講演番号	274

文献番号	20226274

How to Deal with Quantum Computer and Key-Leakage Using General-purpose Cryptographic Technologies

Kyohei TAKEUCHI [1)] **Kohei KISHIMOTO** [1)] **Yuuki NAWA** [1)]

Koji HORI [1)] **Kenichi KOGA** [1)] **Kazukuni KOBARA** [2)]

1) TOKAI RIKA Co., Ltd
3-260 Toyota, Oguchi, Niwa, Aichi, 480-0195, Japan
2) National Institute of Advanced Industrial Science and Technology
Tokyo Waterfront, 2-3-26 Aomi, Koto-ku, Tokyo, 135-0064, Japan

KEY WORDS:**information, communication, and control, secure communication protocol**, quantum computer [E2]

Quantum computers are expected to be able to perform highly parallel processing in specific fields compared to conventional computers due to the quantum superposition. In the field of cryptography, the National Institute of Standards and Technology (NIST) reported that the advent of quantum computers could compromise many cryptographic algorithms currently in use. Quantum computers can solve some mathematical problems that are the root of security for public-key cryptography. Therefore, public-key cryptography will need to be replaced with a secure algorithm against quantum computers.

We investigated a method of having quantum computer resistance using only conventional cryptographic techniques applicable for the automotive microcontroller. As an example of the vehicle system to be hardened against quantum computers, we focused on a digital key system in which a user device opens and closes the vehicle's doors and starts the vehicle's engine. In this paper, we consider a key exchange sequence between the user device and the vehicle, which is secure against quantum computers.

As a core idea of countermeasure to quantum computers, we choose a method called Pre-Shared Key (PSK). If PSK has enough entropy, the secret value shared through our method, which combines Diffie-Hellman (DH) key exchange and PSK, is expected to be secure against quantum computers. This method has only little impact on memory and runtime of the microcontrollers that can implement conventional DH key exchange.

The sequence is shown in Figure 1. At first, the owner inputs *psk* on the owner device (Step 1). The owner device and the vehicle exchange ephemeral DH public keys (Step 2 and 3). The owner device calculates V_A and K from *psk* and *key* shared through DH key exchange, and then sends V_A to the vehicle (Step 4). The vehicle compares the value calculated from *psk* and *key* with the received V_A. If the two values are the same, the vehicle stores K (Step 5). In the next communication, the owner device and the vehicle can establish a secure channel using the stored K.

In our sequence, even if an attacker could use quantum computers, it would not lead to a threat such as unauthorized use of the vehicle. If the attacker eavesdrops on the communicated public key, the attacker would be able to solve its private key by using quantum computers, and then eventually calculate the value shared by DH key exchange. However, unless *psk* is leaked, the attacker cannot calculate the V_A and K. Therefore, the sequence can securely share the secret key between the user devices and the vehicle even in the era of practical quantum computers and against leakage of *psk* before the era.

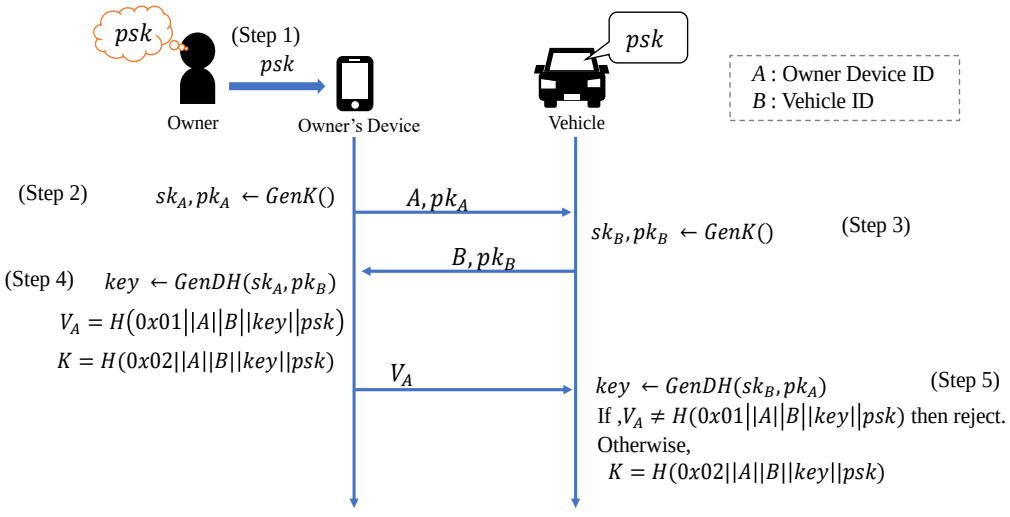

Figure 1 Key exchange sequence