MemComputing and implications for security

Massimiliano Di Ventra

University of California, San Diego, La Jolla, CA 92093-0319 USA

MemComputing is a new physics-based approach to computation that employs time non-locality (memory) to both process and store information on the same physical location [1]. Time non-locality is a remarkable feature since it can generate dynamical long-range order in the system even if its individual units are interacting locally. Long-range order means that the correlations between the machine units do not decay exponentially, rather algebraically, both temporally and spatially. A memcomputing machine then navigates its phase space by following specific trajectories (instantons) which showcase this long-range order, namely during dynamics the machine can change the values of just a few or as many variables in the problem specification as needed to reach the solution efficiently. I will discuss the physics behind MemComputing, and its application to a variety of combinatorial optimization problems, including prime factorization of RSA numbers. These results demonstrate both the advantages of this computing paradigm over traditional approaches and quantum computing, as well as its threat to modern encryption protocols. Work supported by DARPA, DOE, NSF, CMRR, and MemComputing, Inc. (http://memcpu.com/).

[1] M. Di Ventra, *MemComputing: Fundamentals and Applications* (Oxford University Press, 2022).

Biographical Sketch

Massimiliano Di Ventra obtained his undergraduate degree in Physics *summa cum laude* from the University of Trieste (Italy) in 1991 and did his PhD studies at the Swiss Federal Institute of Technology in Lausanne in 1993-1997. He is now professor of Physics at the University of California, San Diego since 2004. Di Ventra's research interests are in condensed-matter theory and unconventional computing. He has been invited to deliver more than 350 talks worldwide on these topics including 16 plenary/keynote presentations. He has published more than 300 papers in refereed journals, 5 textbooks, and has 11 granted patents (7 foreign). He is a fellow of the American Association for the Advancement of Science, the American Physical Society, the Institute of Physics, the IEEE and a foreign member of Academia Europaea. In 2018 he was named Highly Cited Researcher by Clarivate Analytics, he is the recipient of the 2020 Feynman Prize for theory in Nanotechnology, and is a 2022 IEEE Nanotechnology Council Distinguished Lecturer. He is the co-founder of MemComputing, Inc. (http://memcpu.com/).