【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】令和3年10月28日(2021.10.28)

【公表番号】特表2021-508134(P2021-508134A)
【公表日】令和3年2月25日(2021.2.25)
【年通号数】公開・登録公報2021-010
【出願番号】特願2020-554383(P2020-554383)
【国際特許分類】
Ｇ０６Ｆ　7/58　(2006.01)
Ｇ０６Ｆ　7/38　(2006.01)
Ｇ０２Ｆ　3/00　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　7/58　６８０
Ｇ０６Ｆ　7/38　５１０
Ｇ０２Ｆ　3/00

【手続補正書】
【提出日】令和3年9月17日(2021.9.17)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ランダムなビット文字列を生成するためのシステムであって、
第1のビット文字列と第2のビット文字列を繰り返し生成するように構成されたランダム性の弱いソースであって、あるインスタンスにおいて生成された前記第1のビット文字列および前記第2のビット文字列は、別のインスタンスにおいて生成された前記第1のビット文字列および前記第2のビット文字列と必ずしも同じ値を有するとは限らない、ランダム性の弱いソースと、
前記第2のビット文字列のうちの1つまたは複数を受け取り、量子装置が受け取る前記第2のビット文字列のうちの1つまたは複数の各々について、関連付けられる第3のビット文字列を出力するように構成された量子装置であって、前記量子装置は、複数の量子システムを含む、量子装置と、
前記量子装置が受け取る前記第2のビット文字列のそのような1つまたは複数の各々について、前記第2のビット文字列および前記関連付けられる第3のビット文字列を用いて、テスト統計を計算するように構成されたセキュリティテストロジックシステムであって、
前記計算されたテスト統計に少なくとも部分的に基づいて、前記関連付けられる第3のビット文字列を受け入れるか拒否するかを決定するように、および、前記複数の量子システムが近似的に非シグナリングであるかを決定するように構成されたセキュリティテストロジックシステムと、
前記セキュリティテストロジックシステムが前記関連付けられる第3のビット文字列を受け入れる場合、前記第1のビット文字列のうちの1つまたは複数に基づくビット文字列と、前記第3のビット文字列のうちの1つまたは複数に基づくビット文字列とを受け取ることと、前記ランダムなビット文字列を生成することとを行うように構成された2ソース抽出器と
を含む、システム。
【請求項２】

前記量子装置は、フォトニクスデバイスを含む、請求項1に記載のシステム。
【請求項３】
前記複数の量子システムは、2量子システムまたは4量子システムを含み、前記2量子システムまたは前記4量子システムの各々はキュビットを含む、請求項1に記載のシステム。
【請求項４】
前記複数の量子システムの各々は、前記キュビットに対して測定を行うことと、前記測定の結果を含むビットを出力することとを行うように構成された測定デバイスを含む、請求項3に記載のシステム。
【請求項５】
前記セキュリティテストロジックシステムは、
ベルの不等式の破れが測定される第1のテストを計算することと、
前記複数の量子システムが近似的に非シグナリングであるかどうかを決定するための第2のテストを計算することとと、
前記ベルの不等式の破れおよび前記複数の量子システムが近似的に非シグナリングであると決定したことに応じて、前記関連付けられる第3のビット文字列を受け入れることと、
を行うようさらに構成される、請求項1に記載のシステム。
【請求項６】
前記ランダム性の弱いソースは、少なくとも、前記第1のビット文字列を生成するために第1のランダム性の弱いソースを含み、前記第2のビット文字列を生成するために第2のランダム性の弱いソースを含む、請求項1に記載のシステム。
【請求項７】
前記関連付けられる第3のビット文字列は、少なくとも部分的に、前記第2のビット文字列のうちの前記1つまたは複数を用いて選択される複数の測定設定に基づいて生成される、請求項1に記載のシステム。
【請求項８】
前記複数の量子システムは、前記複数の量子システムの各々の中に前記測定デバイスを含む検出システムを含み、前記検出システムは、複数の検出器を含み、各測定デバイスは前記複数の検出器のうちの少なくとも１つを含み、前記テスト統計は、粒子が前記検出システムの中の前記複数の検出器によって実質的に同時に検出されることに関連付けられる一致の有無のしるしに少なくとも部分的に基づいて計算される、請求項4に記載のシステム。
【請求項９】
前記セキュリティテストロジックシステムは、
複数の測定設定を選択し、
前記複数の選択された測定設定を用いて複数の測定を行い、
前記複数の測定からベースラインヒストグラムを生成し、
前記複数の測定からテストヒストグラムを生成し、
前記ベースラインヒストグラムと前記テストヒストグラムの間の比較に少なくとも部分的に基づいて、前記複数の量子システムが近似的に非シグナリングであると決定する、
ようにさらに構成される、請求項1に記載のシステム。
【請求項１０】
前記セキュリティテストロジックシステムは、第２のテスト統計を計算し、前記計算された第2のテスト統計に少なくとも部分的に基づいて前記関連付けられる第3のビット文字列を受け入れるか拒否するかを決定するようさらに構成される、
請求項1に記載のシステム。
【請求項１１】
前記複数の量子システムの各々は、キュビットを生成するよう構成された状態拡張器を含む、請求項1に記載のシステム。
【請求項１２】

前記セキュリティテストロジックシステムは、前記測定の前記結果を記憶するよう構成された非一時的メモリと、前記記憶された結果に少なくとも部分的に基づいて、前記テスト統計を計算するよう構成されたプロセッサとを含む、請求項4に記載のシステム。
【請求項１３】
ランダムなビット文字列を生成するためのシステムであって、前記システムは、
第1のビット文字列と第2のビット文字列を繰り返し生成するように構成されたランダム性の弱いソースであって、あるインスタンスにおいて生成された前記第1のビット文字列および前記第2のビット文字列は、別のインスタンスにおいて生成された前記第1のビット文字列および前記第2のビット文字列と必ずしも同じ値を有するとは限らない、ランダム性の弱いソースと、
前記第2のビット文字列のうちの1つまたは複数を受け取り、関連付けられる第3のビット文字列を出力するように構成された量子装置であって、前記量子装置は、複数の量子システムを含む、量子装置と、
セキュリティテストロジックシステムであって、
前記量子装置が受け取る前記第2のビット文字列のそのような1つまたは複数の各々について、前記第2のビット文字列および前記関連付けられる第3のビット文字列を用いて、テスト統計を計算するように構成された第1のセキュリティテストと、
複数の測定設定を選択し、
前記複数の選択された測定設定を用いて複数の測定を行い、
前記複数の測定からベースラインヒストグラムを生成し、
前記複数の測定からテストヒストグラムを生成し、
前記ベースラインヒストグラムと前記テストヒストグラムの間の比較に少なくとも部分的に基づいて、前記複数の量子システムが近似的に非シグナリングであると決定する、
ように構成された第2のセキュリティテストと、
を行うように構成された、セキュリティテストロジックシステムと、
前記セキュリティテストロジックシステムは、前記第1のセキュリティテスト及び前記第2のセキュリティテストに少なくとも部分的に基づいて、前記関連付けられる第3のビット文字列を受け入れるか拒否するかを決定するようにさらに構成され、
前記セキュリティテストロジックシステムが前記関連付けられる第3のビット文字列を受け入れる場合、前記第1のビット文字列のうちの1つまたは複数に基づくビット文字列と、前記第3のビット文字列のうちの1つまたは複数に基づくビット文字列とを受け取ることと、前記ランダムなビット文字列を生成することとを行うように構成された2ソース抽出器と
を含む、システム。
【請求項１４】
前記量子装置は、フォトニクスデバイスを含む、請求項13に記載のシステム。
【請求項１５】
前記複数の量子システムは、2量子システムまたは4量子システムを含み、各量子システムはキュビットを生成する、請求項13に記載のシステム。
【請求項１６】
前記複数の量子システムの各々は、前記キュビットに対して測定を行うことと、前記測定の結果を含むビットを出力することとを行うように構成された測定デバイスを含む、請求項15に記載のシステム。
【請求項１７】
前記ランダム性の弱いソースは、少なくとも、前記第1のビット文字列を生成するために第1のランダム性の弱いソースを含み、前記第2のビット文字列を生成するために第2のランダム性の弱いソースを含む、請求項13に記載のシステム。
【請求項１８】
前記関連付けられる第3のビット文字列は、少なくとも部分的に、前記第2のビット文字列のうちの前記1つまたは複数を用いて選択される第2の複数の測定設定に基づいて生成さ

れる、請求項15に記載のシステム。
【請求項１９】
前記複数の量子システムは、前記複数の量子システムの各々の中に前記測定デバイスを含む検出システムを含み、前記検出システムは、複数の検出器を含み、各測定デバイスは前記複数の検出器のうちの少なくとも１つを含み、前記テスト統計は、粒子が前記検出システムの中の前記複数の検出器によって実質的に同時に検出されることに関連付けられる一致の有無のしるしに少なくとも部分的に基づいて計算される、請求項16に記載のシステム。
【請求項２０】
前記セキュリティテストロジックシステムは、
前記測定の前記結果を記憶するよう構成された非一時的メモリと、
前記記憶された結果に少なくとも部分的に基づいて、前記テスト統計を計算するよう構成されたプロセッサとを含む、
請求項16に記載のシステム。
【請求項２１】
前記テスト統計は、ベルの不等式の破れのレベルを決定することを含む、請求項13に記載のシステム。
【請求項２２】
前記ベルの不等式は、CHSH(クラウザー・ホーン・シモニー・ホルト)の不等式を含む、請求項21に記載のシステム。
【請求項２３】
前記複数の量子システムの各々は、キュビットを生成するよう構成された状態拡張器を含む、請求項13に記載のシステム。
【請求項２４】
前記セキュリティテストロジックシステムは、第２のテスト統計を計算し、前記計算された第2のテスト統計に少なくとも部分的に基づいて前記関連付けられる第3のビット文字列を受け入れるか拒否するかを決定するようさらに構成される、
請求項13に記載のシステム。