Advances in processor architectures for accelerating cryptographic algorithms, and their potential influence on servers' efficiency

Shay Gueron

Abstract: In the talk, we will explore a few processor architectures features that have been recently introduced, for accelerating cryptographic algorithms. We will demonstrate some performance trends and how they improve the efficiency of high-end communication (SSL/TLS) servers. We will show how these improvements make some modern cryptographic suite advantageous from the performance viewpoint, and can therefore lead to ecosystem changes.

Biography: Prof. Shay Gueron is a faculty member at the Department of Mathematics of the University of Haifa, Israel.
He is also an Intel Principal Engineer, working at the Intel Architecture Group at the Intel Development Center, Haifa, Israel.
His interests include applied security, cryptography, and algorithms.
He holds a Ph.D. degree in applied mathematics from the Technion—Israel Institute of Technology.