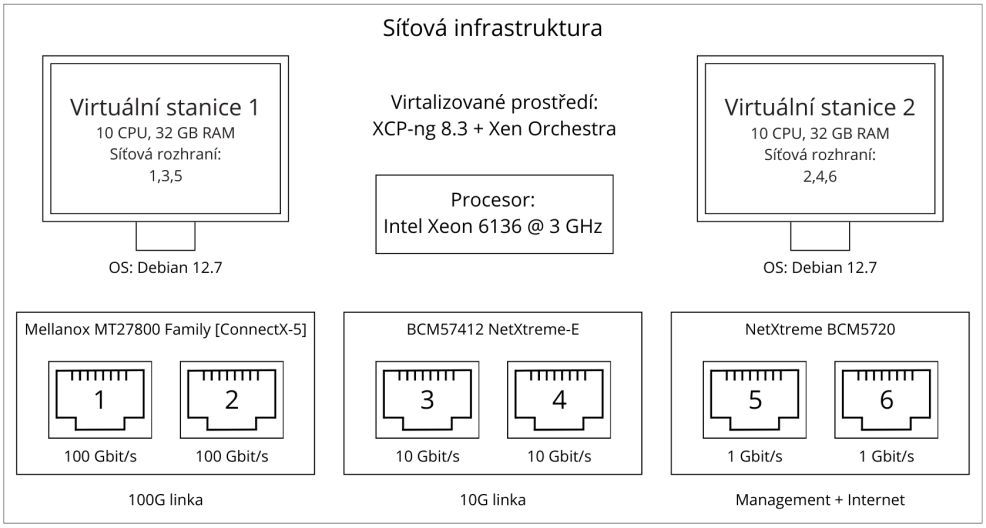
1 Implementace testbedu, testované prvky a metodika měření

1.1 Úvod

Protokol shrnuje postup a výsledky získané při výkonových testech postkvantových šifrátorů. Testované prvky zahrnovaly šifrátory založené na platformě FPGA, které byly vyvíjeny na VUT FEKT, a srovnání s komerčně dostupnými firewally Juniper SRX4200. Testování na platformě FPGA zahrnovalo dva různé typy šifrátorů – Xilinx UltraScale+ a Agilex hardware. Výkonové testy byly realizovány především v podobě testů propustnosti, přičemž teoretické maximum bylo 100 Gbit/s pro FPGA a 10 Gbit/s pro Junipery. Schopnosti šifrátorů byly dále ověřeny v dlouhodobých testech a v reálných aplikacích.

1.2 Praktická implementace testbedu

Pro praktické řešení byla sítě využita virtualizace. Virtualizované prostředí zahrnovalo hypervizora XCP-ng 8.3 s grafickým rozhraním Xen Orchestra. Zde byly vytvořeny dvě virtuální stanice, které představovaly koncové body komunikace a mezi kterými byly utvářeny linky pro síťovou komunikaci. Do těchto linek byly postupně zapojovány testované prvky. Každé stanici bylo přiděleno 10 jader CPU (Intel Xeon 6136), 32 GB RAM a příslušná síťová rozhraní. Tester obsahoval více síťových karet, každou disponující dvěma rozhraními, což umožňovalo realizaci spoje mezi virtuálními stanicemi o daných rychlostech. Realizaci testeru blíže prezentuje obr. č. 1.1.

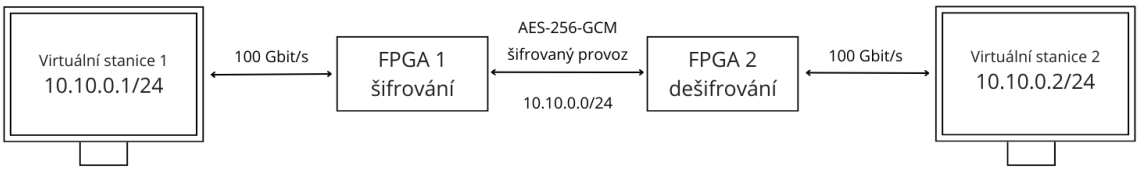


Obr. 1.1: Vizualizace topologie pro testování s šifrátory na platformě FPGA.

1.3 Testované prvky

1.3.1 Platforma FPGA

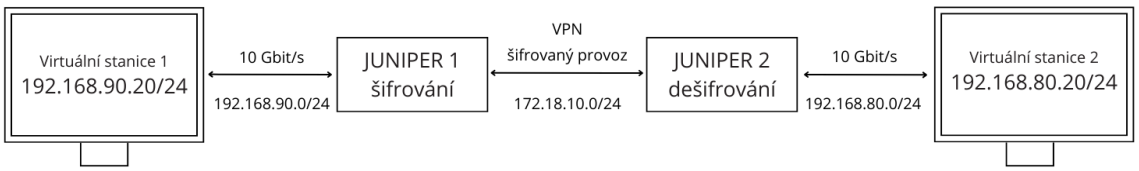
Platforma FPGA nabízí flexibilní a efektivní řešení pro různé výpočetní úlohy, jelikož ji lze programovat přímo pro danou činnost. Efektivita platformy spočívá v akceleraci a paralelním zpracování s využitím hardwarových obvodů. Testované šifrátory FPGA byly vyvíjeny na VUT FEKT a pro šifrovací algoritmus byl využit AES v módu GCM a délkou klíče 256 bitů. Šifra AES-256-GCM nabízí autentizované šifrování dat, je vhodná pro vysoké propustnosti a zároveň je také kvantově odolná. V rámci práce byly testovány dva různé typy šifrátorů zahrnující Xilinx UltraScale+ a Agilex harware. Realizace 100G linky proběhla s využitím síťové karty Mellanox MT27800 ConnectX-5. Předpokladem pro výsledky šifrovaného provozu pomocí FPGA byla žádná či minimální limitace oproti hodnotám propustnosti provozu bez šifrování. Topologii pro testování propustností šifrátorů FPGA zobrazuje obr. č. 1.2.



Obr. 1.2: Vizualizace topologie pro testování s šifrátory na platformě FPGA.

1.3.2 Firewally Juniper SRX4200

Firewally Juniper SRX4200 jsou komerční síťové prvky. Podporují standard RFC 8784, což umožňuje realizovat kvantově bezpečné spojení pomocí IPsec a IKEv2. Firewally SRX4200 disponují 10G rozhraním, testování tedy probíhalo na samostatné lince o teoretické rychlosti 10 Gbit/s. V případě testeru se jednalo o rozhraní 10G síťové karty Broadcom BCM57412. Pro zhotovení testů byly využity dva firewally, mezi nimiž byl ustanoven kvantově odolný VPN spoj. Topologii pro testování propustností s šifrátory Juniper prezentuje obr. č. 1.3.



Obr. 1.3: Vizualizace topologie pro testování s šifrátory Juniper.

1.4 Metodika testování

Testování propustnosti bylo realizováno za pomoci nástroje iPerf. Nástroj iPerf nabízí různé verze, díky kterým lze testovat jednovláknový výkon (iPerf3) nebo vícevláknový výkon (iPerf2). Při realizaci výkonových testů byl iPerf používán v obou verzích. Přidělení konkrétního počtu jader procesu `iperf` při testech, které to vyžadovaly, bylo realizováno pomocí nástroje `taskset`. Úvodní testy nešifrovaného provozu zahrnovaly testy pro různé velikosti MTU a počty užitých CPU jader. Velikosti MTU byly zvoleny následovně:

- 576 B – minimální velikost IPv4 paketu, může sloužit jako referenční hodnota, pokud by docházelo k fragmentaci,
- 1300 B – referenční velikost pro minimální velikost IPv6 paketů (1280 B) nebo šifrovaný provoz, kdy se mohou enkapsulací přidávat nová záhlaví apod.,
- 1500 B – běžná hodnota pro Ethernet/Ethernet II (1518 B),
- 9000 B – používané ve vysokorychlostních infrastrukturách.

Doba trvání jednotlivých testů byla 30 sekund. Tato délka byla zvolena kvůli dostatečné vypovídající hodnotě o aktuální dosažitelné propustnosti. Každý test byl opakován minimálně třikrát, čímž byla ověřena jednoznačnost hodnot. Pro každou kombinaci MTU, počtu jader CPU a typu provozu byla nejprve nalezena strukura příkazu, kterou bylo dosaženo maximálního vytížení CPU jader tak, aby zároveň nedocházelo k přetížení. Pro každou linku byly nejprve realizovány testy nešifrovaného provozu – přímé propojení virtuálních stanic. Testy šifrovaného provozu zahrnovaly postupné zapojování testovaných prvků do dané linky. Tyto testy byly zaměřeny především na nejvyšší výkon (využití všech CPU jader). Pro referenci byly testy šifrovaného provozu provedeny i pro jednojádrový výkon a výsledné hodnoty těchto testů jsou uvedeny v tabulkách spolu s hodnotami maximálního výkonu. Hodnoty šifrovaného provozu jsou zároveň v podobě průměrné hodnoty, vypočtené ze všech provedených testů, s odchylkou, která značí získanou hodnotu, která byla nejvíce vzdálená a průměrné. Testované kategorie MTU byly v průběhu testování přizpůsobovány schopnostem šifrátorů. Změny MTU byly prováděny na virtuálních stanicích příkazem `sudo ip link set dev <interface> <velikost>`.

Hodnota latence byla testována pomocí nástrojů `ping` a `traceroute`. Analýza provozu probíhala zachycením provozu v programu Wireshark v prostředí virtuálních stanic.

2 Realizace zátěžových testů

2.1 Platforma FPGA

V úvodní fázi byly zhotoveny testy propustnosti nešifrovaného provozu 100G linky. Testy zahrnují hodnoty rychlostí pro různá CPU jádra a velikosti MTU. Následující dvě tabulky prezentují výsledky pro TCP a UDP provoz po provedení optimalizace.

Tab. 2.1: Výsledky testů propustnosti pro nešifrovaný TCP provoz.

Počet CPU jader	MTU [B]			
	576	1300	1500	9000
1	14,0 Gbit/s	26,0 Gbit/s	30,6 Gbit/s	32,4 Gbit/s
2	24,4 Gbit/s	39,4 Gbit/s	46,5 Gbit/s	55,1 Gbit/s
4	32,1 Gbit/s	63,6 Gbit/s	64,7 Gbit/s	69,1 Gbit/s
6	34,0 Gbit/s	72,8 Gbit/s	76,0 Gbit/s	92,1 Gbit/s
8	36,1 Gbit/s	78,4 Gbit/s	82,4 Gbit/s	96,1 Gbit/s
10	38,9 Gbit/s	81,7 Gbit/s	85,4 Gbit/s	96,4 Gbit/s

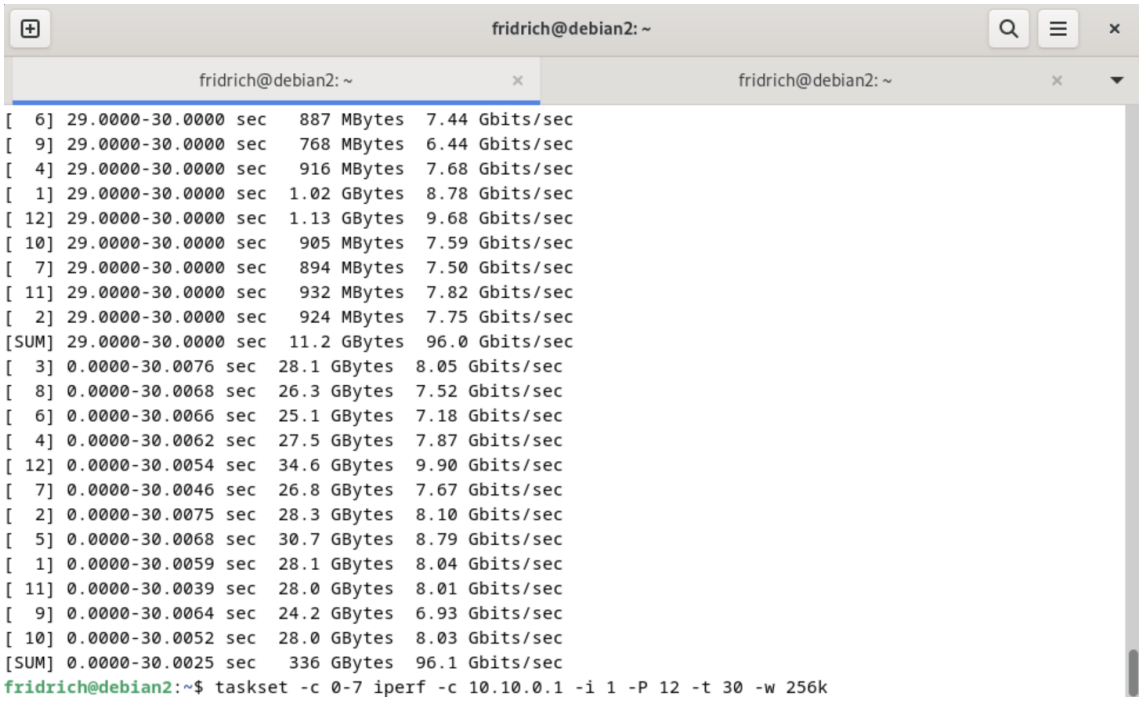
Pro běžnou velikost MTU bylo dosaženo 85 Gbit/s s využitím všech jader, která byla k dispozici. Pro velikost MTU 9000 B bylo dosaženo 96,4 Gbit/s – téměř teoretického maxima. Dále byly realizovány testy UDP provozu.

Tab. 2.2: Výsledky testů propustnosti pro nešifrovaný UDP provoz.

Počet CPU jader	MTU [B]			
	576	1300	1500	8000
1	1,3 Gbit/s	3,1 Gbit/s	3,6 Gbit/s	15,7 Gbit/s
2	2,3 Gbit/s	5,9 Gbit/s	5,8 Gbit/s	28,9 Gbit/s
4	4,5 Gbit/s	10,6 Gbit/s	11,5 Gbit/s	52,6 Gbit/s
6	6,3 Gbit/s	15,1 Gbit/s	16,9 Gbit/s	75,2 Gbit/s
8	7,8 Gbit/s	18,6 Gbit/s	22,7 Gbit/s	95,2 Gbit/s
10	9,4 Gbit/s	21,4 Gbit/s	24,4 Gbit/s	∼100,0 Gbit/s

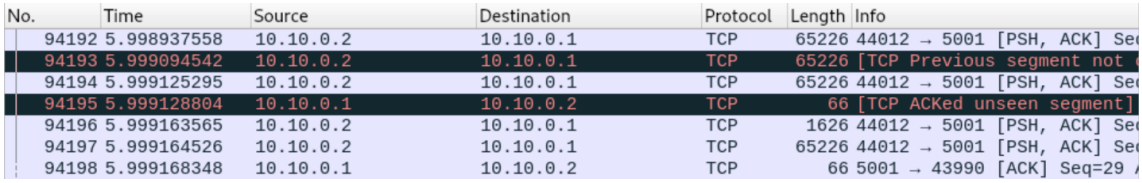
Propustnost UDP provozu byla tedy výrazně nižší v porovnání s TCP provozem. Pro UDP provoz byla největší testovaná velikost MTU 8000 B, protože při užití všech deseti jader procesoru již rychlost přesahovala teoretické maximum. Při testech s většími MTU bylo zjevné zvýšení propustnosti díky nižší frekvenci generování datagramů. Nedocházelo tak k zahlcení procesoru, takže byly pro 8 a 10 jader, při MTU 8000 B, rychlosti srovnatelné s hodnotami TCP provozu.

Průběh testování TCP provozu spolu s užitým příkazem pro dosažení maximální propustnosti osmijádrového výkonu a velikost MTU 9000 B zobrazuje obr. č. 2.1.



Obr. 2.1: Struktura příkazu iPerf a průběžné hodnoty propustnosti TCP – 8 CPU.

Důležitými parametry pro dosažení těchto propustností byly optimální počet proudů `-P` a velikost TCP okna `-w`. V rámci testování proběhla také analýza provozu programem Wireshark za účelem ověření, že komunikace probíhala dle interpretace iPerf. Provoz zachycený programem Wireshark prezentuje obr. č. 2.2



Obr. 2.2: Ukázka testovacího TCP provozu s maximálním vytížením.

Celková délka zasílaných segmentů byla 65226 B. Jednalo se o vliv offload mechanismů, kdy dělení segmentů do velikosti jednotlivých paketů probíhalo až na úrovni síťové karty. Rozdílné porty identifikovaly různé paralelní proudy, jejichž počet byl specifikován v `iperf` příkazu.

Testování UDP provozu probíhalo obdobně. Při testech UDP provozu bylo nutné v příkazu určit typ provozu `-u`, šířku pásma `-b 100G`, optimální počet proudů `-P` a správnou velikost datagramu `-l` pro dosažení maximální propustnosti. Hodnota

latence 100G linky, testovaná pomocí příkazu `ping`, se pro 10+ dotazů a opakovaná měření, pohybovala v rozmezí 0,231–0,288 ms před i po přidání šifrátorů do linky.

Po zhotovení testů nešifrovaného provozu 100G linky byly dále realizovány testy šifrovaného provozu. Výsledky testů propustnosti jsou prezentovány v následujících čtyřech tabulkách. Testy byly zaměřeny na nejvyšší výkon – užití všech 10 CPU jader. Pro referenci byly realizovány také testy jednojádrového výkonu. Nejvyšší testovaná velikost MTU je 1500 B, šifrátory mají velikost MTU implicitně nastavenou na hodnotu 1526 B a větší jednotky jsou považovány za neplatné.

Tab. 2.3: Výsledky testů propustnosti, TCP – FPGA UltraScale+ (Mango).

Počet CPU jader	MTU [B]		
	576	1300	1500
1	14,0 ± 0,9 Gbit/s	23,5 ± 1,4 Gbit/s	25,7 ± 2,0 Gbit/s
10	42,0 ± 5,4 Gbit/s	75,2 ± 2,6 Gbit/s	79,6 ± 3,6 Gbit/s

Tab. 2.4: Výsledky testů propustnosti, UDP – FPGA UltraScale+ (Mango).

Počet CPU jader	MTU [B]		
	576	1300	1500
1	1,3 ± 0,2 Gbit/s	3,1 ± 0,4 Gbit/s	3,4 ± 0,2 Gbit/s
10	10,4 ± 0,4 Gbit/s	22,5 ± 2,4 Gbit/s	26,5 ± 2,1 Gbit/s

Tab. 2.5: Výsledky testů propustnosti, TCP – FPGA Agilex (Intel).

Počet CPU jader	MTU [B]		
	576	1300	1500
1	15,2 ± 0,5 Gbit/s	23,5 ± 1,0 Gbit/s	25,3 ± 1,5 Gbit/s
10	43,3 ± 2,0 Gbit/s	81,3 ± 1,0 Gbit/s	85,8 ± 1,4 Gbit/s

Tab. 2.6: Výsledky testů propustnosti, UDP – FPGA Agilex (Intel).

Počet CPU jader	MTU [B]		
	576	1300	1500
1	1,3 ± 0,1 Gbit/s	2,9 ± 0,5 Gbit/s	3,5 ± 0,1 Gbit/s
10	10,5 ± 0,1 Gbit/s	23,2 ± 1,6 Gbit/s	26,5 ± 2,3 Gbit/s

Rychlosti dosažené při testech propustnosti byly srovnatelné s hodnotami nešifrovaného provozu. Limitace provozu šifrátory byla maximálně v řádu jednotek Gbit/s.

Pro šifrátory FPGA Intel byl dále testován režim QKD a funkčnost šifrátorů v dlouhodobém intervalu, protože v průběhu testování docházelo k desynchronizaci klíčů. To bylo vyřešeno komunikací s vývojáři FPGA a průběžnými aktualizacemi firmware. Výsledné hodnoty provozu při QKD prezentují následující dvě tabulky.

Tab. 2.7: Výsledky testů propustnosti, TCP – FPGA Agilex (Intel), QKD.

Počet CPU jader	MTU [B]		
	576	1300	1500
1	14,9 ± 1,1 Gbit/s	23,3 ± 2,5 Gbit/s	24,6 ± 1,8 Gbit/s
10	43,0 ± 0,2 Gbit/s	81,7 ± 2,7 Gbit/s	84,0 ± 2,8 Gbit/s

Tab. 2.8: Výsledky testů propustnosti, UDP – FPGA Agilex (Intel), QKD.

Počet CPU jader	MTU [B]		
	576	1300	1500
1	14,9 ± 1,1 Gbit/s	23,3 ± 2,5 Gbit/s	24,6 ± 1,8 Gbit/s
10	43,0 ± 0,2 Gbit/s	81,7 ± 2,7 Gbit/s	84,0 ± 2,8 Gbit/s

Režim QKD neměl na výsledné propustnosti vliv. Hodnoty pro TCP i UDP provoz byly v rámci odchylek téměř shodné s předchozími testy.

Dlouhodobé testy byly realizovány pro časové intervaly 2, 6 a 20 hodin. Jednalo se o testy s vytížením jednoho jádra CPU na každé stanici, kdy bylo cílem úspěšně realizovat provoz po celý časový interval. Tyto testy byly provedeny pro provoz v režimech s i bez QKD a proběhly úspěšně. Průměrné rychlosti uvádí tab. č. 2.9.

Tab. 2.9: Výsledky dlouhodobě šifrovaného provozu – FPGA Intel.

Režim provozu	Délka testu		
	2 hodiny	6 hodin	20 hodin
bez QKD	12,8 Gbit/s	12,8 Gbit/s	12,7 Gbit/s
s QKD	11,2 Gbit/s	14,9 Gbit/s	11,6 Gbit/s

Výsledky testů propustnosti TCP provozu 100G linky a MTU 1500 B shrnuje tabulka č. 2.10. Tabulka uvádí u každé hodnoty procentuální hodnotu odchylky, která byla odvozena od odchylky v Gbit/s z výše prezentovaných tabulek. Hodnoty nešifrovaného provozu jsou pouze ve formě průměrné hodnoty. Při testech nešifrovaného provozu v úvodní části byla pozornost věnována dosažení maximálních propustností a odchylky vypočítávány nebyly. Velikosti odchylek nešifrovaného provozu by však byly srovnatelné s šifrovaným provozem.

Tab. 2.10: Shrnutí výsledků TCP provozu 100G linky – MTU 1500 B.

Nešifrovaný provoz			
Počet CPU jader	MTU [B]		
	576	1300	1500
1	14,0 Gbit/s	26 Gbit/s	30,6 Gbit/s
10	38,9 Gbit/s	81,7 Gbit/s	85,4 Gbit/s
UltraScale+ (Mango)			
Počet CPU jader	MTU [B]		
	576	1300	1500
1	14,0 Gbit/s ± 6,4 %	23,5 Gbit/s ± 6,0 %	25,7 Gbit/s ± 7,8 %
10	42,0 Gbit/s ± 12,9 %	75,2 Gbit/s ± 3,5%	79,6 Gbit/s ± 4,5 %
Agilex (Intel)			
Počet CPU jader	MTU [B]		
	576	1300	1500
1	15,2 Gbit/s ± 3,3 %	23,5 Gbit/s ± 4,3 %	25,3 Gbit/s ± 5,9 %
10	43,3 Gbit/s ± 4,6 %	81,3 Gbit/s ± 1,2 %	85,8 Gbit/s ± 1,6 %
Agilex (Intel), QKD			
Počet CPU jader	MTU [B]		
	576	1300	1500
1	14,9 Gbit/s ± 7,4 %	23,3 Gbit/s ± 10,7 %	24,6 Gbit/s ± 7,3 %
10	43,0 Gbit/s ± 0,5 %	81,7 Gbit/s ± 3,3 %	84,0 Gbit/s ± 3,3 %

Pro šifrátory FPGA byl naplněn předpoklad minimální limitace provozu.

2.2 Firewally Juniper

Protože firewally Juniper disponovaly pouze 10G rozhraním, byla pro následující testování využit samostatná linka. Pro tuto linku byly testy nešifrovaného provozu zhotoveny samostatně a jsou zobrazeny v tabulce 2.11. Tyto testy byly realizovány pro přímo propojené stanice před přidáním firewallů.

Tab. 2.11: Výsledky testů propustnosti 10G linky pro nešifrovaný provoz.

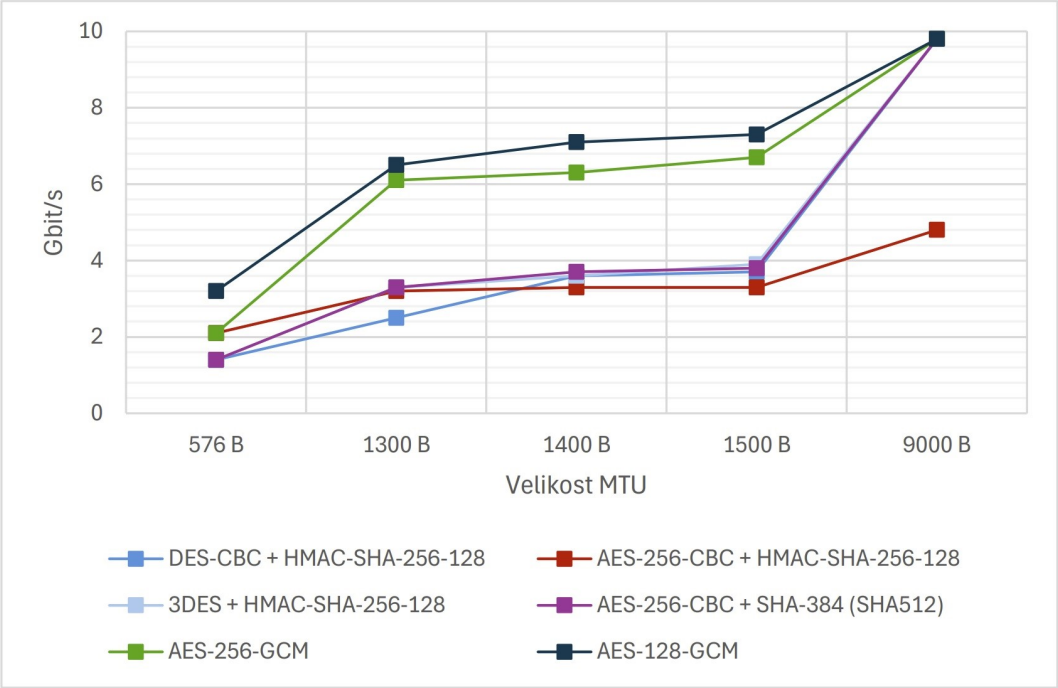
TCP				
Počet CPU jader	MTU [B]			
	576	1300	1500	9000
1	8,5 Gbit/s	9,3 Gbit/s	9,4 Gbit/s	9,9 Gbit/s
10	8,5 Gbit/s	9,3 Gbit/s	9,4 Gbit/s	9,9 Gbit/s
UDP				
Počet CPU jader	MTU [B]			
	576	1300	1500	9000
1	1,2 Gbit/s	1,9 Gbit/s	8,0 ± 1 Gbit/s	8,0 ± 1 Gbit/s
10	2 Gbit/s	7,0 Gbit/s	8,0 ± 1 Gbit/s	8,5 ± 1 Gbit/s

Rychlosti TCP provozu byly stejné pro jednojádrový i desetijádrový výkon. Provoz byl limitován kapacitou linky, ne vytížením CPU. Provoz UDP byl opět výrazně limitován a proměnné rychlosti jsou uvedeny s odchylkou. Průměrné hodnoty latence se pohybovaly v rozmezí 0,300 ms až 0,405 ms.

Pro šifrování provozu umožňují firewally volit a kombinovat vybrané parametry VPN komunikace. Lze volit různé autentizační mechanismy (ověřující přenášená data) a autentizační metodu (autentizující zdroj zpráv IKE, jako např. certifikáty, předsdílené klíče apod.). Pro parametry IPsec lze volit různé autentizační algoritmy (typ hashovacího algoritmu – ověřující data v paketech) a samotné šifrovací algoritmy. Cílem následujících testů tedy bylo nalézt nejvýkonnější a zároveň bezpečnou kombinaci těchto parametrů, která by byla vhodná pro kvantově odolný kanál. Pro daný model SRX4200 je výrobcem uvedena maximální propustnost IPsec VPN (Virtual Private Network) komunikace 35 Gbit/s. Tento prvek však disponuje 8x10G Ethernet rozhraními, takže se jedná o celkovou propustnost při komunikaci uskutečněnou s více rozhraními. Následující testy byly zhotoveny pro jedno 10G rozhraní na každém z firewallů. Zároveň výrobce u hodnoty propustnosti VPN uvádí jednotku MTU 1400 B, proto byly následující testy provedeny i pro tuto velikost. Maximální MTU pro IPsec bylo na Juniperech nastaveno na hodnotu 9192 B. To umožnilo testovat propustnost pro MTU 9000 B na koncových stanicích, aniž by docházelo

k „přetékání“ vlivem zapouzdřovacích IPsec dat.

Pro autentizační metodu a autentizační mechanismus VPN komunikace byla zvolena kombinace předsdíledných klíčů (PSK) a SHA-256. Tyto parametry zůstaly po celou dobu testování stejné, jelikož nebyl předpokládán výrazný dopad na propustnost v důsledku změn těchto parametrů. Ostatní parametry byly průběžně měněny a pro dané kombinace byly realizovány testy propustnosti. Shrnutí maximálních propustností pro každou kombinaci a velikost MTU zobrazuje graf na obr. č. 2.3.



Obr. 2.3: Graf hodnot propustností pro různé parametry VPN – Juniper SRX4200.

Výše testované kombinace zahrnují téměř všechny parametry, které lze na firewallech nastavit. Parametry, které testovány nebyly, zahrnují hash typu MD5 nebo různé délky šifrovacích klíčů algoritmu AES-CBC. Při užití těchto parametrů nebyly předpokládány výrazné odchylky od získaných hodnot. Šifry DES, 3DES a AES-CBC dosahovaly přibližně stejného výkonu. Určitý vliv na výkon měl také typ autentizačního algoritmu – hashe, který byl zvolen pro ověřování dat. Jednoznačně nejvýkonnějším šifrovacím algoritmem byl AES v módu GCM. Při užití AES-GCM bylo dosaženo propustností ∼7 Gbit/s pro běžné velikosti MTU pro TCP i UDP provoz. Propustnost při velikosti MTU 9000 B byla limitována schopnostmi 10G linky. Tím bylo dosaženo maximální teoretické propustnosti pro jednu fyzickou linku. Kombinace parametrů, která splňovala požadavky pro kvantově odolný kanál, byla zvolena následovně: Pro VPN kombinace PSK + SHA256 a pro IPsec šifrovací algoritmus AES-256-GCM. Zvolený šifrovací algoritmus byl stejný i pro šifrování na platformě FPGA.

2.3 Reálné aplikace

Na závěr byly testovány schopnosti šifrátorů v reálných aplikacích. Nejprve byla testována výkonnost síťové infrastruktury pro webovou komunikaci, a to v podobě měření rychlosti stahování souborů. K tomu byly využity webové servery Python HTTP a NGINX. Po zprovoznění serverů byla maximální rychlost stahování 550 MB/s, limitující faktor byla rychlost zápisu na disk klienta. Pro odstranění limitace byla část RAM využita jako další úložiště. Maximální rychlost zápisu na RAM disk byla 2,1 GB/s a této rychlost bylo dosaženo při stahování dvou souborů současně pomocí nástroje `wget2`. V další fázi proběhly testy zaměřené na provoz v reálném čase za pomoci video streamu. Přenos videa byl realizován pomocí přehrávače VLC. Video bylo vysílané z úložiště na virtuální stanici. Pro využití větší šířky pásma byly dále realizovány dva přenosy současně. Všechna videa zobrazené na stanici klienta byla bez viditelného zkreslení obrazu. V poslední části proběhlo testování provozu přes vysokorychlostní přepínač (Mikrotik CRS518-16XS-2XQ-RM), který byl přidán do 100 Gbit/s linky. Tyto testy měly za cíl zjistit, zda bude nějakým způsobem ovlivněn síťový provoz, pokud se nebude jednat o přímé propojení testovaných prvků. Testy propustnosti v této části firewally Juniper SRX4200 nezahrnovaly kvůli nižším dosažitelným rychlostem. Postup při realizaci testů propustnosti byl totožný s předchozím testováním. Výsledky zobrazují tab. č. 2.12 a tab. č.2.13.

Tab. 2.12: Provoz přes switch, TCP – FPGA Agilex (Intel).

Počet CPU jader	MTU [B]		
	576	1300	1500
1	13,7 ± 0,6 Gbit/s	21,7 ± 2,1 Gbit/s	25,4 ± 1,1 Gbit/s
10	42,2 ± 1,7 Gbit/s	72,6 ± 2,0 Gbit/s	80,0 ± 0,1 Gbit/s

Tab. 2.13: Provoz přes switch, UDP – FPGA Agilex (Intel).

Počet CPU jader	MTU [B]		
	576	1300	1500
1	1,1 ± 0,1 Gbit/s	2,4 ± 0,1 Gbit/s	3,2 ± 0,2 Gbit/s
10	9,1 ± 0,3 Gbit/s	20,1 ± 1,0 Gbit/s	22,9 ± 0,9 Gbit/s

Nejvyšší dosažená propustnost byla 80 Gbit/s. V případě propustnosti bez přepínače se jednalo o 85 Gbit/s. Přepínač tedy mírně limitoval provoz.

Závěr

Obsahem protokolu z měření je popis využité testovací infrastruktury a prezentace dosažených výsledků postkvantových šifrátorů. Síť byla realizována za pomoci virtualizace v podobě hypervizora XCP-ng a prostředí Xen Orchestra. Zde byly vytvořeny dvě virtuální stanice, které představovaly koncové body komunikace a mezi kterými byly utvářeny linky pro síťovou komunikaci. Do těchto linek byly postupně zapojovány testované prvky. Testy byly realizovány pro rychlosti až 100 Gbit/s.

Úvodní testování bylo zaměřené na dosažení maximální propustnosti 100G linky. Provoz byl limitován virtualizovaným prostředím a proto byla provedena optimalizace. Nejdůležitějšími kroky optimalizace byla změna síťových parametrů v systémové konfiguraci stanic, povolení PCI passthrough pro síťové karty a zapnutí offloading mechanismů. Po optimalizaci byla průměrná hodnota maximální propustnosti 96,4 Gbit/s (TCP) při velikosti MTU 9000 B. Hodnota latence klesla na třetinu.

Po optimalizaci byly realizovány testy propustnosti nešifrovaného a šifrovaného TCP a UDP provozu, které byly provedeny pro různý počet jader CPU a různé velikosti MTU. Pro běznou velikost MTU – 1500 B byla průměrná propustnost nešifrovaného TCP provozu 85,4 Gbit/s. Jednalo se o maximální výkon s využitím všech CPU jader. Testování šifrovaného provozu zahrnovalo dva typy FPGA šifrátorů (UltraScale+ a Agilex hardware) a firewally Juniper SRX4200. Při testech s FPGA šifrátory a velikostí MTU 1500 B přesahovala propustnost 80 Gbit/s pro oba typy hardware. Limitace provozu samotnými šifrátory tak byla minimální. Pro FPGA Agilex (Intel) byly dále realizovány testy v režimu QKD a dlouhodobé testy s i bez QKD, tyto testy proběhly v pořádku a nebyla pozorována žádná další limitace. Firewally Juniper SRX4200 disponovaly pouze 10G rohzraním. Testy s firewally zahrnovaly různé kombinace parametrů IPsec a VPN. Nejvyšší vliv na výkon měl šifrovací algoritmus. Nejvýkonnější šifrovací algoritmus byl jednoznačně AES-GCM.

Na závěr proběhly testy se skutečným síťovým provozem. Tyto testy zahrnovaly webovou komunikaci, přenos videa v reálném čase a provoz přes vysokorychlostní přepínač. Všechny šifrátory dokázaly tyto typy provozu spolehlivě šifrovat a nebyly pozorovány další výrazné limitace.

Seznam symbolů a zkratek

CPU	Central Processing Unit
FPGA	Field-Programmable Gate Array
IPsec	Internet Protocol Security
MTU	Maximum Transmission Unit
OS	Operating System
PCI	Peripheral Component Interconnect
PSK	Pre-Shared Keys
QKD	Quantum Key Distribution
RAM	Random Access Memory
TCP	Transmission Control Procotol
UDP	User Datagram Procotol
VPN	Virtual Private Network