MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

cesnet

VŠB TECHNICKÁ UNIVERZITA OSTRAVA

NESPOQ

Kybernetická bezpečnost sítí v postkvantové éře

Projekt výzvy MVČR Impakt VJ01010008

ZÁKLADNÍ INFORMACE O PROJEKTU

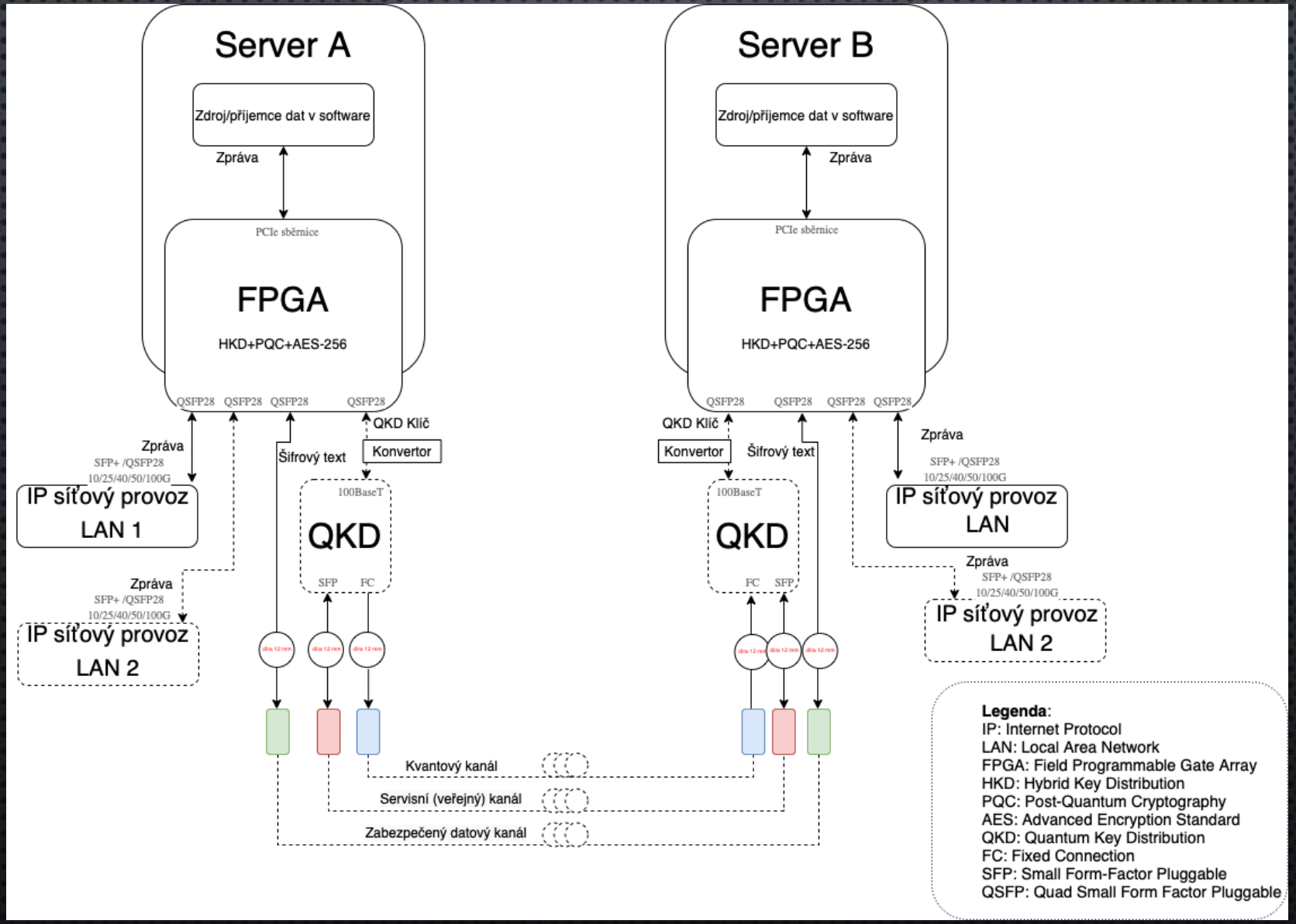
- **Název projektu: Kybernetická bezpečnost sítí v postkvantové éře**
- Začátek projektu: 01/2021
- Konec projektu: 12/2025
- Hlavní řešitel: doc. Ing. Jan Hajný, Ph.D. (VUT v Brně)
- Aplikační garant: NÚKIB

NÚKIB

Základní informace o projektu

- Účastníci projektu
  - **Vysoké učení technické v Brně** - Fakulta elektrotechniky a komunikačních technologií
    - Hlavní řešitel: doc. Ing. Jan Hajný, Ph.D.
    - Vedoucí týmu optických sítí: doc. Ing. Petr Münster, Ph.D.
    - Manažer, komunikace s poskytovatelem: doc. Ing. Lukáš Malina, Ph.D.
    - Oblasti: Postkvantová kryptografie, FPGA, optické sítě
  - **CESNET**
    - Další řešitel: Ing. Josef Vojtěch, Ph.D.
    - Oblasti: optické sítě, QCI, ultrapřesné časování
  - **Vysoká škola báňská** - Technická univerzita Ostrava - Fakulta elektrotechniky a informatiky
    - Další řešitel: prof. Ing. Miroslav Vozňák Ph.D.
    - Oblasti: kvantová kryptografie, QCI

VÝSLEDKY PROJEKTU



PLNĚNÍ ČINNOSTÍ (AKTIVIT) ČASOVÉHO HARMONOGRAMU PROJEKTU

Plán na rok 2021

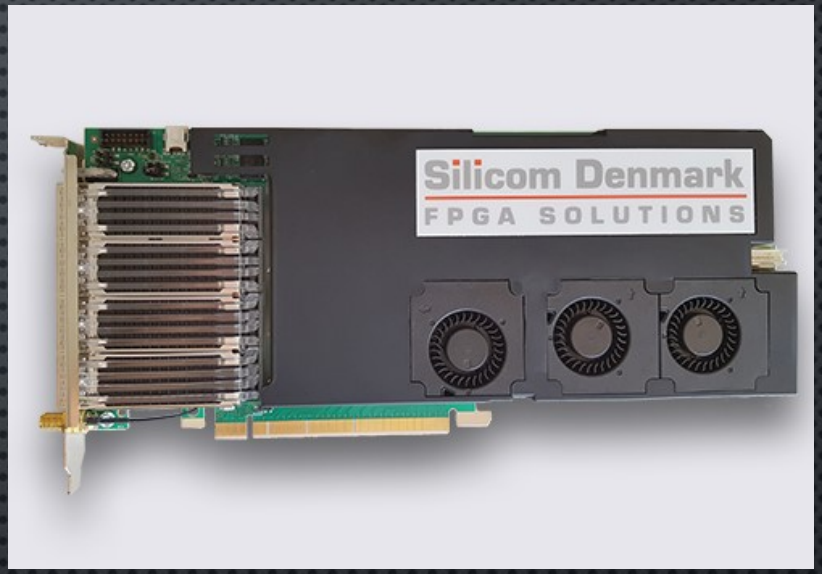
- Analýza rizik a identifikace požadavků – Zpráva 1.1
- Příprava pořízení hardwaru pro kvantový subsystém (QKD) – Zpráva 1.2
- QKD - analýza technologií, aktualizace state of the art – Zpráva 1.3
- Ověření základních parametrů QKD systému a požadavků – Zpráva 1.4
- Návrh bezpečnostní koncepce
- Definice parametrů pro testbed
- Sestavení testbedu
- Návrhy nových přístupů QoS pro QKD

Etapa 1: Analýza rizik a identifikace požadavků (VUT)

- **Analýza rizik**
- Projektová rizika řízena sdíleným nástrojem (Ing. Horváth)
- Analýza rizik spojená s návrhem systému uvedena ve **zprávě 1.1**:
  - Analýza bezpečnostních hrozeb a útoků na kryptografické a zabezpečovací systémy – zaměření na PQC a QKD systémy a hardwarové implementace
  - Sledování dobré praxe (ETSI TVRA, STRIDE, ENISA, NIST), známých incidentů a současného stavu
  - Systémové (návrhové), implementační, provozní a další hrozby
  - Zhodnocení možností pasivního a aktivního útočníka
  - Vyhodnocení pravděpodobnosti výskytu a míry závažnosti (nízká, střední, vysoká, kritická)

ETAPA 1: ANALÝZA RIZIK A IDENTIFIKACE POŽADAVKŮ (VUT)

- **Identifikace požadavků**
- Identifikace požadavků uvedena ve **zprávě 1.1**:
  - Kryptografické komponenty
  - Hardware šifrátorů – FPGA
  - Hardware QKD
  - Výpočetní prostředky – servery



Algorithm	Mathematical problem the algorithm is based on	Secret key size [bytes]	Public key size [bytes]	Time needed to establis keys [µs]	Code available?	Language of the code	Software implementations	Hardware implementations
McEliece	Hardness of decoding a linear code (Goppa code)	?	1046738 [39]	?	yes [42]	C	SUPERCOP [42]	Artix-7 FPGA Virtex-7 FPGA [42]
NTRU	RLWE problem	1422 [44]	1140 [44]	?	yes [43]	Python C	Open Quantum Safe AVX2 [43]	?
CRYSTALS-KYBER	MLWE problem	3168 [40]	1568 [40]	1.5 K (ASIC) [40]	yes [40]	C	PQClean BoringSSL SUPERCOP [40]	ASIC [40]
SABER	MLWR problem	2304(1344) [41]	992 [41]	21.8 (UltraScale+) [45, p.20]	yes [41]	C	C AVX Cortex-M0 Cortex-M4 [41]	Artix-7 FPGA UltraScale+ FPGA [41]

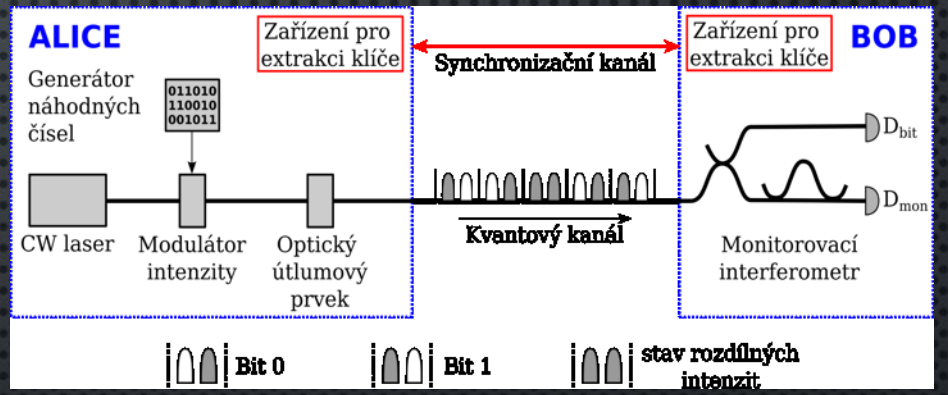
Etapa 2: Příprava pořízení hardwaru pro kvantový subsystém (VUT)

- Prvotní průzkum trhu pro zjištění výrobců QKD systémů.
  - Respektovat varování NÚKIB.
  - Požadované parametry systému vs. doba dodání.
- Komerčně dostupná řešení:
  - ID Quantique, Qrate, Toshiba, QUBITEKK, KETS, QUASKY, MagiQ, QuantumCTek, Quintessence Labs.
- Veřejným výběrovým řízením přes tenderarenu byl zakoupen systém IDQ Clavis3.
  - Detailní přehled požadovaných parametrů (viz zpráva – Etapa 1.2).

Navrhované sestavy QKD Serverů		
Model	Clavis3	MUX QKD
Výrobce	IDQ	Toshiba
QKD protokol	COW	T12
Rychlost generování klíče	1,4 kb/s	4 kb/s
Maximální útlum (dB)	14	17
Dosah kvantového kanálu (km)	58	70
Řešení	Samostatně	Samostatně
Grafické rozhraní (GUI)	Ano	Ano
ETSI API	Ano	Ano
Velikost (19”ATCA šasi)	4U	3U
Integrovaný šifrátor	Ne	Ne
QRNG	Ano	Ano
Topologie	Bod-Bod	Bod-Bod
Podpora WDM	Ano	Ano
Kvantový kanál	1551,72 nm	1310 nm
Klasický kanál 1	1563,047 nm	1550 nm
Klasický kanál 2	1563,863 nm	———

Etapa 3: QKD - analýza technologií, aktualizace state of the art (CESNET)

- Analýza možností a slabin QKD technologií
  - Vychází z poznatků etapy 1.2 a rešerše dostupných zdrojů
- State of the art
  - Přehled problematiky
  - QKD projekty a aktivity u nás i ve světě
  - Standardy, protokoly (BB84, COW, T12)
  - Bezpečnostní rizika, konkrétní útoky, zranitelnosti a hrozby včetně protiopatření
- Nový typ útoku na COW (implementuje pořízené zařízení)
  - Zero-error attack – Útok Eve negeneruje chyby, klíč ale sestavit nejde
  - Výrobce pracuje na opravě (firmware update)



Etapa 4: Ověření základních parametrů QKD systému a požadavků (VUT)

- Dodané řešení - Cockpit
  - Aplikace podporuje jenom Centos7
  - Ukazuje data jenom v Cockpit aplikaci
  - Data ukládá do CSV
  - Nutno ukončit aplikaci pro zpracování CSV
- Vyvinuto nové řešení
  - Data čtena pomocí SNMPv3
  - Uložená v InfluxDB
  - Zobrazená pomocí projektu Grafana
  - Webová aplikace
  - Data v reálném čase a dlouhá historie, možnost volby časového okna

ETAPA 4: OVĚŘENÍ ZÁKLADNÍCH PARAMETRŮ QKD SYSTÉMU A POŽADAVKŮ (VUT)

Zhodnocení dosavadního průběhu projektu a budoucí práce

- V rámci dosavadního průběhu byly splněny etapy 1 až 4 podle harmonogramu.
- zvolen a pořízen klíčový hardware pro řešení projektu.
- Dosažení 2 publikačních výsledků typu RIV-D (Secrypt 2021 a EEICT 2021).
- Uspořádání workshopu pro aplikačního garanta probíhá (W).
- Doposud evidovány 3 změny projektu (2 nepodstatné, 1 podstatná) – změny byly schváleny.

- Do konce roku 2021 budou dokončeny zbylé etapy 5 až 8.
- V příštím roce pokračování podle harmonogramu beze změn (měření primitiv PQC a parametrů QKD, rozpracování případů užití, Implementace QKD řízení atd.).

DĚKUJI ZA POZORNOST

CESNET, z. s. p. o.

Ing. Josef Vojtěch, Ph.D.

Zikova 4

160 00 Praha 6

+420 234 680 377

VUT v Brně

doc. Ing. Jan Hajný, Ph.D.

Technická 12

616 00 Brno

+420 608 823 522

VŠB TUO

prof. Ing. Miroslav Vozňák, Ph.D.

17. listopadu 2172/15,

Ostrava-Poruba 708 00

+420 603 565 965