Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

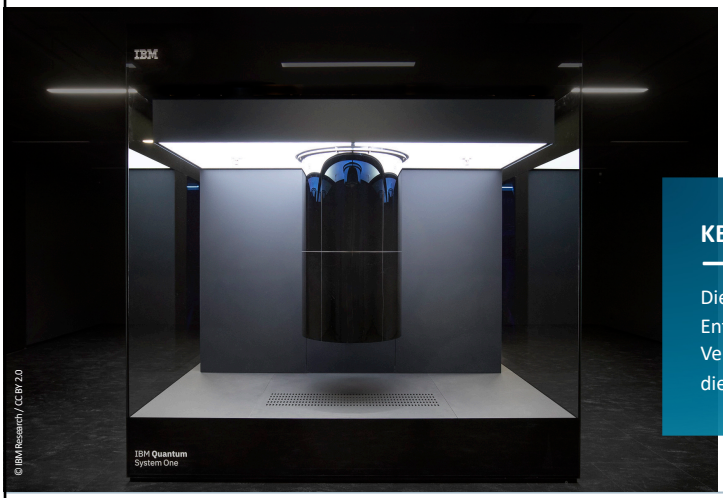
KBLS – Kryptobibliothek Botan für langlebige Sicherheit
Omnisecure 2022

22.06.2022
Tudor A. A. Soroceanu

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

1

Langlebige Sicherheit durch quantencomputerresistente Kryptografie



KBLS

Die Kryptobibliothek Botan wird erweitert, so dass Entwickler:innen auf Basis der von der Bibliothek zur Verfügung gestellten Funktionen Lösungen entwickeln können, die langlebige Sicherheit umsetzen.

2

Kryptobibliothek Botan

- Sprache: C++
- Offene Entwicklung auf GitHub
  - Simplified BSD License
- Kryptografische Protokolle und Primitive
  - TLS 1.2
  - X.509
  - AEAD Verfahren
  - Elliptic-Curve-Verfahren
  - PKCS#11
  - …

3

Kryptobibliothek Botan
BSI Projekt 197

Bundesamt für Sicherheit in der Informationstechnik

„Sichere Implementierung einer allgemeinen Kryptobibliothek“

- Ziel: Sichere Implementierung einer allgemeiner Kryptobibliothek
- Untersuchung und Aktualisierung von Botan v2.4 durch Rohde&Schwarz Cybersecurity
- Einfache Anwendung für Hersteller von VS-NfD Produkten
- Projektende 2017

4

KBLS
Projektpartner

Fraunhofer AISEC

nexenio

KBLS

ROHDE&SCHWARZ Cybersecurity

Technische Universität Berlin

5

KBLS
Projektziele

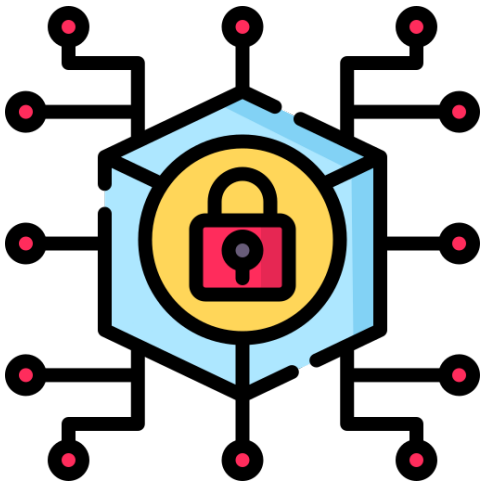
Projektziele

1 **Post-Quanten-Kryptografie**

2 **Kryptoagilität**

3 **Benutzbarkeit**

6



Post-Quanten-Kryptographie

7

NIST-Standardisierungsverfahren
Kandidaten für Runde 2

RQC
CRYSTALS-Kyber
CRYSTALS-Dilithium
Picinc
NTRU Prime
FALCON
Rainbow
Round5
BIKE
FrodoKEM
qTESLA
LAC
SABER
Classic McEliece
MQDSS
NewHope
LEDAcrypt
HQC
SIKE
Three Bears
NTS-KEM
SPHINCS+
NTRU
ROLLO
LUOV
GeMSS

8

Auswahl der Post-Quanten-Verfahren
Entwicklung von pqdb

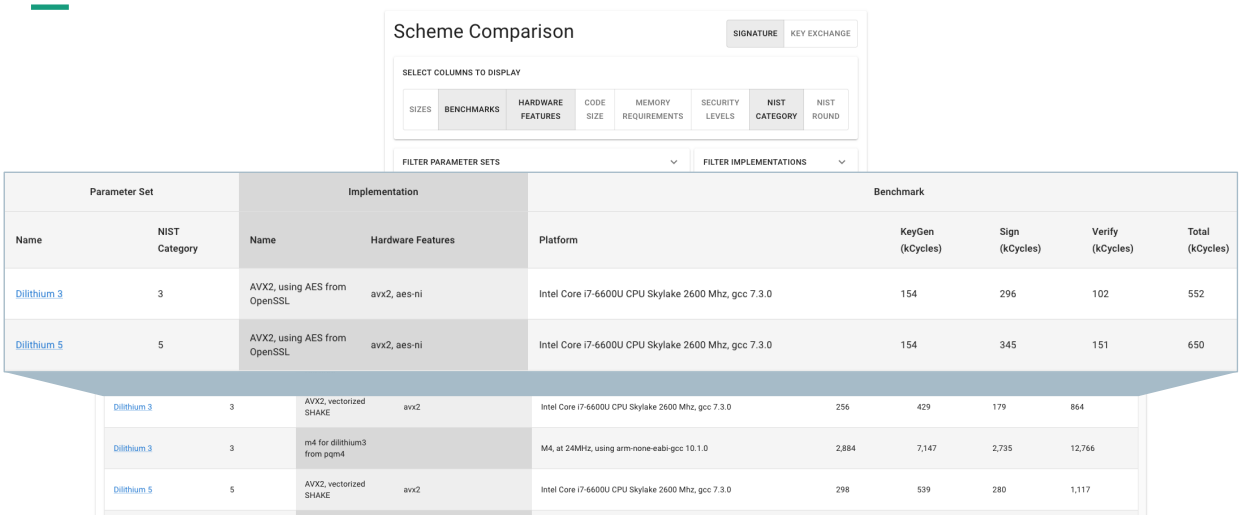
›› A comprehensive list of post-quantum crypto schemes and their properties. ‹‹

Entwicklung
https://github.com/cryptoeng/pqdb

Frontend
https://cryptoeng.github.io/pqdb

9

Vergleichsansicht



Parameter Set		Implementation		Benchmark				
Name	NIST Category	Name	Hardware Features	Platform	KeyGen (kCycles)	Sign (kCycles)	Verify (kCycles)	Total (kCycles)
Dilithium 3	3	AVX2, using AES from OpenSSL	avx2, aes-ni	Intel Core i7-6600U CPU Skylake 2600 Mhz, gcc 7.3.0	154	296	102	552
Dilithium 5	5	AVX2, using AES from OpenSSL	avx2, aes-ni	Intel Core i7-6600U CPU Skylake 2600 Mhz, gcc 7.3.0	154	345	151	650
Dilithium 3	3	AVX2, vectorized SHAKE	avx2	Intel Core i7-6600U CPU Skylake 2600 Mhz, gcc 7.3.0	256	429	179	864
Dilithium 3	3	m4 for dilithium3 from pqm4		M4, at 24MHz, using arm-none-eabi-gcc 10.1.0	2,884	7,147	2,735	12,766
Dilithium 5	5	AVX2, vectorized SHAKE	avx2	Intel Core i7-6600U CPU Skylake 2600 Mhz, gcc 7.3.0	298	539	280	1,117

10

KBLS – Aktueller Projektstand
Implementierung der PQC-Verfahren

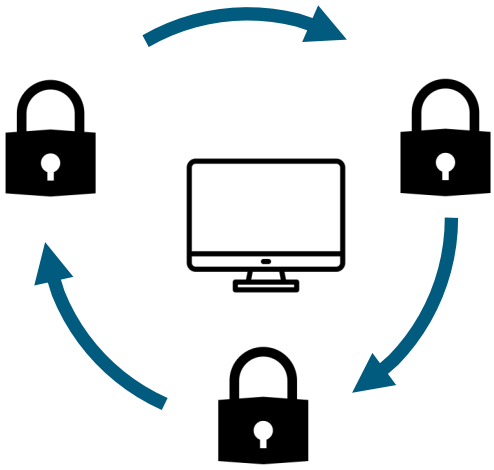
CRYSTALS Kyber

Implementierung beendet und in Botan integriert

CRYSTALS Dilithium

Implementierung beendet, Pull-Request noch offen

11



Kryptoagilität

12

KBLS
Demonstratoren

Demonstrator RSCS

Demonstrator neXenio

Post-Quantum TLS Without Handshake Signatures

Full version, March 15, 2022

Peter Schwabe
Max Planck Institute for Security and Privacy & Radboud University
peter@cryptojedi.org

Douglas Stebila
University of Waterloo
dstebila@uwaterloo.ca

Thom Wiggers
Radboud University
thom@thomwiggers.nl

13

Usability

14

KBLS
Usability

Dokumentation

Anwendungsbeispiele

15

KBLS
Einsatz und Weiterentwicklung von Botan

FLOQI – https://floqi.org/

- Einsatz in Signaturzertifikaten

BSI Projekt 480 – PQC@Thunderbird

- Verwendung von Botan für E2E-Verschlüsselung

BSI Projekt 481 – Pflege und Weiterentwicklung der Kryptobibliothek Botan

- Aktualisierung von Botan mit Schwerpunkt auf PQC

16

Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Kontakt

Tudor A. A. Soroceanu, M.Sc.
Department Secure Systems Engineering
Tel. +49 89 3229986-241
tudor.soroceanu@aisec.fraunhofer.de

kbls@aisec.fraunhofer.de

Fraunhofer AISEC
Breite Str. 12
14199 Berlin
www.aisec.fraunhofer.de

17

Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Vielen Dank für Ihre Aufmerksamkeit

18