In June 1942, in order to ensure that the United States and the United Kingdom could afford high-level protection to their naval wireless traffic, it was therefore agreed that adaptors should be designed for both Sigaba and Typex by the United States Navy to transform them into a common machine, the Combined Cipher Machine (CCM). The extremely ingenious adaptor for Typex for this purpose was designed by Commander Don Seiler, who also devised the related adaptor for Sigaba. Although the design work was completed quickly, production delays prevented the CCM from entering service, except on a few minor circuits, until late 1943. The CCM was used in November 1943 for limited communications between the Royal Navy and the United States Navy and became operational with all five British and American services in April 1944. From then on, the Germans collected material on it and made counts on Hollerith punched card machines, but made no headway. The Allies had been lucky, because the CCM had a serious flaw.

Experiments in testing the CCM's period (the number of letters enciphered before its rotors returned to their starting point) had started as early as the spring of 1943 at the US Naval Computing Machine Laboratory in Dayton, Ohio. They revealed that, with some rotors, the period was only 338, which was dangerously short, instead of a minimum of 4,394, as intended. On 4 June 1943, an instruction was therefore issued restricting the length of signals between the Laboratory and the US Navy codebreaking unit, Op-20-G, to 100 groups. However, similar restrictions do not appear to have been applied to other CCM circuits until early 1944. Even more surprisingly, although the CCM was in limited service with the Royal Navy and the US Navy at the end of 1943, a detailed study of the CCM's period was not begun by Op-20-GM until 16 January 1944 - a full six months after the short cycle defect was first discovered. This revealed that on one CCM circuit alone, keys between 12 February and 20 April 1944 produced the 338 period on seven days.

In February 1944, C. H. O'D. Alexander, the head of Bletchley Park's Hut 8 (responsible for breaking naval Enigma) was told about the CCM's short cycle problem when he was visiting Op-20-G, since Hut 8 was the principal user of the circuit between Op-20-G and GC & CS which employed the CCM. He immediately signalled GC & CS to limit messages on the CCM to only 70 groups, instead of the previously agreed 200.

The reason for the CCM's short cycle is much too complex to explain here, but it depended on the way in which some rotors were notched. Notching was intended to hamper cryptanalysis by making the CCM's stepping action unpredictable, but it had succeeded all too well with the rotors in question: not even the CCM's designers had fully anticipated the results with certain rotor combinations. However, once the problem of the short period had been fully identified, it was fairly easily avoided by banning certain rotor combinations.

A technical investigation of the CCM's security apparently found that, using a 1,000 group message that was actually sent, the wiring of the rotors could be recovered. In addition, if a CCM and a set of rotors had been captured, there was a small chance that the enemy would be able to read the traffic for "an occasional day", but no more than that. Although the number of possible rotor combinations with the CCM, which made it proof against a "bombe" type attack, plus the fact that, unlike Enigma, a letter could encipher itself (which prevented the accurate alignment of plain and cipher text) led Op-20-G to conclude that "the designers of the CCM did a very good piece of work", there was some doubt as to whether it could safely be used "for Ultra dispatches of the bean-spilling variety", given that a machine could be captured. Special security precautions, including the rigid enforcement of the 200 group limit, a change in the indicator system and the avoidance of so-called "lobstering" rotors (which resulted in all rotors turning at the same time, thereby facilitating cryptanalysis) were therefore recommended. But problems with "lobsters" were still being detected as late as March 1945.

notes omitted

From: GCCS
To: Signal Security Agency
Msg No GCCS 3293 101835Z Mar 45

...
Study by British on CCM faults have been discovered in notch patterns on Army CCBP 0114 (CSP 1814) and on naval nets BRUSA (CSP 2513 and CSP 2514) KADYQ (CSP 1580) and CEMIZ (CSP 1581). On CCBP 0114 rotors there is possibility of lobsters due to notches occurring as result of further (wu) simultaneously on each side of rotors. This occurs 10 times on rotor number 40, 5 on 41, 7 on 42, 10 on 43, 8 on 44, 6 on 45, 8 on 46 5 on 47, 5 on 48, 7 on 49. On BRUSA circuit to be in force August 1945 rotors numbered 40 through 49 lobsters occur as follows 7-6-5-3-7-4-5-7-4-8. On current BRUSA rotors 30 through 39 as follows 2-5-9-7-1-3-10-0-3-4. ON KADYQ 4-4-4-4-6-9-8-8-5-10. On CEMIZ numbered 10 through 19 5-5-5-5-5-7-7-3-7-8. Also 338 cycle occurs on 4 out of 5 wheels whenever CEMZI 10 is in position 4 or 10R in 2; in current BRUSA whenever rotor 33R is in 4 or 33 in 2; on August BRUSA whenever rotor 43 is in 3 or 43R in 3 or 47 in 3 or 43R in 3. These last BRUSA rotors are identical to famous "rotor 14" in that number of notches at odd positions equals number of notches at even positions. The fact that certain rotors in positions 2 and 4 give rise to 338 cycle of four wheels is due to sum of every other group of intervals equalling 13. This last was just discovered by Major Babbage here. Above information except that pertaining to CCBP 0114 is no direct concern of Army but am passing to you for your information ...

From: GCCS
To: Signal Security Agency
Msg No GCCS 3420 114112Z Mar 45
...
In GCCS 3293 I gave 2 reasons for short cycles to occur in CCM. These reasons were wrongly interchanged. Famous rotor 14 had alternate intervals between notches summing to 13. Other rotors in positions 2 and 4 had number of notches at even positions equal to odd. Believe both these possibilities known to us last summer when we studied CCM. ...