを示さない点は、特定の制限(破線)を超えることはできません。これにより、数学的に可能な結果がない、上への禁制領域が形成されます。下部の実線は、保守的な境界を示します。これらの境界は、補足資料[40]で概説されているように、公平なコインのエントロピーの誤差伝播によって事前に得られます。赤：期待される最小エントロピーからの 1σ 偏差。紫：外れ値確率を 2^{-100} と仮定。予想どおり、この線より下の値は見つかりません。

きに、エントロピーが 1 になる可能性は非常に低いです。これは公平なコインにも当てはまります。以下では、ジェネレーターの結果を分析し、エントロピーが予測値と一致するかどうかを計算します。

図 4 は、サンプルサイズ N に対する提示されたデータセットの計算されたシャノンエントロピーと最小エントロピーを示しています。このグラフは、対数スケールで完全エントロピーに対する偏差を示していることに注意してください。サンプルサイズ N が小さい場合(左側)、サンプルの数が多くなり、表示されるポイントの数が多くなります。前述のように、サンプルサイズ N が大きいほど、エントロピーは 1 に近づきます。条件付きシャノンエントロピーはNに比例しますが、最小エントロピーは$\sqrt{N}$に比例します。最小エントロピーの値と分布は、条件付き確率が最大化されるため、シャノンエントロピーの場合よりも大幅に小さくなります。図 4 には、事前に取得されたエントロピー境界も示されています。これらには、完全エントロピーの理想的なケースに加えて、特定のサンプルサイズでのエントロピーの 2 番目に高い値が含まれます。これは、長さ N のデータセットに、エントロピーが最小限に変化する単一ビットフリップが存在する場合に発生する可能性がある最大値です。これらの曲線は、上で紹介した平均傾斜動作に対して 2 次的にスケールします。したがって、条件付きシャノンエントロピーの平均値は、1 ビットの反転が存在する最高の最小エントロピーと平行線を形成します。

最小エントロピーは保守的な境界であり、ランダムビットのセット内で最大の条件付き確率を選択します。完全なランダム文字列が無限に長い場合、すべての可能性のある発生がこのシーケンスのサブセットに表示されます。

すると、上記の説明とは矛盾して、一見ランダムでないビットの非常に長いシーケンス（たとえば、**1111111**…など）が発生する可能性があるため、計算されたエントロピーのセットは最終的に非常に小さくなります。これらのケースでは、計算されたエントロピーはゼロに削減される可能性があります。したがって、現実的な検討では、たとえば、長いシーケンスのすべてのビットが 1 であるような、非常に起こりそうなイベントを除外することが重要です。

ジェネレーターの特定の同等の結果セットの発生のこのような計算は、上記のコイントス定数の計算で示されています（表 I）。さらに、ランダム性抽出の可能性のある誤差境界は、Troyer と Renner によって[48]$1/2^{100} \approx 1/10^{30}$ として導入されました。このような境界は、「ϵ ランダム性」を保証するためにも説明されています[43]。提案された境界 $1/2^{100}$ は、宇宙の年齢において 1×10^6 個のジェネレーターが同じ結果(つまり、いわゆる 2 つのジェネレーターの衝突)を示す選択肢を持たないことを保証します。ガウス分布イ

ベントの場合、これは分布の中心から約 11.5 標準偏差に相当します。図4は、この境界を、補足資料[40]で概説されているように、公平なコインのエントロピーに関するエラー伝播によって事前に得られた最低の曲線として示しています。生のビット分析から示唆されるように、選択されたビットのサブセットはこの線を下回っていません。これは、導入されたジェネレーターには完全なコイントスのモデルが適切であると思われることを示唆しています。
提示したサンプルサイズ 2.25×10^{8} の場合、ビットあたりの条件付き最小エントロピーは 99.95%と推定できます。これは、右側の図 4 から簡単に読み取ることができます。もちろん、この値は有限のサンプルボリュームによってのみ制限されます。エントロピー差の 1 に対する最も保守的な境界(11.5σ)は約 1 桁異なり、エントロピーは 99.5%になります。

上で説明したように、生のビットだけでなく、計算されたエントロピーのメリットによって、記録されたビットストリームは、完全なコイン投げと測定可能な方法では変わらないことを証明できます。したがって、放出された各ビットはランダムビットとして使用できます。十分に大きなビット文字列を使用する場合、それ以上のランダム性の抽出を考慮する必要はありません。もちろん、この仮定は、記録されたビット文字列のサイズに制限されてのみ証明できます。

VI.結論と展望

我々は、偏りのない全光コイントスを紹介します。これは、P2 状態で動作する非線形ファイバーフィードバックを備えた光パラメトリック発振器の双安定結果に基づいています。検出方式は、外部参照パルスに対する位相検出に依存しています。この実装は、OPO の縮退動作を必要としないため、以前に公開された実験[20–22]よりも大幅に単純です。縮退動作の欠点は、信号およびアイドラー周波数コムの相対的な光位相をポンプ周波数コムに固定するために、アクティブ干渉安定化共振器、または安定化のためにエラー信号を生成するためにキャビティ長を定期的に変更する「ディザおよびロック」アルゴリズムを使用する「シェーカー」のいずれかが必要になることです。これにより、システムにノイズが導入されますが、これは非縮退動作によって回避できます。

周期倍増に基づく実装された検出方式は曖昧さがなく、つまり、ランダムビットシーケンスの 0 と 1 として解釈できる、400 以上の標準偏差で区切られた 2 つの結果のみを持ちます。これにより、基本的なランダム性プロセスが検出原理から独自に切り離されます。ここでの検出はロックインアンプに基づいていますが、より単純な方式を開発することもできます。復調器または無線周波数ミキサーとコンパレーターを使用すると、実装コストが削減され、ランダムシーケンスが、たとえばロジックレベル出力に直接出力されます。

1 つの制限はチョッパーのサンプルレートで、この設計では 10kHz に制限されています。このサンプルレートは、OPO が安定状態になるまでの過渡プロセスと位相検出に必要な時間によって最終的に制限されます。現在の検出システムでは、位相を決定するための測定時間は 1μs です。これは、将来の実験で 10 分の 1 に短縮される可能性があります。したがって、より高速なチョッパーをインストールすることもできます。図 2(c)から明らかなように、平衡化の時間はおよそ 300ns、位相状態のあいまいさのない検出は 2〜3 サイクル、つまり 100〜150ns と見積もられています。説明した OPO を使用し、より高速なチョッパーを導入することで、1MHz を超えるランダムビットレートを実現できます。ポンプレーザーの繰り返しレートを高くすることで、さらに高速化を実現できます。このような変更により、GHz 範囲に達する OPO が報告されています[49]。副作用として、実験構成全体の設計がはるかにコンパクトになります。さらに、導入された原理をフォトニックチップ上の最先端技術で実装することで、よりコンパクトな乱数発生器を構築できます[50–52]。

開放量子システム、特に P2 状態の完全な量子力学的記述は、今後の研究で取り組む必要があります。一般的に、OPO の双安定結果のプロセスは、量子力学的真空変動から生じる量子プロセス[22–28]として説明されます。過渡プロセスの注意深い分析（チョッパーの代わりに光ファイバー電気光学変調器を導入する可能性もあります）と、出力依存性に関するさらなる研究により、このプロセスと P2 状態がさらに詳細に特徴付けられる可能性があります。基礎となる物理をより深く理解することで、位相検出の高速化とランダムビットレートの高速化が可能になり、将来的には量子情報処理や量子シミュレーションへの実装にもつながる可能性があります[53]。

謝辞

図 1 の 3D レンダリングは Ingmar Jakobi 氏のサポートによるものです。T.S.は Carl Zeiss Foundation に感謝します。さらに、MPG、BW Stiftung、DFG、SFB Project No. CO. CO. MAT/TR21、ERC (Complexplas)、BMBF、Eisele Foundation、プロジェクト Q.COM、および SMel からの資金提供にも感謝

します。T.S.と J.N.G.は、この研究に同等の貢献をしました。

[1] F. Galton, Dice for Statistical Experiments, Nature (London) 42, 13 (1890).
[2] A. K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter, Ron Was Wrong, Whit Is Right, https://eprint.iacr.org/2012/064.
[3] G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, Stealthy Dopant-Level Hardware Trojans, in Cryptographic Hardware and Embedded Systems, edited by G. Bertoni and J. S. Coron, Lecture Notes in Computer Science Vol. 8086 (Springer, New York, 2013), pp. 197–214.
[4] D. Knuth, The Art of Computer Programming: Seminumerical Algorithms (Addison-Wesley, Reading, MA, 1998), Vol. 2.
[5] H. Bauke and S. Mertens, Pseudo Random Coins Show More Heads Than Tails, J. Stat. Phys. 114, 1149 (2004).
[6] W. Feller, An Introduction to Probability Theory and Its Applications, 3rd ed. (Wiley, New York, 1968).
[7] D. B. Murray and S. W. Teare, Probability of a Tossed Coin Landing on Edge, Phys. Rev. E 48, 2547 (1993).
[8] M. Finkelstein and R. Whitley, Fibonacci Numbers in Coin Tossing Sequences, Fibonacci Q. 16, 539 (1978). [9] J. Ford, How Random is a Coin Toss, Phys. Today 36 No. 4, 40 (1983).
[10] V. Z. Vulović and R. E. Prange, Randomness of a True Coin Toss, Phys. Rev. A 33, 576 (1986).
[11] M. Stipčević, Fast Nondeterministic Random Bit Generator Based on Weakly Correlated Physical Events, Rev. Sci. Instrum. 75, 4442 (2004).
[12] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, Optical Quantum Random Number Generator, J. Mod. Opt. 47, 595 (2000).
[13] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, A Fast and Compact Quantum Random Number Generator, Rev. Sci. Instrum. 71, 1675 (2000).
[14] M. Stipčević and B. M. Rogina, Quantum Random Number Generator Based on Photonic Emission in Semiconductors, Rev. Sci. Instrum. 78, 045104 (2007).
[15] H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, High Speed Optical Quantum Random Number Generation, Opt. Express 18, 13029 (2010).
[16] R. Colbeck, Quantum and Relativistic Protocols for Secure Multi-Party Computation, arXiv:0911.3814.
[17] S. Pironio, A. Acin, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random Numbers Certified by Bell's Theorem, Nature (London) 464, 1021 (2010).
[18] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Quantum Random Number Generation on a Mobile Phone, Phys. Rev. X 4, 031056 (2014).
[19] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, True Random Numbers from Amplified Quantum Vacuum, Opt. Express 19, 20665 (2011).
[20] A. Marandi, N. C. Leindecker, V. Pervak, R. L. Byer, and K. L. Vodopyanov, Coherence Properties of a Broadband Femtosecond Mid-IR Optical Parametric Oscillator Operating at Degeneracy, Opt. Express 20, 7255 (2012).
[21] Y. Okawachi, M. Yu, K. Luke, D. O. Carvalho, M. Lipson, and A. L. Gaeta, Quantum Random Number Generator Using a Microresonator-Based Kerr Oscillator, Opt. Lett. 41, 4194 (2016).
[22] A. Marandi, N. C. Leindecker, K. L. Vodopyanov, and R. L. Byer, All-Optical Quantum Random Bit Generation from Intrinsically Binary Phase of Parametric Oscillators, Opt. Express 20, 19322 (2012).
[23] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum Random Number Generators, Rev. Mod. Phys. 89, 015004 (2017).
[24] Z. Wang, A. Marandi, K. Wen, R. L. Byer, and Y. Yamamoto, Coherent Ising Machine Based on Degenerate Optical Parametric Oscillators, Phys. Rev. A 88, 063853 (2013).
[25] P. D. Drummond, K. Dechoum, and S. Chaturvedi, Critical Quantum Fluctuations in the Degenerate Parametric Oscillator, Phys. Rev. A 65, 033806 (2002).
[26] C. D. Nabors, S. T. Yang, T. Day, and R. L. Byer, Coherence Properties of a Doubly Resonant Monolithic Optical Parametric Oscillator, J. Opt. Soc. Am. B 7, 815 (1990).
[27] S. E. Harris, M. K. Oshman, and R. L. Byer, Observation of Tunable Optical Parametric Fluorescence, Phys. Rev. Lett. 18, 732 (1967).
[28] W. H. Louisell, A. Yariv, and A. E. Siegman, Quantum Fluctuations and Noise in Parametric Processes. I, Phys. Rev. 124, 1646 (1961).
[29] L. Oberreiter and I. Gerhardt, Light on a Beam Splitter: More Randomness with Single Photons, Laser Photonics Rev. 10, 108 (2016).
[30] T. Südmeyer, J. A. der Au, R. Paschotta, U. Keller, P. G. R. Smith, G. W. Ross, and D. C. Hanna, Femtosecond FiberFeedback Optical Parametric Oscillator, Opt. Lett. 26, 304 (2001).
[31] T. Steinle, F. Neubrech, A. Steinmann, X. Yin, and H. Giessen, Mid-Infrared Fourier-Transform Spectroscopy with a High-Brilliance Tunable Laser Source: Investigating Sample Areas Down to 5μm Diameter, Opt. Express 23, 11105 (2015).
[32] K. Ikeda, Multiple-Valued Stationary State and Its Instability of the Transmitted Light by a Ring Cavity System, Opt. Commun. 30, 257 (1979).
[33] L. Lugiato, C. Oldano, C. Fabre, E. Giacobino, and R. Horowicz, Bistability Self-Pulsing and Chaos in Optical Parametric Oscillators, Nuovo Cimento Soc. Ital. Fis. D10, 959 (1988).
[34] C. Richy, K. Petsas, E. Giacobino, C. Fabre, and L. Lugiato, Observation of Bistability and Delayed Bifurcation in a

Triply Resonant Optical Parametric Oscillator, J. Opt. Soc. Am. B 12, 456 (1995).
[35] G. Steinmeyer, D. Jaspert, and F. Mitschke, Observation of a Period-Doubling Sequence in a Nonlinear Optical Fiber Ring Cavity Near Zero Dispersion, Opt. Commun. 104, 379 (1994).
[36] M. Kues, N. Brauckmann, T. Walbaum, P. Groß, and C. Fallnich, Nonlinear Dynamics of Femtosecond Supercontinuum Generation with Feedback, Opt. Express 17, 15827 (2009).
[37] N. Akhmediev, J. M. Soto-Crespo, and G. Town, Pulsating Solitons, Chaotic Solitons, Period Doubling, and Pulse Coexistence in Mode-Locked Lasers: Complex GinzburgLandau Equation Approach, Phys. Rev. E 63, 056602 (2001).
[38] 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, 728 (2008).
[39] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, An Optical Ultrafast Random Bit Generator, Nat. Photonics 4, 58 (2010).
[40] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevX.7.041050 for details on the experimental setup, additional randomness measures, the entropy calculation, and the in-depth calculation of Feller's coin tossing constants.
[41] T. Steinle, F. Mörz, A. Steinmann, and H. Giessen, UltraStable High Average Power Femtosecond Laser System Tunable from 1.33 to 20μm, Opt. Lett. 41, 4863 (2016).
[42] K. Svozil, Three Criteria for Quantum Random-Number Generators Based on Beam Splitters, Phys. Rev. A 79, 054306 (2009).
[43] M. W. Mitchell, C. Abellan, and W. Amaya, Strong Experimental Guarantees in Ultrafast Quantum Random Number Generation, Phys. Rev. A 91, 012314 (2015).
[44] L. Bassham et al., NIST Report No. SP 800-22 Rev. 1a, 2010, https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final.
[45] P. L′Ecuyer and R. Simard, Testu01: A C Library for Empirical Testing of Random Number Generators, ACM Trans. Math. Softw. 33, 22:1 (2007).
[46] C. S. Calude, Information and Randomness: An Algorithmic Perspective, 2nd ed. (Springer, New York, 2010).
[47] C. S. Calude, M. J. Dinneen, M. Dumitrescu, and K. Svozil, Experimental Evidence of Quantum Randomness Incomputability, Phys. Rev. A 82, 022102 (2010).
[48] M. Troyer and R. Renner, ID Quantique SA, Carouge Internal Report, 2012, http://marketing.idquantique.com/acton/attachment/11868/f-004d/1/-/-/-/-/quantis-rndextracttechpaper.pdf.
[49] J. M. Roth, T. G. Ulmer, N. W. Spellmeyer, S. Constantine, and M. E. Grein, Wavelength-Tunable 40-GHz Picosecond Harmonically Mode-Locked Fiber Laser Source, IEEE Photonics Technol. Lett. 16, 2009 (2004).
[50] J. Niehusmann, A. Vörckel, P. H. Bolivar, T. Wahlbrink, W. Henschel, and H. Kurz, Ultrahigh-Quality-Factor Siliconon-Insulator Microring Resonator, Opt. Lett. 29, 2861 (2004).
[51] B. Kuyken, X. Liu, R. M. Osgood, R. Baets, G. Roelkens, and W. M. J. Green, A Silicon-Based Widely Tunable ShortWave Infrared Optical Parametric Oscillator, Opt. Express 21, 5931 (2013).
[52] C. Abellan, W. Amaya, D. Domenech, P. M. Muñoz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, Quantum Entropy Source on an InP Photonic Integrated Circuit for Random Number Generation, Optica 3, 989 (2016).
[53] T. Inagaki, Y. Haribara, K. Igarashi, T. Sonobe, S. Tamate, T. Honjo, A. Marandi, P. L. McMahon, T. Umeki, K. Enbutsu, O. Tadanaga, H. Takenouchi, K. Aihara, K.-i. Kawarabayashi, K. Inoue, S. Utsunomiya, and H. Takesue, A coherent Ising machine for 2000-node optimization problems, Science 354, 603 (2016).