Research Report

Introduction:

As a member of the Privacy Technologies for Financial Intelligence (PTFI) team, I have been exploring the concept of Secure Multi-Party Computation (MPC) and its potential applications in the financial domain. MPC is a cryptographic technique that allows multiple parties to perform computations on their private inputs without revealing the actual values to each other. This technology has significant implications for enhancing privacy and security in financial intelligence, enabling secure collaboration and data sharing among different entities.

Overview of MPC:

MPC is based on the principle of performing computations on secret-shared data. Each party involved in the computation splits their private input into shares and distributes them among the other parties. The computations are then performed on these shares, and the final result can be obtained by combining the computed shares. The key advantage of MPC is that it allows parties to compute a function on their collective inputs while keeping their individual inputs private.

Simplified Code Example:

To illustrate the basic concept of MPC, I have provided a simplified code example in the report. The code simulates a scenario where two parties want to perform a secure bitwise XOR operation on their private inputs without revealing the actual values to each other. The code demonstrates the steps involved in sharing secrets among parties, performing secure computations on the shares, and obtaining a public result without disclosing the individual inputs.

It's crucial to emphasize that the code example is a simplified simulation and does not represent a secure MPC protocol. In real-world MPC implementations, advanced cryptographic techniques, such as homomorphic encryption and secret sharing schemes, are used to ensure the privacy and security of the data. The actual protocols are more complex and involve secure communication channels and robust mathematical foundations.

```python
import random

def bitwise_xor(a, b):
  """Simulates bitwise XOR operation on bits a and b."""
  return (a + b) % 2

def share_secret(secret, num_parties):
  """Simulates sharing a secret using random bits among parties."""
  shares = []
  remaining_bits = bin(secret)[2:].zfill(num_parties)  # Convert secret to binary string with leading zeros
  for i in range(num_parties):
    share = int(remaining_bits[i], 2)
    share ^= random.getrandbits(1)  # XOR with random bit for obfuscation (not secure in real MPC)
    shares.append(share)
  return shares

def main():
  # Define number of parties
  num_parties = 2

  # Define secret inputs for each party (replace with actual bit values)
  party1_input = 1  # 1 in binary is 001, so LSB is 1
  party2_input = 0  # 0 in binary is 000

  # Simulate sharing secret bits
  party1_shares = share_secret(party1_input, num_parties)
  party2_shares = share_secret(party2_input, num_parties)

  # Simulate secure addition using XOR (not secure in real MPC)
  result_shares = []
  for i in range(num_parties):
    result_shares.append(bitwise_xor(party1_shares[i], party2_shares[i]))

  # Combine shares (in real MPC, this would involve collaboration and secret reconstruction)
  public_result = sum(result_shares) % 2  # Recover the least significant bit

  # Print results (for demonstration purposes only)
  print(f"Party 1's shares: {party1_shares}")
  print(f"Party 2's shares: {party2_shares}")
  print(f"Public result (LSB of sum): {public_result}")
```

```
if __name__ == "__main__":
 main()
```

Applications in Financial Intelligence:

MPC has numerous potential applications in the financial intelligence domain. Some specific use cases include:

- **Secure Data Aggregation:** MPC can enable financial institutions to securely aggregate sensitive data from multiple sources without revealing the individual contributions. This can facilitate collaborative analysis and insights while preserving the privacy of each institution's data.
- **Privacy-Preserving Data Analysis:** MPC allows financial institutions to perform joint data analysis and machine learning on sensitive customer data without compromising privacy. It enables the extraction of valuable insights from collective data while ensuring that individual records remain confidential.
- **Fraud Detection and Risk Assessment:** MPC can be employed to securely compute risk scores or detect fraudulent activities across multiple financial institutions. By sharing relevant data in a privacy-preserving manner, institutions can collaborate to identify and mitigate risks more effectively.

Challenges and Considerations:

While MPC offers significant benefits for privacy and security in financial intelligence, there are some challenges and considerations to keep in mind:

- **Computational Overhead:** MPC protocols often involve complex cryptographic operations, which can result in increased computational overhead compared to traditional computations. Efficient implementations and optimizations are necessary to ensure practical feasibility.
- **Communication Overhead:** MPC requires secure communication channels among the participating parties. The amount of data exchanged during the computation can be substantial, especially for large-scale

computations. Efficient communication protocols and network infrastructure are essential.

- **Trust and Security Assumptions:** MPC relies on certain trust and security assumptions, such as the honesty of the majority of participants and the security of the underlying cryptographic primitives. Careful evaluation and analysis of these assumptions are necessary to ensure the robustness and security of MPC implementations.

Conclusion:

Secure Multi-Party Computation (MPC) is a promising technology for enhancing privacy and security in financial intelligence. It enables multiple parties to collaborate and perform computations on sensitive data without revealing the individual inputs. The simplified code example provided in this report demonstrates the basic principles of MPC, although it is important to note that secure MPC implementations require advanced cryptographic techniques and careful design.

MPC has various potential applications in the financial domain, including secure data aggregation, privacy-preserving data analysis, fraud detection, and risk assessment. However, it is crucial to consider the challenges and considerations associated with MPC, such as computational overhead, communication overhead, and trust and security assumptions.

As the PTFI team continues to explore privacy technologies for financial intelligence, MPC represents a valuable tool to enable secure collaboration and data sharing while preserving the confidentiality of sensitive information. By leveraging established MPC frameworks and protocols and addressing the associated challenges, we can harness the power of MPC to enhance privacy and security in our financial intelligence workflows.