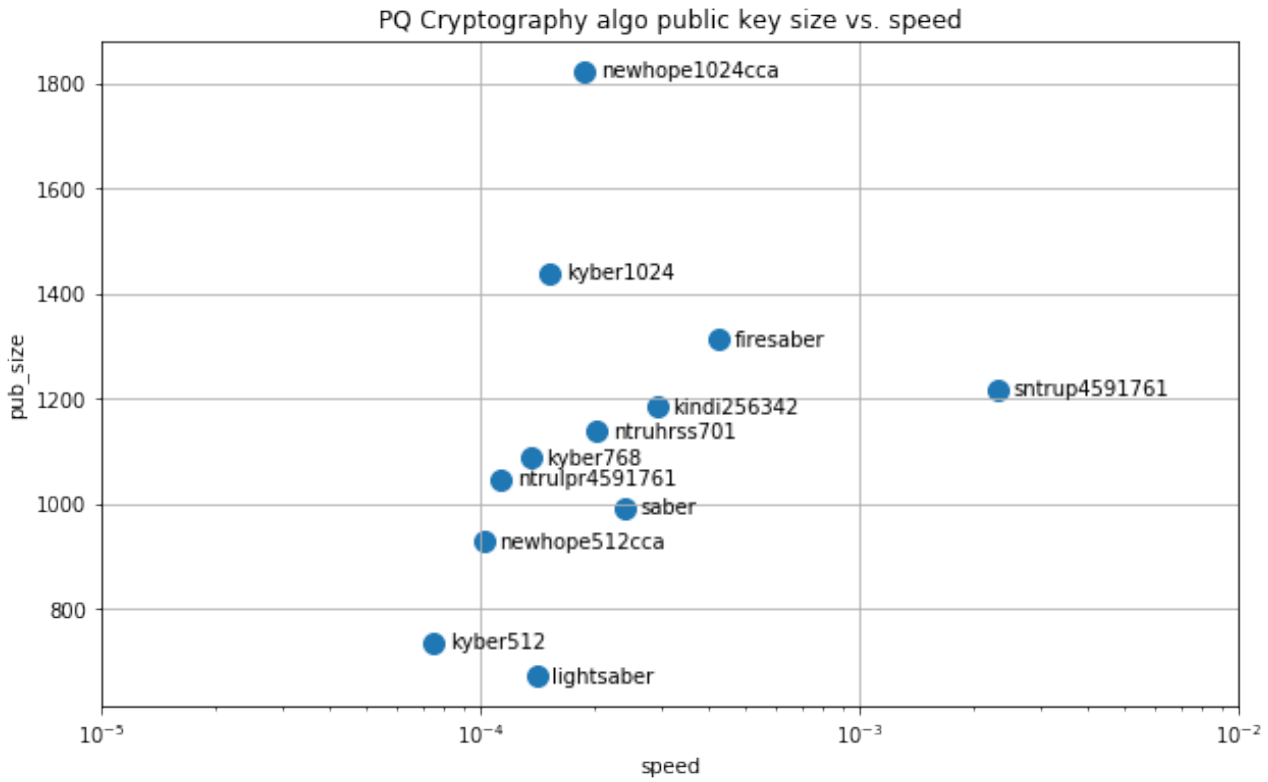
Kryptografia postkwantowa

Mikołaj Koszowski 274392
Hubert Nowakowski 274415

Zad 6. wariant 4
Kod źródłowy: github.com/Fisher16/KiBD

Stworzyliśmy notebooki pokazujące wymianę kluczy algorytmem NewHope, a następnie wykorzystujące AES do komunikacji. Uważa się, że symetryczna kryptografia jest odporna na ataki z wykorzystaniem komputerów kwantowych. Algorytm Grovera redukuje czas ataku *brute-force* to pierwiastka klasycznej wartości, zatem AES-256 po nadejściu wydajnych komputerów kwantowych zostanie zredukowany do AES-128, który jest nadal uważany za bezpieczny.
Porównaliśmy również implementację w czystym pythonie z tą w C/C++, ta druga była 300 razy szybsza, co pokazuje istotność optymalizacji, o której wspominali na konferencji (*35C3 - The year in post-quantum crypto*). Odtworzyliśmy porównanie prędkości wymiany klucza sesji do wielkości klucza publicznego, widoczne poniżej:



Eksperymenty postkwantowe z TLS. W roku 2016 badacze z google'a przeprowadzili testy protokołu o nazwie CECPQ1 wykorzystywał on krzywe eliptyczne i algorytm NewHope. W roku 2018 wykonali badania nad nową wersją protokołu CECPQ2, zastępującym algorytm NewHope NTRU_HRSS.

Źródła:

Quantum Security Analysis of AES: https://eprint.iacr.org/2019/272.pdf
Lattices: Algorithms, Complexity, and Cryptography https://www.youtube.com/watch?v=GOQkjFdSG94
Intel intrinsics functions https://software.intel.com/sites/landingpage/IntrinsicsGuide/
CECPQ2 (12 Dec 2018) https://www.imperialviolet.org/2018/12/12/cecpq2.html
A Guide to Post-Quantum Cryptography https://medium.com/hackernoon/a-guide-to-post-quantum-cryptography-d785a70ea04b

Szczegóły do wykresu nr.1 :

	name	pub_key [bytes]	Speed [s]
1	firesaber	1312	0.000424
2	kindi256342	1184	0.000291
3	kyber1024	1440	0.000152
4	kyber512	736	0.000075
5	kyber768	1088	0.000135
6	lightsaber	672	0.000140
7	mceliece6960119	1047319	1.683
8	mceliece8192128	1357824	0.936
9	newhope1024cca	1824	0.000188
10	newhope512cca	928	0.000102
11	ntruhrss701	1138	0.000203
12	ntrulpr4591761	1047	0.000113
13	ramstakers216091	27044	0.0155
14	ramstakers756839	94637	0.0672
15	saber	992	0.000240
16	sntrup4591761	1218	0.002309