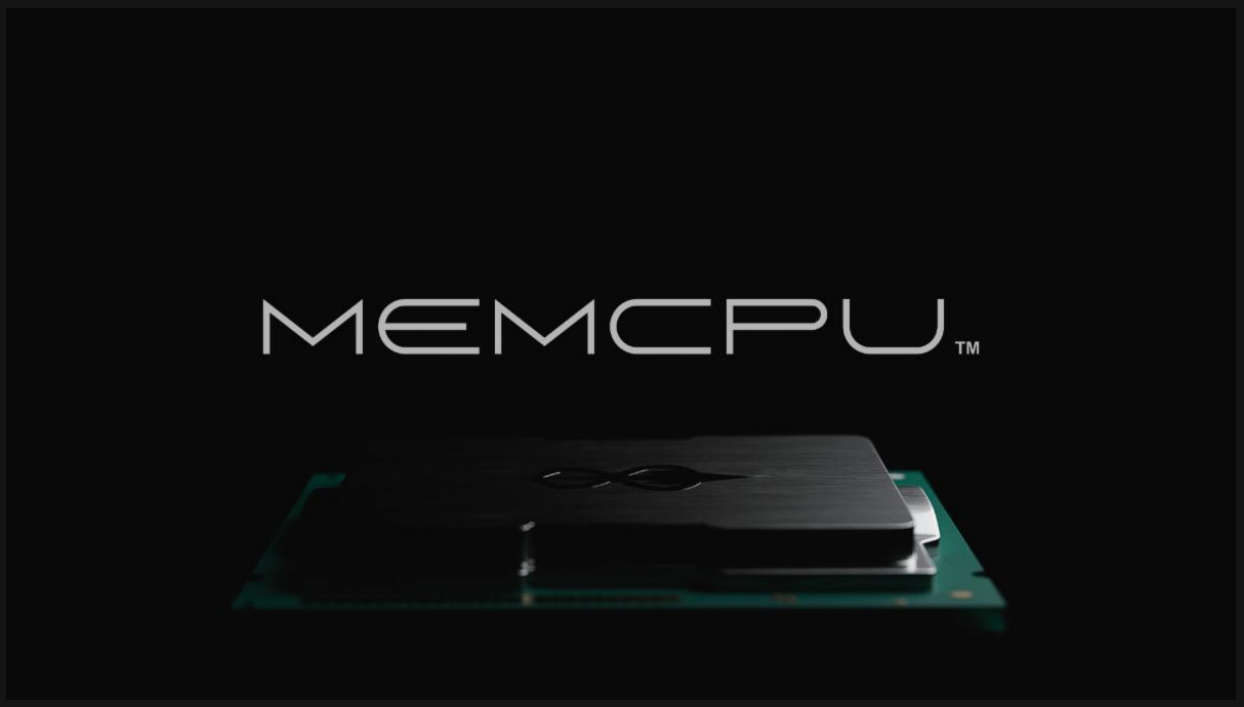
MemComputing

September 2023



Prime Factorization

The MEMCPU Platform™ has been meticulously programmed to derive congruences among integers, paving the way for efficient biprime factorization using standard sieving methods. A comprehensive set of RSA-like biprimes served as the benchmark for an in-depth performance analysis. As anticipated, existing methodologies like the General Number Field Sieve (GNFS) and commercial Integer Linear Programming (ILP) solvers exhibited super-polynomial scaling on this benchmark. Remarkably, MemComputing was put to the test up to 300 bits, displaying scaling that adheres to a 2nd-degree polynomial fit. This achievement signifies a leap towards addressing complex computational problems with enhanced efficiency and scalability, potentially unlocking new possibilities in cryptography and beyond.

Press Release

Prime Factorization Capability

See MemComputing's press release on our capability to address Prime Factorization at scale.

Read More

“With this latest achievement, MemComputing reaffirms its unwavering commitment to spearheading innovation in the computational domain,” said John Beane, CEO of MemComputing, Inc. “This latest development not only showcases the raw power and versatility of our technology but also paves the way for significant advancements in fields that rely heavily

on prime factorization, such as computer science and cryptography."

New Paper

Implementation of Digital MemComputing...

Dr. Max Di Ventra, co-founder of MemComputing, has unveiled a paper shedding light on a novel DMM hardware design, leveraging conventional electronic components for marked improvements in speed & stability, addressing more complex problems!

Paper

Implementation of digital MemComputing using standard electronic components

Yuan-Hang Zhang and Massimiliano Di Ventra, *Fellow, IEEE*

***Abstract*—Digital MemComputing machines (DMMs), which employ nonlinear dynamical systems with memory (time non-locality), have proven to be a robust and scalable unconventional computing approach for solving a wide variety of combinatorial optimization problems. However, most of the research so far has focused on the numerical simulations of the equations of motion of DMMs. This inevitably subjects time to discretization, which brings its own (numerical) issues that would be absent in actual physical systems operating in continuous time. Although hardware realizations of DMMs have been previously suggested, their implementation would require materials and devices that are not so easy to integrate with traditional electronics. In this study, we propose a novel hardware design for DMMs that leverages only conventional electronic components. Our findings suggest that this design offers a marked improvement in speed compared to existing realizations of these machines, without requiring special materials or novel device concepts. Moreover, the absence of numerical noise promises enhanced stability over extended periods of the machines' operation, paving the way for addressing even more complex problems.**

***Index Terms*—MemComputing, nonlinear dynamical systems, combinatorial optimization, hardware acceleration, circuit simulations, self-organization**

I. Introduction

Over the past half century, the rapid development of computers has mirrored the prediction of Moore's law, with the number of transistors doubling approximately every two years [1]. As we near the physical limits of this growth, formidable challenges such as quantum tunneling, heat dissipation, and escalating production costs [2] necessitate a pivot towards novel computational paradigms. Unconventional computing, encompassing areas like quantum [3], neuromorphic [4], optical [5], and molecular computing [6], promises to not only sustain computational growth but also foster more energy-efficient and adaptable systems, capable of tackling problems currently beyond the reach of classical computers.

One key idea in unconventional computing is to harness physical principles to greatly accelerate the solution of certain problems. For instance, an ideal (decoherence-free) quantum computer could in principle solve integer factorization in polynomial time utilizing quantum entanglement and interference [7]. A new class of machines, dubbed "MemComputing" [8], leverages time non-locality (memory) to solve a wide variety of computational problems efficiently [9], [10]. In particular, their digital version (digital MemComputing machines or DMMs) have been designed to solve combinatorial optimization problems [11].

We stress here that the prefix "Mem" stands for "memory", which is generally intended as "time non-locality", not necessarily storage [12]. Time non-locality is the *non-equilibrium* property of a physical system that when perturbed, the perturbation affects the system's state at a later time [10]. Under appropriate conditions, it induces spatial non-locality [12]. This, in turn, initiates dynamical long-range order in the system [13], [14], which is exploited by DMMs to scrutinize the structure of the target problem, thereby solving it efficiently.

In the present paper we focus on DMMs [11], which have a finite set of input and output states that can be written/read with finite precision, hence are scalable to large problem sizes. The dynamics of a DMM are governed by a set of ordinary differential equations (ODEs) [11], [15], whose equilibria correspond to the solutions (if they exist) of the target problem. In continuous (physical) time, it has been proved that if such systems have equilibria (solutions) periodic orbits and chaos can be avoided [16], [17], and the convergence to the equilibrium point(s) can be reached with a number of instantonic jumps (namely trajectories connecting critical points of the dynamics of different stability) that scales polynomially with problem size [13], [14].

Studies have illustrated that numerical simulations of DMM's equations can effectively solve a plethora of complex combinatorial optimization problems [11], [15], [18]–[20], significantly surpassing traditional algorithms in performance (see also industrial case studies performed at MemComputing, Inc. [21]). Recently, it was numerically shown that MemComputing can solve the hardest integer factorization problems with quadratic complexity up to 300 bits [22], with projections to factor 2048-bit RSA keys [23] within weeks in software.

However, the numerical simulation of ODEs inevitably necessitates time discretization, leading to the accumulation and possible amplification of numerical errors over time [24]. Given that DMMs typically require extended simulation times to reach the solution of very large problems (in the hundreds of thousand or millions of variables), the numerical errors may ultimately cause the simulations of DMMs to fail [25]. Although better numerical methods and careful control of such simulations can tame this issue, it comes with additional numerical overhead.

Therefore, it would be advantageous to construct a *physical* DMM that operates in continuous time. Naturally, physical noise will persist under such circumstances, but unlike numerical noise, physical noise is typically localized in space and

This work was supported by the NSF grant No. ECCS-2220860.

Yuan-Hang Zhang and Massimiliano Di Ventra are with the Department of Physics, University of California, San Diego, La Jolla, CA 92093, USA (emails: yuz002@ucsd.edu, diventra@physics.ucsd.edu)

Latest Presentation

Prime Factorization Presentation

In case you missed it, here is our presentation to the Defense Information Systems Agency (DISA) demonstrating our approach to Prime Factorization.

Presentation

See who's talking about our achievement

Quantum Zeitgeist Articles:

- MemComputing claims Breakthrough in Large-Scale Prime Factorization, Potentially Revolutionising Cryptography.
- Quantum Inspired MemComputing says RSA 2048 can be broken in real-time.

Yahoo FInance:

- MemComputing Releases Manuscript Addressing Prime Factorization Capability

Times of San Diego:

- Startup Achieves Quantum-Speed Math Processing

Latest Award

Will Reed Top 100

Out of 2,500+ Seed & Series A companies, Will Reed just named MemComputing a top early-stage company shaping the future of workplace culture. Congrats team!

Top 100

EVENTS

2023

EDGE 2023 Supply Chain Exchange Exhibition

October 1-4

MemComputing is exhibiting at the EDGE 2023 Supply Chain Exchange Exhibition where we will be showcasing our technology to industry leaders and clients.

MEMCPU
PLATFORM

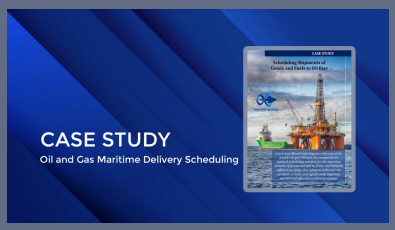
The cloud-based MEMCPU™ Platform is a novel computing paradigm designed to solve complex optimization problems at unprecedented speed and scale. Whereas classical optimization algorithms iteratively search for solutions, the MEMCPU Platform naturally converges to the solution in one massively parallel transaction, enabling our clients to achieve truly optimal solutions in near real time.

Get Started

-In Case You Missed It-

Phase I USAF SBIR
Read More

Latest Explainer Video
Watch Now



O&G Case Study
Read More

Was this newsletter forwarded to you?

Subscribe

MemComputing