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

Sonia Code & Gemini

February 2026

Abstract

For 47 years, the realization of a purely decentralized, dealer-less card game has been constrained by the computational overhead of verifiable multi-party computation. This paper introduces the Sovereign Referee Protocol (SRP), a stateless, peer-to-peer architecture designed for Arbitrum Stylus. By replacing traditional Merkle Trees with dynamically scaled Lagrange Polynomial Commitments over the BLS12-381 curve, SRP compresses the entire game state into a single 48-byte G_1 root. This document details the exact state transitions of a Sovereign Poker game, demonstrating how commutative encryption, KZG proofs, and an economic heartbeat combine to eliminate the trusted house.

1 Introduction

The theoretical foundation for dealer-less card games was established in 1979 with the Mental Poker algorithm. However, moving complete 52-card state histories on-chain has historically destroyed commercial viability due to gas constraints.

SRP resolves this by treating the blockchain strictly as a "Stateless Referee." Utilizing the custom `crum_bls` library, the protocol offloads all state management to the peer-to-peer layer. Furthermore, SRP introduces Dynamic Degree Scaling, an optimization that completely truncates "dead" cards, ensuring cryptographic energy is spent exclusively on the cards in active play.

2 Core Architecture

2.1 Pillar 1: The Commutative Mask

All cards are represented as points on the G_1 elliptic curve. Each player generates a secret scalar sk_i. Because scalar multiplication on the curve is commutative, players can apply and remove their cryptographic locks in any order without corrupting the underlying card point.

2.2 Pillar 2: Dynamic Degree Scaling & Polynomial Anchors

A standard Texas Hold'em hand requires exactly $K = 5 + 2N$ cards, where N is the number of players. Anchoring a full 52-card Merkle Tree wastes computation. Instead, SRP treats the active deck as a mathematical curve.

Players interpolate a Lagrange polynomial $D(x)$ of degree $K - 1$, where evaluating the polynomial at index i yields the fully masked card C_i. Using a KZG commitment, this entire polynomial is compressed into a single G_1 point ($Root$), which is submitted to Arbitrum.

2.3 Pillar 3: The Stateless Audit

Verifying a card peel requires zero sibling-hashes. A player simply provides their unmasked point and a single G_1 evaluation proof (π). The Arbitrum Stylus contract validates the polynomial proof using an $O(1)$ Miller Loop (Bilinear Pairing), comparing it against the anchored *Root* and the player's G_2 Public Key.

2.4 Pillar 4: The Economic Heartbeat

SRP enforces liveness through economic slashing. Every cryptographic transition is bound by a 120-second timeout. If a player fails to provide their unmasking scalar, their stake is forfeited to the honest participants via the smart contract.

3 The Sovereign Game Lifecycle

3.1 1. Player Joins the Game (Staking & Registration)

- A player calls `join_table()` on the Arbitrum Stylus contract, depositing their USDC stake.
- The player registers their G_2 Public Key (PK_i), establishing their verifiable identity for the Miller Loop audit.

3.2 2. The Truncated Sovereign Shuffle

The deck begins as a sorted vector of 52 G_1 points.

- **Shuffle-and-Mask:** Player 1 masks all 52 points with sk_1, randomly permutes the vector, and passes it to the next player. This repeats until Player N finishes.
- **Truncation:** The fully locked, fully shuffled 52-card vector is truncated to the top K points required for the specific game format (e.g., $K = 9$ for Heads-Up Hold'em).
- **Commitment:** Players compute the Lagrange polynomial $D(x)$ for these K points. The resulting KZG *Root* (G_1 point) is submitted to the Stylus contract as the immutable anchor for the hand.

3.3 3. Posting Blinds & Pre-Flop Deal

- Players agree on blind deductions via P2P threshold signatures (`crum_bls::lagrange::combine`), committing the new balance state.
- To view hole cards (indices 0 and 1), Player 1 requests the unmasking values from all other players. The other players transmit U_0 and U_1 by applying their modular inverses (sk_i^{-1}). Player 1 applies their final inverse to secretly reveal the cards.

3.4 4. Betting Rounds & Community Cards (Flop, Turn, River)

- **Betting:** Players broadcast actions (Call, Raise, Fold) P2P. Active players sign the updated pot state, creating a cryptographically secure Hand History.
- **Dealing:** For the Flop (indices 2, 3, 4), all active players broadcast their inverse scalars simultaneously. The three G_1 points are publicly reconstructed. This process repeats for the Turn and River.

3.5 5. The Showdown

Remaining players reveal their private hole cards by broadcasting their final unmasking scalars. The table verifies that the revealed cards mathematically correspond to the KZG polynomial *Root*. The winner submits the threshold-signed final state to the Stylus contract for instant USDC settlement.

4 The Unhappy Path: Malice and Disconnections

If a losing player attempts to stall the game by withholding an unmasking scalar:

1. **Dispute Initiation:** The honest player submits the threshold-signed game state to Arbitrum Stylus.
2. **The Timer:** A 120-second countdown begins, demanding the stalling player submit their unmasking point directly on-chain.
3. **The Audit:** If submitted, the contract runs the `crum_bls` Miller Loop against the polynomial *Root*.
4. **Slashing:** If the pairing fails (the math is manipulated) or the timer expires, the malicious player is slashed. Their USDC is distributed to the honest players, and the hand terminates.

5 Conclusion

By converging 1979 Mental Poker theory with 2026 KZG polynomial commitments and Arbitrum Stylus, the Sovereign Referee Protocol achieves $O(1)$ verification costs and absolute autonomy. It provides the definitive architecture for a mathematically enforced, dealer-less financial ecosystem.