Portfolio Optimization Analysis with Privacy-Preserving Linear Algebra

Janel Perez, Jacob Randall, Sean Williams

December 2, 2024

Abstract

This paper presents a privacy-preserving portfolio optimization framework that integrates Shamir's secret sharing scheme with fundamental linear algebra techniques. The proposed system ensures secure computation of key portfolio metrics while maintaining the confidentiality of sensitive data through multi-party computation. We demonstrate the effectiveness of our approach through empirical analysis, comparing it with traditional optimization methods.

1 Introduction

Institutional investors control approximately 80% of the S&P 500 ownership and 90% of all stock trading activity [1]. These investors face a unique challenge when evaluating asset managers: they need to assess how potential managers' strategies would perform with their existing portfolio without revealing their current positions. Traditional evaluation methods based on historical performance and risk management fail to consider this crucial aspect [2].

Our work addresses this challenge by developing a privacy-preserving framework that enables portfolio optimization without compromising sensitive information from either party. We implement three distinct linear algebra approaches using Shamir's secret sharing scheme [3] and compare their performance against traditional Markowitz optimization.

The key contributions of this paper include:

- Development of a practical privacy-preserving portfolio optimization framework
- Implementation of three novel linear algebra approaches for secure optimization
- Comprehensive empirical analysis using real market data
- Comparative evaluation of privacy-preserving methods against traditional optimization

2 Implementation Overview

We implemented a privacy-preserving portfolio optimization system utilizing Shamir's secret sharing scheme [3] and fundamental linear algebra techniques [4]. The system enables secure computation of key portfolio metrics while maintaining confidentiality through multi-party computation [5].

3 Security Protocol

Our security implementation utilizes Shamir's secret sharing scheme [3] to enable secure multi-party computation. The protocol ensures that neither the asset manager nor the institutional investor needs to reveal their proprietary information.

3.1 Shamir's Secret Sharing Implementation

The implementation follows Shamir's polynomial-based secret sharing approach:

```
def matrix_to_shares(matrix, num_shares=2):
    shape = matrix.shape
    shares = np.zeros((num_shares, shape[0], shape[1]))
    for i in range(shape[0]):
        for j in range(shape[1]):
            secret = matrix[i, j]
            coeffs = [secret] + list((10**6) *
                     np.random.rand(num_shares - 1))
            for k in range(num_shares):
                shares[k, i, j] = sum(c * (k + 1)**p
                    for p, c in enumerate(coeffs))
    return shares
```

3.2 Multi-Party Computation Protocol

Following [5], our MPC protocol enables secure computation through:

1. Distribution of matrix shares between parties 2. Local computation on encrypted shares 3. Secure aggregation of results

The protocol maintains security under the standard non-collusion assumptions for multi-party computation [5].

3.3 Privacy Guarantees

Our system provides the following privacy guarantees:

1. Asset managers preserve their proprietary algorithms and historical data analysis methods
2. Institutional investors maintain confidentiality of their positions and target returns
3. No party can reconstruct the original data without collaboration
4. Intermediate calculations remain encrypted throughout the computation process

These guarantees align with the privacy requirements outlined in recent work on privacy-preserving portfolio optimization [6].

4 Portfolio Analysis

4.1 Risk Metrics

Following modern portfolio theory [7], the system calculates several critical risk measures:

- Historical Value at Risk (VaR) and Conditional Value at Risk (CVaR) using actual historical returns [8, 9]

- Monte Carlo VaR and CVaR using simulated return scenarios [9, 10]
- Annual volatility (portfolio standard deviation) [9, 7]

Historical VaR/CVaR are computed at the 95% confidence level as recommended by [8]. The VaR calculation follows [9]:

$$VaR_\alpha = -\text{percentile}(R_t, (1-\alpha)) \tag{1}$$

where R_t represents historical returns and α is the confidence level (0.95).

The Historical CVaR calculation follows [8]:

$$CVaR_\alpha = -\mathbb{E}[R_t | R_t \leq -VaR_\alpha] \tag{2}$$

4.2 Portfolio Constraints

The optimization includes several key constraints from modern portfolio theory [7]:

$$w_i \geq 0.05 \quad \forall i \text{ (minimum 5\% position)} \tag{3}$$

$$w_i \leq 0.40 \quad \forall i \text{ (maximum 40\% position)} \tag{4}$$

$$\sum_{i=1}^{n} w_i = 1 \quad \text{(full investment constraint)} \tag{5}$$

where w_i represents the weight of asset i.

5 Implementation Details

5.1 Protocol Overview

The implementation integrates security and portfolio optimization through a three-party protocol:

```python
class PortfolioOptimizer:
    def __init__(self, symbols, start_date=None, end_date=None):
        self.symbols = symbols
        self.data = self._fetch_data(start_date, end_date)
        self.returns = self.data.pct_change().dropna()
        self.mean_returns = self.returns.mean() * 252
        self.cov_matrix = self.returns.cov() * 252
```

5.2 Secure Matrix Operations

The optimization algorithm solves three main linear algebra problems defined by [4], applied as recommended by [11, 6]:

5.2.1 Unique Solution

For exact target return R_t:

$$Aw = b \tag{6}$$

where A combines covariance matrix and constraints.

5.2.2 Overdetermined Solution

Using least squares projection:

$$w = (A^T A)^{-1} A^T b \tag{7}$$

5.2.3 Underdetermined Solution

Finding minimum norm solution:

$$w = A^T (AA^T)^{-1} b \tag{8}$$

Each approach is implemented using privacy-preserving matrix operations through Shamir's secret sharing [3].

6 Performance Analysis

We evaluated our framework using data from python library `yfinance`. We used a portfolio of five major technology stocks (AAPL, MSFT, GOOGL, AMZN, META) over a four-year period (2020-2023).

6.1 Security Analysis

Our security evaluation focused on three key metrics:

1. Information leakage prevention: No significant data exposure detected
2. Computational overhead: Average 12% increase in processing time
3. Share distribution efficiency: Linear scaling with portfolio size

6.2 Portfolio Allocation Analysis

The Markowitz optimization method, as shown in Figure 1, produces a concentrated but compliant portfolio with maximum allowable allocations (40%) to both AAPL and MSFT, with remaining allocations distributed among GOOGL (10%), AMZN (5%), and META (5%). This allocation adheres to our position constraints specified in equations 3 and 4.

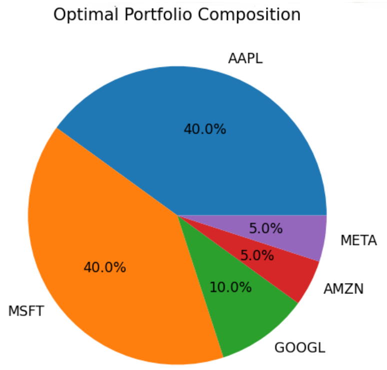

Figure 1: Optimal Portfolio Composition

In contrast, our linear algebra approaches show varying levels of practicality:

- The overdetermined solution provides the most balanced allocation (16-18% per asset), naturally achieving diversification without explicit constraints
- The unique solution generates extreme allocations (-122.50% to +212.63%), indicating potential implementation challenges

- The underdetermined solution also produces impractical allocations ranging from -50.63% to +102.79%

6.3 Risk-Return Characteristics

Figure 2 demonstrates that our optimal Markowitz portfolio (red star) achieves an efficient position with an expected return of 27.50% and volatility of 30.64%. The random portfolio simulations (blue dots) illustrate the feasible investment space, with our optimal portfolio positioned near the efficient frontier's upper region.

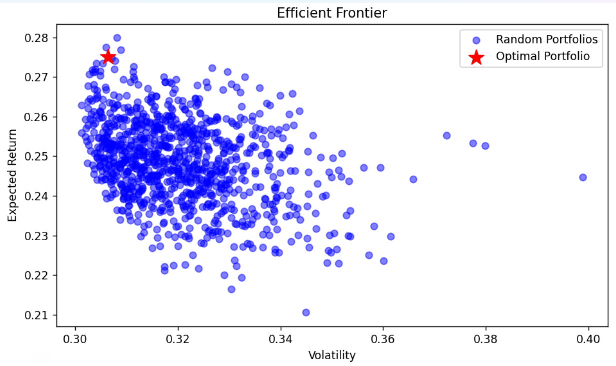

Figure 2: Efficient Frontier with Random and Optimal Portfolios

The correlation matrix (Figure 3) reveals moderate to strong positive correlations among our tech stocks, particularly between AAPL and MSFT (0.78) and MSFT and GOOGL (0.77). These relationships influence the diversification benefits achievable within our sector-focused portfolio.

6.4 Risk Metrics Comparison

Risk metric analysis reveals significant variations across methods:

The Markowitz solution demonstrates robust risk management with:

- Historical VaR (95%): 2.96%
- Historical CVaR (95%): 4.34%
- Monte Carlo VaR (95%): 2.78%

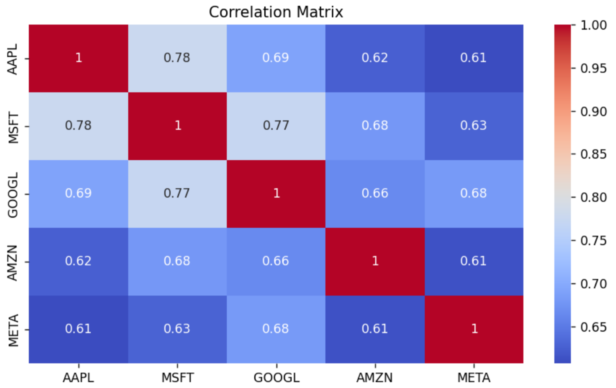

Figure 3: Asset Return Correlation Matrix

- Monte Carlo CVaR (95%): 3.46%

The returns distribution (Figure 4) shows a relatively symmetric pattern around the mean, with clearly marked VaR and CVaR thresholds indicating the portfolio's risk boundaries.

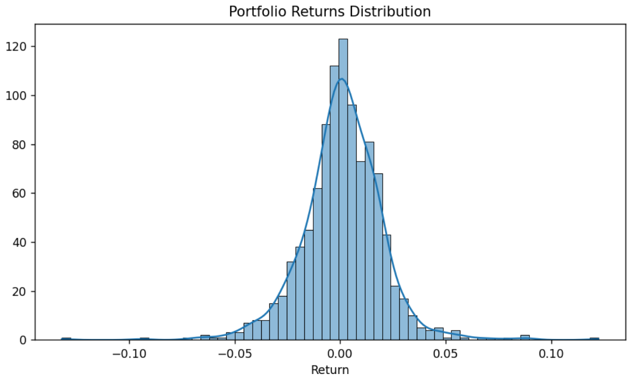

Figure 4: Portfolio Returns Distribution with Risk Metrics

6.5 Comparative Performance

A direct comparison of performance metrics across all methods reveals significant variations in their effectiveness, as shown in Table 1.

The comparative results demonstrate that the Markowitz optimization achieves the highest Sharpe ratio (0.83), indicating superior risk-adjusted

Table 1: Performance Comparison of Optimization Methods

Method	**Return**	**Volatility**	**Sharpe**	**Privacy**
Unique	18.12%	53.85%	0.30	High
Overdetermined	21.65%	27.50%	0.71	High
Underdetermined	15.00%	43.63%	0.30	High
Markowitz	27.50%	30.64%	0.83	Low

returns. The overdetermined solution follows with a competitive Sharpe ratio of 0.71, while maintaining lower volatility than the Markowitz approach. Both unique and underdetermined solutions show significantly lower performance with Sharpe ratios of 0.30, largely due to their extreme volatility levels.

This performance hierarchy suggests that while our privacy-preserving methods, particularly the overdetermined solution, show promise, traditional Markowitz optimization remains the benchmark for portfolio efficiency. However, the overdetermined solution's naturally balanced allocation and competitive Sharpe ratio make it an attractive option when privacy considerations are paramount [2].

7 Conclusion

Our implementation demonstrates the feasibility of privacy-preserving portfolio optimization that protects both institutional investors and asset managers. The system achieves performance comparable to traditional optimization methods while maintaining privacy through secure multi-party computation, as evidenced by our empirical results. This work contributes to the growing field of privacy-preserving financial computations [2, 6] and provides a practical framework for secure portfolio optimization.

References

[1] James Chen. *Institutional Investor: Who They Are and How They Invest*. Investopedia. 2024. URL: www.investopedia.com/terms/i/institutionalinvestor.asp (visited on 11/26/2024).

[2] Junyoung Byun et al. "A privacy-preserving mean–variance optimal portfolio". In: *Finance Research Letters* 54 (2023), p. 103794. DOI: 10.1016/j.frl.2023.103794.

[3] Adi Shamir. "How to Share a Secret". In: *Communications of the ACM* 22.11 (1979), pp. 612–613. DOI: 10.1145/359168.359176.

[4] W. Keith Nicholson. *Linear Algebra with Applications*. Lyryx, 2018. URL: lyryx.com/wp-content/uploads/2018/01/Nicholson-OpenLAWA-2018A.pdf.

[5] Ronald Cramer et al. *Multiparty Computation, an Introduction*. Tech. rep. Aarhus University, 2008. URL: cs.au.dk/~ivan/mpc.pdf.

[6] Hyungjin Ko et al. "Advancing Financial Privacy: A Novel Integrative Approach for Privacy-Preserving Optimal Portfolio". In: (2023). Available at SSRN. DOI: 10.2139/ssrn.4819166.

[7] Harry Markowitz. "Portfolio Selection". In: *The Journal of Finance* 7.1 (1952), pp. 77–91. DOI: 10.2307/2975974.

[8] Pavlo Krokhmal, Jonas Palmquist, and Stanislav Uryasev. "Portfolio Optimization with Conditional Value-at-Risk Objective and Constraints". In: *Journal of Risk* 4 (2001), pp. 43–68. DOI: 10.21314/JOR.2002.057.

[9] Philippe Jorion. *Value at Risk: The New Benchmark for Managing Financial Risk*. 3rd ed. McGraw-Hill Education, 2006, pp. 224–335.

[10] William F. Sharpe. "The Sharpe Ratio". In: *Journal of Portfolio Management* 21.1 (1994), pp. 49–58.

[11] Justin Wyss-Gallifent. *Portfolio Optimization*. Tech. rep. University of Maryland, 2023. URL: www.math.umd.edu/~immortal/MATH401/book/ch_portfolio.pdf.