A KVANTUMSZÁMÍTÁS SZOFTVERTECHNOLÓGIÁJA

KOZSIK TAMÁS (ELTE IK)

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

WP6: Software technology for quantum computing

1. Software technology for programming quantum computers
   - Design of designs
   - Piquasso
   - Qubla
2. Quantum computer emulation laboratory
   - Data-flow engine
   - SQUANDER gate synthesis
3. Postquantum cryptography

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Fotonikus kvantumszámítógépek szimulációja

- Python alapú platform
- Gyorsított számítások (C++, FPGA)
- TensorFlow integráció

- Sparse and Shallow Gaussian Boson Sampling

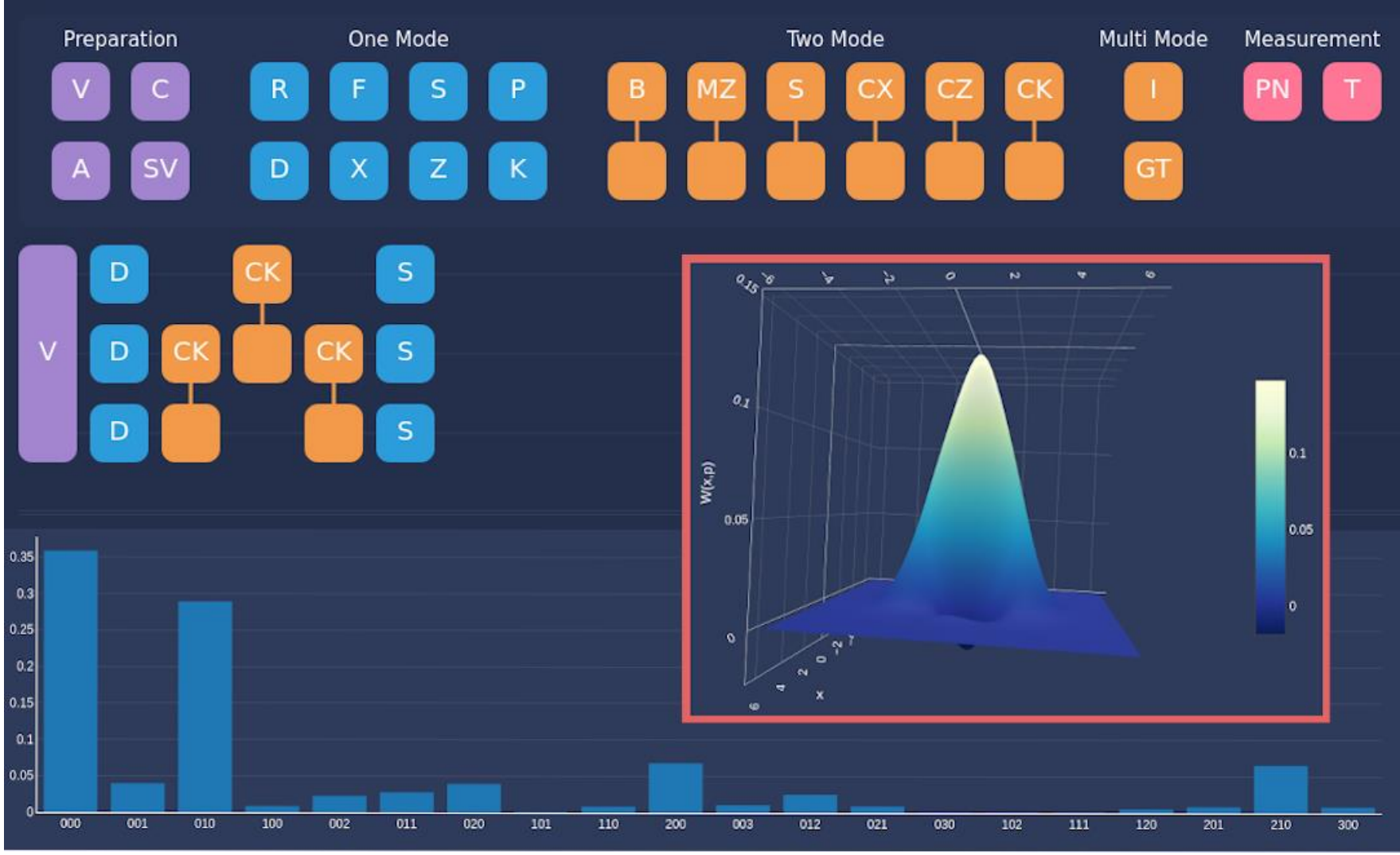
PIQUASSO

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

PIQUASSO

piquasso.com



Piquasso Web Interface

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

- Qubla -

```
function corrected(x, N){
  return ifelse(x<N, x, x-N);
}

function modular_multiply(x, y, N){
  local n = len(x),
        wzero = uword{n+1}(0),
        ret = wzero,
        ytmp = uword{n+1}(y);
  for(i : seq(len(x))){
    if(i > 0) ytmp = modcorr(ytmp<<1, N);
    ret = corrected( ret + ifelse(x[i], ytmp, wzero), N );
  }
  return uword{n}(ret[seq(n)]);
}

n = 6;
N = 35;
a = 11;
x = input(quword{n});
z = modular_multiply(x, uword{n}(a), N);
output(z);
```

- Qubit alapú programozási nyelv
- „Kvantumlogikát” állítunk elő
- Kvantumagnosztikus definíciók
- Python-könyvtár
- Qubitszám-csökkentés

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Design konstrukciók

- Unitér designok tulajdonságainak vizsgálata
- Mély reprezentációelméleti módszereket használva konstrukciók kidolgozása
- Unitér csoport tenzorhatványának irreducibilis felbontásának vizsgálata
- Véges csoportok keresése, amelyeknek tenzorhatványának valamelyik irrep komponensre megszorítva irrep marad, ezekből unitér designok konstruálása
- Ortogonális vagy szimplektikus 2-designokból unitér 2-design készítése bázistranszformációval

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Adatfolyam alapú számításgyorsítás FPGA-val

- Adatok átfolyatása a chipen
- Elemi műveletek a chip különböző pontjain
- Nagyfokú párhuzamosítás
- Data-flow engine (DFE) = adatfolyam-programozás + FPGA hardver
- Pl. permanens számítása

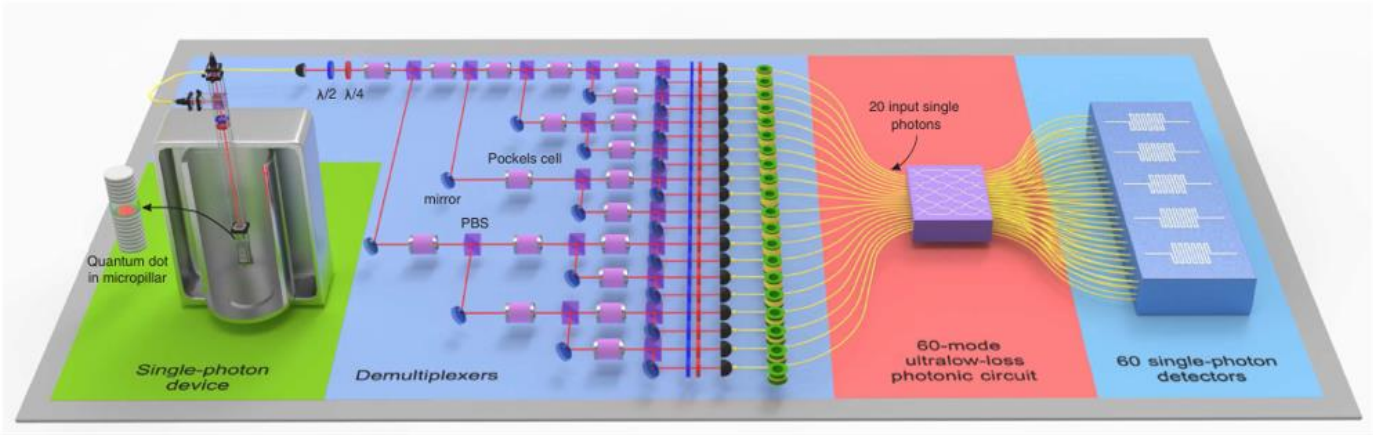
MAXELER Technologies
Maximum Performance Computing

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Boson Sampling kísérlet szimulációja DFE-vel

PHYSICAL REVIEW LETTERS **123,** 250503 (2019)



Peter Clifford, Raphaël Clifford: arXiv:1706.01260, arXiv:2005.04214

20 photons: ~0.03 sec/sample
30 photons: ~2-9 sec/sample
40 photons: ~430 sec/sample

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kapufelbontás: SQUANDER

Circuit name	n	IBM QX (*39*)		QISKIT (*40*)		SQUANDER (*41*)			comp.
		CX	D	CX	D	CX	D	f	rate
4gt12-v0_87	6	112	131	625	1146	47	73	0.0028	93.6%
4gt12-v0_88	6	86	108	853	1647	44	71	0.0072	95.7%
4mod5-bdd_287	7	31	41	1037	1825	26	41	0.012	97.8%
alu-bdd_288	7	38	48	224	408	30	35	0.0038	91.4%
C17_204	7	205	253	2992	5915	104	133	0.0042	97.8%
ex2_227	7	275	355	2852	5554	133	161	0.0128	97.1%
majority_239	7	267	344	4024	7950	143	175	0.0127	97.8%
rd53_131	7	200	261	6538	12320	93	119	0.0129	99.0%
rd53_135	8	134	159	26126	50436	120	147	0.0195	99.7%
rd53_138	8	60	56	18567	35172	87	117	0.061	99.7%
cm82a_208	8	283	337	11246	22284	86	67	0.0129	99.7%
con1_216	9	415	508	55822	109798	205	229	0.118	99.8%

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kvantumrezisztens kriptográfia

- Izogénia alapú módszerek vizsgálata
- SCALLOP séma: könnyen számolható csoportstruktúra
- pSIDH: ellenáll a SIDH elleni támadásoknak
- Kvantumalgoritmus izogénia keresésére
- Sémák törhetőségének vizsgálata

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

NEMZETI KUTATÁSI, FEJLESZTÉSI
ÉS INNOVÁCIÓS HIVATAL

AZ NKFI ALAPBÓL
MEGVALÓSULÓ
PROJEKT