3-4 Secure Transmission of Video Data Relayed by UAV

Ryoji NISHIZAWA, Kazuo ICHIHARA, Toshiyuki ITOH, Mikio FUJIWARA, and Masahide SASAKI

Highly-secure communications with One-Time Pad (OTP)encryption for controls of UAVs was demonstrated in the automatic-book-delivery experiment by UAV which was implemented at Senpoku-city in Akita prefecture on 12th April, 2016 [1][2]. At that time, random numbers used in OTP were provided from the physical random number generator. By using this technology, we newly develop technologies of relay and transmission of OTP encrypted video-data from an UAV with a camera to the ground station relayed by another UAV. Both field experiment which simulated monitoring an outdoor facility, and the indoor experiment which simulated searching missing-person at the time of disaster, were accomplished successfully. In this paper, contents of this development, mainly, and also these experiments are described.

1 Background of development

The quantum ICT advanced development center has already succeeded in a demonstration experiment of encrypted control communication using a drone. The control communication of the drone is performed at a low rate of several hundred Kbps, so it was relatively easy to implement the concealing of data perfectly by using One-time Pad (OTP) encryption. On the other hand, a large volume of data such as videos between drones or between a drone and a ground station is transmitted at a high rate of several Mbps to several tens of Mbps. Hence, a technology to prepare a large amount of random number sequences and synchronize them as keys is necessary. A technology of relaying video via a drone as a wireless repeater is also necessary, because drones for monitoring key facilities or keeping watch over large-scale events need to move around wide areas to capture videos of them. So, we started to develop these technologies.

2 OTP encryption and true random numbers

OTP encryption is a method in which both a sender and a receiver share a true random number sequence as an encryption/decryption key and the sender encodes a plaintext message by applying exclusive OR (XOR) with the encryption key, and the receiver decrypts it by XOR with the same key. After each communication completion, both the sender and the receiver dispose of the used encryption keys as if peeling post-it notes. This method is only one encryption protocol which is certified as information theoretically secure [3]. Also, as XOR at the encryption and decryption is a simple process, the calculation could not be delayed if only true random number sequences whose sizes are the same as that of the data (plaintexts) are shared.

The load capacity of a drone for small distributions is about 5 kilograms and its battery life is about 20 minutes, so the size of the onboard computer is limited in general. The security of public key encryption widely used today depends on the computational complexity, so if the capacity of the computer is limited, the calculation delays or radio interference due to these delays may deteriorate the communication quality. Also, simpler encryption devices increase the risk of decryption by powerful computers. By using OTP encryption, we can conduct information theoretically secure communications without constraints due to a limitation of the capacity of computers until the supplied true random number sequences are used up.

The true random number sequence is a sequence of completely random numbers without any regularity or reproducibility. Random numbers generated by a device which adopts unpredictable physical phenomena such as thermal noise or quantum mechanical phenomena have such a property. As generation rates with such generation methods are low, pseudo-random numbers generated by a determined computational algorithm are used for most cases of cryptography in general. However, pseudo-random number sequences have periodicity and powerful computers can decrypt such cryptography. Therefore, true random

number sequences are indispensable to implement information theoretically secure communications.

In OTP encryption, the same size of true random number sequences as that of the transmitted data is necessary. However, it is sufficiently possible to minimize the amount of random number sequences enough to implement the secure communication despite a small capacity of memory, because the flight time of drones is so limited. Also, the delay time in calculation process is very small in encryption and decryption because only XOR between the key and data or cryptogram is applied, so it is possible to implement a very light physical circuit constitution with a fast encryption process at low cost. Stealing encryption keys by unauthorized drone can be eliminated by a device authentication using true random number sequences, though the true random number sequences should be shared with communication terminals in advance.

This device authentication is an application of message authentication where a device is authenticated as a client when the Message Authentication Codes[*1] between communication devices derived from the shared message (a true random number sequence) by using the Hash Function[*2] coincide (Wegman-Carter authentication method [4]). Moreover, both the shared message and the Hash Function are generated by true random number sequences and the device authentications are conducted by both devices to implement a strongly secure function to prevent spoofing.

3 Video data relays

In a camera drone equipped with a video camera, a cryptogram of a packet (a bit sequence) of video data from the camera is generated by XOR with the encryption key and transmitted to a relay drone. The relay drone receives the encrypted video data with a directional antenna and relays the data to a ground station without decryption. The received cryptogram is decrypted by the encryption key at the ground station (Fig. 1).

Low-cost commercial Wi-Fi devices (Air Station Pro WAPS-AG300 H: directional sectored-antenna WLE-HG-DA/AG with horizontal pattern 60 ± 5°, vertical pattern 65 ± 5°, is attached: comply with IEEE 802.11 b/g, made by Buffalo), which does not require a radio license, are used for this system. Implementation of secret video data transmission in an area out of radio wave attainment range using an inexpensive and easy method with the general outdoor Wi-Fi frequency (2.4 GHz band) (Fig. 2).

The camera drone for taking video and the ground station share a true random number sequence as the encryption key in advance to provide communication with perfect secrecy by using OTP encryption for each packet of control communication or data communication. As a loss of data occurs frequently in drone communications due to large variation of properties of channels, a new system is necessary to synchronize a large amount of encryption keys accurately between the drone and the ground station and to update it. We developed a technology to transmit a key synchronization code at an optimized packet interval depending on the channel properties. This technology makes it possible to continue to transmit new video data taken by the camera with low latency, while suppressing deterioration of data transmission efficiency and implementing a key synchronization.

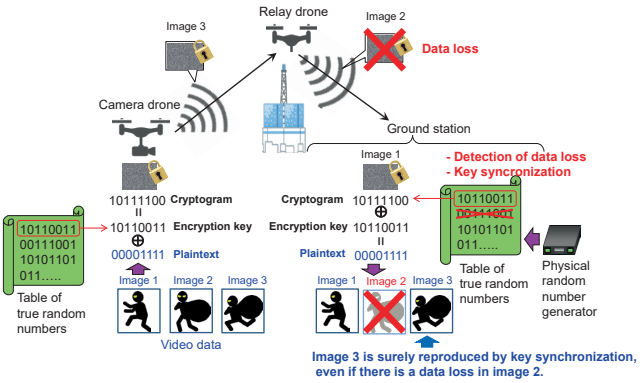

Fig. 1 Relaying data by a drone with perfect secrecy

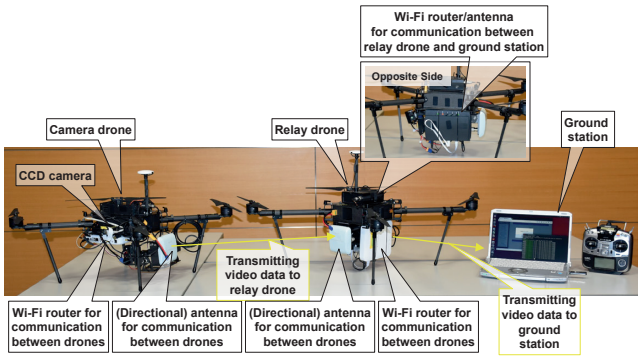

Fig. 2 Components of the system
(Left: Camera drone, Center: Relay drone, Right: Ground station)

*1 Message Authentication Code (MAC) is a small fixed length code to authenticate that the transmitted message is not falsified. MAC is obtained by calculating a message using the Hash Function.

*2 A Hash Function is a one-directional function that outputs code (bit sequence) of a small fixed length from input data. It always outputs the same code if the input data is the same.

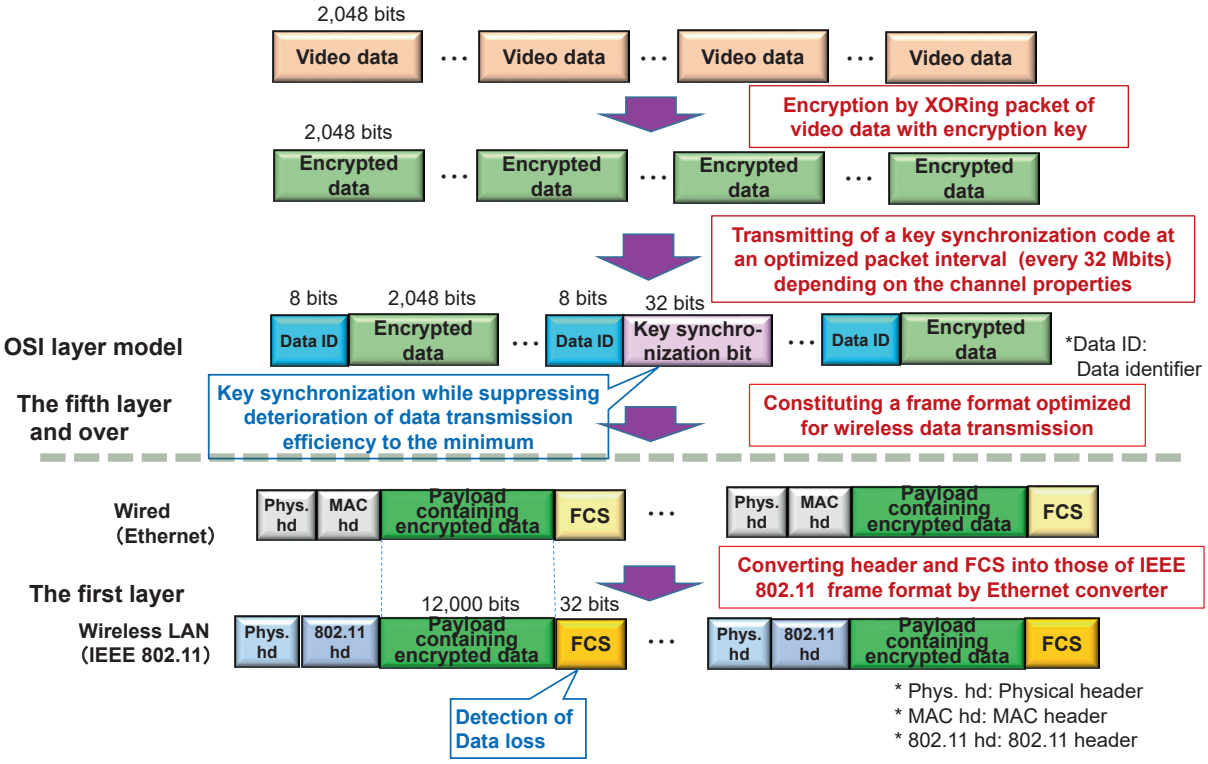

Fig. 3 Outline of OTP encryption for video data in case of data loss

4 Communication packet structure

The video data is comprised of 15 frames per second (standard frame size is 320 × 240 pixel) compressed with H.264 (one of the video compression standards of MPEG). The rate of data transmission is relatively high at 12 Mbps and the duration of shooting and transmission per experiment is about 15 minutes. Therefore, the necessary size of the true random numbers per experiment is about 11 Gbits.

As the channel property of the drone communications easily fluctuates and loss of data occurs frequently, a system to synchronize many true random number sequences and update the encryption key to conceal transmitted video data perfectly was needed. So, we developed a technology to transmit key synchronization codes at an optimized packet interval depending on the channel properties to cope with such packet losses during the data transmission. Also, as a real-time capture of the monitored target is required for monitoring systems by video cameras, UDP (User Datagram Protocol) as a protocol in the fourth layer (transport layer) of the OSI layer model was used in this experiment not to retransmit lost data but to reproduce the video in real time as possible by synchronizing with the key of the next packet. Also, even if a loss of long-time (one-second) data occurs, this system enables guaranteeing the key synchronization between the sender and the receiver by transmitting a key synchronization code at an optimized bit interval (32 Mbit in this experiment).

A rough structure of the packets is shown in Fig. 3. Each segment, into which the video data is divided at 2,048 bits, is XORed with a true random number sequence of the same size as that of the segment, and is prefixed with an 8-bit ID header. Here, a key synchronization code of 32 bits is inserted into the video data at every 32 Mbits (identification ID header is also added to this code). These are payloads which are packetized below a transport layer. Here, a packet is a Media Access Control Frame[*3] according to the Ethernet frame format. The MAC header is removed by Ethernet converter when transmitted by wireless to be encapsulated according to IEEE 802.11. Data loss due to packet loss in wireless transmission is detected by 32-bit FCS (Frame Check Sequence) added at encapsulation.

The video data from the camera drone is sent at low latency with accurate OTP encryption, while suppressing deterioration of data transmission efficiency by correcting the time gap of synchronization of the true random number sequences of the above key synchronization code. Also, in case that a loss of data is detected, the ground station

*3 Media Access Control (MAC) frame is a small data group to which control information such as destination is added in Ethernet. Data is exchanged by frame in Ethernet of which the size range is 514-12,144 bits.

does not require resending the data and the next received packet is decrypted abandoning the previous lost packet in order not to miss the movement of the monitored target while continuing to receive the data from the camera drone.

5 Open-air field experiments

We conducted an experiment on Wednesday, February 22, 2017, at an open-air test field in the suburbs of Toyota city in Aichi Prefecture. We simulated a monitoring mission from the sky of a video of a suspicious person (monitored target) taken by a camera drone which is received by a ground station via a relay drone (Fig. 4).

The experiment was conducted several times, for about 15 minutes each time. The camera drone flew around the patrol area behind trees where it could not be seen from the ground station. Then, the camera drone transmitted encrypted video data to the relay drone waiting in the air 50-100 meters away from the camera drone. The relay drone received the video data with a directional antenna and relayed the data to the ground station placed about 10 meters away from the relay drone. The ground station decrypted and reproduced the video by using the same encryption key as that used in the camera drone. The experiments were conducted assuming that the video data taken by a monitoring camera is transmitted with perfect secrecy.

To simulate disconnection of relay, the relay drone moved (left end in Fig. 4) so that communication between the drones was interrupted by the forest when the camera drone moved to the boundary of the experiment area (upper edge in Fig. 4). Before the experiment, we received permission from Toyota city in Aichi Pref. who managed the area (as for controls of the drone, we assigned one operator for one drone so that any unexpected incidents such as flights out of direct line of sight or unforeseen crashes could be prevented by manual operation at any time).

We observed the communication status between the ground station and the camera drone, by taking a video of reproduced video by a handheld video camera and by recording the response time of PING[*4] sent every one second from the ground station to the video camera. In addition to the reproduced video, the whole view and actual conditions of the experiment were recorded by a handheld video camera (see NICT's press release "Development of relaying video data by a drone with perfect secrecy" (only in Japanese): http://www.nict.go.jp/press/2017/03/22-1.html)

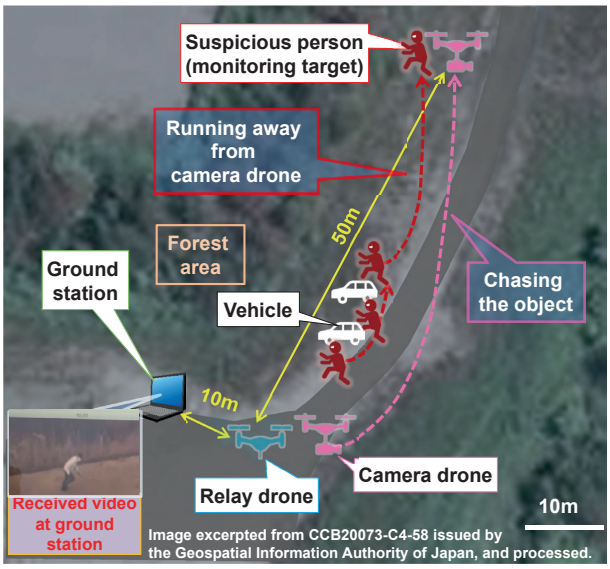

Fig. 4 Experiment of simulation of monitoring mission using drone implementing data relay system with perfect secrecy. Configuration of ground station — relay drone — camera drone. The inserted image is a received video at the ground station.

The videos were reproduced smoothly in real time at the ground station without drop-frames (loss of image data). Hence, the function of video relay, encryption and decryption of the video data in this component system were verified to work without problems at this experiment. When the relay drone moved to hide behind the forest (coverage hole) to simulate communication disruption, video reproduction at the ground station froze and the PING response disappeared completely. But the PING response reappeared and the video reproduction restarted again skipping the video taken when the communication was disrupted after the relay drone moved back to the original position for relaying. From the above, it was confirmed that encrypted data was decrypted by matching the encryption key at both the sender and the receiver with key synchronization code inserted into the video data periodically, even though the transmission of encrypted video data was disrupted.

We succeeded in relaying video data without any serious problems, but a phenomenon occurred where reproduction of the video paused for about 5 seconds when the

*4 PING is standard software installed to verify the reachability of a node on the IP (Internet Protocol) network. Network connection can be verified by sending a packet of a certain size and confirming its response. As it shows response speed, the speed of the network can also be confirmed. The name stems from the echo ("ping") of active sonar that submarine sounds in underwater, because the behavior is like sonar.

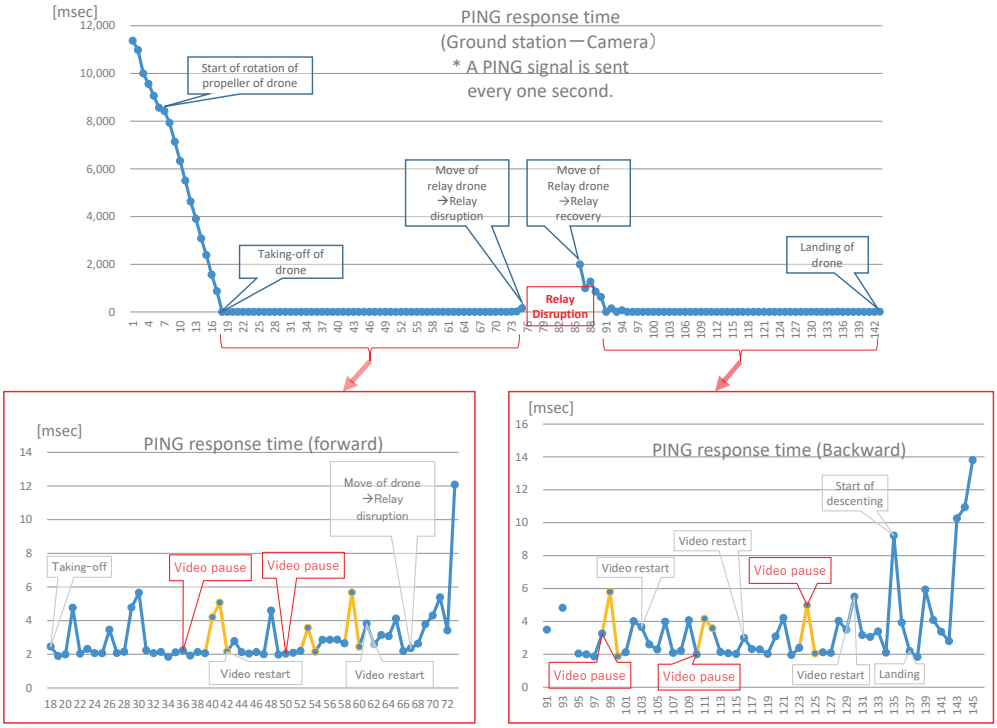

Fig. 5 PING response time between the ground station and the camera drone (horizontal axis represents the serial number assigned to the PING signals)

camera drone passed a certain area (around the vehicles seen at the center in Fig. 4) and then reproduced at faster speed without drop-frames. We supposed that such delays in the transmission of the video data occurred due to Interference Fading[*5] caused by the reflection of communication radio waves due to iron plates of the vehicle. So, we moved all vehicles to outside the experiment area, but the same phenomenon occurred. Hence, we concluded that some reason other than the effect of the vehicle might have caused the delay in communication at that point (Actually, the PING response time always increased slightly when video reproduction paused. Fig. 5).

There were three base stations for mobile phones near the test field. We will investigate the cause of such phenomena including the effect by the base stations.

6 Indoor experiment

We conducted an indoor experiment on Sunday, February 26, 2016, at the auditorium (20 m × 17 m × 7 m height) in the No.4 building of NICT in Koganei city, Tokyo. We simulated the investigation mission in an important facility in danger of collapse due to a disaster. We simulated the condition where image data taken by the camera drone that is visually isolated from the ground station set outside of the auditorium was transmitted to the ground station via the relay drone (Fig. 6).

Several experiments were conducted, each of them was about ten minutes. The distances between drones and between the relay drone and the ground station were kept at about 10 meters, according to the scenario where the camera drone investigated inside the auditorium. In addition, a partition (7.8 m width × 1.8 m height) was set between the camera drone and the ground station so that the radio waves emitted from the camera drone would not reach to the ground station directly. Communications of encrypted video data and the procedure to reproduce the video data were verified in the same way as conducted by the open-air fields experiments. However, the experiment of disruption was skipped because it was outside the scope of verifying the indoor communication condition.

As for the condition of communication between the ground station and the camera drone, we verified only the security of data transmission inside the building and reproduction of the video data. For this purpose, we observed it by taking videos of reproduced video data at the ground station. In addition to the reproduction of the video data,

*5 Interference fading is a phenomenon that the received signal level at the radio station varies due to constructive and destructive interference, because the phases of the radio waves from the sender to the receiver shift at the receiver due to the difference of the path caused by reflection by objects therein. Sometimes radio waves cannot be received.

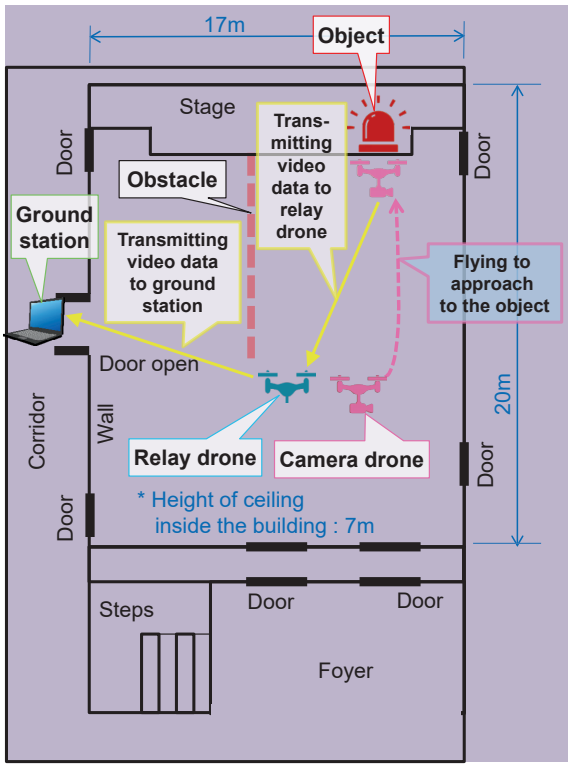

Fig. 6 Configuration of indoor experiment. Operators were assigned for manual operation of drones. (between ground station and relay drone, the distance between each drone is about 10 meters)

the whole view of the experiment was taken by a handheld video camera (see NICT's press release "Development of relaying video data by a drone with perfect secrecy" (only in Japanese): http://www.nict.go.jp/press/2017/03/22-1.html)

The videos were reproduced smoothly in real time at the ground station without drop-frames (loss of image data). The phenomenon of paused reproduction of video data seen in the open-air experiment did not occur. From the above, the functions of video relay and encryption and decryption of the video were confirmed to work without problems under not only outdoor but also indoor environmental conditions.

7 Prospects for the future

In the future, we will promote the development of compact and reliable encryption and decryption devices. Also, we will conduct experiments to study the distribution of radio wave intensity in the data transmission with the system of the components we used for these experiments, by conducting a communication experiment in a non-echoic chamber which will be utilized in developing technologies of relaying data. Moreover, we will develop technologies to construct a flexible relaying network for various purposes and large areas by increasing both cameras and relay drones, as well as continue implementing experiments on reliability to utilize for monitoring key facilities which it is difficult for humans to enter.

References

1 T. Itoh, et al. "Security Enhanced Drone Control System and Its Application," IEICE Society Conference 2016 – Engineering Sciences Society / NOLTA Society, AI-3-5, SS-33, Sept. 2016.
2 T. Itoh, et al. "Highly Secure Drone Communications Network," IEICE General Conference 2017, AI-3-2, SS-50, March 2017.
3 C. E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, vol.28(4), pp.656–715 (1949).
4 M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," Journal of Computer and System Sciences, vol.22, no.3 pp.265–279 (1981).

Ryoji NISHIZAWA
Engineer, Quantum ICT Advanced Development Center, Advanced ICT Research Institute
UAV communications

Kazuo ICHIHARA
Managing Director, Prodrone Co., Ltd.
UAV controls & communications

Toshiyuki ITOH, Ph.D
Researcher, Quantum ICT Advanced Development Center, Advanced ICT Reseach Institute
Physical layer cryptography, Free space optical communication

Mikio FUJIWARA, Ph.D
Research Manager, Qunatum ICT Advanced Development Center, Advanced ICT Reseach Institute
Quantum key distribution, Photon detection techology, Cryogenic electronics

Masahide SASAKI, Ph.D

Distinguished Researcher, Advanced ICT Research Institute
Quantum communication, Quantum cryptography