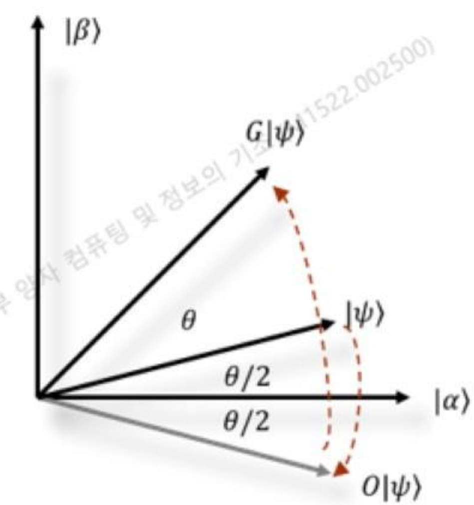
Summary of previous lecture

- Factoring algorithm (Shor's algorithm)
  - Discrete Fourier transform ➔ Quantum Fourier transform ➔ Example of QFT circuit
  - Origin of quantum speed-up
    - Simultaneous calculation of $a^x \pmod{N}$ for x from 0 to $2^{2\cdot\mathrm{ceil}(\log_2 N)}$
    - Fast Quantum Fourier transform

- Grover search algorithm
  - Algorithm is designed to maximize the probability of measuring the answer to the given search problem.
  - Quantum speed-up
    - In classical case: $O\left(\frac{N}{M}\right)$ oracle query
    - In quantum case: $O\left(\sqrt{\frac{N}{M}}\right)$ oracle query

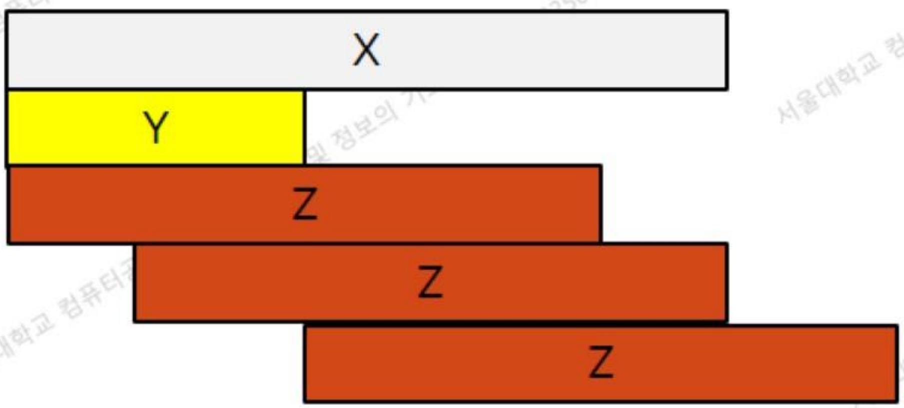


Quantum Cryptography

- Quantum communication? Quantum cryptography?
- 양자 암호, 양자 암호 통신, 양자 통신, 양자 인터넷, ...
- Currently the terminology is not precisely defined
- Public key system
  - Example: RSA (Rivest–Shamir–Adleman) public-key cryptosystem
  - The security of RSA is guaranteed by the difficulty of factoring a large number ➔ RSA factoring challenge
  - Also very useful for authentication
- Symmetric key system
  - Quantum key distribution (QKD) system

Post-Quantum Cryptography (PQC)

- Is the current security system safe until the working quantum computer will be fully developed?
  - X years: the number of years to develop a large-scale quantum computer
  - Y years: the number of years to develop a new security system which is resilient to quantum computing attack
  - Z years: the lifetime of a secret



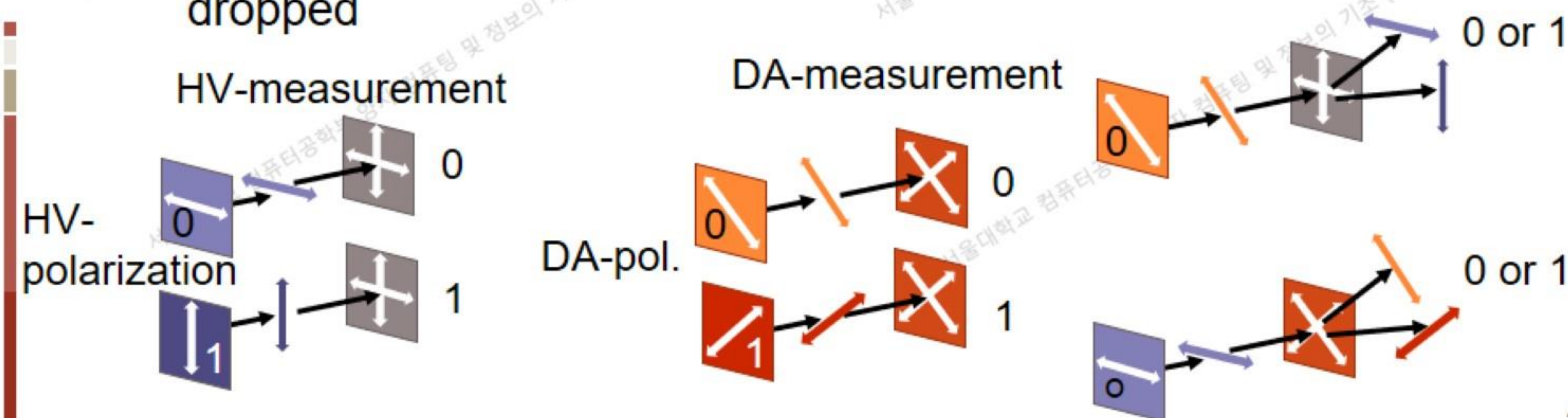
- Alternative: lattice-based cryptography

Quantum Key Distribution (QKD)

- QKD: Quantum Key Distribution
  - One-time pad (OTP) ➔ guarantees the absolute security
  - Provable security system compared to public key infrastructure
- If there is an attempt to eavesdrop on secret key distribution, it can detected by the no-cloning property and superposition principle of quantum mechanics

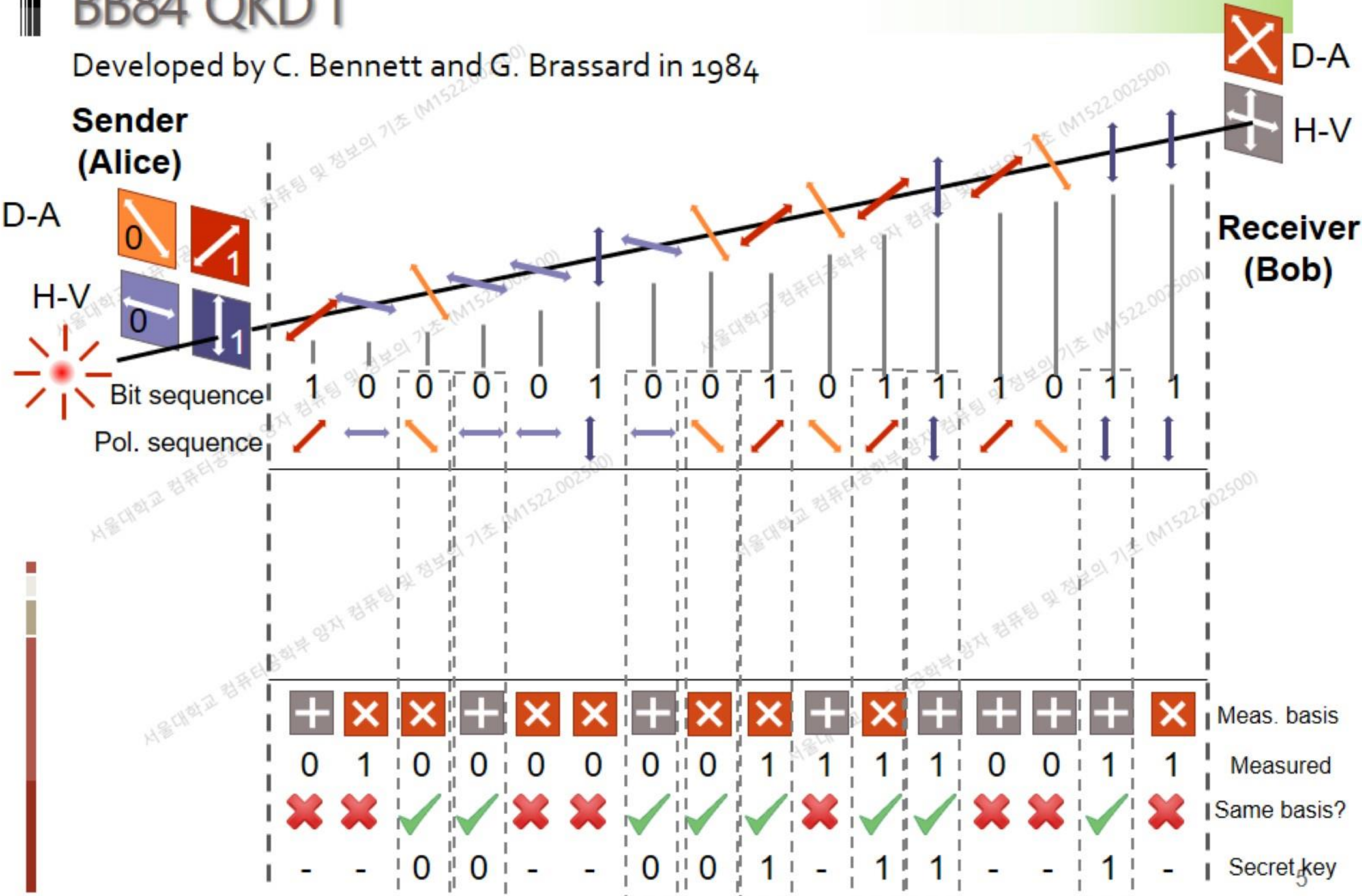
Secret key 0 0011 011... 0 0011 011...

- Secret key does not contain any information by itself
  - Not all the keys need to be transmitted
  - If there is any attempt for eavesdropping, the affected key can be dropped

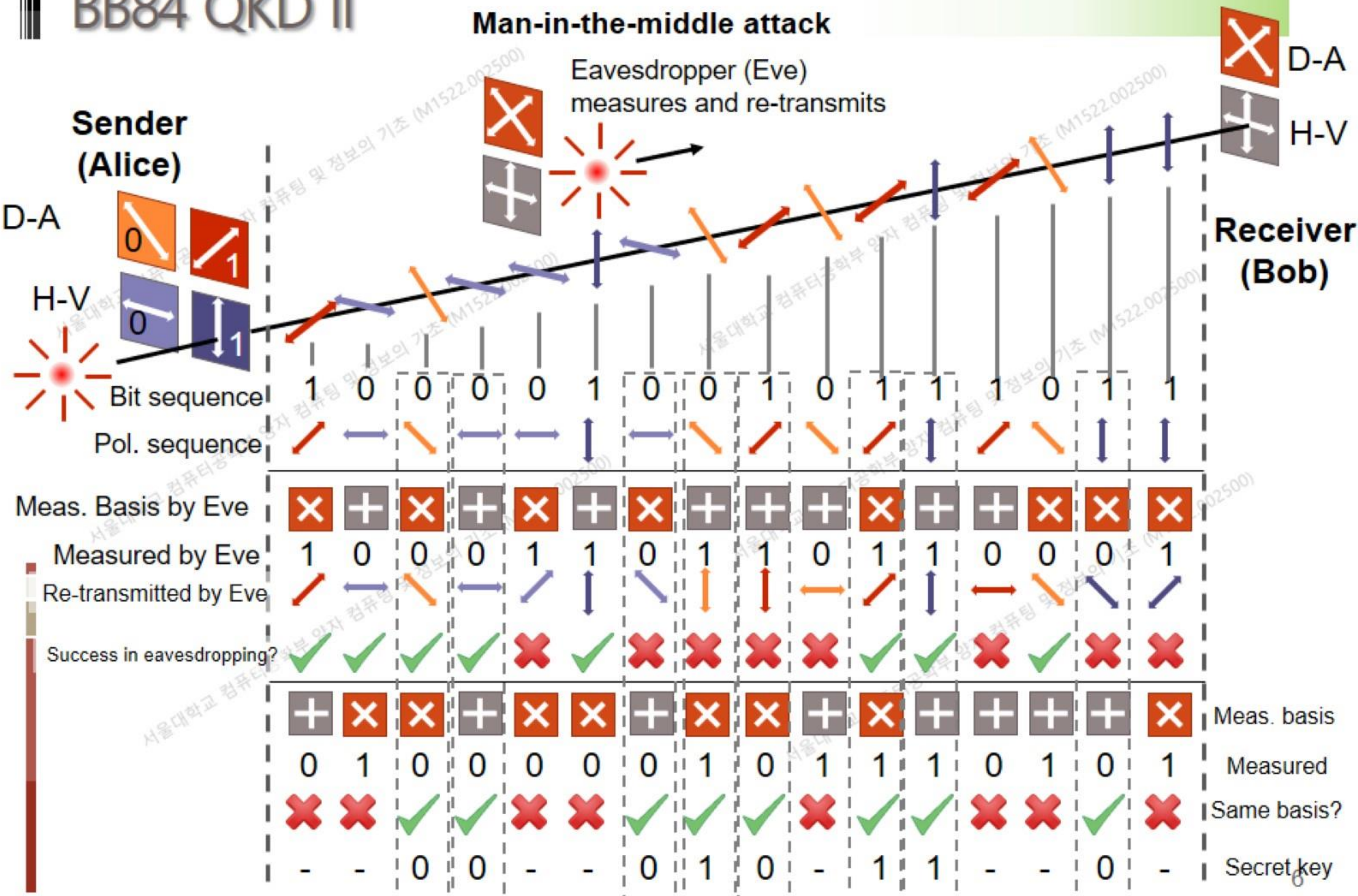


BB84 QKD I

Developed by C. Bennett and G. Brassard in 1984



BB84 QKD II



Man-in-the-middle attack
Eavesdropper (Eve)
measures and re-transmits
Sender
(Alice)
D-A
H-V
0
1
0
1
D-A
H-V
Receiver
(Bob)
Bit sequence 1 0 0 0 0 1 0 0 1 0 1 1 1 0 1 1
Pol. sequence
Meas. Basis by Eve
Measured by Eve 1 0 0 0 1 1 0 1 1 0 1 1 0 0 0 1
Re-transmitted by Eve
Success in eavesdropping?
Meas. basis
Measured 0 1 0 0 0 0 0 1 0 1 1 1 0 1 0 1
Same basis?
Secret key - - 0 0 - - 0 1 0 - 1 1 - - 0 -

Special Property of the Secrete Key

- Recall: secret key does not contain any information by itself
  - Not all the keys need to be transmitted
  - If there is any attempt for eavesdropping, the affected key can be dropped

Secret key `0 0011 011...` `0 0011 011...`

Summary of BB84 QKD protocol I

1. Choice of sender's basis
   - The sender chooses one basis out of two possible bases (+, ×) randomly
2. Choice of sender's bit
   - The sender randomly chooses either 0 (↔, ⤡) or 1 (↕, ⤢) corresponding to basis selected in the step 1 and send the photon.
3. Choice of receiver's basis
   - The receiver also chooses one basis out of two possible basis (+, ×) randomly
4. Measurement by the receiver
   - The receiver measures the polarization of the received photon using the basis selected in the step 3.
5. Repeat step 1 to 4 for a fixed number of times without any additional information exchange
6. Comparison of the basis only
   - The sender and the receiver announces their choice of the basis (in step 1 and 3) for each photon through a public channel
   - However the sender do not share the choice in step 2 and the receiver keeps the measurement result in step 4 secretly

Summary of BB84 QKD protocol II

7. Generation of the 1^{st}-stage secrete key
   - When there is no eavesdropping attack, whenever they used the same basis, the sender's bit in step 2 and the value measured by the receiver in step 4 should be the same
   - These bit sequences become the secret key (sifted key)
   - They discard the bit information when they used the different basis
8. Detection of eavesdropping
   - The sender and the receiver compare randomly-selected part of the secret key generated in step 7 (this can be done in public channel)
   - If there is no discrepancy in this comparison, they can conclude that there was no eavesdropping attack
   - They keep the unexposed part of the 1^{st} –stage secret key as the 2^{nd} –stage secret key
9. Error correction
   - To check if there is any error in the 2^{nd} –stage key obtained in step 8, they calculate a checksum value using a block of secret key. It can be as simple as parity bit.
   - By comparing these checksum values, either error can be corrected or that block can be discarded
10. Privacy amplification
    - During error correction process in step 9, some amount of information about the secret key is exposed
    - To minimize the leakage, the final key with smaller number of bits is extracted from the key from step 9.