May the Fourth Be With You: A Microarchitectural Side Channel Attack on Several Real-World Applications of Curve25519

Daniel Genkin[1,2] Luke Valenta[1] Yuval Yarom[3,4]

[1] University of Pennsylvania
{danielg3,lukev}@cis.upenn.edu
[2] University of Maryland
[3] University of Adelaide
yval@cs.adelaide.edu.au
[4] Data 61, CSIRO

In recent years, applications increasingly adopt security primitives designed with better countermeasures against side channel attacks. A concrete example is Libgcrypt's implementation of ECDH encryption with Curve25519. The implementation employs the Montgomery ladder scalar-by-point multiplication, uses the unified, branchless Montgomery double-and-add formula and implements a constant-time argument swap within the ladder. However, Libgcrypt's field arithmetic operations are not implemented in a constant-time side-channel-resistant fashion.

Based on the secure design of Curve25519, users of the curve are advised that there is no need to perform validation of input points. In this work we demonstrate that when this recommendation is followed, the mathematical structure of Curve25519 facilitates the exploitation of side-channel weaknesses.

We demonstrate the effect of this vulnerability on three software applications—encrypted git, email and messaging—that use Libgcrypt. In each case, we show how to craft malicious OpenPGP files that use the Curve25519 point of order 4 as a chosen ciphertext to the ECDH encryption scheme. We find that the resulting interactions of the point at infinity, order-2, and order-4 elements in the Montgomery ladder scalar-by-point multiplication routine create side channel leakage that allows us to recover the private key in as few as 11 attempts to access such malicious files.