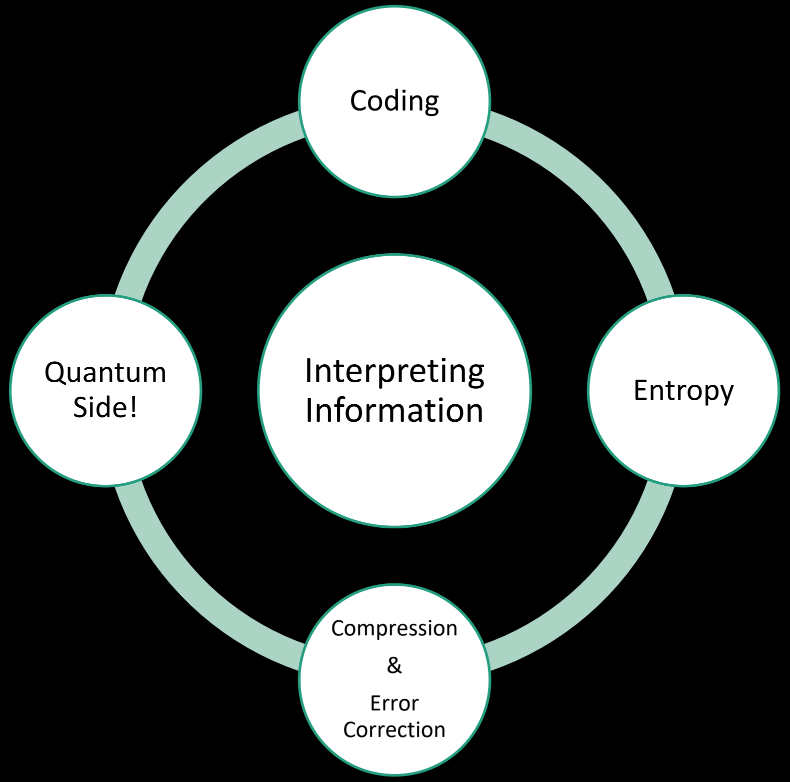
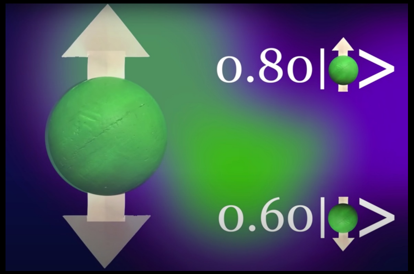
Paper 1 Takeaways!



$$H=\sum_{i=1}^{n} p_i \times \log_2\left(\frac{1}{p_i}\right)$$

$$H=-\sum_{i=1}^{n} p_i \times \log_2(p_i)$$



On and Beyond: Cryptography in a Post-Quantum World!

1) Asymmetric Encryption &
Grover's Algorithm ; Shor's Algorithm

2)

N	AQ	$\overline{Tq}$	$\overline{Tc}$
32	32	$5{,}14\cdot10^{4}$	$4{,}30\cdot10^{9}$
56	56	$2{,}11\cdot10^{8}$	$7{,}21\cdot10^{16}$
88	88	$1{,}38\cdot10^{13}$	$3{,}10\cdot10^{26}$
112	112	$5{,}66\cdot10^{16}$	$5{,}19\cdot10^{33}$
128	128	$1{,}45\cdot10^{19}$	$3{,}40\cdot10^{38}$
184	184	$3{,}89\cdot10^{27}$	$2{,}45\cdot10^{55}$
256	256	$2{,}67\cdot10^{38}$	$1{,}16\cdot10^{77}$

Table 1. N - quantity of bits, AQ - quantity of qubits, $\overline{Tq}$ - the average quantum time described by function $f(n)$ ($\overline{Tq}=f(n)$), $\overline{Tc}$ - the average classical time described by function $g(n)$ ($\overline{Tc}=g(n)$)

Fig: Symmetric Keys

	Factorization		
	AQ	$\overline{Tq}$	$\overline{Tc}$
N	q_1	f_1	g_1
512	1024	$5{,}37\cdot10^{8}$	$2{,}47\cdot10^{16}$
1024	2048	$4{,}29\cdot10^{9}$	$1{,}01\cdot10^{22}$
2048	4096	$3{,}43\cdot10^{10}$	$5{,}80\cdot10^{29}$
4096	8192	$2{,}75\cdot10^{11}$	$4{,}85\cdot10^{39}$
8192	16384	$2{,}20\cdot10^{12}$	$4{,}23\cdot10^{52}$
16384	32768	$1{,}76\cdot10^{13}$	$2{,}05\cdot10^{70}$
32768	65536	$1{,}41\cdot10^{14}$	$5{,}54\cdot10^{92}$

Fig: Asymmetric Keys - Factorization

3)
Projects: zk-STARKs (Zero-Knowledge Scalable Transparent ARguments of Knowledge), PQCrypto , SAFEcrypto, PROMETHEUS

NIST - (National Institute of Standards and Technology)

1. https://ir.cwi.nl/pub/13851/13851B.pdf - "Handbook on the Philosophy of Information, 2008"
2. H. Lone and R. Naaz, "Demystifying Cryptography behind Blockchains and a Vision for Post-Quantum Blockchains," *2020 IEEE International Conference for Innovation in Technology (INOCON)*, 2020, pp. 1-6, doi: 10.1109/INOCON50539.2020.9298215.
3. T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," in IEEE Access, vol. 8, pp. 21091-21116, 2020, doi: 10.1109/ACCESS.2020.2968985.
4. V. S. Igumnov and V. N. Lis, "Influence of Quantum Computers on Classical Cryptography," 2007 8th Siberian Russian Workshop and Tutorial on Electron Devices and Materials, 2007, pp. 220-224, doi: 10.1109/SIBEDM.2007.4292963.