Communication and information processing

Secure, fast, light encryption based on non-commutative algebra

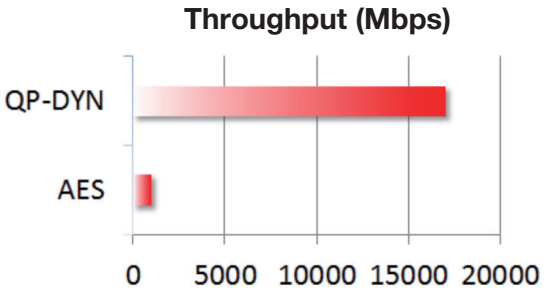
Satoshi IRIYAMA (Associate Professor, Department of Information Sciences, Faculty of Science and Technology, Tokyo University of Science)

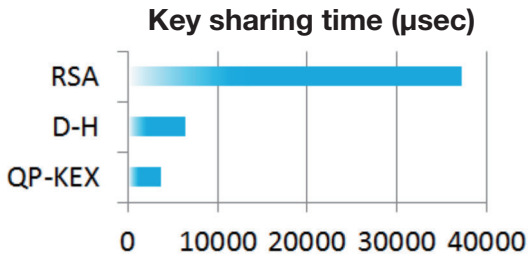
Purpose of Research

Prof. Emeritus Ohya (TUS) and Prof. Accardi (University of Rome II) have developed a novel encryption method as a result of their more than 20 years of study on mathematics (noncommutative algebra and noncommutative probability theories). We are studying a cipher based on noncommutative algebra and an encryption method based on a new principle.

Summary of Research

The shared key stream cipher (QP-DYN), based on a unique mathematical theory, can generate high-quality random numbers. The public key exchange (QP-KEX) is based on mathematics that can be reduced to a matrix type discrete logarithm problem and is safe. It does vector calculation and allows parallel processing for fast encryption.





Cryptobox
(8 cm x 8 cm, 500 g)

Points

- **Safer One-Time-Pad cipher**
- **Faster key generation, key exchange, and encryption**
- **Smaller and lighter circuit**

Comparison with Conventional or Competitive Technology

Throughput more than 10 times faster than AES was achieved. Key generation and key exchange was about 10 times faster than RSA. When implemented on FPGA, the circuit size was about 75% that of AES.

Expected Applications

- High-speed processing by a cloud server, etc.
- Higher safety in a mobile environment
- Real-time processing for 4K/8K video distribution

Challenges in Implementation

- Development of attractive services
- Registration as an encryption standard
- Standardization of specifications

What We Expect from Companies

Collaboration on the installation on a smaller chip and the product/service/application development of the new encryption method.

Future Developments

Many pilot products are being developed. These will be broadly publicized both in Japan and overseas.

■Prototype:
Portable encryption device “Cryptobox,” Email encryption (compatible with Outlook and Google), and mobile App.