Post-Quantum

Cryptography Conference

Working on Quantum-Safe Encrypted Emails

Tan Teik Guan
CEO at pQCee

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

Working on Quantum-safe Encrypted Emails

Dr. TAN Teik Guan

1

pQCee - Post Quantum Cybersecurity

Dr TAN Teik Guan,
PhD (Cybersecurity),
Exited-Founder

LOH Chay Hiah,
Chartered
Accountant

Ongoing Projects:

Our collaboration with pQCee allows us to address the evolving security needs of our customers with world-class solutions that offer protection against tomorrow's threats.

- Mr Eugene Lam, Deputy CEO, Netrust

Investors:

Under the CyberCall programme, pQCee will develop a quantum-safe public key infrastructure ("P-K-I") to address emerging cyber threats from threat actors capitalising on quantum computers to exploit new vulnerabilities.

- Dr Janil Puthucheary,
Senior Minister of State, SG

Data is already under threat from Quantum

Web applications

End-Users using public wi-fi to perform online transactions

- Internet Banking, payments
- Tax/Statutory filing
- eCitizen applications
- Insurance claims

VPN connectivity

VPNs are used to protect sensitive traffic between

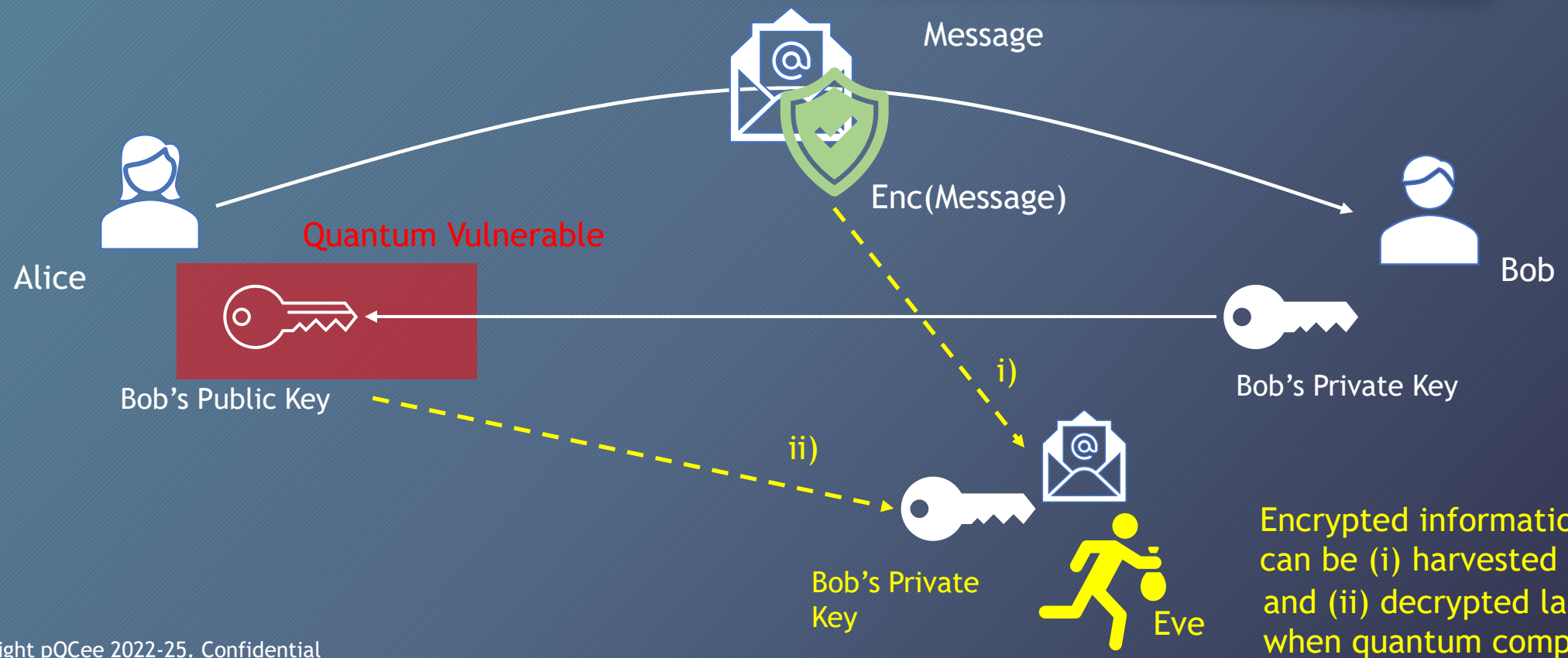
- Data centers
- HQ to branch
- Remote offices

E-documents

Electronic documents that contain sensitive or confidential information are exchanged using:

- APIs
- Emails, PDF documents
- File transfer with web browser

Quantum Threat to Data Confidentiality



Encrypted information can be (i) harvested now and (ii) decrypted later when quantum computers are powerful enough

Can a post-quantum secure email do the job?

Typical Secure Email

- Needs a PKI to issue keys+certs for every user
- Uses S/MIME format to package the email for sending
- Non-repudiation and data confidentiality is supported
- For intra-enterprise email use-case

How about external recipients?

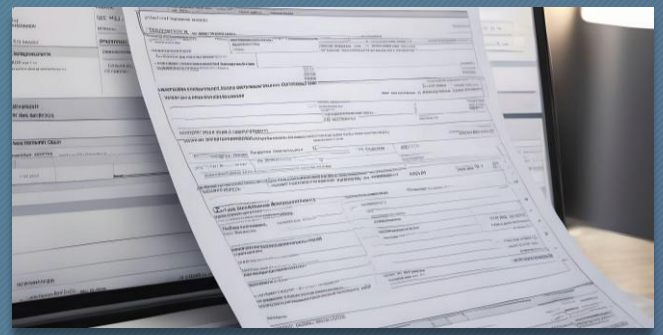
X CA may not support issuance to external users

X External email system may not ready for post quantum PKI keys or S/MIME

X Protection against HNDL is priority

X Not so suitable to use for B2C or C2C use-cases

Encrypted Email use-cases



External reporting

Enterprises require to send confidential documents (e.g. financial reports, transaction details, board meeting minutes) to external partners and customers on a regular basis.

Privacy protection

Users need to submit sensitive information (e.g. passport, identity cards, biometric, social security numbers) via email for KYC, registration purposes.

Secret management

Login credentials, API keys, administrator passwords need to be sent securely to specific recipients during onboarding / account resets.

Requirements for Encrypted Emails

R1: Secure against HNDL attacks

- Emails eavesdropped in transit/storage cannot be decrypted using a quantum computer

R2: Minimal Key Management

- Key Management should be automated. Email recipients should not need to pre-setup/generate and maintain their own keys to use the system

R3: Prevent Data Leaks / AI training

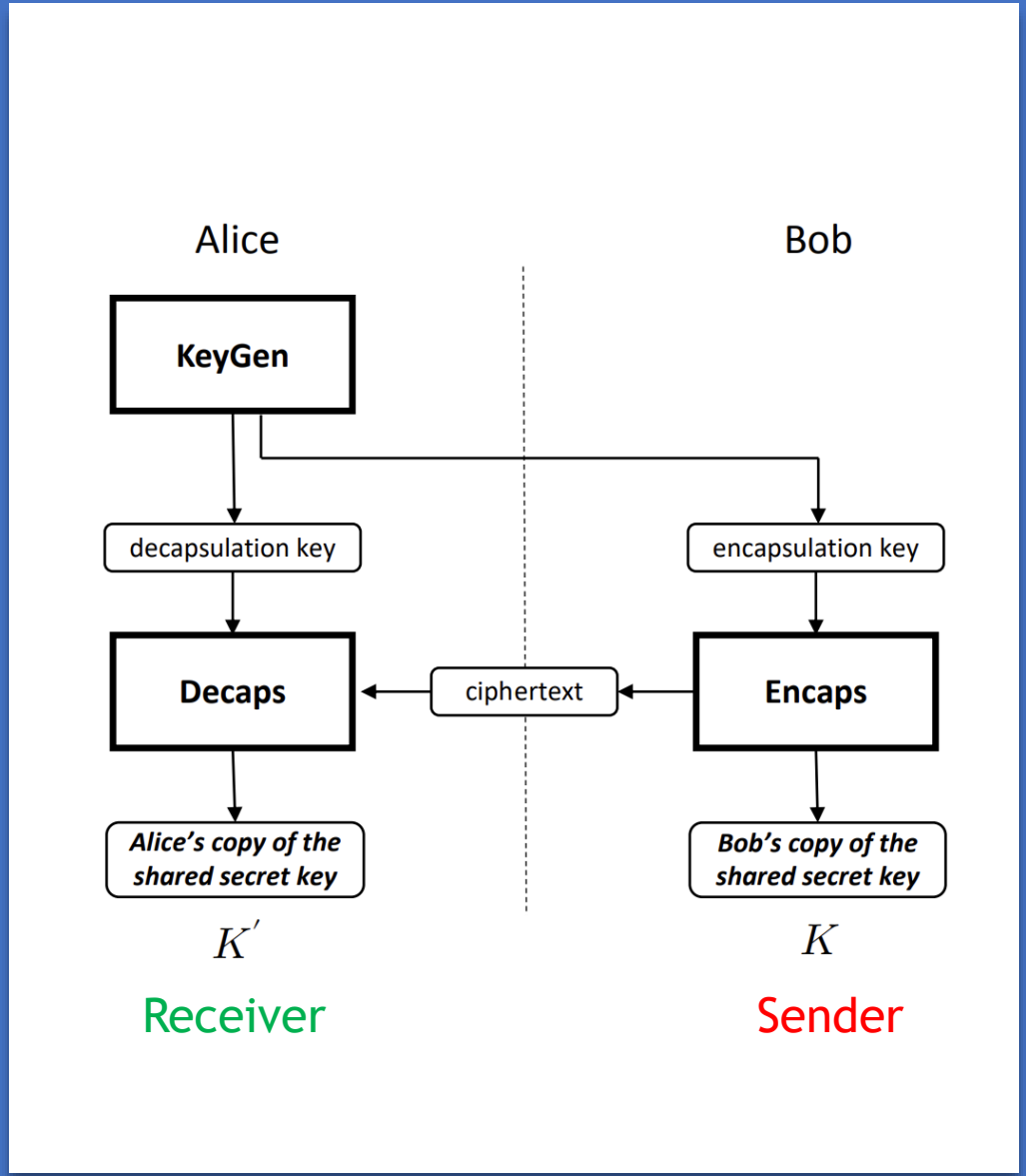
- Email provider should not have access to the email contents.

R1: Secure against HNDL

- Cryptography
  - RSA is vulnerable against quantum computers.
  - We need to use MLKEM (NIST FIPS 203)
- Interoperability concerns
  - We focus on encryption of the email message body and attachments
  - TLS connections are service-provider dependent which we have no control
    - Email recipients and subject are not quantum-safe

→Encrypt the email contents and replace it in the message body

https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf



R2: Minimal Key Management

- Typical secure email implementations
  - Generate a keypair to be issued to every user. RSA is often used as it can support both encryption and digital signing using the same key pair.
  - Operate a PKI and directory service to support encryption and non-repudiation of email
  - Are often limited to intra-organization due to its complexity

- Our encrypted email
  - New keypair is generated for each email. MLKEM is used to ensure post-quantum security. Can be changed to other algorithms dynamically (crypto-agile)
  - Focus only on encryption (no end-user digital signing). No PKI certificates.
  - Able to use across agencies and with external users

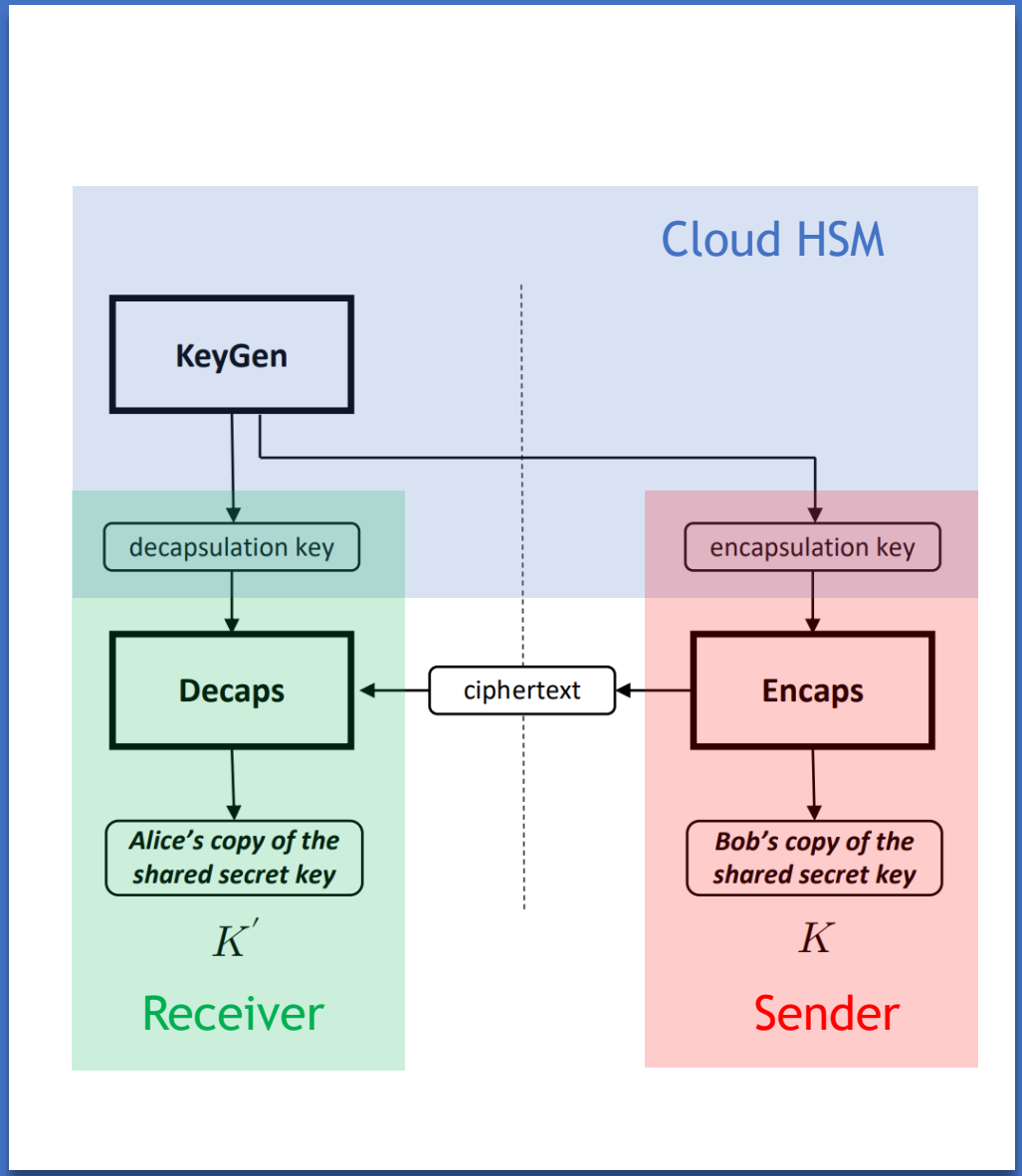
→Need to rely on an external authentication source (e.g. Email provider) when decrypting email

R3: Prevent data leaks

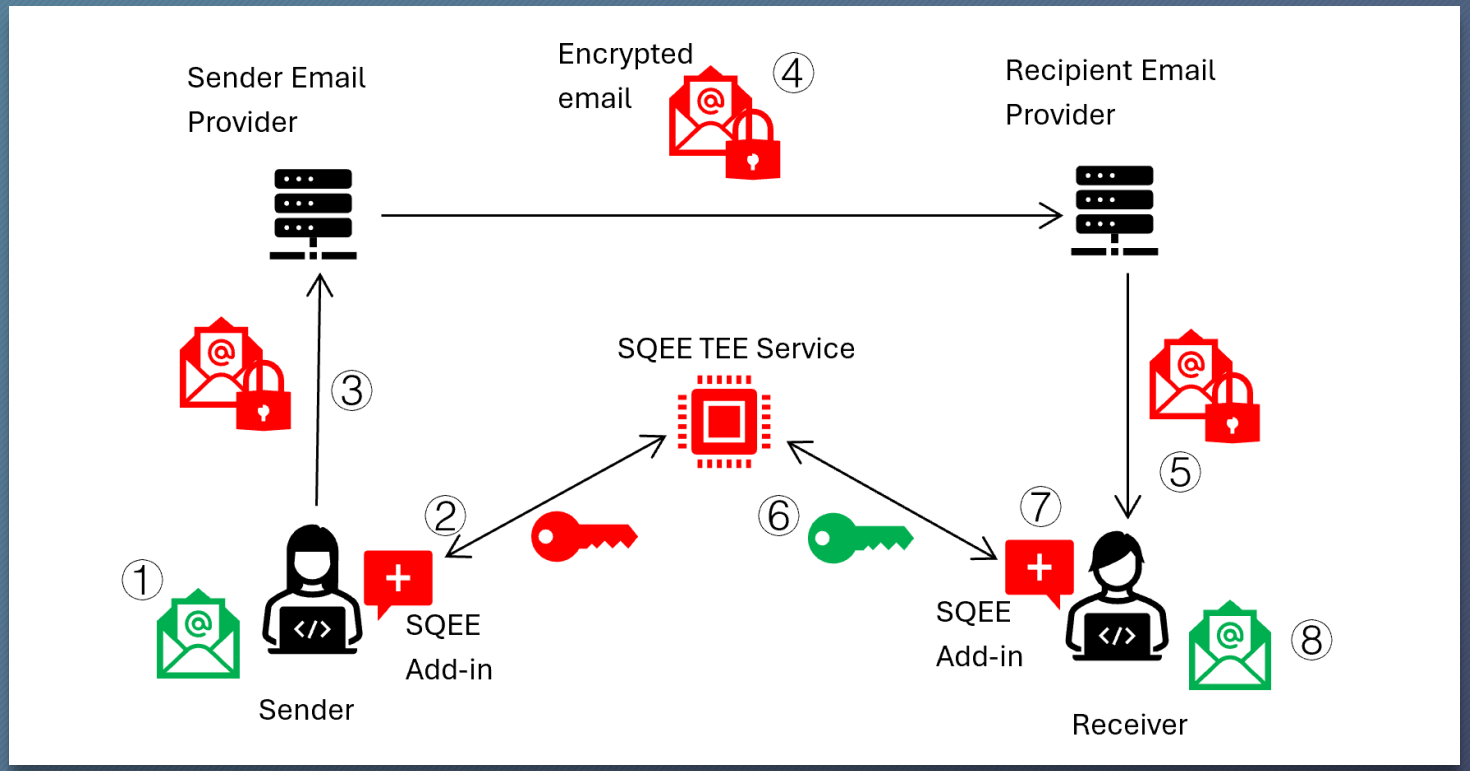
- Backend Cloud HSM to do KeyGen:
  →Can be done using a confidential compute node (e.g. TEE) in the cloud
- Implement end-to-end encryption at client-side. Data is never decrypted in the backend:
  - For sender: MLKEM encapsulation + AES encryption
  - For receiver: MLKEM decapsulation + AES decryption

  →Can be done using Javascript

https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf



1. Sender drafts email
2. SQEE add-in uses MLKEM key from SQEE TEE service to encrypt email
3. Email client sends encrypted email is sent to email provider
4. Encrypted email is forwarded to recipient's email provider



5. Recipient downloads email using email client
6. User selects SQEE add-in to view email. SQEE add-in requests TEE service to get decryption key
7. SQEE add-in decrypts email
8. Email is displayed to recipient

Putting it altogether

SafeQuard Encrypted Email (SQEE)

Encrypted Email =/= Secure Email

Typical Secure Email

- Needs a PKI to issue keys+certs for every user
- Uses S/MIME format to package the email for sending
- Non-repudiation and data confidentiality is supported
- For intra-enterprise email use-case

Encrypted Email

- Encryption keys are generated for each email (crypto-agile)
- Message body and attachments are inline encrypted
- Data confidentiality of email is supported. Relies on OAuth authentication with email provider
- For B2C or C2C email use-case

Are your important emails quantum-safe yet?

13

Contact

- Technology:
  - Dr. Teik Guan TAN
  - teikguan@pqcee.com
- Finance & Operations:
  - Chay Hiah LOH
  - chayhiah@pqcee.com