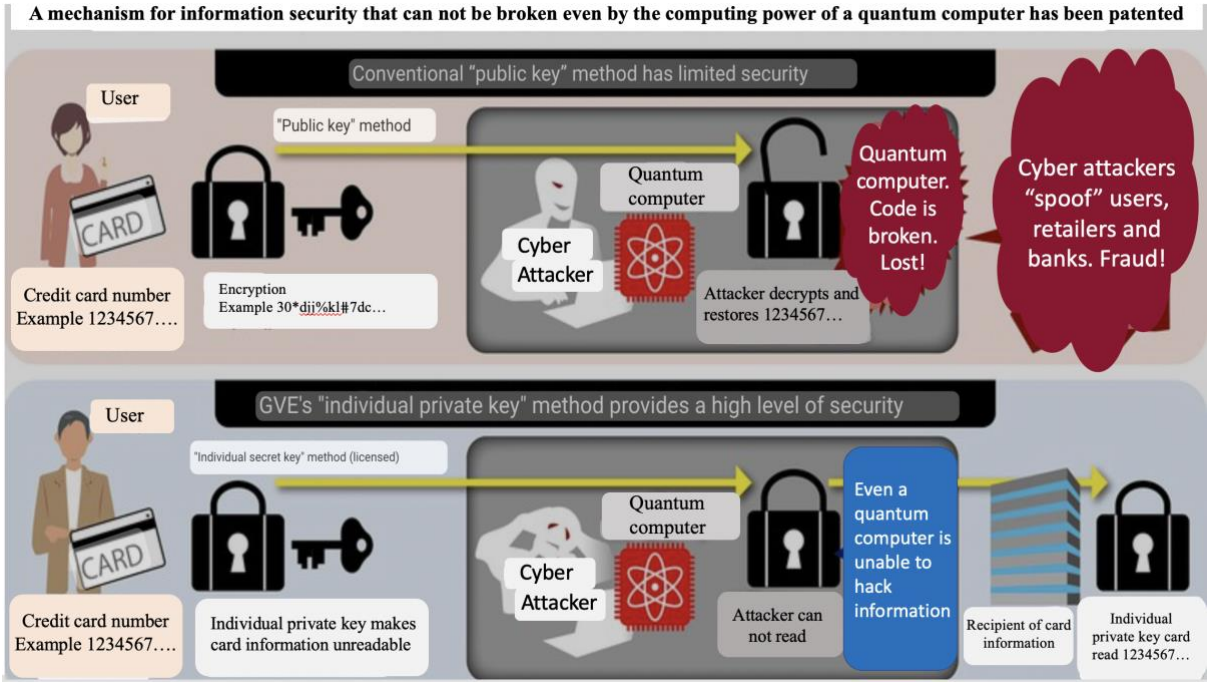
The Weekly Economist 22 August, 2022

A ground breaking cyber security ‘basic patent,’ filed by GVE heralds the arrival of a Japanese company set to stand alongside the GAFAM

Tatsuya Ohori



With the advent of quantum computers in the mid-2020s, experts believe that all existing encryption technology will become obsolete. The very foundations of the information society will be undermined.

A Technology likely to become a basic patent underpinning the Internet is set to rival the GAFA(M)

On April 26 2022, Tokyo based Fintech company GVE was granted a patent in Japan for its ‘cyber security’ mechanism that provides protection against hacking, and other forms of cyber-attacks, which are now a chronic problem for on line Internet payment systems.

The fundamental flaw of the Internet

特　許　証
(CERTIFICATE OF PATENT)

特許第７０６４２１９号
(PATENT NUMBER)

発明の名称
(TITLE OF THE INVENTION)

秘密鍵方式の電子署名装置
Private key electronic signature device.

特許権者
(PATENTEE)

東京都中央区日本橋兜町１３番１号

ＧＶＥ株式会社

GVE's patent is a 'private key electronic signature device.' Since its foundation in 2017, GVE has regarded cybersecurity as the fundamental problem in the 'digital space,' defying even the best efforts of the world's largest IT companies. The development of a technology, and mechanism to solve the problem of security has been at the heart of the company's growth strategy. As highlighted previously in this publication, work on the issue of security has proceeded alongside GVE's efforts to introduce its EXC digital currency platform, to emerging countries, such as Nepal, which are aiming to introduce central bank digital currencies (CBDC).

Koji Fusa, the president of GVE, has had a long career in the financial sector, including serving as the head of the Japanese subsidiary of the UBS Group, an international financial institution based in Switzerland. It became obvious to Koji that, "the constant data leaks, which occur when sending money, and verifying identities on line are due to the fundamental characteristics of the Internet, an unrestricted domain, open to an unspecified number of people." There are various cryptographic technologies that protect information on the Internet, but the world has not yet developed a means of "protecting information perfectly."

Against this background, in 2017, Koji Fusa teamed up with a former Sony engineer, Susumu Kusakabe. Susumu is famous for his work in inventing 'FeliCa,' the contactless IC

card technology that enables payment functions, such as NTT Docomo's Smartphone payment system, 'Osaifu-Keitai.' "We set out to develop 'the ultimate information protection mechanism.'" On December 1, 2020, just four years after the company was established, "we filed an 'international application,' with the aim of obtaining a patent."

Mr. Fusa says, "our goal was to develop a technology, which would establish a 'basic patent,' which would stand comparison with the GAFA(M)." A basic patent is a patent that serves as the 'foundation,' from which various patents are derived. According to the Japan Patent Office, patents are defined as "inventions that enable new functions not realized by prior art." Many improvement patents are derived from basic patents. For example, the biggest reason for the success of US IT companies, such as the GAFA(M), is that they have obtained strong basic patents, which have served as the basis for establishing global standards.

'Individual private keys' overturning common sense

Koji Fusa states, "our technology has gone beyond the 'limitations' of current cryptographic technology. These limitations mean that current encryption mechanisms will be easily broken when next generation ultra-high-speed computers such as quantum computers appear."

Currently, the cryptography employed in credit card numbers, for example, uses ciphers, (RSA cryptography) based on 'prime numbers,' a natural number equal to, or greater than 2, which is only divisible by 1 and itself. For example, online shopping users encrypt their credit card numbers, and send them to merchants. In this case, the number used for encryption is a prime number, actually a product of huge prime numbers, called a 'public key.'

In the current 'public key' format, encryption and decryption, decryption and the restoration of contents, are performed using a combination of a 'private key' held individually by the user, or retailer, and an 'individual public key' created from the public key established by the card company.

The decryption side notifies the encryption side of its own public key in advance. It makes it public, so it is called a 'public key.' As users, since a series of such encryption flows are performed automatically, we are not usually aware of the process.

Only the user knows the private key. Security is maintained as long as the private key is not leaked. In order to discover the card number based only on knowledge of the public key, without knowing the private key, you would need to "factorize an extremely large number." Even today's supercomputers cannot discover card numbers in "real time." Almost all mechanisms that use public key methods, including RSA encryption, are based on the premise that the private key cannot be guessed from the public key.

Conversely, this means that the foundation of the mechanism will collapse the moment "a technology that can guess the private key from the public key" is developed. If quantum computers continue to develop at their current speed, even difficult calculations such as

factoring a huge number of primes will be completed instantaneously, and current encryption methods will be easily broken.

Once ‘encryption rules’ are deciphered then information such as account numbers, and passwords become “naked.” The figure at the top of this article illustrates how the unauthorized acquisition of such information permits financial fraud through ‘spoofing.’

In Japan, an example of such action occurred in 2020 when fraudulent withdrawals occurred via NTT DoCoMo's electronic payment service, DoCoMo Kouza. Criminals who obtained the account numbers, and PINs of depositors at multiple regional banks opened DoCoMo accounts by pretending to be depositors, and then withdrew money from the deposits held at the bank accounts. If cryptographic technology remains in its current form, then the arrival of quantum computers may make such events common place.

Therefore, as a mechanism that cannot be broken by quantum computers, GVE came up with the idea of creating individual keys for each user, and for each service when sending information.

This mechanism is called an ‘individual private key.’(Fig.). In contrast to the conventional RSA based encryption mechanism, which uses a public key, individual private keys are secure even from quantum computers. GVE has been granted a payment for the individual private key mechanism.

The individual private key is completely different from the current public key. Koji Fusa says that even without the advent of quantum computers, a higher level of security can be achieved by moving away from public keys to individual private keys.

In order to realize the idea of individual private keys, advances in technology were also required. In order to put individual private keys into practical use, it is necessary to give each individual user a different individual private key for each service, requiring a vast number of keys. For example, if 100 million people each use 10 services, that alone would require 1 billion individual private keys. The world has a population of 8 billion people and 300 million corporations. A very large number of keys are required to handle this many individuals and corporations. GVE has also created a system, which can facilitate the creation of the necessary number of keys.

However, it is the idea of the individual private key that is revolutionary. “Individual private keys” is an area that until now no one has attempted to implement. “Cybersecurity is a ‘blue ocean,’” says Koji Fusa. A blue ocean refers to a completely new market that did not exist before, the opposite of a ‘red ocean,’ a state of excessive competition .

The power of a basic patent

GVE also aims to obtain a patent in the United States. Koji Fusa says, “since we were able to obtain a patent in Japan through an international application, we believe that the originality of

the idea will be recognized in the United States as well." I asked Koji if GVE will work with credit card companies to encourage them to switch to the individual private key system? He replied, "even if we were not to do so, then once they know that the conventional method is dangerous, the card company will come to us and say, "we want you to use your patented technology." It is a simple as that.""

There are currently no innovations comparable to the individual private key mechanism. It is highly unique. This is a feature of a basic patent. If we look back over the last twenty years, US IT 'Big Tech' offers typical examples of successful companies, which hold basic patents. Apple originated the concept of a 'Smartphone,' and patented its technical features into a basic patent. Scores of manufacturers have adopted the idea, and are paying patent fees. The inventors of basic patents, such as Apple, create mega-hit products, the iPhone, and, at the same time earn huge patent income.

Other examples of basic patents are Google's core search engine technology, 'PageRank,' that determines the importance of a web page, and Amazon's '1-Click,' an order and payment mechanism, which facilitates on line sales.

As of the end of July 2022, US Big Tech occupied the top tier of companies in the world by market capitalization. Starting with Apple, the world's most valuable company at US$2.7 trillion, Google's parent company, Alphabet (4th), and Amazon (5th), have all expanded their businesses based on basic patents.

On the other hand, one of the reasons why Japanese companies are said to have fallen behind in the Internet age is that they have been unable to develop basic patents, which establish global standards.

Of course, it is very difficult to identify an invention that can be used as a basic patent for creating a new business. Therefore, many Japanese companies choose to develop business models based on platforms built by US Big Tech. These are not basic patents, but the improved patents derived from the basic patent.

Trying to create something new that has not yet appeared in the world is a tough road. However, the fruits of success are great. Apple founder Steve Jobs, who brought the iPhone to the world, Google co-founders Larry Page and Sergey Brin, who published a paper on search engines when they were students at Stanford University, and Microsoft founder, Bill Gates, who created the personal computer OS Windows, are prime examples.

When quantum computers become reality, and if individual private keys are used as an essential element for data security around the world, then there is a real possibility that Big Tech will emerge from Japan.

Tatsuya Ohori, Editorial Department