【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】平成28年9月29日(2016.9.29)

【公表番号】特表2015-534673(P2015-534673A)
【公表日】平成27年12月3日(2015.12.3)
【年通号数】公開・登録公報2015-075
【出願番号】特願2015-531099(P2015-531099)
【国際特許分類】
Ｇ０６Ｆ　7/58　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
Ｈ０３Ｋ　3/354　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　7/58　Ｚ
Ｇ０９Ｃ　1/00　６５０Ｂ
Ｈ０３Ｋ　3/354　Ｂ

【手続補正書】
【提出日】平成28年8月10日(2016.8.10)
【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】
少なくとも１つのリングオシレータ構造を備え、
前記リングオシレータ構造は、
直列に接続された奇数個のインバータのインバータチェーンを有し、発振入力の受信に応じて発振出力を生成するよう動作するリングオシレータと、
前記リングオシレータと接続されているテスト構造と、
を有し、
前記テスト構造は、前記リングオシレータからのフィードバック信号として受信される前記発振出力と、前記テスト構造において受信される観測可能なチェーン入力又はテスト入力のいずれかとに基づき、指定されたジッター制限内において目的の発振周波数の発振出力が前記リングオシレータによって生成されているか否かを確認するように構成されており、
前記観測可能なチェーン入力は、前記リングオシレータへのフィードバック信号の有効化又は無効化に関連するフォールトを観測するための信号を表し、
前記テスト入力は、前記目的の発振周波数を持つ入力信号を表す、装置。
【請求項２】
前記テスト構造は、前記リングオシレータの構造テスト及び機能テストのうちの少なくとも１つを可能にするため、前記リングオシレータをテスト可能な構造に再構成するように動作する、請求項１に記載の装置。
【請求項３】
前記少なくとも１つのリングオシレータ構造を含む複数のリングオシレータ構造と、
フィードバック経路と、を有し、
前記複数のリングオシレータ構造は、前記複数のリングオシレータ構造における最初のリングオシレータ構造から最後のリングオシレータ構造への信号経路を提供する直列チェーンとして接続されており、

前記フィードバック経路は、前記直列チェーンにおける前記最後のリングオシレータ構造のテスト出力を前記複数のリングオシレータ構造における前記最初のリングオシレータ構造へフィードバックするように構成されており、
前記テスト出力は、前記最初のリングオシレータ構造によって受信されるテスト入力と共に、前記発振出力の周波数を制御する、請求項１に記載の装置。
【請求項４】
前記最後のリングオシレータ構造の前記テスト出力をフィードバックするために、フィードバック有効化信号を受信することに応じてフィードバック経路を条件付きでアクティベートするゲートをさらに備え、
前記ゲートは、前記直列チェーンにおける前記最初のリングオシレータ構造に接続されている、請求項３に記載の装置。
【請求項５】
前記最初のリングオシレータ構造によって受信される前記テスト入力と、前記最後のリングオシレータ構造からの前記テスト出力とについて XOR 演算を実行するように構成されている XOR ゲートをさらに備える、請求項３に記載の装置。
【請求項６】
前記直列チェーンの前記複数のリングオシレータ構造における１つ又は複数のリングオシレータ各々は、前記１つ又は複数のリングオシレータ各々に対応する有効化信号に基づき、テストのために選択される、請求項３に記載の装置。
【請求項７】
前記複数のリングオシレータ構造における前記最初のリングオシレータ構造から前記最後のリングオシレータ構造までの信号経路において、前記インバータチェーンは奇数個のインバータを含む、請求項３に記載の装置。
【請求項８】
AND ゲートをさらに備え、
前記 AND ゲートの出力は前記リングオシレータの入力に結合されており、
前記 AND ゲートは、フィードバック有効化信号に応じて、前記フィードバック経路を条件付きでアクティベート又はディアクティベートする、請求項１に記載の装置。
【請求項９】
前記テスト構造は、複数の制御信号を受信する、請求項１に記載の装置。
【請求項１０】
前記複数の制御信号のうちの少なくとも１つは、当該装置内部のレジスタから得られるテスト制御信号である、請求項９に記載の装置。
【請求項１１】
前記複数の制御信号のうちの少なくとも１つはテストモード信号であり、
前記テストモード信号は、前記リングオシレータが、自走発振出力を提供する機能モードであるか又は特定の周波数の前記発振出力を提供するテストモードであるかを決定する、請求項９に記載の装置。
【請求項１２】
HDCP（High Definition Content Protection）における秘密鍵の生成に用いられる乱数発生器であって、
少なくとも１つのリングオシレータ構造を備え、
前記リングオシレータ構造は、
直列に接続された奇数個のインバータのインバータチェーンを有し、発振入力の受信に応じて発振出力を生成するよう動作するリングオシレータと、
前記リングオシレータと接続されているテスト構造と、
を有し、
前記テスト構造は、前記リングオシレータからのフィードバック信号として受信される前記発振出力と、前記テスト構造において受信される観測可能なチェーン入力又はテスト入力のいずれかとに基づき、指定されたジッター制限内において目的の発振周波数の発振

出力が前記リングオシレータによって生成されているか否かを確認するように構成されており、
前記観測可能なチェーン入力は、前記リングオシレータへのフィードバック信号の有効化又は無効化に関連するフォールトを観測するための信号を表し、
前記テスト入力は、前記目的の発振周波数を持つ入力信号を表す、乱数発生器。
【請求項１３】
複数のリングオシレータ構造を備え、
前記複数のリングオシレータ構造は、前記複数のリングオシレータ構造における最初のリングオシレータ構造から最後のリングオシレータ構造への信号経路を提供する直列チェーンとして接続されており、
前記複数のリングオシレータ構造における各リングオシレータ構造は、
直列に接続されたインバータのインバータチェーンを有し、発振入力の受信に応じて第１発振出力を生成するよう動作するリングオシレータと、
前記リングオシレータに接続されているリングオシレータテスト構造と、
前記直列チェーンにおける前記最初のリングオシレータ構造に接続されているゲートと、を有し、
前記リングオシレータテスト構造は、観測可能なチェーン入力又はテスト入力のいずれかを受信し、なおかつ前記リングオシレータからのフィードバック信号として第２発振出力を受信するように構成されており、
前記リングオシレータテスト構造は、前記リングオシレータをテスト可能な構造に再構成することで、前記リングオシレータの構造テスト及び機能テストのうちの少なくとも１つを有効化するように動作し、
各前記テストは、前記リングオシレータが目的の発振周波数を生成することができるか否かを確認するためのものであり、
前記ゲートは、フィードバック経路を条件付きでアクティベートすることで、前記フィードバック経路を介して、前記最後のリングオシレータテスト構造のテスト出力を、前記直列チェーンにおける前記最初のリングオシレータ構造における前記複数のリングオシレータ構造へフィードバックし、
前記条件付きのアクティベートは、フィードバック有効化信号に応じて行われ、
前記テスト出力は、前記複数のリングオシレータ構造へフィードバックされ、前記最初のリングオシレータ構造によって受信されるテスト入力と共に、前記複数のリングオシレータ構造における前記最後のリングオシレータ構造の発振出力の周波数を制御するために用いられる、装置。
【請求項１４】
前記最初のリングオシレータ構造によって受信される前記テスト入力と、前記最後のリングオシレータ構造からの前記テスト出力とについて XOR 演算を実行するように構成されている XOR ゲートをさらに備える、請求項１３に記載の装置。
【請求項１５】
前記直列チェーンの前記複数のリングオシレータ構造における１つ又は複数のリングオシレータ各々は、前記１つ又は複数のリングオシレータ各々に対応する有効化信号に基づき、テストのために選択される、請求項１３に記載の装置。
【請求項１６】
前記複数のリングオシレータ構造における前記最初のリングオシレータ構造から前記最後のリングオシレータ構造までの信号経路において、前記直列チェーンは奇数個のインバータを含む、請求項１３に記載の装置。
【請求項１７】
構造テストのため、定常状態における前記複数のリングオシレータのうちの少なくとも１つのフィードバックを無効化するように結合されたゲート論理をさらに備え、
前記ゲート論理は前記複数のリングオシレータ構造に接続されている、請求項１３に記載の装置。

【請求項１８】
暗号生成において秘密鍵の生成に用いられる乱数発生器であって、
複数のリングオシレータ構造を備え、
前記複数のリングオシレータ構造は、前記複数のリングオシレータ構造における最初のリングオシレータ構造から最後のリングオシレータ構造への信号経路を提供する直列チェーンとして接続されており、
前記複数のリングオシレータ構造における各リングオシレータ構造は、
直列に接続されたインバータのインバータチェーンを有し、発振入力の受信に応じて第１発振出力を生成するよう動作するリングオシレータと、
前記リングオシレータに接続されているリングオシレータテスト構造と、
前記直列チェーンにおける前記最初のリングオシレータ構造に接続されているゲートと、を有し、
前記リングオシレータテスト構造は、前記リングオシレータからのフィードバック信号として第２発振出力を受信するように構成されており、
前記リングオシレータテスト構造は、前記リングオシレータテスト構造において受信される観測可能なチェーン入力又はテスト入力のいずれかを受信することに基づいて、指定されたジッター制限内において目的の発振周波数の前記第１発振出力が前記リングオシレータによって生成されているか否かを確認するように構成されており、
前記観測可能なチェーン入力は、前記リングオシレータへのフィードバック信号の有効化又は無効化に関連するフォールトを観測するための信号を表し、
前記テスト入力は、前記目的の発振周波数を持つ入力信号を表し、
前記リングオシレータテスト構造は、前記リングオシレータをテスト可能な構造に再構成することで、前記リングオシレータの構造テスト及び機能テストのうちの少なくとも１つを有効化するように動作し、
各前記テストは、前記リングオシレータが目的の発振周波数を生成することができるか否かを確認するためのものであり、
前記ゲートは、フィードバック経路を条件付きでアクティベートすることで、前記フィードバック経路を介して、前記最後のリングオシレータテスト構造のテスト出力を、前記直列チェーンにおける前記最初のリングオシレータ構造における前記複数のリングオシレータ構造へフィードバックし、
前記条件付きのアクティベートは、フィードバック有効化信号に応じて行われ、
前記テスト出力は、前記複数のリングオシレータ構造へフィードバックされ、前記最初のリングオシレータ構造によって受信されるテスト入力と共に、前記複数のリングオシレータ構造における前記最後のリングオシレータ構造の発振出力の周波数を制御するために用いられる、乱数発生器。
【請求項１９】
少なくとも１つのリングオシレータ構造を有し、
前記リングオシレータ構造は、
直列に接続された奇数個のインバータのインバータチェーンを有し、発振入力の受信に応じて発振出力を生成するように動作するリングオシレータと、
前記インバータチェーンから前記発振出力を受信し、なおかつ前記インバータチェーンへ前記発振入力を提供するように構成されているフィードバック経路と、を有し、
前記フィードバック経路は、
前記リングオシレータからのフィードバック信号として前記発振出力を受信し、なおかつ観測可能なチェーン入力又はテスト入力を受信するように構成されているテスト構造と、
フィードバック有効化信号に応じ、前記フィードバック経路を条件付きでアクティベート又はディアクティベートするゲート要素と、
を有し、
前記観測可能なチェーン入力は、前記リングオシレータへのフィードバック信号の有効

化又は無効化に関連するフォールトを観測するための信号を表し、
前記テスト入力は、前記目的の発振周波数を持つ入力信号を表す、装置。