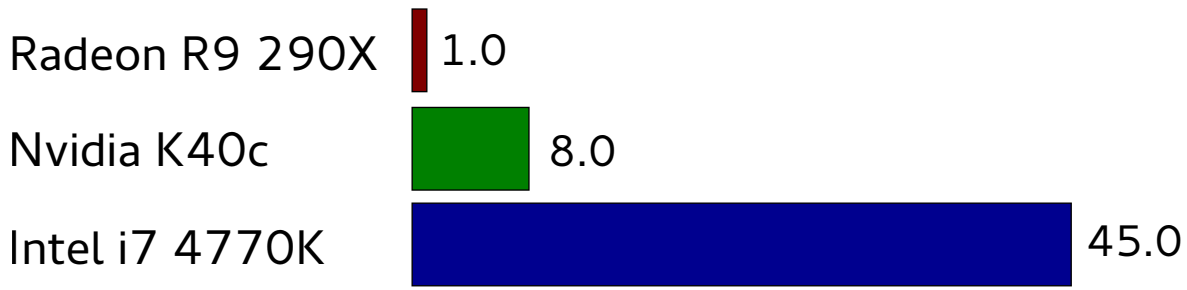
HPC & SIDE-CHANNEL CRYPTANALYSIS

Our framework:

- Extensible HPC & GPU code accelerating attacks/testing;
- Mix of C++ / OpenCL

E.g. CPA attacking 32-bits of key:



- $2^{53.4}$ (23.3 quadrillion) calls to a KDE kernel function
- $2^{46.4}$ (91 trillion) 32-bit (sub)keys searched using HW-CPA

HPC & SIDE-CHANNEL CRYPTANALYSIS

Papers using the framework:

- ePrint 2014/365, Asiacrypt 2014 (to appear)
- ePrint 2013/298, Asiacrypt 2013

Interested or have a problem for which this might be the solution: **please** get in touch!

luke.mather@bristol.ac.uk (University of Bristol)

Also: PhD studentship available in this area (UK only)