

Bezpieczeństwo danych oparte na kratkach i haszowaniu: Nowoczesny system zarządzania kluczami i podpisem cyfrowym.

Autorzy: Krzysztof Madajczak, Julia Sadecka,
Marcel Trzaskawka, Jakub Młócek



Liboqs

Liboqs to otwarto-źródłowa biblioteka napisana w C, implementująca zestaw **postkwantowych algorytmów kryptograficznych**, takich jak Kyber (KEM) oraz Dilithium, Falcon i SPHINCS+ (podpisy cyfrowe). Oferuje również **wrapper dla Pythona**. Biblioteka zapewnia spójne API, ułatwiając integrację i eksperymentowanie z kryptografią odporną na ataki kwantowe.

Wykorzystane algorytmy postkwantowe

Kyber

- Główny standard NIST do szyfrowania i wymiany kluczy.
- Bezpieczeństwo oparte na strukturach kratowych (Module-LWE).
- Cechuje się wysoką wydajnością i małymi rozmiarami kluczy.

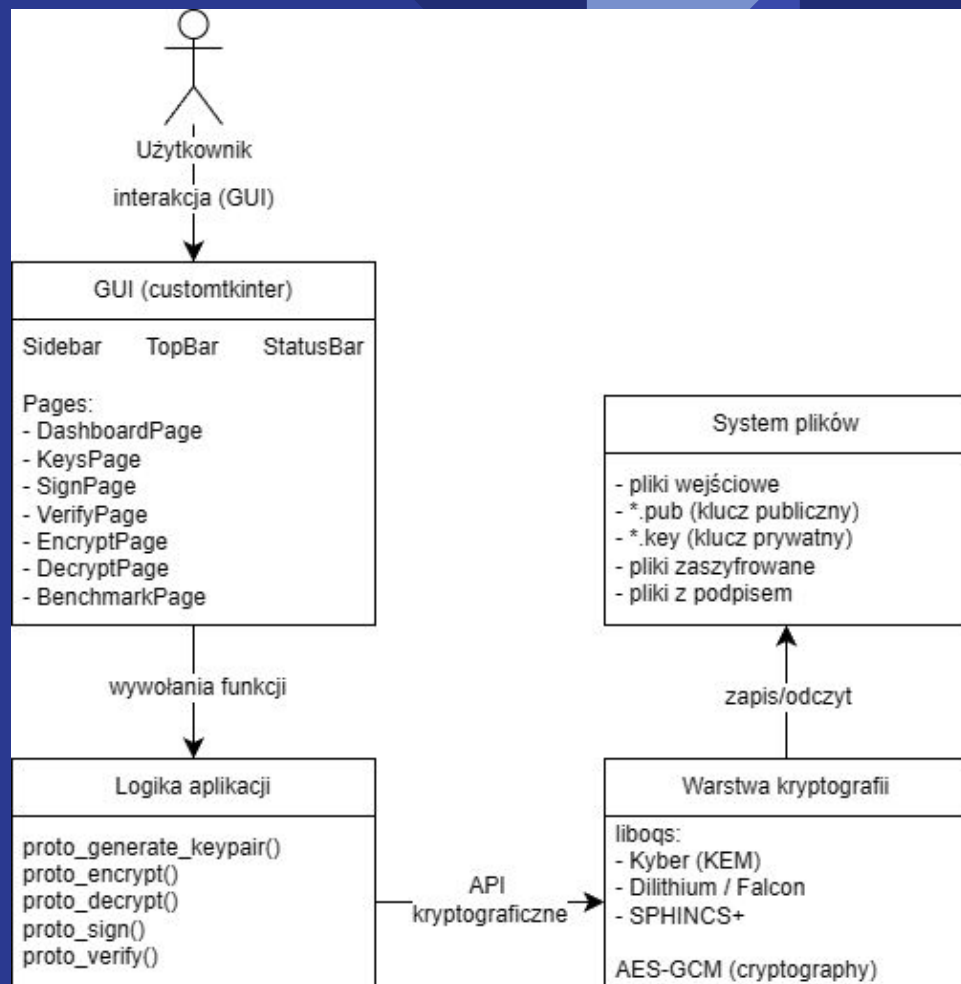
Dilithium i Falcon

- Dilithium - bazuje na kratowych problemach LWE i SIS. Rekomendowany przez NIST do podpisów cyfrowych
- Falcon - bazuje na kratowych sygnaturach NTRU. Rekomendowany przez NIST do podpisów cyfrowych w miejscach gdzie przepustowość łącza jest krytyczna. Trudniejszy do implementacji od Dilithium

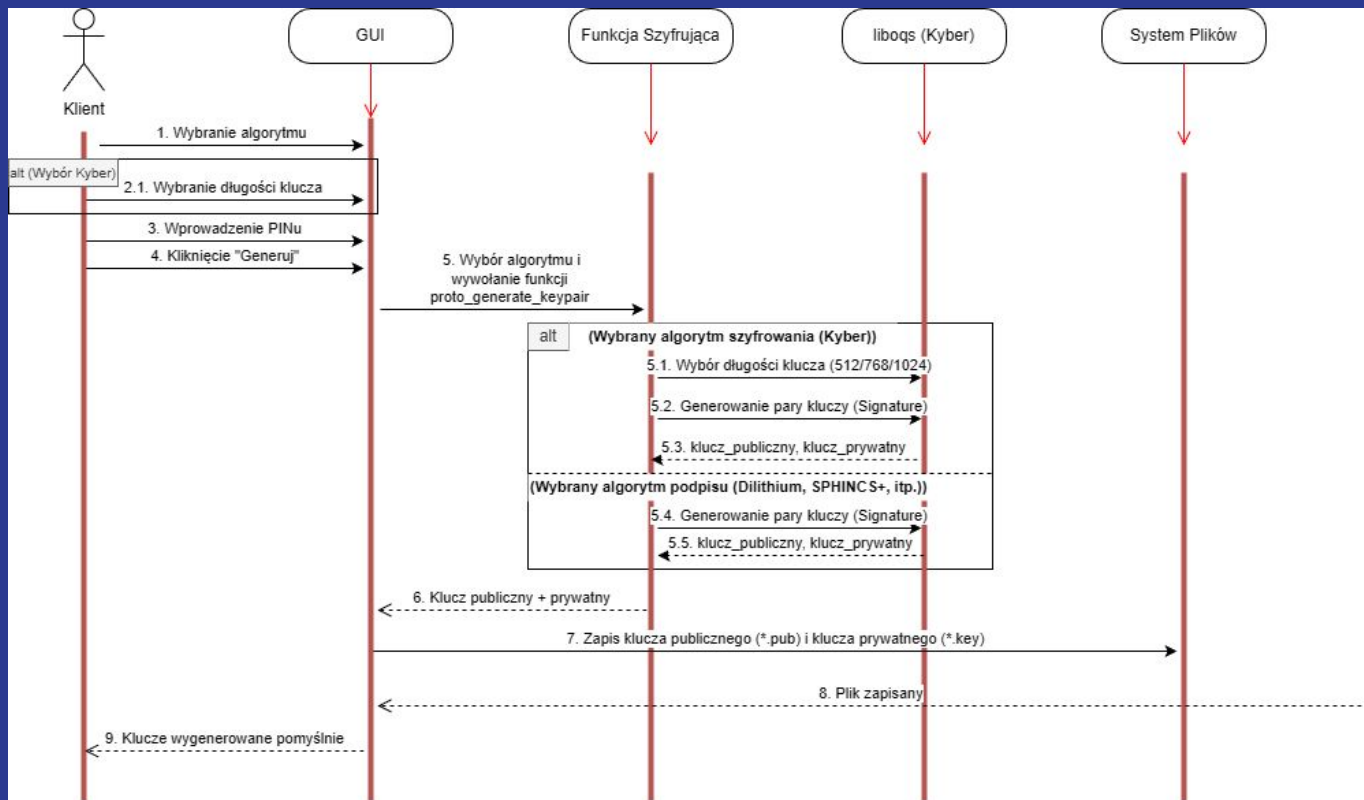
Cross i SPHINCS++

- SPHINCS++ - Algorytm podpisu cyfrowego oparty na funkcjach skrótu - alternatywa dla problemów kratowych jednak wolniejsza.
- Cross - Algorytm podpisu cyfrowego opartego na teorii kodów jednak nie jest finalnym standardem NIST

Diagram architektury systemu



Generowanie Kluczy



Generowanie Kluczy

Generate keys

Algorithm

Dilithium

Dilithium

Falcon

Cross

SPHINCS+

Kyber

Generate key pair

Generate keys

Algorithm

Falcon

PIN

Confirm PIN

Generate key pair

PINs do not match!

Generate keys

Algorithm

Falcon

PIN

Confirm PIN

Save Key Pair (Select base filename)

Directory: /home/julia

.cache	.local	Desktop
.conda	.pki	Documents
.config	.ssh	Downloads
.dotnet	.vscode	kyber_demo
.fonts	_oqs	liboqs
.gnupg	compose-demo	liboqs-python

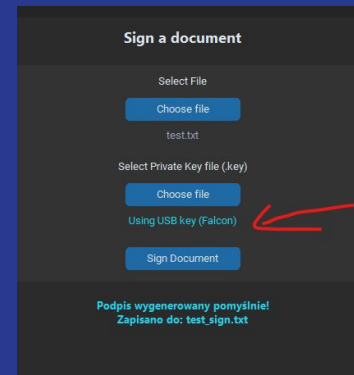
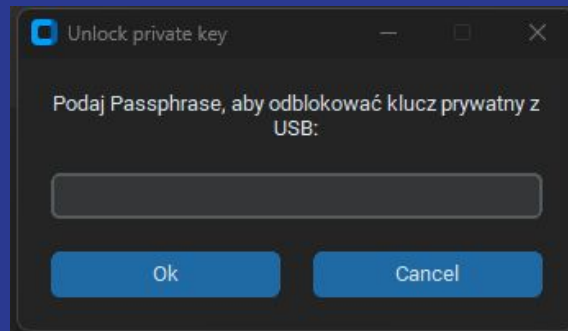
File name: f

Files of type: Pub Files (*.pub,*.key)

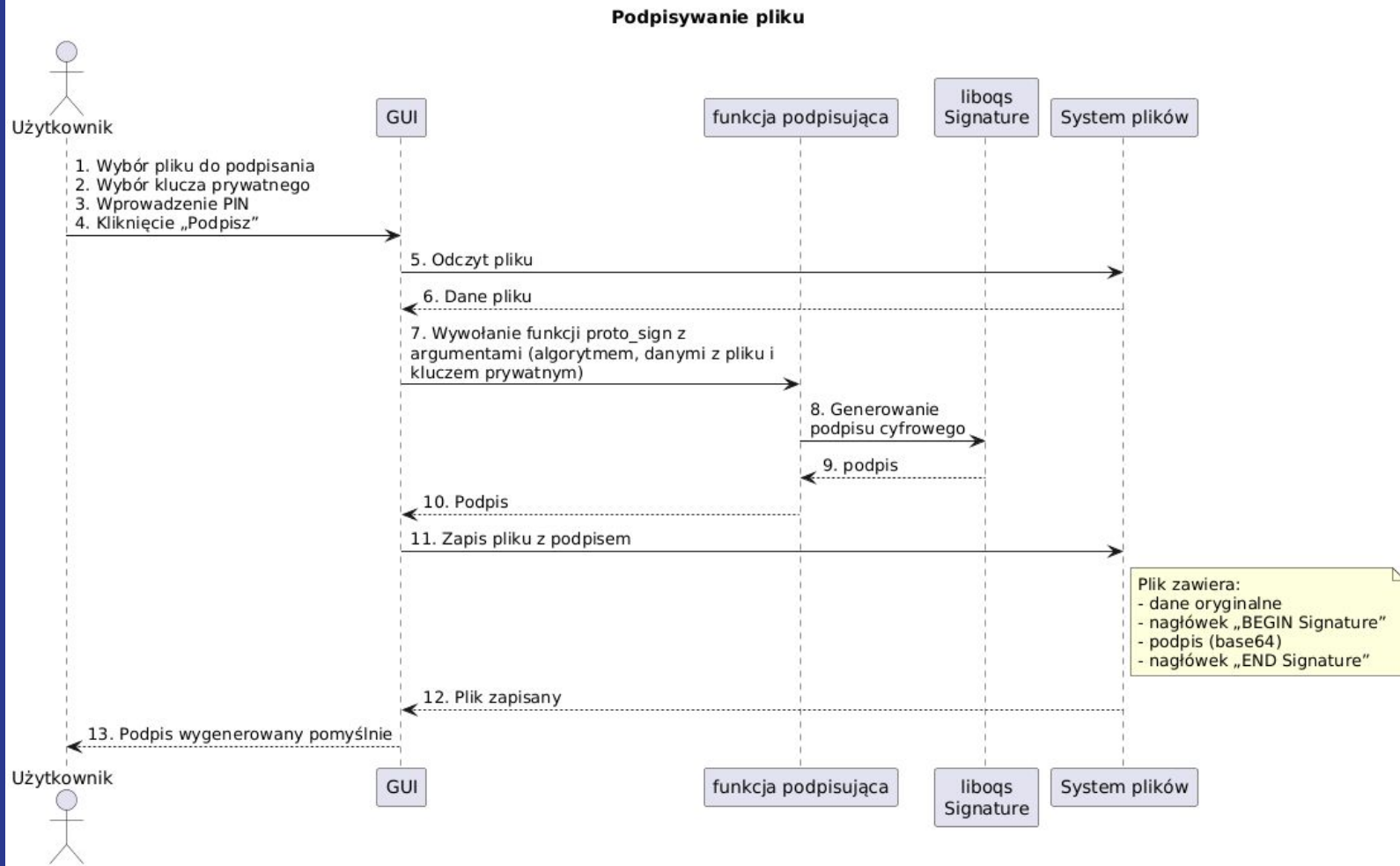
Save

Cancel

Wykorzystanie Pendrive



Podpis dokumentu



Podpis dokumentu

Sign a document

Select File

Choose file

No file selected

Select Private Key file (.key)

Choose file

No file selected

PIN

Sign Document

Sign a document

Select File

Choose file

hello_world.txt

Select Private Key file (.key)

Choose file

Select Key File

Directory: /home/julia

Desktop	Music	Templates
Documents	Pictures	venv
Downloads	post	Videos
kyber_demo	Public	falcon.key
liboqs	snap	
liboqs-python	studio	

File name:

Files of type: Pub Files (*.key)

Open **Cancel**

Verify Signature

Choose document

hello_world_sign.txt

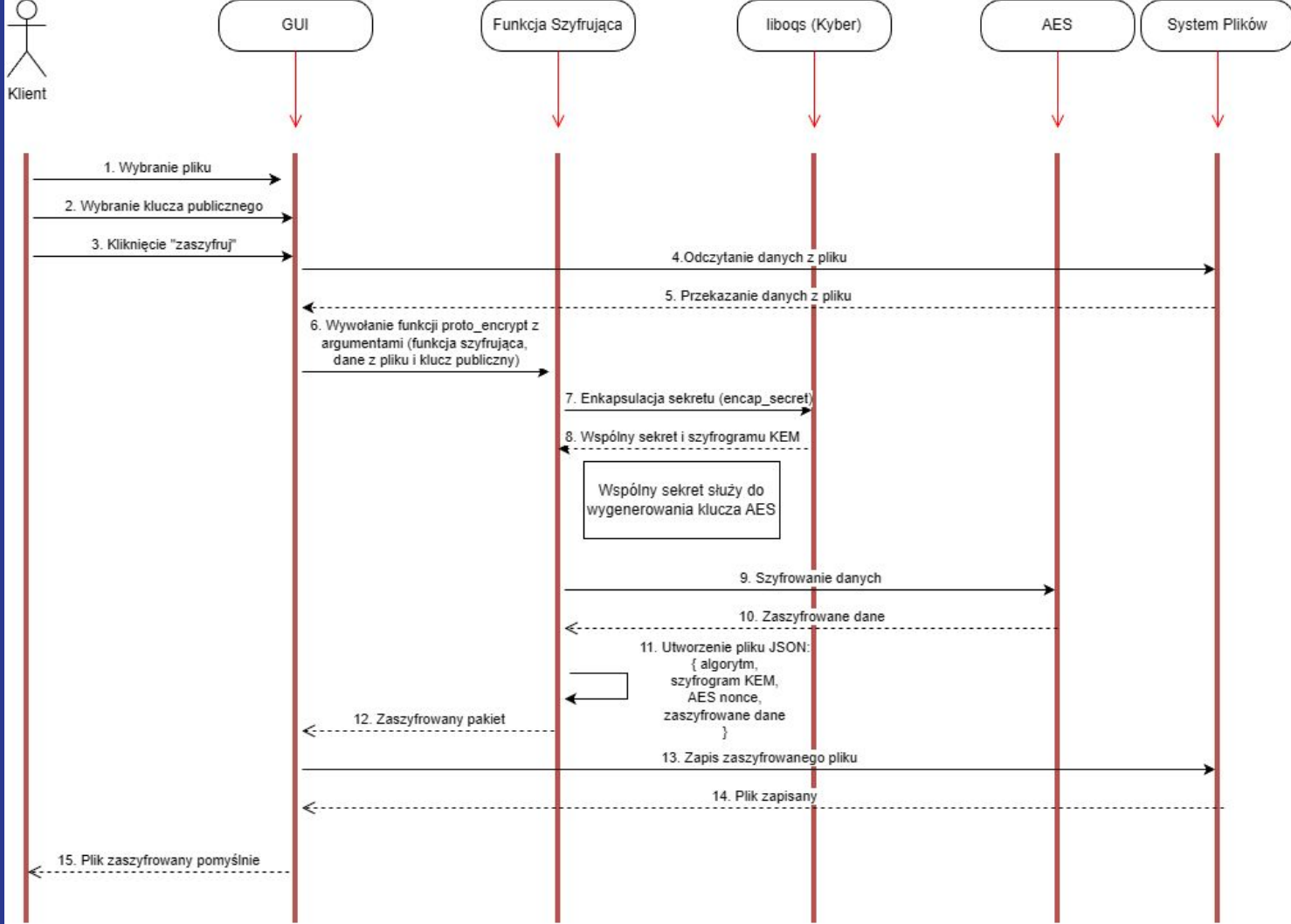
Choose public key

Key file: falcon.pub
Using Falcon algorithm

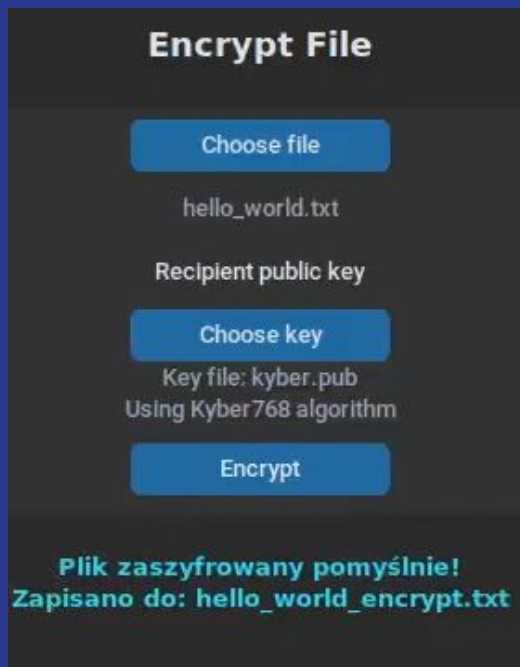
Verify

Podpis jest poprawny!

Szyfrowanie Dokumentu



Szyfrowanie Dokumentu



Benchmarki

Benchmarks

Benchmark available algorithms.

Algorithm Benchmark

Select Algorithm to Benchmark

Cross



- Dilithium
- Falcon
- Cross
- SPHINCS+
- Kyber
- Kyber512
- Kyber768
- Kyber1024

Results:

```
--- Starting Benchmark for Cross ---  
Iterations: 50  
Please wait...
```

```
[Key Generation]  
Total time: 0.0204s  
Avg time: 0.41 ms  
Throughput: 2448.11 ops/s
```

```
[Signing]  
Total time: 0.9444s  
Avg time: 18.89 ms  
Throughput: 52.94 ops/s
```

```
[Verification]  
Total time: 0.5526s  
Avg time: 11.05 ms  
Throughput: 90.48 ops/s  
Success rate: 50/50
```

```
--- Benchmark Complete ---
```

Drużyna



algorytmy
podpisu: Falcon i
Cross, benchmarki

algorytmy podpisu
SPHINCS++ i
Dilithium, headery

GUI, architektura i
logika aplikacji

algorytm szyfrujący
Kyber, dokumentacja

“Przed wyruszeniem w drogę należy zebrać drużynę”



Dziękujemy za uwagę