Prime Match: A Privacy Preserving Inventory Matching System

Antigoni Polychroniadou

(J.P. Morgan AI Research & AlgoCRYPT CoE)

joint work with: Gilad Asharov (Bar Ilan University), Ben Diamond, Tucker Balch, Hans Buehler, Richard Hua, Suwen Gu, Gregory Gimler, Manuela Veloso
Prime Match: Extended Team

Mike Reich, Vaibhav Popat, Sitaraman Rajamani, Dan Stora, James Mcilveen, Oluwatoyin Aguiyi, Niall Campbell, Wanyi Jiang, Grant McKenzie, Steven Price, Vinay Gayakwad, Srikanth Veluvolu, Noel Peters and Jason Sippel
Motivation

- First one-time application of MPC (electronic double auction): Sugar bit auction [Bogetof et al. 2008]
- MPC Dashboard

- Identify a real-world problem for MPC in the traditional financial world
- Academic work on privacy preserving darkpools [CSA19, BPV20, CSA20, MDPB23]
- Prime Match is the first MPC auction running live in the traditional financial world.
Outline

- Prime Match Problem Statement & Motivation
- Cryptographic Contributions in Prime Match
- From Proof of Concept (PoC) to Product
  - Pre-production and Production challenges
- Cryptographic Solution
- Demo
Starting point: Inventory Matching **without** Privacy

**Inventory Matching Process:**

- **JPMC** Prime Brokerage desk **publishes daily** a list of inventory at a discount **to clients**
- Inventory includes a list of symbols, sides, volumes, rates for trades

 Toy Inventory List Example:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Side</th>
<th>Vol.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAPL</td>
<td>Long</td>
<td>800</td>
</tr>
<tr>
<td>MSFT</td>
<td>Short</td>
<td>200</td>
</tr>
<tr>
<td>GOOG</td>
<td>Long</td>
<td>300</td>
</tr>
</tbody>
</table>

- JPMC processes **incoming trades** chosen from the list **by clients**

**Internal Data**
- JPMC inventory
- Financing rates
- Other firm / market data
Starting point: Inventory Matching **without** Privacy

Baseline: Full Inventory

Version 1: Reduced Inventory

Version 2: Inventory with smart noise
Starting point: Inventory Matching **without** Privacy

**Inventory Matching Process:**

**Problems with Inventory Matching:**

- JPM reveals a large portion of its inventory list
- Clients raised concerns about potential leakage of their past trades included in the list
- Reduced inventory list available for matching
- Clients do not send to JPMC their inventory!
Prime Match: Inventory Matching with Privacy

Solution based on Secure Multiparty Computation
Overview of Secure Multi-Party Computation (MPC)

- Enables different organizations / parties / entities to perform a joint computation over their inputs (i.e. trade lists) while keeping it private
- Encryption ≠ Secure Multiparty Computation:
  - Encryption: Parties trust each other, but do not trust some external that might eavesdrop to the conversation
  - Secure Computation: Parties do not trust each other or cannot share their data, but still want to compute on their joint private inputs
- Feasibility [Yao82, GMW87, BGW88, CCD88]: every distributed computation can be computed privately

Client / Partner A
- Internal or External
- Firm Data
  - Firm / Client Positions
  - Internal rates / prices
  - Other internal data
- Model Data
  - JPMC projected Internalization
  - Expected dividends
  - Expected index composition
- Market Data
  - Prices, rates, dividends, etc
  - Index composition
  - Spot, Futures

Encrypt

Secure Computation Engine

Encrypt

Output

Client / Partner B
- Internal or External
Prime Match: Inventory Matching with Privacy

**Main ingredient:** New secure comparison protocol for computing the minimum between two values such as min(100,800)
Prime Match: Privacy-Preserving Inventory Matching with 2PC

Proposed Service (via Secure Two-Party Computation)
- Client sends over their encrypted trade list
- Secure engine provides list of matching trades against its *full* inventory list

**Benefits:**
- More tailored trades matching exact needs of clients; increased inventory availability
- JPM is not exposed to client’s trade list unless there is a match; privacy is preserved:
  - No risk of information leakage to JPMC.
  - Unmatched positions are not revealed.

![Diagram](image)
Prime Match: Privacy-Preserving Inventory Matching with MPC

**Proposed Service (via Secure Multi-Party Computation)**
- Client sends over their encrypted trade list
- Secure engine provides list of matching trades against its full inventory list
- Support provided to match trades against other clients

**Benefits:**
- More tailored trades matching exact needs of clients with the ability to internalize across multiple clients; significantly increased inventory availability
- JPM is not exposed to client’s trade list unless there is a match; privacy is preserved:
  - No risk of information leakage to JPMC.
  - No risk of information leakage to other clients.
  - Unmatched positions are not revealed.

**Toy Example:**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Side</th>
<th>Vol.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAPL</td>
<td>Short</td>
<td>100</td>
</tr>
</tbody>
</table>

Secure Matching Engine

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Side</th>
<th>Vol.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAPL</td>
<td>Long</td>
<td>0</td>
</tr>
<tr>
<td>AAPL</td>
<td>Short</td>
<td>0</td>
</tr>
</tbody>
</table>

J.P. Morgan

AlgoCRYPT CoE

AI Research
Prime Match: Privacy-Preserving Inventory Matching with MPC

Proposed Service (via Secure Multi-Party Computation)
- Client sends over their encrypted trade list
- Secure engine provides list of matching trades against its full inventory list
- Support provided to match trades against other clients

Benefits:
- More tailored trades matching exact needs of clients with the ability to internalize across multiple clients; significantly increased inventory availability
- JPM is not exposed to client's trade list unless there is a match; privacy is preserved:
  - No risk of information leakage to JPMC.
  - No risk of information leakage to other clients.
  - Unmatched positions are not revealed.

Toy Example:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Side</th>
<th>Vol.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAPL</td>
<td>Short</td>
<td>100</td>
</tr>
<tr>
<td>AAPL</td>
<td>Long</td>
<td>500</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Side</th>
<th>Vol.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAPL</td>
<td>Long</td>
<td>0</td>
</tr>
<tr>
<td>AAPL</td>
<td>Short</td>
<td>0</td>
</tr>
</tbody>
</table>

J.P. Morgan

AlgoCRYPT CoE
AI Research
Cryptographic Contributions in Prime Match

Two-Party Secure comparison:

Three-Party Secure comparison with a third party acting as the facilitator:

New two-round secure linear comparison protocol for computing the minimum between two values with one malicious corruption; no preprocessing

Prior works: non-linear; log round

Improved version of SecureNN [WaghGuptaChandran19]
Prime Match: Pre Production and Production challenges
Prior to Prime Match, **No** financial institution had ever utilized Multi-Party Computation (MPC) technology.

The bank **has** long-standing clients.

No financial institution had taken the initiative to implement privacy preserving auctions.
Prime Match: Proof of Concept (PoC) Challenges

1. Connected with Quantitative Research
2. Assess the demand for a type of privacy-preserving auction
3. Design & Demo 1st Prime Match PoC

Internal buy-in to the product

2019
Prime Match: Pre-Production Challenges

1. Connected with clients
2. Demo PoC to Clients
3. Gather comprehensive client feedback; requirements and conditions for using Prime Match

External buy-in to the product

2020
Prime Match: Pre-Production Challenges

Given the innovative nature of the product, the green light for production was given after a long process.

1. Connected with clients
2. Demo PoC to Clients
3. Gather comprehensive client feedback; requirements and conditions for using Prime Match

Decided to move in production
Prime Match: Client Requirements

- **No communication with other clients**, only communication with the bank
- **No heavy installation of code** on client’s machines - a web-based application was required
- Client computation should be **minimal**
- **No resources** for preprocessing data
- **Stronger security guarantees** than semi-honest security
- **Peer review** of the solution
- **Frequent** auctions
Prime Match: Tech Challenges - Architecture
Prime Match: Cryptographic Solution
Cryptographic Contributions in Prime Match

Three-Party Secure comparison with a third party acting as the facilitator:

Three parallel executions

Secret Shared Inputs

\[ a = a_1 + a_2 \]

\[ b_1 \]

\[ b_1 \]

\[ d_1 = \min(a_1, b_1) \]

\[ d = d_1 + d_2 \]

\[ d_2 = \min(a_2, b_2) \]

New **two-round** secure linear comparison protocol
Cryptographic Contributions in Prime Match

Three-Party Secure comparison with a third party acting as the facilitator:

Three parallel executions

\[ a = a_1 + a_2 \]
\[ b = b_1 + b_2 \]

Committed Secret Shares

\[ \text{Com}(d) = \text{Com}(d_1) + \text{Com}(d_2) \]

New **two-round** secure linear comparison protocol
Cryptographic Contributions in Prime Match

Three-Party Secure comparison with a third party acting as the facilitator:

Registration phase +
Three parallel executions

New **two-round** secure linear comparison protocol
Prime Match: High Level Solution

Registration Phase: Need for committed computation

Matching Phase: web based support $\rightarrow$ low round complexity and communication

Improved version of SecureNN [WaghGuptaChandran19]

High level of Comparison (min) circuit: (output 1 if any $d_i=0$)

- $P_0$, $P_1$ compute shares of:

$$c_i = 1 - a_i + b_i + \sum_{j>i} r_j (a_j - b_j)$$

- $P_0$, $P_1$ send to bank shares of $s_i \cdot c_i$

- Bank reconstructs $d_i = s_i \cdot c_i$ and outputs 1 ($a>b$) if any $s_i \cdot c_i = 0$
Demo
Prime Match Demo: Auction Runs
Prime Match Demo: Registration Phase

The image shows a screenshot of a Prime Match Demo interface. The registration phase appears to be in progress, with a timeline indicating the current run timing from 12:20 to 12:25 pm, with 2m 01s until matching.

The interface includes options to download a template and browse files. The legal disclaimer at the bottom mentions that the securities listed in the report are indicative of securities that J.P. Morgan Securities plc, J.P. Morgan SE, J.P. Morgan Securities LLC, or JPMorgan Chase Bank, National Association, London Branch (together J.P. Morgan) might reference in an equity swap transaction with you. The availability of swap transactions over such securities and the indicated rates can change at any time, and the rates in this report are expressed in fees. This report does not constitute an agreement or commitment by J.P. Morgan to enter into a swap transaction referring to such securities (whether at the indicated rate or otherwise). Accordingly, this statement cannot be relied upon at any time to ensure a swap transaction with J.P. Morgan referencing such securities. These materials are further subject to disclaimer, which you should read carefully. This disclaimer can be viewed at [link].

The information in this report is intended to be used for Prime allocation and efficiency purposes only; it should not be used for investment decision or alpha generation purposes.

(Images of the Prime Match Demo interface with various components and options for file upload and download are present.)
Prime Match Demo: Registration Phase
Prime Match Demo: Registration Phase
Prime Match Demo: Registration Phase
Prime Match Demo: Matching Phase
Prime Match Demo: Matching Phase
**Prime Match Demo: Matching Phase**

### Current Run

- **Date:** 21st March 2023 - 12:25 pm
- **Status:** Waiting To Start

### Ax Registration

- **Date:** 12:20

### Matching

- **Date:** 12:25
- **Time:** 03m 54s until Finished Matching...

### Table: Security Match Results

<table>
<thead>
<tr>
<th>Symbol Type</th>
<th>Symbol</th>
<th>ISIN</th>
<th>SEDOL</th>
<th>CUSIP</th>
<th>Name</th>
<th>Direction</th>
<th>Threshold Qty</th>
<th>Full Qty</th>
<th>Match Result</th>
<th>Status</th>
<th>Matched Qty</th>
<th>Spread (bps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLOOMBERG_ID</td>
<td>TEST NA_1</td>
<td>TEST NA_1</td>
<td>TEST NA_1</td>
<td>TEST NA_1</td>
<td>TEST NA_1</td>
<td>LONG</td>
<td>80</td>
<td>90</td>
<td>Partial Match</td>
<td>Partial Match</td>
<td>80</td>
<td>15</td>
</tr>
<tr>
<td>BLOOMBERG_ID</td>
<td>TEST NA_2</td>
<td>TEST NA_2</td>
<td>TEST NA_2</td>
<td>TEST NA_2</td>
<td>TEST NA_2</td>
<td>LONG</td>
<td>20</td>
<td>440</td>
<td>Partial Match</td>
<td>Partial Match</td>
<td>20</td>
<td>15</td>
</tr>
<tr>
<td>BLOOMBERG_ID</td>
<td>TEST NA_3</td>
<td>TEST NA_3</td>
<td>TEST NA_3</td>
<td>TEST NA_3</td>
<td>TEST NA_3</td>
<td>LONG</td>
<td>80</td>
<td>90</td>
<td>Partial Match</td>
<td>Partial Match</td>
<td>80</td>
<td>15</td>
</tr>
<tr>
<td>BLOOMBERG_ID</td>
<td>TEST NA_4</td>
<td>TEST NA_4</td>
<td>TEST NA_4</td>
<td>TEST NA_4</td>
<td>TEST NA_4</td>
<td>LONG</td>
<td>80</td>
<td>90</td>
<td>Partial Match</td>
<td>Partial Match</td>
<td>80</td>
<td>15</td>
</tr>
<tr>
<td>BLOOMBERG_ID</td>
<td>TEST NA_5</td>
<td>TEST NA_5</td>
<td>TEST NA_5</td>
<td>TEST NA_5</td>
<td>TEST NA_5</td>
<td>LONG</td>
<td>20</td>
<td>440</td>
<td>Partial Match</td>
<td>Partial Match</td>
<td>20</td>
<td>15</td>
</tr>
<tr>
<td>BLOOMBERG_ID</td>
<td>TEST NA_6</td>
<td>TEST NA_6</td>
<td>TEST NA_6</td>
<td>TEST NA_6</td>
<td>TEST NA_6</td>
<td>LONG</td>
<td>80</td>
<td>90</td>
<td>Partial Match</td>
<td>Partial Match</td>
<td>80</td>
<td>15</td>
</tr>
<tr>
<td>BLOOMBERG_ID</td>
<td>TEST NA_7</td>
<td>TEST NA_7</td>
<td>TEST NA_7</td>
<td>TEST NA_7</td>
<td>TEST NA_7</td>
<td>LONG</td>
<td>80</td>
<td>90</td>
<td>Partial Match</td>
<td>Partial Match</td>
<td>80</td>
<td>15</td>
</tr>
<tr>
<td>BLOOMBERG_ID</td>
<td>TEST NA_8</td>
<td>TEST NA_8</td>
<td>TEST NA_8</td>
<td>TEST NA_8</td>
<td>TEST NA_8</td>
<td>LONG</td>
<td>20</td>
<td>440</td>
<td>Partial Match</td>
<td>Partial Match</td>
<td>20</td>
<td>15</td>
</tr>
<tr>
<td>BLOOMBERG_ID</td>
<td>TEST NA_9</td>
<td>TEST NA_9</td>
<td>TEST NA_9</td>
<td>TEST NA_9</td>
<td>TEST NA_9</td>
<td>LONG</td>
<td>80</td>
<td>90</td>
<td>Partial Match</td>
<td>Partial Match</td>
<td>80</td>
<td>15</td>
</tr>
<tr>
<td>BLOOMBERG_ID</td>
<td>TEST NA_10</td>
<td>TEST NA_10</td>
<td>TEST NA_10</td>
<td>TEST NA_10</td>
<td>TEST NA_10</td>
<td>LONG</td>
<td>20</td>
<td>440</td>
<td>Partial Match</td>
<td>Partial Match</td>
<td>20</td>
<td>15</td>
</tr>
<tr>
<td>BLOOMBERG_ID</td>
<td>TEST EMEA_11</td>
<td>TEST EMEA_11</td>
<td>TEST EMEA_11</td>
<td>TEST EMEA_11</td>
<td>TEST EMEA_11</td>
<td>LONG</td>
<td>80</td>
<td>90</td>
<td>Partial Match</td>
<td>Partial Match</td>
<td>80</td>
<td>15</td>
</tr>
<tr>
<td>BLOOMBERG_ID</td>
<td>TEST EMEA_12</td>
<td>TEST EMEA_12</td>
<td>TEST EMEA_12</td>
<td>TEST EMEA_12</td>
<td>TEST EMEA_12</td>
<td>LONG</td>
<td>80</td>
<td>90</td>
<td>Partial Match</td>
<td>Partial Match</td>
<td>80</td>
<td>15</td>
</tr>
</tbody>
</table>

---

*Information in this report is intended to be used for Prime allocation and efficiency purposes only. It should not be used for investment decision or alpha generation purposes.*

---

*LEGAL DISCLAIMER*
Prime Match Demo: Matching Phase

The securities listed in this report are indicative of securities that [J.P. Morgan Securities plc, J.P. Morgan SE, J.P. Morgan Securities LLC or JPMorgan Chase Bank, National Association, London Branch (together J.P. Morgan)] might reference in an equity swap transaction with you. The availability of swap transactions over such securities and the indicated rates can change at any time, the rates in this report are expressed in fees. This report does not constitute an agreement or commitment by J.P. Morgan to enter a swap transaction referring to such securities (whether at the indicated rates or otherwise). Accordingly this statement cannot be relied upon at any time to ensure a swap transaction with J.P. Morgan referencing such securities. These materials are further subject to disclaimer, which you should read carefully. This disclaimer can be viewed at: [http://www.jpmorgan.com/hqps/disclosures/market/algocrypt/](http://www.jpmorgan.com/hqps/disclosures/market/algocrypt/)

The information in this report is intended to be used for Prime allocation and efficiency purposes only; it should not be used for investment decision or alpha generation purposes.

LEGAL DISCLAIMER

RESET AXE
Conclusion

- **Identified a real-world problem for MPC** in which the privacy of the previous inventory matching procedure can be significantly enhanced.
- Prime Match protocols—bank-to-client inventory matching and client-to-client inventory matching—completely replace the current method which not only leaks information but also fails to identify potential matches.
  - Our protocols are novel and customized to the particular use case being addressed (privacy preserving auctions).
- At the core of our matching engine lies a new **two-round comparison** protocol that minimizes interaction and requires **only linear operations**.
- Prime Match protocols are implemented and run live for the first time, in production, by a major bank in the US – J.P. Morgan.
Future work:

1. **Fair matching** that ensures no single client can monopolize the majority of the inventory.
2. Extend MPC for:
   1. Privacy preserving *darkpools*
   2. Privacy preserving *portfolio optimization*
Prime Match: A Privacy Preserving Inventory Matching System

Thank you!

https://eprint.iacr.org/2023/400

antigoni.polychroniadou@jpmorgan.com
antigonipoly@gmail.com

J.P.Morgan