The Sovereign Referee Protocol (SRP): A Stateless Architecture for Trustless Peer-to-Peer Poker

Sonia-Code

February 2026

Abstract

For exactly 47 years, the realization of a purely decentralized, dealer-less card game has been constrained by the computational limitations of verifiable multi-party computation (MPC). This paper introduces the Sovereign Referee Protocol (SRP), a stateless, peer-to-peer architecture designed for Arbitrum Stylus. By utilizing commutative encryption over the BLS12-381 elliptic curve, threshold signatures, and a highly optimized on-chain Miller Loop verifier, SRP eliminates the need for a trusted house. The protocol introduces an economic heartbeat to solve the historical "liveness" problem of Mental Poker, creating the first commercially viable, purely sovereign digital casino environment.

1 Introduction

The theoretical foundation for dealer-less card games was established in 1979 with the publication of the original Mental Poker algorithm. However, practical implementations have consistently failed due to two insurmountable friction points: the exorbitant gas costs associated with verifying cryptographic shuffles on-chain, and the vulnerability of the game state to offline participants (the liveness problem).

The Sovereign Referee Protocol (SRP) dismantles these barriers. By leveraging the Arbitrum Stylus WebAssembly (WASM) environment and the custom-built `crum_bls` cryptographic library, SRP offloads all state management to the peer-to-peer layer. The blockchain is relegated to the role of a "Stateless Referee," only executing mathematically intricate audits when settling a hand or resolving a dispute.

2 Core Architecture

The SRP is built upon three foundational pillars that ensure complete privacy, autonomous consensus, and strict execution.

2.1 Pillar 1: The Collective Shuffled State

The deck does not exist as an array of integers on a centralized server. Instead, it is initialized as a vector of 52 distinct points on the G_1 elliptic curve. Each player generates a secret scalar sk_i and applies it to the deck commutatively.

For a given card $C \in G_1$, the fully masked point M in an N-player game is:

$$M = C \cdot sk_1 \cdot sk_2 \cdots sk_N \tag{1}$$

Because the scalar multiplication is commutative, players can remove (peel) their cryptographic locks in any order using the modular inverse of their secret key (sk_i^{-1}).

2.2 Pillar 2: The Stateless Audit

To ensure that no player substitutes a card during the unmasking phase, SRP employs an on-chain verification engine. To maintain a meticulous data footprint, card points and signatures reside in the G_1 group (48 bytes compressed), while player Public Keys (PK) reside in the G_2 group (96 bytes).

When a player claims to unmask a card point M to produce point U, the Stylus smart contract verifies the integrity of the operation using a Bilinear Pairing (Miller Loop):

$$e(U, PK) = e(M, G_2) \tag{2}$$

If the player acted honestly, $U = M \cdot sk^{-1}$ and $PK = G_2 \cdot sk$, satisfying the pairing identity without ever revealing sk to the network.

2.3 Pillar 3: The Economic Heartbeat

To solve the liveness problem, SRP enforces game continuity through economic slashing. Every cryptographic transition is bound by a 120-second timeout mechanism. If a player fails to provide their unmasked point or threshold signature share, their stake is forfeited to the active participants.

3 Implementation: The `crum_bls` Kernel

The protocol relies on the `crum_bls` library, optimized specifically for Arbitrum Stylus. It bridges high-level cryptographic theory with native Ethereum standards via three key components:

- **Keccak-256 Adapter:** A custom implementation of the `digest::Digest` trait allows the native `alloy_primitives::Keccak256` hashing function to map arbitrary data directly to the BLS12-381 curve, ensuring zero-overhead compatibility with Ethereum wallets.
- **Lagrange Interpolation:** Players use M-of-N threshold signatures to reach consensus on betting rounds. If a player drops offline, the remaining threshold can mathematically reconstruct the Master Signature, allowing the game to settle gracefully.
- **Vector Unmasking:** The Stylus verifier is capable of batch-verifying multiple unmasking steps (e.g., a 5-card Texas Hold'em community flop) in a single atomic transaction.

4 Conclusion

The Sovereign Referee Protocol successfully maps a 47-year-old cryptographic theory into a modern, high-performance financial infrastructure. By treating the blockchain strictly as a stateless arbiter of the Miller Loop, SRP provides a blueprint for a fully decentralized, trustless, and infinitely scalable gaming ecosystem.