TACEO

Scaling Private Iris Code Uniqueness Checks to Millions of Users

Remco Bloemen, Daniel Kales, Philipp Sippl, **Roman Walch**

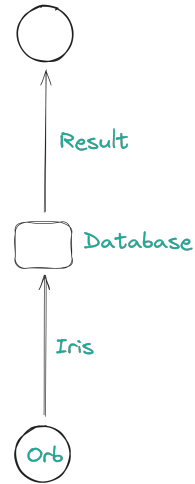
June 5th, 2024

Real World MPC Use Case

- Partnered with Worldcoin for large MPC use case
- World ID:
  - Unique ID for humans, no duplication, no AI
  - Enforced by comparing iris to database
  - Privacy problems!

$\Rightarrow$ Distribute database using MPC

- Previous state-of-the-art: Janus [ELS+24]
  - MPC throughput: 2k iris codes per minute
  - Solution using TEEs: 160k per second
- Worldcoin database: ≈ 6 million and growing fast

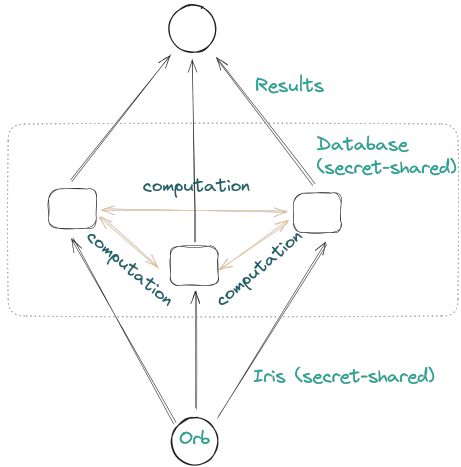


The (Simplified) Protocol

- Comparison of two iris codes:
  - Calculate hamming distance

$$\texttt{hd} = \texttt{PopCount}(\vec{c}_1 \oplus \vec{c}_2)$$

  - Compare to a threshold $\texttt{hd} < t$
- Problems: Mixed operations and large sizes
  - Hamming-distance: XOR and Sum
  - Comparison and aggregation (Boolean)
  - 12800 bits per iris code
  - 6 million entries in database



Better Hamming Distance

TACEO

- Rewrite hamming distance to dot product:

$$\mathtt{hd}(\vec{a}, \vec{b}) = \sum_i a_i + \sum_i b_i - 2 \cdot \langle \vec{a}, \vec{b} \rangle$$

- In honest majority protocols:
  - Communication independent to iris code size

  $\Rightarrow$ Huge decrease of communication

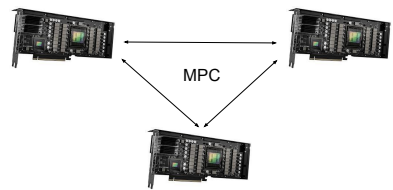
- 3-party protocol:
  - Shamir sharing for dot-product
  - Replicated sharing for threshold comparison and result aggregation

GPU Implementation

- Dot-product well suited for GPU's
- Nvidia NCCL:
  - GPUs directly communicate over network
  - No GPU $\Leftrightarrow$ CPU data transfer

$\Rightarrow$ Execute whole protocol on multiple GPUs

- Result on 3 AWS P5 instances (8x H100 GPUs, 3.2 Tbps) $$$
  - Throughput: 2.48 billion iris code comparisons per second



Conclusion

- Learnings:
  - Consider GPUs for massively improved throughput
  - Clever protocol optimizations + fast hardware:

  $\Rightarrow$ MPC can be fast enough for real world use cases with millions of users
- Project status:
  - Predecessor (only shared dot-product) deployed
  - Prototype of full version done

  $\Rightarrow$ Deployed in the next months
- More details with more optimizations:
  - `https://ia.cr/2024/705`

Bibliography I

[ELS+24] Kasra Edalatnejad, Wouter Lueks, Justinas Sukaitis, Vincent Graf Narbel, Massimo Marelli, and Carmela Troncoso. ''Janus: Safe Biometric Deduplication for Humanitarian Aid Distribution''. In: SP. IEEE, 2024, pp. 115–115.