US Navy Cryptanalytic Bombe - A Theory of Operation and Computer Simulation

Magnus Ekhall
magnus.ekhall@gmail.com

Fredrik Hallenberg
fredrik.hallenberg@gmail.com

Abstract

This paper presents a computer simulation of the US Navy Turing bombe. The US Navy bombe, an improved version of the British Turing-Welchman bombe, was predominantly used to break German naval Enigma messages during World War II. By using simulations of a machine to break an example message it is shown how the US Navy Turing bombe could have been operated and how it would have looked when running.

1 Introduction

In 1942, with the help of Bletchley Park, the US Navy signals intelligence and cryptanalysis group *OP-20-G* started working on a new Turing bombe design. The result was a machine with both similarities and differences compared to its British counterpart.

There is an original US Navy bombe still in existence at the National Cryptologic Museum in Fort Meade, MD, USA. The bombe on display is not in working order and the exact way it was operated is not fully known.

The US Navy bombe was based on the same principles as its British version but had a different appearance and thus a different way of operation. The bombes were used to search through a part of the Enigma key space, looking for a possible Enigma rotor core starting position which would not contradict a given enciphered message and its plaintext (Carter, 2008).

A theory, based on previous research (Wilcox, 2006) and knowledge of how the British bombe works, is presented of how the US Navy bombe was operated and it is shown with a computer simulation that the theory is sound.

The computer simulation presents a graphical user interface and runs at approximately historically accurate speed. The simulator will be made available to the public.

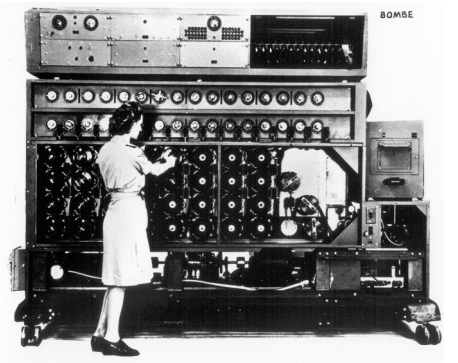

Figure 1: An operator setting up the wheels on a US Navy bombe. Source: NSA

It is assumed that the reader is familiar with the Enigma machine. This knowledge is widely available, for example in (Welchman, 2014).

To find an Enigma message key with the bombe it is necessary to have a piece of plaintext, a crib, corresponding to a part of the encrypted message. A crib could be a common word or a stereotyped phrase which is likely to be present in a message, for example *Wettervorhersage* which is the German word for *weather forecast*. The crib is used to derive a configuration of the bombe and an assumption of the Enigma rotor starting position is made. Once started the bombe will scan through all possible Enigma rotor core positions and stop when a position has been found that does not lead to a logical contradiction for the given crib (Carter, 2008). If a logical contradiction occurs then the state of the bombe represents a setting of an Enigma where it would not be possible to encipher the assumed plaintext to the ciphertext of the crib. Each stop is subject to further tests after

Proceedings of the 1st Conference on Historical Cryptology, pages 103– 108,
Uppsala, Sweden, 18-20 June, 2018

Position:	A	B	C	D	E	F	G	H	I	J	K	L	M
Plaintext:	K	R	K	R	A	L	L	E	X	X	F	O	L
Ciphertext:	L	A	N	O	T	C	T	O	U	A	R	B	B

Table 1: Crib and corresponding ciphertext used throughout this paper

which the bombe is automatically restarted.

If a test is passed, relevant information on the stop in question is automatically printed onto paper (Desch, 1942).

2 Example Message

The bombe simulation will be tested using a real message sent May 1st 1945 (CryptoMuseum, 2017). The crib is the thirteen first letters of the plaintext. The wheels used for this message was β, V, VI and VIII, with the thin C-reflector being used. The original Enigma rotor start position was {CDSZ} (this notation will henceforth be used to show positions of the corresponding wheels). This means that the leftmost rotor on the Enigma, in this case the β rotor, is set to position C, the second rotor is set to D and so on. The ring setting of the rotors for this message was {EPEL}. Note that the difference between the ring setting and the rotor start position is 24, 14, 14, 14 positions respectively. This is called the rotor core starting position.

The row labeled "Position" in table 1 shows what setting the rightmost Enigma wheel would have when encrypting a given plaintext letter into ciphertext. The assumption is that the Enigma machine would have been set to {ZZZZ} before the message was coded. This leads to the first letter being encrypted at position {ZZZ**A**}, the next at {ZZZ**B**} and so on.

The plug board connectors, *Stecker* in German, used on the Enigma for this message was:

A	B	C	D	H	J	L	P	S	V
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
E	F	M	Q	U	N	X	R	Z	W

The letters of the alphabet not listed in the plugboard connector pairs above did not have a wire connected on the plugboard which results in them being electrically connected to themselves. There were normally ten plugboard cables used in the daily Enigma key, leaving six letters self-connected (Copeland et al., 2017).

3 Setting Up the Bombe

Preparing the bombe to work on a message consists of a number of steps. Firstly, the wheels need to be selected and set to the appropriate starting positions. Secondly, the bank switches need to be set according to the letters in the crib. Thirdly, one or two input switches need to be activated. Finally, some of the printer cables are connected to the diagonal board.

3.1 Enigma Rotor Equivalent Wheels

The bombe has sixteen wheel banks of four wheels with each wheel bank representing the rotors of an Enigma machine. Eight wheel banks are on the front of the bombe and eight are on the back.

The bombe was primarily designed to break messages encrypted with the M4 Enigma which had four rotors. However, it could also work on messages encrypted with a three-rotor Enigma such as the one used by the German Army. For this purpose there is a switch which selects between three- or four-wheel mode. In three wheel mode, the slowest wheel in each of the 16 wheel banks would be stationary (Desch, 1942). By observing how the wheels in a wheel bank are interconnected it can be assumed that the bottom wheels of each wheel bank would not move in this configuration.

To configure the bombe for the message, a wheel order which is to be tested is installed. As mentioned in section 2 the correct wheel order is already known in this case. The corresponding wheels are loaded onto all wheel banks of the bombe. Also, the "thin C"-type reflector cables are connected to all the reflector plugs on the bombe.

In reality the wheel order was not known but many different wheel orders could be tested in parallel, one wheel order per bombe. A total of 121 US Navy bombes were built (Wilcox, 2006).

Normally it is assumed that the second wheel of the Enigma does not advance during the crib. Since the second wheel of the Enigma will advance one step once or twice per revolution of the first wheel there is a high probability that this is not the case, and if so, the bombe will fail to find a possible solution. There are techniques that could have been used if a second wheel turnover was suspected, but those are not in the scope of this paper.

With the example message there was in fact a second wheel turnover before the first letter was encrypted. This knowledge will be taken into ac-

count in the following discussion. In practice this could not have been known, but the bombe would still have found a solution since there is no further second wheel movement during the crib; the entire crib has one and only one wheel position for the second wheel. The difference is that the second wheel now has to be set to A instead of Z which it otherwise would have been assumed to be. Therefore the bombe is adjusted so that the wheels on wheel bank 1 are set to 25, 25, 0, 0. This corresponds to {ZZAA}.

The wheels of wheel bank 2 are set to 25, 25, 0, 1 = {ZZAB}, wheel bank 3 to 25, 25, 0, 2 = {ZZAC} and so on all the way up to wheel bank 13 which is set to 25, 25, 0, 12 = {ZZAM}.

The wheel order, reflector plugs and the start position of the bombe wheels are now set up. The next step is to connect the wheel banks according to the letters of the message.

3.2 Bank Switches

There are two 26-step rotary switches for each wheel bank. One for the input letter to the bank and one for the output letter. The rotary switch connects the rotor bank to the diagonal board which utilises the symmetrical properties of the Enigma plugboard to interconnect the bombe wheel banks. All of the 32 switches are located on the front of the bombe. These switches eliminate the need of a plug board as found on the back of the British bombe and thus makes setting up a crib on the bombe much faster (Turing, 1942).

The British bombe, on the other hand, could have up to three cribs or wheel orders connected at the same time on one bombe. The British bombes usually had 36 wheel banks of three wheels each, corresponding to 36 Enigma machines.

The plaintext letters of the message are considered to be the input to the corresponding rotor bank and the ciphertext letters to be the output.

For example, for wheel bank 1 which corresponds to the first letter of the message, the input is K and the output L. Therefore the left switch of the two bank switches corresponding to rotor bank 1 is set to 10 for the letter K. The right switch is set to 11 for L.

For wheel bank switch 2 the input switch is set to 17=R and the output switch to 0=A.

The rest of the wheel bank switches are set up in the same way with the last, number 13, set to 11=L, 1=B according to the last letter of the crib (see table 1).

3.3 Wheel Positioning

Apart from the four wheels in a wheel bank, one for each Enigma rotor, there is also a reflector plug which has the same function as the reflector on the Enigma. Since the top wheel of the bombe is connected to the reflector plug it can be assumed that this represent the leftmost Enigma-rotor which is connected to the reflector of the Enigma. The bottom wheel of the bombe corresponds to the rightmost Enigma-rotor.

3.4 Input Switch

The bombe works by injecting a test current into a position corresponding to a certain letter of the diagonal board. This current then propagates through the system and stops the bombe if it fails to reach all other letters of the alphabet.

To select the letters where test currents are injected the bombe has two 26-step rotary switches marked PRI and SEC for primary and secondary. Normally only the primary input is set. When using a crib where the letters of the crib and the corresponding ciphertext are forming two separate graphs the secondary input is also needed.

The input should be connected to a frequently occurring letter in the crib. L is selected as it occurs at three places in the example message. The primary input switch is switched to 11 which corresponds to L. The secondary input switch is not needed in this case and is set to OFF.

3.5 Printer

On the back of the bombe the cables of the printer are connected to the diagonal board sockets representing the letters in the message. The following letters are present: A, B, C, E, F, K, L, N, O, R, T, U, X. The printer cables for these letters should be connected to their respective socket on the diagonal board with A=0, B=1 and so on.

4 US Navy Bombe Model

A theoretical model is presented of how it is assumed the different parts of the US Navy bombe interacted.

4.1 Diagonal Board

The central component in the US Navy bombe is the diagonal board. The diagonal board has 26 input nodes, one for each letter of the alphabet. Each

input node consists of 26 conductors, one for each letter of the alphabet. The diagonal board utilises the fact that if a letter A on the plugboard of the Enigma is connected to letter B, then it follows by the symmetrical design of the plugboard that letter B must be connected to A. Let conductor y of diagonal board node x be denoted $DB(x,y)$, then the connections on the diagonal board can be described: $DB(x,y)$ is connected to $DB(y,x)$.

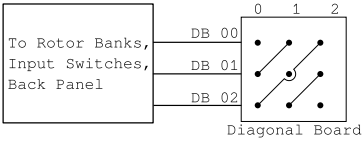

Figure 2: The principle of the diagonal board, here in a simplified form as if the alphabet would only have three letters. The actual diagonal board is of size 26 x 26.

The use of the diagonal board greatly reduces the number of false stops the bombe otherwise would have had. All the rotor banks of the bombe can be connected to any of the letters on the diagonal board.

There are also two input switches which can inject a test current to any node on the diagonal board.

On the back of the US Navy bombe there is a panel which exposes the diagonal board. The checking logic and printer is connected to to the diagonal board through cables plugged into sockets on this panel.

Each input node on the diagonal board thus has quite a large number of potential inputs connected in parallel.

4.2 Rotor Banks

The 16 rotor banks are connected to the diagonal board via the two rotor bank switches A and B (see section 3.2) of each bank as illustrated in figure 3.

5 Operation

Once the message has been set up on the bombe the machine is started. It will iterate through every possible rotor core position, searching for a condition which will satisfy the crib.

The bombe will stop if the test current fails to reach all 26 conductors of the input letter node on the diagonal board. This is called a "cold point test" and was implemented with a *Rossi circuit*

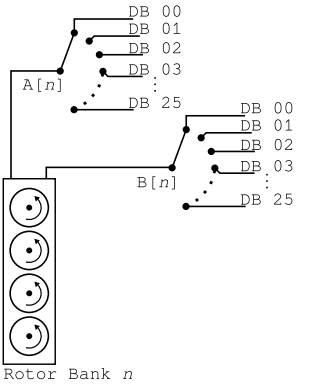

Figure 3: Rotor bank n, where n = 1, ..., 16. All wires in this figure are 26-way. The 26-way input switches A and B of rotor bank n controls where on the diagonal board the two rotor bank nodes are connected. DB 00 is diagonal board position 0, corresponding to the letter A, and so on.

which can be seen as a 26-input AND-gate. Following this, a second test called the "hot point test", is automatically performed. This test applies a voltage in sequence to the 26 conductors of the input letter node on the diagonal board. This test will determine the possible plugboard connections for the stop and if contradicting connections are found the stop is ignored (Desch, 1942).

When a stop which passes the tests mentioned above has occurred, the ring setting for that rotor core position will be printed along with the plugboard connections that could be concluded from the given bombe connections.

The operating speed of the US Navy bombe was much higher than the British Turing Welchman bombe. The fastest wheel on the US Navy bombe rotated at about 1725 revolutions per minute, almost twenty times the speed of the British bombe. A complete four wheel run on the US Navy bombe took approximately 20 minutes (Wilcox, 2006).

The simulation of this example message yields 188 stops out of the $26^4 = 456,976$ possible rotor core positions tested. Of these, only one stop will pass the hot point test resulting in the following information being printed:

- Ring setting: 24 14 14 14
- Plugboard: B/F E/A K/K O/O T/T X/L

The exact format of the original printouts is unclear. The information in the example above would most likely have been represented by numbers only (Wilcox, 2006) as this is the norm on the rest of the bombe. This matches the rotor core starting position of the Enigma used to encrypt the message (see section 2).

The setting found will be subject to further, manual, tests using a simplified Enigma machine: the *M-9 Checking Machine*. The output from this process would be either more of the plugboard connection pairs, or the conclusion that the stop was in fact false.

After this there would be a brief set of trial and error tests to find a suitable ring setting that would decrypt the whole message.

6 Computer Simulation

A computer simulation was setup based on the model described in section 4. The main difficulty of simulating the bombe lies in the parallel nature of the electrical circuit implemented by the bombe. For each rotor position the simulator has to calculate what happens if an input current is injected into a certain position in the circuit. This input current is propagated until it does not reach any new nodes. At that time the stop condition is checked. The US Navy bombe tested about 750 rotor positions per second. Since the simulator aims to run at a historically accurate speed, for every frame drawn on the screen several rotor positions will have to be simulated and tested.

To implement this the simulator uses a switchboard model, which basically is a bi-directional list of nodes that can be connected to each other. Each switchboard node has a state which is a list of 26 booleans, one for each letter of the alphabet. This switchboard does not exist in the bombe but is a way to handle the parallelism described above.

Most components in the modeled bombe will add connections to the switchboard, this includes the rotor banks, the printer, the diagonal board and the bank switch selectors. Each of the components owns one or more switchboard sockets which allows the components to react to voltage state changes from the switchboard and to send an updated state.

At every iteration the simulator clears the states of all the nodes in the switchboard. It is then given the input voltage in one of its nodes. The switchboard propagates this change of state to the node

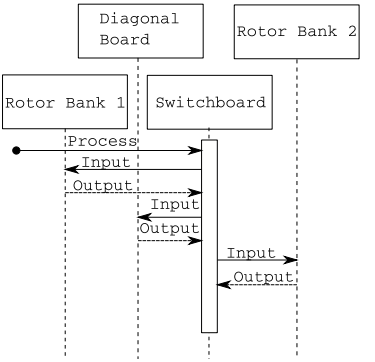

Figure 4: Sequence diagram showing how the central switchboard component of the simulator distribute information between two rotor banks and the diagonal board.

that is connected, according to the list of nodes, to the input. This triggers the owner of the connected node to calculate the effect of this state, which usually will propagate the voltage state to another node in the circuit, and so on. This process is repeated until no node has registered any change. The simulation of that rotor position is then complete. In the real bombe this process would be carried out almost instantaneous. Figure 4 illustrates how the switchboard works.

The simulator, which runs at approximately the same speed as a real US Navy bombe, lets the user setup and run the machine by a graphical user interface as shown in figure 5.

7 Conclusion

It has been shown, using an authentic M4 Enigma message, that the simulated US Navy bombe is able to find the correct rotor core starting position as well as six correct plugboard connector pairs.

The simulated bombe stopped 188 times but only one stop, matching the correct Enigma key, passed the automatic tests. This shows that the theory presented in this paper is plausible but further research is needed to verify if this was exactly how the bombe was operated.

Some effort has been made to make the simulation as graphically accurate as possible. The photographs that exist of the US navy bombes shows that there were several different models in operation. The simulator is mostly based on photographs of the US Navy bombe located in the Na-

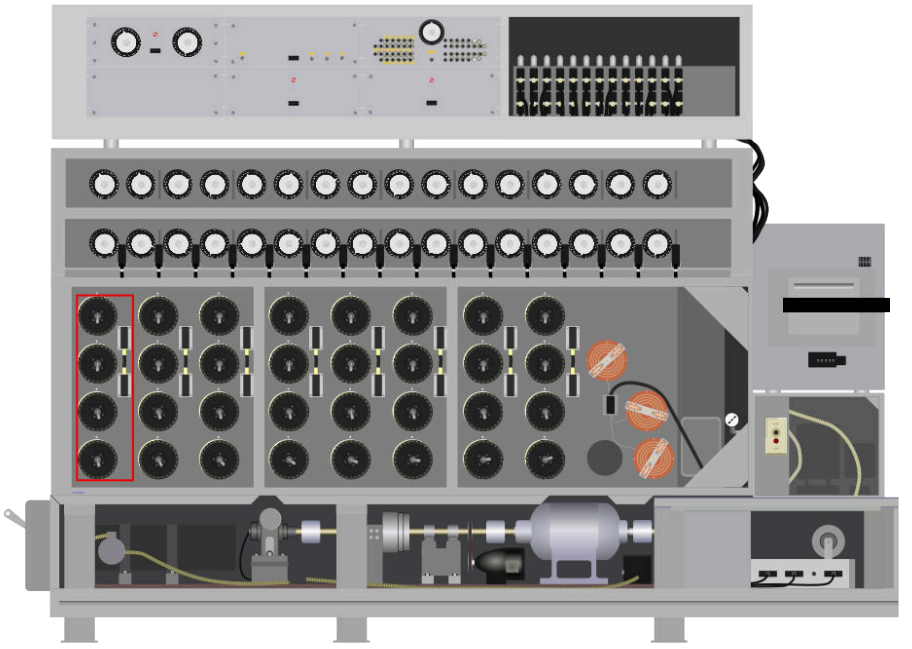

Figure 5: US Navy Bombe computer simulation screenshot showing the front of the bombe. By interacting with the various parts of the bombe in the simulation, a crib can be set up and run. The simulator is written in the *Haxe* programming language and uses the *NME* framework.

tional Cryptologic Museum. This bombe is supposedly the last one manufactured.

8 Acknowledgments

We would like to thank the National Cryptologic Museum for providing us with useful information on the US Navy bombe, and we thank the three anonymous reviewers for their valuable comments. We would also like to thank Dr. J Jacob Wikner, Associate Professor at the Department of Electrical Engineering, Linköping University, Sweden, for hints and tips on how to shape the manuscript.

References

Frank Carter. 2008. *The Turing Bombe*. Report No. 4. Bletchley Park Trust, new edition. ISBN: 978-1-906723-03-3.

B. Jack Copeland, Jonathan P. Bowen, Mark Sprevak, and Robin Wilson. 2017. *The Turing Guide*. Oxford University Press. ISBN: 978-0-19-874782-6.

CryptoMuseum. 2017. Enigma M4 message. `http://www.cryptomuseum.com/crypto/enigma/msg/p1030681.htm`. [Online; accessed 24-October-2017].

Joseph R. Desch. 1942. Memo of Present Plans for an Electro-Mechanical Analytical Machine. `http://cryptocellar.org/USBombe/desch.pdf`. [Published online by Frode Weierud in 2000, accessed 16-September-2016].

Alan M. Turing. 1942. Visit to NCR. `http://cryptocellar.org/USBombe/turncr.pdf`. [Published online by Frode Weierud in 2000, accessed 16-September-2016].

Gordon Welchman. 2014. *The Hut Six Story*. M & M Baldwin, 6 edition. ISBN: 978-0-947712-34-1.

Jennifer Wilcox. 2006. *Solving the Enigma: History of the Cryptoanalytic Bombe*. Center for Cryptologic History, NSA.