svet ako výpočet

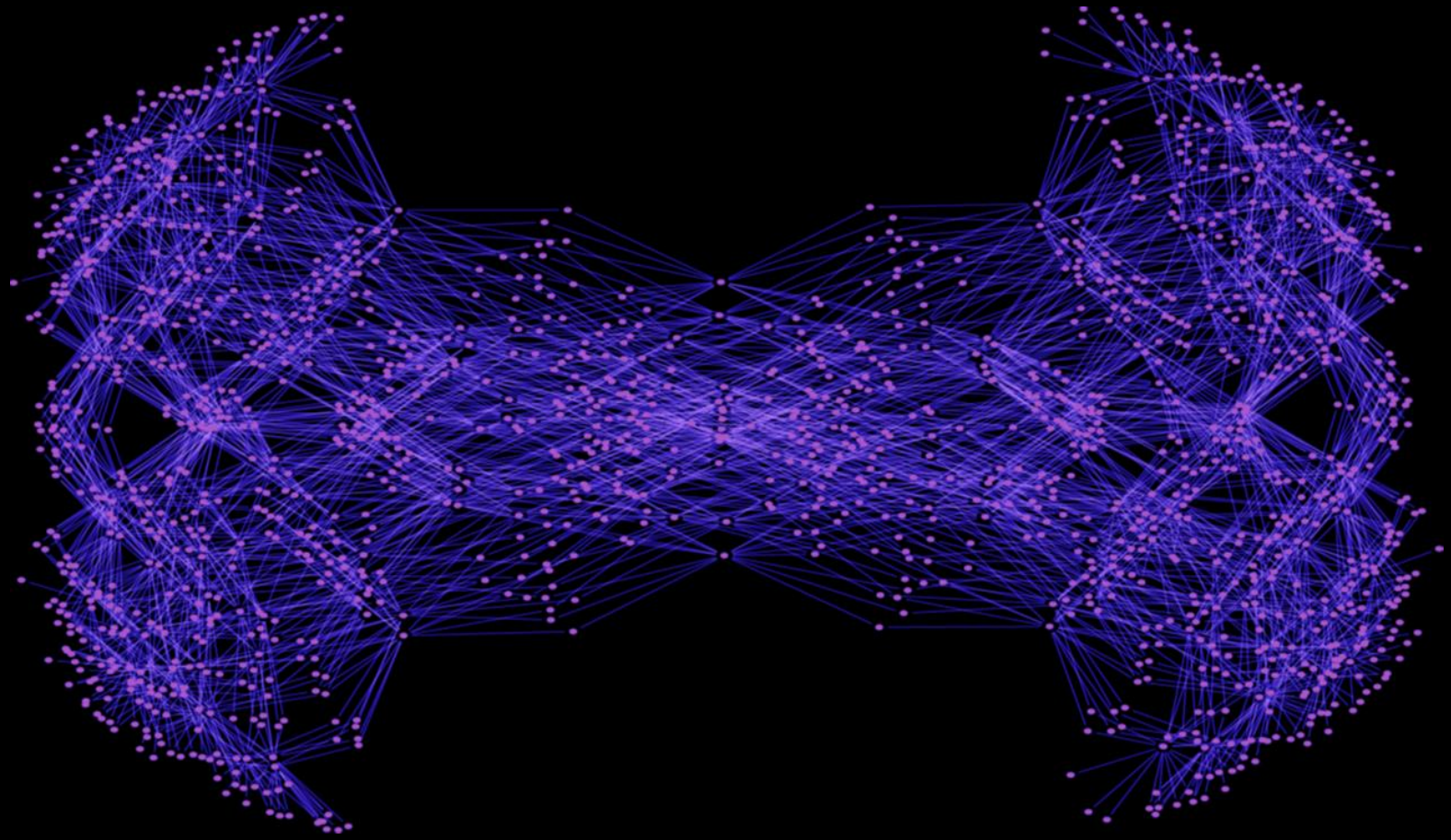
daniel nagaj & rcqi
centrum pre výskum kvantovej informácie
fyzikálny ústav slovenskej akadémie vied

SAS PRO

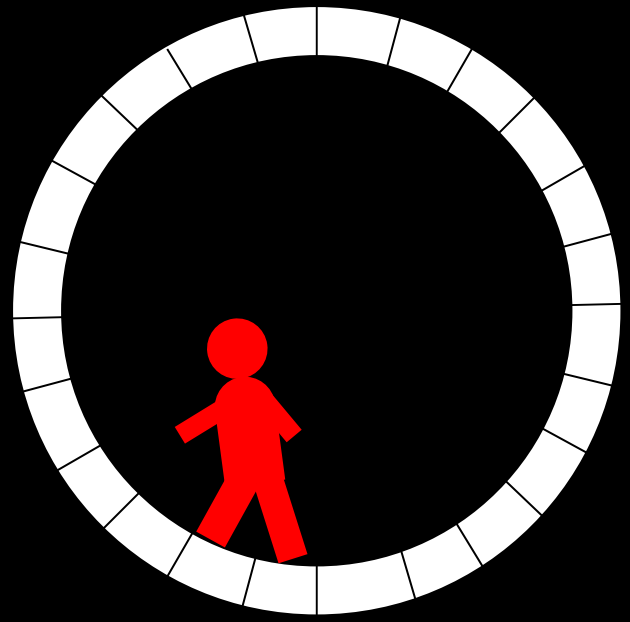
Čo počíta vesmír?

Vlastný vývoj.
Magnetické monopóly.
Kolotanec komét.
Vírenie vody.
Hojdanie hojdačiek.
Zvuk zvonov.
Rádioakivitu rádia.
Konfigurácie kvarkov.
Vibrácie vákua.

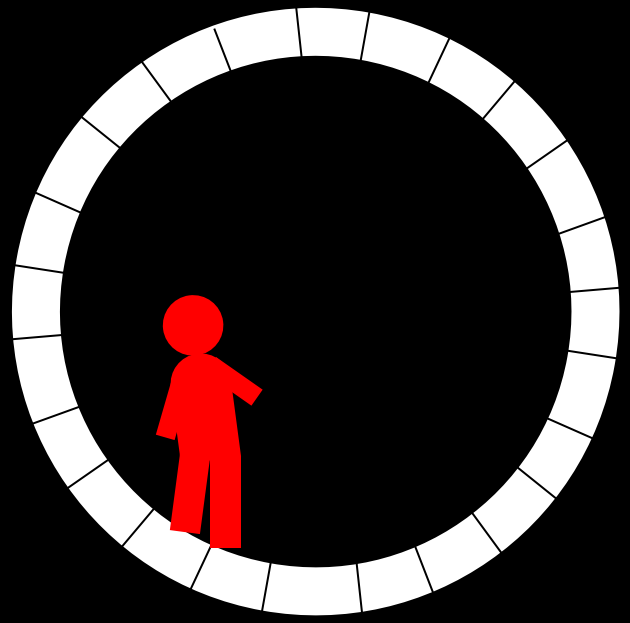
Čo počítame my?



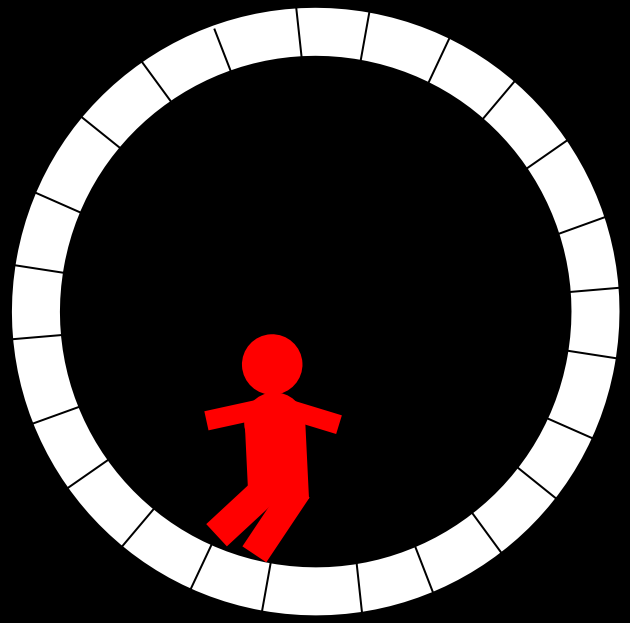
Čo počítame my?



Čo počítame my?

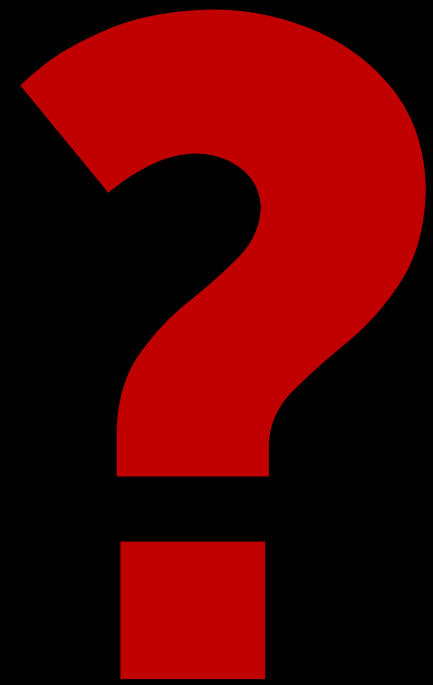


Čo počítame my?



Čo počítame my?

dá sa
všetko
na svete
simulovať na
počítači



všetko fyzikálne
na svete
sa dá efektívne
simulovať na Turingovom
počítači

extended Church
Turing thesis

všetko fyzikálne
na svete
sa dá
simulovať na
počítači

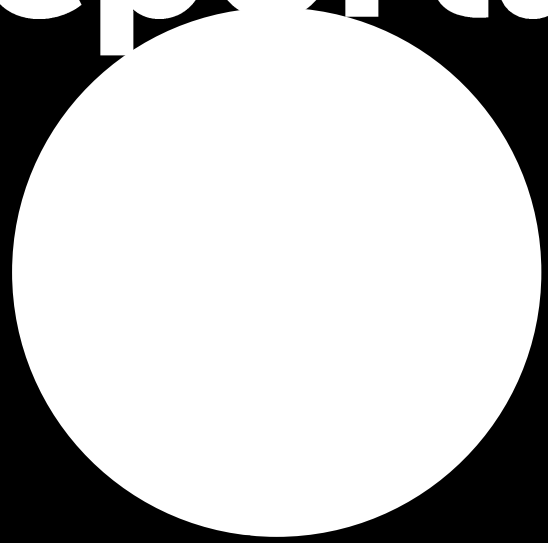
Church
Turing thesis

všetko fyzikálne
na svete
sa dá efektívne
simulovať na kvantovom
počítači

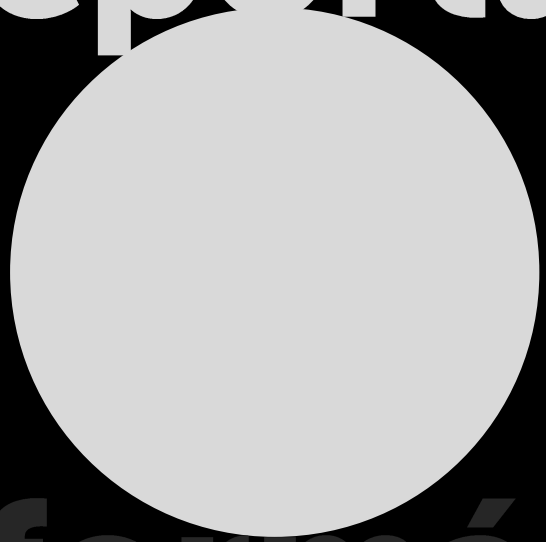
superpozícia

superpozícia

teleportácia

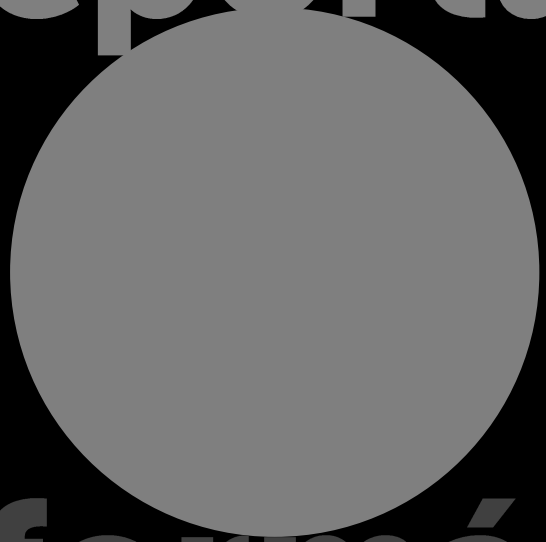


teleportácia



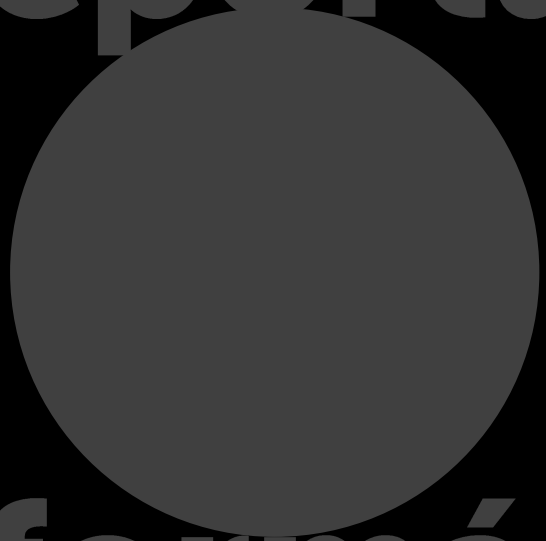
informácia

teleportácia



informácia

teleportácia



informácia

teleportácia

informácia

informácia

informácia
KVANTOVÁ

1 ťažké výpočty

čo chceme a čo príroda dovolí

[wikipedia]

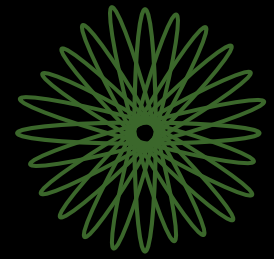
1 ťažké výpočty

čo chceme a čo príroda dovolí

[wikipedia]

2 zvláštna informácia

kvantové stavy a ich spracovanie



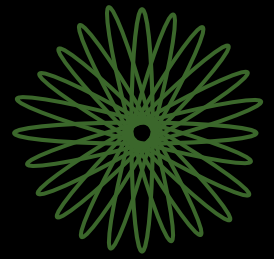
1 ťažké výpočty

čo chceme a čo príroda dovolí

[wikipedia]

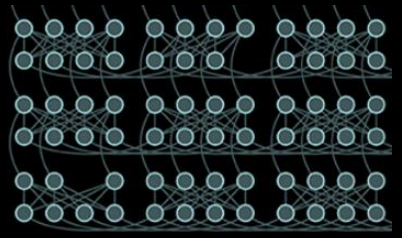
2 zvláštna informácia

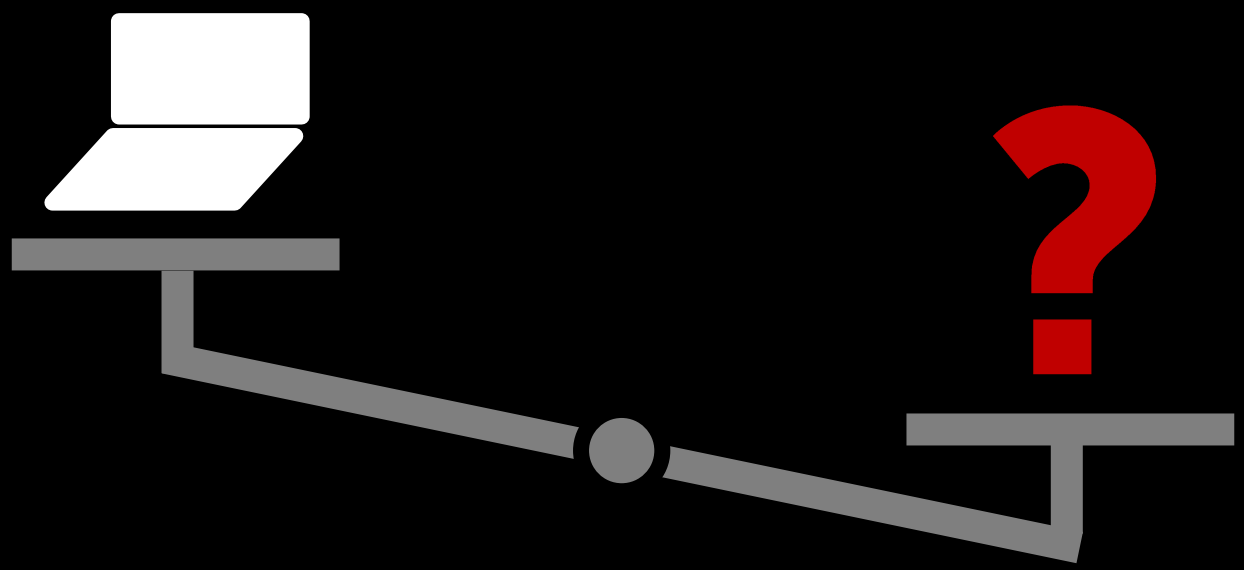
kvantové stavy a ich spracovanie



3 počítame kvantovo

optimalizujeme a simulujeme



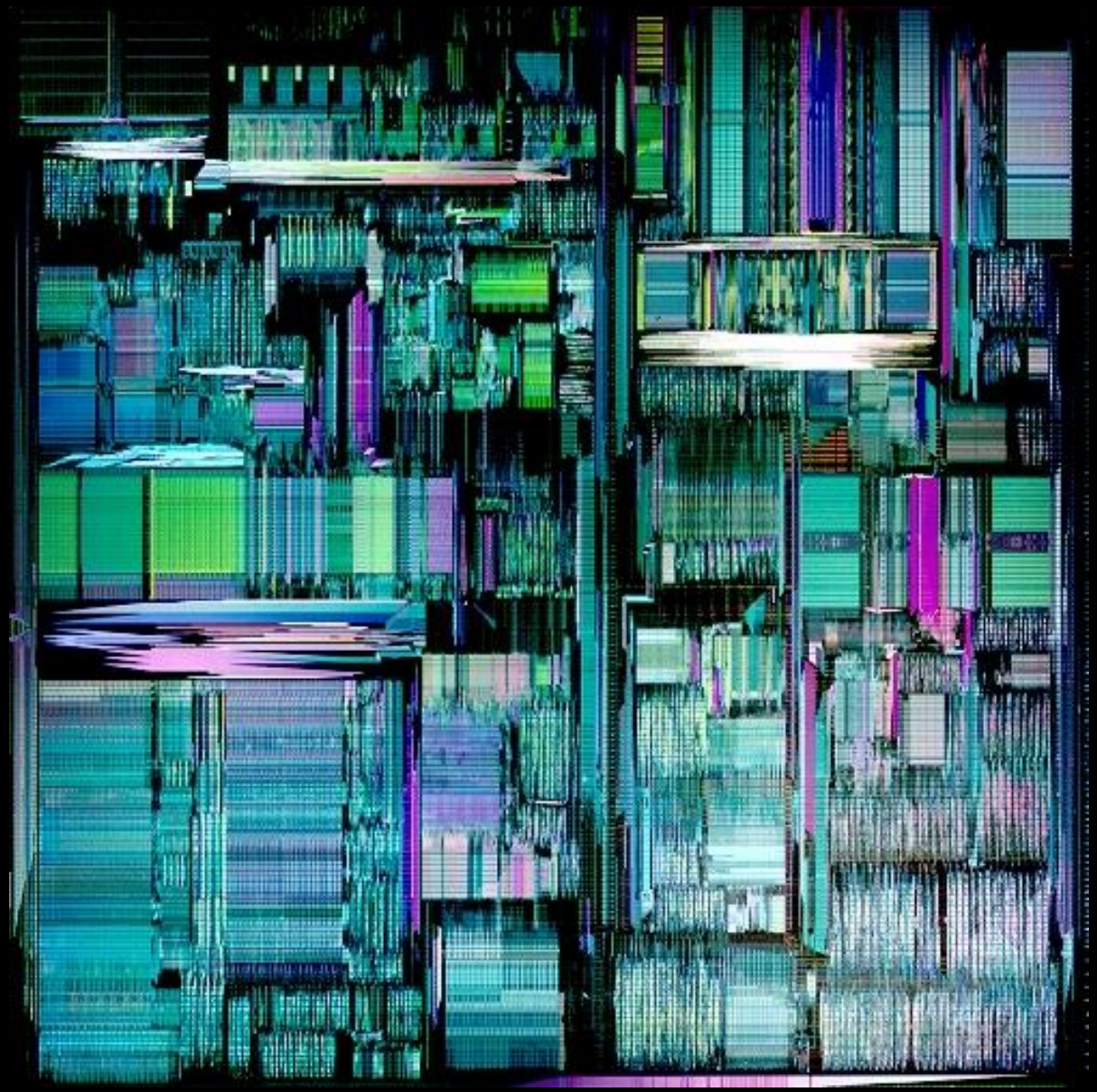


ťažké výpočty

[Nicolas Brodu]

[MIT museum]

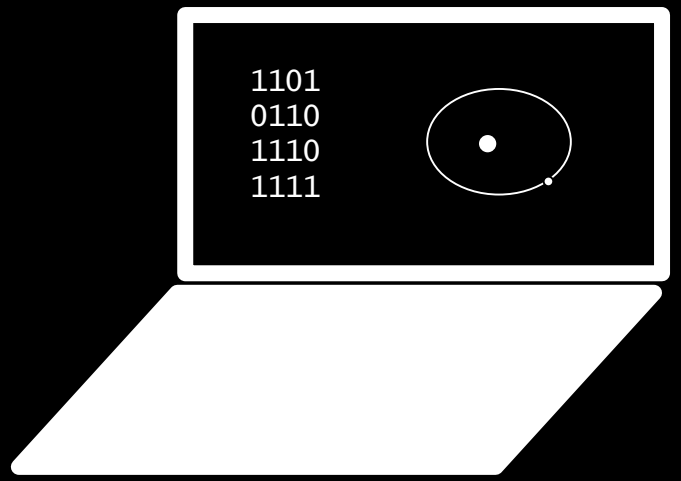
[Zdeněk Starý]

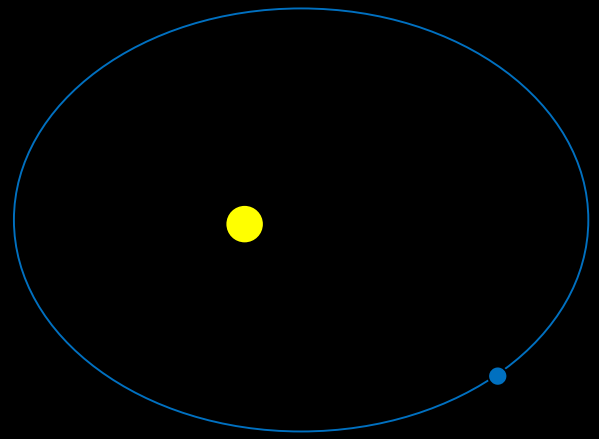


[www.tayloredge.com/museum]

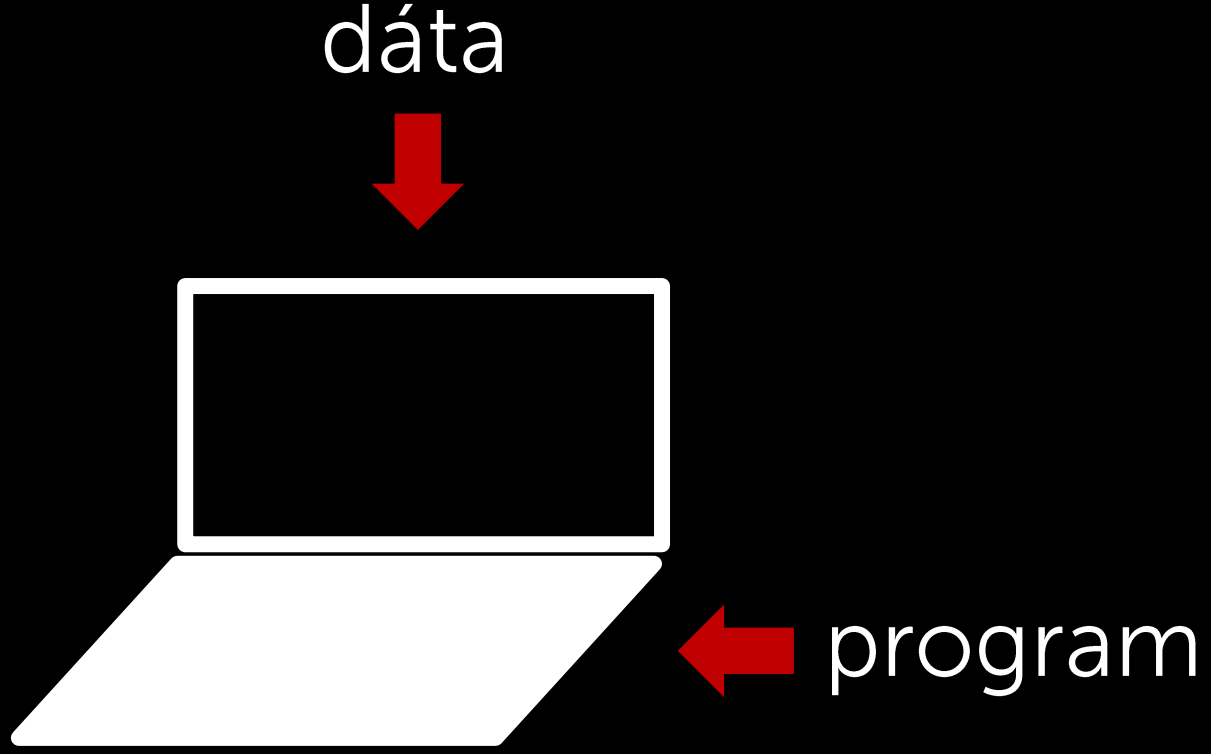
simulácia

realita



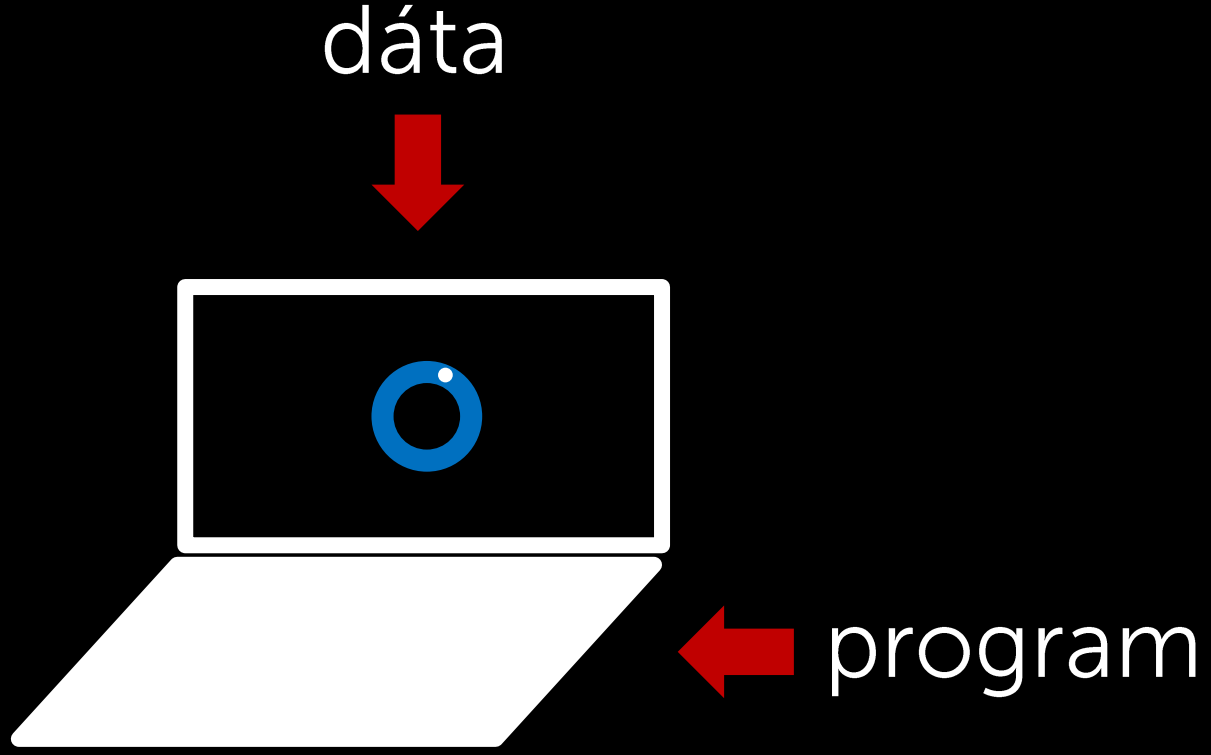


univerzálny počítač



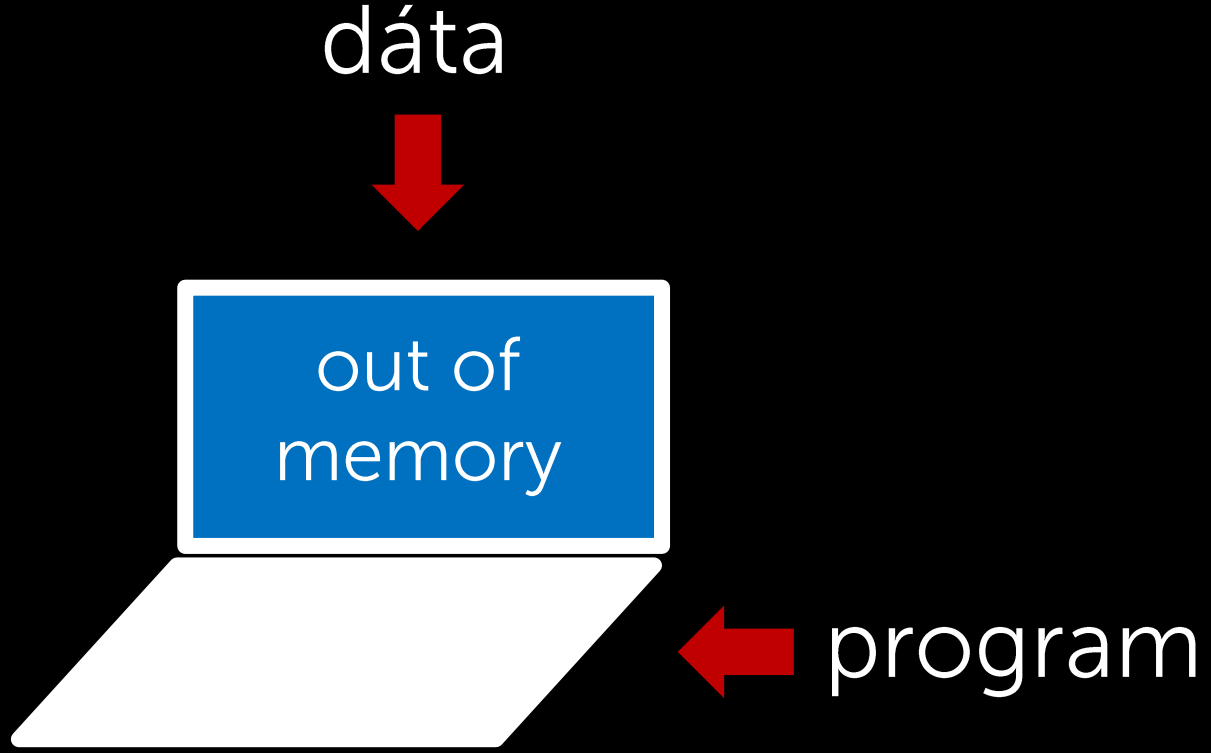
Alan Turing

univerzálny počítač



Alan Turing

univerzálny počítač



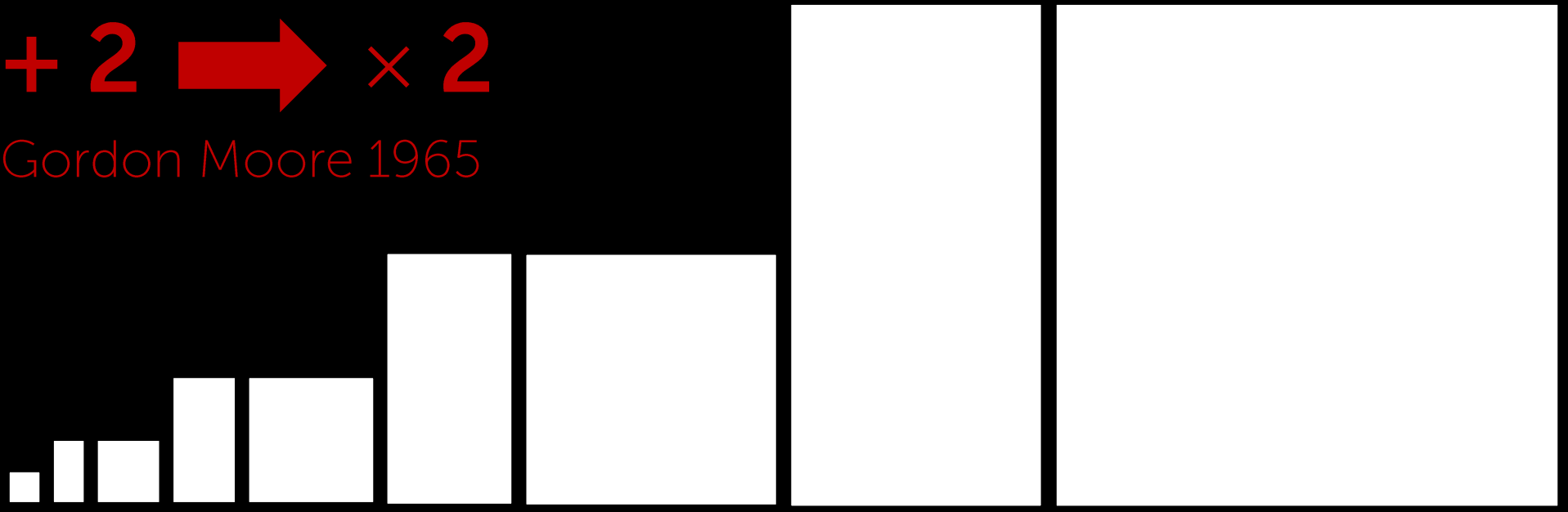
Alan Turing

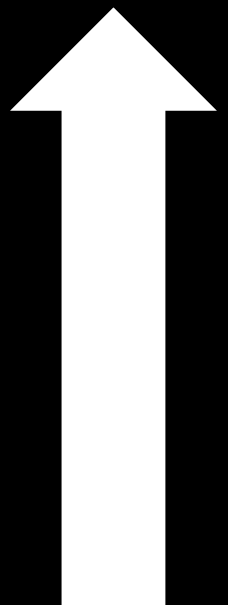
EXPONENCIÁLA

viac, rýchlejšie, lacnejšie (W, €)

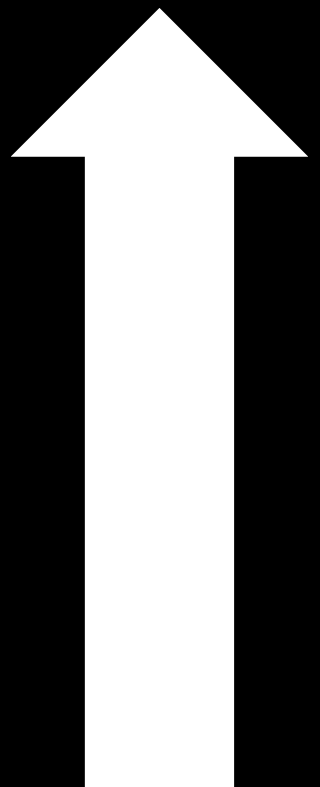
+ 2 ➡ × 2

Gordon Moore 1965

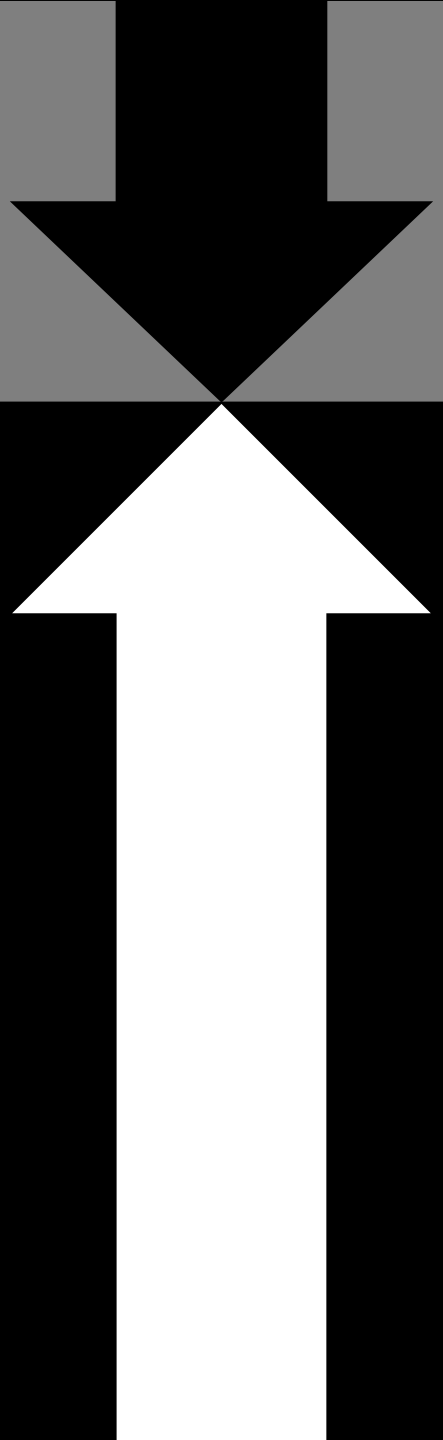




výpočtová sila (hardware)



nové algoritmy (software)
výpočtová sila (hardware)



fyzika

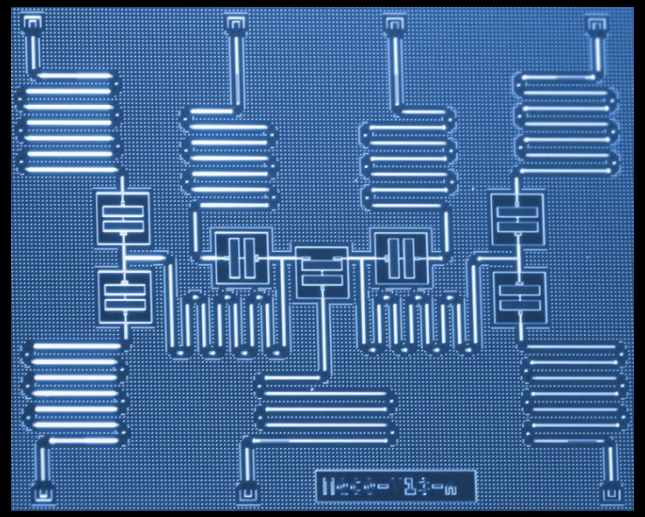
nové algoritmy (software)
výpočtová sila (hardware)

kvantová fyzika

Richard Feynman

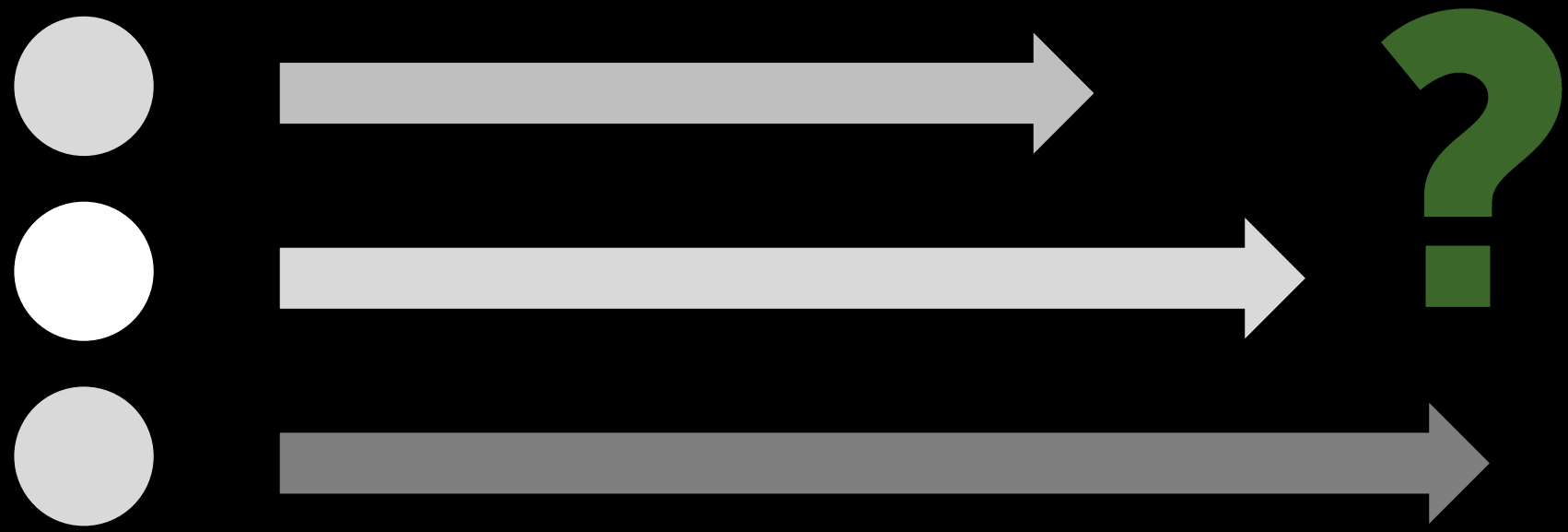
kvantová chémia (elek. štruktúra)
materiály (mnohočasticové systémy)

optimalizácia
kryptografia
štruktúra dát
strojové učenie



[IBM]

zvláštna
informácia

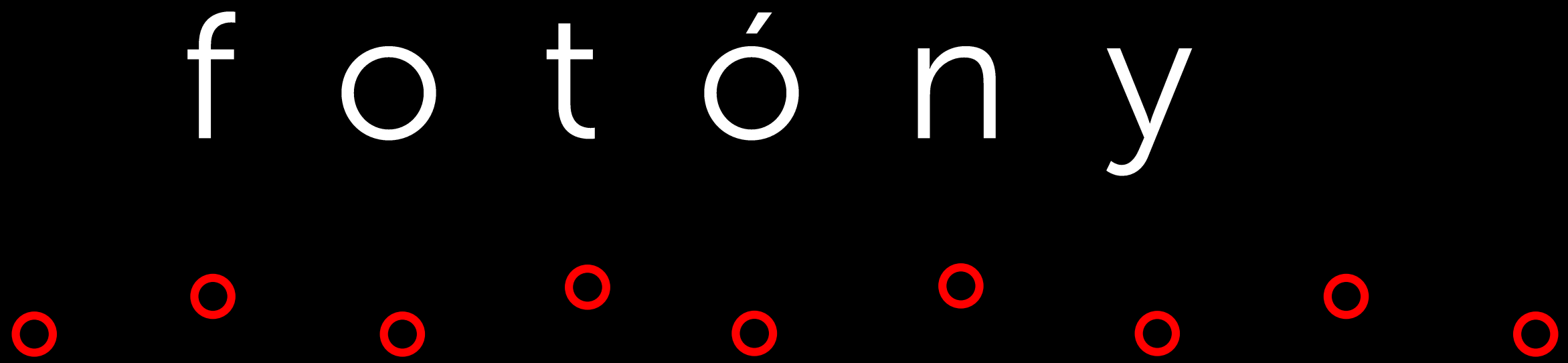


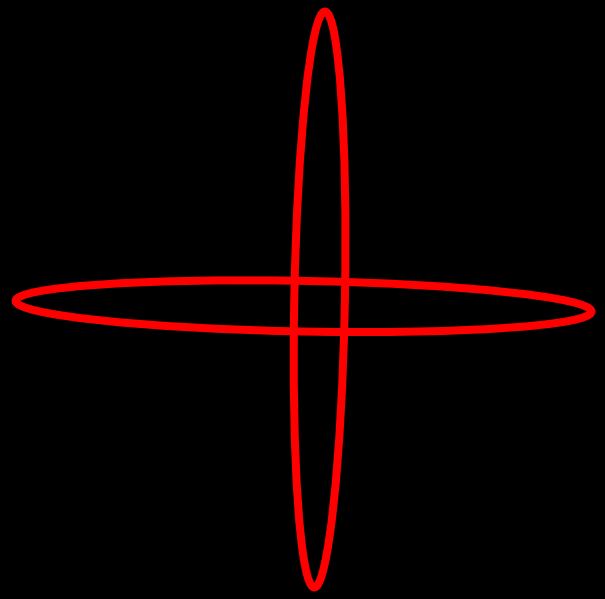
slabšie a slabšie svetlo

slabšie a slabšie svetlo

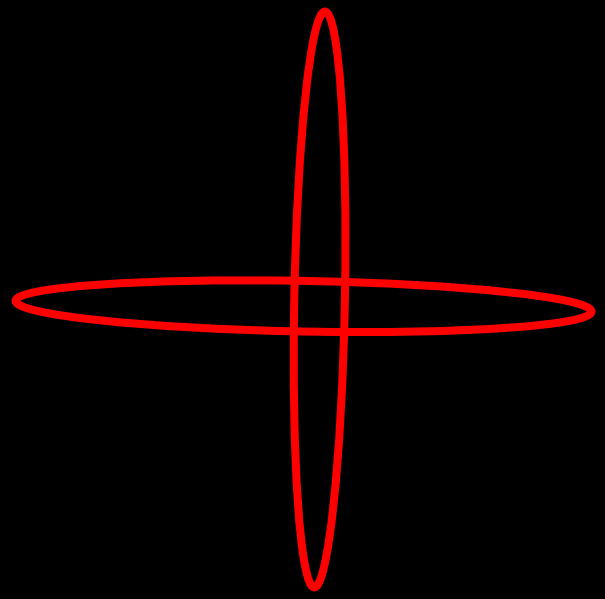
slabšie a slabšie svetlo

slabšie a slabšie svetlo

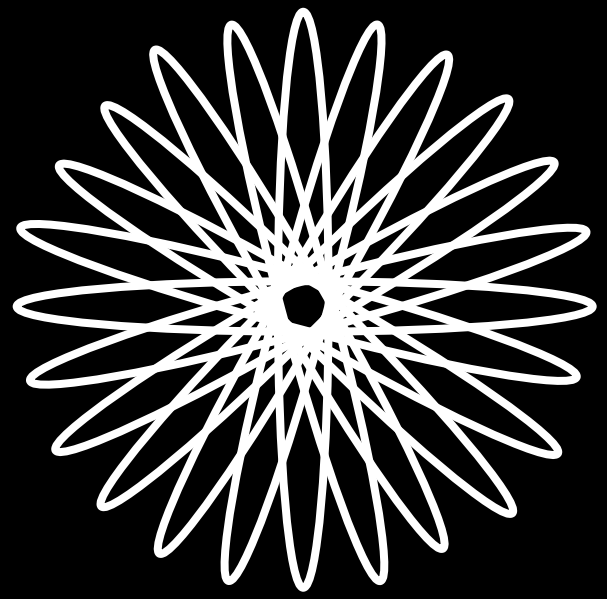

fotóny



bit

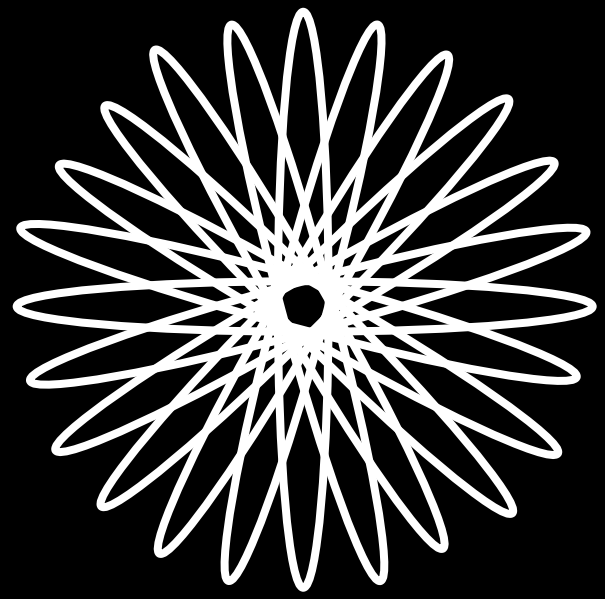


bit

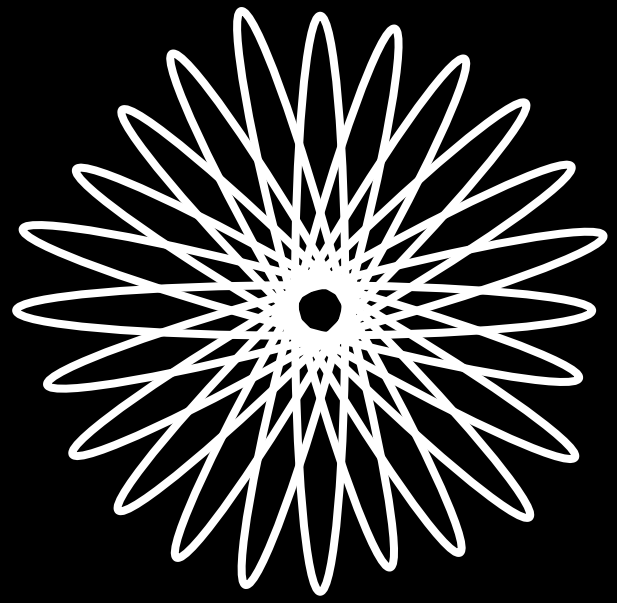


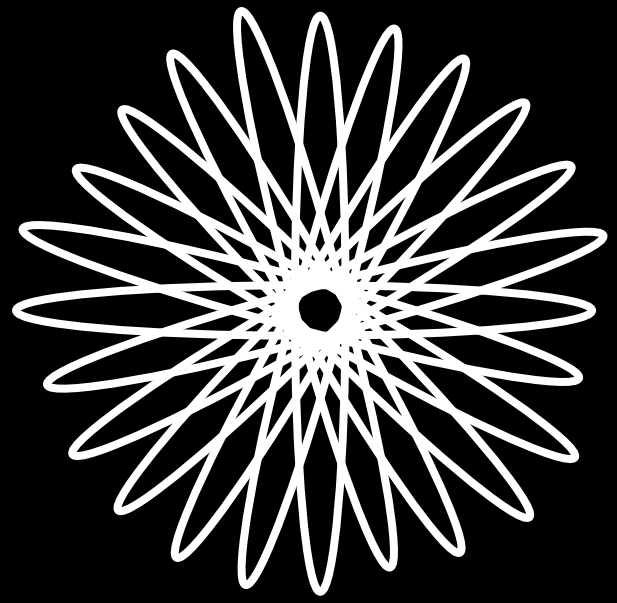
qubit

fotón
atóm
obvod
molekula
nanooscilátor
kvantová bodka

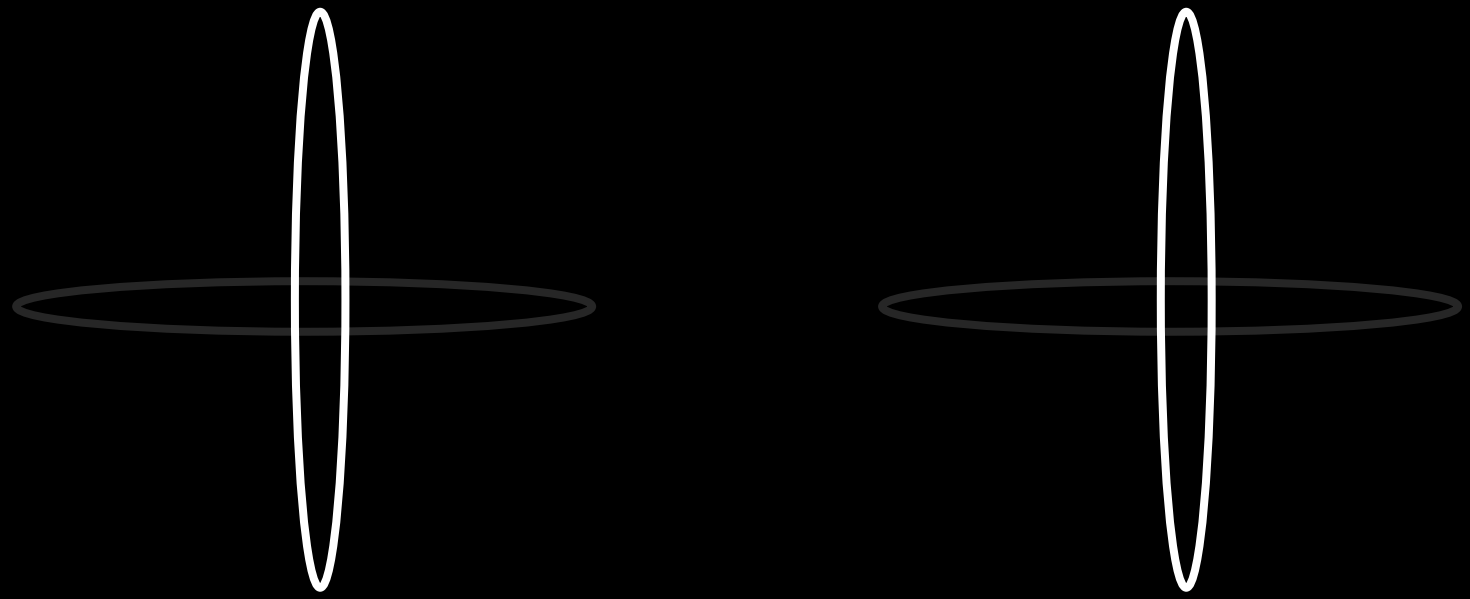


qubit

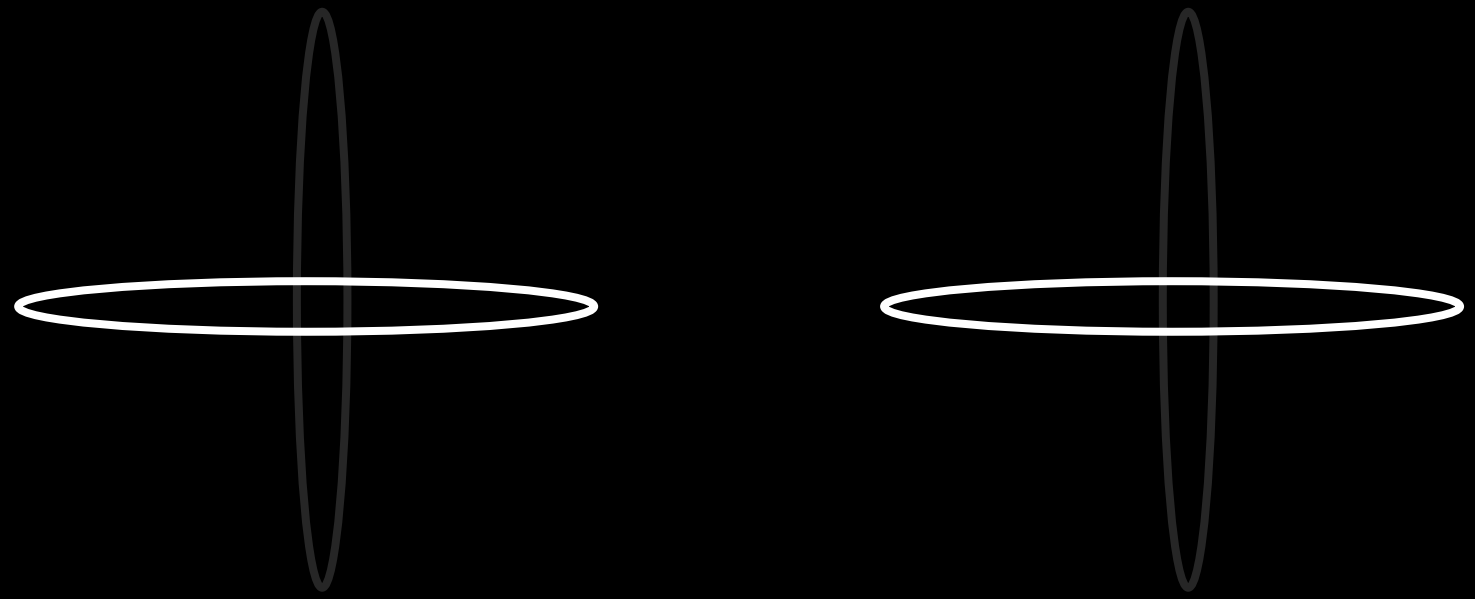




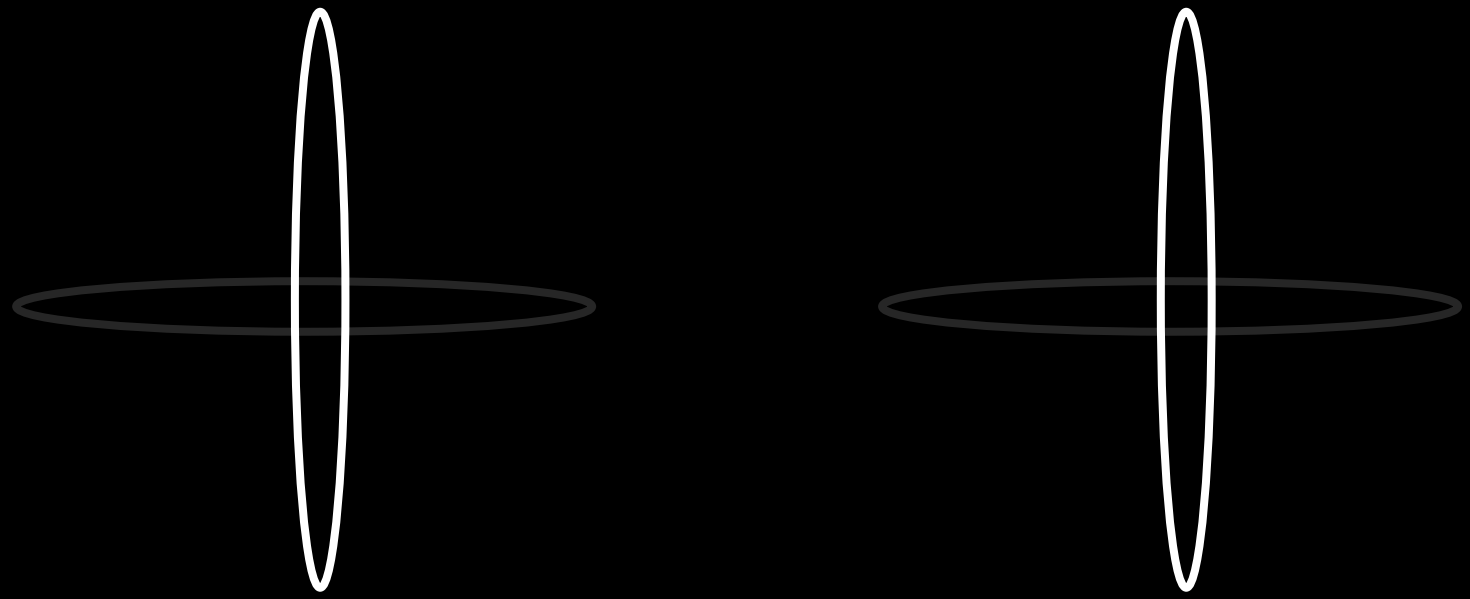
qubit + qubit



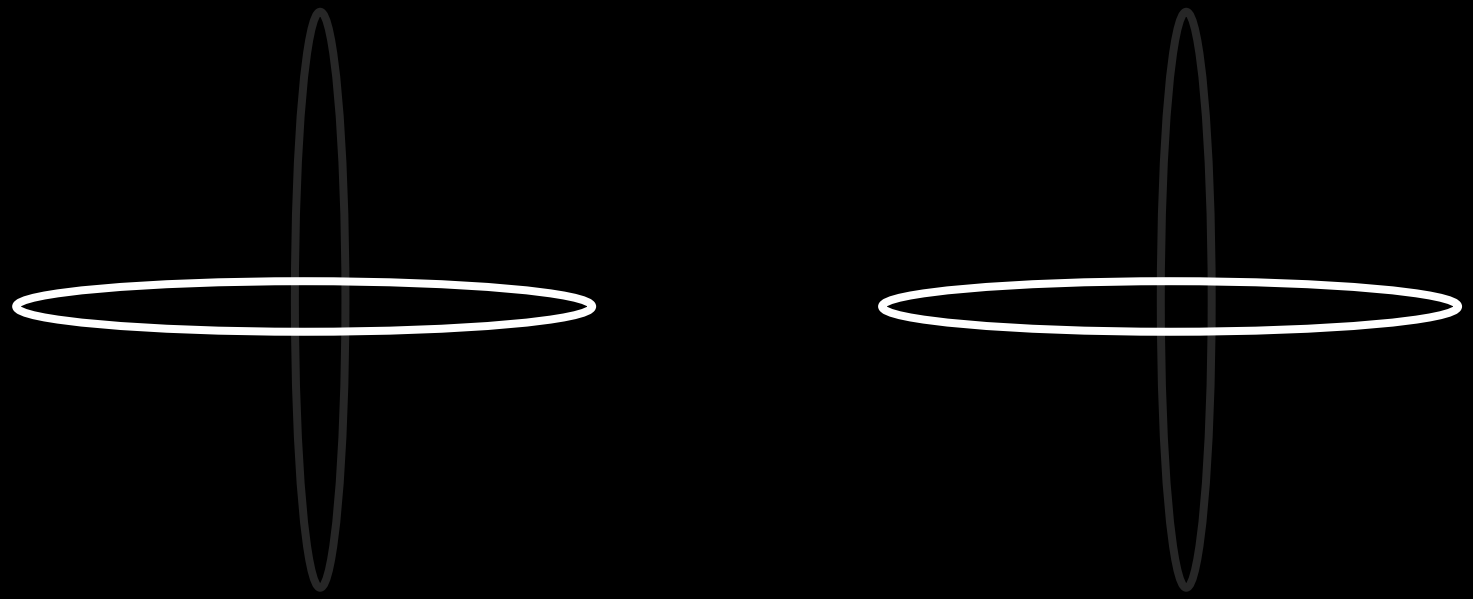
qubit + qubit



qubit + qubit



superpozícia 2 qubitov

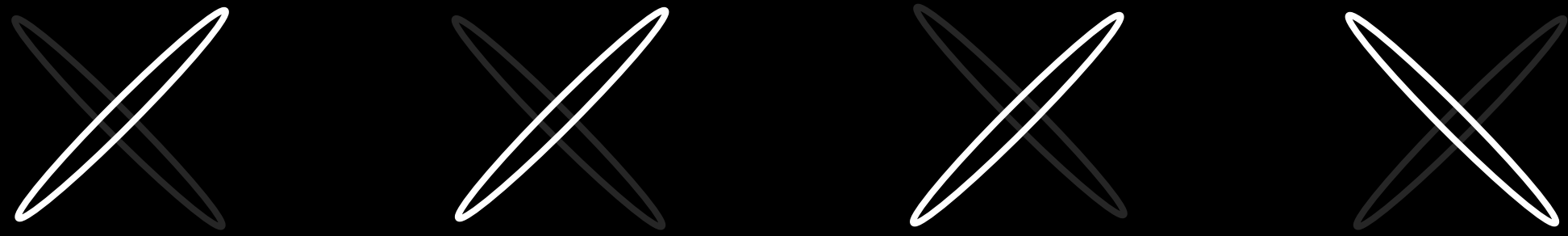


superpozícia 2 qubitov

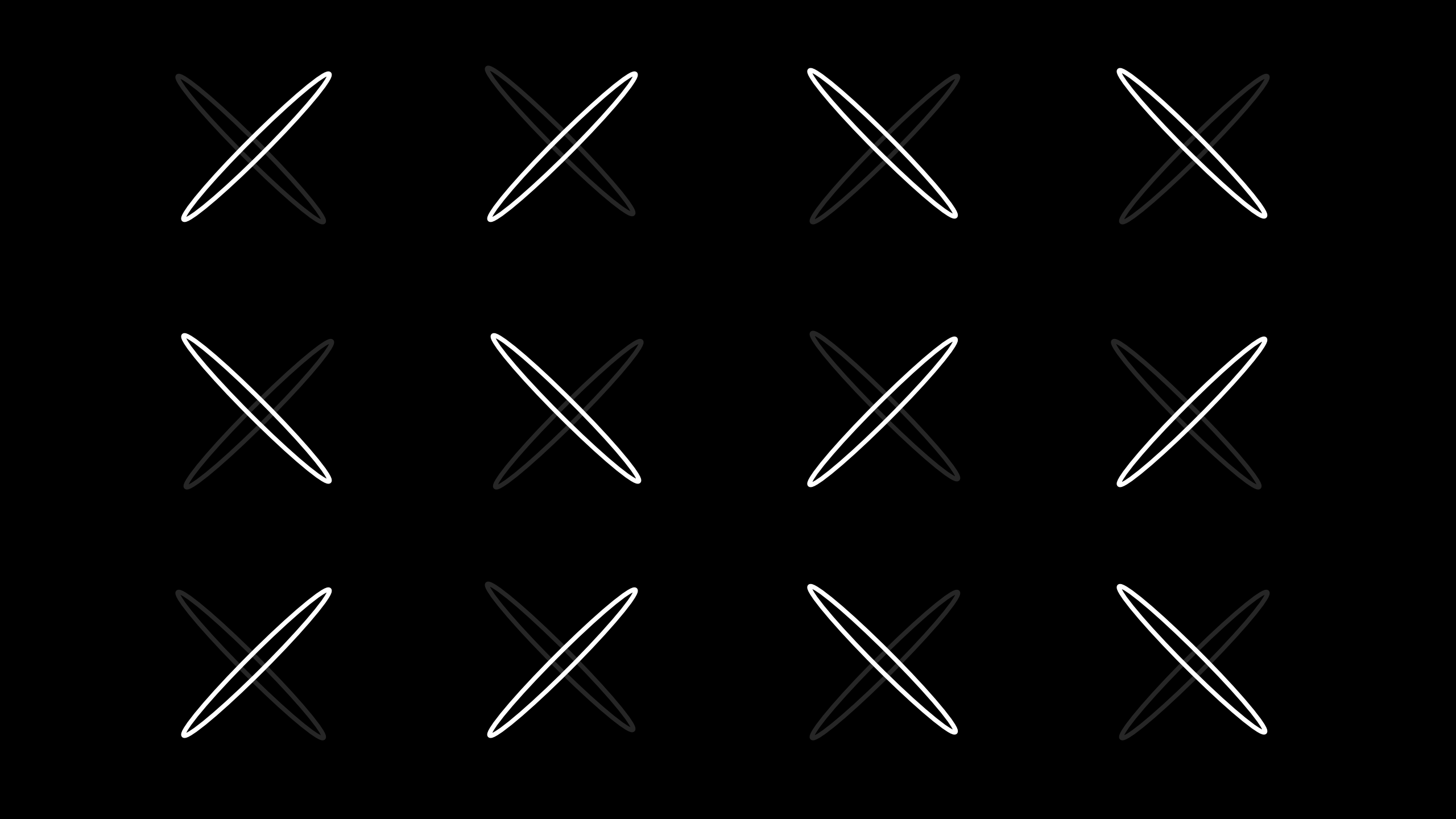
superpozícia N qubitov

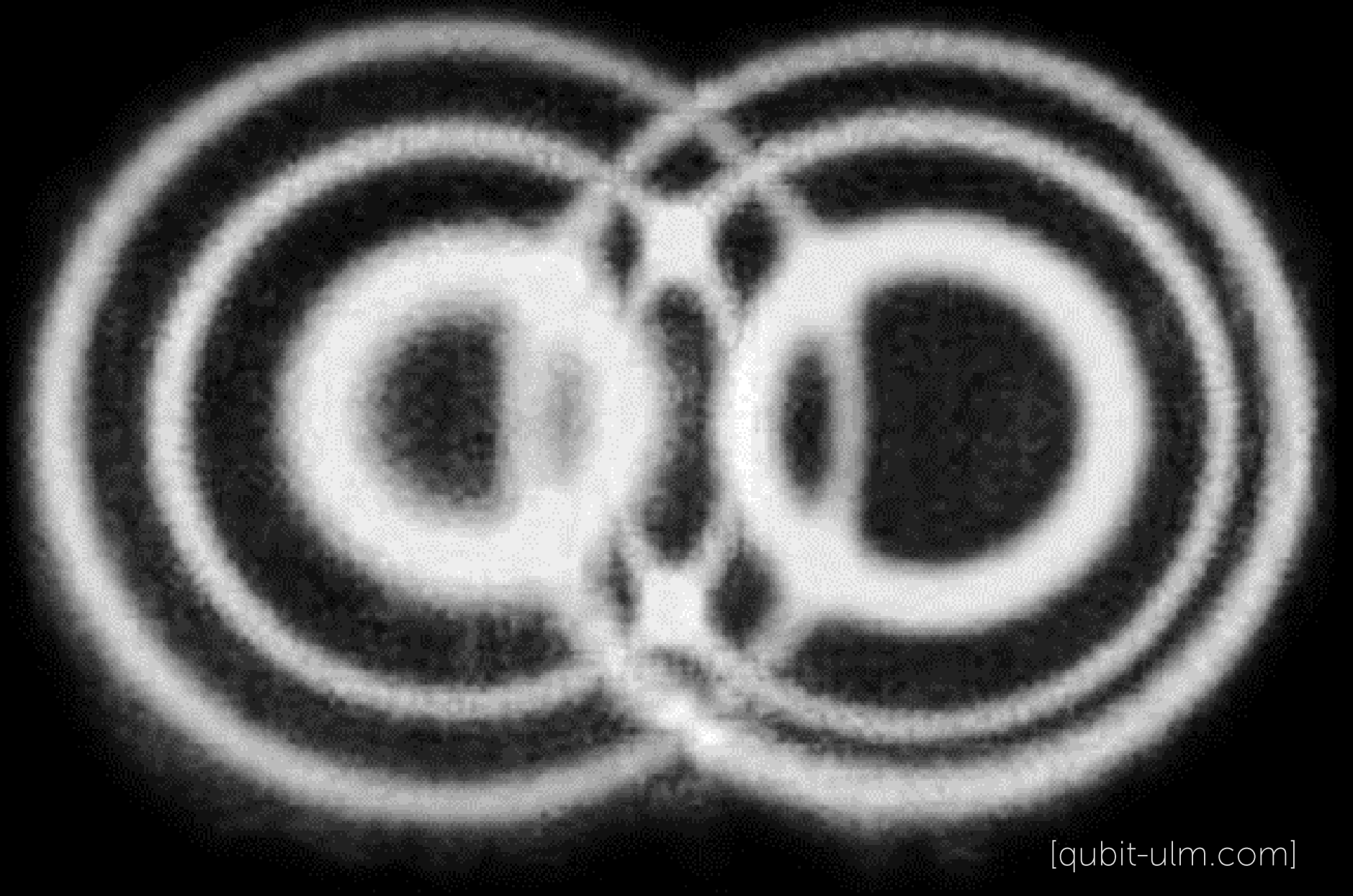
superpozícia N qubitov

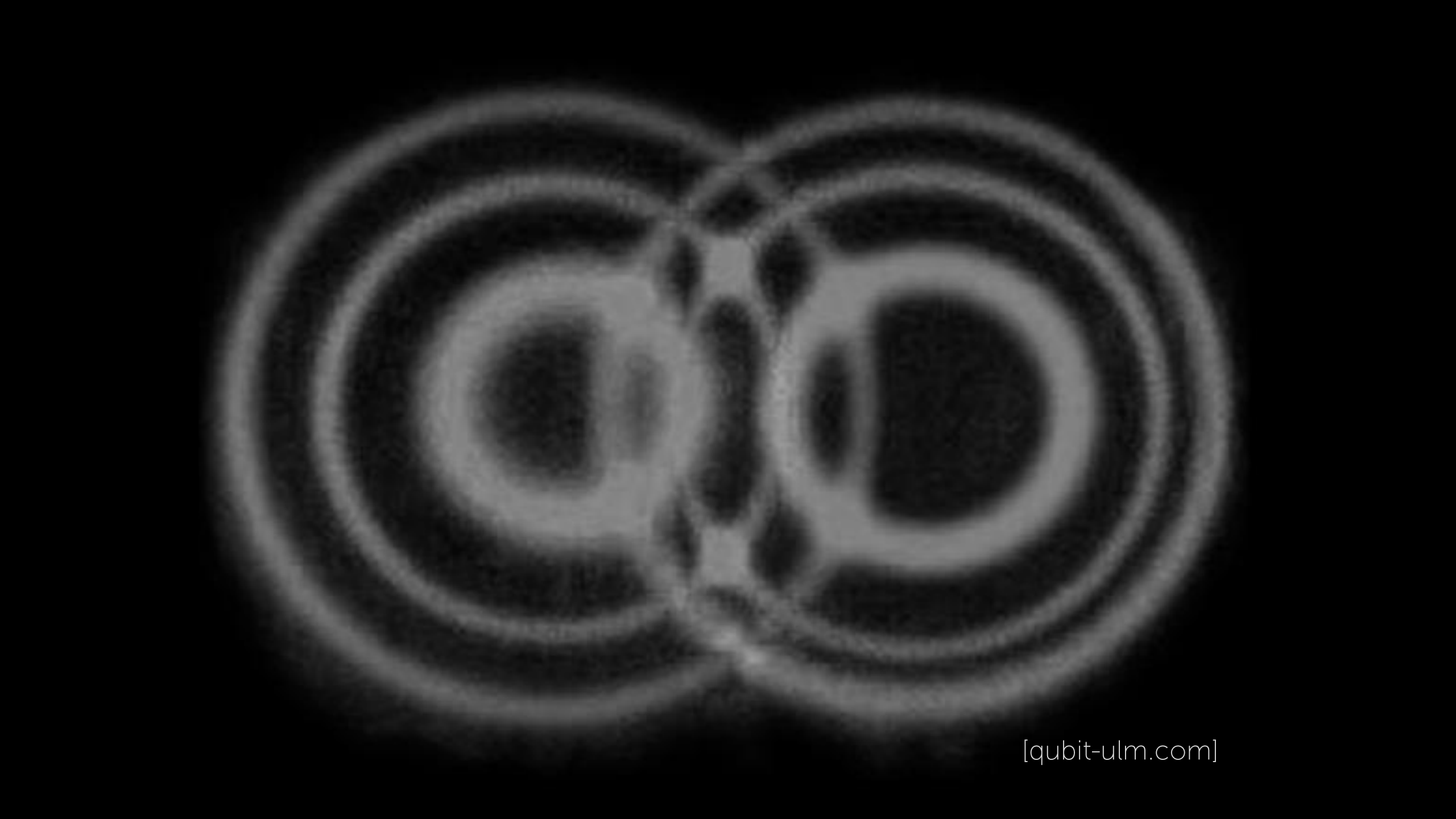
superpozícia N qubitov

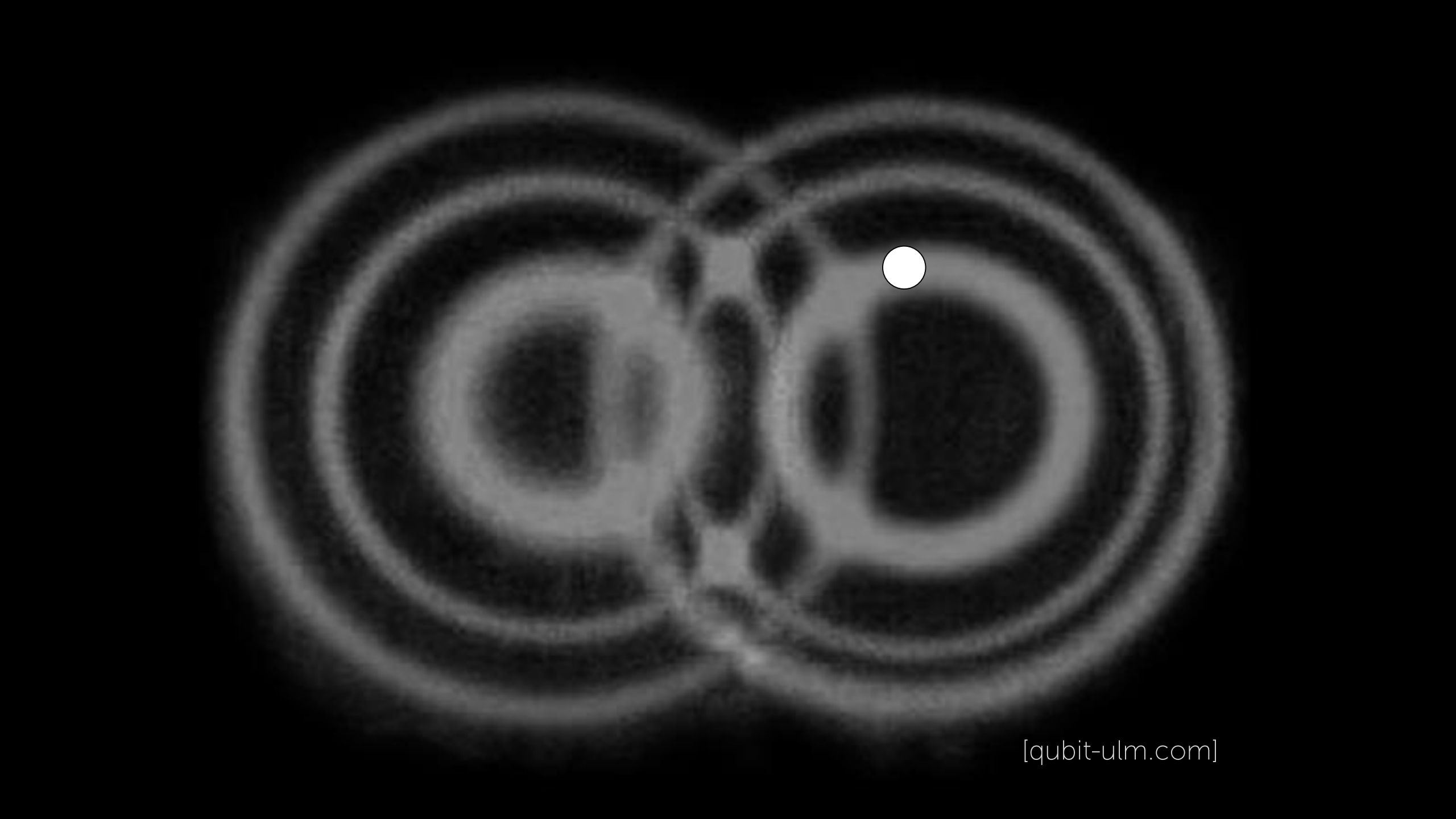


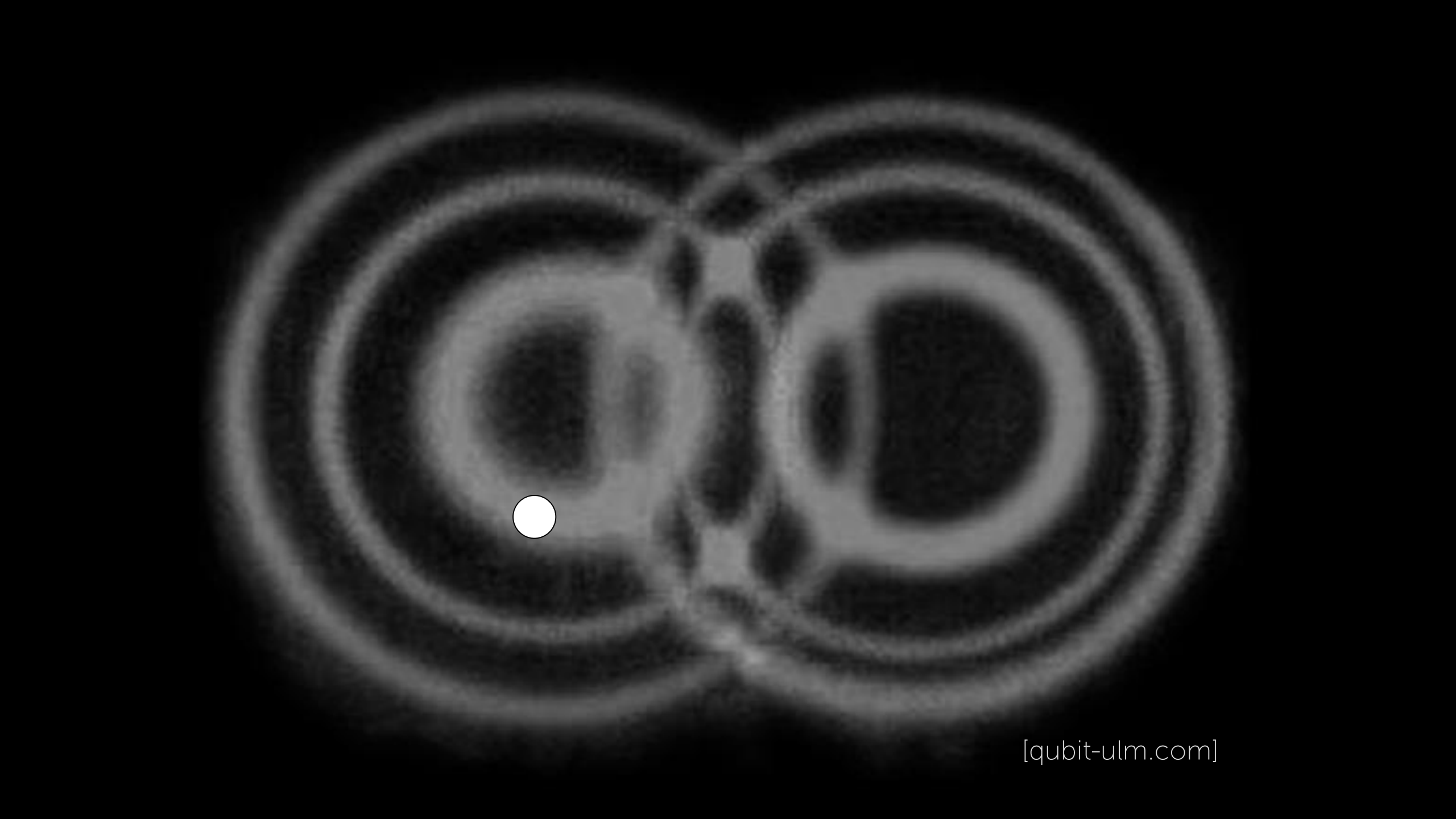
superpozícia N qubitov

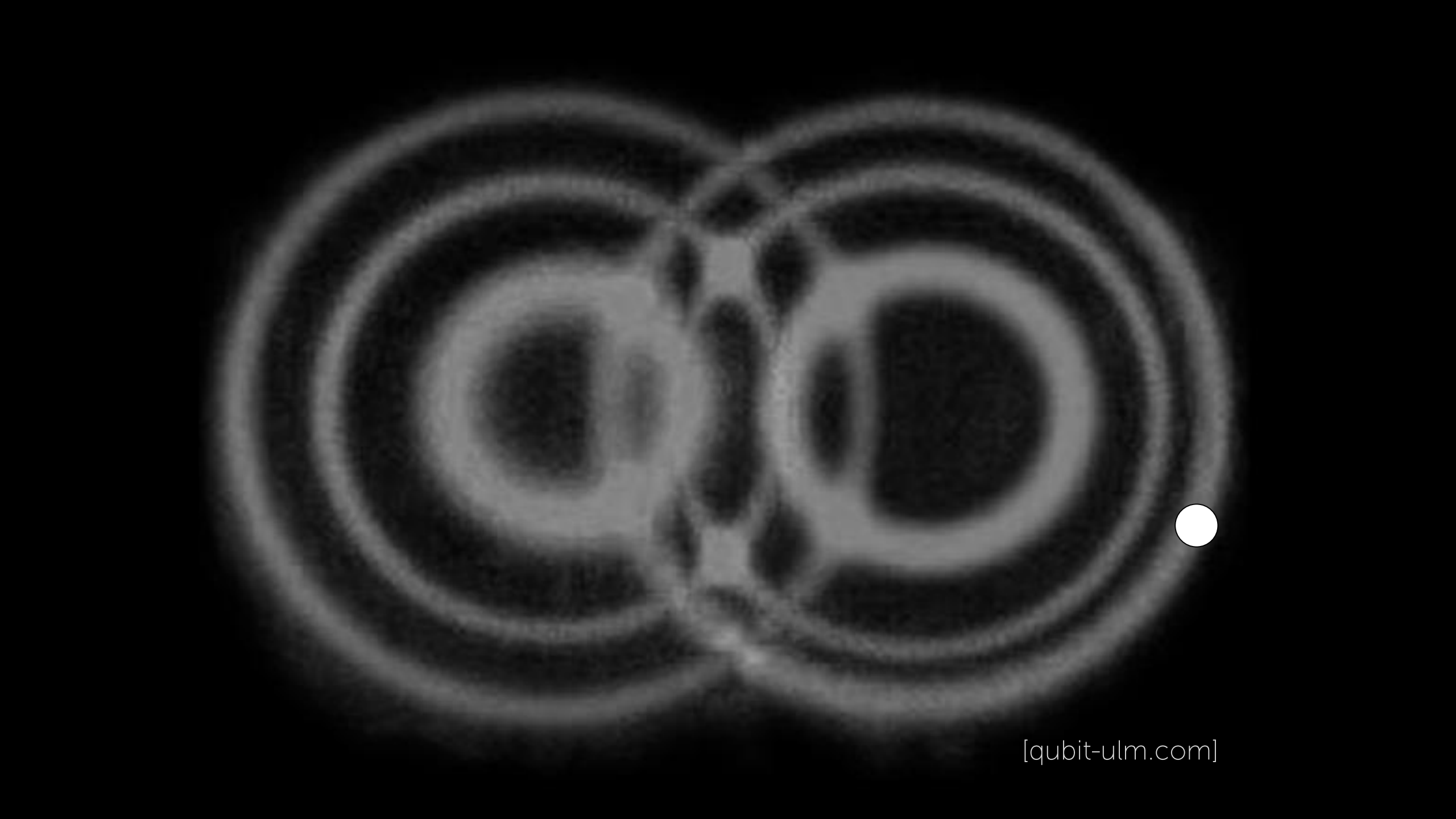


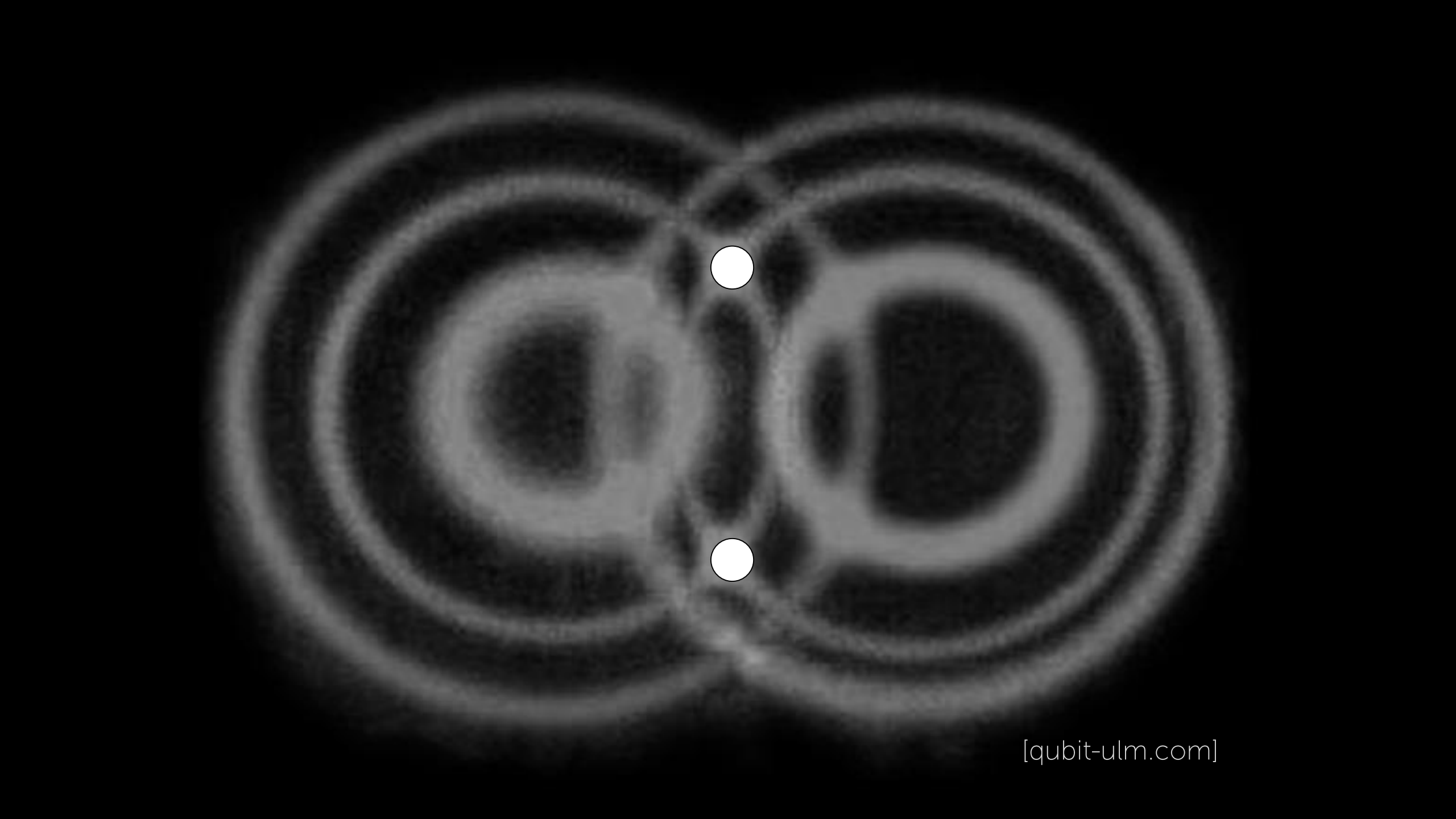

[qubit-ulm.com]

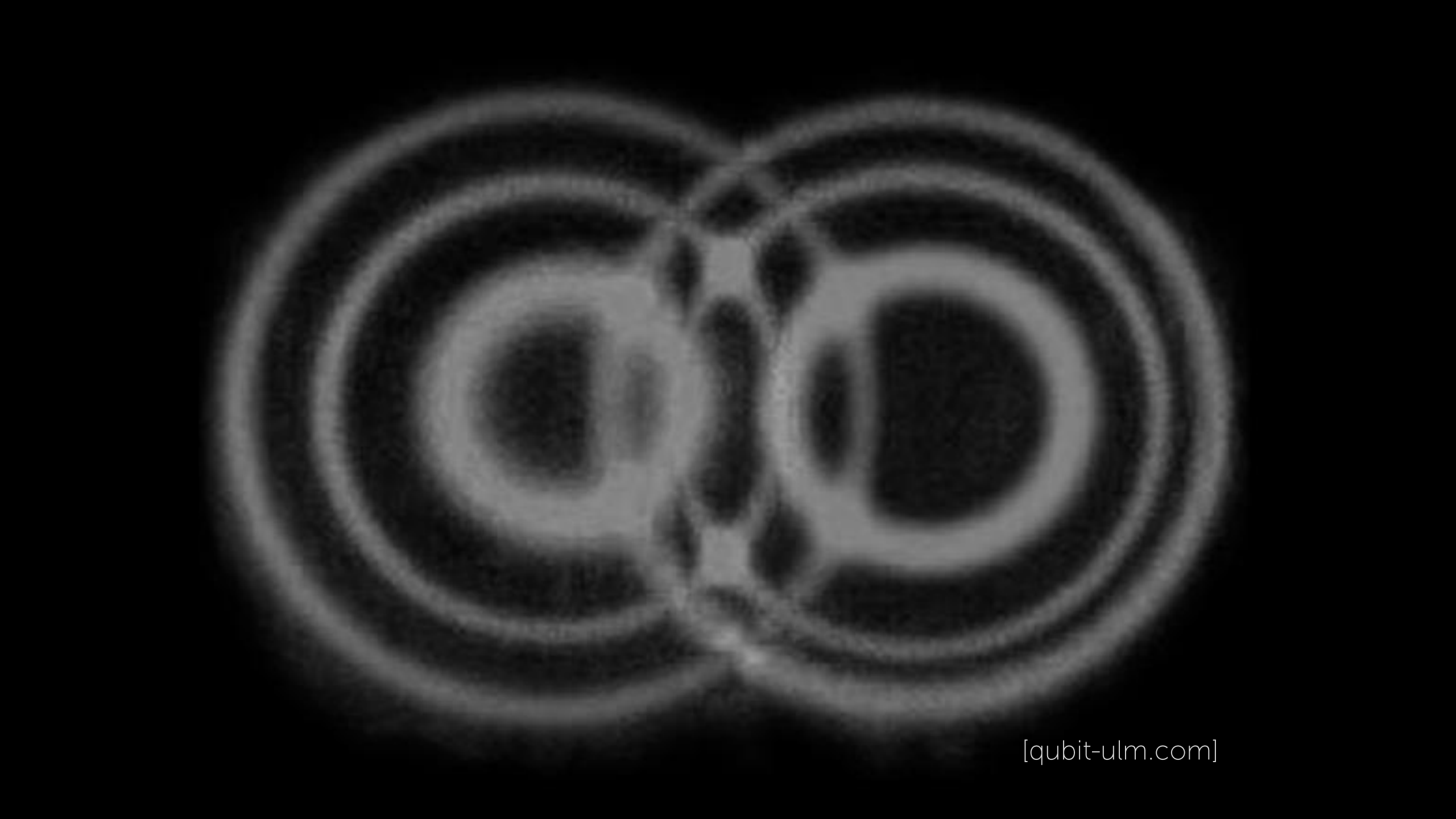

[qubit-ulm.com]

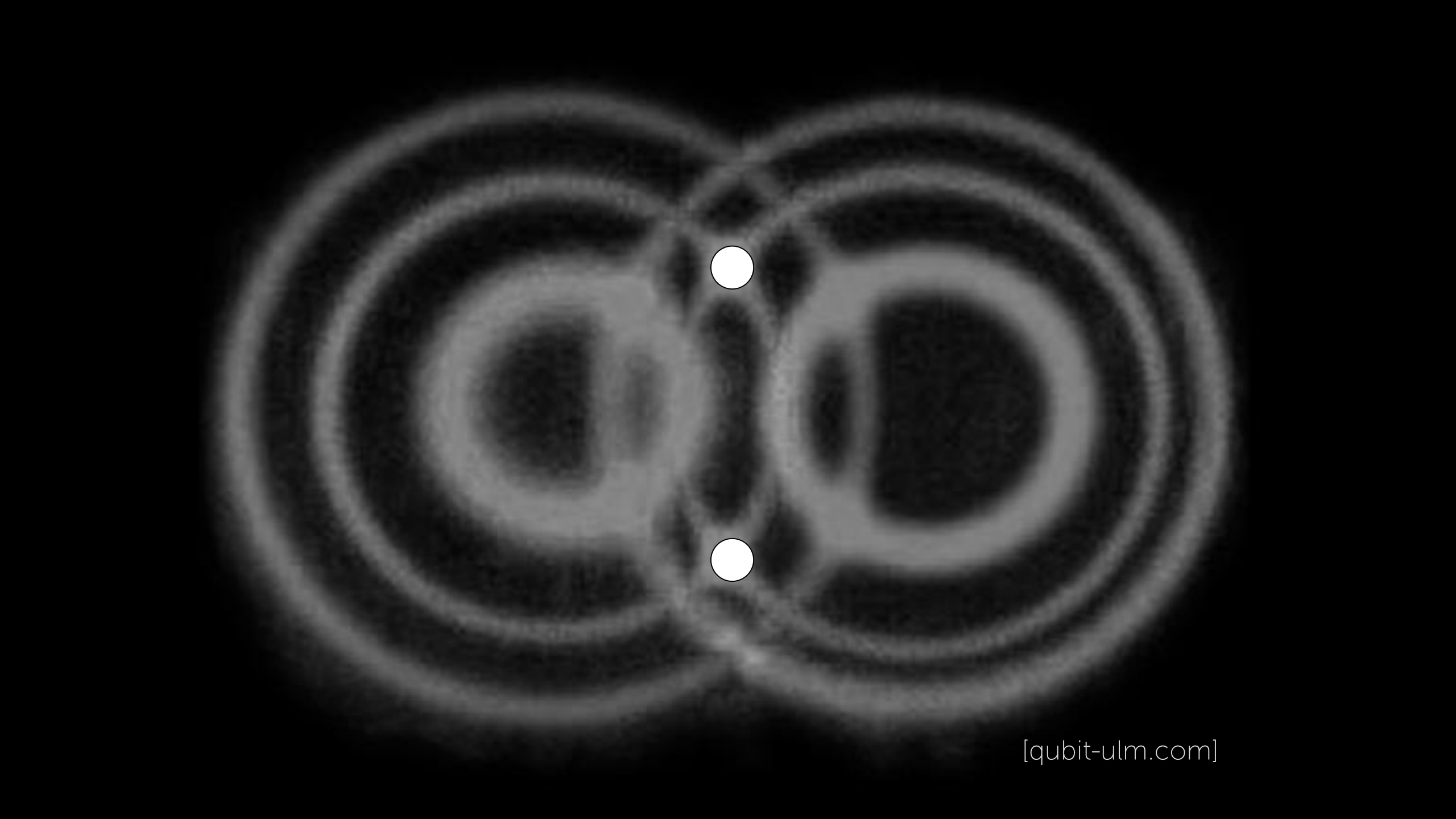

[qubit-ulm.com]

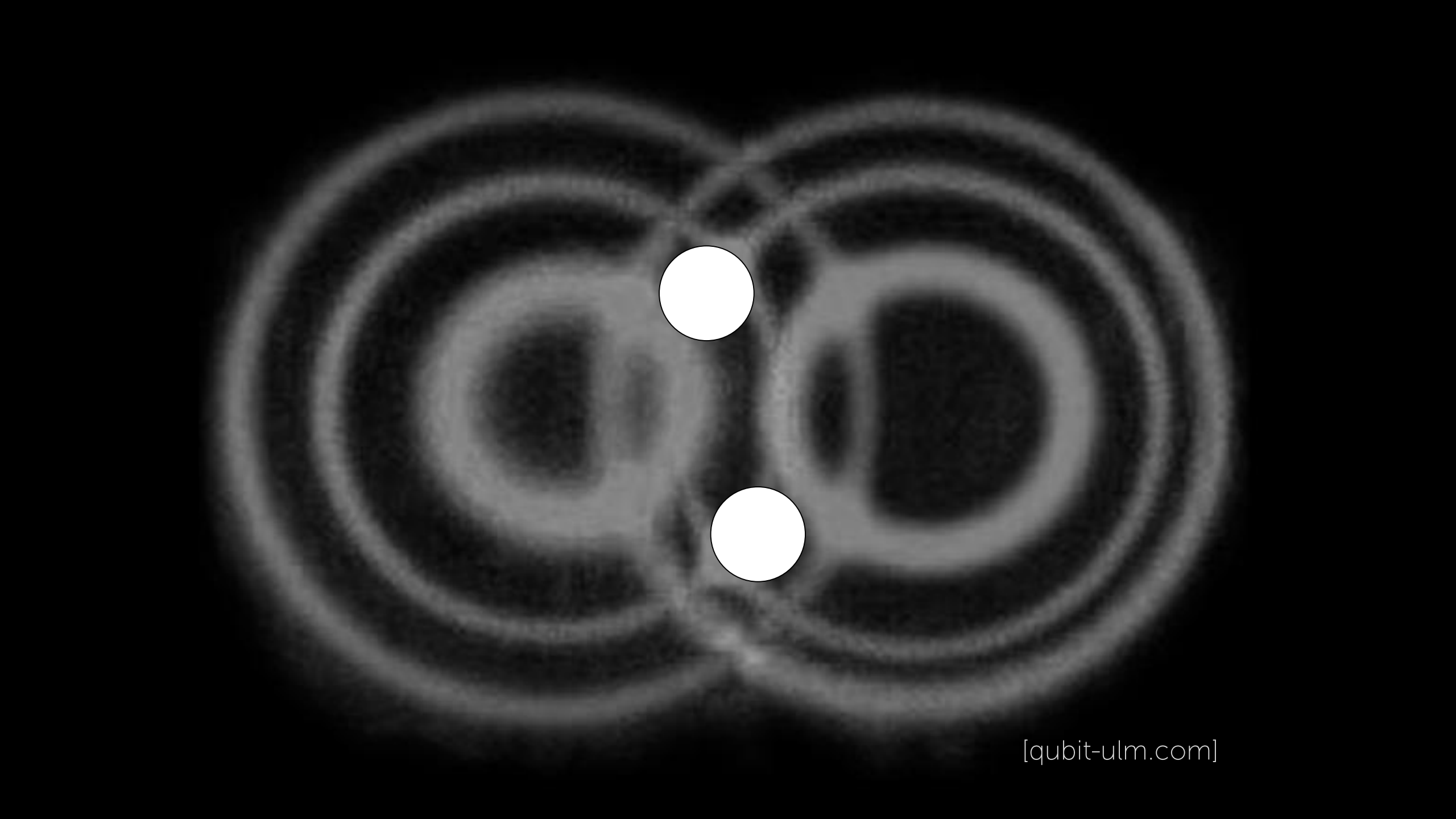

[qubit-ulm.com]

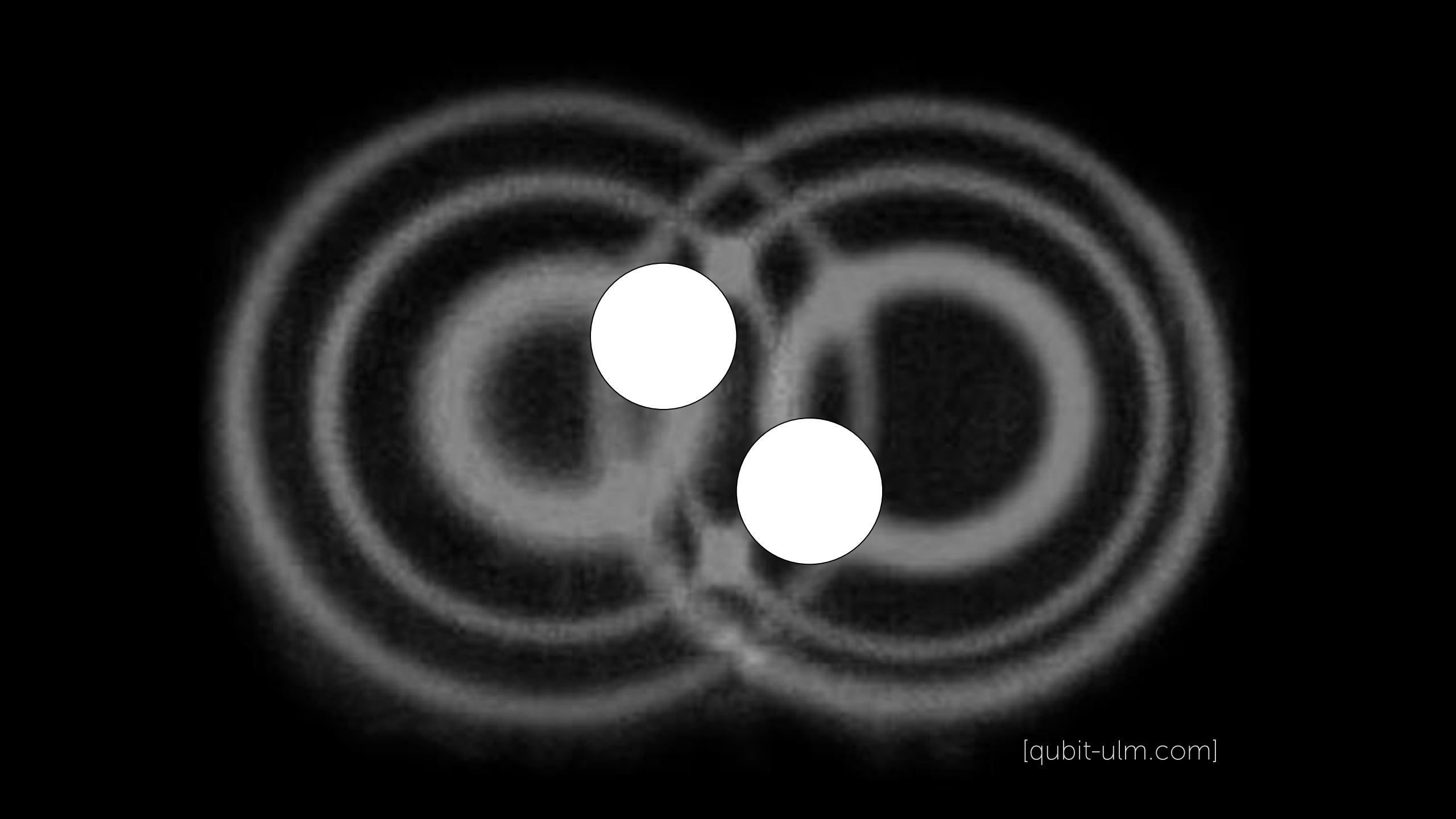

[qubit-ulm.com]

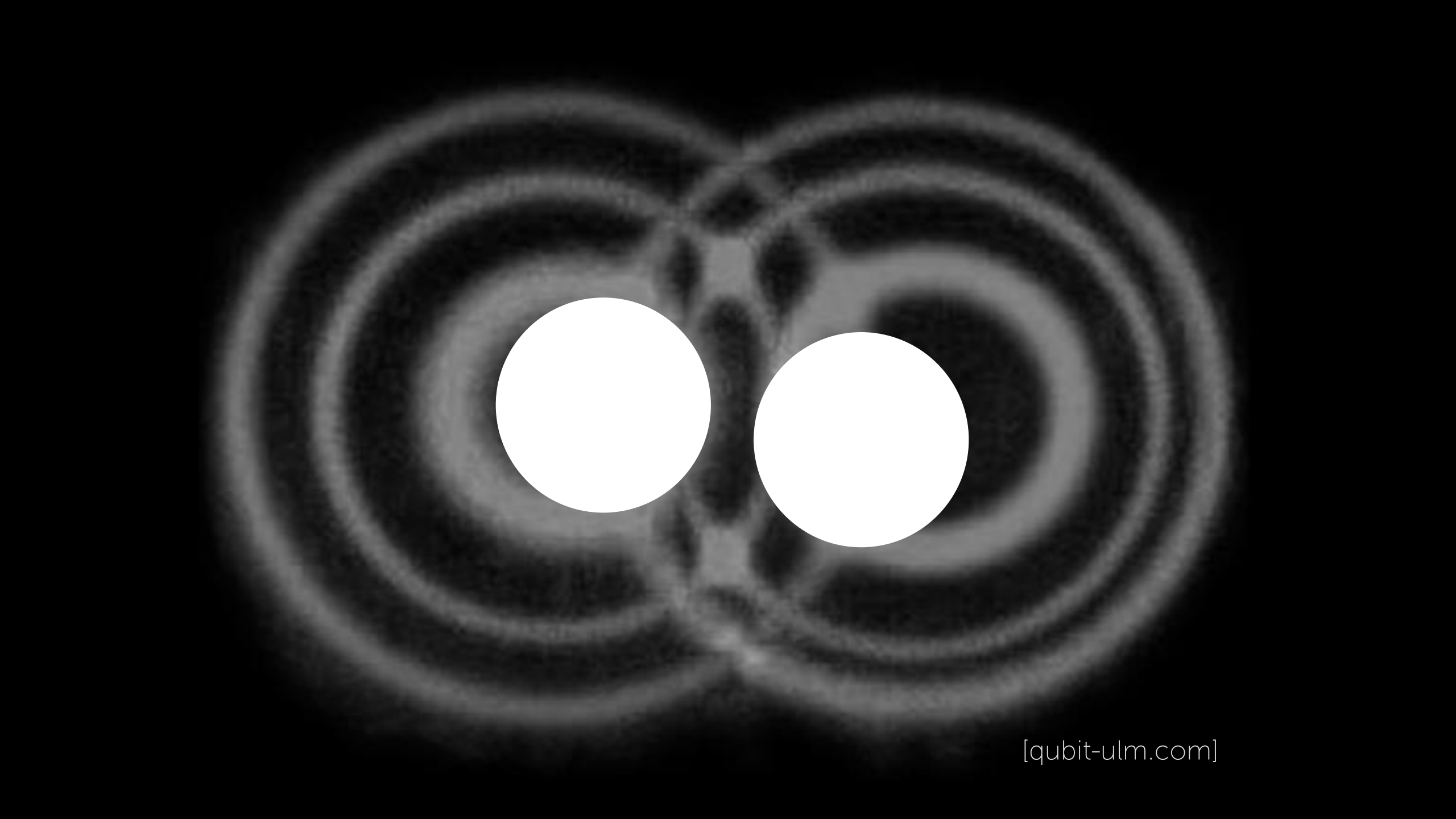

[qubit-ulm.com]

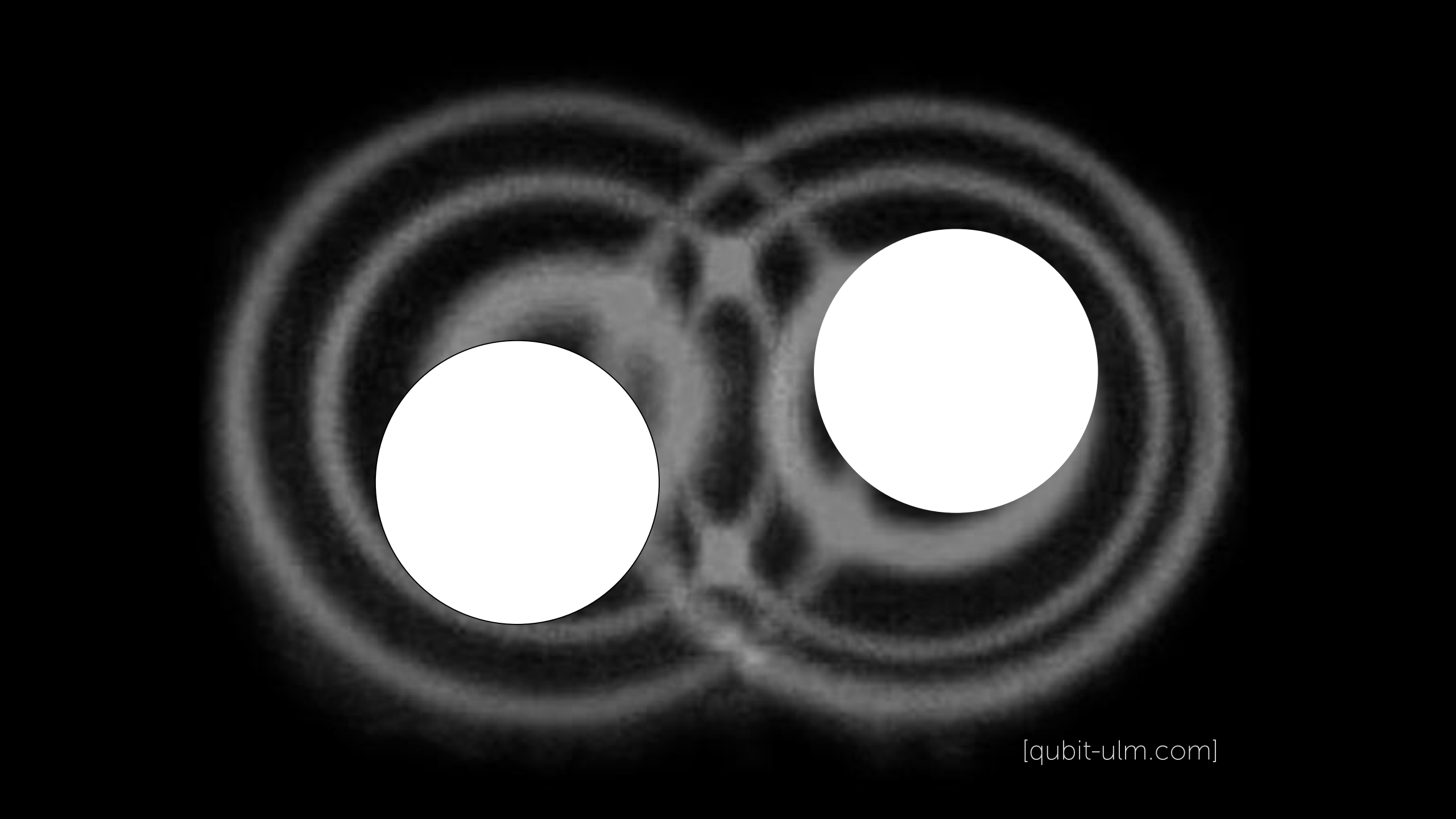

[qubit-ulm.com]

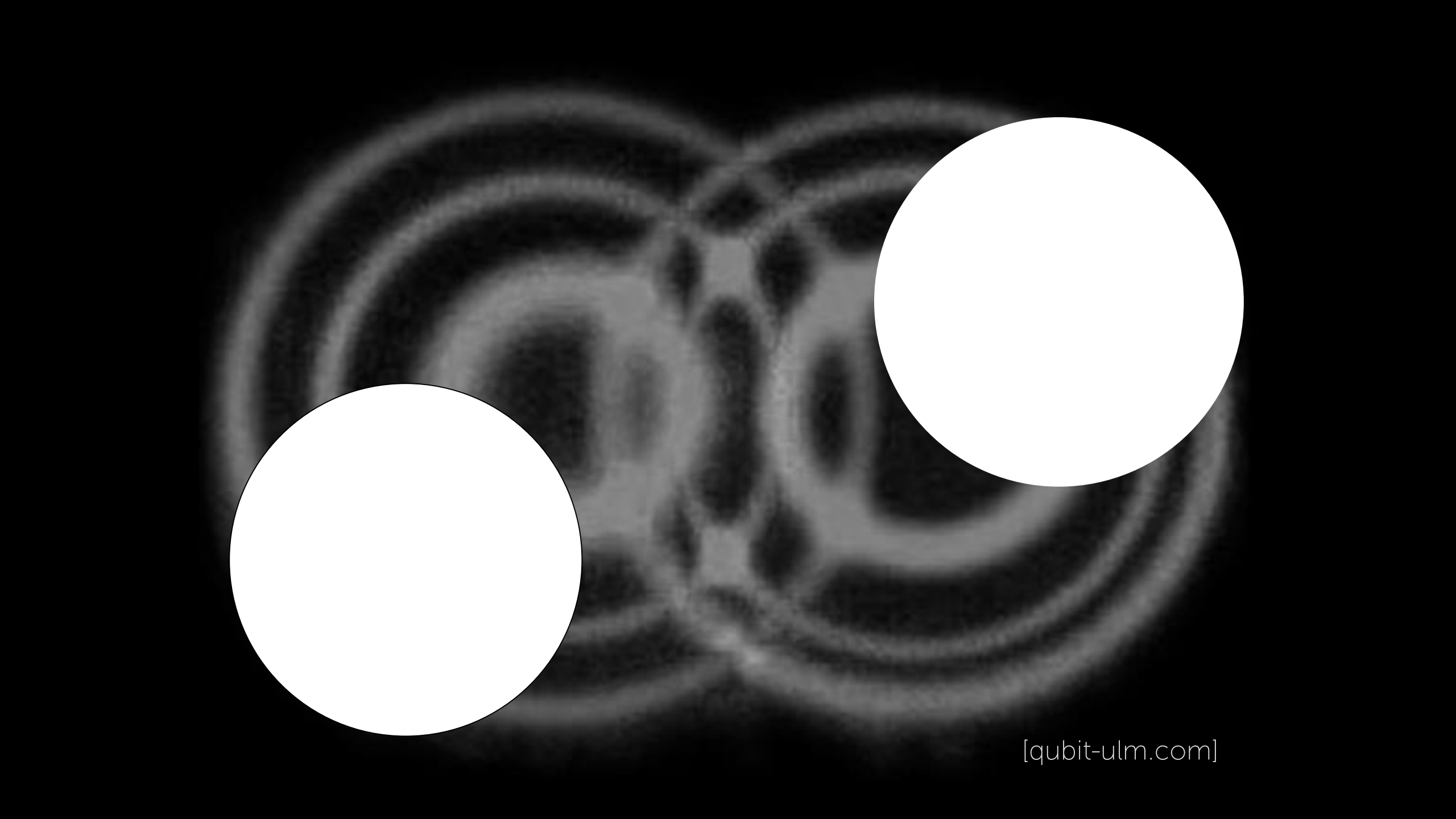

[qubit-ulm.com]

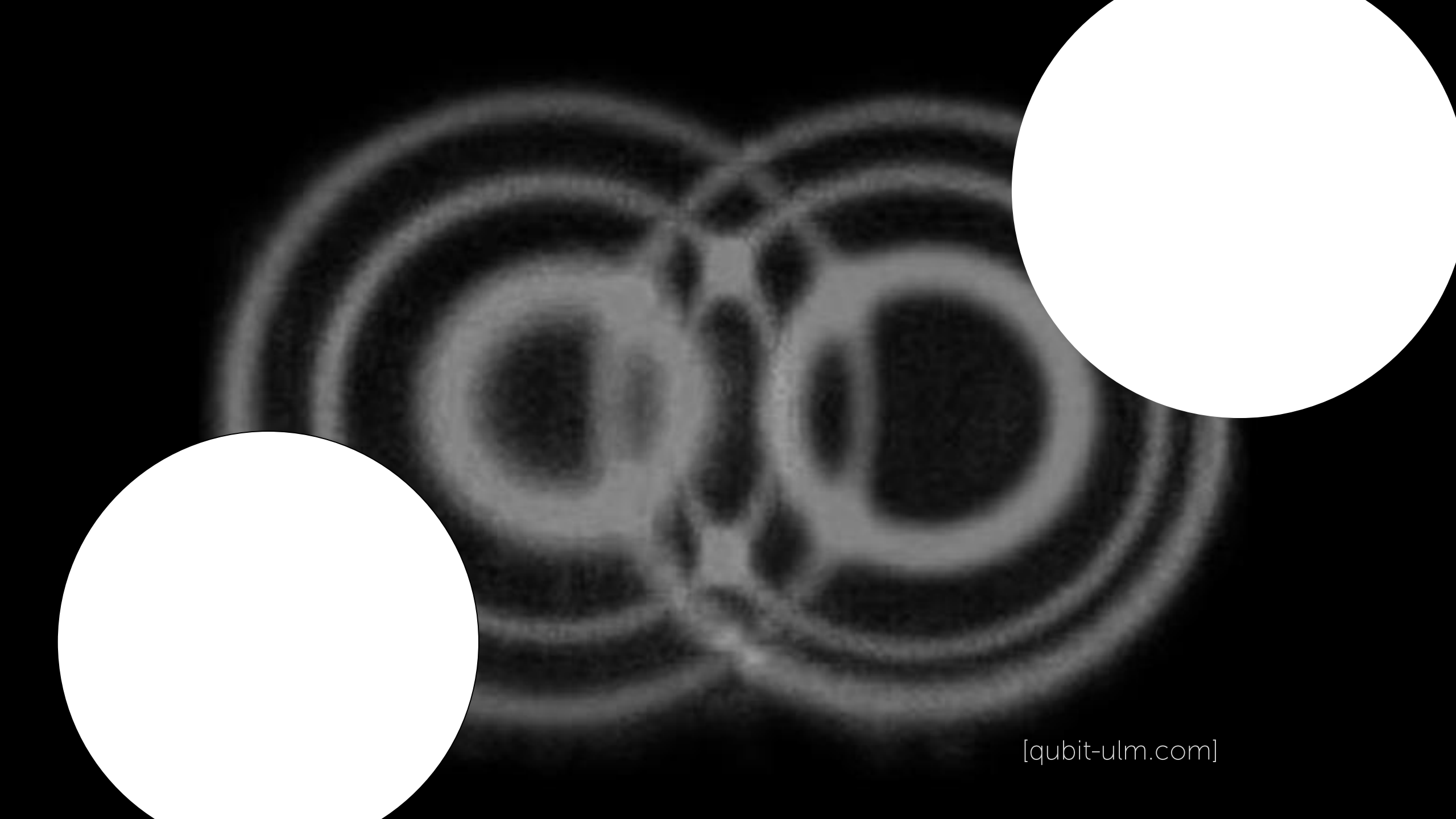

[qubit-ulm.com]

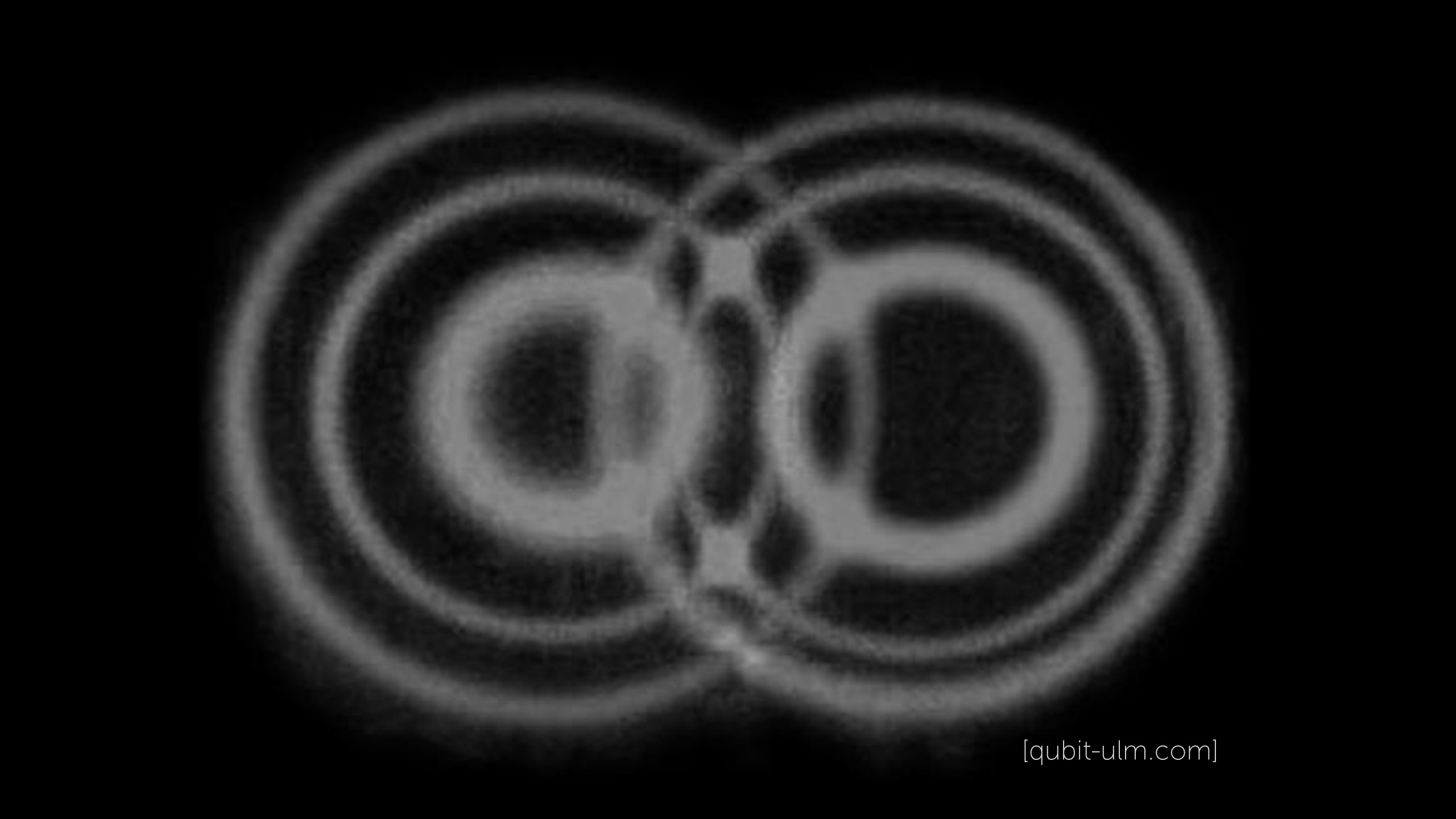

[qubit-ulm.com]


[qubit-ulm.com]


[qubit-ulm.com]


[qubit-ulm.com]

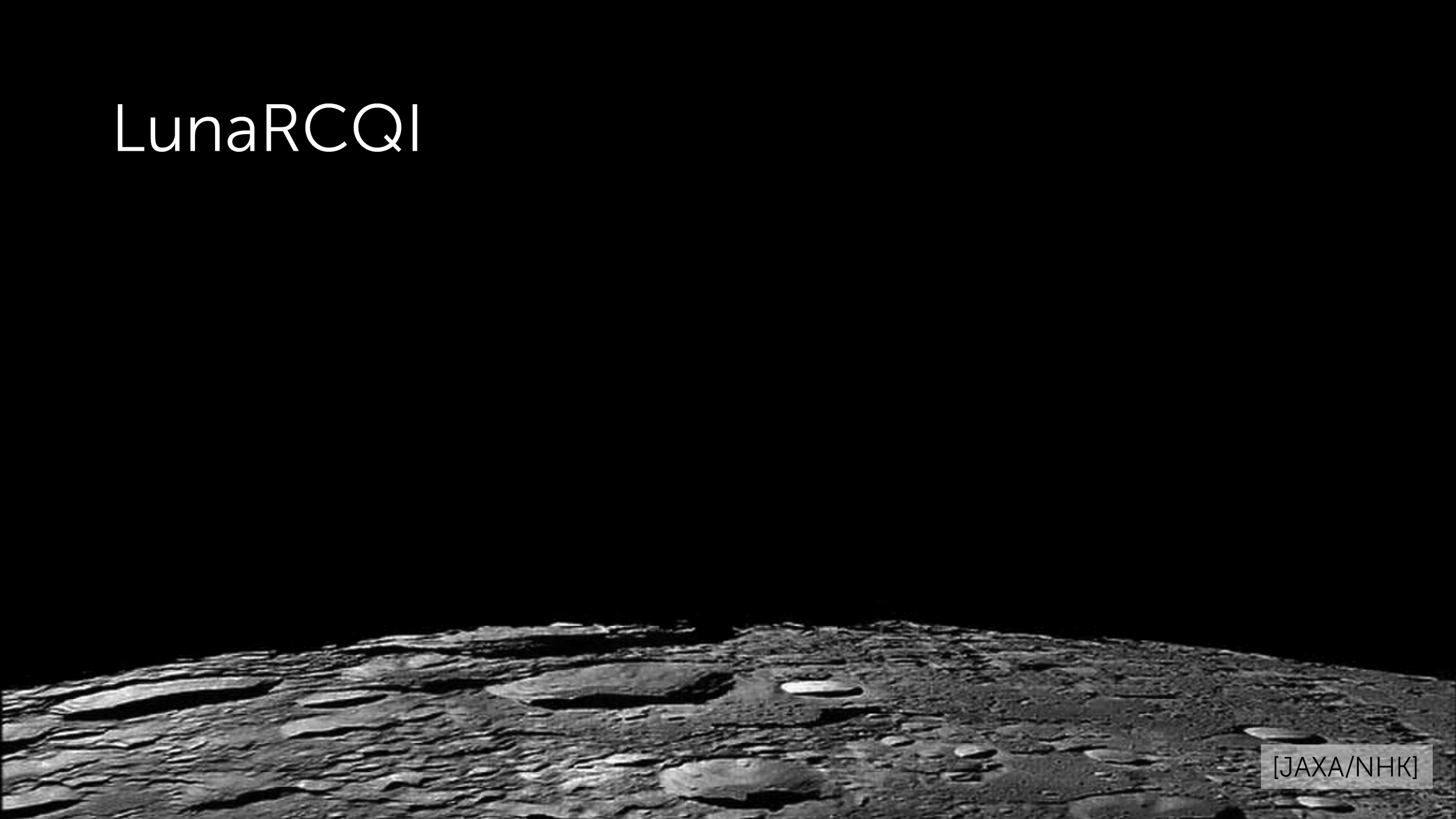

[qubit-ulm.com]


[qubit-ulm.com]

fundamental
fysiks group,
[City magazine]

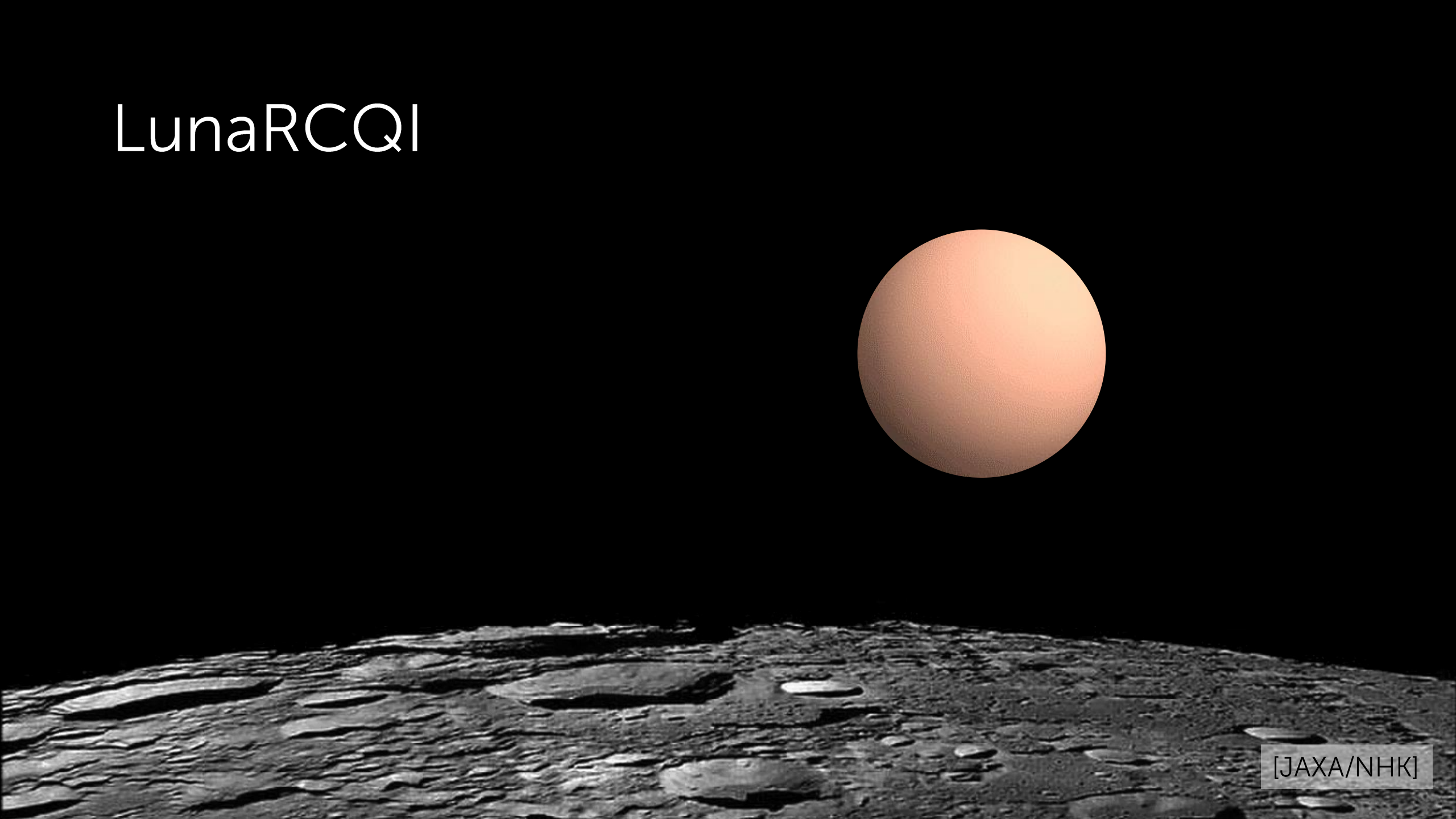
kvantová TELEPORTÁCIA

LunaRCQI



[JAXA/NHK]

LunaRCQI

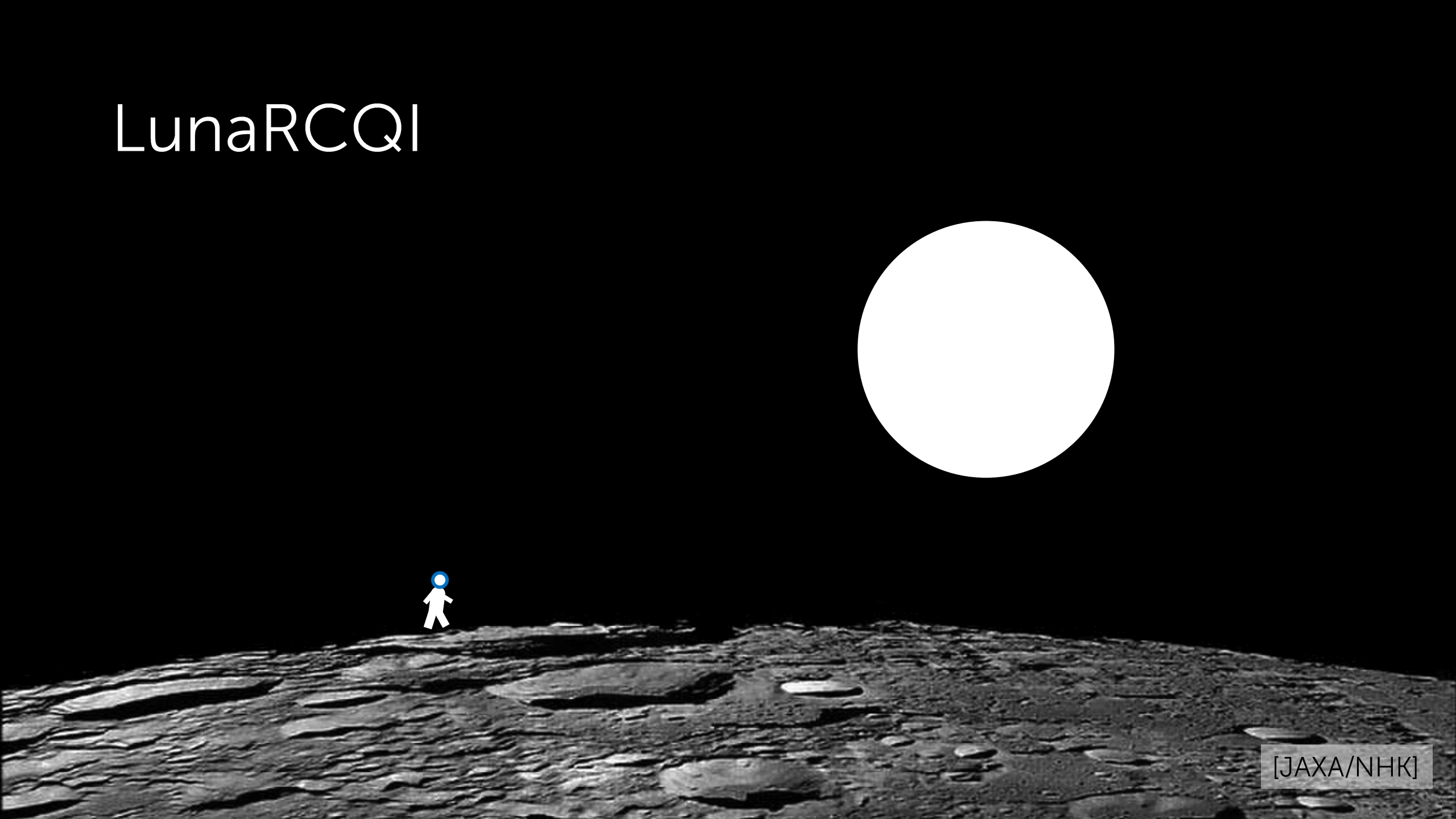


[JAXA/NHK]

LunaRCQI

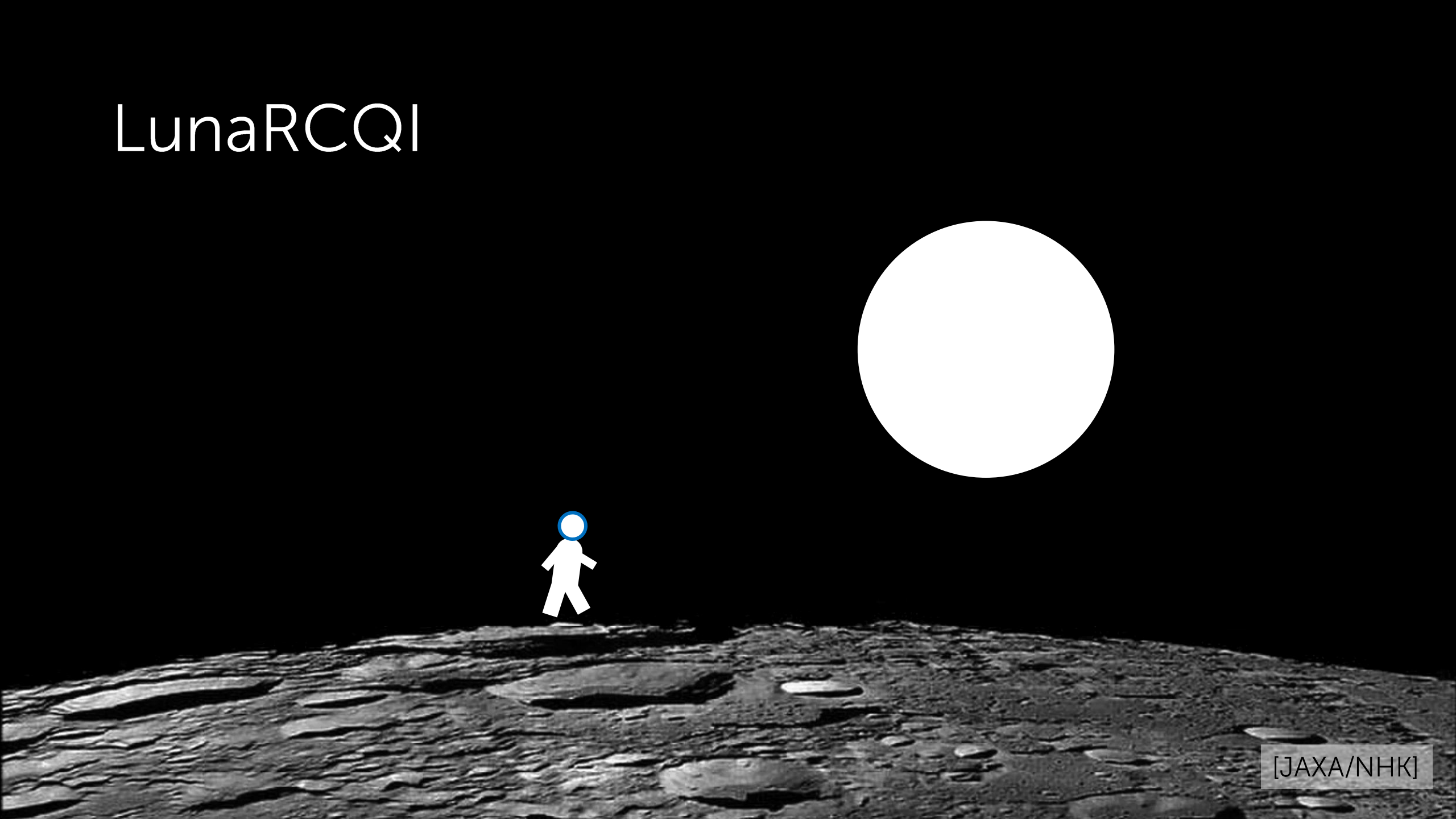
[JAXA/NHK]

LunaRCQI



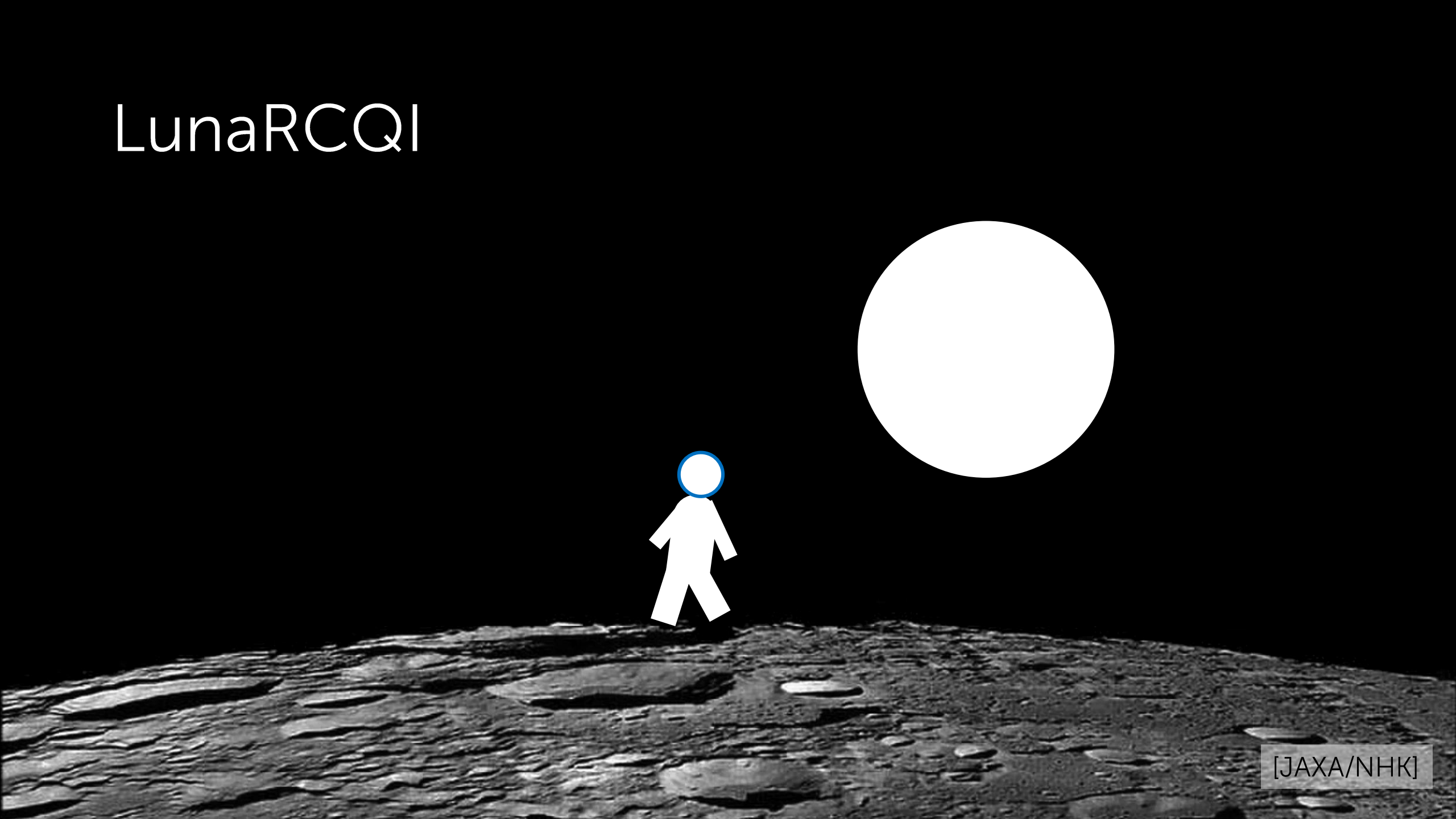
[JAXA/NHK]

LunaRCQI



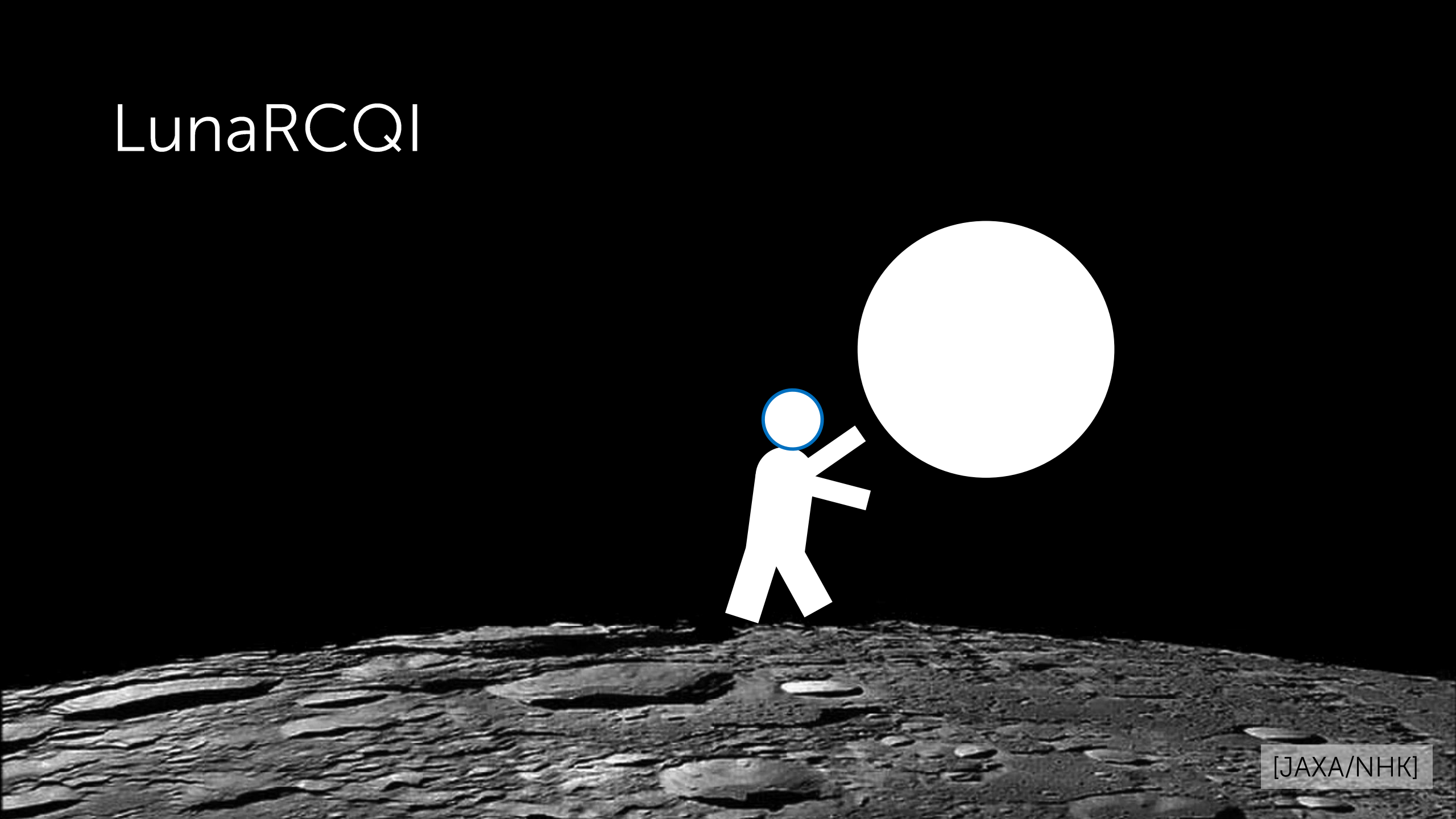
[JAXA/NHK]

LunaRCQI



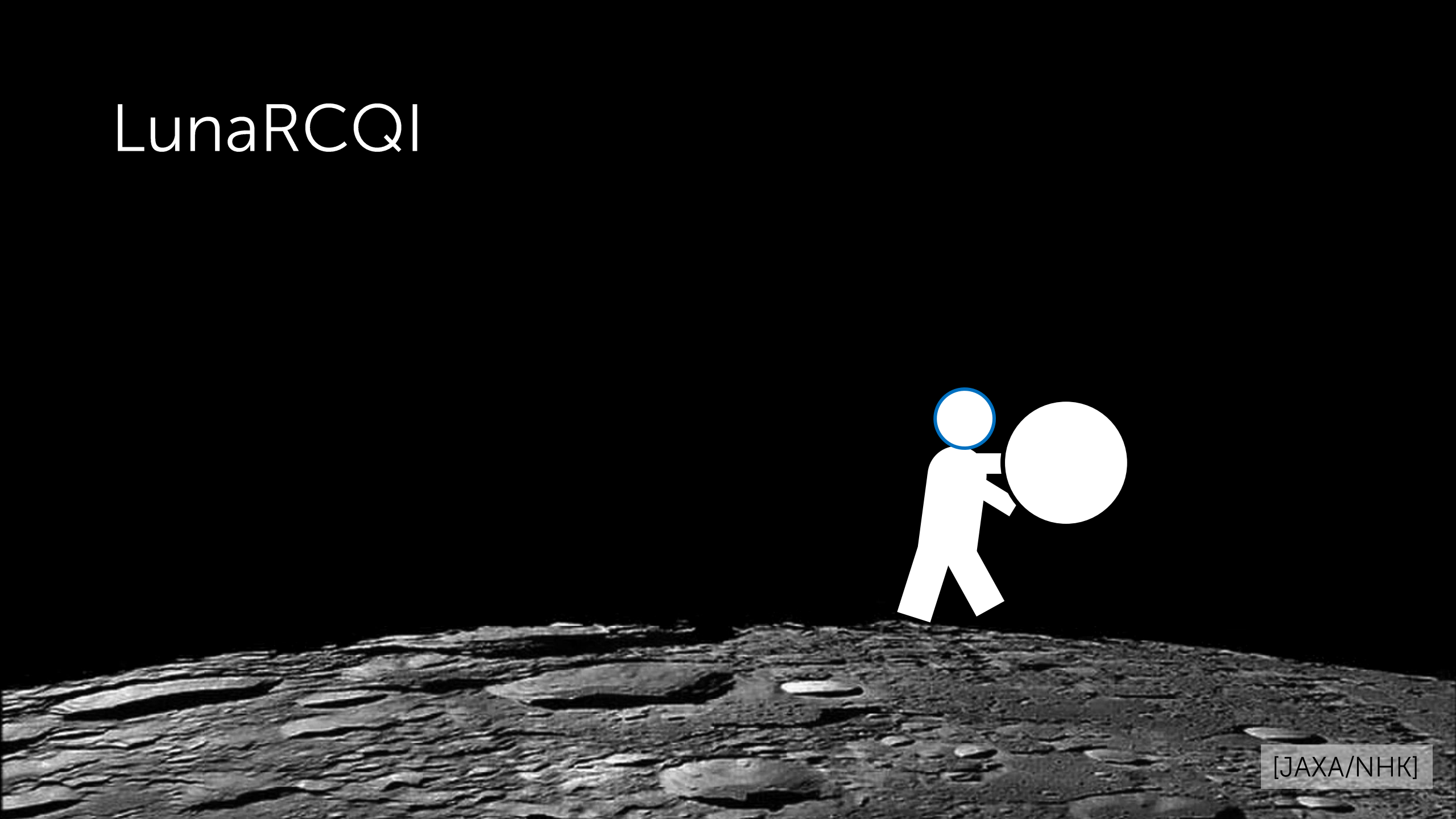
[JAXA/NHK]

LunaRCQI

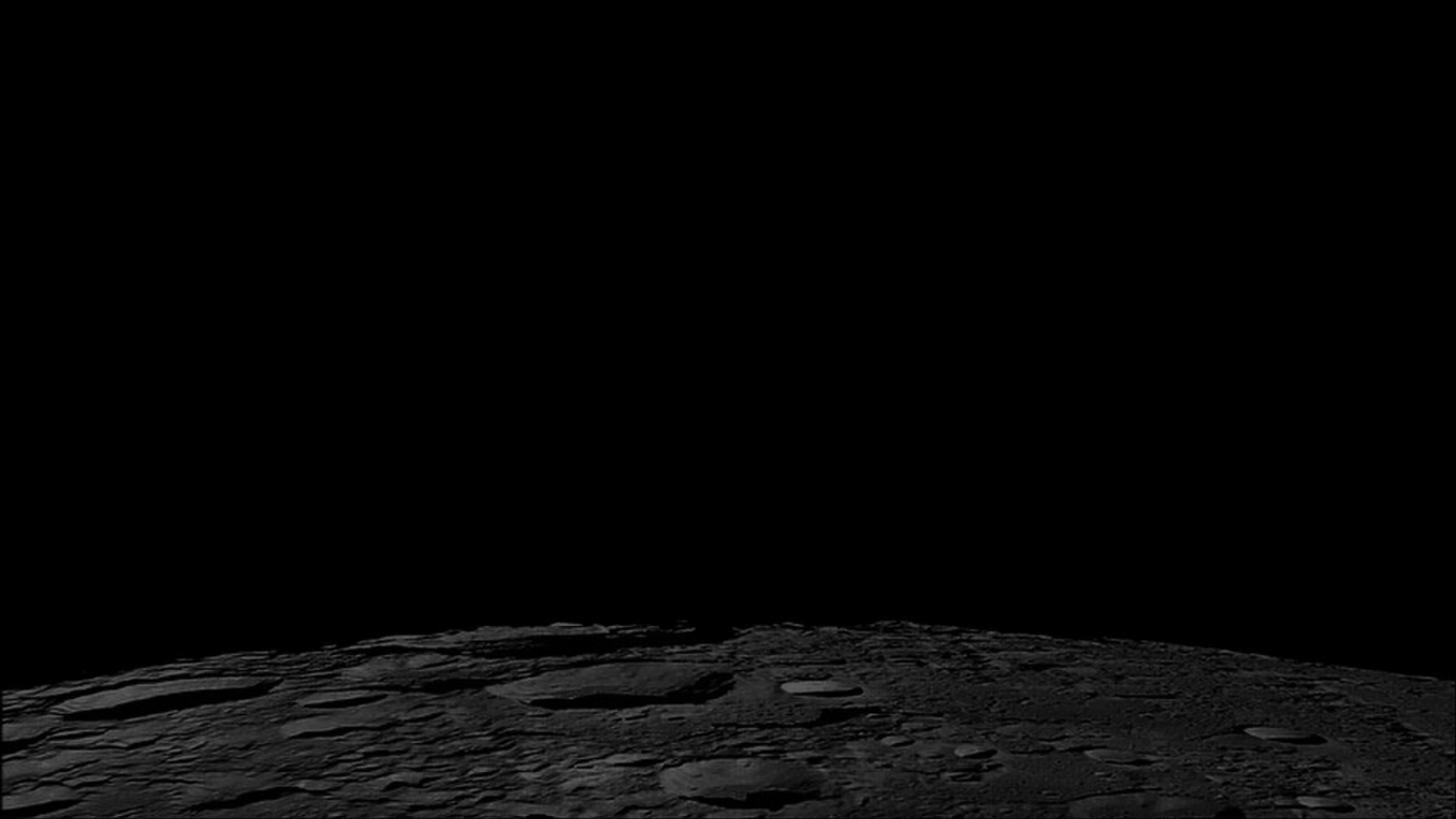


[JAXA/NHK]

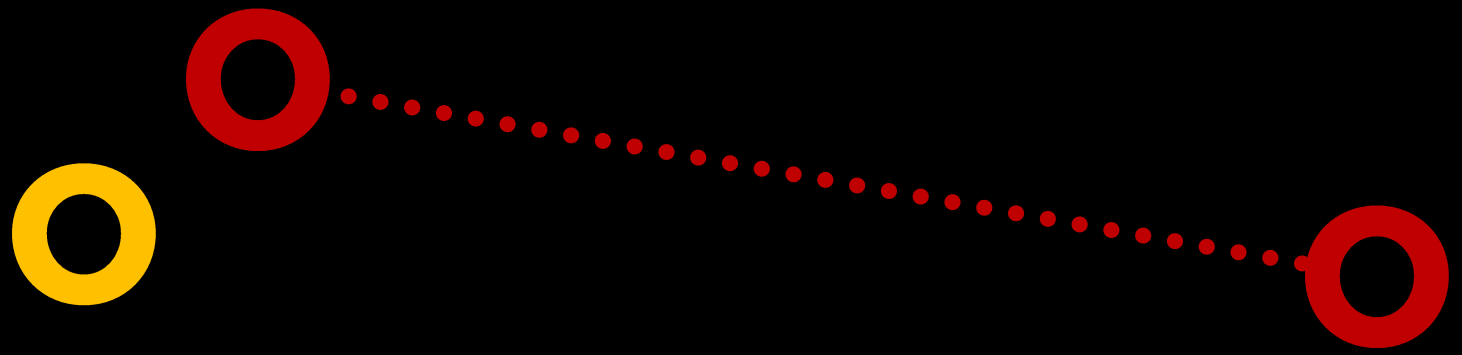
LunaRCQI



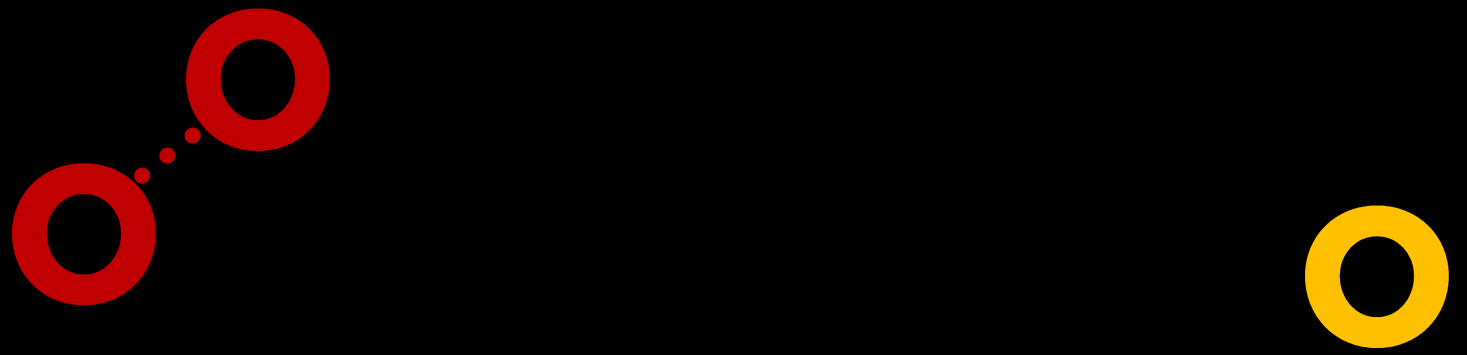
[JAXA/NHK]



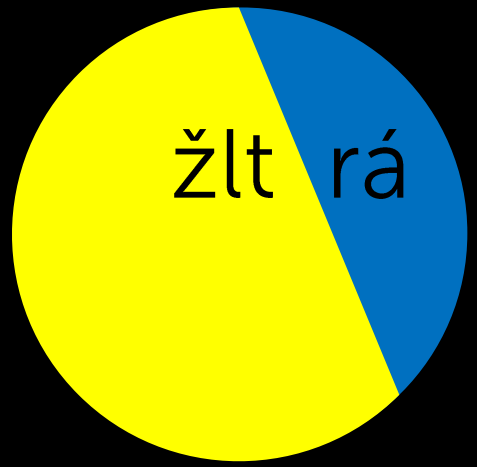
príliš fantastické?



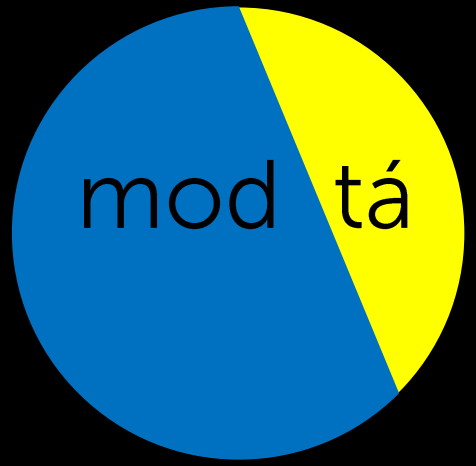
príliš fantastické?



Často na druhej strane výjde správa nejako popletená a treba ju opraviť.



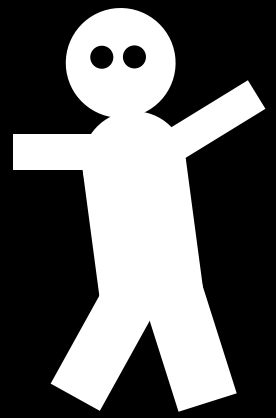
Často na druhej
strane výjde správa
nejako popletená
a treba ju opraviť.



kvantové počítanie

server

2017 = ? × ?

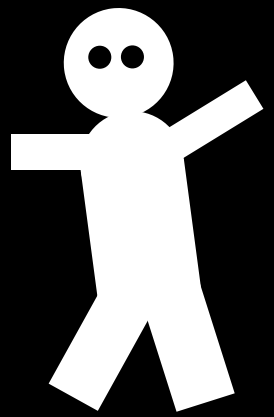


kvantové počítanie

server

2017 = ? × ?

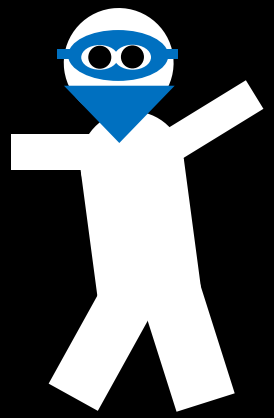
je to prvočíslo



slepé kvantové počítanie

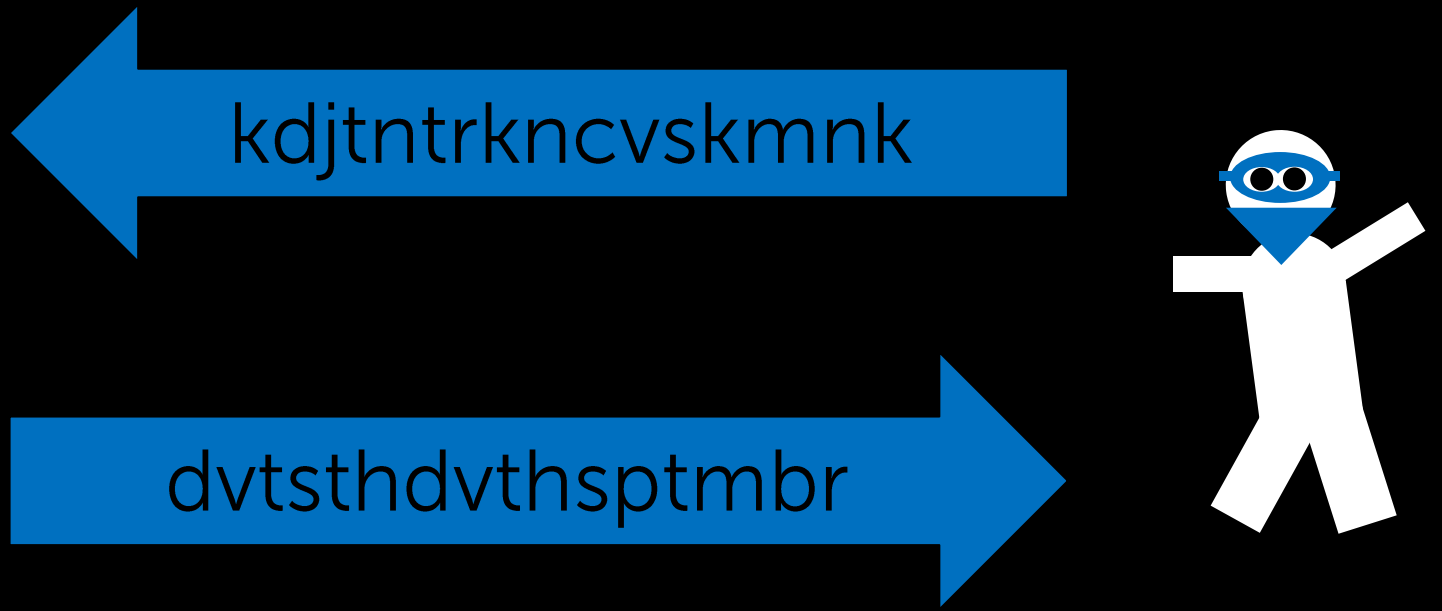
server

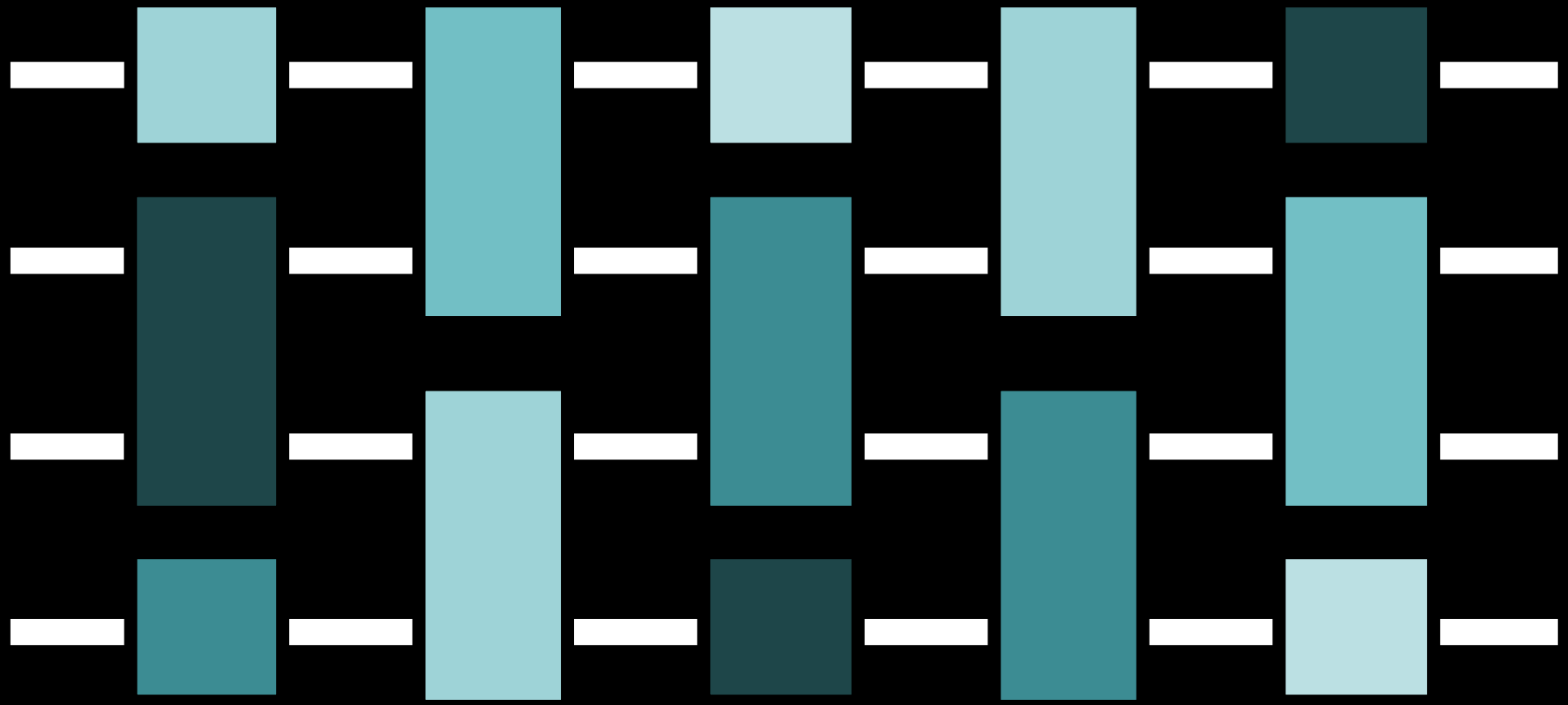
kdjtntrkncvskmnk



slepé kvantové počítanie

server





počítame kvantovo

simulácia

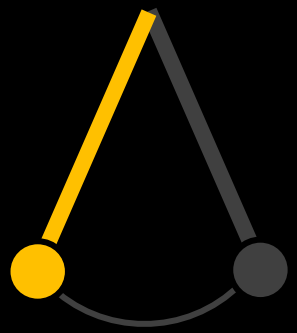
zdroj

Daniel Nagaj
je fascinovaný
hlavolamami.

preklad

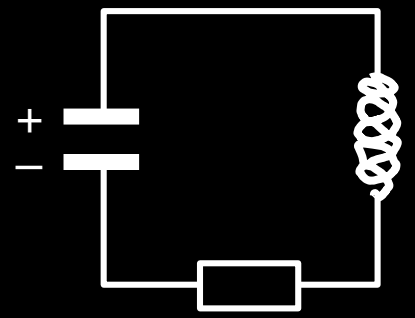
Daniel Nagaj
is fascinated
by puzzles.

reálna fyzika



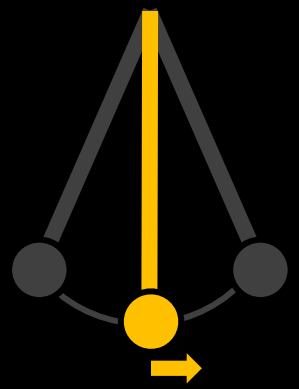
m, l, g

simulácia



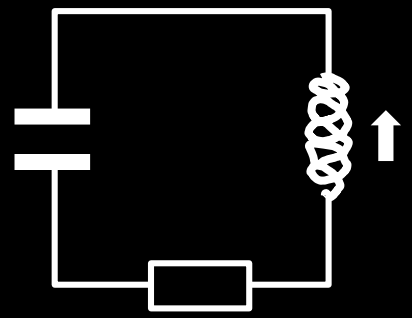
R, L, C

reálna fyzika



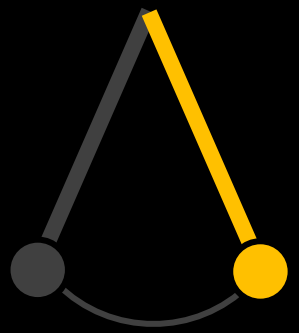
m, l, g

simulácia



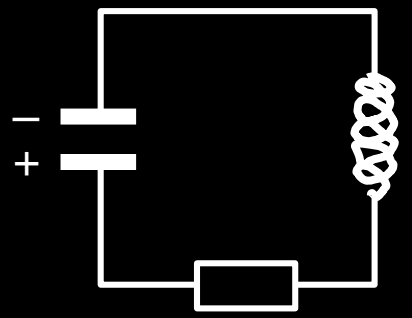
R, L, C

reálna fyzika



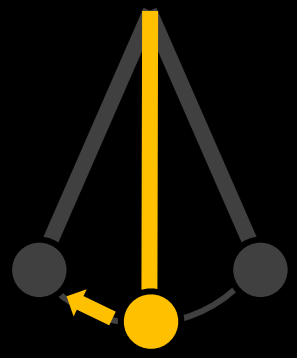
m, l, g

simulácia



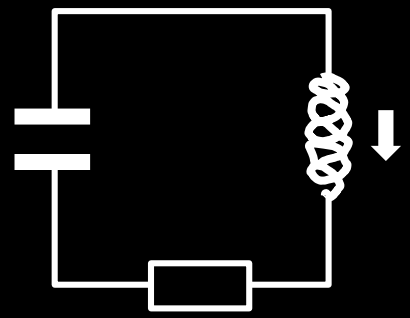
R, L, C

reálna fyzika



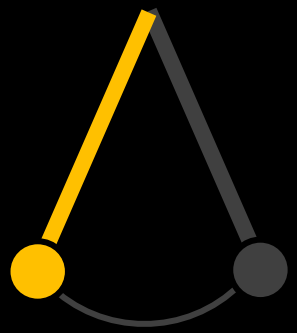
m, l, g

simulácia



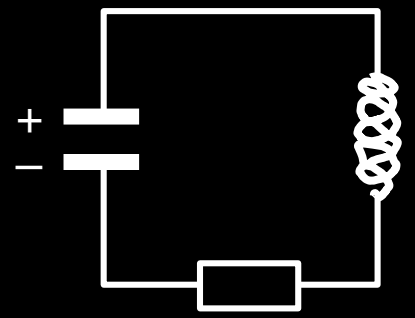
R, L, C

reálna fyzika



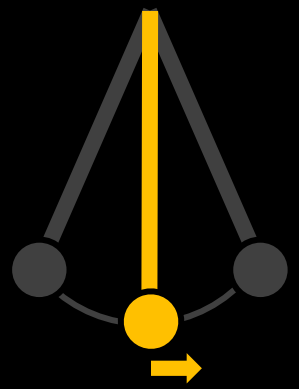
m, l, g

simulácia



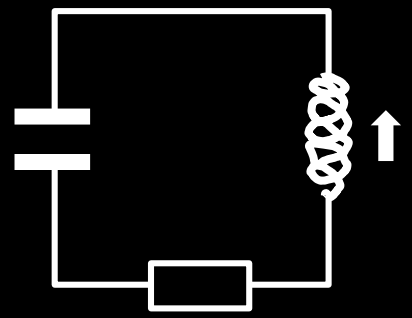
R, L, C

reálna fyzika



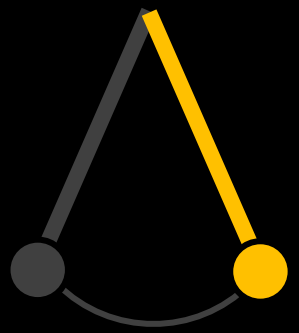
m, l, g

simulácia



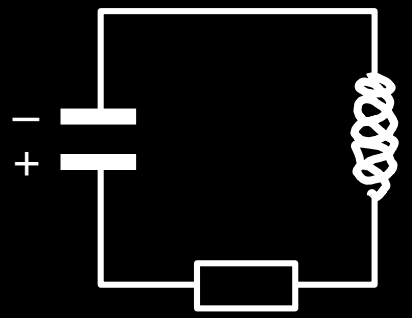
R, L, C

reálna fyzika



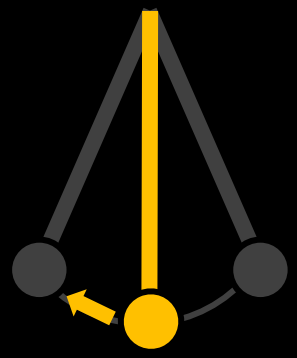
m, l, g

simulácia



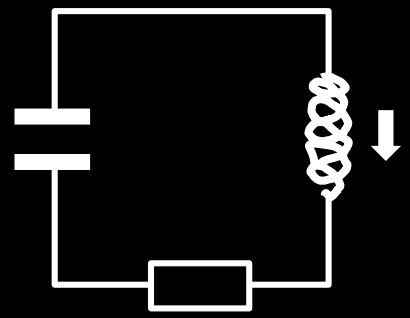
R, L, C

reálna fyzika



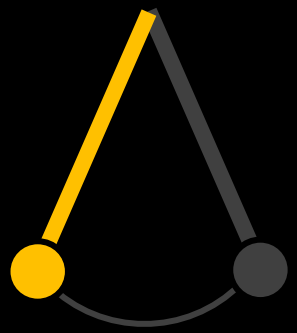
m, l, g

simulácia



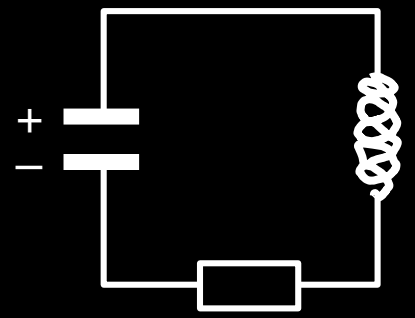
R, L, C

reálna fyzika



m, l, g

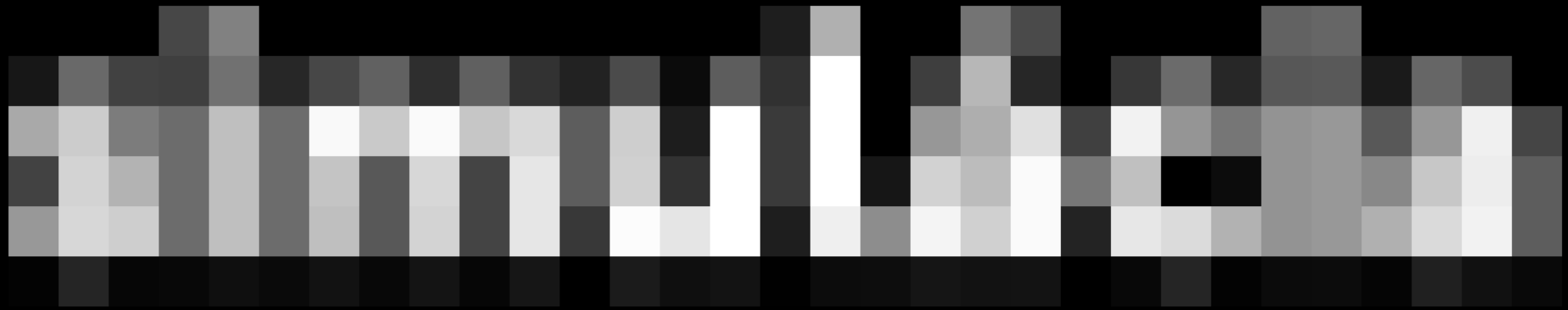
simulácia

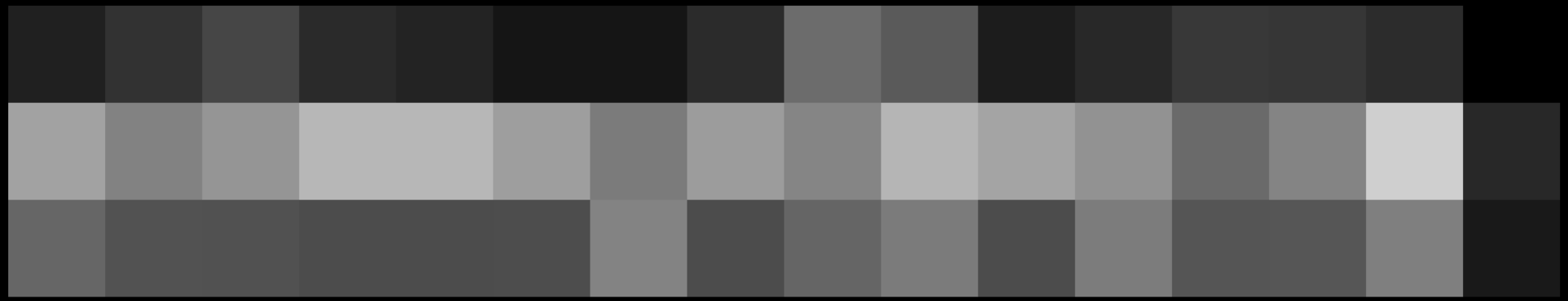


R, L, C

simulácia


simulácia





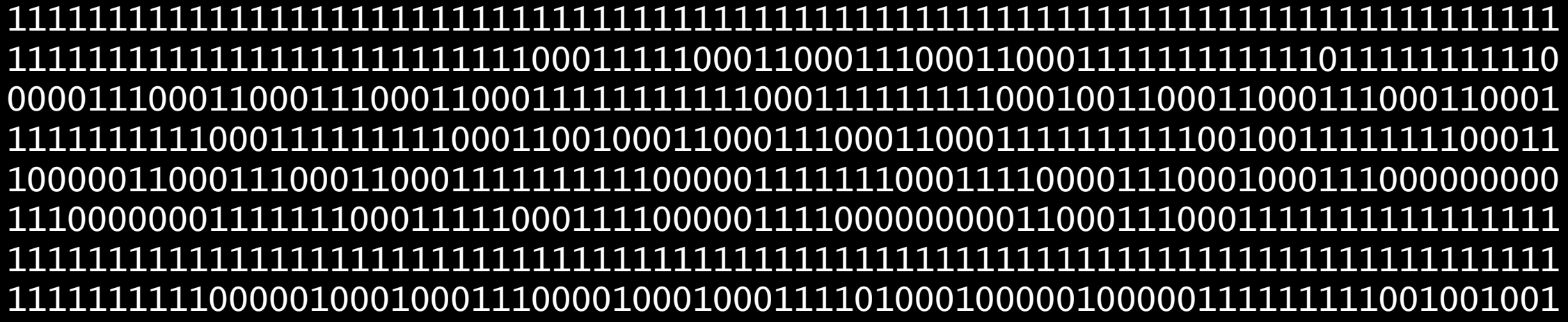
^{87}Rb

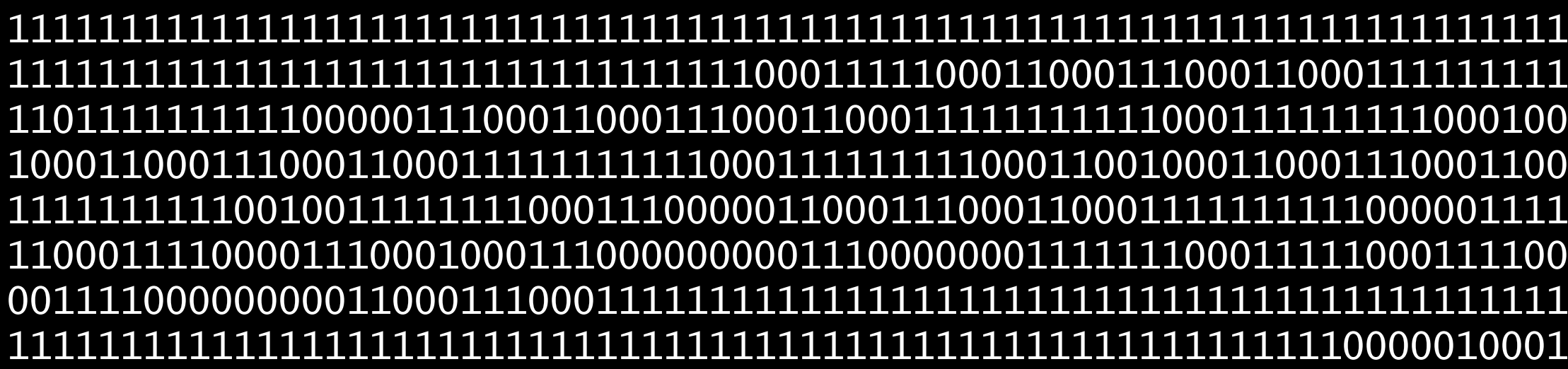
[Endres et al., Science 354, 2016]

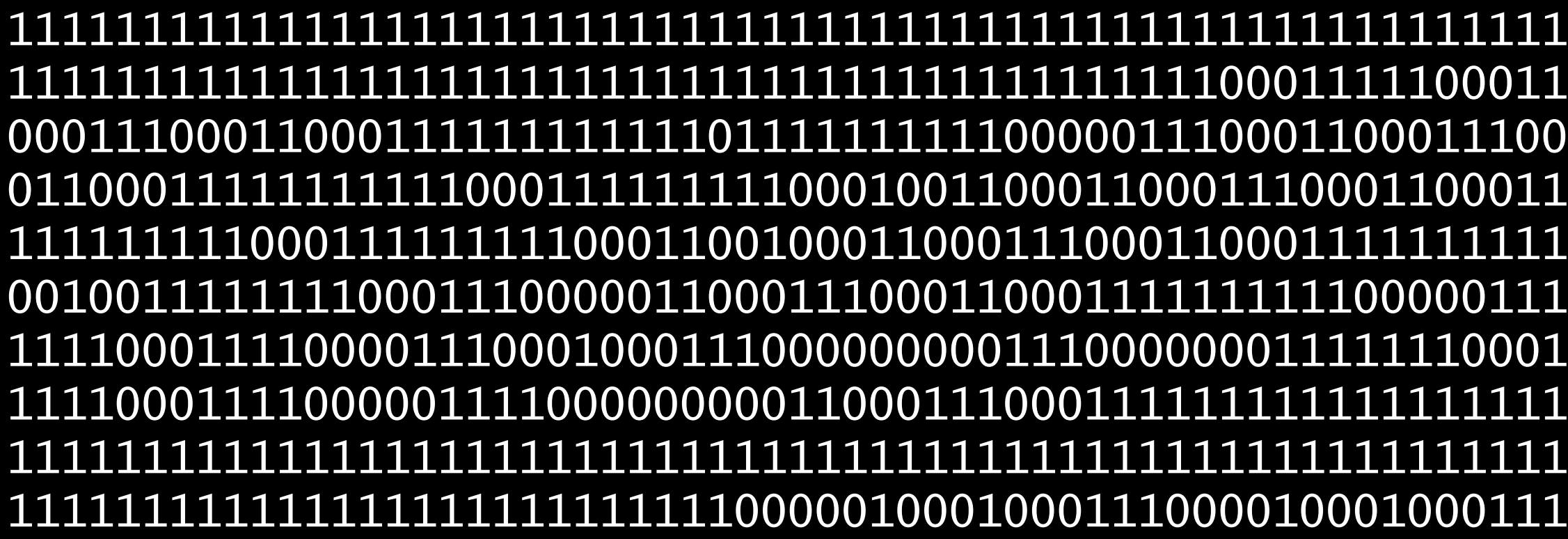
ihla v kope sena ihla v kope sena ihla
v kope sena ihla v kope sena ihla v ko
pe sena ihla v kope sena ihla v kope s
ena ihla v kope sena ihla v kope sena
i hla v kope sena ihla v kope sena ihla
v kope sena ihla v kope sena ihla v ko
pe sena ihla v kope sena ihla v kope s

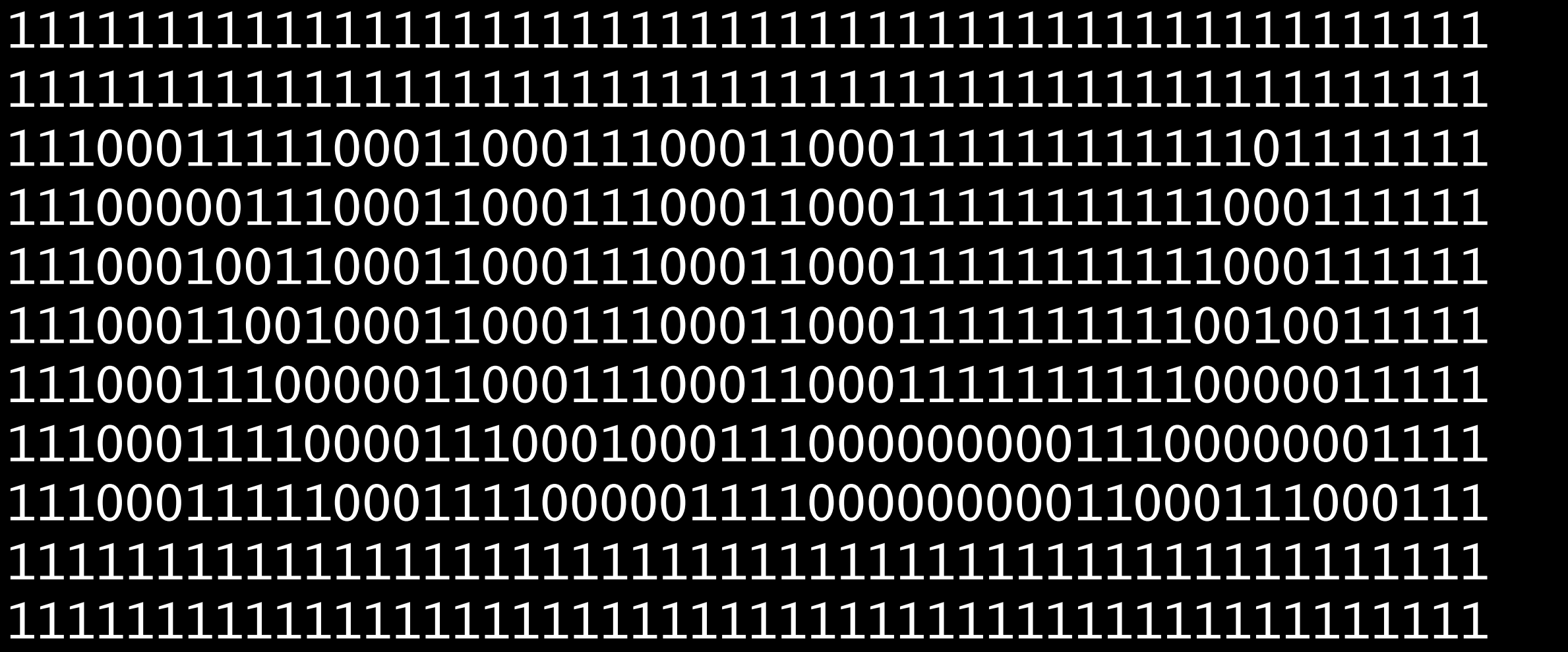
ihla v kope sena ihla v kope sena ihla v kope sena ihla v kope sena ihla v ko pe sena ihla v kope sena ihla v kope s ena ihla v kope sena ihla v kope sena i hla v kope sena ihla v kope sena ihla v kope sena ihla v ko pe sena ihla v kope sena ihla v kope s

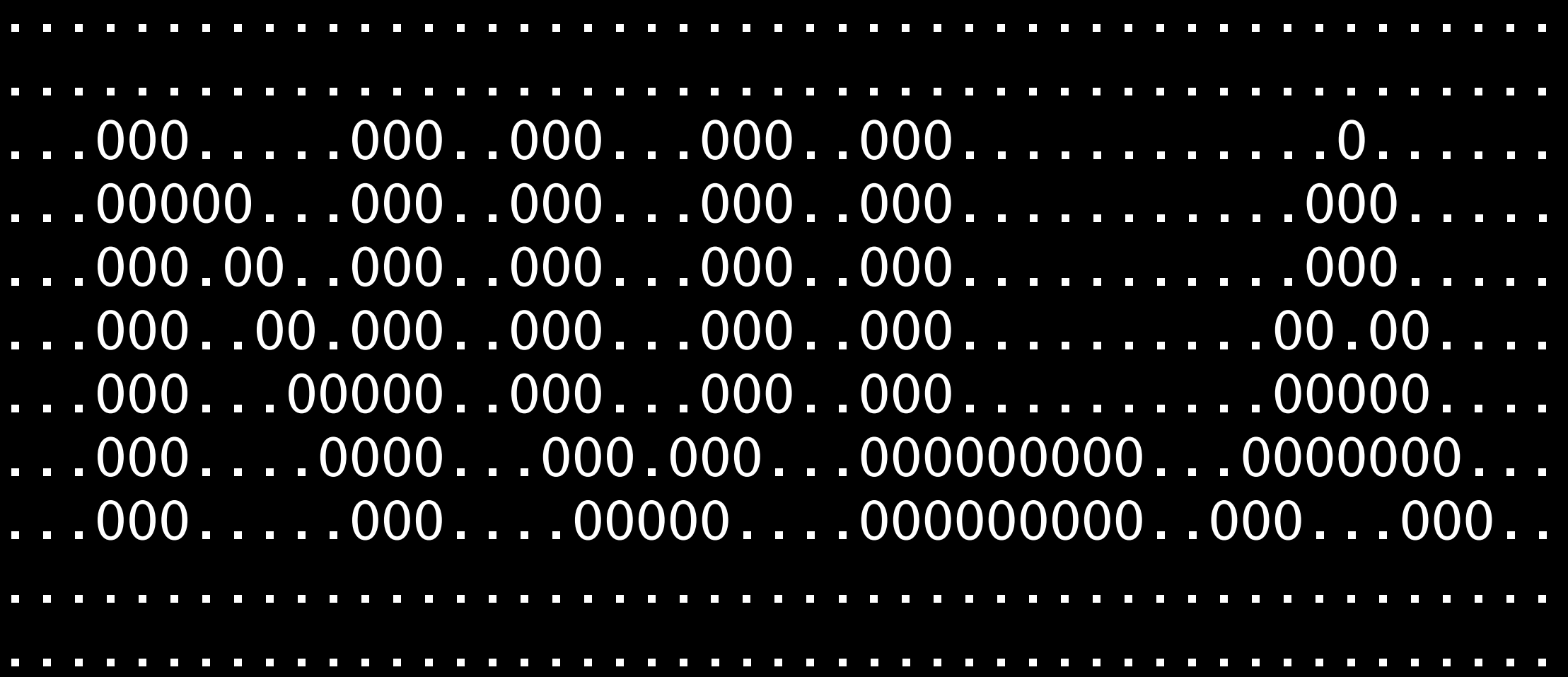
skrytá štruktúra



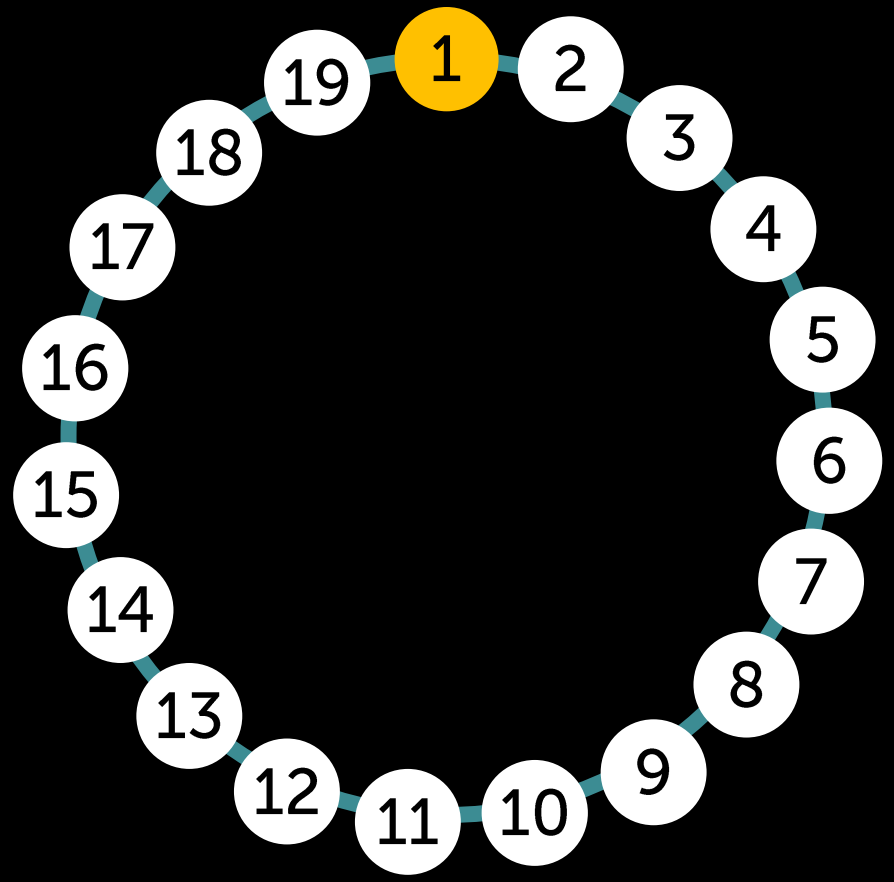

1111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111000111110001100011100011000111111111
1101111111111000001110001100011100011000111111111100011111111100010010
1000110001110001100011111111111000111111111000110010001100011100011000
1111111110010011111111000111000001100011100011000111111111100000111111
1100011110000111000100011100000000011100000001111111000111110001111000
0011110000000011000111000111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111100000100010


1111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111110001111100011
0001110001100011111111111101111111110000011100011000111000
0110001111111111100011111111100010011000110001110001100011
1111111110001111111110001100100011000111000110001111111111
0010011111111000111000001100011100011000111111111100000111
1111000111100001110001000111000000000111000000011111110001
1111000111100000111100000000011000111000111111111111111111
1111111111111111111111111111111111111111111111111111111111
1111111111111111111111111100000100010001110000100010001111

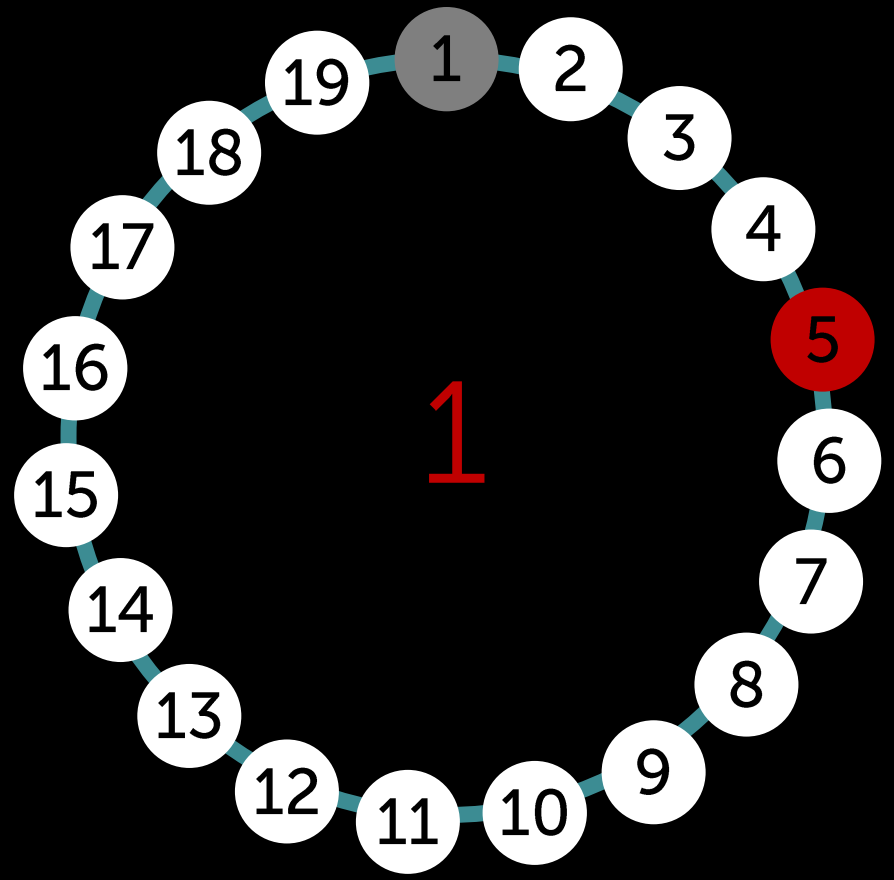

11111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111
11100011111000110001110001100011111111111011111111
11100000111000110001110001100011111111111000111111
11100010011000110001110001100011111111111000111111
11100011001000110001110001100011111111111001001111
11100011100000110001110001100011111111111000001111
11100011110000111000100011100000000011100000001111
11100011111000111100000111100000000011000111000111
11111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111



Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?

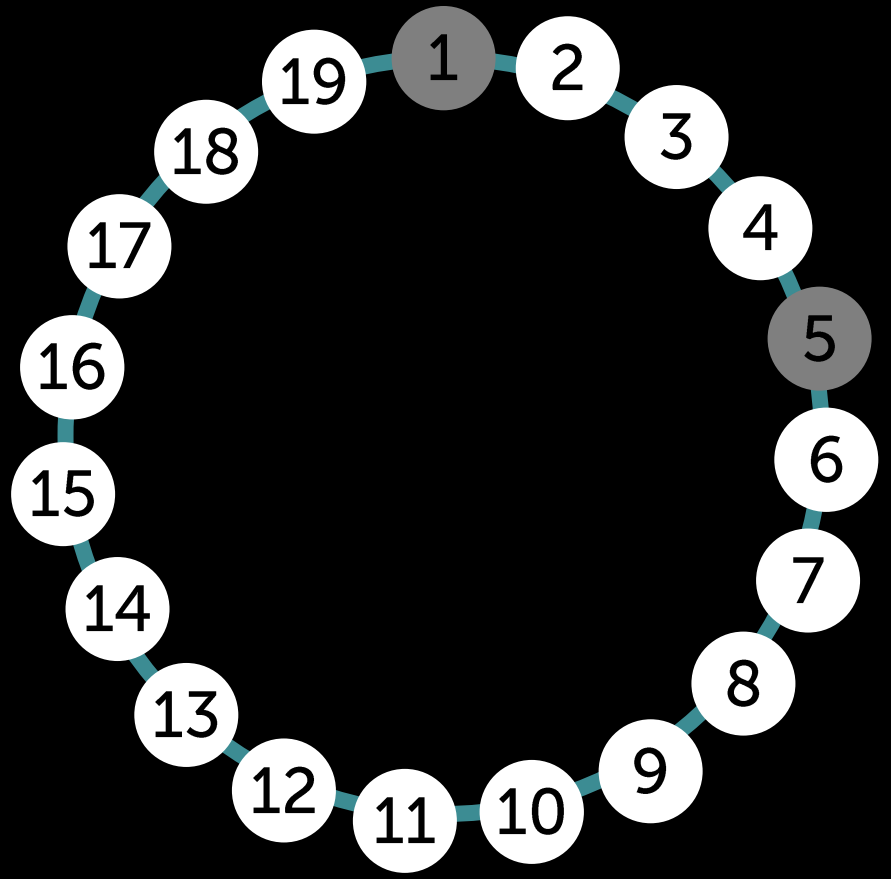


Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



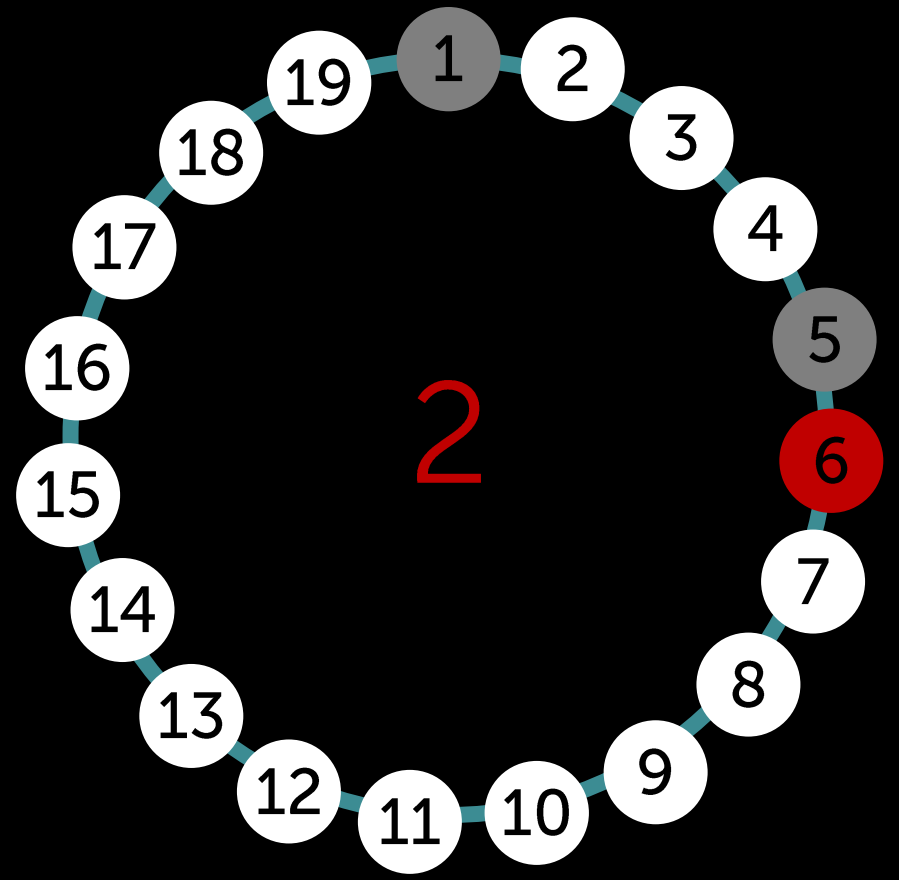
Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?

$5 \times 5 = 25$



Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?

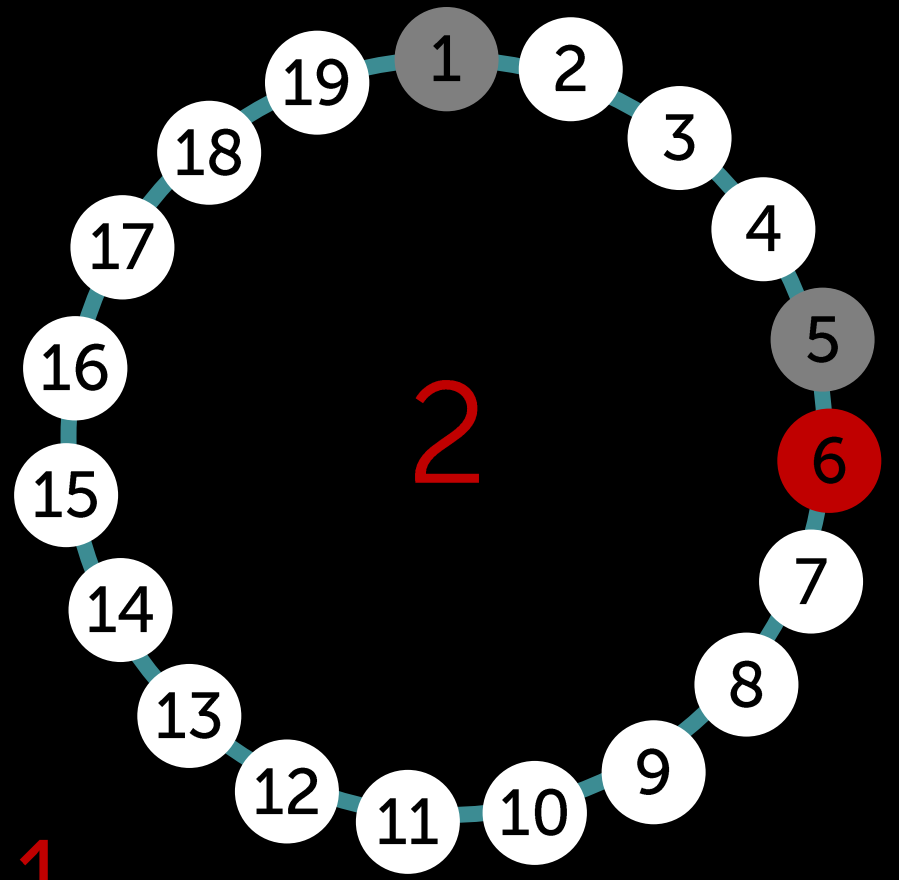
$5 \times 5 = 19 + 6$



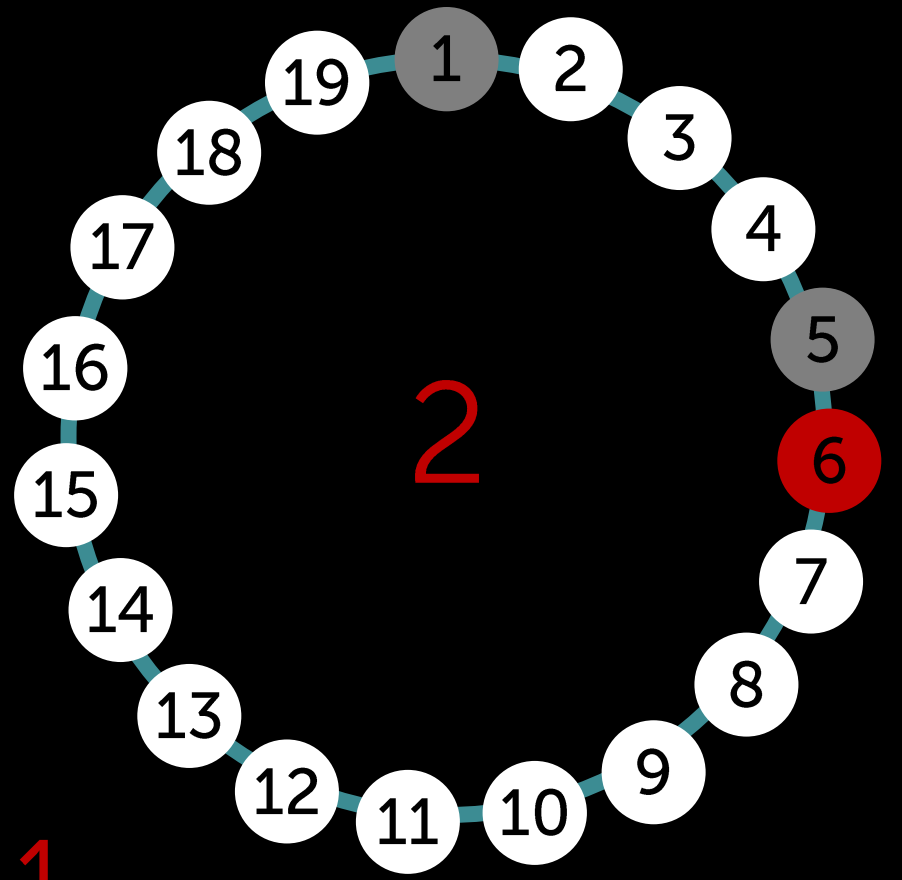
Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?

$$5 \times 5 = 19 + 6$$

$$25 \times 5 = 19 \times \ldots + 11$$



Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?

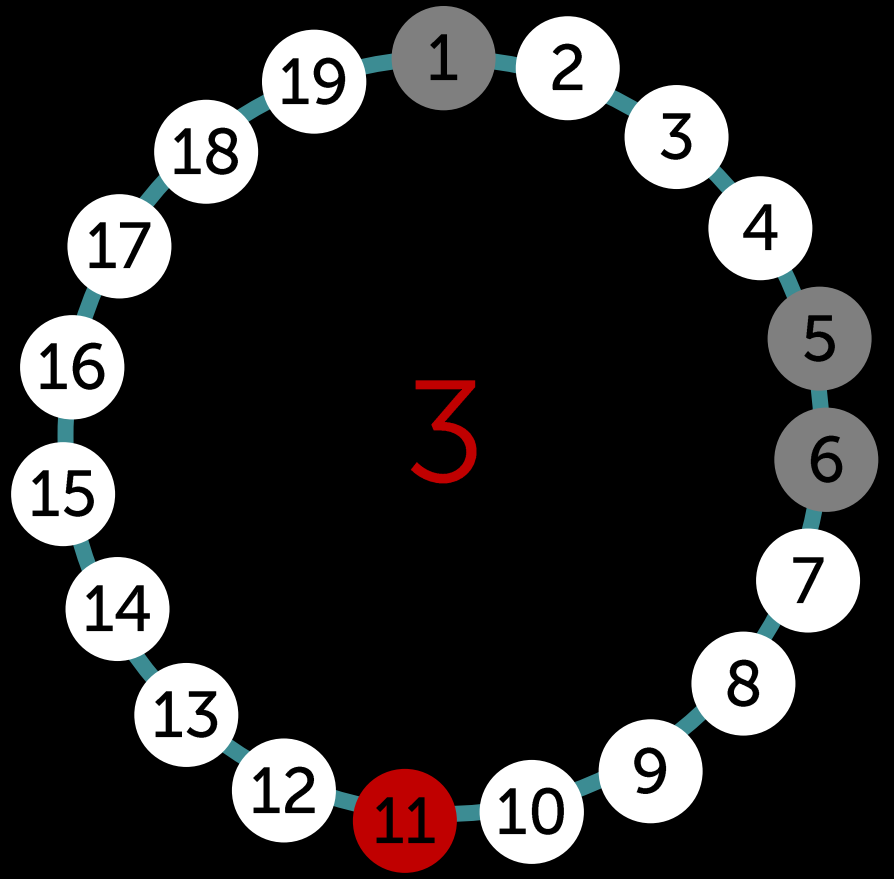


$5 \times 5 = 19 + 6$

$25 \times 5 = 19 \times \ldots + 11$

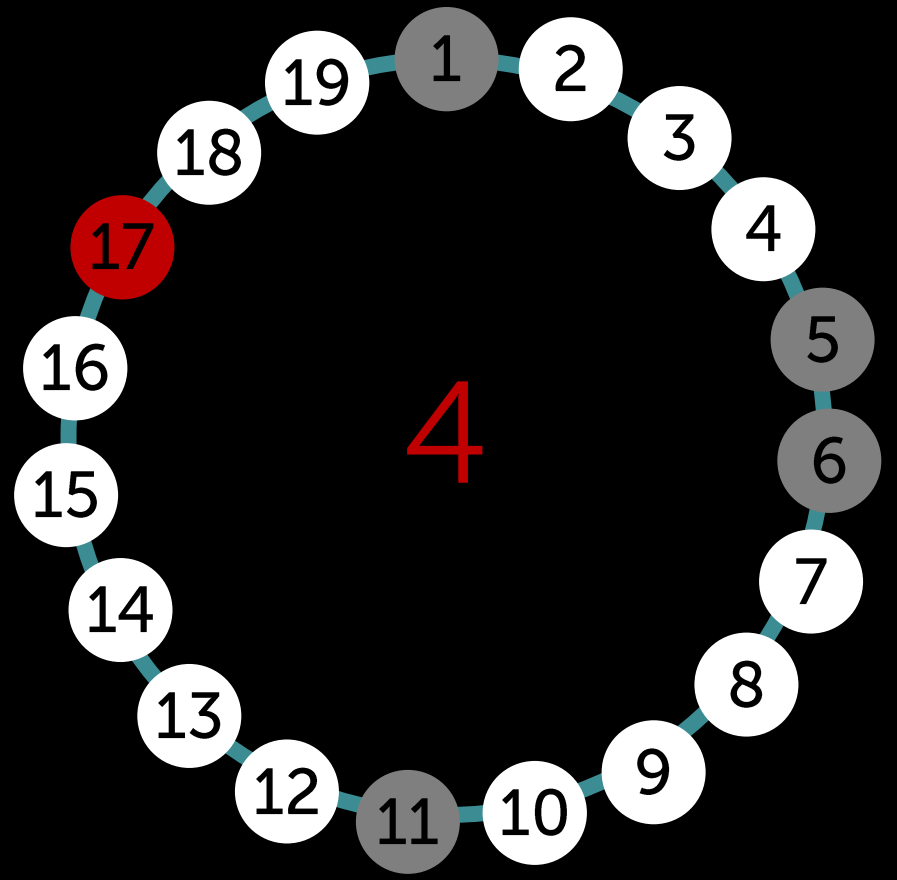
$6 \times 5 = 19 \times \ldots + 11$

Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



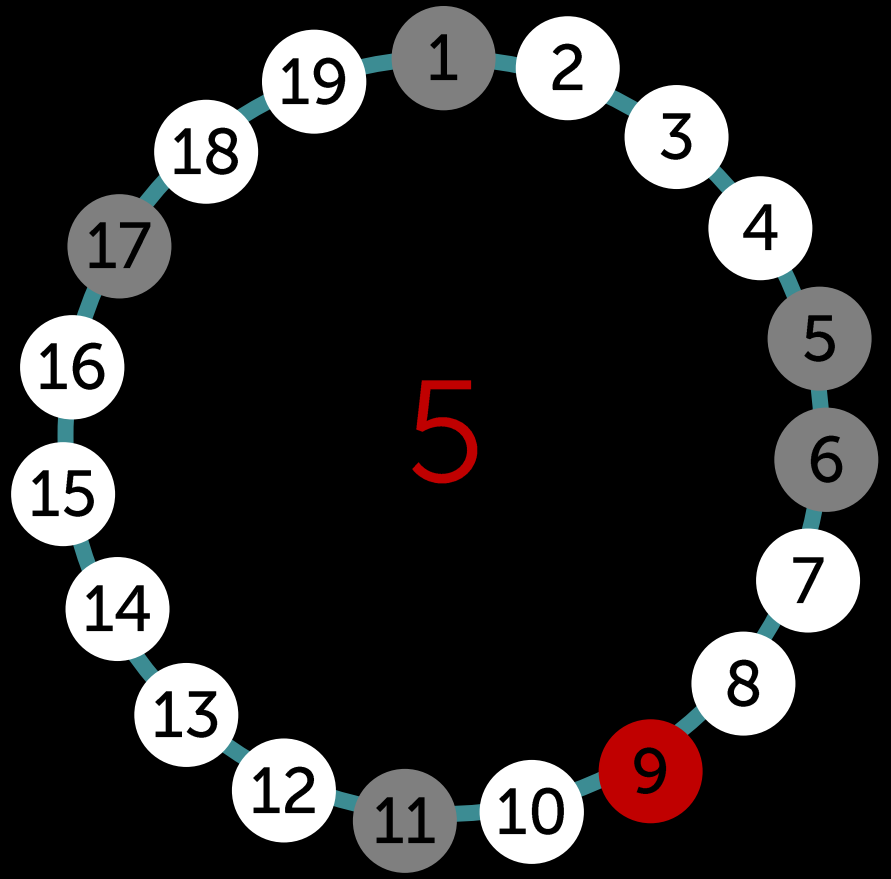
$5^3 = 19 \times \ldots + 11$

Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



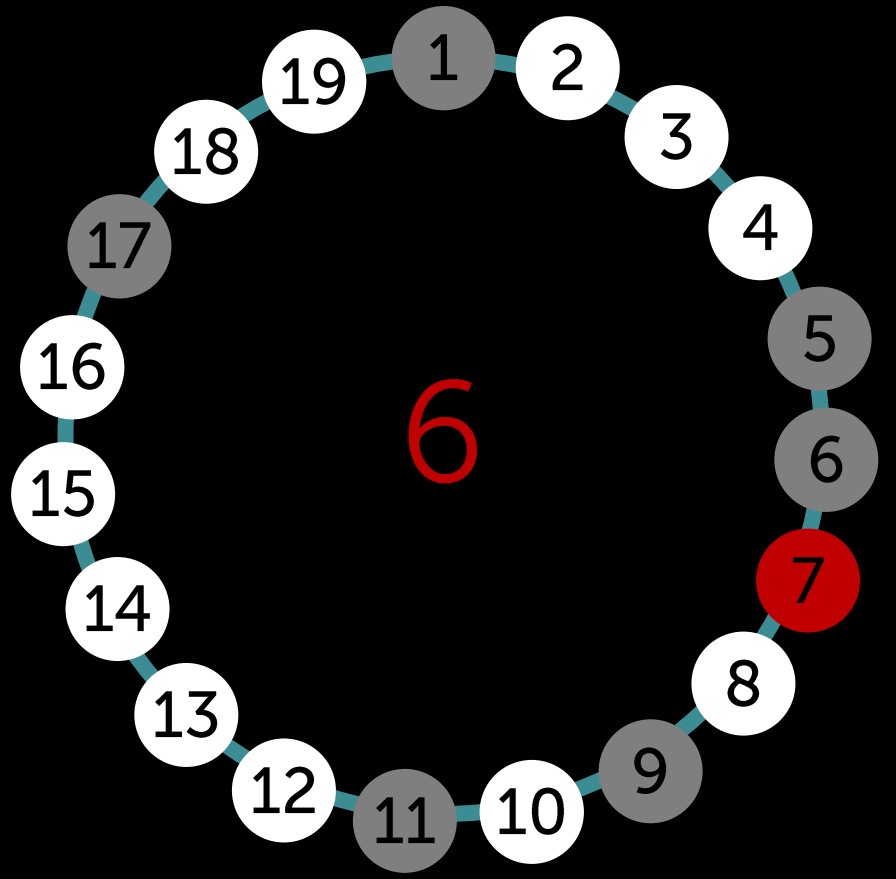
$5^4 = 19 \times \ldots + 17$

Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



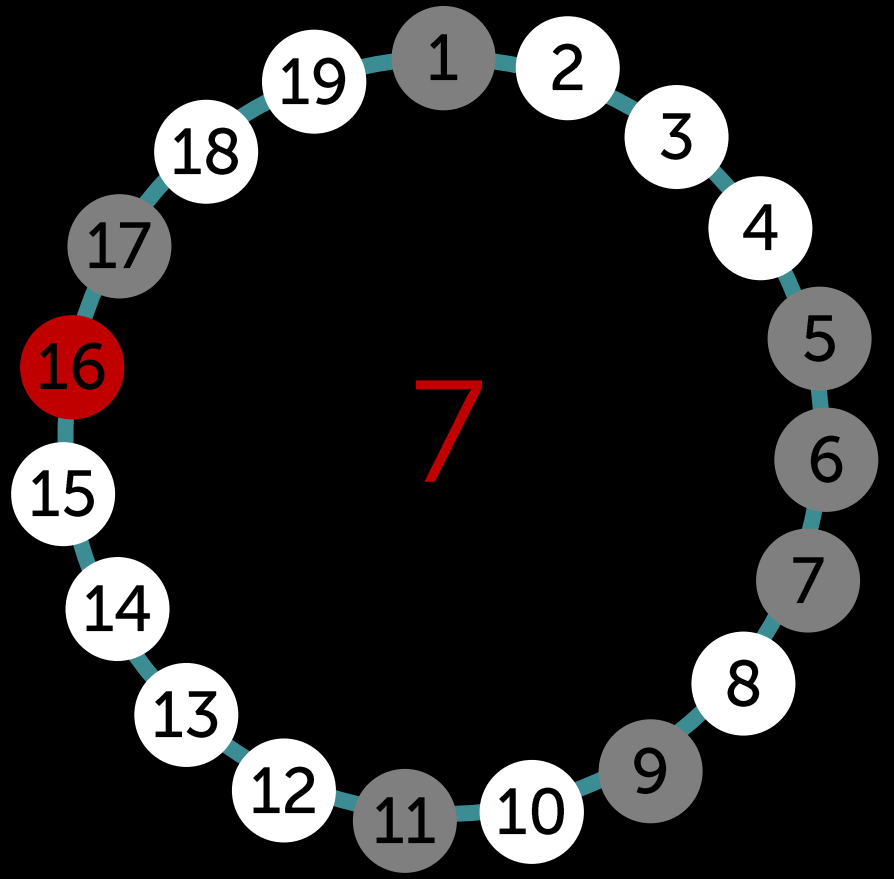
$5^5 = 19 \times \ldots + 9$

Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



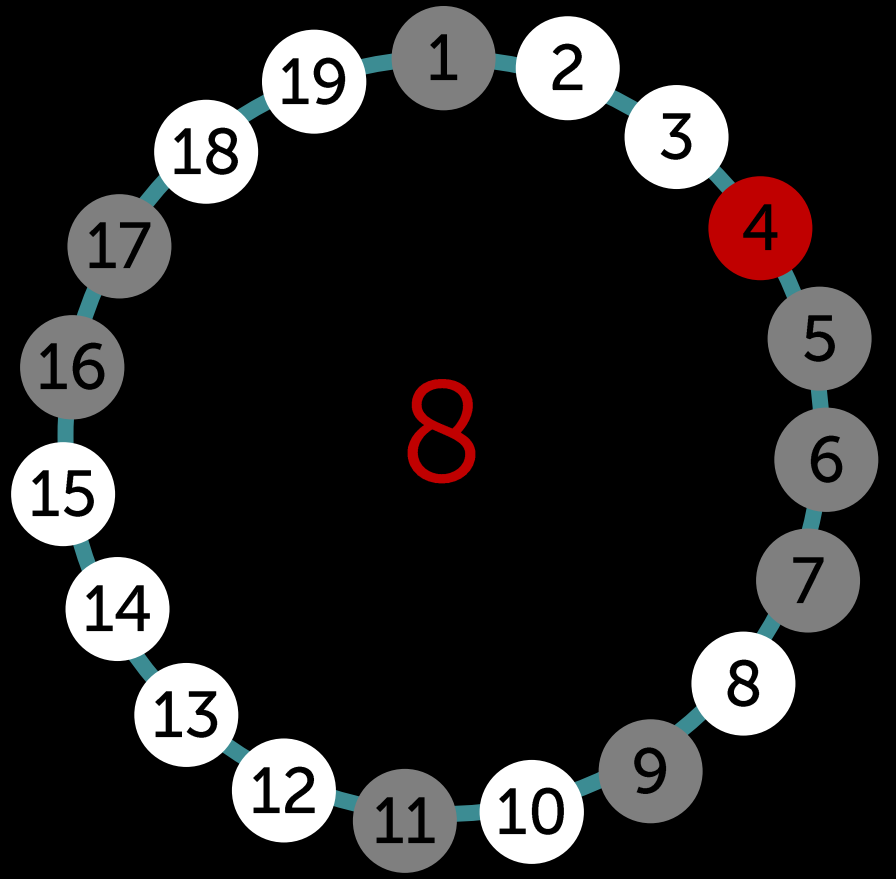
$5^6 = 19 \times \ldots + 7$

Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



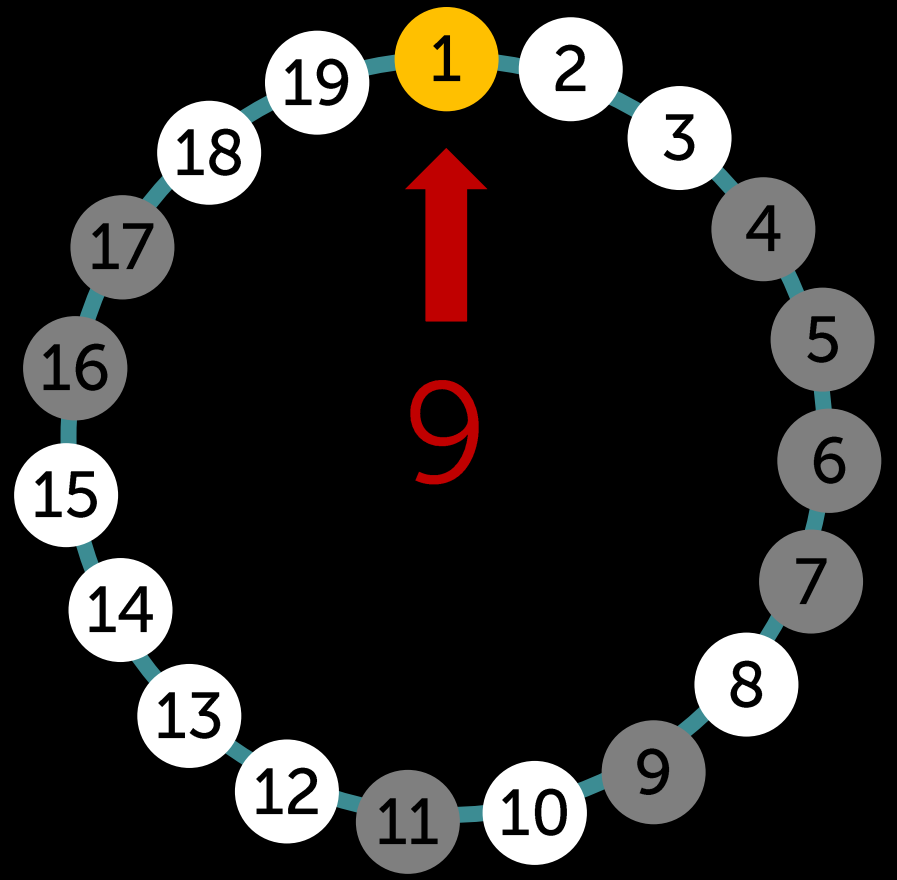
$5^7 = 19 \times \ldots + 16$

Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



$5^8 = 19 \times \ldots + 4$

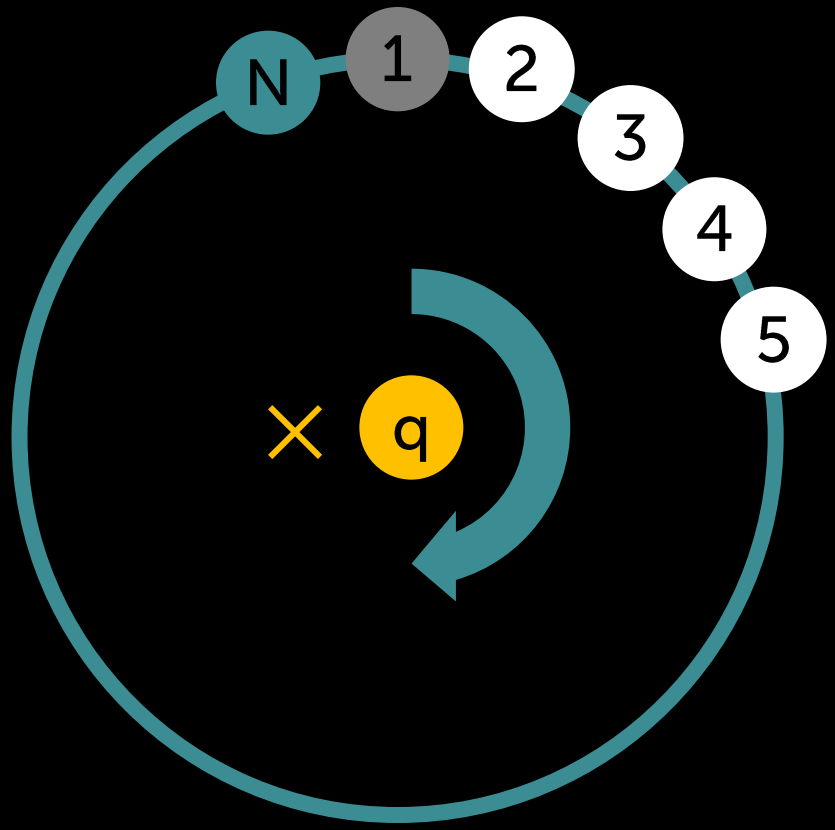
Kruh 19 čísel,
násobím 5.
Kedy sa vrátim?



$5^9 = 19 \times \ldots + 1$

$$q^r = 1 \bmod N$$

$$r = ?$$



ťažká úloha: faktorizácia

teória čísel

superpozície a Fourier

super kvantový algoritmus

Peter Shor

RSA ☹

$21 = 3 \times 7$

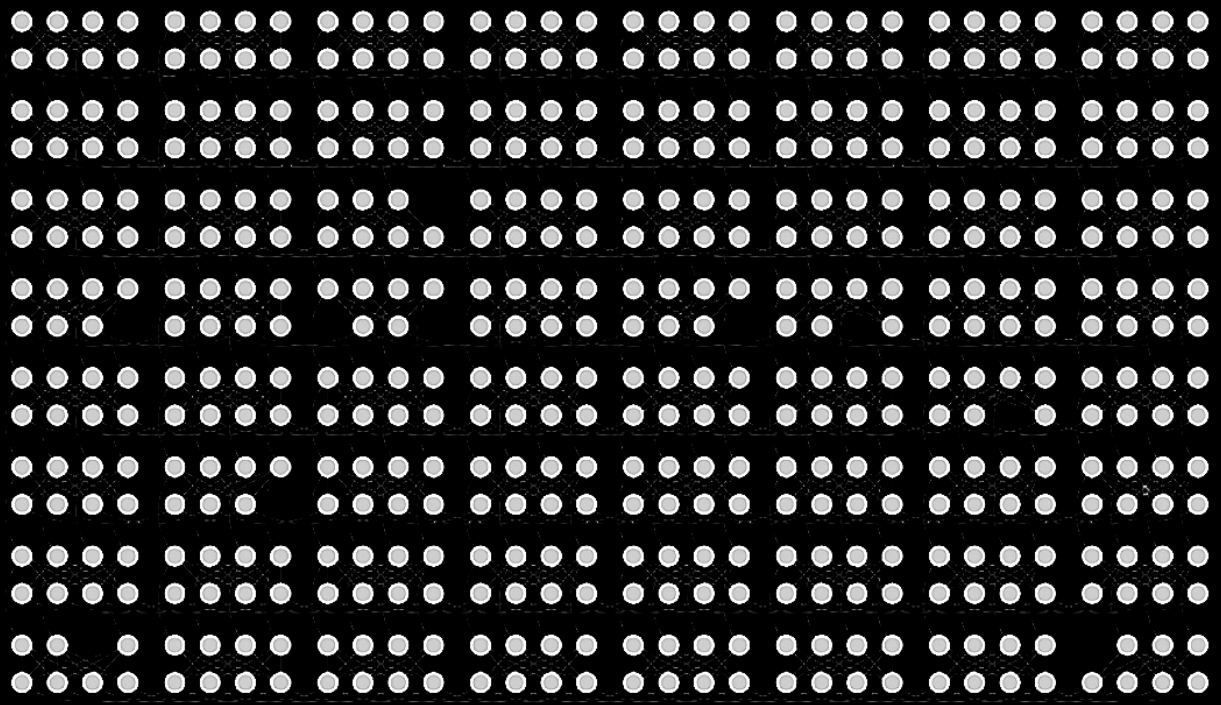
optimalizácia

pm
optimalizácia

optimalizácia na kvantovom ihrisku

adiabatické počítanie

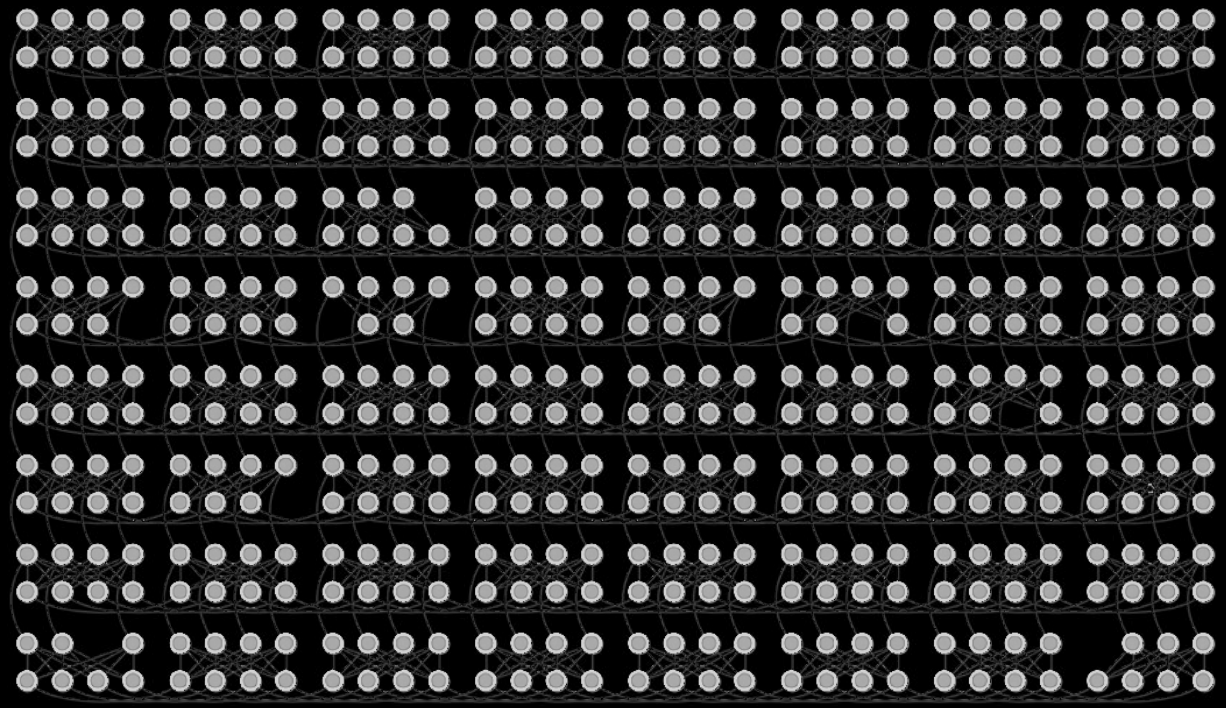
Farhi, Goldstone, Gutmann



optimalizácia na kvantovom ihrisku

adiabatické počítanie

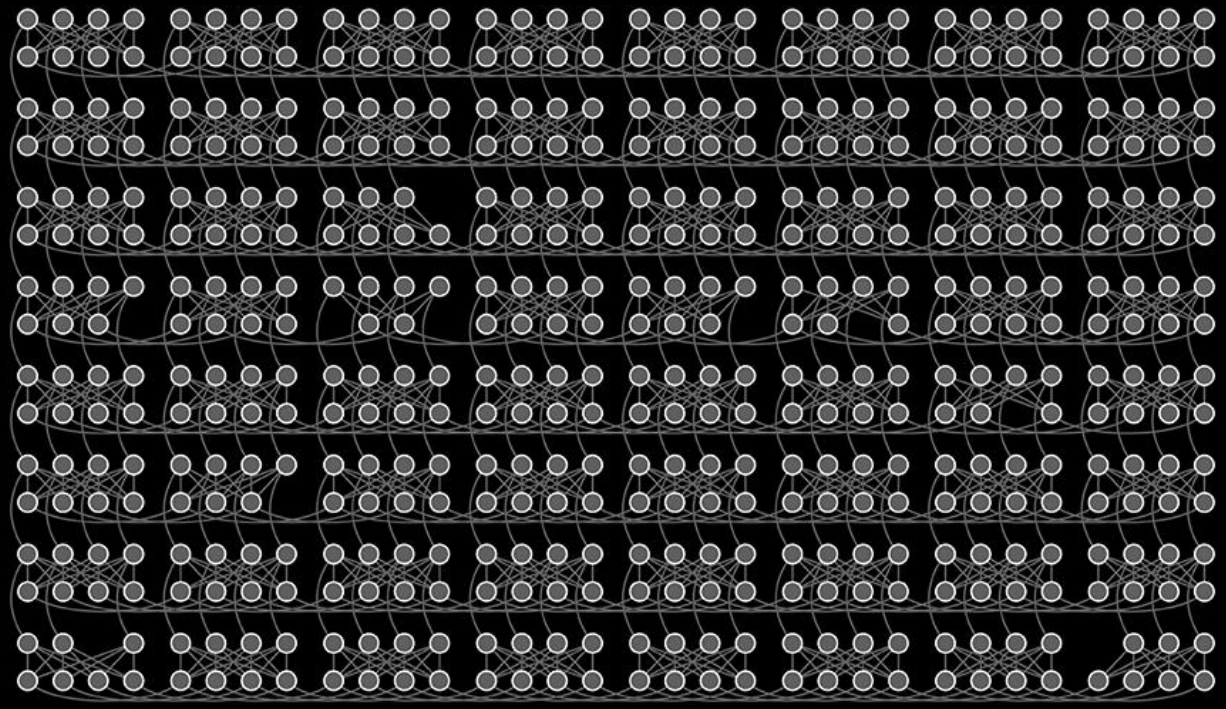
Farhi, Goldstone, Gutmann



optimalizácia na kvantovom ihrisku

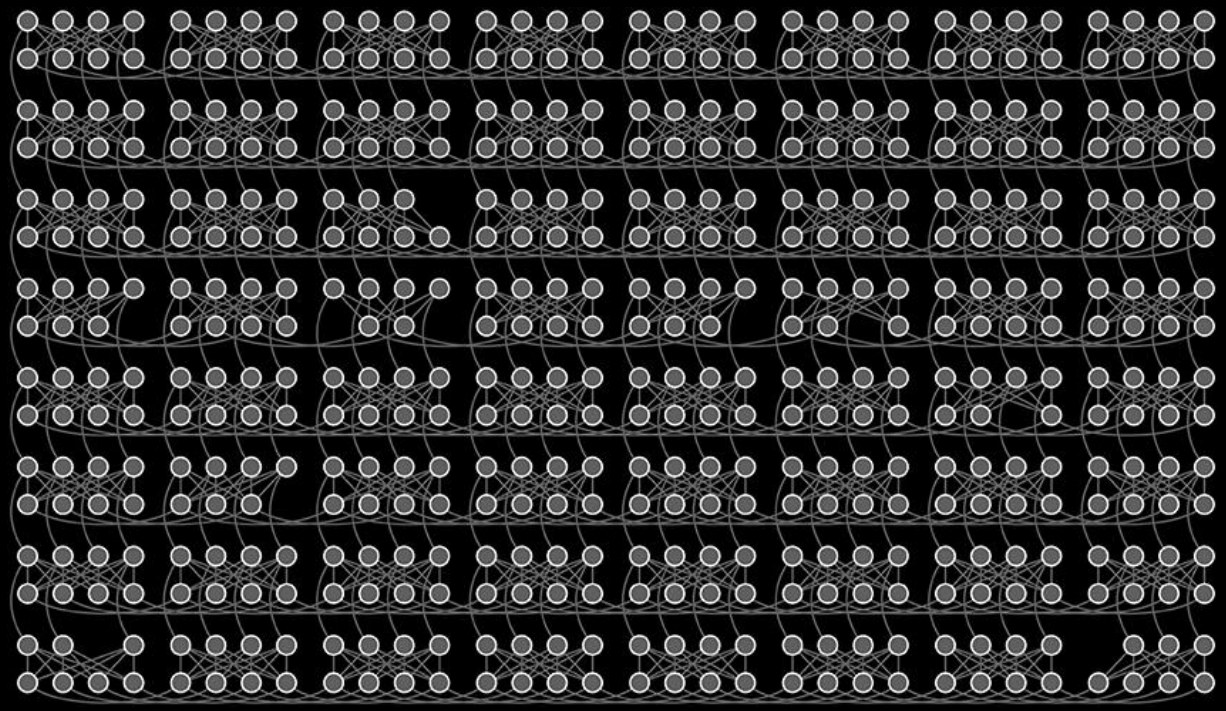
adiabatické počítanie

Farhi, Goldstone, Gutmann



optimalizácia na kvantovom ihrisku

adiabatické počítanie

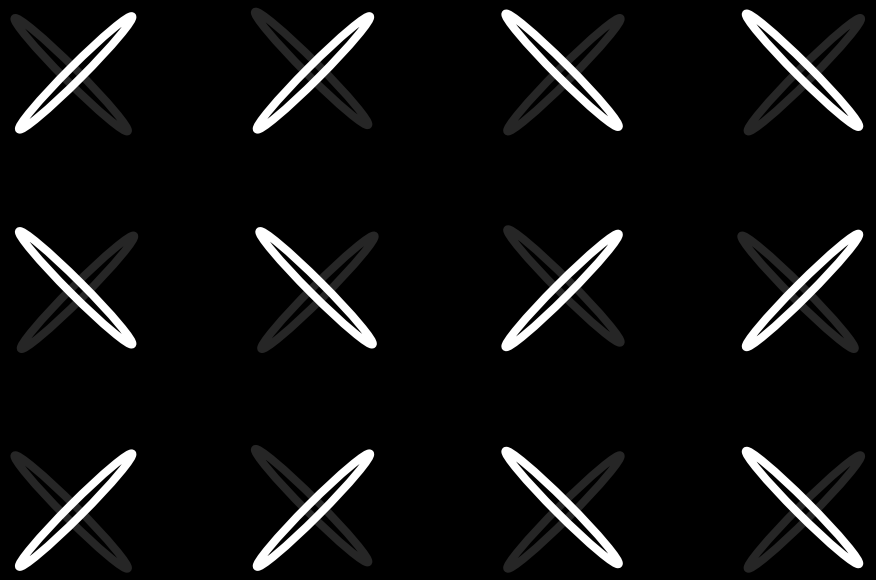


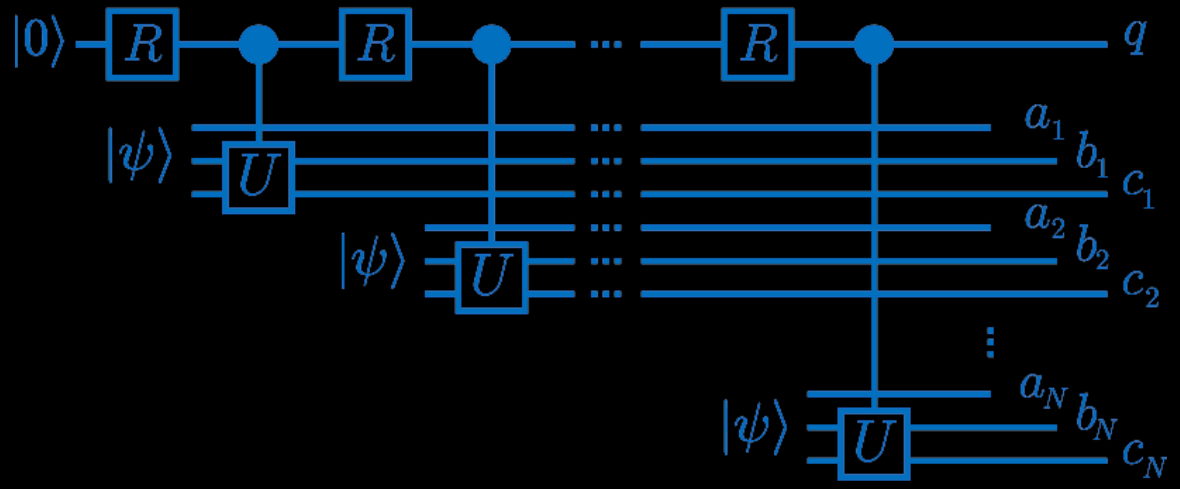
[chimera graph, D-Wave, 2014]

[D-Wave, 2017]

kvantové počítanie

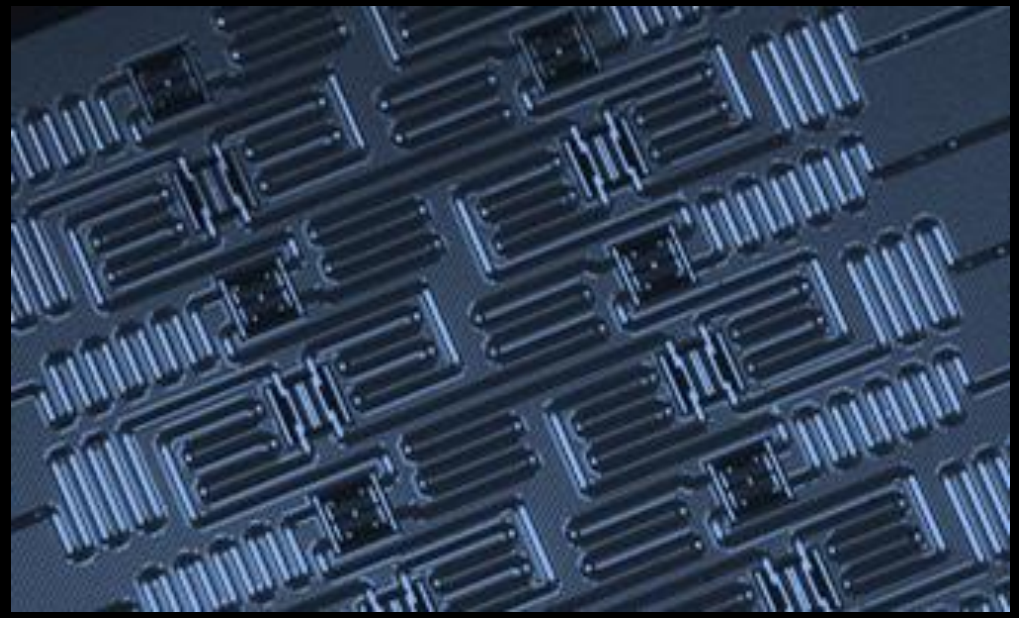
imagined by science





kvantové počítanie

made by science

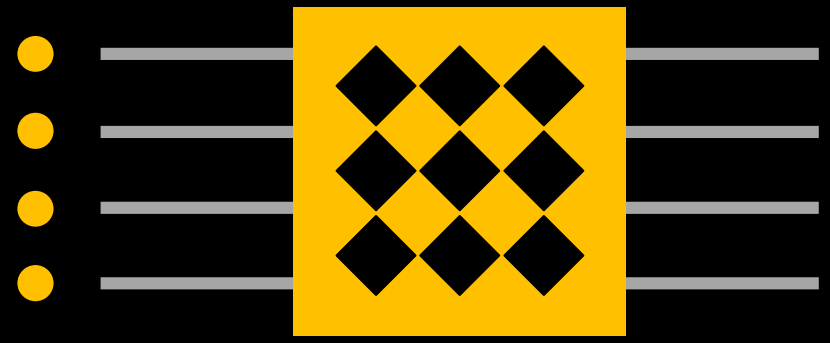


[IBM, 2017]

kvantová

SUPERIORITA

quantum supremacy



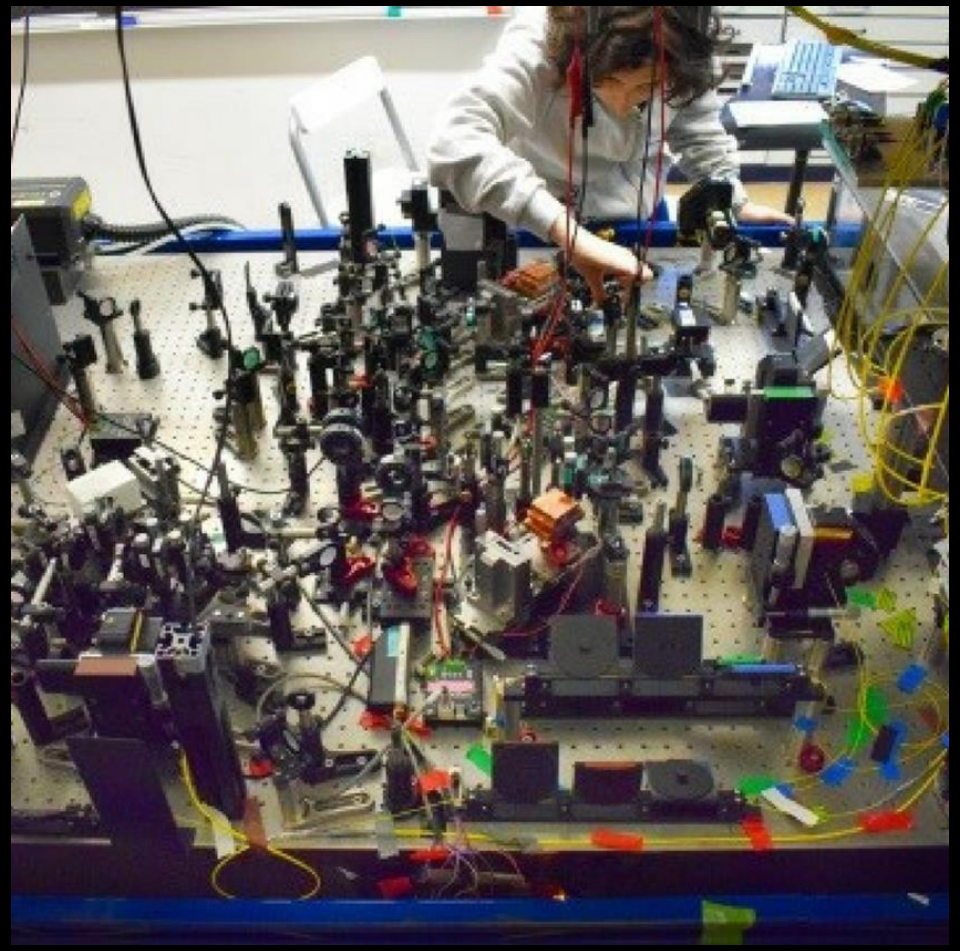
?

bozónové samplovanie

Aaronson, Arkhipov

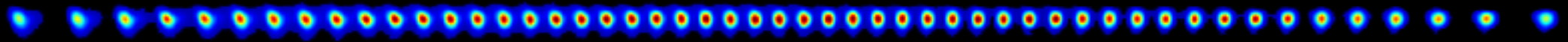
v podstate neužitočné
kvantovo dostupné
klasicky p p p o o o o m m m m a a l é

fotóny



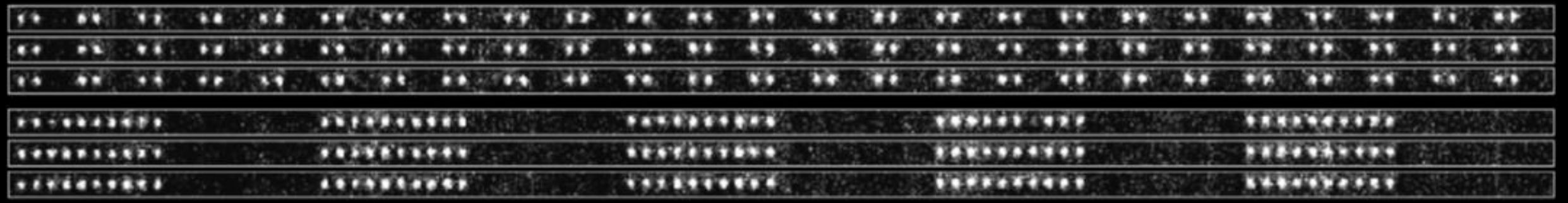
[Uni Wien, P. Walther]

lapené iónyl

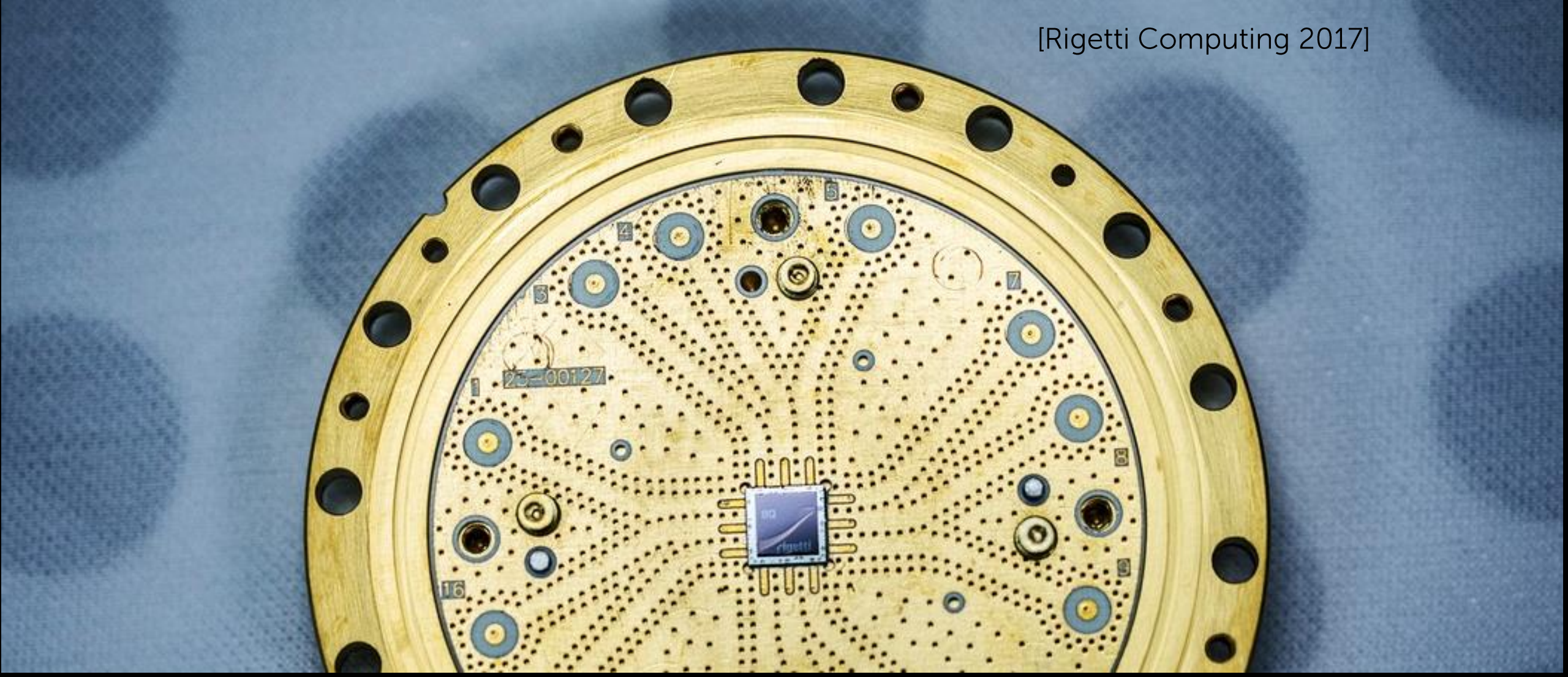


[Uni Innsbruck, R. Blatt]

studené atómy



[Endres et al., Science 354, 2016]

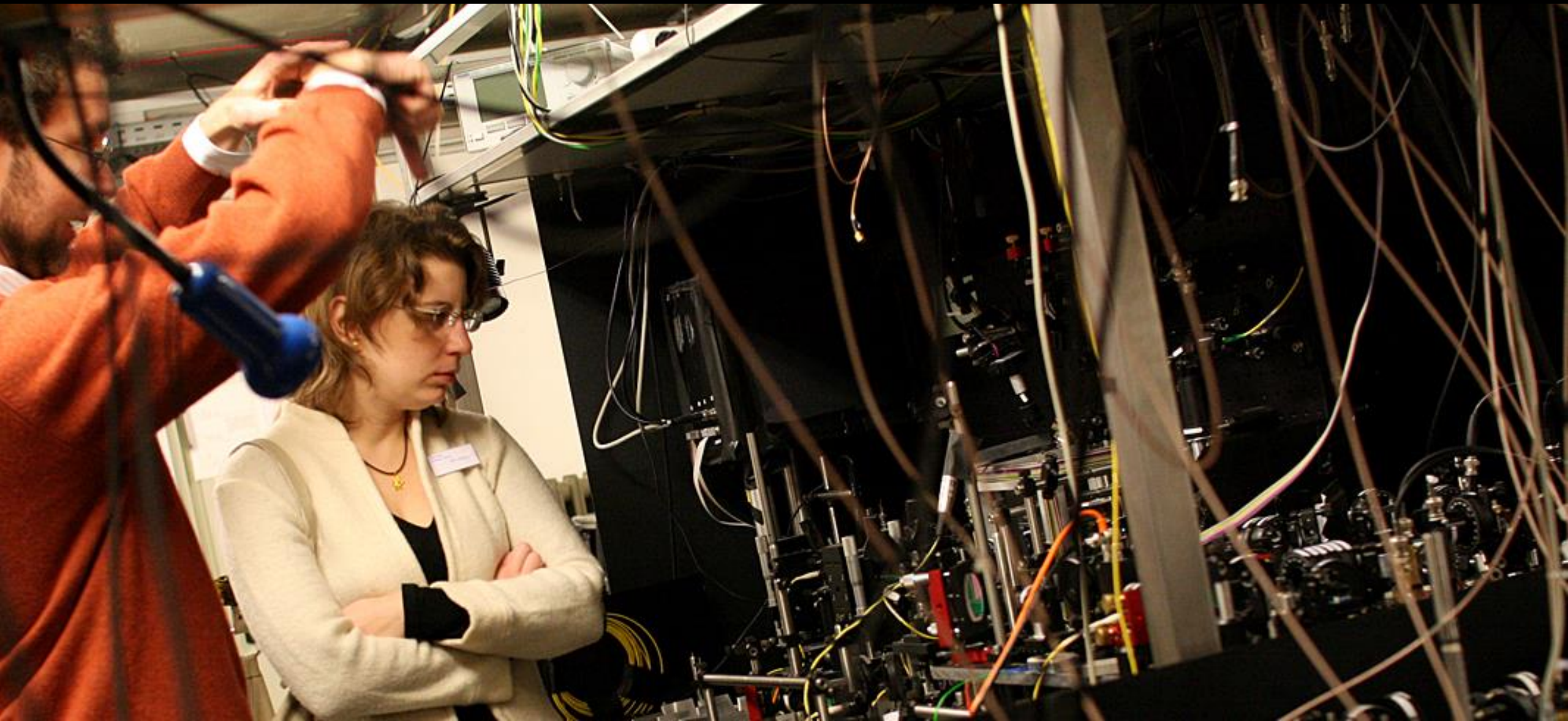


supravodivé obvody

oprava chýb

[Libor Caha]

škálovanie



Quantum Manifesto

A New Era of Technology

May 2016

Quantum Europe 2017: Towards the Quantum Technology Flagship

Centrum pre výskum kvantovej informácie

Fyzikálny ústav SAV BA

siete Bužek
procesy Ziman
obvody Grajcár
spintronika Staňo
simulácie Gendiar
rozlišovanie Sedlák
kráčania Reitzner
štatistika Rapčan
zložitosť Nagaj

svet ako výpočet

daniel nagaj & rcqi
centrum pre výskum kvantovej informácie
fyzikálny ústav slovenskej akadémie vied

SAS PRO

svet ako kvantový počet

daniel nagaj & rcqi
centrum pre výskum kvantovej informácie
fyzikálny ústav slovenskej akadémie vied

SAS PRO

Mišo Sedlák

Libor Caha

Dano Reitzner

Tomáš Rybár

svet ako kvanto výpočet

daniel nagaj & rcqi

centrum pre výskum kvantovej informácie

fyzikálny ústav slovenskej akadémie vied

SAS PRO