The 157th Short Vacuous Presentation

A decade of Darmstadt lattice challenges.[1]

Leo Ducas, Marc Stevens and **Wessel van Woerden**

CWI, Amsterdam

May 21, 2019

1. ± 1 year (`https://www.latticechallenge.org/svp-challenge/index.php`).

Pumping up the power

1 cpu core (40 Gflops)

Pumping up the power

1 cpu core (40 Gflops)

multiple cpu cores (800 Gflops)

Pumping up the power

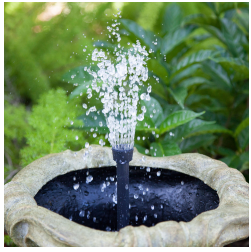
1 cpu core (40 Gflops)

multiple cpu cores (800 Gflops)

GPU cuda cores (16.000 Gflops)

Pumping up the power

1 cpu core (40 Gflops)



multiple cpu cores (800 Gflops)

GPU cuda cores (16.000 Gflops)

GPU tensor cores (130.000 Gflops)

Our preliminary G6K-adaptation: using GPU (cuda cores)

SVP challenge solution dimension 157!

- Challenge seed $= 0$.
- The short vector:

$$
\begin{aligned}
&(202, 557, -33, -282, 144, 17, 38, 263, 89, -72, -57, 323,\\
&-545, -282, -238, 254, 328, 301, 353, 425, 75, 33, 452, 11, -134, -434, 29,\\
&-214, 290, -373, -756, 88, 271, -433, 274, -268, -118, 278, -234, 314, -88,\\
&-231, 89, 98, -52, 246, 208, -57, -451, -169, 38, -131, 51, 10, 235, -130, 280,\\
&126, -559, 365, 41, -83, 409, -301, 239, -580, 214, 35, 345, 199, 87, -8, -70,\\
&-53, -143, 244, 241, -42, -209, -43, -418, -543, 221, 484, -65, 36, -189, -82,\\
&167, -36, -175, 393, -436, 180, 304, -175, -34, -54, -150, 210, -403, -196,\\
&-260, 94, -107, 294, 275, -434, -71, 385, -20, 196, 538, -112, -273, 663, -6,\\
&77, 539, 49, -137, -307, -37, 346, -110, 7, -70, 60, 350, -182, -121, 67, 325,\\
&-35, 286, -396, 72, -656, 324, -25, -149, 21, 205, 45, -173, -88, -287, 239,\\
&-95, -61, -500, -66, 29, 272, -125, -67, -199)
\end{aligned}
$$

- Please verify in your head..