パリミュチュエル方式におけるプライバシー保護技術の応用

上段 浩輝[1]　李 陽[1]　崎山 一男[1]　宮原 大輝[1]

概要：パリミュチュエル方式は、競馬やドッグレースなどの公営ギャンブルで用いられるベッティング方式である。この方式では、オッズ（払戻倍率）は各結果に賭けられた金額の割合に応じて変動する。ユーザはこのオッズを参考にして賭け先を決定するが、オッズは主催者によって算出されるため、仮にその算出過程が操作されていても、ユーザがそれを検知する術はない。この問題を解決する一つの方法として、ブロックチェーンを用いた非中央集権的なベッティングシステムが考えられる。しかし従来のブロックチェーンベースのシステムでは、すべてのベット情報が即時かつ公開状態で記録されるため、個々のユーザの投票内容が容易に特定される。これはプライバシーの侵害のみならず、ベッティング戦略の模倣というリスクも引き起こす。これに対し本研究では、投票内容を加法準同型暗号により暗号化した上で、複数ユーザの投票をリアルタイムではなくバッチとして処理することにより、オッズの変化から個別のベットが逆算されるのを防ぐ手法を設計する。また、バッチ処理に伴って生じる匿名性とリアルタイム性のトレードオフにも着目し、そのバランスの重要性を議論する。さらに、本プロトコルが満たすべきセキュリティ要件についても整理し、ベッティングにおけるプライバシーと透明性の両立を可能にする新たな枠組みとしての有効性を論じる。

Application of Privacy-Preserving Techniques in Parimutuel Betting Systems

Hiroki Uedan[1]　Yang Li[1]　Kazuo Sakiyama[1]　Daiki Miyahara[1]

Abstract: Parimutuel betting is a wagering system commonly used in public gambling such as horse racing and greyhound racing. In this system, the odds (i.e., payout multipliers) fluctuate based on the proportion of the total amount bet on each outcome. While users refer to these odds to decide where to place their bets, the odds themselves are calculated by the organizer. This centralized calculation process introduces a potential risk: if the calculation process is manipulated, users have no means of detecting it. One potential solution to this problem is the use of blockchain technology to build a decentralized betting system. However, in conventional blockchain-based systems, all betting information is recorded immediately and publicly, making it easy to identify individual users' voting behaviors. The immediate public disclosure of bets not only poses a privacy threat but also introduces the risk of betting strategy imitation. To address this, we propose a protocol in which bet details are encrypted using additive homomorphic encryption and processed in batches rather than in real time. The encrypted batch processing prevents the inference of individual bets from the fluctuations in odds. We also highlight the trade-off between anonymity and real-time performance introduced by batch processing and discuss the importance of balancing these factors. Furthermore, we examine the security requirements that the proposed protocol must satisfy and argue for its potential as a new framework that reconciles both privacy and transparency in betting systems.

1. 始めに

パリミュチュエル方式（Parimutuel Betting）は、競馬やドッグレースなどの公営ギャンブルにおいて広く採用されている賭け方式である。この方式では、すべての賭け金を一つのプールに集め、レース終了後に的中者に対して配当を行う。具体的には、各結果に賭けられた金額の比率に基づき、払戻**オッズ**が決定される。すなわち、ある結果に賭ける人が少ないほど、その結果に的中した際のオッズは高くなる。この方式の特徴は、賭け期間中にオッズが動的に変動する点にある。賭け期間の初期には、各結果に投じられた金額が少ないため、オッズは流動的である。この変化

[1] 電気通信大学
The University of Electro-Communications

は参加者の意思決定に大きな影響を与えるため、リアルタイムなオッズ表示と正確な集計が極めて重要となる。

パリミュチュエル方式は、単なる娯楽としての賭博に留まらず、地域経済や公共財源の確保にも寄与してきた歴史を持つ。日本では日本中央競馬会（JRA）など、公的機関や公認事業者が運営主体となる場合が多く、その売上の一部は自治体や公共事業に還元される仕組みが一般的である。そのため、公正な運営と信頼性の高いシステム設計は、単に参加者保護の観点だけでなく、社会的な信頼性の維持にも直結する。

1.1 従来方式の課題

従来のパリミュチュエル方式では、オッズの計算と配当の決定は主催者の中央サーバ上で行われる。主催者は全てのベット情報を集約してオッズを算出し、それを参加者に提示する。しかし、このプロセスはブラックボックス化しており、参加者はオッズ計算過程を直接検証することができない。極端な場合、もし主催者や内部関係者が不正を行えば、オッズを意図的に操作することも理論的には可能である。実際には公営競技において不正が頻発しているわけではないものの、検証不能であるという構造的問題は残り続ける。

近年、**ブロックチェーン**技術 [11] は分散型台帳としての特性を活かし、金融取引や電子投票、サプライチェーン管理など幅広い分野で応用が進んでいる。パリミュチュエル方式においても、ベット情報やオッズ計算過程をブロックチェーン上に記録すれば、誰もが取引履歴を検証でき、主催者による恣意的な改ざんが事実上不可能となる。このアプローチにより、オッズ計算の完全な透明化と参加者による独立検証が可能になる。さらに、スマートコントラクトを用いれば、配当計算や送金を自動化でき、人的介入によるエラーや不正のリスクを低減できる。

しかし、既存のブロックチェーンベースのパリミュチュエル方式 [10, 17] には重大な課題が残る。それは、全てのベット情報が即時かつ公開状態で記録されるため、個々のユーザの投票内容が容易に特定可能となる点である。ウォレットアドレスは一見匿名的であるが、過去の取引や外部情報と突き合わせれば特定の人物に紐づけられる可能性が高い。また、レース締切前に投票情報が逐次公開されるため、特定の熟練プレイヤーのベッティングパターンを模倣する危険性もある。これは市場の健全性を損ない、参加者間の公平性を著しく低下させる要因となる。

暗号化投票の分野では、差分解析による個表推定を防ぐために複数の入力をまとめて処理する**バッチ処理**がが応用されてきた。例えば電子投票システム Helios [1] では、投票を逐次的に復号すると選挙人の選好が推測されるリスクがあるため、複数票をまとめて開示する設計が採用されている。また、匿名通貨 Monero [18] や Zcash [5] においても、取引をまとめる仕組みによって匿名性を高めている。これらはいずれも匿名性確保を目的とした応用であり、パリミュチュエル方式のようにリアルタイムに変動するオッズを逐次公開する場面にバッチ処理を導入した事例はこれまでにない。

1.2 本研究の貢献

本研究では、パリミュチュエル方式をブロックチェーン上で実装するにあたり、各ユーザの投票内容および賭け金額を暗号化したまま集計する仕組みを設計する。投票データは主催者の公開鍵で暗号化されるため、第三者からは不可視であり、プライバシーが保護される。一方で、主催者は秘密鍵を保持しているため個別投票を復号可能であるが、レース終了後に秘密鍵を公開することで、全ユーザが主催者の提示したオッズ算出過程を追跡・検証できるようにした。これにより、従来の中央集権的なシステムでは困難であった透明性と検証可能性を実現する。

パリミュチュエル方式のオッズ計算は、各結果に賭けられた金額の単純な加算によって導かれるため、暗号化状態で必要とされる演算は加法のみである。本研究では、この性質を利用し、完全準同型暗号ではなく加法準同型暗号を用いることで、計算効率についても考慮する。また、オッズのリアルタイム性に対応するため、複数票をまとめたバッチ処理によって暫定オッズを公開する方式を採用する。ユーザは変動するオッズを参照しながらも、差分解析による個別投票の特定は防ぐことができる。バッチ処理は匿名性を高める手段として既存の投票システム [1] や匿名通貨 [5, 18] などで用いられてきたが、本研究ではそれをベッティングに応用し、さらに主催者がレース終了後に秘密鍵を公開する仕組みとすることで、ユーザ自身が過去に提示された暫定オッズの正当性を検証できるようにする。これらにより、従来の暗号化投票に関する研究が提供してきた匿名性に加えて、パリミュチュエル方式特有のリアルタイム性とオッズ算出過程の透明性・検証可能性を同時に実現するプロトコルを設計する。

さらに、本研究で提案するプロトコルが満たすべきセキュリティ要件を以下に整理する。これらはいずれも電子投票や匿名認証の分野で議論されてきた典型的な性質を参考にしている。

- **投票内容秘匿性**：各ユーザの投票内容が第三者から推測されないこと [7]。
- **集計過程と結果の検証可能性**：すべての投票者や第三者が集計過程および最終結果の正当性を検証できる性質 [1, 9]。
- **法的要請に応じた特定可能性**：通常は匿名性が保証されるが、特定の条件下（例：法的要請）では投票者を識別可能とする性質 [8]。
- **ベット否認耐性 (Non-repudiation)**: 投票者が後から自

らの投票や賭けを否認できない性質 [12]。

これらの要件を踏まえ、透明性とプライバシーの両立を可能にするプロトコル設計を提示する。

2. 関連研究

本節でブロックチェーンベースの関連システムを紹介し、本研究との差異を述べる。

2.1 パリミュチュエル方式

ブロックチェーンを利用したパリミュチュエルベッティング [10, 17] は、賭け金やオッズ計算過程を分散台帳に記録することで透明性と改ざん耐性を実現するプロトコルである。一般的には、主催者が集計や配当をスマートコントラクトに委ね、全ユーザが取引履歴を検証できる仕組みを採用する。これにより、中央集権型で問題となるオッズ操作や不正集計の可能性が原理的に排除される一方、全ベット履歴がリアルタイムに公開されるため、特定ユーザの行動や戦略が模倣されるリスクが残る。

2.2 電子投票システム

電子投票におけるブロックチェーン応用では、投票内容の秘匿性と集計結果の検証可能性を両立させるため、加法準同型暗号やグルーピング（ミックスネットやシャッフル）を組み込むプロトコルが多く提案されている。準同型暗号を用いる方式では、各投票は暗号化されたまま加算集計され、最終集計時にのみ復号が行われるため、投票期間中に他者の投票内容を推測することは困難である。一方、グルーピング方式は投票順や送信元をランダム化して匿名性を高める。これらの手法は、ブロックチェーンが提供する透明性に加えて、暗号技術による秘匿性を付加し、参加者のプライバシーを強化する。実際に、Paillier 暗号 [13] や秘密分散とシャッフルを組み合わせた方式 [4] など、複数の電子投票プロトコルが提案されている。

2.3 加法準同型暗号の応用

オークションや投票プロトコルにおいても、加法準同型暗号は入札額や投票内容を秘匿したまま集計・比較を行う手段として広く用いられている。この種のプロトコルは、暗号化された数値同士を直接加算できる性質を利用し、落札者や多数派の決定といった結果のみを公開する。特に、多数量型オークション（Multiunit Auction）や二重オークションでは、入札情報を秘匿したまま価格決定やマッチングを行う構成が一般的である [6, 16, 19]。これらの研究は、金銭的価値や戦略性の高い情報を扱う場面で、秘匿性と検証可能性の両立が実用的に成立することを示しており、プライバシー保護型ベッティングプロトコルの設計においても参照すべき枠組みとなる。

2.4 既存手法との比較

本研究が対象とするパリミュチュエル方式は、投票内容に応じてオッズを更新して公開する必要があり、その点が電子投票やオークション（集計結果を最後に公開）と異なる。そこで集計を即時に行うか、ある程度間隔を持たせるのかの 2 パターンが考えられる。即時集計型は、各取引発生時に集計結果を更新し、最新の状態を常に公開するため、利用者はリアルタイムの情報に基づいて意思決定できる。しかし、逐次更新される結果は個別の取引内容を推測する材料となりやすく、プライバシーリスクを伴う。バッチ集計型では、一定期間または件数ごとに暗号化データをまとめて集計・復号し、結果のみを公開することで、取引内容の逆算を困難にする。その代償として、情報更新の遅延が発生し、リアルタイム性が低下する。

プライバシー保護の強度は集計間隔やバッチサイズの増加とともに高まる一方で、リアルタイム性は低下する。電子投票のように途中経過の公開が不要で、最終結果のみが開示されればよいケースでは、強い匿名性を優先できる。しかし、ベッティング市場のように刻々と変動するオッズが戦略に直結する場面では、このバランスの最適化が不可欠である。既存のブロックチェーン型パリミュチュエル方式は即時集計型であり、匿名性を高める設計には制約がある。本研究は、加法準同型暗号を活用したバッチ集計により、このバランスを制御可能な設計を提示する点に新規性がある。

3. 準備

3.1 パリミュチュエル方式の数理モデル

パリミュチュエル方式は、競馬やドッグレースなどの公営ギャンブルにおいて広く採用される配当計算方式である。本方式では、全参加者が購入したチケットの売上金を一つのプールに集約し、レース終了後に的中者に配分する。オッズ（払戻倍率）は、各選択肢に投じられた金額の割合に応じて変動する。

レースにおいて n 個の選択肢（競馬の場合は競走馬）が存在し、それぞれの選択肢 i に投じられた金額を B_i とする。このとき全体の売上金総額は $T = \sum_{i=1}^{n} B_i$ で与えられる。主催者が徴収する手数料率（テイクアウト率）を r とすると、配当に回される金額の総額は $P = (1 - r) \cdot T$ となる。このとき選択肢 i の配当倍率 O_i は次式の通りとなる。

$$O_i = \frac{P}{B_i} = \frac{(1 - r) \cdot T}{B_i} \tag{1}$$

したがって、人気の低い選択肢（B_i が小さいほど）オッズは高くなり、的中時の払戻金額が増加する。一方、人気の高い選択肢はオッズが低くなるため、低配当となる。このオッズは賭け期間中に参加者の投票に応じてリアルタイムで変化し、参加者の戦略に大きな影響を与える。

数理モデルとしては、賭け期間中におけるオッズ変動を

時系列データとして扱うことができ、最終オッズ O_i^{final} は締切時刻 t_{close} における $B_i(t)$ の値によって確定する。

3.2 Avalanche

Avalanche は、2020 年 9 月に Ava Labs によってローンチされた高性能なスマートコントラクト対応ブロックチェーンプラットフォームである [3,15]。これは Ethereum Virtual Machine（EVM）互換の環境を備えつつ、独自のコンセンサスプロトコルである Avalanche Consensus を採用し、トランザクションの高速確定（ファイナリティ）と高スループットを実現している。この設計により、数秒以内の取引確定と数千件/秒規模の処理性能を両立し、分散性・安全性を維持しながら低手数料での利用が可能となっている 。

Avalanche ネットワークは 3 本の相互運用可能なブロックチェーンで構成される。

- **X-Chain（Exchange Chain）**：デジタル資産の作成と送受信に特化し、UTXO モデルを採用する。
- **P-Chain（Platform Chain）**：バリデータの管理やサブネット（Subnet）の作成・管理を担う。サブネットは独自のバリデータ集合とチェーン構成を持つことができ、特定用途や規制要件に適合したチェーンを構築可能である。
- **C-Chain（Contract Chain）**：Ethereum 互換のアカウントモデルを採用し、Solidity 言語によるスマートコントラクト実行を可能にする。C-Chain は EVM と完全互換であるため、Ethereum 上で動作する多くの DApp をほぼそのまま移植できる。

Avalanche Consensus [14] は、従来の BFT（Byzantine Fault Tolerance）型コンセンサスの亜種であり、部分的ランダムサンプリングと繰り返し投票による確率的合意形成を行う。ノードは取引やブロックの承認についてランダムに少数の他ノードに問い合わせ、過半数の同意が得られるまで複数ラウンドの投票を繰り返す。この過程により、全ノードが短時間で高確率に同じ結論に収束する。この手法は、従来の全員投票型 BFT に比べ通信量が小さく、ノード数の増加に対するスケーラビリティが高いという特長を持つ。

3.3 Encrypted ERC（eERC）

Encrypted ERC（eERC）[2] は、Avalanche C-Chain 上で動作する暗号化トークン規格であり、Ethereum の ERC-20 と同様のインターフェースを持ちながら、残高や送金額を暗号化し、ゼロ知識証明（ZKP）によって正当性を検証可能にした拡張仕様である。

暗号モデル

ユーザの残高 $B_u \in \mathbb{Z}_q$ および送金額 $t \in \mathbb{Z}_q$ は、楕円曲線上の加法準同型 ElGamal 暗号により暗号化される。有限巡回群 $\mathbb{G}$ の生成元 g を用い，秘密鍵 $x \in \mathbb{Z}_q$，公開鍵 $h = g^x$ とする。

平文 $m \in \mathbb{Z}_q$ の暗号化は乱数 $r \leftarrow \mathbb{Z}_q$ を用いて

$$E_{pk}(m) = (c_1, c_2) = (g^r,\ g^m \cdot h^r) \in \mathbb{G} \times \mathbb{G} \tag{2}$$

と定義される。復号は

$$g^m = c_2 \cdot (c_1^{-x}) \tag{3}$$

により g^m を得て，必要に応じて離散対数を解くことで m を復元する。

この方式は加法準同型性を備えており, 任意の $m_1, m_2 \in \mathbb{Z}_q$ に対して

$$E_{pk}(m_1) \cdot E_{pk}(m_2) = E_{pk}(m_1 + m_2) \tag{4}$$

が成り立つ。したがって暗号文を直接操作することで，残高や送金額の加算を行うことができる。各ユーザの残高は暗号文 $C_u = E_{pk}(B_u)$ として保持される。

送金処理

金額 t の送金時，送金元と送金先の残高は以下のように C'_u, C'_v に更新される。

$$C'_u = C_u \cdot (g^{-t}, h^{r'_u}) \tag{5}$$

$$C'_v = C_v \cdot (g^{t}, h^{r'_v}) \tag{6}$$

これらの更新は加法準同型性

$$E_{pk}(B_a) \cdot E_{pk}(B_b) = E_{pk}(B_a + B_b) \tag{7}$$

を利用して暗号化状態のまま実行可能である。

ゼロ知識証明による検証

送金トランザクションには以下の条件を満たすゼロ知識証明 π が添付される。

(1) 残高充足性：$B_u \geq t$

(2) 非負制約：$B'_u, B'_v \geq 0$

(3) 更新正当性：C_u, C'_u が t の減算、C_v, C'_v が t の加算に対応していること

これにより、スマートコントラクトは平文を知ることなく送金の正当性を検証できる。検証は以下の関数として表される。

$$\text{Verify}(pk, C_u, C_v, C'_u, C'_v, \pi) \stackrel{?}{=} \text{true} \tag{8}$$

監査機能

規制遵守や監査のために，特定の監査者用の復号鍵 $sk_{\text{audit}} = x_{\text{audit}}$ を設定できる。監査者は暗号文 $C_u = (c_1, c_2)$ に対して

$$g^{B_u} = c_2 \cdot (c_1^{-x_{\text{audit}}}) \tag{9}$$

を計算することで g^{B_u} を得る。ここで B_u は残高であり，$m = B_u$ が取り得る値の範囲はシステム設計上あらかじめ制限されている（例えば投票口数や賭け金単位の合計）。したがって監査者は g^m のテーブルを事前に構築しておくこ

とで,

$$B_u = \log_g(g^{B_u}) \tag{10}$$

を効率的に計算できる。

4. 提案プロトコル

本節では、本研究で提案する方式の安全性を議論するための前提条件と設計の全体像を示す。具体的には、まず想定する脅威モデルと、それに基づいて満たすべきセキュリティ要件を整理する。次に、方式を構成する要素とその役割を定義し、最後にプロトコル全体を形式的に記述する。

4.1 脅威モデルとセキュリティ要件

ブロックチェーンベースのパリミュチュエル方式は、1.2 節で示した 4 つの要件を満たす必要がある。それぞれの詳細を述べる。

ベット内容秘匿性

ベット内容秘匿性とは、各参加者がどの選択肢にいくら賭けたかという情報を、許可されていない第三者が直接または間接的に知ることができないように保護する性質である。これは賭け戦略や資金配分といった個人の意思決定情報を守るために重要であり、他者による戦略模倣や市場操作を防止する効果がある。秘匿性が欠如すると、特定の高勝率プレイヤーの行動を模倣することで不均衡が生じたり、差分解析によって小規模なベットの内容が特定される危険がある。秘匿性の確保には、暗号化、匿名化、集計単位の調整など、技術的および運用的な対策が必要となる。

集計過程と結果の検証可能性

集計過程と結果の検証可能性とは、発表されたオッズや払戻額が、全ての有効なベットに基づいて正しく計算されたことを、第三者を含むすべての利害関係者が独立に確認できる性質である。この要件は、中央集権的な信頼に依存しない公平性を担保し、不正操作や計算ミスの検出を可能にする。検証可能性を確保するためには、集計アルゴリズムや計算ロジックが公開され、入力データが正確で改ざんされていないことを保証できることが望ましい。暗号的コミットメント、公開監査証跡、完全な取引履歴の開示などが実現手段として挙げられる。

法的要請に応じた特定可能性

法的要請に応じた特定可能性とは、通常時は参加者の匿名性を維持しつつ、正式な法的手続きや規制当局からの要請があった場合に限り、特定のベットや取引の実施者を実世界の身元と結びつけられる性質である。これは、マネーロンダリング防止（AML）、顧客確認（KYC）、課税義務の履行など、法令遵守のために必要となる。匿名性を完全に排除するとプライバシー保護が損なわれる一方、完全匿名では法的規制への対応が困難になるため、両者のバランスを取る仕組みが求められる。特定可能性を実現するには、安全に管理された身元情報データベース、分散型 ID（DID）、ゼロ知識証明などが利用される。

表 1: 本研究で用いる記号とその定義

記号	説明
$\mathcal{H} = \{1, \ldots, H\}$	馬の集合
$\mathcal{U}$	ユーザ集合
$\nu \in \mathbb{Z}_{>0}$	1 口あたりの賭け金額
$\alpha \in [0, 1)$	税・控除率
$\tau_{\mathrm{cl}} \in \mathbb{N}$	締切時刻
β : Tx 列 $\to \{1, \ldots, B\}$	バッチ分割関数
$(pk_{\mathrm{race}}, sk_{\mathrm{race}}) \leftarrow \mathsf{KeyGen}(1^\lambda)$	レース専用の鍵生成
$E(m; r) = \mathsf{Enc}_{pk_{\mathrm{race}}}(m; r)$	暗号化関数
$\mathsf{Dec}_{sk_{\mathrm{race}}}(E(m; r)) = m$	復号関数
$\otimes$	暗号文の加法準同型演算
$\mathsf{Dec}_{sk}(C_1 \otimes C_2)$	$\mathsf{Dec}_{sk}(C_1) + \mathsf{Dec}_{sk}(C_2)$ に対応

ベット否認耐性

ベット否認耐性とは、参加者が過去に行ったベットの存在や内容を否認できないようにし、また運営側が特定のベットの存在を消去・改ざんできないようにする性質である。これは、後からのトラブルや紛争解決において重要であり、証拠の完全性を保証する。否認耐性が確保されていない場合、参加者は不利益な結果となったベットを否定し、運営側は不正な利益を得るためにベット記録を改ざんする可能性がある。対策としては、取引の完全な記録、暗号的署名、改ざん検知可能なデータ構造が一般的に用いられる。

4.2 システム構成と役割

本研究で提案するパリミュチュエル方式の実装は、以下の 3 つの主要コンポーネントによって構成される。

ユーザ

レース情報を取得し、主催者が公開した公開鍵を用いて投票情報を暗号化して送信する。レース終了後、主催者が秘密鍵を公開すると、払戻金の正当性を検証し、スマートコントラクトから払戻金を受け取る。

主催者

レースの開催主体であり、公開鍵・秘密鍵の生成、レース情報（参加馬）の登録、レース結果の入力、秘密鍵の公開、および自身の取り分の受領を行う。

スマートコントラクト

投票受付、暗号化ベットの保管、レース結果と秘密鍵の公開後の復号処理、払戻請求の検証および送金、主催者の取り分送金を実行する。

4.3 プロトコルの形式化

プロトコルの形式化に用いる記号を表 1 に示す。各馬 $i \in \mathcal{H}$ に eERC のプール識別子（サブアカウント） part(i) を割り当てる。時刻 τ で発行されたユーザ u による馬 i への投票トランザクションを

$$t = (u, i, m_{u,i}^{(t)}, \tau_t, c_t), \quad c_t = E(m_{u,i}^{(t)}; r_t), \quad m_{u,i}^{(t)} \in \nu \cdot \mathbb{Z}_{\geq 0}$$

と表す。β により Tx 列はバッチ $b \in \{1, \ldots, B\}$ に分割される。

(1) **トークン準備と鍵生成**

主催者は eERC トークンコントラクトアドレスを A_{eERC} とし，

$$(pk_{\text{race}}, sk_{\text{race}}) \leftarrow \mathsf{KeyGen}(1^{\lambda})$$

を生成して pk_{race} をスマートコントラクトに登録する。sk_{race} はレース終了まで秘匿保持する。

(2) **レース設定**

主催者は以下をコントラクトに確定・登録する。

$$\left(\mathcal{H},\ \tau_{\text{cl}},\ \alpha,\ \nu,\ \{\text{part}(i)\}_{i\in\mathcal{H}},\ \beta\right)$$

いかなる投票 Tx も $\tau_t \leq \tau_{\text{cl}}$ を満たす必要がある。

(3) **レース情報取得**

任意のユーザは以下の公開パラメータ集合

$$\mathsf{PP} = \left(A_{\text{eERC}},\ pk_{\text{race}},\ \{\text{part}(i)\}_{i\in\mathcal{H}},\ \tau_{\text{cl}},\ \alpha,\ \nu,\ \beta\right)$$

をスマートコントラクトから参照できる。

(4) **秘匿投票**

ユーザ u が馬 i に $n_{u,i}^{(t)} \in \mathbb{Z}_{\geq 0}$ 口投票する場合，

$$m_{u,i}^{(t)} = \nu \cdot n_{u,i}^{(t)}, \qquad c_t = E(m_{u,i}^{(t)}; r_t)$$

を生成する。ユーザは暗号文 c_t を eERC 上で part(i) に対応するプールへ送金し，この送金は $\tau_t \leq \tau_{\text{cl}}$ を満たす場合に限り受理される。送金時には eERC により残高充足性と更新正当性が検証され，個票 $m_{u,i}^{(t)}$ は暗号文 c_t としてのみ公開される。

(5) **暫定オッズ公開**

バッチ b が確定するたびに、各馬 i の暗号化合計を次のように定義する。

$$\mathcal{T}_{i,b} = \{\, t \mid t \text{ は馬 } i \text{ への投票 Tx かつ } \beta(t) = b \,\},$$

$$C_{i,b} = \bigotimes_{t\in\mathcal{T}_{i,b}} c_t$$

主催者は

$$M_{i,b} = \mathsf{Dec}_{sk_{\text{race}}}(C_{i,b})$$

を得て公開し、累積合計

$$A_i^{(b)} = \sum_{b'=1}^{b} M_{i,b'}, \qquad S^{(b)} = \sum_{i\in\mathcal{H}} A_i^{(b)}$$

を計上する。単勝型の暫定オッズ倍率は

$$O_i^{(b)} = \frac{(1-\alpha)\,S^{(b)}}{A_i^{(b)}} \quad (A_i^{(b)} > 0)$$

として計算・掲示される（$A_i^{(b)} = 0$ のとき未定義）。

(6) **レース結果入力**

レース終了後、主催者は勝利馬 $w \in \mathcal{H}$ をスマートコントラクトに登録する。

(7) **秘密鍵の公開**

レース終了後、主催者はレース専用の秘密鍵 sk_{race} を公開する。任意の検証者は、各 b, i について $\hat{M}_{i,b} = \mathsf{Dec}_{sk_{\text{race}}}(C_{i,b}) \stackrel{?}{=} M_{i,b}$ を独立に確認でき、暫定オッズおよび最終オッズの正当性を検証できる。

(8) **払戻金の受領**

最終合計を $A_i^{(B)}$、総販売額を $S = S^{(B)}$ とする。勝ち馬 w への総賭金は

$$W = \sum_{u\in\mathcal{U}} \sum_{\substack{t\in\mathcal{T}_w \\ \text{owner}(t)=u}} m_{u,w}^{(t)} = A_w^{(B)}.$$

ユーザ u の勝ち馬への賭金合計

$$m_{u,w} = \sum_{\substack{t\in\mathcal{T}_w \\ \text{owner}(t)=u}} m_{u,w}^{(t)}$$

に対する払戻額は

$$p_u = (1-\alpha)\,S \cdot \frac{m_{u,w}}{W} \qquad (W > 0).$$

(9) **主催者の取り分受領**

主催者取り分は $R = \alpha S$ と定義され、レース終了後に主催者が受領する。

5. 安全性・プライバシー分析

本節では、4.1 節で示した 4 つのセキュリティ要件に基づき、本プロトコルの安全性を分析する。具体的には、ベット内容秘匿性、集計過程と結果の検証可能性、法的要請に応じた特定可能性、ベット否認耐性のそれぞれについて検討を行う。

5.1 ベット内容秘匿性

本研究では、加法準同型暗号を用いることで各ユーザのベット内容を暗号化したままブロックチェーンに記録する。暗号文は乱数化されており、同じ金額を賭けても毎回異なる暗号文が生成されるため、暗号文同士のパターン比較によって取引をリンクすることは困難である。公開される情報は暗号文のみであり、平文ベット額を直接知ることは不可能となる。さらに、復号処理はバッチ単位でのみ実行されるため、単一ユーザの投票内容を逐次的に切り出すこともできない。この仕組みにより、ベット内容秘匿性は強固に担保される。

また、リアルタイムオッズ推測攻撃や差分解析攻撃に対しても防御効果を持つ。従来方式では新しいベットが行われるたびにオッズが即時更新されるため、その差分を観測するだけで対象選択肢と金額を逆算できた。例えば、ある馬のオッズが大きく変動した場合、少数の候補のいずれか

に大口ベットが入ったと容易に推定できる。しかし本方式では、複数のベットがまとめて処理されるため、オッズ変動がどのユーザに起因するのか切り分けられない。バッチに含まれるユーザ数が増えるほど、特定の個票を追跡する確率は低下し、匿名性は実質的に強化される。匿名集団の規模を表す「匿名集団サイズ」を指標とすれば、例えばバッチ内に 10 件の取引が含まれる場合、単一ユーザを特定できる確率は単純化すれば 1/10 に低下する。さらに異なる選択肢への複数ベットが混在すれば推測困難性は指数的に増加し、現実的な追跡は不可能となる。

5.2 集計過程と結果の検証可能性

本研究のプロトコルでは、集計の正当性を暗号学的に担保する仕組みを導入している。まず、すべてのベットは加法準同型暗号により暗号化され、スマートコントラクト上に記録される。スマートコントラクトは暗号文同士の演算を通じて集計処理を行うため、平文を知ることなく合計金額を更新でき、改ざんは極めて困難となる。さらに、レース終了後には主催者がレース専用の秘密鍵を公開し、全ユーザが独立に復号を実施できる。この過程により、主催者が公表した暫定オッズや最終オッズが、実際に暗号化された投票データに基づいて正しく計算されたものであるかを誰もが確認可能となる。

秘密鍵の公開による事後検証することで、参加者に対して高い透明性を提供する。具体的には、各バッチごとに集計された暗号文の合計値 $C_{i,b}$ を復号し、得られた平文 $M_{i,b}$ が主催者の公表値と一致するかを第三者が独立に確認できる。もし不一致が生じた場合、主催者による不正あるいはシステム障害を即座に検知できる。したがって、集計過程は単なる主催者依存ではなく、検証可能な手続きであることが暗号学的に保証される。

さらに、ブロックチェーン自体が持つ不可逆的な台帳構造も、検証可能性を補強する要素である。すべてのトランザクションが時系列順に記録され、外部から監査可能であるため、取引履歴の欠損や改ざんは不可能である。主催者は既存データを操作できず、ユーザは任意の時点で取引履歴を再計算してオッズの正当性を確認できる。

5.3 法的要請に応じた特定可能性

本プロトコルは、通常時にはユーザの匿名性を維持しつつ、法的要請が生じた場合に限り特定のユーザを識別できる構造を備える必要がある。

具体的には、ユーザ登録時に KYC 手続きを行い、その結果をオフチェーンの安全なデータベースに保持する仕組みが望ましい。また、各ユーザには DID を発行し、オンチェーン上のウォレットアドレスと一意に紐付けることで、匿名性を維持しながら規制要件を満たすことが可能となる。さらに、マネーロンダリングや不正利用が疑われる場合、あるいは規制当局から正式な要請があった場合には、オフチェーンの KYC データベースを参照することで、暗号化されたベットを実ユーザに対応付けることができる。

5.4 ベット否認耐性

本プロトコルでは、すべての取引がブロックチェーン上に記録され、暗号署名によって検証可能な形式で保持される。各ユーザは自身の秘密鍵で署名を行うため、記録された取引は本人のものであることが暗号学的に保証される。したがって、一度発行されたベットをユーザ自身が否定することはできない。

さらに、ブロックチェーンの不可逆的な台帳構造により、運営側が特定の取引を削除したり改ざんしたりすることも不可能である。すべてのトランザクションは公開かつ分散的に保持され、外部の監査者や他の参加者が独立に検証できる。これにより、運営が不正に有利なベットを消去したり、不利益な取引を改ざんする余地は排除される。

また、レース終了後に主催者が秘密鍵を公開する仕組みも、否認耐性を補強する。ユーザは過去の取引と照合し、集計結果や払戻額が自身のベットに基づいて正しく計算されているかを独立に確認できる。もし不一致があれば、暗号文とブロックチェーン上の記録を根拠に異議を申し立てることが可能である。これは、ベットが存在しなかったとされることや、集計から不当に排除されることを防止する強力な手段となる。

6. 考察

6.1 匿名性とリアルタイム性のトレードオフ

本研究で採用したバッチ処理モデルは、匿名性とリアルタイム性の間に明確なトレードオフを有する。バッチの集計間隔を長くすれば、単一ベットの影響を差分解析で特定することが困難になり、匿名性は強化される。しかしその一方で、オッズ更新の遅延が大きくなり、ユーザは最新の市場状況に基づいた意思決定が行いにくくなる。逆に、集計間隔を短くするとリアルタイム性は向上するが、匿名集団のサイズが小さくなり、特定のベット内容が推測されやすくなる。実運用においては、参加者数やベット頻度に応じてバッチ間隔を動的に調整する適応的アプローチが有効と考えられる。

6.2 高額 Priority Fee 問題とユーザ体験

ブロックチェーン上での取引は、ネットワーク混雑時に手数料（Gas Fee）が急騰することがある。特に、優先的に処理されるために高額の Priority Fee を設定するユーザが現れると、他のユーザの取引が遅延し、結果的にオッズ変動情報にアクセスするタイミングやベット確定時刻に不公平が生じる。この問題はユーザ体験の悪化や市場の健全性低下を招く可能性がある。対策としては、ベットの受付と

集計をオンチェーンから切り離してオフチェーンで一時保管する設計や、Priority Fee の影響を受けにくいレイヤ 2 ソリューションの活用が考えられる。

6.3 他の暗号方式との比較可能性

加法準同型暗号は、暗号化されたまま合計値を計算できるため集計処理に適している。一方で、ゼロ知識証明（ZKP）を用いれば、暗号化せずともある条件を満たすベットであることや合計値が正しいことを秘密のまま証明することが可能である。ZKP は証明サイズや生成時間の面でオーバーヘッドが大きくなる可能性があるが、選択肢数が多い場合や複雑な条件付きベットの検証が必要な場合には有利となる。また、秘密分散方式やマルチパーティ計算（MPC）など、異なる暗号基盤との比較評価も今後の課題となる。

6.4 実運用における規制・税務上の課題

分散型ベッティングシステムは、各国のギャンブル規制や税務要件に適合する必要がある。多くの法域では、ギャンブル事業者に対して免許取得や顧客本人確認（KYC）、資金洗浄対策（AML）が義務付けられており、これらを満たさない場合は違法となる可能性がある。また、払戻金は課税対象となる場合が多く、利用者の居住国ごとに異なる税務処理を考慮する必要がある。特に、匿名性の高いシステムでは課税当局による所得捕捉が困難になるため、法的要求とプライバシー保護のバランスを慎重に設計する必要がある。国際的な利用を想定する場合は、多国間の規制調和や越境データ移転の法的制約にも対応できる運用モデルが求められる。

7. 結論と今後の課題

本研究では、パリミュチュエル方式のベッティングにおいて発生するプライバシー侵害の問題に対し、加法準同型暗号とバッチ処理を組み合わせたプロトコルを提案した。本手法は、各ベット内容を暗号化してブロックチェーンに記録し、一定期間または件数ごとに集計・復号を行うことで、個別ベットの特定や戦略模倣を困難にする。また、バッチ処理による匿名性向上と、ブロックチェーンによる透明性・検証可能性を両立させる構造を示した。さらに、脅威モデルに基づき、ベット内容秘匿性、集計過程と結果の検証可能性、法的要請に応じた特定可能性、ベット否認耐性という 4 つのセキュリティ要件を整理し、それらに関連する攻撃シナリオと防御策についても検討した。

加法準同型暗号は集計処理に適した特性を有するが、証明や条件付き計算を必要とする場面ではゼロ知識証明（ZKP）、秘密分散、マルチパーティ計算（MPC）など他の暗号技術が有効となる場合がある。将来的には、これらの方式を組み合わせたハイブリッド型プロトコルにより、匿名性・リアルタイム性・計算効率のバランスを最適化することが期待される。また、暗号方式の選択はイベント規模、参加者数、規制要件など運用環境に依存するため、利用シナリオごとの比較評価が今後の課題となる。

参考文献

[1] B. Adida. Helios: Web-based open-audit voting. In *Proceedings of the 17th USENIX Security Symposium*, 2008.

[2] Ava Labs. What is encrypted erc? https://docs.avacloud.io. Accessed: 2025-08-16.

[3] Ava Labs. Avalanche documentation, 2025.

[4] S. Bartolucci et al. Sharvot: secret share-based voting on the blockchain. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 88–96. IEEE, 2018.

[5] E. Ben-Sasson, A. Chiesa, C. Garman, et al. Zerocash: Decentralized anonymous payments from bitcoin. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2014.

[6] F. Brandt and T. Sandholm. Efficient privacy-preserving protocols for multi-unit auctions. In *International Conference on Financial Cryptography and Data Security*, pages 298–312. Springer, 2005.

[7] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In *EUROCRYPT*. Springer, 1997.

[8] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In *ACM Workshop on Privacy in the Electronic Society (WPES)*, 2005.

[9] A. Kiayias and M. Yung. Self-tallying elections and perfect ballot secrecy. In *ASIACRYPT*. Springer, 2002.

[10] T. Moore, N. Marshall, and E. Burger. Fortuna: A novel staked voting system for distributed parimutuel gaming. In *2022 IEEE International Conference on Blockchain (Blockchain)*, pages 244–249. IEEE, 2022.

[11] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[12] C. A. Neff. A verifiable secret shuffle and its application to e-voting. In *Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS)*, 2001.

[13] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in Cryptology — EUROCRYPT '99*, pages 223–238. Springer, 1999.

[14] T. Rocket, M. Yin, K. Sekniqi, and E. G. Sirer. Scalable and probabilistic leaderless BFT consensus through metastability. arXiv preprint arXiv:1906.08936, 2020.

[15] K. Sekniqi, D. Laine, S. Buttolph, and E. Sirer. Avalanche platform 2020/06/30, 2020.

[16] S. Suzuki and M. Yokoo. Secure generalized vickrey auction using homomorphic encryption. In *International Workshop on Security Protocols*, pages 137–146. Springer, 2003.

[17] H. Uedan, Y. Li, K. Sakiyama, and D. Miyahara. Parimutuel betting on Blockchain: A case study on horse racing. In L. Barolli, editor, *Advanced Information Networking and Applications*, volume 246 of *LNDECT*, pages 177–187, Cham, 2025. Springer.

[18] N. van Saberhagen, S. Noether, K. Sarang, et al. Bulletproofs in monero. https://web.getmonero.org/2018/10/18/bulletproofs.html, 2018.

[19] Y. Xu et al. Privacy-preserving double auction mechanism based on homomorphic encryption. *arXiv preprint arXiv:1909.07637*, 2019.