PET-Exchange: A Privacy Enhanced Trading Exchange using Homomorphic Encryption

David Hasselquist[1,2], Jacob Wahlman[1,3], Niklas Carlsson[1]

[1] Linköping University, Sweden
[2] Sectra Communications, Sweden
[3] Nasdaq, Inc.

Proc. International Conference on Privacy, Security, and Trust (PST), Copenhagen, Denmark, August 2023

Securities exchange

- Trading platforms
- Electronic shift
  - High-frequency trading
- Unfair, unethical, or illegal trading
  - Front running
  - Penny jumping
  - Insider trading

FINANCIAL TIMES

ETF Hub Exchange traded funds + Add to myFT

Insider traders use ETFs to front-run M&A deals, academics say

Research identifies $2.75bn worth of potential 'shadow trades' in US between 2009 and 2021


FINANCIAL TIMES
ETF Hub
Exchange traded funds
+ Add to myFT
Insider traders use ETI
M&A deals, academics
Research identifies $2.75bn worth of potent
between 2009 and 2021
REUTERS®
World
Business
Markets
Sustainability
More
U.S. Markets
Securities trader charged in New York with front-running employer's trades
Reuters
December 14, 2022 11:56 PM GMT+1 · Updated 8 months ago
Aa


FINANCIAL TIMES
ETF Hub
Exchange traded funds
+ Add to myFT
Insider t
M&A de
Research identif
between 2009 a
REUTERS®
World
Business
Markets
Sustainability
More
in New
mployer's
Aa
CNN BUSINESS
Markets
Tech
Media
Calculators
Videos
Prosecutors charge three investors with insider trading in Trump SPAC deal
By Matt Egan and Kara Scannell, CNN
Updated 12:58 PM EDT, Thu June 29, 2023
Donald Trump's media company owns Truth Social. Investors seeking a merger with his company were charged with insider trading.
New York (CNN) — Federal prosecutors arrested three investors on Thursday on insider trading charges related to a deal to take former President Donald Trump's media business public.

Securities trading

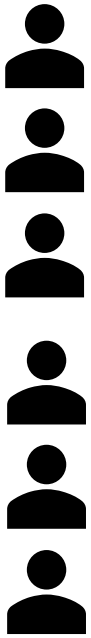
- Transparency in public exchanges
- Dark pools
  - Less transparent, lack of regulation
- Cryptography
  - May prevent unfair practices
- Homomorphic encryption
  - Not trivial due to large overheads

Contributions

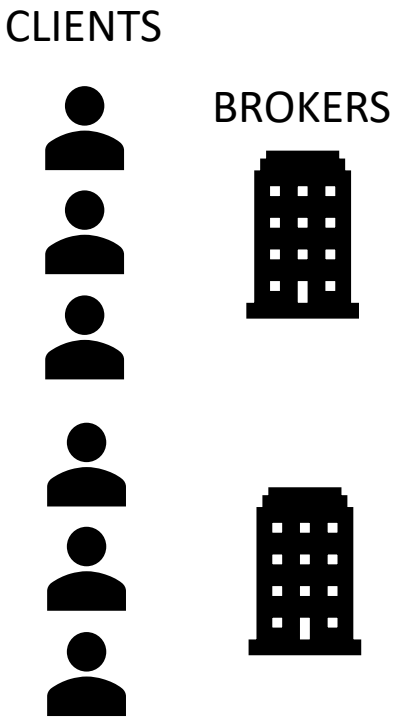
- We present PET-Exchange, a privacy-preserving trading framework using homomorphic encryption for trading securities, partially matching limit orders between multiple buyers and sellers
- Using various conditions and configurations, we provide insights into the most attractive tradeoffs applicable to a wide range of exchanges and use cases
- We provide insights into current performance bottlenecks and validate that we can achieve high accuracy with many decimals of precision

Securities exchange

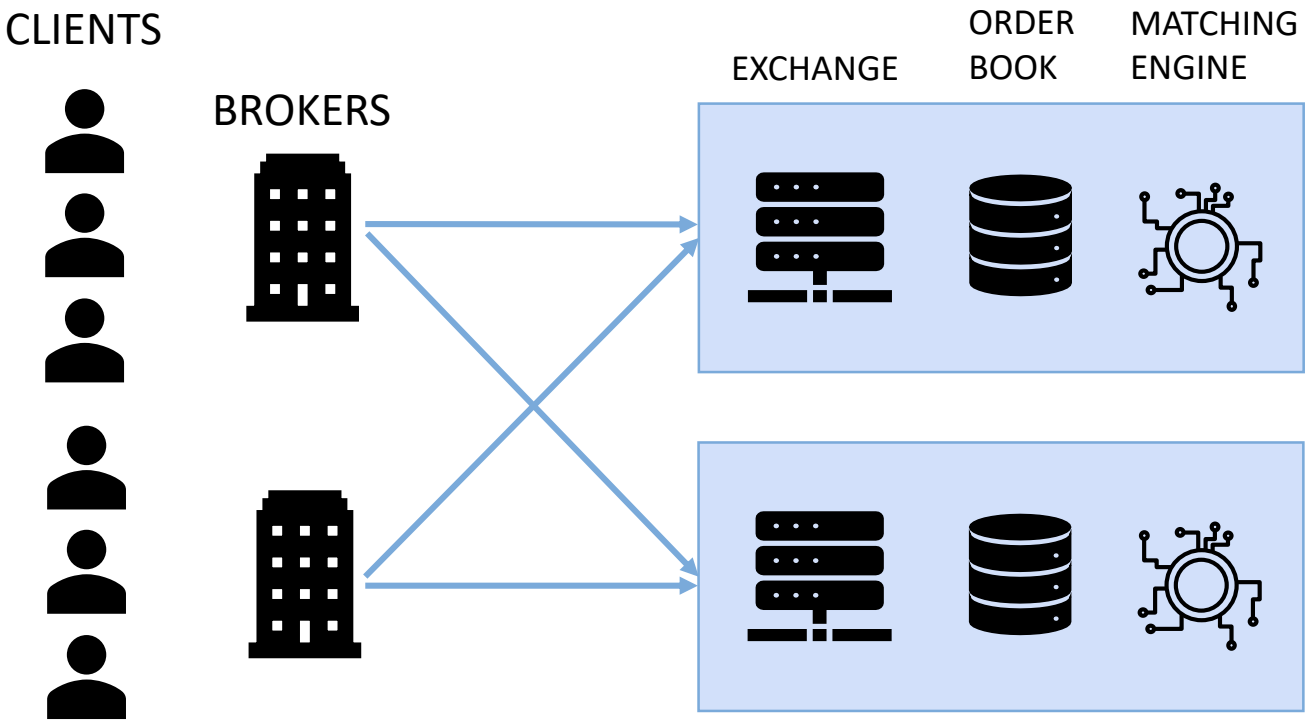
CLIENTS



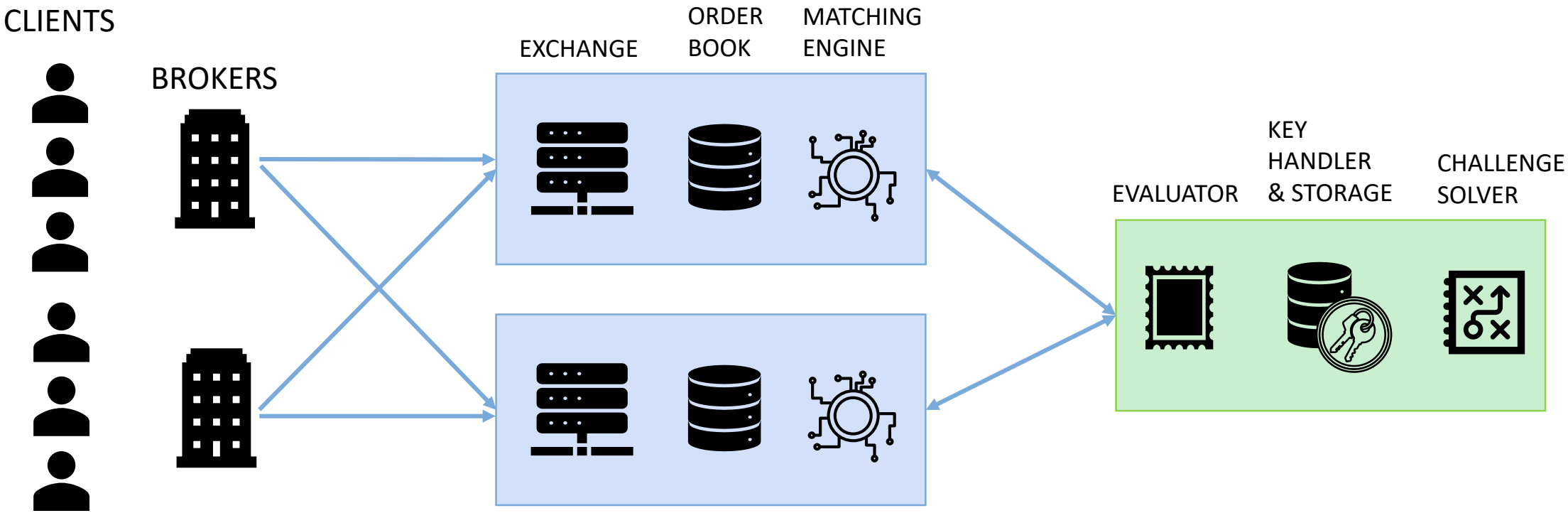
Securities exchange



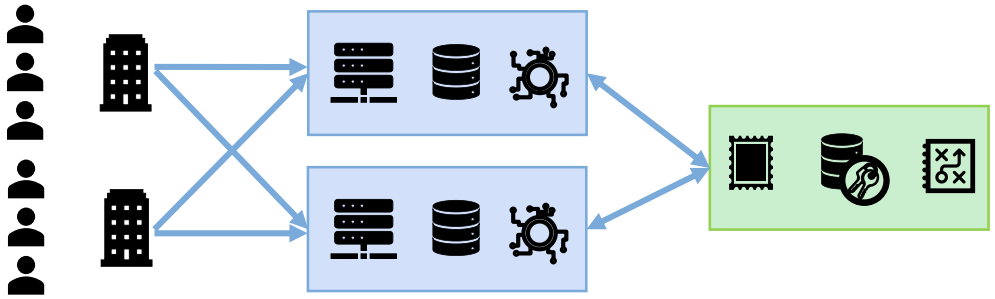
Securities exchange



PET-Exchange

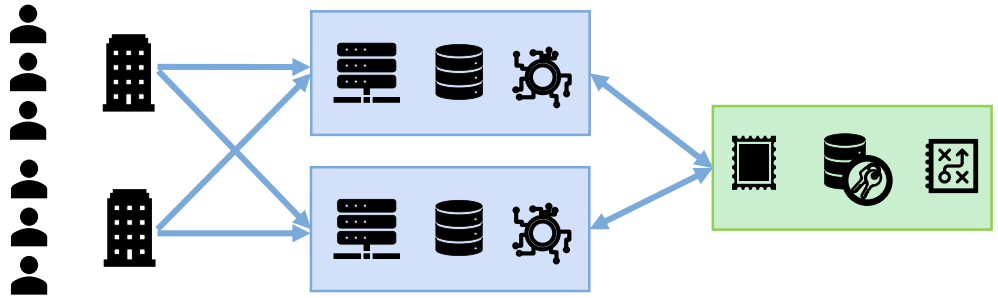


Encrypted order handling



- Order entry
  - Sorted order book
  - Binary search on encrypted orders
- Values cannot be compared directly
  - Local comparison
  - Remote comparison

Encrypted order handling

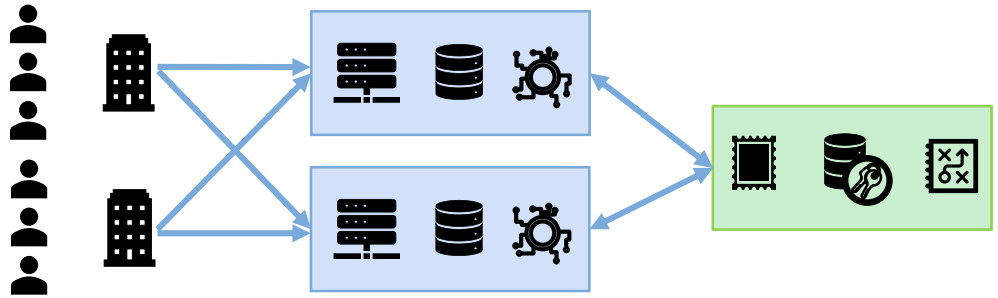


- Local comparison
  - Approximation

$$k = f(\theta^A,\ \theta^B) \approx \begin{cases} 0, & \text{if } \theta^A < \theta^B \\ 0.5, & \text{if } \theta^A = \theta^B \\ 1, & \text{if } \theta^A > \theta^B \end{cases}$$

  - Challenge creation + validation

Encrypted order handling

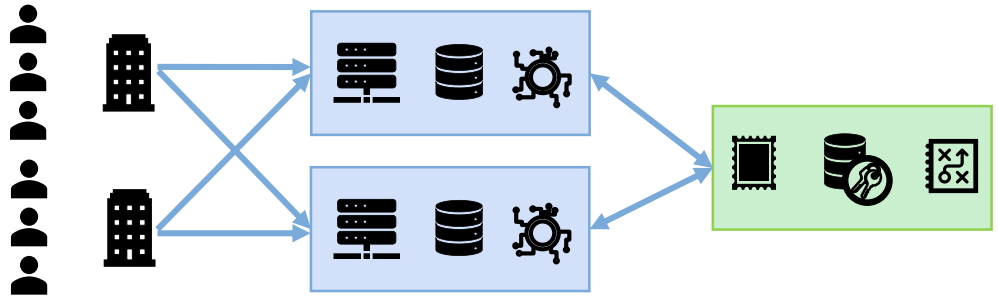


- Local comparison
  - Approximation

$$k = f(\theta^A,\ \theta^B) \approx \begin{cases} 0, & \text{if } \theta^A < \theta^B \\ 0.5, & \text{if } \theta^A = \theta^B \\ 1, & \text{if } \theta^A > \theta^B \end{cases}$$

  - Challenge creation + validation
- Remote comparison
  - Padded order values instead of approximation value

Encrypted order handling



- Order matching and execution
  - Local or remote comparison method
  - Homomorphic subtraction to continuously match partially filled orders

Configuration parameters

» CKKS configuration parameters and their overheads

Name	Level	Poly. modulus degree	Security level	E[Order size]	E[Remote challenge size]	E[Local challenge size]
CKKS-11	1	2,048	128	66 KB	66 KB	N/A
CKKS-12	1	4,096	256	130 KB	131 KB	N/A
CKKS-14	6	16,384	128	3.15 MB	3.15 MB	2.10 MB
CKKS-15	6	32,768	256	6.29 MB	6.29 MB	4.19 MB
Plain	N/A	N/A	N/A	0.33 KB	0.18 KB	0.31 KB

Configuration parameters

» CKKS configuration parameters and their overheads

Name	Level	Poly. modulus degree	Security level	E[Order size]	E[Remote challenge size]	E[Local challenge size]
CKKS-11	1	2,048	128	66 KB	66 KB	N/A
CKKS-12	1	4,096	256	130 KB	131 KB	N/A
CKKS-14	6	16,384	128	3.15 MB	3.15 MB	2.10 MB
CKKS-15	6	32,768	256	6.29 MB	6.29 MB	4.19 MB
Plain	N/A	N/A	N/A	0.33 KB	0.18 KB	0.31 KB

Configuration parameters

» CKKS configuration parameters and their overheads

Name	Level	Poly. modulus degree	Security level	E[Order size]	E[Remote challenge size]	E[Local challenge size]
CKKS-11	1	2,048	128	66 KB	66 KB	N/A
CKKS-12	1	4,096	256	130 KB	131 KB	N/A
CKKS-14	6	16,384	128	3.15 MB	3.15 MB	2.10 MB
CKKS-15	6	32,768	256	6.29 MB	6.29 MB	4.19 MB
Plain	N/A	N/A	N/A	0.33 KB	0.18 KB	0.31 KB

Configuration parameters

» CKKS configuration parameters and their overheads

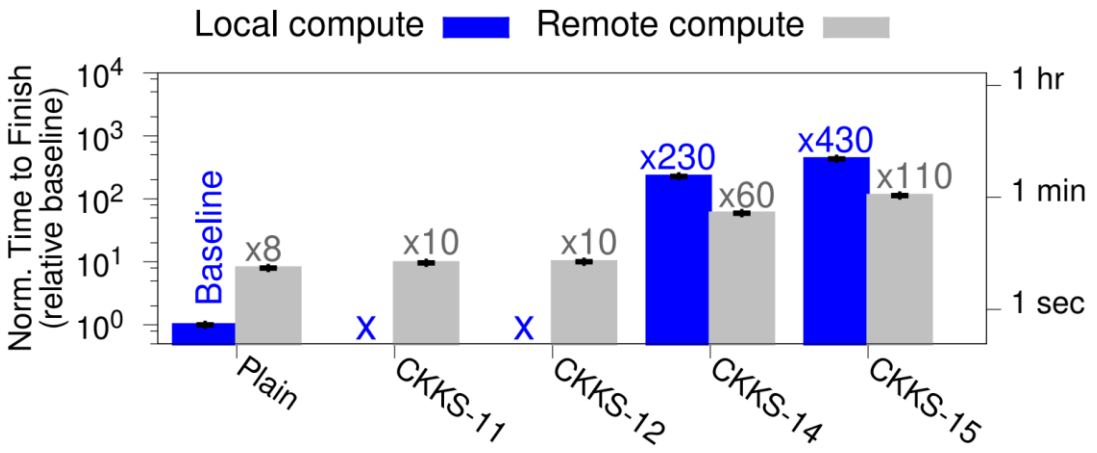
Name	Level	Poly. modulus degree	Security level	E[Order size]	E[Remote challenge size]	E[Local challenge size]
CKKS-11	1	2,048	128	66 KB	66 KB	N/A
CKKS-12	1	4,096	256	130 KB	131 KB	N/A
CKKS-14	6	16,384	128	3.15 MB	3.15 MB	2.10 MB
CKKS-15	6	32,768	256	6.29 MB	6.29 MB	4.19 MB
Plain	N/A	N/A	N/A	0.33 KB	0.18 KB	0.31 KB

Performance metrics

- Time-to-Finish (TTF)
  - Total runtime for trading session
- Time-to-Match (TTM)
  - Time spent on matching encrypted orders
- Time-to-Insert (TTI)
  - Time spent on inserting encrypted order into order book
- Time-to-Solve-Challenges (TTSC)
  - Time spent on evaluator solving challenges

Evaluation

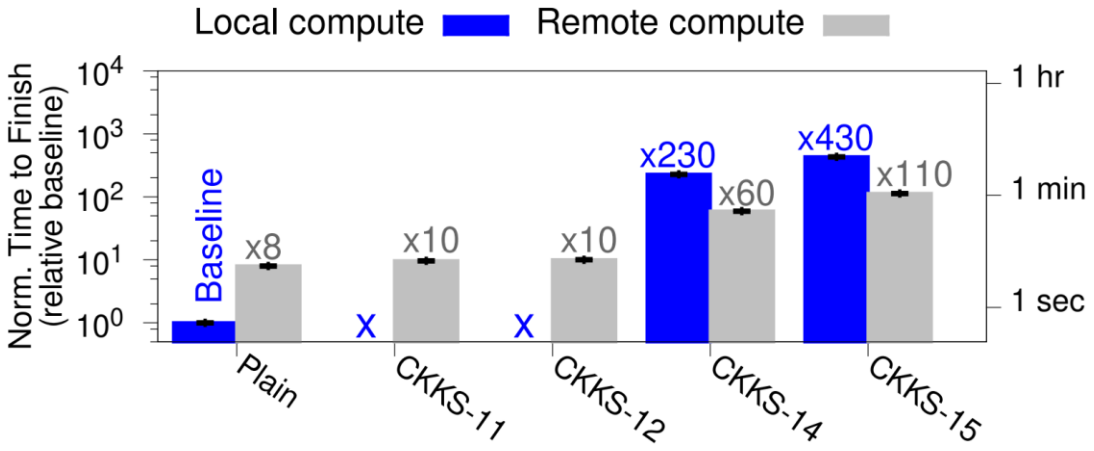
» Increase in time to finish (TTF) relative just doing the non-encrypted (i.e., plain) comparisons locally.

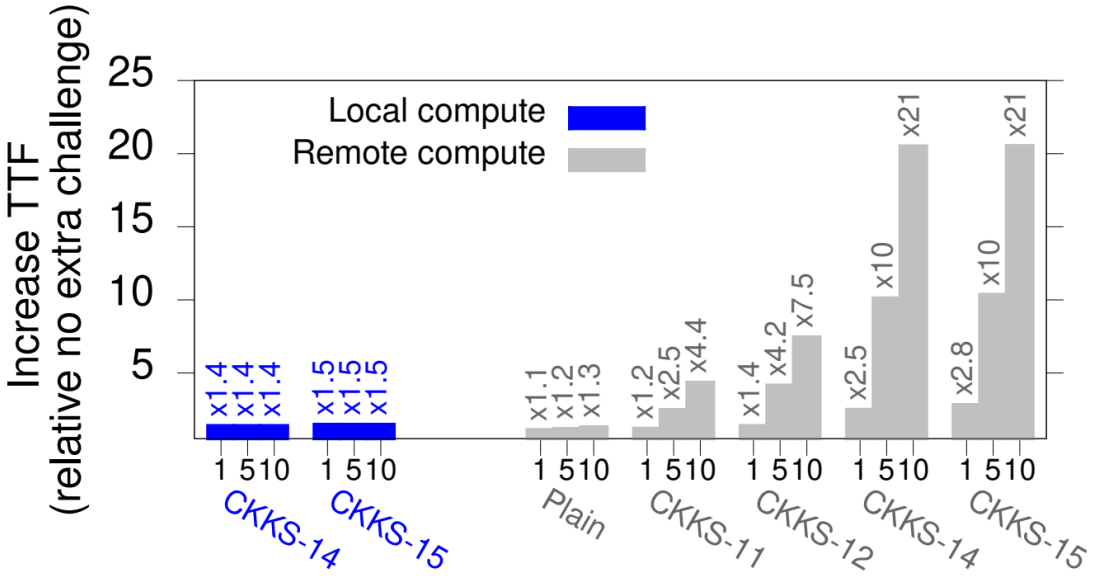


Evaluation

- Increase in time to finish (TTF) relative just doing the non-encrypted (i.e., plain) comparisons locally.

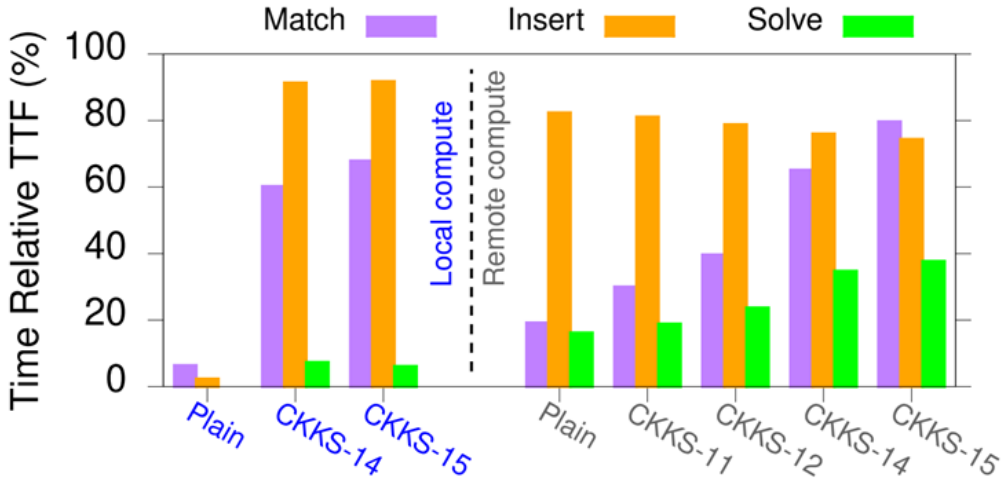
- Increase in time to finish (TTF) when adding N additional challenges to every challenge.



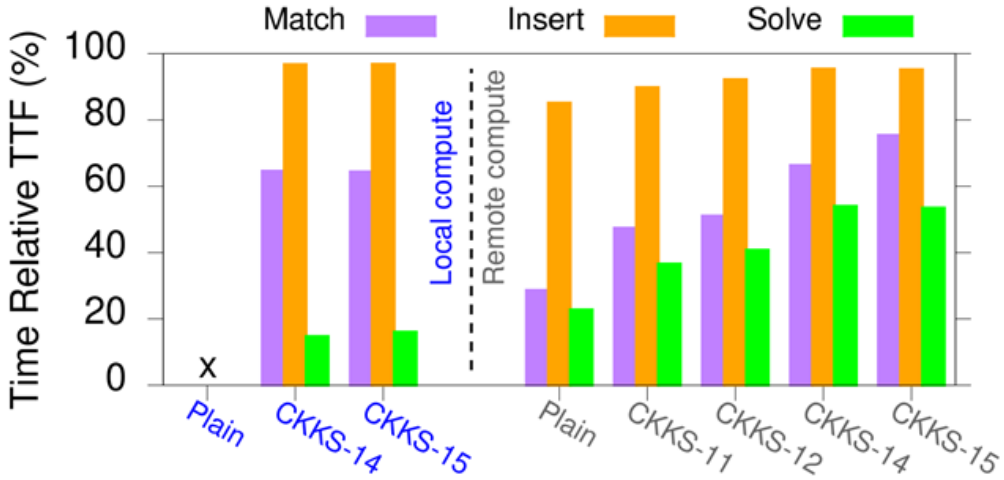


Bottlenecks

» Relative time consumed on different tasks (executed in parallel) relative to the overall time to finish (TTF).



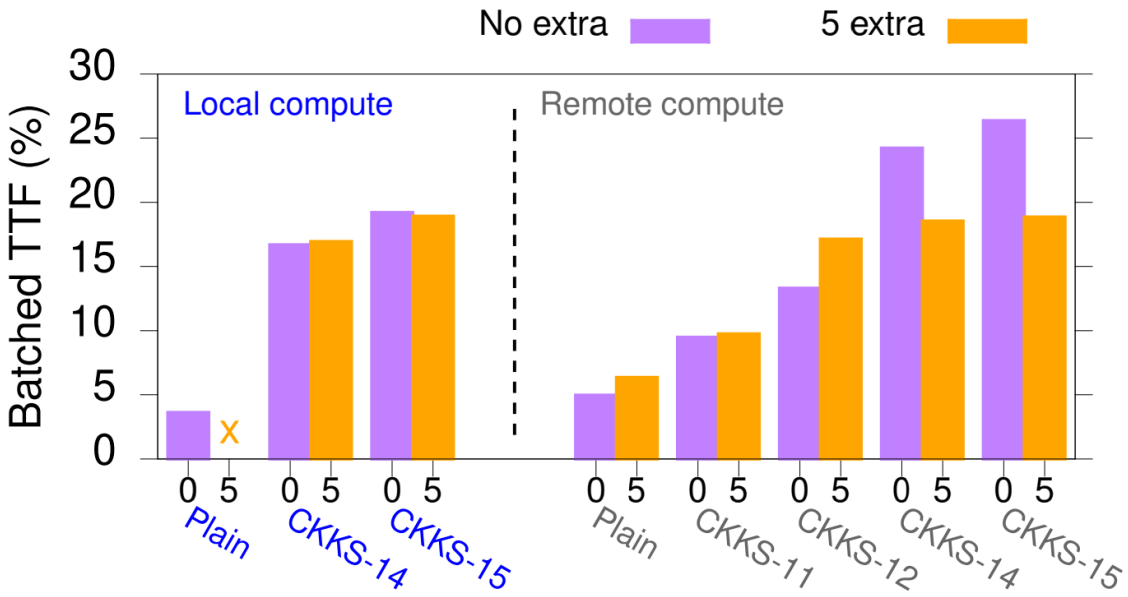
No extra challenges



Five extra challenges per challenge

Batched-based workload

» Relative time to finish (TTF) for batched workload use case compared to the default use case.



Precision and Accuracy

- Operations must be performed with sufficient precision and accuracy

- Average deviation from expected value per configuration and decimal precision

Dec.	Plain	CKKS-11	CKKS-12	CKKS-14	CKKS-15
≤ 8	0	0	0	0	0
9	0	10^{-7}	10^{-5}	10^{-7}	0
10	0	$1.08 \cdot 10^{-6}$	$2.11 \cdot 10^{-8}$	$1.14 \cdot 10^{-8}$	0
11	0	$4.81 \cdot 10^{-8}$	$3.14 \cdot 10^{-8}$	$1.11 \cdot 10^{-8}$	0
12	0	$1.59 \cdot 10^{-6}$	$3.12 \cdot 10^{-8}$	$2.19 \cdot 10^{-9}$	0
13	0	$1.61 \cdot 10^{-8}$	$2.30 \cdot 10^{-8}$	$1.52 \cdot 10^{-9}$	0
14	10^{-11}	$1.11 \cdot 10^{-8}$	$2.83 \cdot 10^{-8}$	$4.44 \cdot 10^{-9}$	10^{-11}
15	10^{-11}	$1.46 \cdot 10^{-8}$	$1.97 \cdot 10^{-8}$	$6.51 \cdot 10^{-9}$	10^{-11}

Precision and Accuracy

- Operations must be performed with sufficient precision and accuracy

- Average deviation from expected value per configuration and decimal precision

Dec.	Plain	CKKS-11	CKKS-12	CKKS-14	CKKS-15
≤ 8	0	0	0	0	0
9	0	10^{-7}	10^{-5}	10^{-7}	0
10	0	$1.08 \cdot 10^{-6}$	$2.11 \cdot 10^{-8}$	$1.14 \cdot 10^{-8}$	0
11	0	$4.81 \cdot 10^{-8}$	$3.14 \cdot 10^{-8}$	$1.11 \cdot 10^{-8}$	0
12	0	$1.59 \cdot 10^{-6}$	$3.12 \cdot 10^{-8}$	$2.19 \cdot 10^{-9}$	0
13	0	$1.61 \cdot 10^{-8}$	$2.30 \cdot 10^{-8}$	$1.52 \cdot 10^{-9}$	0
14	10^{-11}	$1.11 \cdot 10^{-8}$	$2.83 \cdot 10^{-8}$	$4.44 \cdot 10^{-9}$	10^{-11}
15	10^{-11}	$1.46 \cdot 10^{-8}$	$1.97 \cdot 10^{-8}$	$6.51 \cdot 10^{-9}$	10^{-11}

Precision and Accuracy

- Operations must be performed with sufficient precision and accuracy

- Average deviation from expected value per configuration and decimal precision

Dec.	Plain	CKKS-11	CKKS-12	CKKS-14	CKKS-15
≤ 8	0	0	0	0	0
9	0	10^{-7}	10^{-5}	10^{-7}	0
10	0	$1.08 \cdot 10^{-6}$	$2.11 \cdot 10^{-8}$	$1.14 \cdot 10^{-8}$	0
11	0	$4.81 \cdot 10^{-8}$	$3.14 \cdot 10^{-8}$	$1.11 \cdot 10^{-8}$	0
12	0	$1.59 \cdot 10^{-6}$	$3.12 \cdot 10^{-8}$	$2.19 \cdot 10^{-9}$	0
13	0	$1.61 \cdot 10^{-8}$	$2.30 \cdot 10^{-8}$	$1.52 \cdot 10^{-9}$	0
14	10^{-11}	$1.11 \cdot 10^{-8}$	$2.83 \cdot 10^{-8}$	$4.44 \cdot 10^{-9}$	10^{-11}
15	10^{-11}	$1.46 \cdot 10^{-8}$	$1.97 \cdot 10^{-8}$	$6.51 \cdot 10^{-9}$	10^{-11}

Precision and Accuracy

- Operations must be performed with sufficient precision and accuracy

- Average deviation from expected value per configuration and decimal precision

Dec.	Plain	CKKS-11	CKKS-12	CKKS-14	CKKS-15
≤ 8	0	0	0	0	0
9	0	10^{-7}	10^{-5}	10^{-7}	0
10	0	$1.08 \cdot 10^{-6}$	$2.11 \cdot 10^{-8}$	$1.14 \cdot 10^{-8}$	0
11	0	$4.81 \cdot 10^{-8}$	$3.14 \cdot 10^{-8}$	$1.11 \cdot 10^{-8}$	0
12	0	$1.59 \cdot 10^{-6}$	$3.12 \cdot 10^{-8}$	$2.19 \cdot 10^{-9}$	0
13	0	$1.61 \cdot 10^{-8}$	$2.30 \cdot 10^{-8}$	$1.52 \cdot 10^{-9}$	0
14	10^{-11}	$1.11 \cdot 10^{-8}$	$2.83 \cdot 10^{-8}$	$4.44 \cdot 10^{-9}$	10^{-11}
15	10^{-11}	$1.46 \cdot 10^{-8}$	$1.97 \cdot 10^{-8}$	$6.51 \cdot 10^{-9}$	10^{-11}

Conclusions

- We present PET-Exchange, a privacy-preserving trading framework using homomorphic encryption for trading securities, partially matching limit orders between multiple buyers and sellers
- Using various conditions and configurations, we provide insights into the most attractive tradeoffs applicable to a wide range of exchanges and use cases
- We provide insights into current performance bottlenecks and validate that we can achieve high accuracy with many decimals of precision

PET-Exchange: A Privacy Enhanced Trading Exchange using Homomorphic Encryption

David Hasselquist
Jacob Wahlman
Niklas Carlsson

Paper is online!

David Hasselquist (david.hasselquist@liu.se)

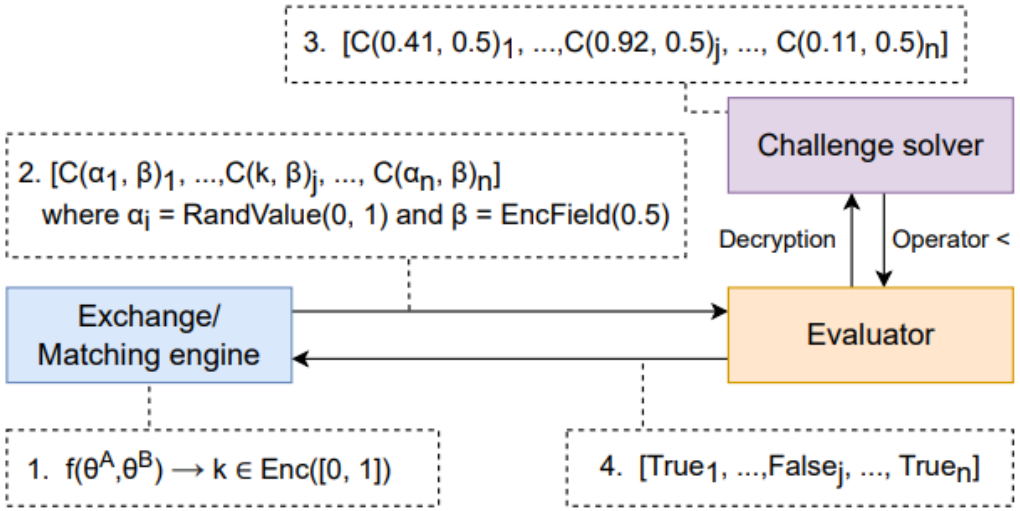
LINKÖPING UNIVERSITY

WASP WALLENBERG AI, AUTONOMOUS SYSTEMS AND SOFTWARE PROGRAM

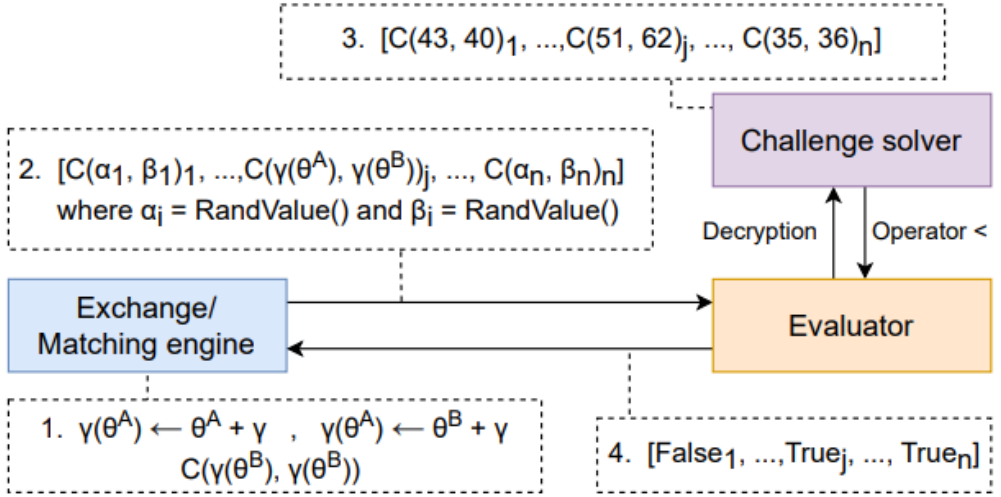
SECTRA

Extra slides

Local vs. remote comparison method



Local comparison



Remote comparison