KYBER CRYSTALS

Bezpieczeństwo ery post-kwantowej

inż. Zuzanna Gołębiewska, promotor: dr Bartosz Naskręcki

Wprowadzenie

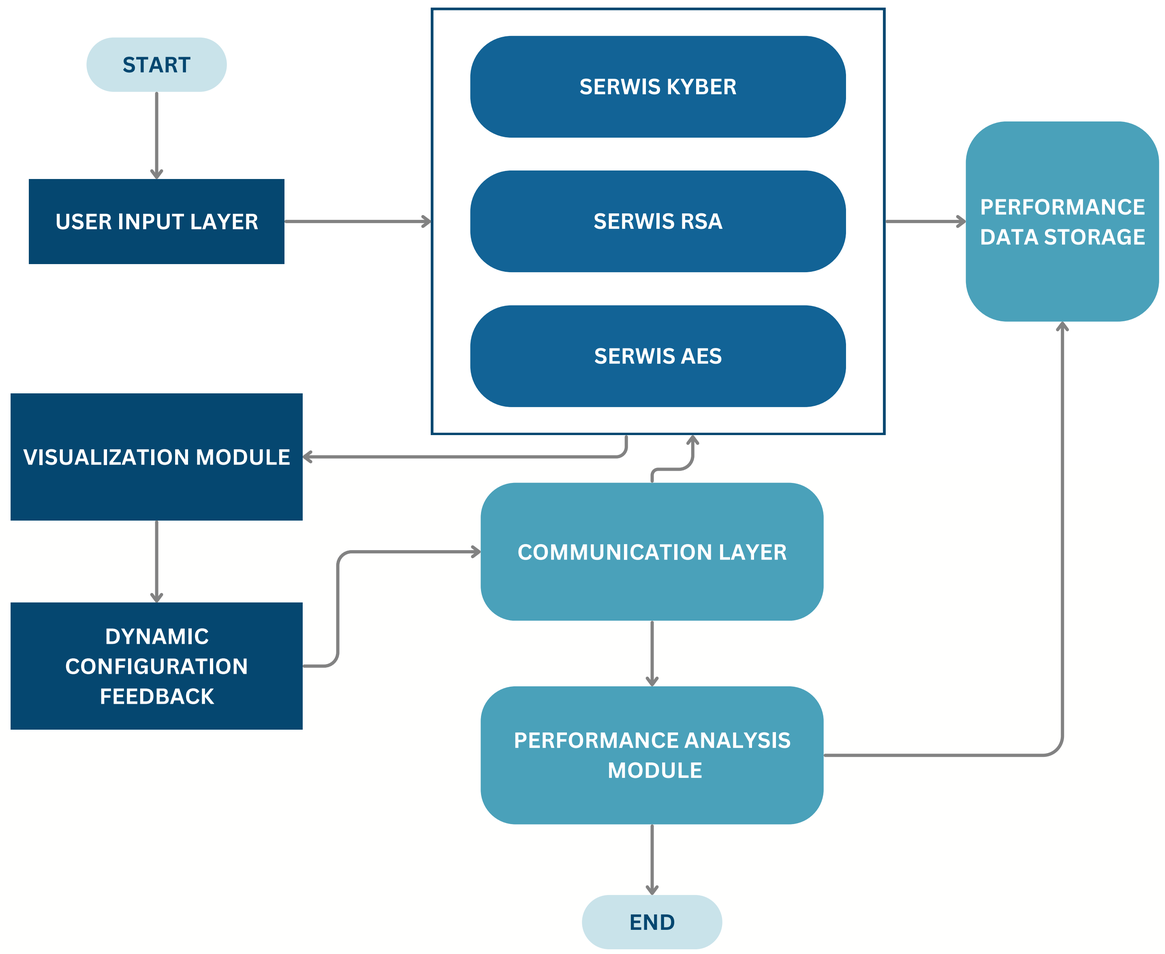
W erze **dynamicznego rozwoju technologicznego**, komputery kwantowe stają się coraz bardziej **realnym zagrożeniem** dla tradycyjnych metod kryptograficznych, takich jak RSA czy AES. W odpowiedzi na te wyzwania, wprowadzono **algorytmy postkwantowe**, które zapewniają **odporność** na ataki wykorzystujące zaawansowane algorytmy komputerów kwantowych, takie jak algorytm Shora.

Celem mojej pracy badawczej

jest analiza **bezpieczeństwa i wydajności** algorytmu ***Kyber*** w porównaniu z tradycyjnymi rozwiązaniami, takimi jak **RSA czy AES**. Dodatkowo, projekt obejmuje stworzenie **interaktywnej** aplikacji webowej, która w sposób dynamiczny prezentuje sposób działania algorytmu Kyber, mierząc **czas i efektywność** procesu szyfrowania oraz deszyfrowania wiadomości. Aplikacja ma na celu wsparcie **deweloperów i firm technologicznych** w zrozumieniu i przyjęciu bezpiecznych rozwiązań kryptograficznych odpornych na **ataki kwantowe.**

Projekt jest krokiem w stronę popularyzacji i wdrożenia nowoczesnych metod ochrony danych, co ma kluczowe znaczenie w zapewnieniu bezpieczeństwa w erze postkwantowej.

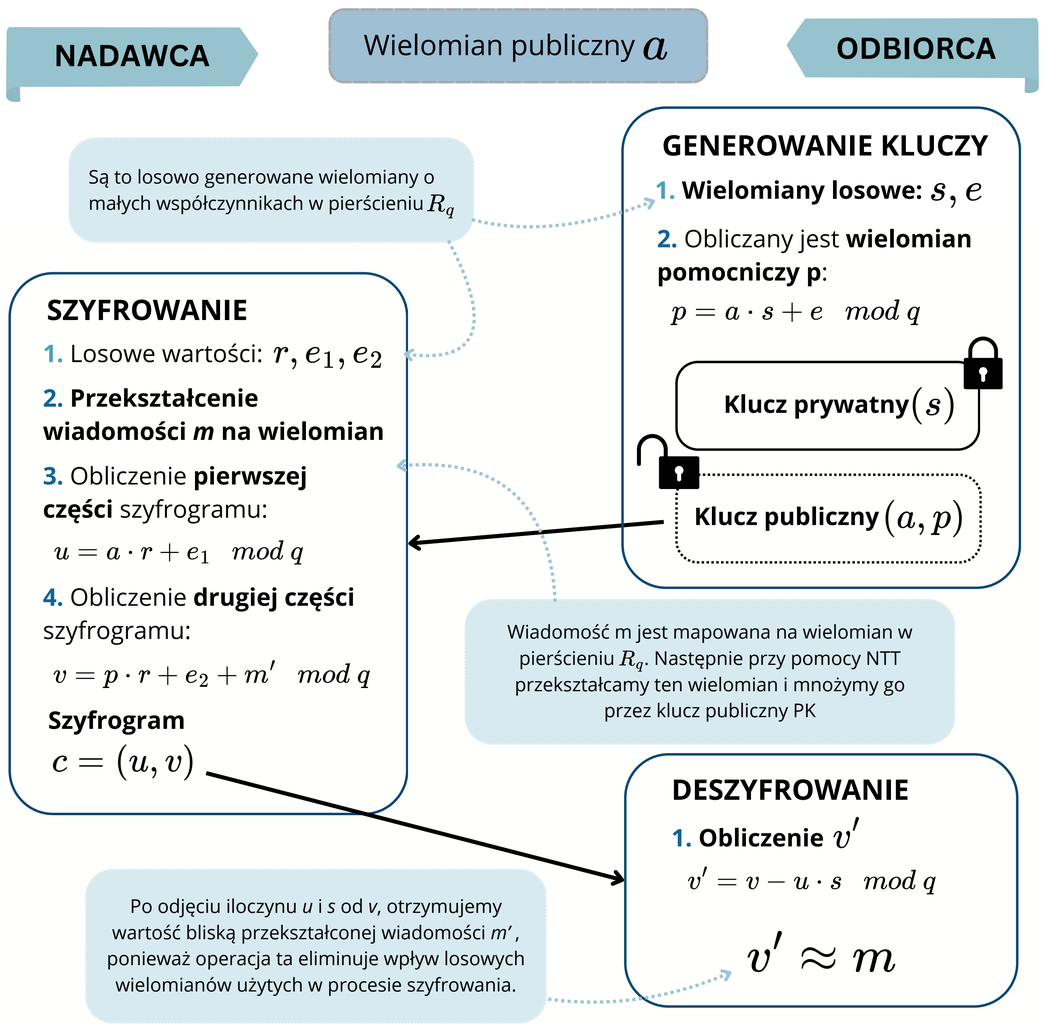
Architektura systemu



Wszystkie te operacje są monitorowane przez **Moduł bezpieczeństwa i wydajności**, napisany w Pythonie. Moduł ten analizuje procesy za pomocą metryk porównawczych z innymi popularnymi algorytmami, takimi jak AES i RSA, co pozwala ocenić **skuteczność i bezpieczeństwo Kybera**.

Kyber jako standard

13 sierpnia 2024r. ***Kyber Crystals*** stał się standardem **FIPS 203** (Federal Information Processing Standard) jako część działań mających na celu przygotowanie systemów kryptograficznych na nadejście **ery komputerów kwantowych.**



Kyber opiera się na problemach matematycznych związanych z kratami **(LATTICES)**, takich jak Learning with Errors **(LWE)**. Problemy te są uważane za **niezwykle trudne** do rozwiązania, nawet dla komputerów kwantowych.

Metodologia badawcza

Metodologia pracy jest oparta na moich badaniach w ramach programu grantowego **Study@Research**, w którym zajmuje się pogłębioną analizą skuteczności i niezawodności algorytmu ***Kyber CRYSTALS***.

W początkowym stadium moich badań skupię się na dogłębnym przeanalizowaniu pojęć związanych z teorią grup i pierścieni, aby następnie móc przestudiować działanie algorytmu CRYSTALS-Kyber mając ogląd na cały jego kontekst algebraiczny.

W głównej fazie, przy pomocy pakietów matematycznych oraz opanowanych przeze mnie języków programowania mam zamiar przetestować rozwiązania wykorzystywane w algorytmie.

Dzięki szerokiej znajomości wszystkich składowych algorytmu, w ostatniej fazie planuję podjąć próbę wyliczenia realnego bezpieczeństwa w.w. algorytmu

Literatura

Strona NIST:
National Institute of Standards and Technology prowadzi obszerną dokumentację i publikacje na temat Kyber oraz innych algorytmów kryptografii post-kwantowej. Można tam znaleźć oficjalne raporty, analizy i wyniki badań.

Książki:
Wiele książek na temat kryptografii i bezpieczeństwa danych zawiera rozdziały poświęcone algorytmom post-kwantowym, w tym Kyber. Przykładowe tytuły to "Post-Quantum Cryptography" oraz "Quantum Computing and Post-Quantum Cryptography".

Publikacje akademickie:
Portale takie jak Google Scholar oferują dostęp do licznych artykułów naukowych i prac badawczych na temat Kyber i jego zastosowań.

Członkostwo w organizacjach:
Organizacje takie jak International Association for Cryptologic Research (IACR) oferują zasoby, konferencje i publikacje na temat najnowszych trendów w kryptografii, w tym Kyber.