A JEALOUS CRYPTANALYST

In search of a short vector

A story by Leo Ducas, Marc Stevens

and Wessel van Woerden

ONCE UPON A TIME…

ONCE UPON A TIME…

A cryptanalyst visited the machine learning group.

ONCE UPON A TIME…

A cryptanalyst visited the machine learning group.

And fell in love ❤

ONCE UPON A TIME…

A cryptanalyst visited the machine learning group.

And fell in love ❤

With…

The spec sheet of their GPUs:

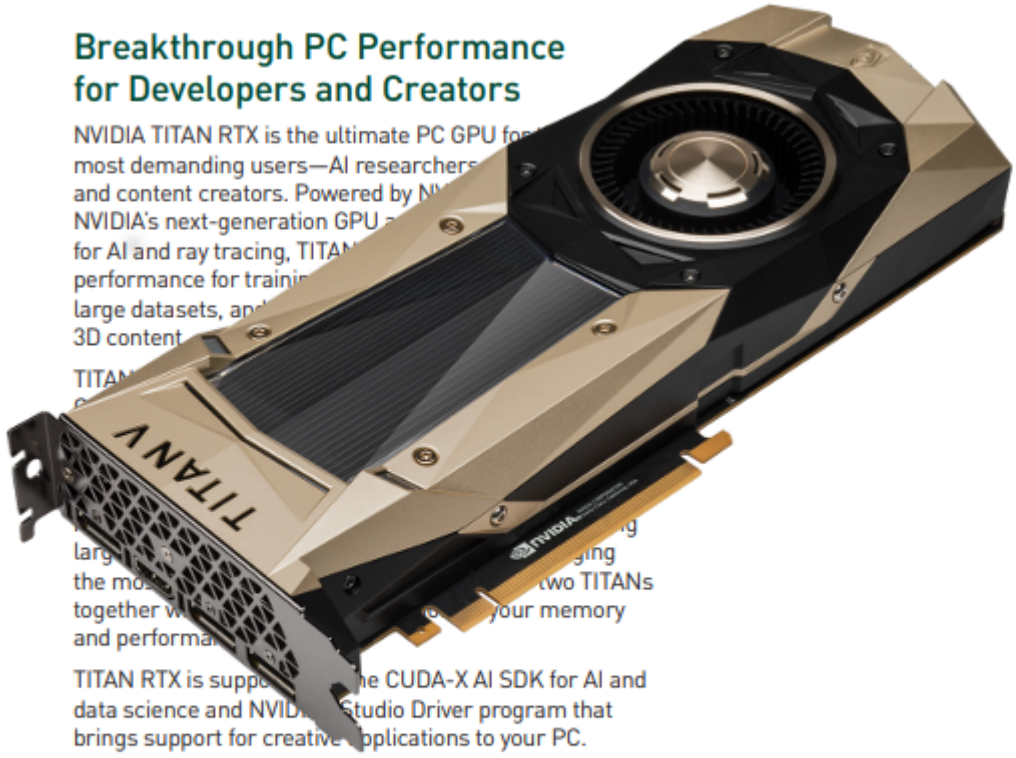
Breakthrough PC Performance for Developers and Creators

NVIDIA TITAN RTX is the ultimate PC GPU fo
most demanding users—AI researchers
and content creators. Powered by N
NVIDIA's next-generation GPU a
for AI and ray tracing, TITA
performance for traini
large datasets, an
3D content

TITA

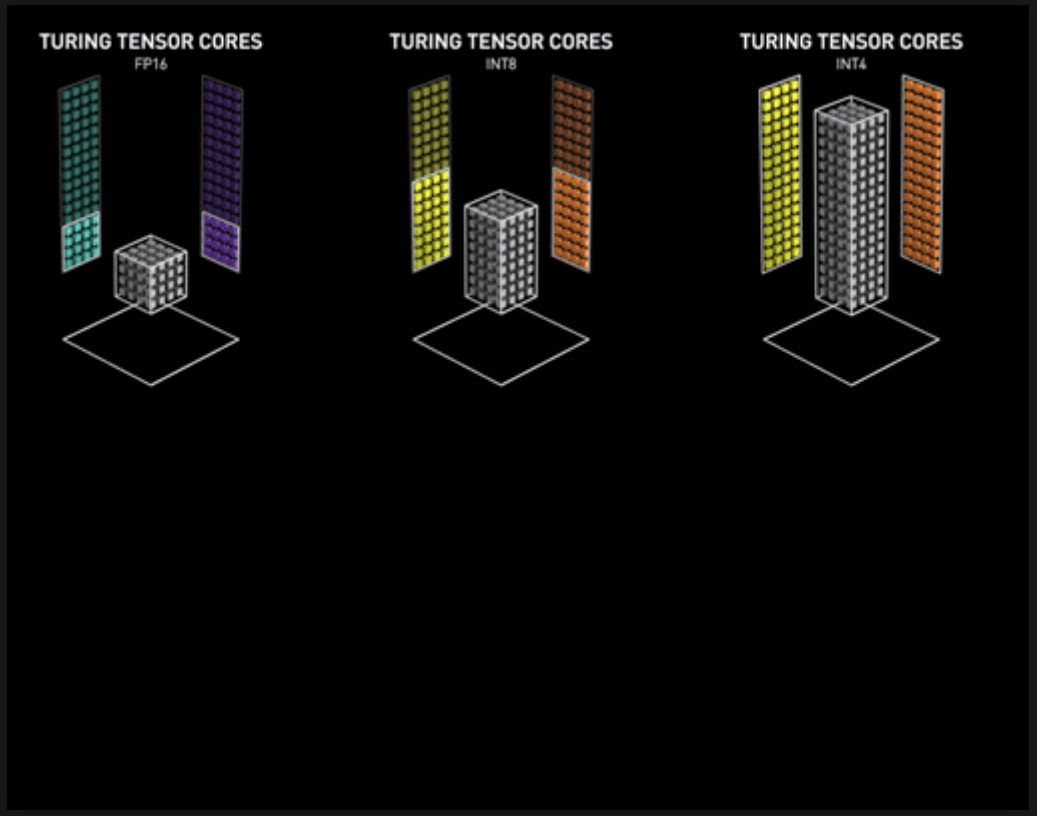
larg ging
the mo two TITANs
together w our memory
and performa

TITAN RTX is suppo he CUDA-X AI SDK for AI and
data science and NVID Studio Driver program that
brings support for creativ pplications to your PC.

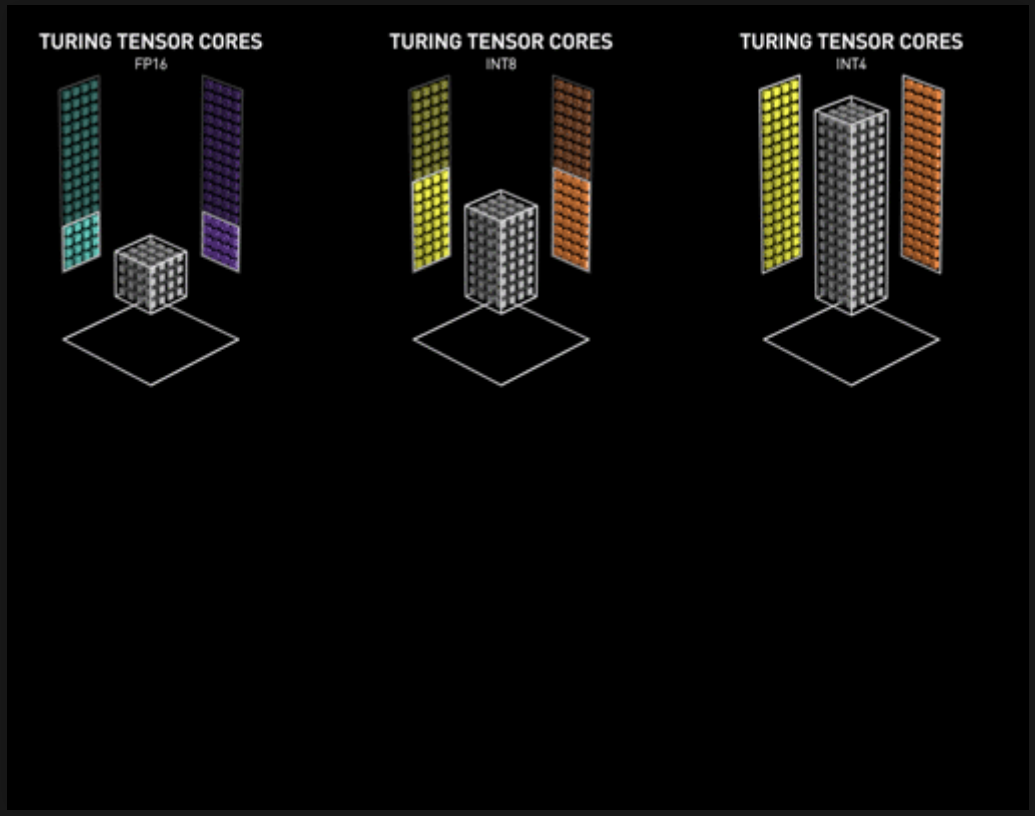


SPECIFICATIONS	
GPU Memory	**24 GB GDDR6**
Memory Interface	**384-bit**
Memory Bandwidth	**Up to 672 GB/s**
NVIDIA CUDA® Cores	**4,608**
NVIDIA Tensor Cores	**576**
NVIDIA RT Cores	**72**
Single-Precision Performance	**16.3 TFLOPS**
Tensor Performance	**130 TFLOPS**
NVIDIA NVLink	**Connects 2 TITAN RTX GPUs**
NVIDIA NVLink Bandwidth	**100 GB/s (bidirectional)**
System Interface	**PCI Express 3.0 x 16**
Power Consumption	**280 W**
Thermal Solution	**Active**
Form Factor	**4.4" H x 10.5" L, Dual slot, full height**
Display Connectors	**3x DisplayPort, 1x HDMI, 1x USB Type-C**
Max Simultaneous Displays	**4x 4096 x 2160 @ 120 Hz, 4x 5120 x 2880 @ 60 Hz, 2x 7680 x 4320 @ 60 Hz**
Encode/Decode Engines	**1x encode, 1x decode**
VR Ready	**Yes**
Graphics APIs	**Microsoft DirectX 12 API[3], Vulkan API[4], OpenGL 4.6[4]**
Compute APIs	**CUDA, DirectCompute, OpenCL™**

Or more specifically, their Tensor cores:



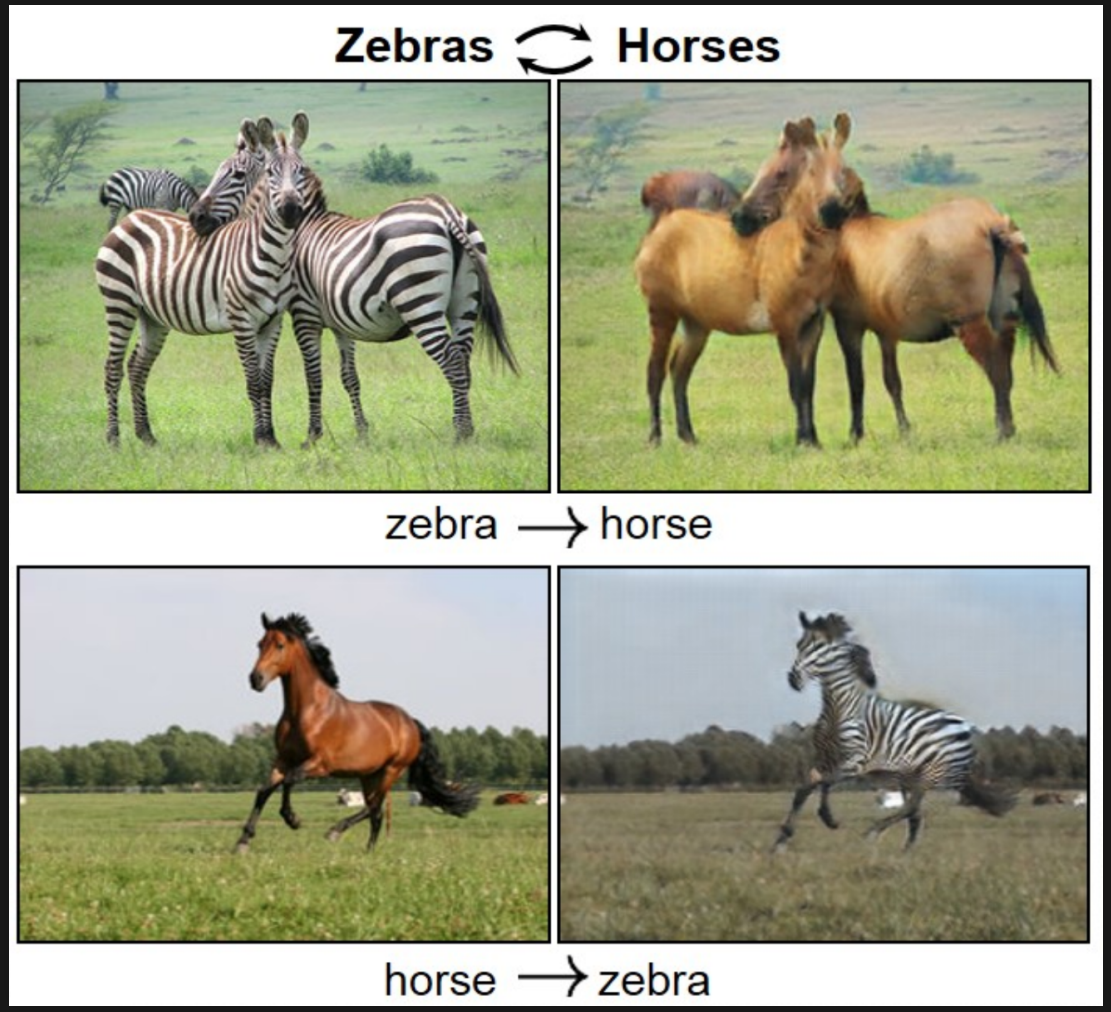
Or more specifically, their Tensor cores:



with 130.000 GigaFlops$^{(fp16)}$ of raw power.

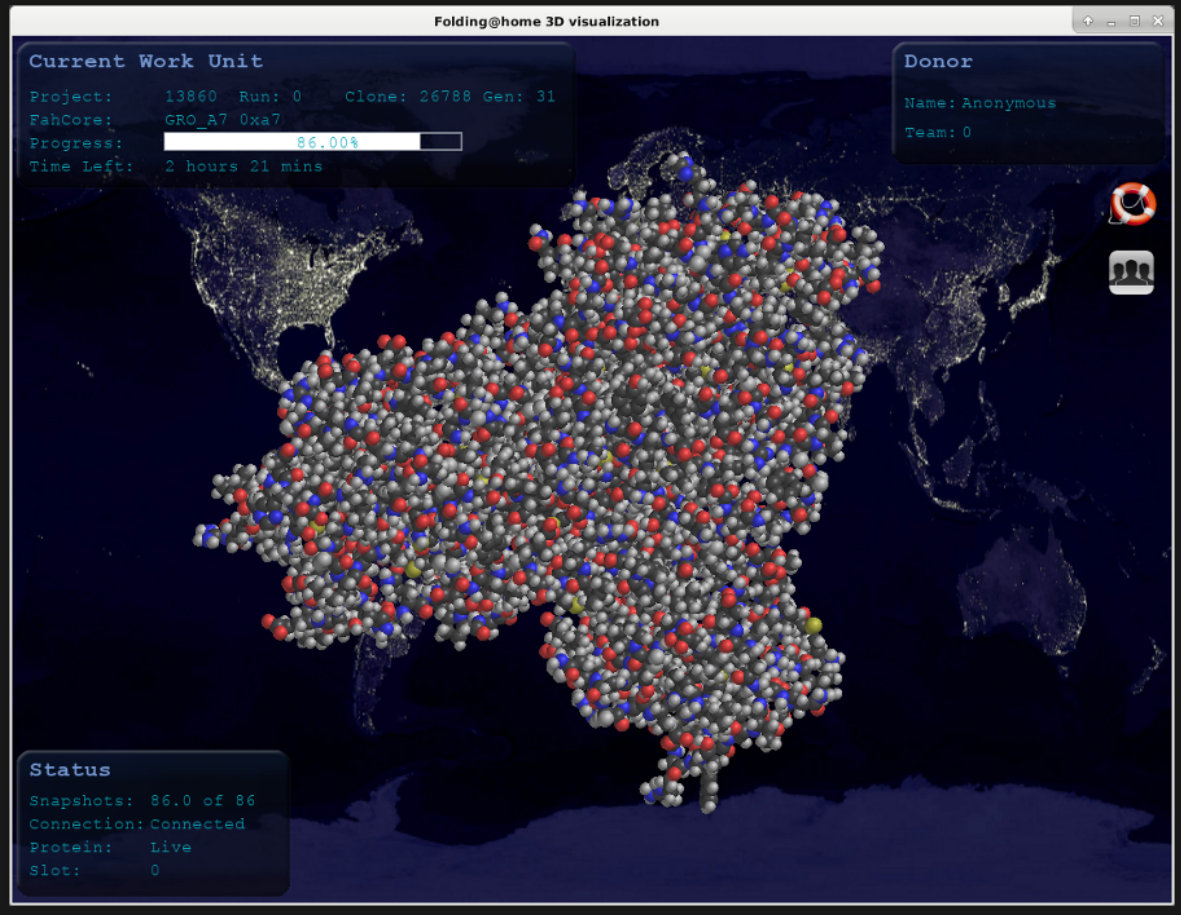
The ML group had great stories about their use

Changing species



(CycleGAN)

Eradicating diseases

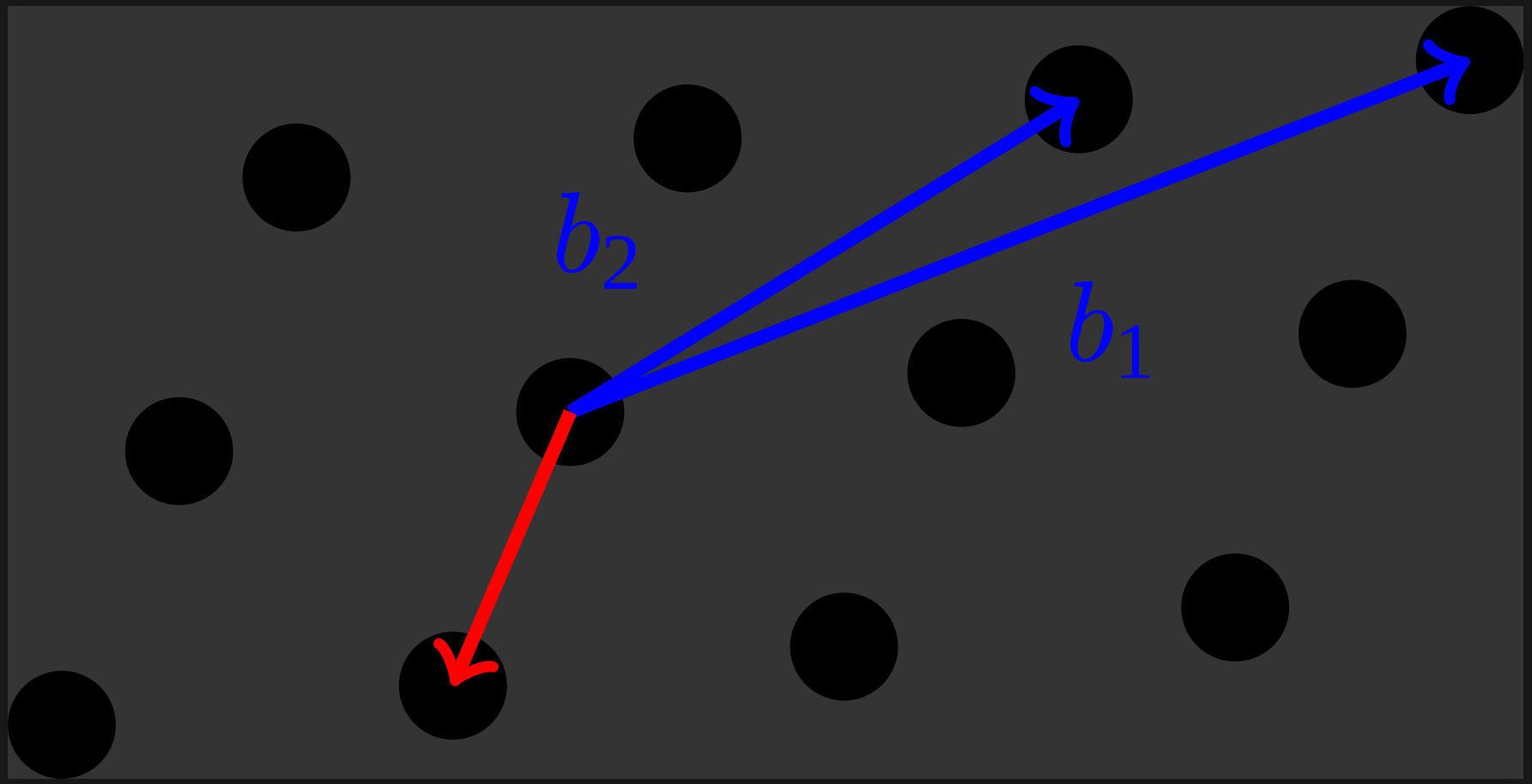


World peace

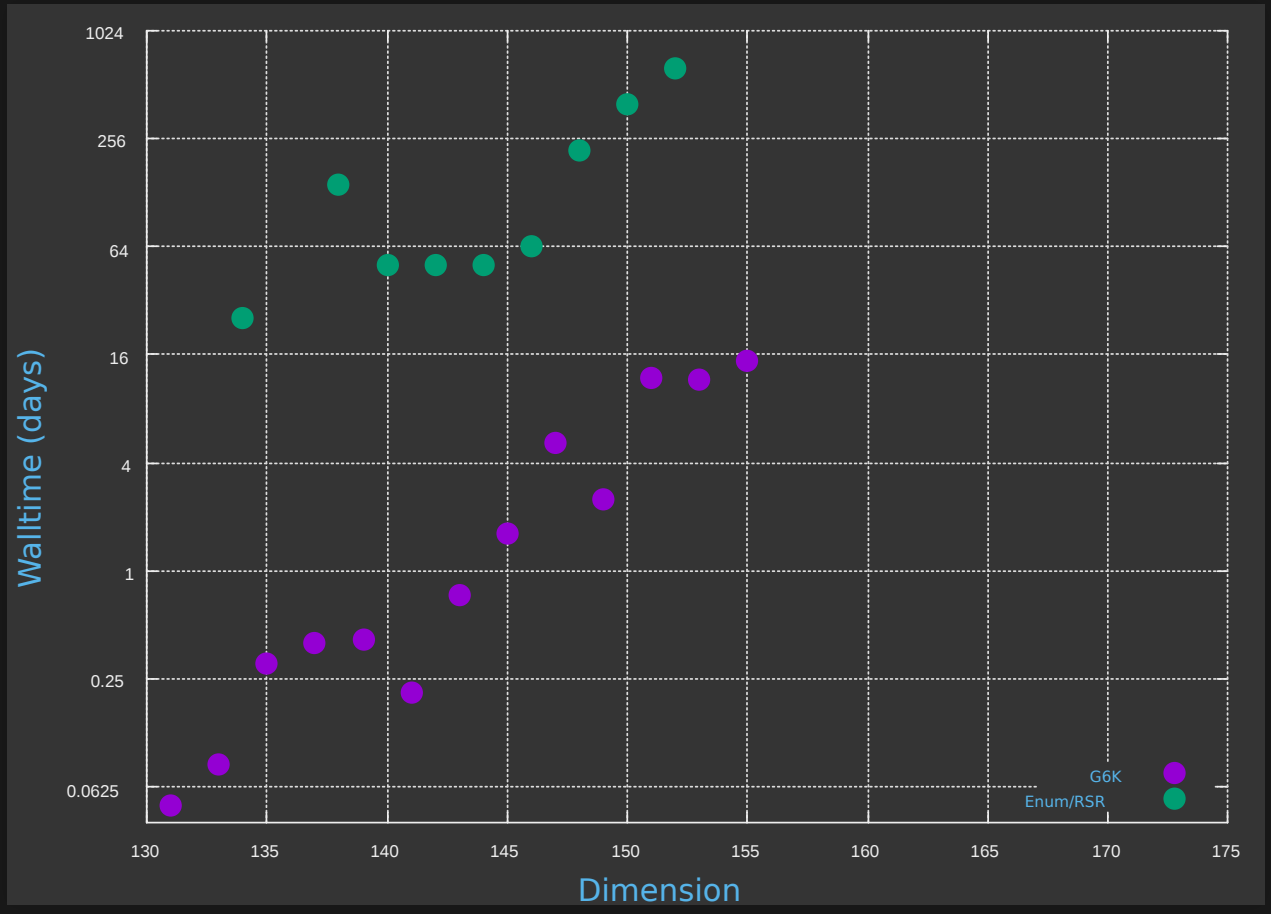
But the cryptanalyst saw only one good use:

But the cryptanalyst saw only one good use:

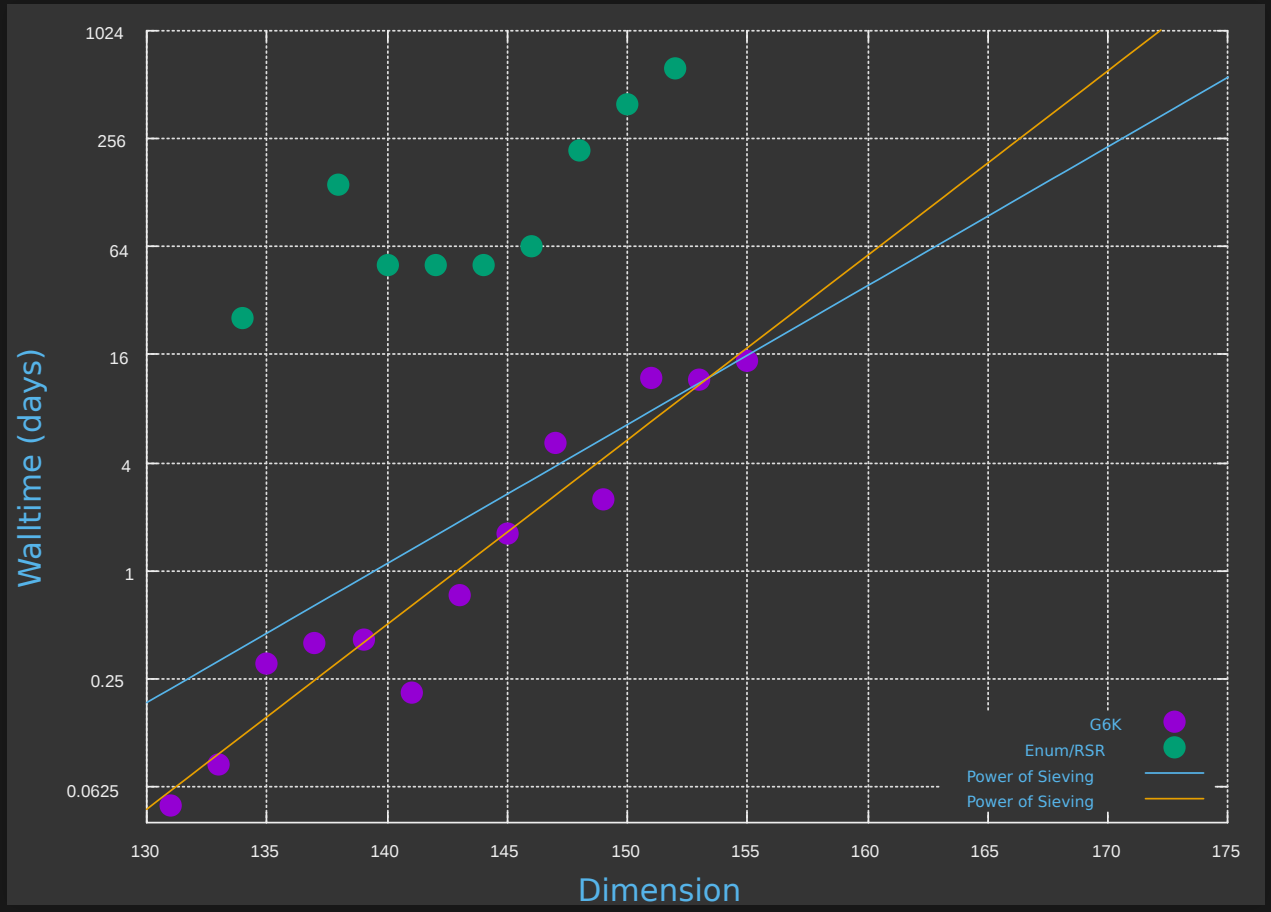
finding a short lattice vector



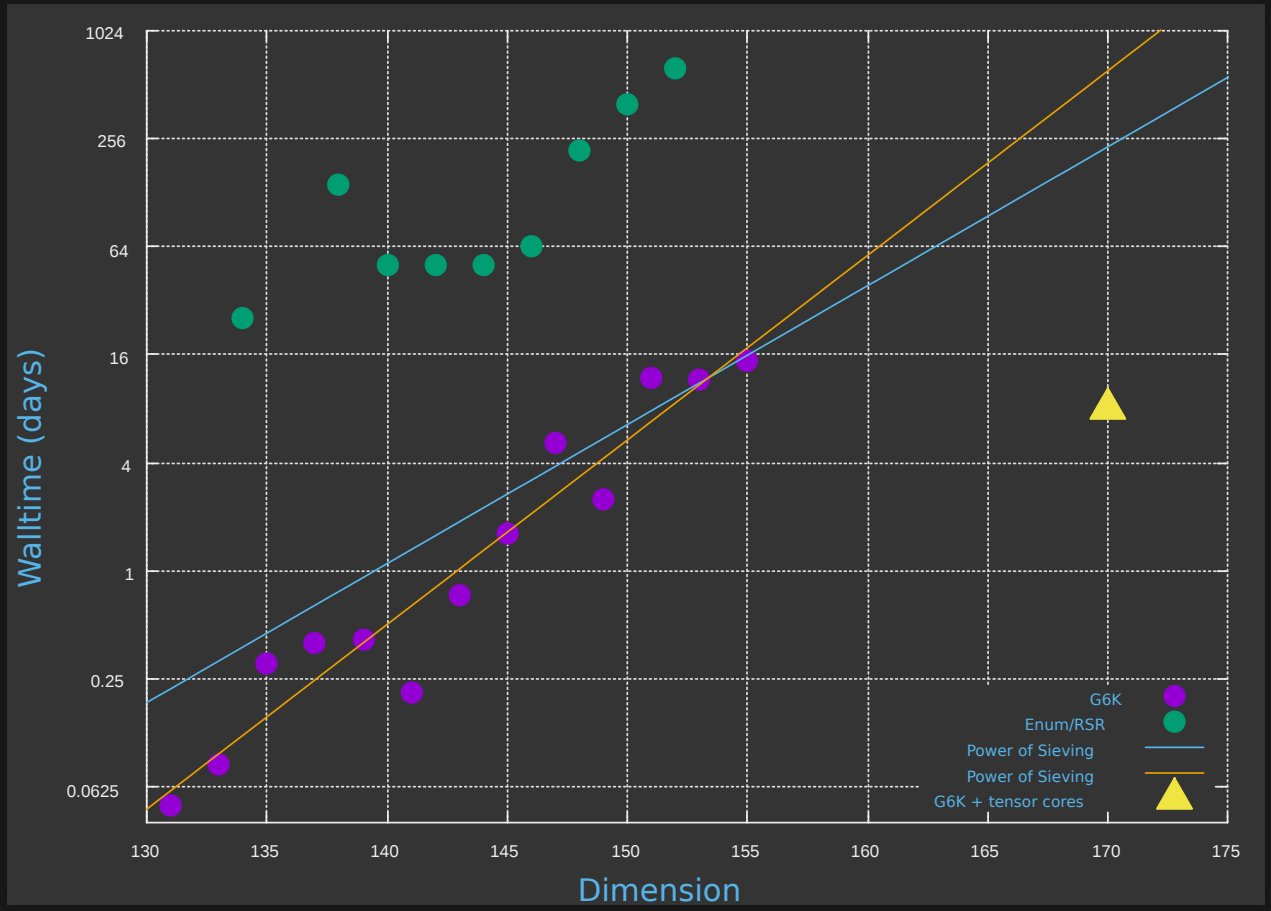
TU Darmstadt SVP Challenge



TU Darmstadt SVP Challenge



TU Darmstadt SVP Challenge



🎉 New World Record! 🎉

$$d = 170, \text{seed} = 0, \text{Walltime} \approx 8 \text{ days}$$

```
[-92 -354 -573 177 387 -31 -114 -13 -316 -22 302 65 43 -195
28 -213 -187 -196 -798 321 -153 343 165 -253 -298 59 -38
468 88 -124 253 196 -518 99 449 -12 79 -382 379 287 161 67
195 -279 -206 158 -310 -256 270 301 123 71 237 326 191 -299
9 -23 46 -82 313 -206 27 -210 52 -128 135 225 130 164 -61
267 -111 426 113 149 -220 -133 45 657 -446 -605 152 -396 -245
46 -252 128 338 -55 228 644 101 -52 233 -154 232 -319 35
-339 -222 -183 -211 -173 -126 30 594 -214 89 33 263 53 -38
365 -127 4 -124 -575 65 -169 130 359 -189 381 375 -315 52
74 181 107 -604 119 423 12 -51 151 279 210 -372 380 -194 2
-91 -49 24 122 -208 -267 -288 146 -475 108 -152 -302 26 -83
-312 284 -320 -242 23 374 -403 -69 177 -11 69 -158 630 440]
```

And they lived happily ever after…