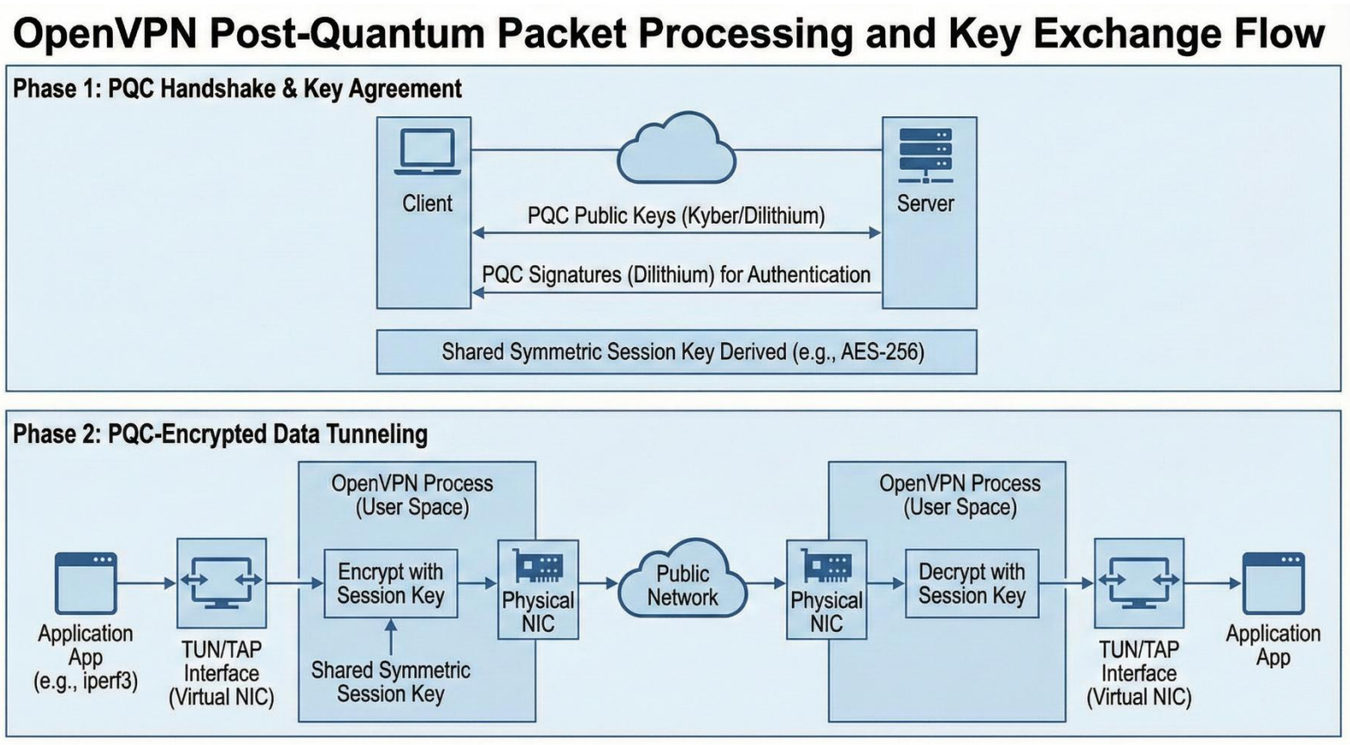
使用VPN框架在Jetson Nano、Jetson Orin Nano和Jetson Orin Nano Super上對CRYSTALS-Kyber和CRYSTALS-Dilithium演算法進行效能分析與比較

專題生: 電機四 4111064118 林玉玲

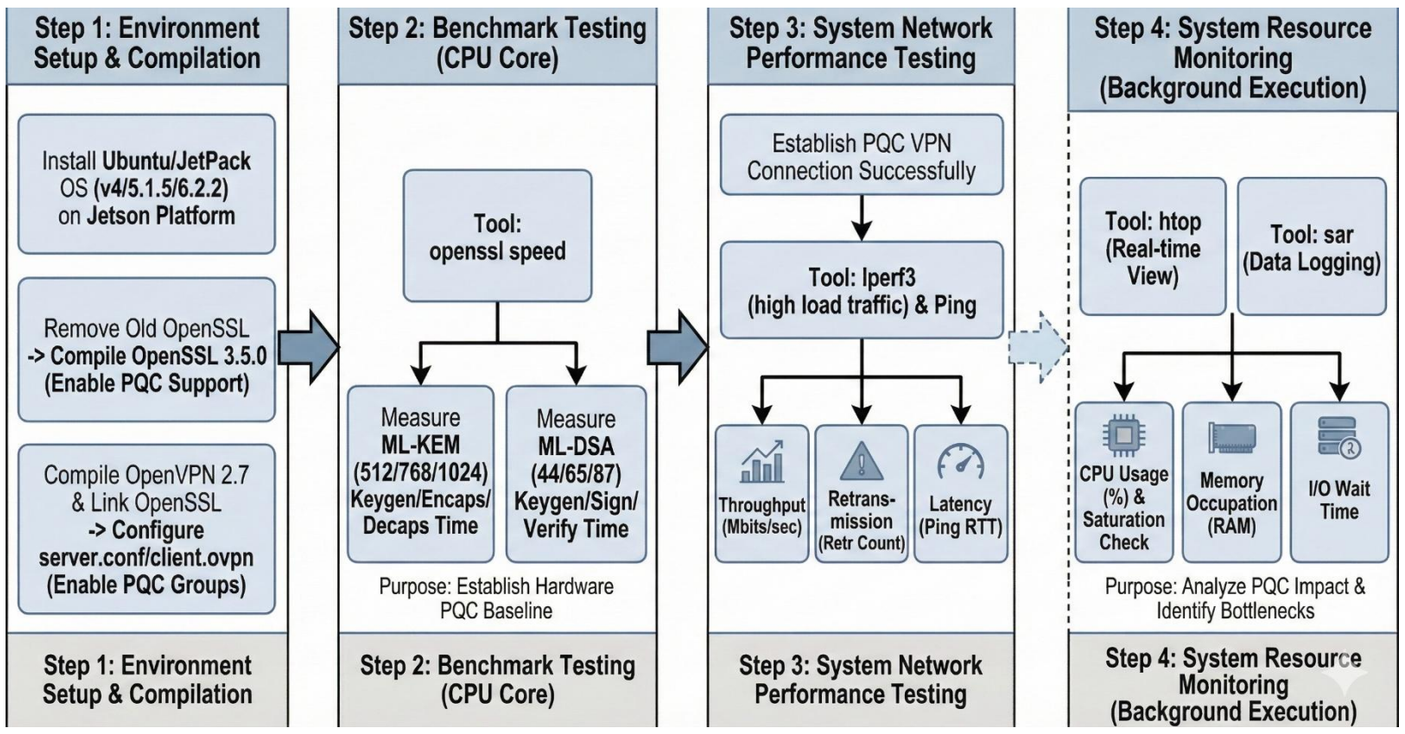
研究動機與系統架構

隨著量子計算技術的發展，傳統 RSA 與 ECC 加密面臨被破解的「Q-Day」危機。本研究旨在將美國國家標準暨技術研究院 (NIST) 最新選定的後量子密碼標準（PQC）——ML-KEM與ML-DSA，整合至嵌入式 VPN 系統中 。 我們成功在邊緣裝置上編譯 OpenSSL 3.5.0 與 OpenVPN 2.7，構建出抗量子攻擊的安全通道。如右圖展示 PQC 如何整合進 VPN 流程。

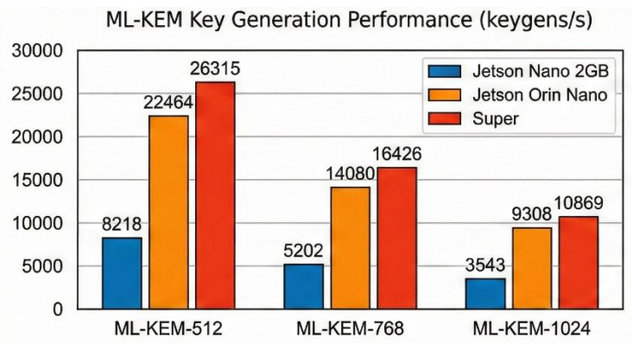


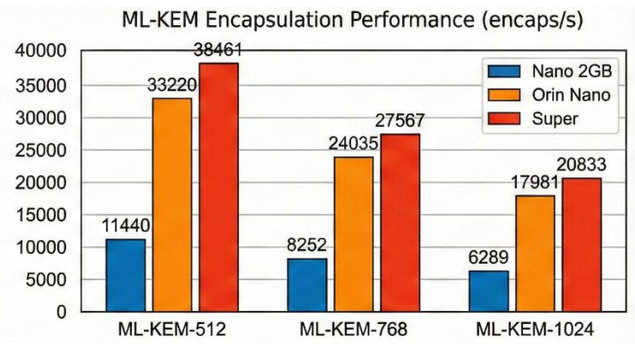
硬體平台與實驗方法

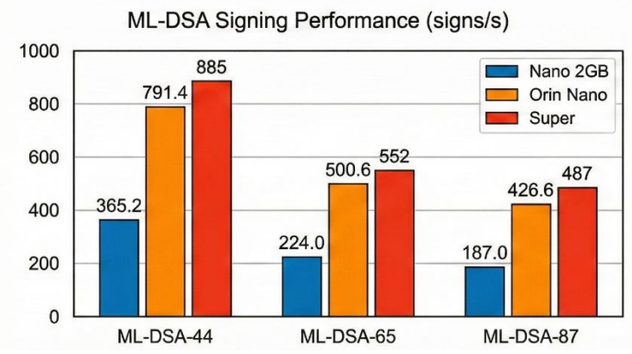
為了驗證 PQC 在邊緣運算的適用性，本研究選用 NVIDIA Jetson 系列進行效能對比。測試對象包含入門級的 Jetson Nano (2GB) 以及新一代 AI 運算平台 Jetson Orin Nano 與 Orin Nano Super 。 實驗設計分為兩階段：首先進行演算法基準測試，量測金鑰生成與簽章耗時；接著進行高負載網路壓力測試，分析吞吐量、延遲與 CPU 資源消耗，以識別硬體效能瓶頸 。

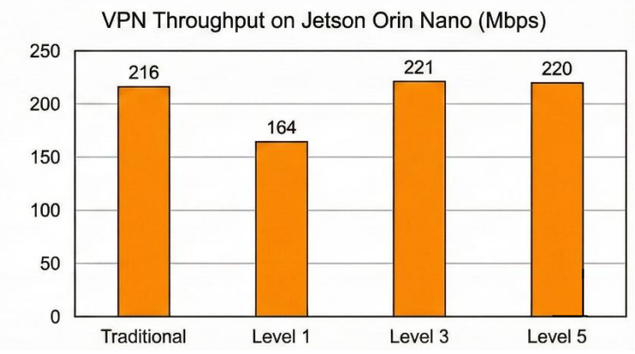


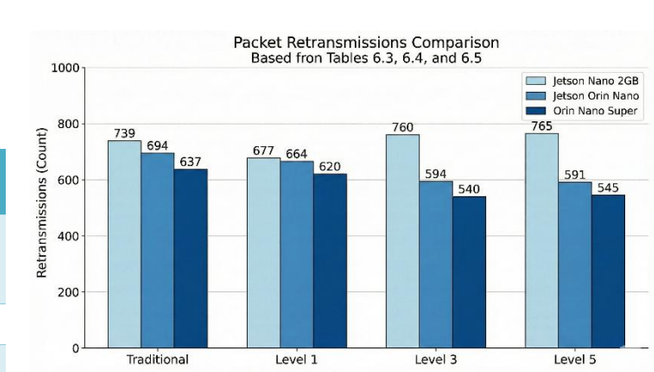
硬體特性	NVIDIA Jetson Nano (2GB)	NVIDIA Jetson Orin Nano	NVIDIA Jetson Orin Nano Super
作業系統環境	**JetPack 4.6.6**	**JetPack 5.1.5**	**JetPack 6.2.1**
GPU 架構	Maxwell (128 cores)	Ampere (1024 cores)	Ampere (1024 cores)
GPU 時脈	921 MHz	635 MHz	**1,020 MHz**
CPU 架構	4-core Cortex-A57	6-core Cortex-A78AE	6-core Cortex-A78AE
CPU 時脈	1.43 GHz	1.5 GHz	**1.7 GHz**
AI 算力 (INT8)	472 GFLOPS (FP16)	40 TOPS (Sparse)	**67 TOPS (Sparse)**
記憶體規格	2 GB LPDDR4	8 GB LPDDR5	8 GB LPDDR5
記憶體頻寬	25.6 GB/s	68 GB/s	**102 GB/s**
模組電源 (TDP)	10W	7W / 15W	7W / 15W / **25W**
			

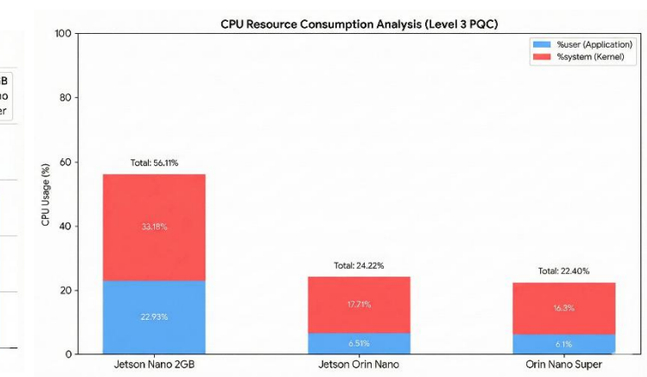












	Device	keygen (µs)	encaps (µs)	decaps (µs)	keygens/s	encaps/s	decaps/s
ML-KEM-512	Jetson Orin Nano	45	30	47	22464	33220	21286
	SUPER	38	26	40	26315	38461	25011
	Jetson Nano 2GB	122	87	140	8218	11440	7166
ML-KEM-768	Jetson Orin Nano	71	42	65	14080	24035	15383
	SUPER	60	36	55	16426	27567	18181
	Jetson Nano 2GB	192	121	194	5202	8252	5146
ML-KEM-1024	Jetson Orin Nano	107	56	86	9308	17981	11567
	SUPER	92	48	73	10869	20833	13698
	Jetson Nano 2GB	282	159	255	3543	6289	3922
RSA-2048	Jetson Orin Nano	124146	47	1704	81	21452	587
	SUPER	96301	40	1446	10.4	24993	691
	Jetson Nano 2GB	353448	169	6170	28	5914	162

	Device	keygen (µs)	sign (µs)	verify (µs)	keygens/s	signs/s	verifys/s
ML-DSA-44	Jetson Orin Nano	4379	1263.6	244.1	228.3	791.4	4096.7
	SUPER	3950	1130	215	253	885	4650
	Jetson Nano 2GB	6297	2738.3	543.4	158.8	365.2	1840.2
ML-DSA-65	Jetson Orin Nano	432	1997.7	371.3	2314.8	500.6	2693.4
	SUPER	385	1810	330	2597	552	3030
	Jetson Nano 2GB	823	4464.2	827.2	1215.1	224.0	1208.9
ML-DSA-87	Jetson Orin Nano	620	2344.0	575.9	1612.9	426.6	1736.4
	SUPER	560	2050	510	1785	487	1960
	Jetson Nano 2GB	1192	5348.5	1273.2	838.9	187.0	785.4

結論 本研究在嵌入式邊緣平台上，成功實作整合後量子 VPN ，證實了新一代抗量子演算法（ML-KEM/ML-DSA）在資源受限環境中具備極高的運算效率與可行性 ，為未來IoT與邊緣運算的資料傳輸安全，提供了關鍵的實測數據與硬體選型參考 。