# Mathematics and War in Japan

Setsuo Fukutomi*

The first, shorter part of the article describes the anti-war movement among Japanese mathematicians during the Vietnam War. In the second, longer part, the author decribes the decoding program of the Japanese Army during World War II, in which he worked himself as a drafted soldier, at the defeat, all written evidence regarding this program and its collaborators was destroyed. Today, the only surviving participant in the project apart from the author is Commander Kamaga, its initiator and leader (alias Kato Masataka, his pen name as a cryptographic author).

## 1 The Movements of Japanese Mathematicians against the Vietnam War

In April 1965, Professor Laurent Schwartz was in Japan. He informed the Japanese mathematicians that Steven Smale, mathematics professor at the University of California at Berkeley, had created a protest movement against the Vietnam War, and invited the Japanese mathematicians to support Professor Smale's initiative. He received 183 signatures from Japanese mathematicians in solidarity with Professor Smale's anti-war campaign, which was announced publicly at the annual meeting of the Mathematical Society of Japan in May 1965.

At that moment, a civic movement against the American war in Vietnam was already in existence, arranged by the Japan "Peace for Vietnam" Committee (BEHEIREN in Japanese abbreviation, henceforth JPVC).

While the U.S. "Vietnam Day Committee" (of which Professor Smale was one of the principal organizers) was founded in Berkeley, Makoto Oda, president of the JPVC and writer, agreed with Professor Smale to organize a coordinated manifestation against the Vietnam War on the same day in Japan and in the United States, namely on May 22, 1965. They decided to establish a lasting collaboration between the two countries against this war in Vietnam, thus making the JPVC one of the foci of the Japanese movements against the Vietnam War. The anti-war movement of Japanese mathematicians ("Committee of Japanese Mathematicians Against the War in Vietnam", henceforth CJMAWV) often collaborated with the JPVC.

The mathematicians of the University of Kyushu (South Japan) demonstrated against the Vietnam War three times each month, the 10$^{th}$, the 20$^{th}$ and the 30$^{th}$ ("demonstrations of the ten"). The mathematicians were leading in the movements

* Professor of mathematics (retired) at the Tokyo University of Agriculture and Technology.

Gut-zu-Druck: 29.7.2003

of Japanese scientists against the Vietnam War and the American invasion of Vietnam.

In February 1966, CJMAWV made an appeal and organized a demonstration against the American B52 bombings of North Vietnam, asking at the same time the Japanese population to express solidarity with its activities. An appeal was also made to the mathematicians of the whole world to organize a meeting on the occasion of the International Congress of Mathematicians (ICM) in Moscow in August 1966. Indeed, this meeting was held in Moscow thanks to the efforts and the collaboration of the mathematicians L. SCHWARTZ, E. B. DYNKIN, S. IYANAGA, Chandler DAVIS and others, who were joined by Professor SMALE. Professor SCHWARTZ and Professor DYNKIN also invited the mathematicians of the whole world to sign an appeal against the Vietnam War. The appeal voiced the strong opposition of the mathematicians gathered in Moscow to the war that was waged by the American armed forces and was becoming increasingly cruel every day, and stated that President JOHNSON's strategy of "escalation" could lead to no equitable solution; the appeal affirmed the sovereignty of the Vietnamese people and its right to self-determination, and finally expressed its solidarity with those American mathematicians who fought against this Vietnam War which dishonoured their country.

The appeal was published in Tokyo and Paris with 628 signatures of mathematicians from 26 countries (Japan excluded) and 1333 signatures of Japanese mathematicians.

Afterwards, several dozens of Japanese mathematicians went on organizing manifestations against the invasion of Vietnam by the American armed forces on the occasions of the Annual Meetings and the Autumn Meetings of the Mathematical Society of Japan in the cities where these meetings took place.

The (rather vague) notions of a professional community of mathematicians, shaped in research and teaching activities, allowed the mathematicians to continue these movements against the Vietnam War lastingly. These were thus civic movements carried by a community that was defined professionally and not geographically. The participants did not think of themselves primarily as mathematicians, nor was it much discussed whether and how mathematics (and mathematicians) were involved in the war...

In spite of this ambiguity, the mathematicians were the only Japanese scientists that organized meetings and manifestations against the French nuclear tests in the Pacific (Mururoa), against the terrorist attacks in New York, and against G. W. BUSH's wars of revenge in Afghanistan.

## 2 Japanese Mathematicians' Military Research and Collaboration with the Military during World War II

The following treats of the author's own experience in cryptographic research, in particular in decoding (cryptanalysis), in the Japanese armed forces during the 1940s.

Gut-zu-Druck: 29.7.2003

Toward June 1943, Commander Kazuo KAMAGA from the General Staff of the Army requested the collaboration of mathematicians with the armed forces for studies of the mathematical foundations of military coding. At first his idea was to create an undecipherable (unbreakable) cryptography, but later he concentrated on mathematical research in decoding (cryptanalysis). He asked for the collaboration of the Mathematics Department of the Imperial University of Tokyo.

Commander KAMAGA started by giving preparatory cryptography courses to mathematicians, mainly coming from the Imperial University of Tokyo. This resulted in the official establishment of the Mathematical Seminary of the Army on April 3, 1944, formed by mathematicians from the Imperial University of Tokyo, of Tohoku, and of Osaka.

Studies of Euler squares were considered important for the creation of a new code and for the error-free transmission of coded messages; so were studies of the theory of Galois fields. Professor Y. KAWADA undertook profound studies of the distribution of consecutive letters in English phrases applying the theory of Markov chains. Professor Kunihiko KODAIRA (winner of the Fields Medal 1954) studied some types of permutations for the analysis of the Enigma. Commander KAMAGA himself concentrated on studies of error-correcting encoding. His studies in this domain are precursors of the modern theory of such codes, for instance the encoding theory of R. W. HAMMING.

With KAMAGA, a team headed by the mathematician Kōichi YAMAMOTO, engineer of the General Staff of the Army, worked much on constructing Euler squares of order n, aiming first of all at the creation of a new cryptography. After the war, this engineer-mathematician became Professor of mathematics at several universities, making fruitful teaching and research in the theory of combinatorics.

Before the war, the Japanese Army had "stolen" the American strip-cipher code (i.e., code book). One had secretly photographed the diplomatic code-books for communication between Washington, Tokyo, and Tch'ang-Tch'ouen. This code was based on several tens (between 50 and 100) of bars, each carrying the same permutation of the alphabet twice. Each day, a number of bars (from 20 to 30) were chosen in order to create a clear text, picking one letter from one vertically positioned bar, another one from another bar, etc., ordering them afterwards from left to right so as to produce a text horizontally. In a certain distance upwards or downwards, if reading a line of letters from left to right, one obtains an apparently illegible text as encoded text (see Figure 2).

This encoding was very efficacious and resistant to decoding. We were no longer able to decode it after the Americans changed the code-books that had been "stolen". We worked much on breaking its keys. The studies of the distribution of consecutive letters of the alphabet in English phrases served the same purpose. The author (S. FUKUTOMI) used indeterminant equations for breaking strip cipher.

Concomitantly, the Japanese Army had decided in 1943 to recruit graduates in mathematics for work in cryptanalysis. Its interests concentrated on the "strip-cipher" and the cipher machine "M209". The machine M209 was furnished with six coaxial disks arranged on a horizontal bar. They carried, respectively, 26, 25, 23, 21, 19 and 17 letters of the alphabet (pairwise relatively prime integers). If one

Gut-zu-Druck: 29.7.2003

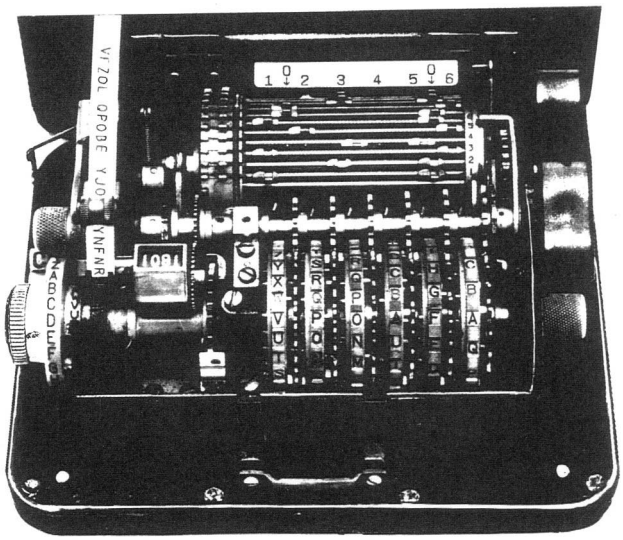

**Figure 1.**
US Army Hagelin M-209 cipher machine. [Photo: Masataka KATO [Kazuo KAMAGA]]

writes a clear text turning the handle carrying the alphabet, the first disk begins to rotate, dragging the neighbouring disk by means of a pin which it carries, and this second disk drags again by a pin which it carries, and so on. These motions of the six disks thus produced random numbers with a period of c. 100 millions (26×25×23×21×19×17), finite but enormous, for producing an encoded text on a paper tape, transcribed according to a pre-arranged position of the pins of the six disks in agreement with a cryptographic key for M209 (see Figure 1).

These M209 encoding-machines were in general use at the front divisions of the American armed forces. The General Staff of the Japanese Army had bought a prototype of this machine in Sweden before the war. The military engineer YAMAMOTO mentioned above guessed that "M209" was an adaptation of this Swedish prototype. He could even determine the details of the modifications of the prototype that had produced M209.

At that time, I was serving as a soldier working at the General Staff. I noticed that the keys of the codes of the M209 were so-called "double keys", and I succeeded in breaking these double-keys. After that, a team including a number of drafted officers including myself were sent to the Philippines. We managed to obtain some good decoding results, but the way the Americans made the daily change of coding keys was such that we were unable to break their codes every day, which strongly restricted the benefits we earned from our work.

By the way, the American "Strip-cipher" codes we speak of were also given to us by the Germans, who at the moment were our allies, and our work was based on these documents. Now, the material which was brought from Germany by the last U-Boot arriving in Japan in 1945 I found inconsistent with the preceding documents in our possession, in spite of the commentaries that attested to the authenticity of these documents. I understood that beyond purely tactical relations the confidence even among allies was not necessarily unlimited.

Gut-zu-Druck: 29.7.2003

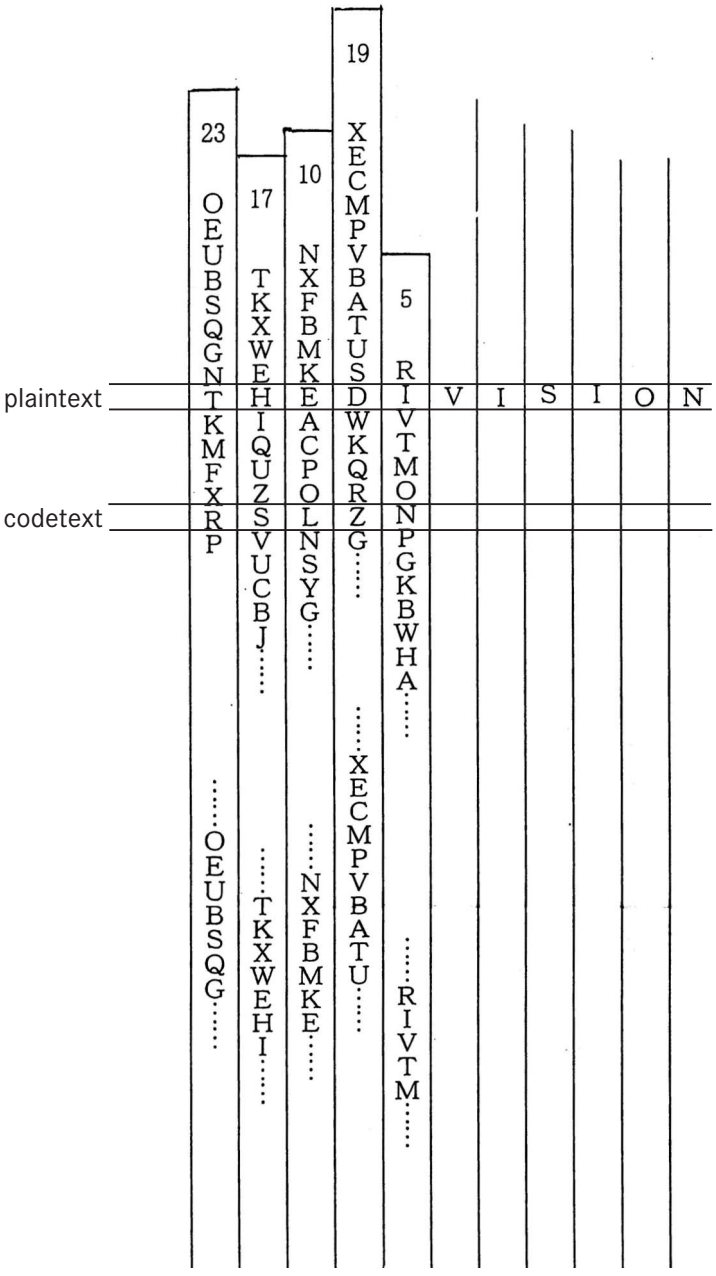


**Figure 2.** Strip cipher principle. (1) Each of the bars that carries twice the same permutation of the alphabet is numbered. (2) Every day, some 20 to 30 bars are chosen for the codes of this day. The keys of the cryptography are these numbers and their order for each day of the year providing two-sided equivalents in the form of a code book. (3) On the image, the plaintext THE DIVISION ... is indicated on top and the codetext RSLZN ... below. (4) With two permutations of the alphabet on each bar, it was always possible to find the necessary letters.

Gut-zu-Druck: 29.7.2003

After the German capitulation there were rumours running among us Army workers on coding and decoding that all German cryptographers had been executed. Therefore, after 14 August 1945 (the day before the surrender of Japan) we received orders to destroy and burn all material linked to military cryptography. No document concerning the cryptography of the 1940s, neither new cryptography nor code breaking, has thus survived. The career officers from the cryptography section of the Army vanished from the scene as if they had never existed. They burnt all documents that might compromise the university professors they had made collaborate with the armed forces, obliterating all traces of the existence of the Mathematical Seminary of the Army. They also sent several members of the cryptography section of the Army (including myself) to the professors concerned, giving them the directive to speak in no way about their collaboration with the armed forces.

I now believe certain documents in the archives should have conserved so as to make them public later as historical records. However, the Japanese authorities of the times had no notion of creating archives of administrative and official documents at some moment after the events as historical assets. Therefore the "memoirs" of former military people often contain nothing but accretions of deformations and disinformation or their own self-defence.

In any case, in the eyes of those who actually work on modern cryptography such as "public key" or "elliptic coding", all our efforts from the 1940s almost look like fairy tales from former times. The new cryptographic theories are much more deeply linked with mathematics, with information theory and with informatics, and speaking of them exceeds my competence.

Commander KAMAGA, who worked hard to create and develop the cryptography of the Japanese Army before the war (and, not least, during the war) is 85 years old today and is in good health. His gigantic work *Treatise of Cryptography* (published under the name of Masataka KATO) has a unique status within classical cryptography.

All those who are spoken of in this chapter have died, except Kamaga and myself.

## 3 Conclusions

In American bombers shot down by the Japanese, tables of numbers were found for the "space-probing pilotage" destinated to overseas bombing flight by astronomical observations. The Japanese armed forces recruited mathematics students to prepare numerical tables of the same kind. I have heard about mathematicians recruited by the armed forces for ballistic calculations, but I am not informed about the details of this.

It was impossible to refuse orders or demands of the armed forces during the regime of the imperial powers. Orders from the armed forces were treated as direct orders of the emperor himself. So were the orders to mathematicians to collabo-

Gut-zu-Druck: 29.7.2003

rate with the armed forces. One may easily imagine that the pressure was even greater on scientists belonging to so-called applied disciplines.

The idea to make use of mathematicians to improve the efficiency of warfare did not come early to the armed forces – much later indeed than the other scientific domains. Even for cryptographic research, linguists were first recruited. Commander KAMAGA himself loved mathematics. He presented himself to Teiji TAKAGI, emeritus professor of mathematics at the Imperial University of Tokyo, the patriarch of the Japanese mathematical community and known throughout the world for his monograph *Algebraic Number Theory – Generalities and Class Field Theory* (MR 14, 953a). Commander KAMAGA sought the collaboration of mathematicians for research in military cryptography within the Army. Initially, Professor TAKAGI was rather sceptical about the utility of mathematics within the domain of military coding. He finished by promising, however, to examine together with the mathematicians of the Imperial University of Tokyo the possibility of cooperating with the armed forces. This was the origin of the Mathematical Seminary of the Army which was mentioned in Section 2.

At the Imperial University of Tokyo, Professor Shokiti IYANAGA was the key figure of this seminary. Being a soldier in the Army and a member of the cryptography study group of the General Staff of the Army, I myself belonged on the side of those who invited the mathematicians.

In 1985, this Professor Shokiti IYANAGA referred publicly in a meeting of the "Association of Japanese Mathematicians Aiming to Eliminate All Nuclear Weapons" to his remorse for having supported the war in his capacity as a mathematician. He ended his talk with the words "I collaborated with the armed forces during the war as a mathematician; which I should not have done. Since then, my conscience as a scientific worker has never been released from these bitter memories. With NAKASONE's ascent to power, I feel something threatening to peace in Japan. One must make an effort to make sure Japan will not again find itself on the slippery road leading to war".

I was deeply touched by his sincere statement. Many university professors collaborated with the armed forces during the war. And yet I know of no university professor in Japan except him who publicly regretted his collaboration as a scientist with the armed forces for the war.

## Reference

KATO Masataka, *Fundamental Theory of Cryptography.* I. *For Security in Informatics* (in Japanese). (Information and Computing). Tokyo: Saiensusha, 1989 [LC Control No 90115183].

Gut-zu-Druck: 29.7.2003

http://www.springer.com/978-3-7643-1634-1

Mathematics and War
Booß-Bavnbek, B.; Høyrup, J. (Eds.)
2003, VIII, 420 p. 79 illus., Softcover
ISBN: 978-3-7643-1634-1
A product of Birkhäuser Basel