PROVISIONAL PATENT APPLICATION

ADAPTIVE ARTIFICIAL INTELLIGENCE SYSTEM FOR DYNAMIC CRYPTOGRAPHIC PROTOCOL ORCHESTRATION IN MULTI-PARTY FINANCIAL TRANSACTIONS

Inventor: Brian James Rutherford

Docket No.: RUTHERFORD-020-PROV

BACKGROUND OF THE INVENTION

[0001] **Field of the Invention.** This invention relates to artificial intelligence systems for cryptographic protocol management, specifically to adaptive AI-driven selection and orchestration of multiple privacy-preserving cryptographic protocols including zero-knowledge proofs (ZKP), homomorphic encryption (HE), and secure multi-party computation (MPC) for financial transaction processing in defensive cybersecurity platforms.

[0002] **Description of Related Art.** Financial institutions process diverse transaction types requiring different privacy and performance characteristics. Current systems employ static cryptographic approaches: either zero-knowledge proofs for all private transactions, homomorphic encryption for all encrypted computations, or secure multi-party computation for all collaborative operations. These single-protocol approaches create inefficiencies—using computationally expensive ZKP for simple transactions wastes resources, while using lightweight encryption for high-value transactions creates security vulnerabilities.

[0003] Existing blockchain systems like DERO implement homomorphic encryption uniformly across all transactions. JPMorgan's Quorum uses static privacy configurations. Microsoft SEAL and IBM HElib provide homomorphic encryption libraries but require manual protocol selection. No existing system provides intelligent, automated selection among multiple cryptographic protocols based on real-time transaction analysis.

[0004] The fundamental problem is that different financial transactions have vastly different requirements: micropayments need speed over privacy, international transfers need regulatory compliance with selective disclosure, inter-bank settlements need collaborative computation, and high-value transactions need maximum privacy. Using one cryptographic approach for all creates either security vulnerabilities or performance bottlenecks.

[0005] Furthermore, regulatory requirements vary by jurisdiction, transaction amount, and party types. A transaction between two retail customers has different privacy requirements than one involving a sanctioned entity. Current systems cannot dynamically adapt their cryptographic approach based on these multifaceted requirements.

BRIEF SUMMARY OF THE INVENTION

[0006] The present invention provides an adaptive artificial intelligence system that dynamically orchestrates multiple cryptographic protocols for financial transactions. The system analyzes each transaction's characteristics in real-time and intelligently selects the optimal combination of zero-knowledge proofs, homomorphic encryption, and secure multi-party computation to balance privacy, performance, and regulatory compliance.

[0007] The AI system employs a multi-dimensional decision framework considering: transaction attributes (amount, parties, type, urgency), regulatory context (jurisdiction, reporting requirements, threshold triggers), privacy requirements (counterparty relationships, data sensitivity, audit needs), computational resources (available processing power, network latency, queue depth), and historical patterns (previous similar transactions, learned optimizations, performance outcomes).

[0008] Unlike static systems, the invention continuously learns from transaction outcomes, adjusting its selection criteria based on actual performance metrics, regulatory feedback, and security events. This creates an evolving system that improves over time, adapting to new transaction patterns, regulatory changes, and threat landscapes.

DETAILED DESCRIPTION OF THE INVENTION

[0009] **Core Innovation: Adaptive AI Orchestration Layer.** The adaptive AI orchestration layer represents the primary innovation, employing multiple AI techniques working in concert. This layer operates as part of a comprehensive Mathematical Woven Responsive Adaptive Swarm Platform (MWRASP) for defensive cybersecurity applications.

[0010] **Transaction Analysis Engine.** Neural networks classify incoming transactions across multiple dimensions simultaneously. Rather than simple categorization, the system extracts feature vectors representing privacy needs, performance requirements, regulatory constraints, and risk factors. These vectors feed into the protocol selection matrix. The AI agents within this engine operate as defensive security agents, continuously monitoring for threat patterns while optimizing cryptographic protocol selection.

[0011] **Protocol Selection Matrix.** A reinforcement learning system maintains a constantly updating matrix mapping transaction feature vectors to optimal protocol combinations. The matrix considers not just individual protocol performance but synergistic effects when protocols are combined. For example, using lightweight ZKP for transaction validation while employing HE for amount verification. This matrix forms part of the MWRASP's adaptive response mechanism.

[0012] **Dynamic Orchestration Controller.** The controller implements the selected protocol configuration, but uniquely monitors execution in real-time. If performance degrades or new information emerges (such as a party being flagged), the controller can switch protocols mid-transaction, migrating from one cryptographic approach to another without restarting. This capability is essential for the defensive AI agent platform's ability to respond to emerging threats.

[0013] **Learning Feedback Loop.** Every transaction outcome updates the AI models. Success metrics include not just completion time but regulatory acceptance, audit satisfaction, and counterparty trust scores. Failed transactions or regulatory challenges trigger immediate model updates, ensuring the system rapidly adapts to new requirements. This continuous learning mechanism enables the MWRASP platform to evolve its defensive capabilities.

[0014] **Multi-Protocol Coordination Architecture.** The system uniquely coordinates multiple cryptographic protocols simultaneously as part of its comprehensive defensive strategy.

[0015] **Hierarchical Protocol Application.** Rather than applying one protocol to an entire transaction, the system applies different protocols to different aspects. Transaction metadata might use simple encryption, amounts might use homomorphic encryption for computation, party identities might use zero-knowledge proofs, and multi-party validations might use secure computation. This hierarchical approach is coordinated by the MWRASP's AI agent network.

[0016] **Protocol Bridging Mechanisms.** Novel bridging algorithms allow seamless transition between protocols. A transaction can begin with lightweight encryption, escalate to zero-knowledge proofs if suspicious patterns are detected, and invoke secure multi-party computation if multiple institutions need to validate without seeing each other's data. These bridges operate under the control of defensive AI agents.

[0017] **Resource Optimization Engine.** The AI system maintains awareness of computational resources across the network. When homomorphic encryption servers are overloaded, it might route transactions through zero-knowledge proof validators. This dynamic load balancing ensures consistent performance despite varying transaction volumes, a critical feature of the MWRASP platform's scalability.

[0018] **Regulatory Adaptation Framework.** The system includes an AI-driven regulatory adaptation framework operated by specialized compliance AI agents within the MWRASP ecosystem.

[0019] **Jurisdiction Detection.** Machine learning models identify applicable jurisdictions not just from explicit declarations but from transaction patterns, IP addresses, institution codes, and currency types. This multi-factor analysis ensures correct regulatory framework application even when parties attempt to obscure jurisdictions. The detection AI agents operate as part of the defensive monitoring network.

[0020] **Threshold Learning.** Rather than hard-coded thresholds, the system learns regulatory thresholds from patterns. When multiple transactions just below

$10,000 occur, the system recognizes potential structuring and adjusts its privacy approach accordingly. This adaptive threshold detection is managed by specialized AI agents focused on regulatory compliance.

[0021] **Compliance Proof Generation.** The AI system automatically generates cryptographic proofs of compliance tailored to each regulator's requirements. These proofs demonstrate adherence to regulations without revealing unnecessary transaction details. The proof generation is handled by dedicated AI agents within the MWRASP framework.

[0022] **Advanced Selection Heuristics.** The AI system employs sophisticated heuristics beyond simple rule-based selection, coordinated by the MWRASP's swarm intelligence capabilities.

[0023] **Temporal Pattern Analysis.** Transaction timing influences protocol selection. Rapid sequential transactions might indicate automated trading requiring lightweight protocols, while isolated high-value transfers might warrant maximum privacy protection. The temporal analysis AI agents continuously monitor transaction patterns for anomalies.

[0024] **Relationship Mapping.** The system maintains an encrypted graph of entity relationships, influencing protocol selection. Transactions between long-term partners might use lighter protocols than those between unknown parties. This relationship graph is managed by dedicated AI agents ensuring privacy while enabling intelligent decision-making.

[0025] **Threat-Responsive Adaptation.** When security threats are detected anywhere in the network, the system automatically adjusts protocol selection globally. A detected attack on homomorphic encryption systems triggers temporary increased use of alternative protocols. This rapid threat response is coordinated by the MWRASP's defensive AI agent swarm.

[0026] **Economic Optimization.** The AI considers economic factors including computational costs, network fees, and opportunity costs of delayed transactions. This ensures protocol selection optimizes not just technical metrics but economic outcomes. Economic optimization AI agents balance cost and security considerations.

[0027] **Implementation Specifics.** The system implements several novel technical approaches within the MWRASP framework.

[0028] **Federated Learning Architecture.** AI models are trained across multiple institutions without sharing sensitive data. Each institution's AI agent contributes learned patterns to a global model while maintaining local privacy. This federated approach enables collaborative defense while preserving institutional sovereignty.

[0029] **Quantum-Resistant Preparation.** The AI system includes quantum threat assessment, automatically increasing post-quantum cryptographic protocol usage as quantum computing capabilities advance. Quantum-resistance AI agents continuously evaluate threat levels and adjust protocols accordingly.

[0030] **Explainable AI Components.** Despite complexity, the system provides clear explanations for protocol selections, essential for regulatory compliance and audit requirements. Explanation AI agents generate human-readable justifications for all cryptographic decisions.

[0031] **Failover Intelligence.** If selected protocols fail, the AI system doesn't just switch to backups but learns from failures, updating models to prevent similar failures. Failover AI agents manage resilience and recovery processes.

[0032] **Transaction Lifecycle Management.** The AI system manages the complete transaction lifecycle through coordinated AI agent actions.

[0033] **Pre-Transaction Analysis.** Before transaction initiation, the system analyzes participant history, regulatory requirements, and network conditions to pre-select optimal protocols. Pre-transaction AI agents prepare the cryptographic environment for optimal performance.

[0034] **Dynamic Mid-Transaction Adjustment.** Unlike static systems, protocols can be changed during transaction processing based on emerging information or changing conditions. Mid-transaction AI agents monitor and adjust protocols in real-time.

[0035] **Post-Transaction Learning.** After completion, the system analyzes outcomes, updating models and adjusting future selections based on observed performance. Post-transaction AI agents extract learnings and update the global knowledge base.

[0036] **Performance Optimization Through Intelligence.** The system achieves performance optimization through intelligent routing rather than raw computational power, a key advantage of the MWRASP approach.

[0037] **Predictive Protocol Caching.** Machine learning models predict likely protocol needs, pre-initializing cryptographic contexts before transactions arrive. Predictive AI agents anticipate needs and prepare resources accordingly.

[0038] **Intelligent Batching.** The AI system groups transactions requiring similar protocols, enabling batch processing efficiencies while maintaining individual transaction privacy. Batching AI agents optimize throughput while preserving security.

[0039] **Network-Aware Routing.** Protocol selection considers network topology, routing transactions through paths optimized for selected cryptographic approaches. Routing AI agents ensure optimal path selection for each protocol configuration.

[0040] **Integration with MWRASP Platform.** The adaptive AI cryptographic orchestration system operates as a core component of the Mathematical Woven Responsive Adaptive Swarm Platform (MWRASP), providing comprehensive defensive cybersecurity capabilities through coordinated AI agent networks. This integration enables enterprise-wide protection against evolving threats while maintaining transaction efficiency and regulatory compliance.

CLAIMS

1. An adaptive artificial intelligence orchestration system for simultaneous coordination of multiple heterogeneous cryptographic protocols in financial transactions comprising:

   a transaction decomposition engine using machine learning to segment each financial transaction into distinct operational components including metadata, monetary values, party identities, and validation requirements;

   a multi-protocol orchestration matrix employing reinforcement learning to simultaneously assign different cryptographic protocols from a set including zero-knowledge proofs, homomorphic encryption, and secure multi-party computation to each segmented component of a single transaction;

   a dynamic protocol bridging controller that maintains cryptographic state consistency while executing different protocols in parallel on different transaction components and enables protocol migration during active transaction processing without rollback;

a continuous learning feedback system that measures actual versus predicted performance of protocol combinations and updates orchestration decisions based on multi-objective optimization including privacy preservation, computational efficiency, regulatory acceptance, and economic cost;

wherein said system operates multiple distinct cryptographic protocols concurrently on different aspects of the same transaction, unlike prior art systems that select a single protocol per transaction;

wherein said orchestration matrix learns optimal protocol combinations through actual transaction outcomes rather than static configuration, distinguishing from rule-based selection systems;

wherein said system performs real-time protocol switching during transaction execution based on emerging information, beyond mere protocol selection at transaction initiation.

2. The system of claim 1, further comprising a hierarchical protocol application mechanism wherein:

transaction metadata, amounts, identities, and validations are separately analyzed;

different cryptographic protocols are applied to each component based on specific requirements;

protocols are coordinated to maintain transaction integrity while optimizing individual components.

3. The system of claim 1, wherein said protocol selection matrix comprises:

a multi-dimensional space mapping transaction features to protocol combinations;

synergy factors calculating combined effectiveness of multiple protocols;

continuous updates based on reinforcement learning from transaction outcomes;

consideration of resource availability and network conditions in real-time.

4. The system of claim 1, further comprising a regulatory adaptation framework wherein:

machine learning models identify applicable jurisdictions from multiple transaction indicators;

the system learns regulatory thresholds and requirements from transaction patterns;

compliance proofs are automatically generated using appropriate cryptographic methods;

protocol selection adapts to jurisdiction-specific requirements without manual configuration.

5. The system of claim 1, wherein said dynamic orchestration controller comprises:

protocol bridging mechanisms enabling seamless transition between cryptographic approaches;

mid-transaction protocol switching capabilities triggered by emerging information;

parallel protocol execution for different transaction aspects;

rollback and recovery mechanisms maintaining transaction atomicity across protocol changes.

6. The system of claim 1, further comprising a federated learning architecture wherein:

multiple institutions' AI agents contribute to a shared learning model;

local transaction patterns inform global protocol selection improvements;

privacy is maintained through secure aggregation of learned parameters;

institutions benefit from collective intelligence without sharing sensitive data.

7. A method for adaptively orchestrating cryptographic protocols using artificial intelligence comprising:

analyzing financial transactions using machine learning to extract multi-dimensional features;

applying reinforcement learning to select optimal combinations of cryptographic protocols;

dynamically orchestrating selected protocols with ability to switch during execution;

continuously learning from outcomes to improve future selections;

wherein protocol selection considers privacy, performance, regulatory, and economic factors;

wherein different protocols are applied to different transaction aspects;

wherein the method adapts to changing conditions without manual reconfiguration.

8. The system of claim 1, integrated within a Mathematical Woven Responsive Adaptive Swarm Platform (MWRASP) for defensive cybersecurity wherein:

the AI orchestration layer interfaces with defensive AI agent networks;

threat detection AI agents trigger automatic protocol adjustments;

compliance AI agents ensure regulatory adherence across jurisdictions;

the system provides comprehensive enterprise protection through coordinated AI agent swarms.

ABSTRACT

An adaptive artificial intelligence system for dynamically orchestrating multiple cryptographic protocols in financial transactions. The system employs machine learning to analyze transaction characteristics and reinforcement learning to select optimal combinations of zero-knowledge proofs, homomorphic encryption, and secure multi-party computation. Unlike static approaches, the system applies different protocols to different aspects of transactions, switches protocols during execution based on emerging information, and continuously learns from outcomes. The AI system considers privacy requirements, performance constraints, regulatory compliance, and economic factors simultaneously, adapting to new patterns, threats, and regulations without manual reconfiguration. A federated learning architecture enables multiple institutions to benefit from collective intelligence while maintaining privacy. The invention provides intelligent cryptographic protocol selection that

optimizes across multiple objectives, improving upon single-protocol systems through adaptive, learned orchestration. The system operates as part of a comprehensive Mathematical Woven Responsive Adaptive Swarm Platform (MWRASP) providing defensive cybersecurity capabilities through coordinated AI agent networks.