【書類名】　　明細書
【発明の名称】意味生成ＯＳ・素数リズム暗号・GD-Attention に基づく同期判定、鍵導出および資源管理装置、方法、半導体回路およびプログラム
【技術分野】
【０００１】
本発明は情報セキュリティ及び暗号通信に関し、アプリケーション層とＯＳ／半導体実装の同期・鍵管理に関する。
【背景技術】
【０００２】
従来のオペレーティングシステム（ＯＳ）は、ＣＰＵ時間、メモリ、入出力などの資源管理に特化し、アプリケーションが扱う「意味」や「同期（セマンティックな一致）」はＯＳ外で個別に実装されてきた。暗号機能も多くはアプリケーション層またはカーネル付随のライブラリに分離配置され、ＯＳの資源管理と暗号鍵ライフサイクルが疎結合であった。
【０００３】
公開鍵暗号では、大きな素数や素因数分解の困難性、楕円曲線上の離散対数の困難性など、素数分布の性質に依拠するものが中心である。一方で、量子計算の進展を踏まえ、格子・符号・多変数・アイソジェニー等の耐量子暗号が提案・標準化されつつある。
【０００４】
半導体実装においては、熱雑音等を用いる真性乱数生成器（ＴＲＮＧ）や、製造ばらつきを指紋化するＰＵＦが鍵素材の源として用いられる。また副チャネル攻撃対策（電力平坦化、マスキング等）やタンパ検知も広く検討されている。
【０００５】
しかし、アプリケーションが検出する意味的な同期（例：特徴の位相一致・構造整合）と、暗号資源の生成・割当・失効をＯＳ資源スケジューラの粒度で一体的に制御する枠組みは十分に整備されていない。結果として、(i) 同期イベントと鍵確立の対応が曖昧、(ii) 参加していない傍観者が生成過程を後追い解析し得る、(iii) 半導体実装とＯＳポリシの一貫性保証が弱い、などの課題があった。
【０００６】
さらに、意味的な選択・同期を連続値の重み平均で表現する従来方式では、選択集合の一意性や有限エネルギー制約を厳密に担保しにくい。これにより、リソース飽和や曖昧な認証境界が生じ、鍵管理との直結が難しいという実装上の制約があった。
【０００７】
一方、素数列、素数間隔、マンゴルト関数等の数論系列（素数リズム）は、同期の感度を調整する指標（閾値・許容帯）の設計に資する。素数分布の偏差に対する評価（リーマン型の偏差エンベロープや零点密度境界など）は、同期判定の保守性を規定する工学的パラメータとして導入可能である。
【０００８】

しかしながら、これらの数論的知見を、意味同期の検出・鍵確立・ＯＳ資源管理・半導体実装を同一の因果鎖で結ぶ形で体系化した基盤は十分ではなかった。

【０００９】

加えて、量子計算を前提とした将来環境においては、同期イベントを耐量子鍵カプセル化（ＫＥＭ）や量子鍵配送（ＱＫＤ）のハンドシェイク条件として統合し、当事者の観測路に鍵導出を強制的にバインドする枠組みが望まれている。

【先行技術文献】

【特許文献】

【００１０】

US 2009/0083833 A1, “Authentication with Physical Unclonable Functions”, 2009-03-26.

【００１１】

US 10,038,564 B2, “Physical Unclonable Function using Augmented Memory for Authentication”, 2018-07-31.

【非特許文献】

【００１２】

RFC 5869: “HMAC-based Extract-and-Expand Key Derivation Function (HKDF)”, H. Krawczyk, P. Eronen, 2010-05.

【００１３】

“Attention Is All You Need”, A. Vaswani et al., NeurIPS 2017.

【発明の概要】

【００１４】

本発明は、意味的同期の検出と暗号資源のライフサイクル管理とを、ＯＳ資源管理の粒度で一体化し、半導体実装まで貫通させる基盤に関する。

【００１５】

入力特徴から同期指標を算出し、閾値比較で同期成立を決定する。この指標は、意味特徴に加えて数論系列（素数リズム）を組み合わせて導出され、偏差エンベロープ等の数論的パラメータにより保守性・感度を可調整とする。

【００１６】

同期成立イベントをトリガとして、ＴＲＮＧ／ＰＵＦ等の物理源と組み合わせた鍵素材からセッション鍵を確立し、意味チャネル単位での割当・ローテーション・失効・消去を行う。これらの処理はＯＳの意味資源として監査・隔離され、当該資源の利用は同期に参加した主体に限定される（強制参加性）。

【００１７】

同期指標の算出には、非線形選択機構である GD-Attention を用い、選択集合の一意性および有限エネルギー制約を課すことで、意味的一貫性とリソース飽和回避を両立する。

【００１８】

実装は、アナログ前段（増幅・帯域選択・Ａ／Ｄ）とデジタル後段（指標演算・閾値判定）からなるハイブリッド半導体回路とし、副チャネル対策およびタンパ

検知により鍵素材・セッション鍵を保護する。
【００１９】
本基盤は、耐量子暗号（格子等）と互換であり、必要に応じてＱＫＤとも連携し得る。同期成立イベントは、これら鍵配送・認証プロトコルのハンドシェイク条件として利用される。
【００２０】
以上により、意味同期→鍵確立→ＯＳ資源管理→半導体実装の流れを単一の設計原理で結び、傍観者による後追い再現を実質的に不能化しつつ、古典・量子の双方にわたり拡張可能な暗号基盤を提供する。なお、数論的パラメータの設定は、リーマン型偏差評価または無条件な零点密度境界のいずれでも運用可能であり、理論仮定に依存せず保守的に設計できる。
【発明が解決しようとする課題】
【００２１】
従来のＯＳにおいて、意味的同期の検出と暗号鍵ライフサイクル管理とは疎結合であり、同期イベントと鍵確立との因果対応が不明確であるという課題があった。
【００２２】
意味的同期に参加していない傍観者が、観測や事後解析により暗号資源を再構成し得るおそれがあり、当事者性が暗号学的に担保されていないという課題があった。
【００２３】
素数分布等の数論的知見を同期判定の閾値設計に反映する統一的枠組みが不足し、感度と保守性のトレードオフを体系的に制御しにくいという課題があった。
【００２４】
重み平均型の選択機構では選択集合の一意性および有限エネルギー制約の担保が弱く、誤同期および資源飽和を招き得るという課題があった。
【００２５】
半導体実装における副チャネル攻撃およびタンパに対し、装置・ＯＳ・暗号の跨りで一貫した保護・監査が行われにくいという課題があった。
【００２６】
量子計算環境において、耐量子暗号や量子鍵配送と同期イベントとを整合的に連携させる仕組みが不足しているという課題があった。
【課題を解決するための手段】
【００２７】
本発明は、同期指標の導出、暗号資源の生成・割当・失効・消去、及び意味資源としての監査を、ＯＳ資源管理の粒度で一体化し、半導体実装まで貫通させる基盤を提供する。
【００２８】
入力特徴に数論系列（素数列、素数間隔、マンゴルト関数、チェビシェフ関数、素数計数に基づく統計量等）を組み合わせ、窓関数畳込み、差分、相関、モジュ

ラ写像等により加工した系列から同期指標を導出する。また本明細書における「素数リズム派生量 R」は、数論系列 U（素数列 p_n、素数間隔 g_n = p_{n+1} − p_n、マンゴルト関数 Lambda(n)、チェビシェフ関数 theta(x), psi(x) の少なくとも一つ）から、以下の処理のうち二つ以上を順に適用して得られる特徴量ベクトルである：窓関数畳込み（窓長 W）、差分/微分近似、自己相関（ラグ L）、モジュラ写像（基数 m）。R の構成パラメータは実装上の制約に応じて設定され、例えば W in [64, 4096], L in [1, 64], m in {97, 101, ...} の範囲から選択される。ちなみに用語の定義としては以下である。(1) Acc(E)：無条件包絡 E に対する受理集合。S ∈ Acc(E) とは、S(x) >= E_upper(x) + delta が tau 連続の成立をいう。(2) E_upper(x)：素数分布の偏差に対する無条件上界から導かれる上包絡。参照モデルの識別子を監査ログに記録する。(3) CHID：意味チャネル識別子。鍵ライフサイクルの割当・監査の単位。(4) salt, ikm, SK：KDF に入力する salt := (R || CHID)、ikm := (TRNG || PUF)、導出結果をセッション鍵 SK とする。(5) 記号の表記：本明細書では delta, tau 等の記号を ASCII で表記し、ギリシャ文字との混用を行わない。

【００２９】

同期の閾値又は許容帯は、素数分布の偏差に対する無条件上界に基づき定義する。無条件包絡 E は、当該上界から導かれる上包絡 E_upper(x) を少なくとも含む。同期成立は次の受理規則で定義する：「S ∈ Acc(E) ⇔ S(x) >= E_upper(x) + delta が tau 以上連続」。 ここで delta > 0 および tau > 0 は校正手順により設定する。設計手順は、(i) 同期指標 S(x) を算定、(ii) 参照無条件上界から E_upper(x) を構成、(iii) ROC 最適化により (delta, tau) を選定し、当該受理規則を固定する、である。運用時は、delta・tau・参照 E_upper の識別子を監査ログに記録し、逸脱時は再校正を行う。本明細書における無条件上包絡 E_upper は、参照無条件上界の表形式モデルから構成する。参照ソース B は {PSI（Chebyshev φ）、THETA（θ）、PI（π(x) の上界差）、GAP（素数間隔統計）} のいずれかとし、各ソースはバージョン v と有理値テーブル T = {(x_j, U_j)}*{j=1..m}* *を持つ。実装は次のいずれかでよい：（i）右連続階段 E_upper(x) = max{ j : x_j <= x } U_j*、（ii）単調区分線形補間 E_upper_lin(x)。モデル識別子は E_upper_ID := “EUP/⟨B⟩/⟨v⟩/⟨hash(T)⟩” とし、校正時に (delta, tau, E_upper_ID) を固定し、運用中は変更を再校正扱いとする。例：B=PSI, v=1.0, T は有理分数 (p/q) で格納し、hash(T) は後述の H（SHA3-256 または BLAKE3）で算出する。

【００３０】

同期指標の算出には GD-Attention を用い、非線形選択、選択集合の一意性制約および有限エネルギー制約により、誤同期の抑制と資源飽和回避を両立する。「同期指標 S」は、入力特徴列と前記 R を結合した特徴集合に対し、GD-Attention による非線形スパース選択（選択集合サイズ <= k）を適用して算出する。選択集合には一意性制約および有限エネルギー制約を課し、演算/電力バジェット B <= P_max を超えないように設定する。本明細書における GD-Attention とは、

候補特徴集合に対する非線形スパース選択機構であって、(a) 選択集合サイズ <= k、(b) 一意性制約としてマージン Delta>0 を満たす argmax の一意性、(c) 有限エネルギー制約として重み列 w について sum_i |w_i| <= B を満たす、を同時に満足するものをいう。実装は L1 ないし L0 近似正則化、閾値ハード選択、又は分岐探索のいずれでもよい。GD-Attention は、(a) L1 又は L0 近似正則化に基づくスパース選択、(b) 閾値ハード選択、(c) 分岐探索の少なくとも一つで実現できる。B の単位は、ソフトウェアでは 1 秒当たりの乗算加算回数、ハードウェアでは同等電力（mW）又はクロック当たり演算回数として計測する。GD-Attention の最小実施手順（貪欲・一意マージン検査付き）：(1) 候補特徴集合 F={f_i} を用意し、スコア s_i := score(f_i; R, params) を算出（例：相関・相互情報・ROC 利得など任意の実装一意関数）。(2) S = {}, 累積ノルム L = 0 で開始。以後繰返し： a) s_(1) と s_(2) を最大と次点とし、一意性マージン s_(1) - s_(2) >= Delta を満たさなければ停止（曖昧として不選択終了）。 b) i* = argmax_i s_i を選び、重み w_{i*} := normalize(s_{i*})。c) 有限エネルギー制約を検査：L + |w_{i*}| <= B を満たすときのみ S ← S ∪ {i*}, L ← L + |w_{i*}|。満たさない場合は停止。 d) |S| = k に達したら停止。 (3) 同期指標 S(x) は S と w から定義（例：加重合成、スパース投影等）。計算量は O(k*|F|)（貪欲）または O(|F|log|F|)（ソート）。ログには (k, B, Delta, 選択インデックス列, w の L1) を記録する。タイブレークは決定的規則（インデックス昇順など）で固定し再現性を担保する。

【００３１】

暗号資源は、ＴＲＮＧ／ＰＵＦから得る鍵素材と素数リズム由来系列を鍵導出関数（ＫＤＦ）で合成して確立し、当該導出を参加主体の観測路又はＰＵＦ応答に強制的にバインドすることで、非参加者による再現を実質的に不能化する。鍵導出関数（KDF）は、例えば HKDF を用い、salt := (R || CHID)、ikm := (TRNG || PUF) としてセッション鍵 SK を導出する。ここで CHID は意味チャネル識別子である。前記構成により、導出鍵は前記 R と観測路/PUF 応答に強制的にバインドされ、非参加者は当該入力にアクセスせずに SK を実質的に再現できない。 KDF の例は HKDF(SHA3-256) 又は KMAC128。監査ログの最小必須項目は〈CHID, H_R, E_upper_ID, delta, tau, timestamp, device_cert〉。

ここで H_R := H(R || params)、H は SHA3-256 又は BLAKE3 とし、出力長は 256bit（少なくとも 128bit の衝突耐性を満たす）。salt には (R||CHID) の**識別子（H_R の短縮表現）**を用いてもよい。

【００３２】

確立したセッション鍵は意味チャネル単位で割当・ローテーション・失効・消去を行い、状態機械とポリシ制御によりＯＳの意味資源として監査・隔離する。

【００３３】

実装は、アナログ前段（増幅・帯域選択・Ａ／Ｄ）とデジタル後段（指標演算・閾値判定）からなるハイブリッド半導体回路とし、電力平坦化、タイミングランダマイズ、マスキング、ノイズ注入等の副チャネル対策およびタンパ検知・即時

消去を備える。
【００３４】
鍵配送・認証は、**耐量子暗号（格子等）と整合し、必要に応じて量子鍵配送（ＱＫＤ）**と連携し、同期成立イベントをプロトコルのハンドシェイク条件として用いる。
【００３５】
以上の各構成は、ソフトウェア、ハードウェア又はそのハイブリッドの態様として実現可能であり、単体機器又は分散システムに適用できる。
【発明の効果】
【００３６】
意味的同期→鍵確立→ＯＳ資源管理→半導体保護の因果鎖を単一原理で統合し、端点から物理層まで整合したトレーサビリティを実現できる。
【００３７】
鍵導出を参加主体の観測路／ＰＵＦ応答にバインドすることで、強制参加性を付与し、傍観者による事後再現を実質的に不能化できる。
【００３８】
数論系列および偏差パラメタにより、同期判定の感度・保守性を体系的に調整でき、リーマン型評価又は無条件境界のいずれでも運用可能である。
【００３９】
GD-Attention により選択の一意性と有限エネルギー制約が担保され、誤同期の低減、資源飽和の抑止、意味的一貫性の向上が得られる。従来の重み平均型注意機構（Ｓｏｆｔｍａｘ等）と比較し、誤同期率（％）、見逃し率（％）、レイテンシτ（ms）、エネルギーバジェットＢ（mW 相当）、鍵合意成功率（％）を評価指標とする。GD-Attention は一意選択と有限エネルギー制約により、同一Ｂで誤同期率・見逃し率の低減とτの短縮を示す。
【００４０】
副チャネル対策およびタンパ検知・即時消去により、半導体実装レベルでの攻撃耐性が向上し、鍵素材及びセッション鍵の安全性が高まる。
【００４１】
耐量子暗号およびＱＫＤとの連携により、量子計算環境においても継続的に安全な鍵配送・認証が可能となる。
【００４２】
ソフト／ハードの各態様に適用でき、単体機器から分散環境までスケーラブルに展開できるため、広範な用途での実装可能性が高い。
【００４３】
本発明によれば、鍵導出が参加主体の観測路又はＰＵＦ応答にバインドされるため、傍観者による事後再現（リプレイ又は後追い生成）を実質的に不能化できる。
【００４４】
本発明の GD-Attention は一意選択と有限エネルギー制約を備え、同一エネルギーバジェットＢの下で、従来の重み平均型注意機構と比較して誤同期率及び見逃

し率を低減し、レイテンシτを短縮できる。
【００４５】
同期閾値の設計はリーマン型評価又は無条件境界のいずれにも対応し、理論仮定に依存しない保守構成を選択できるため、規格移行期を含む長期運用における実装リスクを低減できる。
【００４６】
意味チャネル単位の鍵ライフサイクル管理と監査により、マルチテナント環境における隔離性とエンドツーエンドのトレーサビリティを向上でき、意味的同期→鍵確立→ＯＳ資源管理の因果整合を維持できる。
【００４７】
副チャネル対策及びタンパ検知・即時消去（ゼロ化経路）により、半導体実装レベルで鍵素材及びセッション鍵の残留リスクを低減できる。
【図面の簡単な説明】
【００４８】
【図１】素数リズムと GD-Attention で同期を検出し、その結果を用いて鍵を導出・配布し、OS 層で管理しつつ半導体レベルで保護する一連の流れを示す図である。
【図２】素数由来の系列を GD-Attention で選択・整形し、同期指標 S を算出して偏差エンベロープ E(x)で判定へ渡す工程を示す図である。
【図３】TRNG と PUF 応答に、チャネル情報と素数リズム派生量をバインドして KDF でセッション鍵 SK を導出する流れを示す図である。
【図４】セッション鍵ＳＫ１６１を受けて、意味資源管理部１７０が各プロセスに対する鍵配布・隔離・監査・失効／消去を一元制御する構成を示す図である。
【図５】鍵の生成前から消去までの単調な状態遷移と、逸脱検知／タンパ検知による強制失効経路を示す図である。
【図６】 アナログ前段で信号品質を確保し、デジタル後段で同期指標演算と閾値判定を行うハイブリッド回路２００の構成を示す図である。
【図７】ハードウェア回路２００に対して副チャネル対策部１８０と耐タンパ処理部１９０を配し、鍵保管領域（セッション鍵ＳＫ１６１等）への漏えいを抑止し、タンパ検知時に即時消去１９２を発動する構成を示す図である。
【図８】 装置Ａと装置Ｂ（及び必要に応じてサーバ）が、同期成立イベントを契機に、ＰＱ‐ＫＥＭ２１１及びＰＱ署名２１２を実行し、任意でＱＫＤインタフェース２１３による鍵素材を並行利用する時系列を示す図である。
【図９】素数列 p(n)、素数間隔 g(n)、マンゴルト関数Λ（ｎ）、チェビシェフ関数θ（ｘ）・φ（ｘ）を入力とし、加工部１１５で窓畳込み・差分・自己相関・モジュラ写像を行って素数リズム系列を出力する構成を示す図である。
【図１０】同期指標Ｓ（１３１）に対し、偏差エンベロープＥ（１３３）および閾値により受理領域を定め、誤同期を抑制する設計方針を示す概念図である。
【図１１】複数ノードの部分鍵（２２１）を閾値ｔ／ｎの秘密分散（２２２）

で合成し、セッション鍵ＳＫ（１６１）を復元してＯＳ管理部（１７０）に引き渡す構成を示す図である。

【図１２】本発明の主要ブロックを単一チップ上にＩＰとして配置し、内部バス・制御線・ゼロ化経路を含む物理レベルの実装態様を示す図である。

【発明を実施するための形態】

【００４９】本発明の一形態は、意味的同期の検出・暗号資源の導出・ＯＳ資源管理・半導体実装を一体化する基盤であり、少なくとも以下の機能ブロックを備える。

（ａ）数論系列生成部（素数リズム生成器）：素数列、素数間隔、マンゴルト関数、チェビシェフ関数、素数計数等に基づく系列を生成・加工する。

（ｂ）同期指標生成部：入力特徴（時系列／トークン列／信号）と数論系列を合成し、同期指標を算出する。

（ｃ）GD-Attention 部：非線形選択機構により候補集合をスパース選択し、唯一性制約および有限エネルギー制約を課す。

（ｄ）閾値設定部：素数分布の偏差に対する評価（リーマン型偏差エンベロープ、零点密度境界、零点自由領域に基づく上界等）をパラメタとして同期判定の閾値／許容帯を定義する。

（ｅ）鍵素材生成部：真性乱数生成器（ＴＲＮＧ）またはＰＵＦから鍵素材を取得する。

（ｆ）鍵導出部（ＫＤＦ）：鍵素材と素数リズム派生量、文脈情報（チャネルＩＤ、エポック等）を入力としてセッション鍵を導出する。

（ｇ）意味資源管理部（ＯＳ層）：意味チャネル単位でセッション鍵の割当・ローテーション・失効・消去・監査を行う。

（ｈ）副チャネル対策部／耐タンパ処理部：電力平坦化、タイミングランダマイズ、マスキング、ノイズ注入、タンパ検知・即時消去を実装する。

（ｉ）ハイブリッド回路部：アナログ前段（増幅・帯域選択・Ａ／Ｄ）とデジタル後段（指標演算・閾値判定）からなる半導体実装。

（ｊ）プロトコル連携部：耐量子ＫＥＭ／署名および必要に応じてＱＫＤと連携し、同期成立イベントをハンドシェイク条件として用いる。また代替実施形態として（Ａ）数論系列Ｕ：電磁雑音、音響、慣性、電源ゆらぎ、ＴＲＮＧ、ＰＵＦ、ネットワーク遅延、センサ融合、並びに素数列ｐ_n、素数間隔ｇ_n、マンゴルト関数Λ(n)、チェビシェフ関数θ(x)，φ(x)、素数計数π(x)に基づく統計量の少なくとも一つ。（Ｂ）GD-Attention のエネルギー族：二峰ガウス、ラプラス、Ｈｕｂｅｒ、Ｔｕｋｅｙ、分割二次、学習済みルックアップの少なくとも一つ。（Ｃ）包絡Ｅの構成：解析式上界、畳み込み上界、ＲＯＣ最適化、確率的（ベイズ）上限の少なくとも一つ。（Ｄ）ハード／ソフト分割：前段アナログ（帯域・Ａ／Ｄ分解能）、ＦＰＧＡ／ＡＳＩＣ（固定小数点幅）、ＣＰＵ／ＧＰＵ／ＤＳＰのいずれでもよい。（Ｅ）鍵派生：ＫＤＦはＨＫＤＦ、ＫＭＡＣ、ＢＬＡＫＥ３‐ＫＤＦ等から選択し、salt はＣＨＩＤ ∥ ＰＵＦ応答 ∥ H(R) ∥ 時刻 ∥ 場所の少なくとも一つを含む。

【００５０】
数論系列生成部は、整数区間に対する窓関数畳込み、差分、自己相関、モジュラ写像等により素数リズムを構成し、同期指標生成部に供給する。素数列 p_n、間隔 g_n = p_{n+1} − p_n、Mangoldt 関数 Lambda(n)、Chebyshev 関数 theta(x), psi(x) のいずれを用いてもよい。

【００５１】同期指標は、意味特徴から得る同期量 *SfeatS_{¥text{feat}}*Sfeat と数論系列から得る同期量 *SprimeS_{¥text{prime}}*Sprime を合成して定義される。合成は線形結合、写像合成、あるいは学習則に基づく加重結合の何れでもよく、政策要件に応じて重みを更新可能である。

【００５２】GD-Attention 部は、候補集合に対し非線形選択を行い、選択集合の唯一性を保つ整合制約と、計算・電力・帯域に関する有限エネルギー制約を課すことで、誤同期および資源飽和を抑止する。

【００５３】閾値設定部は、素数分布偏差の評価をパラメタとして使う。実装においては、リーマン型の偏差エンベロープ（例えば *x¥sqrt{x}*x スケールの項を含む形）を用いても、無条件な零点密度境界・零点自由領域から導かれる上界を用いてもよい。これにより、理論仮定に依存せず保守的な運用が可能となる。

【００５４】鍵導出部は、鍵素材（ＴＲＮＧ／ＰＵＦ）と素数リズム派生量、チャネル文脈を入力とするＫＤＦを適用し、セッション鍵を導出する。導出は参加主体の観測路またはＰＵＦ応答にバインドされ、非参加者による事後再現を実質的に不能化する（強制参加性）。

【００５５】意味資源管理部は、チャネル識別子に基づく状態機械（未同期→鍵確立→利用中→失効→消去）でライフサイクルを管理し、逸脱検知（同期指標の低下、ポリシ違反、タンパ検知）時に直ちに失効・消去へ遷移させる。

【００５６】副チャネル対策部は、演算経路の電力平坦化、時間ゆらぎの注入、確率的マスキング、雑音重畳等を組み合わせ、観測から鍵情報が推定される確率を低減する。耐タンパ処理部は、光・温度・電圧・プロービング検知に応じて鍵素材・セッション鍵を即時消去する。

【００５７】ハイブリッド回路部は、アナログ前段で信号の帯域選択とサンプリング品質を確保し、デジタル後段で同期指標演算と閾値判定を行う。後段は汎用プロセッサ、ＦＰＧＡ、ＡＳＩＣのいずれでもよい。

【００５８】プロトコル連携部は、格子・符号・多変数・アイソジェニー等の耐量子ＫＥＭ／署名に対応し、必要に応じてＱＫＤを併用する。同期成立イベントはハンドシェイク条件として扱われ、鍵配送・認証の整合性が維持される。

【００５９】以上の各構成要素は、ソフトウェア、ハードウェア、またはその組合せとして実現でき、単体機器から分散システムまでスケーラブルに適用可能である。なお、本発明は前記形態に限定されるものではない。

【実施例】

【００６０】
（ソフトウェア中心）サーバ環境において、数論系列生成部は Lambda(n) と

theta(x) を用いた窓畳込み系列を生成し、同期指標生成部はテキスト又はセンサ時系列の特徴と合成する。閾値は無条件境界に基づく保守設定とし、鍵素材はTRNGから取得、KDFでチャネルIDと素数リズム派生量を合成してセッション鍵を導出する。OS層はコンテナ／プロセス単位で鍵を割当・監査する。具体的手順の一例： Input: 連続ストリームX, CHID, TRNG/PUF 1: R ← Preprocess(X; 窓 W, 差分, 自己相関ラグ L, モジュラ基数 m のうち少なくとも二つ) 2: {score_i, Delta} ← GD-Attention(R, 特徴列; k, B) 3: if ∃ 区間 [t_0, t_0 + tau] s.t. S(t) >= E_upper(t) + Delta then 4: salt := (R || CHID), ikm := (TRNG || PUF) 5: SK ← KDF(ikm, salt); OS層へ割当・監査 6: else 再試行／閾値再校正；タンパ検知時は即時消去。

【００６１】

（ハードウェア中心）エッジデバイスにおいて、アナログ前段で帯域選択とＡ／Ｄ変換を行い、デジタル後段を小規模ＡＳＩＣで実装する。ＰＵＦ応答を鍵素材に用い、タンパ検知時には後段ロジックがゼロ化信号を発行し、鍵素材・セッション鍵を即時消去する。副チャネル対策として電力平坦化とタイミングランダマイズを併用する。

【００６２】

（GD-Attention統合）自然言語入力に対し、GD-Attention部がスパース選択を行い、唯一性・有限エネルギー制約を満たす経路のみを同期候補とする。素数リズム派生量を正則化項として同化し、誤同期率を所定上限以下に抑制する。同期成立時にのみＫＥＭハンドシェイクを開始する。

【００６３】

（量子対応）バックエンドで格子ベースＫＥＭを採用し、同期成立イベントをＫＥＭ開始条件とする構成とする。高セキュリティ要求の設備間ではＱＫＤを併用し、同期イベントのメタデータ（時刻・チャネルＩＤ）を鍵配送側の関連付け情報として用いる。

【００６４】

（理論パラメタの選択）閾値設定において、運用方針により（ｉ）リーマン型偏差エンベロープを採用するモード、（ｉｉ）零点密度境界・零点自由領域に基づく無条件上界を採用するモードを切替可能とする。いずれのモードでも同期検出の保守性が担保される。

【００６５】

（分散環境）多数のノードで意味チャネルを分散管理し、各ノードのＰＵＦ応答と局所素数リズム派生量を用いて部分鍵を生成、閾値秘密分散で集約してセッション鍵を確立する。ノード欠損時も所定の閾値を満たせば復元可能である。

【００６６】

本発明の一実施態様として、以下の代表的パラメータセットを例示する（数値は説明のための一例であり、本発明はこれらに限定されない）。

・窓長 W＝〇〇〇

・自己相関ラグ L＝〇〇〇

・モジュラ写像の基数 m＝〇〇〇（素数）
・選択集合の上限 k＝〇〇〇
・有限エネルギー上限 B＝〇〇〇（正規化単位；重み絶対値総和が B 以下）
・唯一性マージン δ＝〇〇〇（＝〇〇〇）
・連続時間閾値 τ＝〇〇〇ms
・TRNG エントロピー 〇〇〇 bit 以上, PUF 安定度 ビット誤り率 10^-3 以下（補正後）
受理規則は、S（x）が E_upper（x）＋δ以上である状態が τ 以上の時間連続して成立したとき同期成立とする。同期成立イベントの都度、salt＝（R と CHID の連結）、**ikm＝（TRNG と PUF の連結）**を用いて KDF によりセッション鍵 SK を導出し、当該導出を観測路又は PUF 応答に強制バインドする。SK は CHID 単位で割当・ローテーション・失効・即時消去を一体的に行い、監査ログには {CHID, H(R), TRNG_ID, PUF_ID, Δt} を必須項目として記録する。
なお、W∈[64,4096]、L∈[1,64]、m は素数、k は実装資源に応じて設定、B・δ・τ は校正により決定され、装置構成や使用環境に応じて適宜変更可能である。
【００６７】
図１は、本発明に係るシステム全体（１００）の機能的構成を示すブロック図である。上段には、数論系列生成部１１０と GD-Attention 部１２０とを含む同期系が配置され、当該系列処理の結果に基づいて同期指標生成部１３０が同期指標Ｓ（１３１）を算出し、閾値設定部１３２が偏差エンベロープＥ（１３３）を設計し、同期判定部１４０が同期成立の有無を判定する構成である。中段には、真正乱数生成器（ＴＲＮＧ）１５０およびＰＵＦ応答取得部１５１からの入力を受ける鍵導出部（ＫＤＦ）１６０が設けられ、導出されたセッション鍵ＳＫ１６１が意味資源管理部１７０に供給される。意味資源管理部１７０は、チャネルＩＤ１７１に基づく割当・隔離、監査ログ１７２、状態機械１７３、ならびに失効・消去制御１７４を備え、鍵資源をオペレーティングシステム層として一元管理する。右側には、副チャネル対策部１８０（電力平坦化１８１、タイミングランダマイズ１８２、マスキング１８３、ノイズ注入１８４）および耐タンパ処理部１９０（タンパ検知１９１、即時消去１９２）が配置され、鍵および内部状態の漏えい・改ざんを抑止する。さらに、プロトコル連携部２１０（ＰＱ-ＫＥＭ２１１、ＰＱ署名２１２、ＱＫＤインタフェース２１３）およびリモートアテステーション部２３０（証明生成器２３１）を備え、外部プロトコルと整合的に鍵確立・真正性証明を行う。下段のハイブリッド回路２００は、アナログ前段２０１から２０４とデジタル後段２０５とを介して、指標演算器２０６および閾値判定器２０７により上記同期判定を回路レベルで支持する。実線矢印はデータ又は同期の流れ、点線矢印は制御又はポリシの流れ、二重線は鍵素材又は鍵の流れをそれぞれ示す。なお、図中のハッチングは層の区別（ＯＳ層・暗号層・半導体層）を表すにとどまり、本発明の技術的範囲を限定するものではない。
【００６８】

図２は、数論系列と GD-Attention とを用いて同期指標Ｓ（１３１）を生成し、偏差エンベロープＥ（１３３）により判定基準を設定する処理パイプラインを示すブロック図である。数論系列生成部１１０は、素数列 p_n、素数間隔 g_n、マンゴルト関数Λ（ｎ）、チェビシェフ関数θ（ｘ）・φ（ｘ）等からなる特徴系列を生成し、窓処理・差分・自己相関・モジュラ写像等（１１５）により所望の統計的性状を付与する。GD-Attention 部１２０は、唯一性制約器１２１および有限エネルギー制約器１２２に基づき、非線形で選択的な特徴抽出を行い、雑音・擾乱に対して頑健な表現を得る。同期指標生成部１３０は、上記抽出結果に基づいて同期指標Ｓを算出し、閾値設定部１３２は、理論境界に基づく偏差エンベロープＥ（ＲＨ型又は無条件境界の少なくとも一方）を設定して誤同期を抑制する許容帯を規定する。同期判定部１４０は、ＳがＥおよび設定閾値を満足したときに同期成立イベントを生成し、当該イベントを図１の意味資源管理部１７０およびプロトコル連携部２１０に通知する。これにより、同期に依存する後続の鍵導出および資源割当を一貫して起動できる。数論系列と GD-Attention により同期指標 S を生成し、偏差エンベロープ E で判定する処理パイプラインを示す。数論系列生成部 110 は p(n), g(n), Lambda(n), theta(x), psi(x) からなる特徴系列を生成し、窓処理・差分・自己相関・モジュラ写像で加工する。GD-Attention 部 120 は唯一性制約と有限エネルギー制約に基づき非線形選択を行う。同期指標生成部 130 は S を算出し、閾値設定部 132 は無条件上界に基づく E を設定する。同期判定部 140 は S が E および設定閾値を満たしたとき同期成立イベントを生成する。

【００６９】

図３は、真正乱数およびＰＵＦ応答に、チャネル情報および素数リズム由来の派生量をバインドして鍵導出を行う構成を示すブロック図である。ＴＲＮＧ１５０とＰＵＦ応答取得部１５１の出力は、鍵導出部１６０に入力され、当該鍵導出部１６０は、チャネルＩＤ１７１および数論系列生成部１１０の加工量（１１５）に由来する派生量をドメイン分離子又はソルトとして付加することにより、観測路・素子個体差・チャネル識別子に強制的に結び付けられた鍵素材を生成する。導出結果はセッション鍵ＳＫ１６１として確定され、図１の意味資源管理部１７０に引き渡されて割当・監査・失効管理の対象となる。かかる構成により、ＰＵＦ／観測路入力を欠く第三者は同一鍵を再現できず（強制参加性）、リプレイ・複製・抽出に対して高い耐性を示す。また、鍵導出部１６０は、反復カウンタやコンテキスト文字列を含む既存のＫＤＦ（例えばＨＫＤＦ）を基盤として実装可能であり、複数セッションへの拡張および将来の耐量子プロトコル（図１の２１０）との連携に容易に適応できる。

【００７０】

図４は、本発明に係るＯＳ層の意味資源管理の基本構成を示すブロック図である。セッション鍵ＳＫ１６１は、意味資源管理部１７０に入力され、同部はチャネルＩＤ１７１に基づき鍵資源を論理チャネル毎に割当てるとともに、プロセス間の隔離を実現する。監査ログ１７２は、鍵の生成・配布・使用・失効・

消去に係るイベントを時系列に記録し、後述のリモートアテステーション部２３０との整合性確認に供される。状態機械１７３は、図５に示すライフサイクル状態（未同期、鍵確立、利用中、失効、消去）を管理し、ポリシ条件の成立時に遷移を駆動する。失効・消去制御１７４は、耐タンパ処理部１９０のタンパ検知１９１、又は副チャネル対策部１８０の逸脱検知に応じて、当該チャネルに属する鍵と関連メタデータを不可逆にゼロ化する。右側のプロセス１から３はユーザ空間又はカーネル空間の代表例であり、各プロセスはチャネルＩＤ１７１を介して必要最小限の鍵マテリアルへの参照権限のみを付与される。なお、１７０は鍵の有効期間、回数制限、端点バインディング（デバイス識別子、ＰＵＦ由来特徴等）をポリシとして保持し、違反時には１７４により直ちに失効又は消去を実行する構成である。意味資源管理部は、CHID、salt 構成要素（R のハッシュ識別子）、ikm 構成要素（TRNG ブロック識別子、PUF 応答識別子）、および時刻スタンプ Delta_t を監査ログの必須フィールドとして記録する。これにより、リモートアテステーション要求に応じて、同期成立イベントと鍵確立の対応関係を提示可能とする。

【００７１】

図５は､セッション鍵のライフサイクル管理手順を状態遷移図として示したものである。初期状態「未同期」から、「同期判定部１４０の成立」により「鍵確立」へ遷移し､鍵導出部１６０によってセッション鍵ＳＫ１６１が確定される。その後､ＯＳ層の意味資源管理部１７０の配布処理により「利用中」へ遷移する。「利用中」状態において、（ｉ）監査ログ１７２に記録された使用回数・期間の超過、（ｉｉ)副チャネル対策部１８０又は耐タンパ処理部１９０による逸脱検知／タンパ検知、（ｉｉｉ）管理者又はプロトコル連携部２１０による失効指示、の少なくとも一つが成立した場合、「失効」へ遷移する。「失効」からは、失効・消去制御１７４の指示により「消去」へ不可逆に遷移し、鍵マテリアルおよび関連メタデータは即時にゼロ化され復元不能となる。かかる構成により、鍵のライフサイクルは時間方向に単調であり、いかなる状態からも「消去」以降への逆遷移は許容されない。状態機械は、「未同期」から「確立」への遷移条件として、[0029A] の判定規則「S(x) >= E_upper(x) + delta が tau 連続」を満たすことを要求する。「利用中」から「失効」への遷移は、(i) 監査ログに記録された使用回数または使用期間の超過、(ii) 副チャネル対策部または耐タンパ処理部による逸脱検知、(iii) 管理者またはプロトコル連携部による失効指示、の少なくとも一つにより駆動される。

【００７２】

図６は、同期検出のためのハイブリッド半導体回路２００の一実施形態を示すブロック図である。アナログ前段は、入力信号のＳＮ比と帯域特性を所定範囲に整える増幅器２０１、帯域選択２０２、およびＡ／Ｄ変換２０３を含む。増幅器２０１は可変利得構成としてもよく、入力振幅の揺らぎに対して飽和と量子化ビットの不足を同時に回避する。帯域選択２０２は、素数リズム由来の特徴周波数帯又は基準チャネル帯域に一致するよう設計され、不要帯域の雑音成

分を抑圧する。Ａ／Ｄ変換２０３は、前段で規定されたダイナミックレンジに対し量子化雑音が指標演算に影響しない分解能で動作する。デジタル後段２０５は、前記ディジタイズ信号から指標演算器２０６に必要な特徴量（差分・自己相関・モジュラ写像等）を抽出し、指標演算器２０６は同期指標Ｓ（１３１）を算出する。閾値判定器２０７は、図２の閾値設定部１３２が与える偏差エンベロープＥ（１３３）と前記Ｓとを比較し、同期成立又は非成立の判定結果を出力する。かかる構成により、回路２００はプロセスばらつきや温度変動に対して頑健な前処理を行いつつ、低レイテンシで同期判定を実現する。

【００７３】

図７は、本発明に係る副チャネル耐性およびタンパ耐性のための構成を示すブロック図である。ハードウェア回路２００の出力又は動作に対し、副チャネル対策部１８０は、電力平坦化１８１、タイミングランダマイズ１８２、マスキング１８３、及びノイズ注入１８４を協調的に適用し、外部観測値と内部秘密（鍵及び中間値）との統計的相関を所定閾値未満に低減する。これら各対策は、処理負荷・温度・電源変動等の運用条件に応じて適応的に重み付けされ、監査ログ１７２（図４参照）へ適用履歴が記録される。耐タンパ処理部１９０は、筐体開封、プロービング、クロック／電圧故障注入等の物理的異常をタンパ検知１９１により検出し、検出時には即時消去１９２を発動して鍵保管領域（ＳＫ１６１を含む）に保持されるキー及び関連メタデータを不可逆に消去する。消去は、揮発性メモリに対する複数回書込み又はゼロ化、及び不揮発領域に対する論理的失効と上書きを含む少なくとも一つの手段により実行される。かかる構成により、本発明は観測ベース及び物理侵襲ベースの攻撃双方に対して多層的防御を提供する。

【００７４】

図８は、本発明に係る鍵確立プロトコルの一例を時系列で示すシーケンス図である。装置Ａ及び装置Ｂは、図２の同期判定部１４０により「同期成立」イベントが生成された後、プロトコル連携部２１０の制御の下で、（ｉ）耐量子鍵カプセル化機構（ＰＱ‐ＫＥＭ２１１）によるエフェメラル鍵素材の確立、及び（ｉｉ）耐量子署名（ＰＱ署名２１２）による相互認証を実行する。さらに、両装置間に量子鍵配送路が利用可能な場合、ＱＫＤインタフェース２１３により生成される物理層鍵素材を並行取得し、ＫＤＦ１６０における鍵導出のソルト又は追加エントロピーとして混合することができる。上記交換の完了後、セッション鍵ＳＫ１６１は装置Ａ及び装置Ｂで一致し、図４の意味資源管理部１７０により各チャネルＩＤ１７１へ割当てられる。なお、メッセージ順序や再送制御は実装に応じて変更可能であり、ＰＱ‐ＫＥＭ２１１及びＰＱ署名２１２の具体方式はＮＩＳＴ標準等の公知方式から適宜選択可能である。

【００７５】

図９は、数論系列生成部１１０の内部構成を示すブロック図である。まず、素数列 p_n（１１１）及び連続素数間隔 g_n（１１２）を生成するとともに、マンゴルト関数Λ（ｎ）（１１３）及びチェビシェフ関数θ（ｘ）、ψ（ｘ）（１１４）を計算する。次いで、加工部１１５は、（ｉ）所定長Ｗの窓関数による

畳込み又は平均化、（ｉｉ）一次又は高次の差分化、（ｉｉｉ）自己相関又は相互相関の評価、及び（ｉｖ）所定法則に基づくモジュラ写像の少なくとも一つを実行し、有限エネルギー条件を満たす特徴系列を生成する。生成された素数リズム系列は、図２のGD-Attention部１２０に入力され、唯一性制約器１２１及び有限エネルギー制約器１２２の下で選択的に利用される。かかる構成により、理論数論に基づく非定常だが規則的な時系列構造を、同期指標Ｓ（１３１）の計算に適した形で抽出でき、雑音環境下でも頑健な同期検出が可能となる。

【００７６】

図１０は、同期指標Ｓ（１３１）の時間又はサンプル位置ｘに対する変動と、閾値設定部（１３２）が生成する偏差エンベロープＥ（１３３）との関係を示す概念図である。Ｅは、少なくとも（ｉ）理論境界に基づくＲＨ型上包絡、（ｉｉ）仮定を置かない無条件境界の二種のうち一つ以上として与えられ、ＳがＥの上側又は所定帯域内に入るときに「受理」、外れるときに「棄却」と判定される。図中の破線・点線はそれぞれ上記二種の包絡の一例を示し、鎖線は固定閾値の一例を示す。閾値設定部（１３２）は、期待誤警報率と見逃し率のトレードオフを所望レベルに調整するため、包絡の幅、時間窓長、及び平滑化係数をパラメータとして出力する。かかる構成により、環境雑音やモデル不確実性の下でも、同期判定部（１４０）は保守的かつ一貫した判定を実現できる。なお、Ｅの具体式や推定法は実装に依存し、図示は本発明の技術的範囲を限定しない。

【００７７】

図１１は、分散環境における鍵確立の一態様を示すブロック図である。ノード１から４は、各々が保持する部分鍵２２１を提供し、これらは閾値秘密分散部２２２で合成される。２２２は、有限体上の補間（例えばラグランジュ補間）等の公知手法により、ｎ個のうち少なくともｔ個の部分鍵が揃ったときのみセッション鍵ＳＫ１６１を復元する。復元されたＳＫ１６１は、意味資源管理部１７０に引き渡され、チャネルＩＤ１７１に基づく割当、監査ログ１７２への記録、状態機械１７３によるライフサイクル管理、及び失効・消去制御１７４の対象となる。ノードの欠損や一部の漏えいが生じても、ｔ未満の部分鍵からはＳＫ１６１に関する情報が統計的に得られないため、可用性と秘匿性の双方が確保される。なお、ノードは物理デバイス、ＴＥＥ、又はプロセス境界のいずれであってもよく、２２２の具体方式はシャミア方式等に限られない。

【００７８】

図１２は、ＣＭＯＳベースのＡＳＩＣ又はＦＰＧＡにおける実装形態の一例を示す配置図である。上段には、真正乱数生成器（ＴＲＮＧ１５０）、ＰＵＦ応答取得部１５１、及び鍵導出部（ＫＤＦ１６０）の各ＩＰを配置し、相互は内部バスで接続される。中段には、ＯＳ意味資源管理部１７０、副チャネル対策部１８０、及び耐タンパ処理部１９０を配置し、１７０から各処理部へは制御線（点線）が、１８０・１９０から鍵保護領域へは監視・ゼロ化の制御線がそ

れぞれ配線される。右側外周には、セキュアエレメント／ＴＰＭおよびリモートアテステーション部２３０、ホストインタフェースを介するプロトコル連携部２１０を配置し、外部装置との鍵共有・認証を行う。鍵素材・鍵（ＳＫ１６１を含む）の流れは二重線で示され、ゼロ化経路は１９０から１７０／鍵記憶域へ直接配線される。電源・クロックは分離ドメインとして設計してもよく、１８０の電力平坦化１８１は電源ネットワークに近接配置される。ＰＵＦ１５１は配線寄生の影響を低減するためＫＤＦ１６０に近接させ、１７０は大容量メモリとの隣接配置により監査ログ１７２の書込み遅延を抑制する。以上の構成により、既存プロセスノードで段階的に機能拡張可能であり、ＦＰＧＡ実装では１８０・１９０のパラメータを運用時に再設定することで、攻撃モデルに応じた適応的防御が実現される。

【００７９】

以上の実施例は一例であり、本発明の範囲はこれらに限定されない。各構成は目的・コスト・信頼性要件に応じて置換・追加・削減が可能である。

【産業上の利用可能性】

【００８０】

本発明は、意味的同期の検出を起点として暗号資源をＯＳ資源として管理し、半導体実装まで一体化する基盤であるため、以下の分野に広く適用可能である。

【００８１】

（１）サイバーセキュリティ／ゼロトラスト：端点・ゲートウェイ・ＤＣ間で同期成立イベントをハンドシェイク条件として用いることで、認証と鍵配送の整合性を高め、傍観者による事後再現を実質的に不能化できる。

【００８２】

（２）ＩｏＴ／エッジ機器：小規模ＡＳＩＣ／ＦＰＧＡ実装により、ＰＵＦ・ＴＲＮＧと組み合わせた軽量な鍵確立を実現し、センサネット・スマートホーム・産業機器の長期運用に適する。

【００８３】

（３）データセンタ／クラウド：意味チャネル単位の鍵ライフサイクル管理により、マルチテナント環境での隔離性と監査可能性を両立し、規制準拠（ログ保全・鍵消去証跡）を支援する。

【００８４】

（４）ＡＩ／モデル提供基盤：学習データ流・推論チャネルごとの同期判定で鍵を割当て、機密プロンプトやモデル重みの漏洩を抑止。GD-Attention 統合により意味的一貫性を保ったアクセス制御が可能。

【００８５】

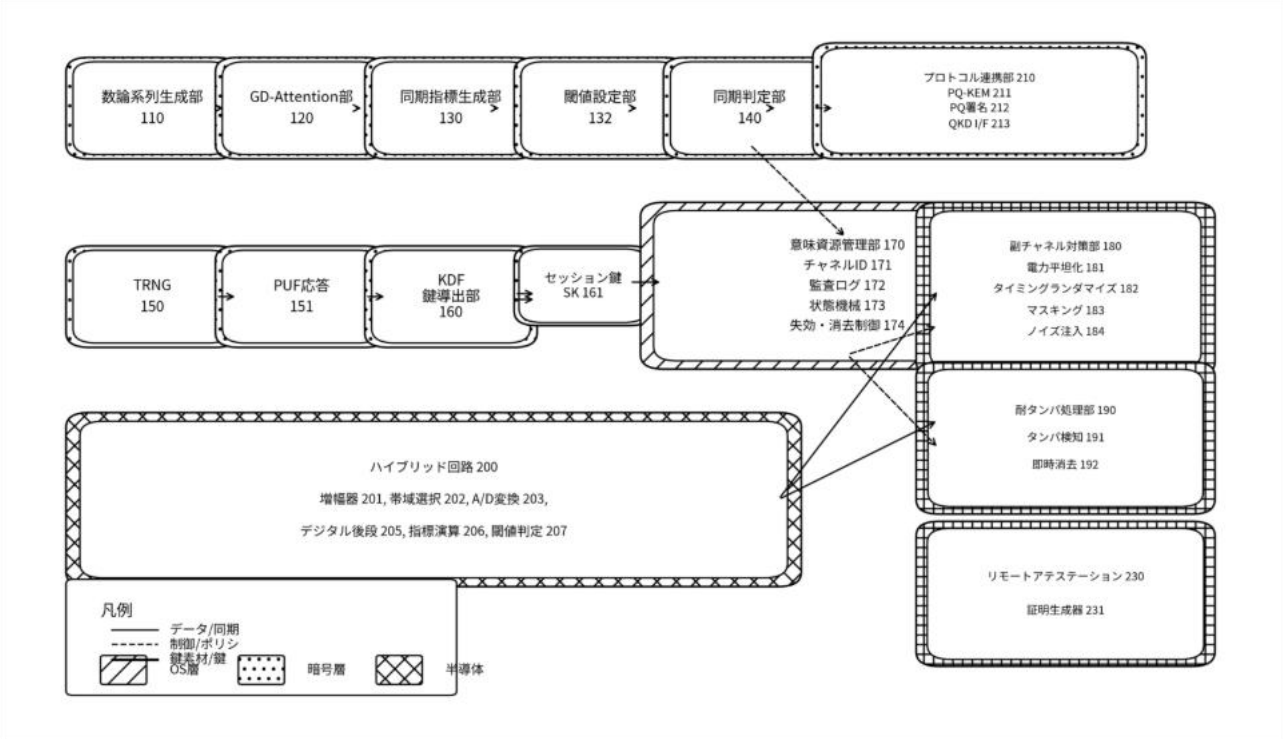
（５）金融／決済：素数リズム由来の同期指標と耐量子ＫＥＭの併用により、決済端末～バックエンド間の長期耐性を確保しつつ、リアルタイム失効・即時消去で事故影響を局所化できる。

【００８６】

（６）医療・公共・インフラ：強制参加性により患者データ・運用データの再現

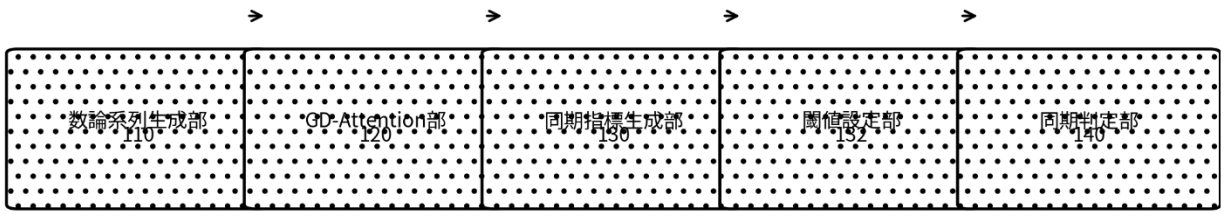
を困難化し、設備監視や電力・交通等の制御通信の安全性を向上させる。
【００８７】
（７）自動車／ロボティクス：ハイブリッド回路実装と副チャネル対策により、ＥＣＵ間通信やファーム更新の改ざん検出・鍵保護に有用。リアルタイム要件下でも状態機械で鍵運用を制御できる。
【００８８】
（８）通信（５Ｇ／６Ｇ、衛星）：同期イベントをリンク層～上位プロトコルの共通トリガとして扱い、端末～基地局～衛星で一貫した鍵管理を実現する。
【００８９】
（９）量子時代対応：格子等の耐量子暗号とＱＫＤに両対応し、将来の量子計算環境でも鍵配送・認証を継続可能である。
【００９０】
（１０）半導体知財・製品化：既存ＣＭＯＳプロセスでＡＳＩＣ／ＩＰコア化が可能で、セキュアエレメント、ＴＰＭ、ＨＳＭ等への組込みや、ファームウェア更新による段階的機能拡張に適する。
【００９１】
さらに、同期閾値の設計はリーマン型評価または無条件境界のいずれでも運用でき、理論仮定に依存しない保守構成を選択可能であるため、長期運用・国際規格移行期における実装リスクを低減できる
【００９２】
以上より、本発明はエッジからクラウド、古典から量子連携までの広範な産業領域で、セキュリティ、監査性、電力効率（有限エネルギー制約による）を同時に満たす基盤技術として有用である。
【符号の説明】
【００９３】
110：数論系列生成部／入力特徴取得
115：加工部（窓畳込み・差分・自己相関・モジュラ写像）
131：同期指標 S
132：閾値設定部
133：偏差エンベロープ E（E_upper を含む）
150：TRNG（真正乱数生成器）
151：PUF 応答取得部
160：鍵導出部（KDF）
161：セッション鍵 SK
170：意味資源管理部（OS 層）
171：チャネル ID（CHID）
172：監査ログ
173：状態機械（生成→利用→失効→消去）
174：失効・消去制御
180：副チャネル対策部（181：電力平坦化／182：タイミングランダマイズ／183：

マスキング／184：ノイズ注入）
190：耐タンパ処理部（191：タンパ検知／192：即時消去）
200：ハイブリッド回路（201：増幅器／202：帯域選択／203：A/D／205：デジタル後段／206：指標演算器／207：閾値判定器）
210：耐量子暗号ブロック（総称）
211：PQ-KEM
212：PQ署名
213：QKDインタフェース
221：部分鍵
222：秘密分散（t/n）
230：リモートアテステーション部（遠隔検証）
【書類名】要約書
アプリケーション層とＯＳ／半導体実装が疎結合であるため、意味的同期イベントと鍵確立との因果対応が不明確であり、傍観者による再現や副チャネル・タンパ攻撃に脆弱であった。また、耐量子ＫＥＭやＱＫＤとの統合も煩雑であった。本発明は、素数系列等の数論系列から得られるリズム派生量Ｒと入力特徴に対し、GD-Attention により非線形選択を行って同期指標Ｓを算出し、無条件包絡Ｅに基づく受理規則「Ｓ≧E_upper＋δ」がτ時間連続して成立したとき同期成立と判定する。この成立をトリガとして、ＴＲＮＧ／ＰＵＦとＫＤＦによりセッション鍵ＳＫを導出し、ＣＨＩＤ単位でＯＳ資源として割当・監査・即時消去まで一体的に管理する。実装は副チャネル対策・耐タンパ機構を備え、ＰＱ-ＫＥＭ／署名およびＱＫＤと連携可能である。
【選択図】図１
【書類名】　　図面
【図１】



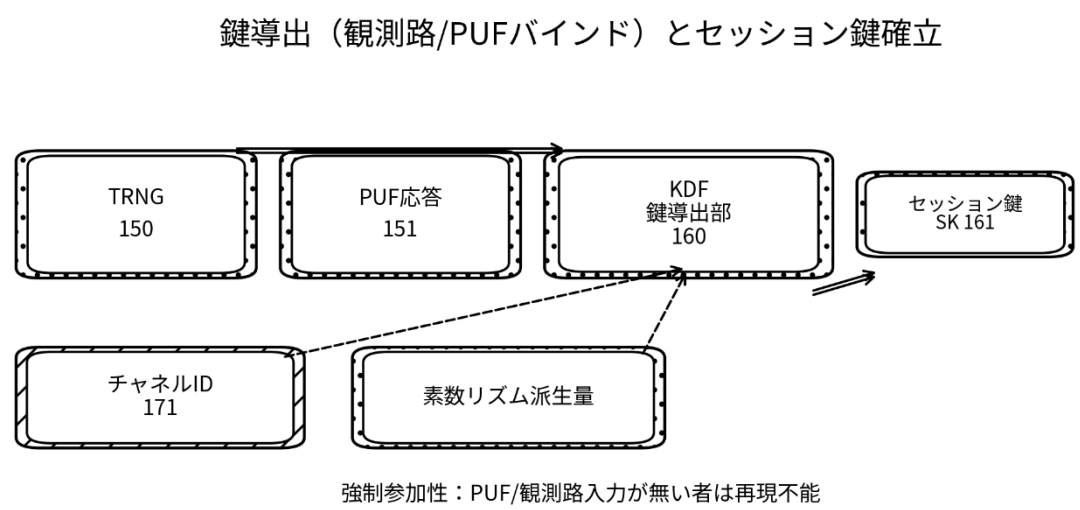
【図２】

同期指標生成パイプライン（素数リズム＋GD-Attention）

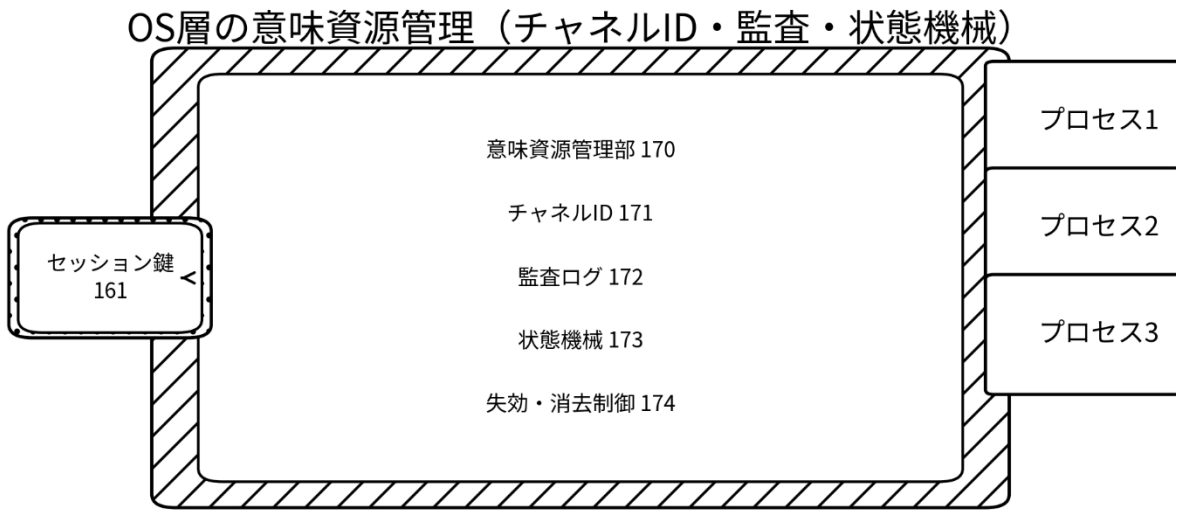


素数リズム：p_n, g_n, Λ, θ, ψ＋加工
非線形選択／唯一性／有限エネルギー

【図３】

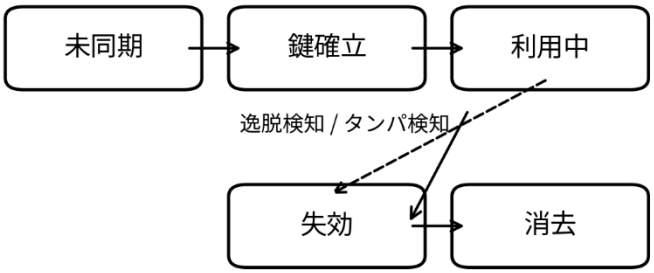

鍵導出（観測路/PUFバインド）とセッション鍵確立
TRNG
150
PUF応答
151
KDF
鍵導出部
160
セッション鍵
SK 161
チャネルID
171
素数リズム派生量
強制参加性：PUF/観測路入力が無い者は再現不能

【図４】


OS層の意味資源管理（チャネルID・監査・状態機械）
意味資源管理部 170
チャネルID 171
監査ログ 172
状態機械 173
失効・消去制御 174
セッション鍵
161
プロセス1
プロセス2
プロセス3

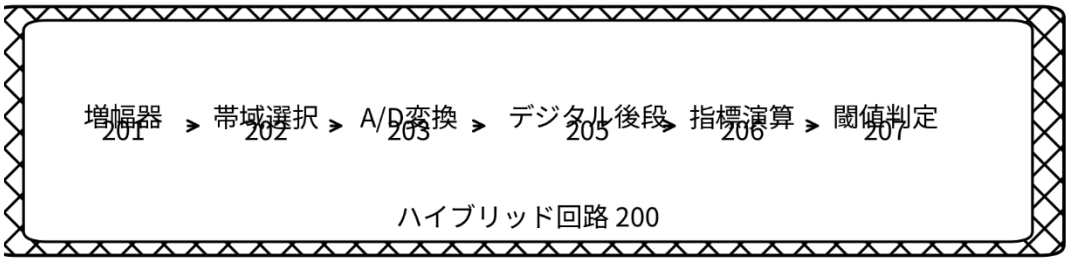
【図５】

鍵ライフサイクル状態遷移（未同期→確立→利用→失効→消去）

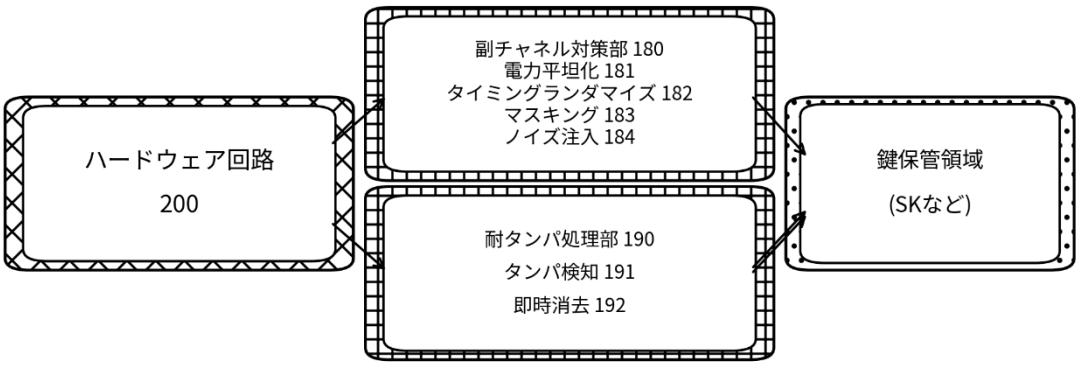


【図６】

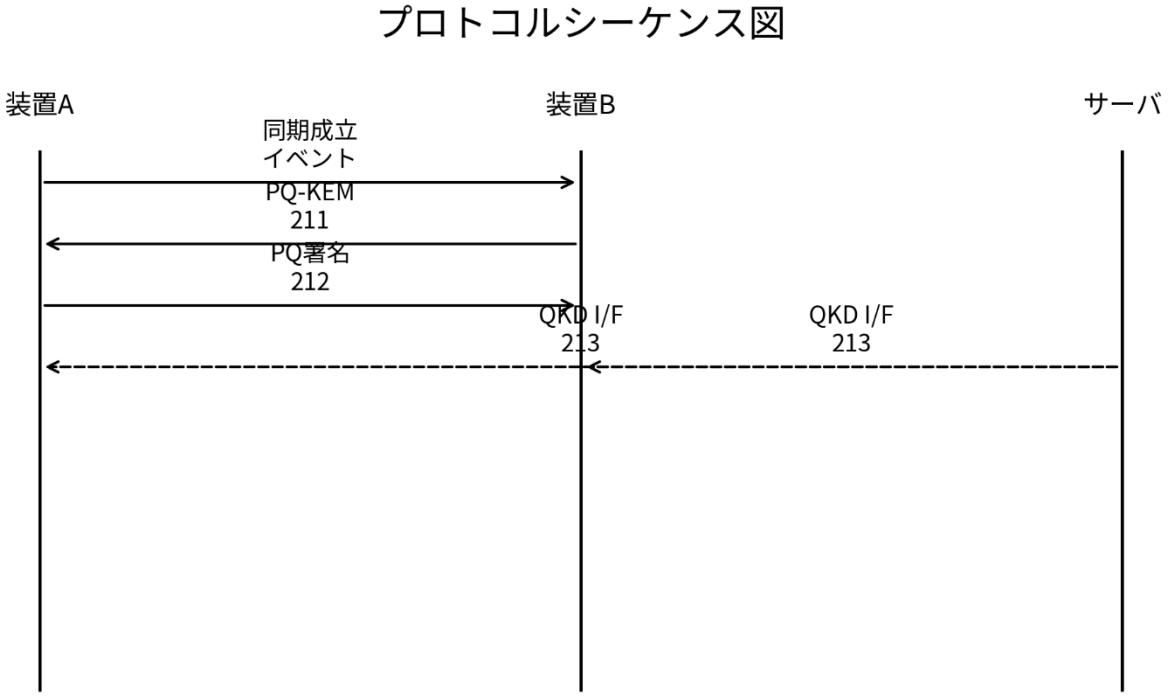
ハイブリッド半導体回路（アナログ前段＋デジタル後段）



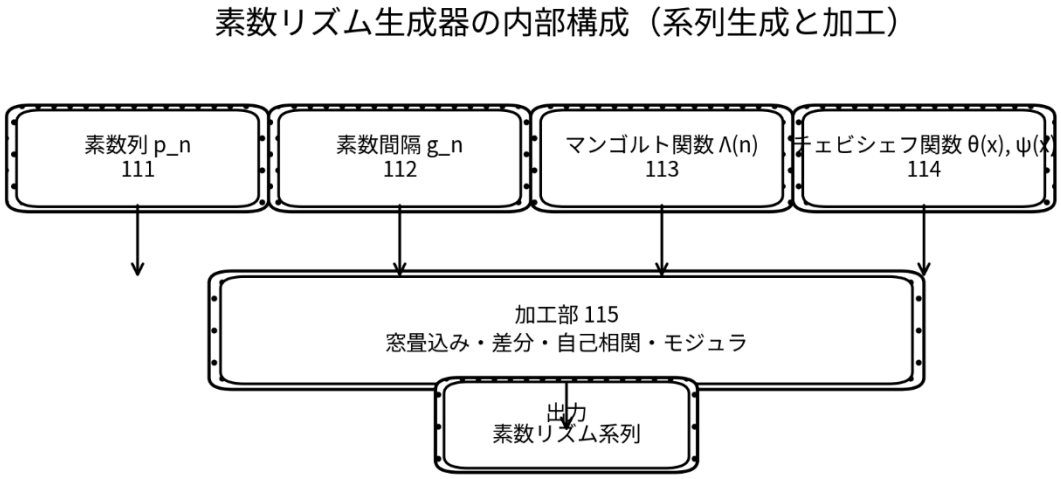
【図７】


副チャネル対策とタンパ検知・即時消去
副チャネル対策部 180
電力平坦化 181
タイミングランダマイズ 182
マスキング 183
ノイズ注入 184
ハードウェア回路
200
鍵保管領域
(SKなど)
耐タンパ処理部 190
タンパ検知 191
即時消去 192
観測相関を確率的に低減／タンパ検知で即時ゼロ化

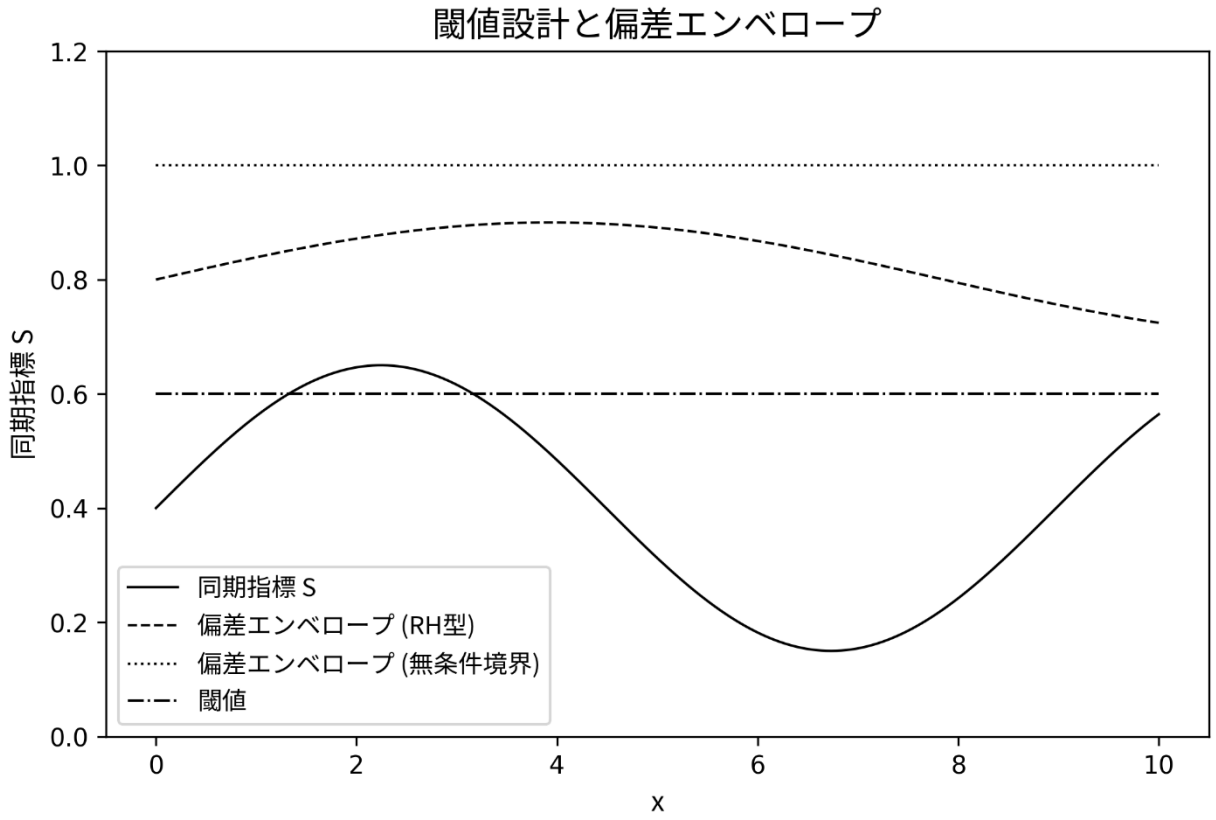
【図８】


プロトコルシーケンス図
装置A
装置B
サーバ
同期成立
イベント
PQ-KEM
211
PQ署名
212
QKD I/F
213
QKD I/F
213

【図９】

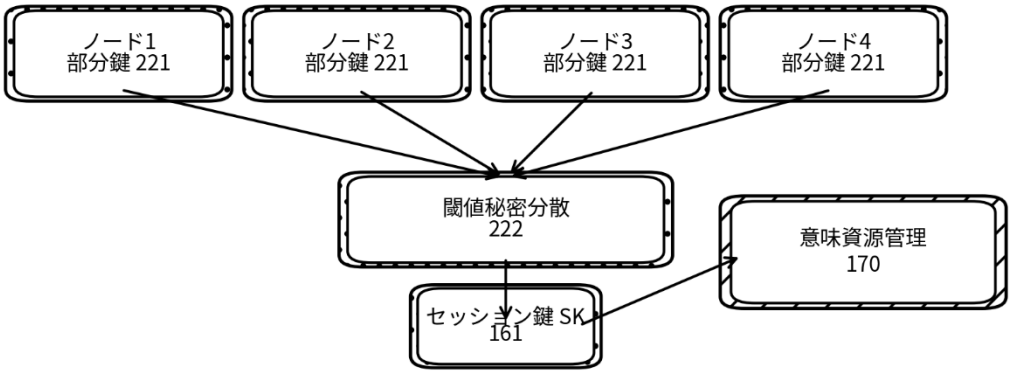

素数リズム生成器の内部構成（系列生成と加工）
素数列 p_n
111
素数間隔 g_n
112
マンゴルト関数 Λ(n)
113
チェビシェフ関数 θ(x), ψ(x)
114
加工部 115
窓畳込み・差分・自己相関・モジュラ
出力
素数リズム系列

【図１０】


閾値設計と偏差エンベロープ
同期指標 S
x
同期指標 S
偏差エンベロープ (RH型)
偏差エンベロープ (無条件境界)
閾値
0.0
0.2
0.4
0.6
0.8
1.0
1.2
0
2
4
6
8
10

【図１１】

分散鍵合成（閾値秘密分散）によるセッション鍵確立



ノード欠損でも t 以上で復元

【図１２】

ASIC/FPGAによる実装形態例とIPブロック配置