Carnegie Mellon University

Bryan Parno, Professor
Kavčić-Moura Professor of
Electrical & Computer Engineering
and Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
(412) 268-2033
parno@cmu.edu

April 8, 2025

Dear colleagues,

I am writing to enthusiastically nominate *Piano: Extremely Simple, Single-Server PIR with Sublinear Server Computation* by Mingxun Zhou, Andrew Park, Elaine Shi, and Wenting Zheng and published at the 2024 IEEE Symposium on Security & Privacy for the NSA Best Scientific Cyber-Security Paper Award.

Background and Importance of the Problem

Private Information Retrieval (PIR) allows users to retrieve records from a database without disclosing the locations visited. PIR underpins numerous applications; e.g., it can hide a user's intentions when they perform web searches, DNS lookups, or LLM queries. Since its proposal by Chor et al. in 1995, our community has dreamed of making PIR truly practical.

Unfortunately, all classical PIR schemes (without preprocessing) suffer from linear (in the database size) cost per query! This linear-cost barrier is provably inherent. Notably, Signal explored using a state-of-the-art classical PIR for private contact discovery. However, based on their talk in the 2023 Confidential Computing Summit, doing so would cost them >$300M per year! To avoid such prohibitive costs, they opted for the second-best choice of using trusted hardware and Oblivious RAM (ORAM).

Therefore, an important question is whether we can achieve practical access pattern privacy without trusted hardware --- this is desired not just by Signal, but also by many blockchain and cloud applications.

Piano's Contributions

To make PIR practical, our best hope is to rely on preprocessing to overcome the linear cost barrier. Piano is the first practical instantiation of this idea; it is a conceptually simple scheme with ~sqrt(N) cost per query, where N is the database size. The construction's extreme simplicity was quite surprising. Moreover, the scheme relies only on PRFs and uses no public-key cryptography, making it possible to employ the AES-NI instructions on modern processors to achieve low latency and high throughput. On a 100GB-scale

database, each query takes only ~73ms on a coast-to-coast link, and of this cost, ~60ms is the ping latency. When compared to state-of-the-art classical PIR schemes like SimplePIR, Piano achieves at least ***three orders of magnitude*** improvement in computational cost.

Piano also makes a significant theoretical contribution. In the single-server setting, classical PIR (without preprocessing) is impossible without public-key cryptography. The fact that Piano can be based on symmetric-key primitives was a surprising theoretical revelation.

Impact and Summary

Piano is a ***landmark result*** that signals a paradigm shift in PIR. Despite being published only in 2024, it has already spurred a flurry of subsequent results that further explore the same algorithmic paradigm. Notably, the subsequent work of Ishai et al. (CRYPTO'24) proved that Piano's client space and bandwidth tradeoff is optimal up to logarithmic factors.

The significance of Piano can be compared with that of Path ORAM in the ORAM literature. Just like Path ORAM has allowed ORAM to evolve from theory to large-scale practical adoption, I believe that Piano is a similar game changer for PIR. Specifically, PIR can provide an alternative solution to the applications that use ORAM today, while removing ORAM's reliance on trusted hardware.

Sincerely,

Bryan Parno
Kavčić-Moura Professor of
Electrical & Computer Engineering
and Computer Science