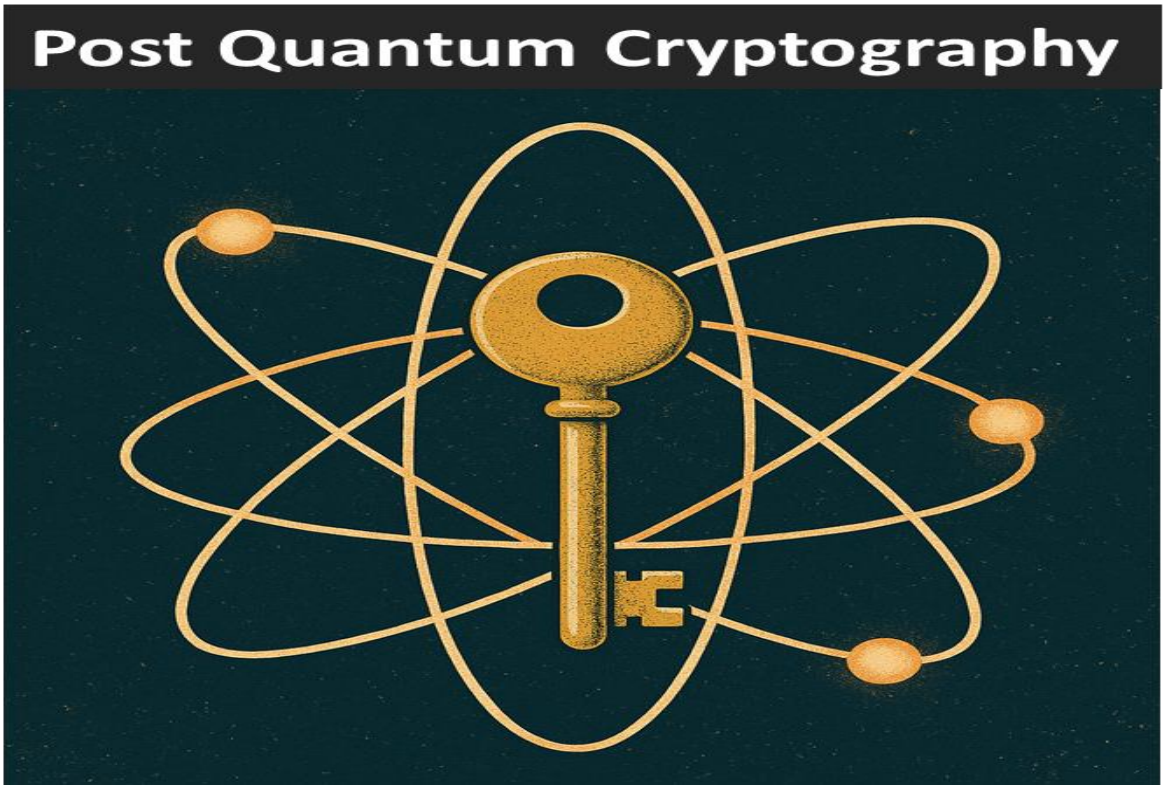
ບົດຄວາມຮູ້ກ່ຽວກັບຄວາມປອດໄພໄຊເບີ

Post-Quantum Cryptography (PQC) ແລະ ການກະກຽມຮັບມືກັບຍຸກຄອມພິວເຕີຄວາມຕຳໃນອະນາຄົດອັນໃກ້ນີ້



1. Post-Quantum Cryptography (PQC) ແມ່ນຫຍັງ?

Post-Quantum Cryptography (PQC) ຫຼື **ການເຂົ້າລະຫັດລັບຫຼັງຍຸກຄວາມຕຳ** ໝາຍເຖິງຊຸດຂອງ **ອັລກໍຣິທຶມ (Algorithms) ການເຂົ້າລະຫັດລັບ**ໃໝ່ທີ່ຖືກອອກແບບມາ ເພື່ອໃຫ້ສາມາດ**ຕ້ານທານການໂຈມຕີ**ຈາກ**ຄອມພິວເຕີຄວາມຕຳ (Quantum Computers)** ທີ່ມີປະສິດທິພາບສູງໃນອະນາຄົດ.

ໃນປັດຈຸບັນ, ລະບົບການເຂົ້າລະຫັດລັບແບບສາທາລະນະ (Public-Key Cryptography) ສ່ວນໃຫຍ່ ເຊັ່ນ: RSA ແລະ ECC (Elliptic Curve Cryptography) ແມ່ນອີງໃສ່ບັນຫາທາງຄະນິດສາດ ທີ່ຄອມພິວເຕີທຳມະດາ (Classical Computers) ໃຊ້ເວລາຫຼາຍໃນການແກ້ໄຂ. ຢ່າງໃດກໍຕາມ, ຖ້າຄອມພິວເຕີຄວາມຕຳ ທີ່ມີຂະໜາດໃຫຍ່ພຽງພໍຖືກສ້າງຂຶ້ນ, ພວກມັນຈະສາມາດໃຊ້ **ອັລກໍຣິທຶມຂອງ Shor** ເພື່ອແກ້ໄຂບັນຫາເຫຼົ່ານີ້ໄດ້ຢ່າງວ່ອງໄວ, ເຊິ່ງຈະເຮັດໃຫ້ລະບົບເຂົ້າລະຫັດລັບໃນປັດຈຸບັນກາຍເປັນອ່ອນແອ ແລະ ຖືກເຈາະໄດ້ຢ່າງງ່າຍດາຍ.

PQC ຈຶ່ງມີເປົ້າໝາຍໃນການສ້າງມາດຕະຖານການເຂົ້າລະຫັດລັບ ທີ່ອີງໃສ່ບັນຫາທາງຄະນິດສາດຊຸດໃໝ່ ທີ່ເຊື່ອກັນວ່າ **ຍັງຍາກ**ຕໍ່ການແກ້ໄຂທັງໂດຍຄອມພິວເຕີທຳມະດາ ແລະ ຄອມພິວເຕີຄວາມຕຳ. ຕົວຢ່າງ ຂອງ PQC ແມ່ນອີງໃສ່ຄະນິດສາດ ເຊັ່ນ: Lattice-based Cryptography, Hash-based Cryptography, ແລະ Multivariate Cryptography.

2. ໃນຍຸກດິຈິຕອນ ມີຄວາມສຳຄັນແນວໃດ?

PQC ມີຄວາມສຳຄັນຢ່າງຍິ່ງໃນຍຸກດິຈິຕອນ ເນື່ອງຈາກເຫດຜົນຫຼັກໆ ດັ່ງນີ້:

❖ **ປົກປ້ອງຂໍ້ມູນໄລຍະຍາວ (Harvest Now, Decrypt Later):** ຂໍ້ມູນທີ່ມີຄວາມລັບສູງ ເຊັ່ນ: ຄວາມລັບຂອງລັດຖະບານ, ຂໍ້ມູນການເງິນ, ຂໍ້ມູນສຸຂະພາບ ຫຼື ຊັບສິນທາງປັນຍາ, ທີ່ຖືກເຂົ້າລະຫັດໄວ້ໃນປັດຈຸບັນ ອາດຈະຖືກດັກຈັບ (Harvested) ແລະ ເກັບໄວ້. ເມື່ອຄອມພິວເຕີຄວາມຕຳມີຂຶ້ນໃນອະນາຄົດ ຂໍ້ມູນເຫຼົ່ານັ້ນຈະຖືກຖອດ

ລະຫັດອອກໄດ້ທັງໝົດ. PQC ຈຶ່ງຈຳເປັນຕ້ອງໄດ້ນຳໃຊ້ຕັ້ງແຕ່ຕອນນີ້ ເພື່ອປົກປ້ອງຂໍ້ມູນຈາກໄພຂົ່ມຂູ່ໃນອະນາຄົດ.

❖ **ຄວາມໝັ້ນຄົງປອດໄພທາງໄຊເບີ (Cybersecurity):** ໂຄງລ່າງພື້ນຖານທີ່ສຳຄັນ (Critical Infrastructure) ຂອງປະເທດ, ການສື່ສານທາງທະຫານ, ລະບົບການເງິນ ແລະ ເວັບໄຊທ໌ທົ່ວໄປ ແມ່ນອີງໃສ່ລະບົບການເຂົ້າລະຫັດລັບເພື່ອຮັບປະກັນການຢັ້ງຢືນຕົວຕົນ (Digital Signatures) ແລະ ຄວາມລັບຂອງການສື່ສານ (Key Exchange). ການປ່ຽນໄປໃຊ້ PQC ເປັນສິ່ງທີ່ຫຼີກລ້ຽງບໍ່ໄດ້ ເພື່ອຮັກສາຄວາມປອດໄພ ຂອງລະບົບເຫຼົ່ານີ້.

❖ **ມາດຕະຖານສາກົນ:** ສະຖາບັນມາດຕະຖານ ແລະ ເຕັກໂນໂລຊີ ແຫ່ງຊາດ ຂອງສະຫະລັດ (NIST) ໄດ້ເລີ່ມຂະບວນການຄັດເລືອກ ແລະ ກຳນົດມາດຕະຖານ PQC ຢ່າງເປັນທາງການແລ້ວ ນີ້ສະແດງໃຫ້ເຫັນວ່າ PQC ຈະກາຍເປັນມາດຕະຖານສາກົນໃນໄວໆນີ້. ເຊິ່ງທຸກອົງກອນທົ່ວໂລກ ຕ້ອງປະຕິບັດຕາມ.

3. ສຳລັບ ສປປ ລາວ ຄວນມີແຜນແນວໃດ ກັບ PQC?

ເຖິງແມ່ນວ່າ ປະເທດລາວອາດຈະຍັງບໍ່ໄດ້ພັດທະນາຄອມພິວເຕີຄວາມຕຳເອງ, ແຕ່ການນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນ ແລະ ລະບົບການສື່ສານສາກົນ ກໍ່ມີຢ່າງກວ້າງຂວາງ. ການກະກຽມຮັບມືກັບ PQC ຈຶ່ງເປັນສິ່ງທີ່ສຳຄັນ.

❖ **ການຮັບຮູ້ ແລະ ສຶກສາ:**

- **ສ້າງຄວາມຮັບຮູ້:** ເຜີຍແຜ່ຄວາມຮູ້ ກ່ຽວກັບໄພຂົ່ມຂູ່ຈາກຄອມພິວເຕີຄວາມຕຳ ແລະ ຄວາມສຳຄັນ ຂອງ PQC ໃຫ້ແກ່ພາກລັດ, ພາກທຸລະກິດ ແລະ ພາກການສຶກສາ;
- **ພັດທະນາບຸກຄະລາກອນ:** ລົງທຶນໃນການຝຶກອົບຮົມນັກວິຊາການ, ວິສະວະກອນ ແລະ ຜູ້ບໍລິຫານດ້ານໄອທີ ເພື່ອໃຫ້ມີຄວາມຮູ້ຄວາມສາມາດໃນການຈັດຕັ້ງປະຕິບັດ PQC.

❖ **ການສຳຫຼວດ ແລະ ວາງແຜນ:**

- **ສຳຫຼວດຊັບສິນ:** ກວດກາລະບົບໄອທີ ທີ່ສຳຄັນທັງໝົດຂອງລັດຖະບານ ແລະ ພາກທຸລະກິດ (ເຊັ່ນ: ລະບົບທະນາຄານ, ຖານຂໍ້ມູນສຳຄັນ, ລະບົບການສື່ສານ) ເພື່ອລະບຸວ່າລະບົບໃດໃຊ້ການເຂົ້າລະຫັດແບບໃດ ແລະ ມີຄວາມສ່ຽງຕໍ່ການໂຈມຕີຄວາມຕຳ.
- **ວາງແຜນການປ່ຽນຜ່ານ:** ສ້າງແຜນຍຸດທະສາດການປ່ຽນຜ່ານໄລຍະສັ້ນ, ກາງ ແລະ ຍາວ (Migration Roadmap) ໄປສູ່ PQC ຕາມມາດຕະຖານສາກົນ ຂອງ NIST. ຄວນເລີ່ມຕົ້ນດ້ວຍການນຳໃຊ້ **ລະບົບປະສົມປະສານ (Hybrid Schemes)** (ໃຊ້ທັງການເຂົ້າລະຫັດແບບເກົ່າ ແລະ PQC ພ້ອມກັນ) ເພື່ອຫຼຸດຜ່ອນຄວາມສ່ຽງ.

❖ **ການຮ່ວມມື:**

- **ຮ່ວມມືສາກົນ:** ຕິດຕາມການພັດທະນາມາດຕະຖານ PQC ຈາກອົງກອນສາກົນ ເຊັ່ນ: NIST ແລະ ຮ່ວມມືກັບປະເທດໃນພາກພື້ນ ເພື່ອແລກປ່ຽນບົດຮຽນ ແລະ ຄວາມຮູ້.

4. PQC ກັບ Y2K ຕ່າງກັນແນວໃດ?

ເຖິງແມ່ນວ່າທັງ PQC ແລະ Y2K (Year 2000 Problem) ລ້ວນແຕ່ເປັນ **ຄວາມສ່ຽງທາງເຕັກໂນໂລຊີຂະໜາດໃຫຍ່ ທີ່ຄາດເດົາໄດ້**, ແຕ່ທັງສອງກໍມີລັກສະນະທີ່ແຕກຕ່າງກັນຢ່າງຫຼວງຫຼາຍ:

ລັກສະນະ	PQC (Post-Quantum Cryptography)	Y2K (Year 2000 Problem)
ສາເຫດ	ການພັດທະນາຂອງເຕັກໂນໂລຊີຄອມພິວເຕີຄວາມຕຳ ທີ່ຈະສາມາດ **ເຈາະ** ລະບົບເຂົ້າລະຫັດລັບໃນປັດຈຸບັນໄດ້.	ຄວາມຜິດພາດໃນການອອກແບບໂປຣແກຣມທີ່ນັບປີພຽງ 2 ຕົວເລກ ເຊິ່ງຈະເຮັດໃຫ້ລະບົບ **ລົ້ມເຫຼວ** ເມື່ອເຂົ້າສູ່ປີ 2000.
ລັກສະນະໄພຂົ່ມຂູ່	**ໄພຂົ່ມຂູ່ດ້ານຄວາມລັບ (Confidentiality) ແລະ ການຢັ້ງຢືນຄວາມສົມບູນ (Integrity)**	**ໄພຂົ່ມຂູ່ດ້ານການໃຊ້ງານ (Availability) ແລະ ການເຮັດວຽກທີ່ຖືກຕ້ອງ** ຂອງລະບົບ.

ລັກສະນະ	PQC (Post-Quantum Cryptography)	Y2K (Year 2000 Problem)
	ຂອງຂໍ້ມູນທີ່ມີຄວາມສຳຄັນໃນໄລຍະຍາວ.	
ເວລາເກີດເຫດ	**ບໍ່ມີກຳນົດເວລາທີ່ແນ່ນອນ** (ອາດຈະພາຍໃນ 10-20 ປີ) ແລະ ອັນຕະລາຍເລີ່ມຕົ້ນຕັ້ງແຕ່ມື້ນີ້ (Harvest Now, Decrypt Later).	**ມີກຳນົດເວລາທີ່ແນ່ນອນ** ຄືວັນທີ 1 ມັງກອນ ປີ 2000.
ວິທີແກ້ໄຂ	ການປ່ຽນໄປໃຊ້ **ອັລກໍຣິທຶມຄະນິດສາດ** ຊຸດໃໝ່ ທີ່ຕ້ອງມີການຄົ້ນຄວ້າ, ຮັບຮອງມາດຕະຖານ, ແລະ ການປ່ຽນແປງໂຄງສ້າງລະບົບທີ່ສັບຊ້ອນ.	ການປ່ຽນແປງ **ການຂຽນໂຄດ (Coding)** ເພື່ອໃຫ້ຮອງຮັບການນັບປີແບບ 4 ຕົວ ເລກ. ເຊິ່ງເປັນການແກ້ໄຂທີ່ຂ້ອນຂ້າງກົງໄປກົງມາ.
ຜົນກະທົບ	ຖ້າບໍ່ແກ້ໄຂ, ຈະສູນເສຍຄວາມລັບຂອງຂໍ້ມູນສຳຄັນທັງໝົດໃນອະດີດ ແລະ ອະນາຄົດ.	ຖ້າບໍ່ແກ້ໄຂ, ລະບົບໄອທີຕ່າງໆ ຈະຢຸດເຮັດວຽກ.

ບົດສະຫຼຸບ

Post-Quantum Cryptography ບໍ່ແມ່ນພຽງແຕ່ບັນຫາທາງເຕັກໂນໂລຊີທີ່ໄກຕົວ, ແຕ່ເປັນ **ວິກິດການຄວາມປອດໄພທາງໄຊເບີ ທີ່ເລີ່ມຕົ້ນແລ້ວ**. ສຳລັບ ສປປ ລາວ ການລິເລີ່ມການສຶກສາ, ການວາງແຜນ ແລະ ການຮ່ວມມື ເພື່ອປ່ຽນຜ່ານໄປສູ່ PQC ຢ່າງຮອບຄອບ ແມ່ນເປັນການຮັບປະກັນອະນາຄົດຄວາມໝັ້ນຄົງປອດໄພທາງດິຈິຕອນ ແລະ ຄວາມລັບຂອງຂໍ້ມູນສຳຄັນຂອງຊາດໃນຍຸກສະໄໝໃໝ່.

ເອກະສານອ້າງອີງ:

1. https://csrc.nist.gov/projects/post-quantum-cryptography
2. https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

ໂດຍ: ກົມຄວາມປອດໄພໄຊເບີ

ເວັບໄຊ: www.laocert.gov.la, www.dcs.gov.la

ອີເມວ: admin@laocert.gov.la