OXFORD

The Computer Journal, 2024, 1–3
https://doi.org/10.1093/comjnl/bxae103
Original Article

Impact over metrics: Turing and the ultimate contribution of cryptology

Steven Furnell *

School of Computer Science, University of Nottingham, Wollaton Road, Nottingham NG8 1BB, United Kingdom
*Corresponding author. School of Computer Science, University of Nottingham, Wollaton Road, Nottingham NG8 1BB, United Kingdom.
E-mail: Steven.Furnell@nottingham.ac.uk

Abstract

Amongst his many lasting contributions, Alan Turing's name is strongly linked to the domain of cryptology, particularly due to his pioneering wartime work in cryptanalysis. However, the fact that his work remained classified until many years later has arguably limited its wider influence on the science of cryptology. Nonetheless, while his research was never able to be properly referenced until many years later, its resulting impact is arguably greater than much that followed it. This article summarizes Turing's crypto work and considers his contribution from this perspective.

1. INTRODUCTION

Mentioning the name of Alan Turing to those generally aware of his work, it is likely that many will gravitate towards the areas of AI and cryptography (Of course, it is arguably ironic to associate Turing with cryptography (i.e. creating codes) when his most prominent contributions were actually in cryptanalysis (i.e. breaking them). For convenience, this article will mainly refer to the meta-discipline of cryptology.). In the latter context, the general view of Turing's contribution in cryptology is inextricably linked to Bletchley Park and the German ENIGMA machines.

Much has already been written about Turing's contribution to the wartime effort, and it is doubtful that new insights can be offered in this context. However, it is perhaps interesting to reflect upon how it compares in the modern academic context, where many now seek to view and judge contribution on the basis of publication metrics.

2. TURING AND CRYPTOLOGY

Having already established himself as a mathematician, with a BA and MA from King's College Cambridge, and a PhD from Princeton, Turing arrived at Bletchley Park in 1939, which was then home to the Government Code & Cypher School (which, in 1946, would go on to be renamed as the Government Communications Headquarters, GCHQ). Building upon earlier work from Polish cryptanalysts, Turing (and his colleague Gordon Welchman) created the Bombe, an electromechanical device used to assist the decryption of the coded messages generated by the German ENIGMA machines. The Bombe helped to determine the settings being used for the ENIGMA devices each day (these being the order and initial settings of the rotors, and the wiring of the plugboard), which essentially represented the key to decrypt the messages. The first Bombe was installed in March 1940, and by the end of the war 211 were in operation (albeit not all of them based at Bletchley) [1]§. It is estimated that some 3–5000 ENIGMA-encoded messages were intercepted each day, and by 1943 Bletchley Park was breaking 84 000 messages per month [2].

While brief summaries of the story may simply give the impression that ENIGMA was broken and the Allies had resulting access to all the messages, the reality of the situation is that the Germans' use of encryption continued to evolve and advance as the war progressed. Different variants of ENIGMA devices were used by different elements of the German military, and new codes emerging required correspondingly new efforts to break. Turing's personal involvement with the ENIGMA codebreaking included work focusing on the German naval variants of ENIGMA [3], as used by U-Boats hunting the Allies' vital conveys in the Atlantic. A particularly notable development here was the introduction of Triton (codenamed 'Shark' by the Bletchley team), which introduced a fourth rotor into the machine, significantly adding to the challenge of breaking the code (indeed, there were later ENIGMA variants that remained unbroken by the end of the war).

While a detailed account of Turing's work here is outside the scope and space of this paper, it is worth noting some of the other significant crypto-related contributions Turing made during this period:

- **Banburismus**: A method to reduce the running time of Bombes by identifying the most likely settings for the middle and right-hand ENIGMA rotors.
- **Turingery:** A manual cryptanalysis method that Turing devised in 1942 as a means of breaking the Tunny (Lorenz) cipher.
- **DELILAH:** A system to enable a key-based scrambling and descrambling of transmitted speech [4].

Received: August 21, 2024. **Revised:** August 21, 2024. **Accepted:** October 2, 2024

While Turing documented his ENIGMA work in a report titled 'Mathematical Theory of ENIGMA Machine' [5] (colloquially known at Bletchley as 'The Prof's book'), this was not publicly disclosed until 1996 (a factor that is common to all his directly crypto-related work, and a theme that is revisited later in the discussion).

Illustrating the influence of his work in that era, Turing spent several months in the winter of 1942–43 visiting the Cryptanalytic Section of the US Navy, sharing his knowledge of ENIGMA and advising on the use of Bombes. However, this sharing was again limited to the restricted context of the military intelligence community.

3. INFLUENCING MODERN CRYPTO?

Turing's innovative contribution to cryptanalysis ultimately stems from his work in probability theory, with the development of new Bayesian inference methods (which also underpinned some of his contribution in the domain of AI). These statistical techniques helped to optimize the code breaking process, and enabled more likely options to be attempted more quickly.

Turing's work in cryptology was not published in the traditional academic sense, not least because it was classified and withheld from public release due to the Official Secrets Act. Indeed, Turing's involvement in the WW2 efforts, and the wider story of ENIGMA, was not declassified until the 1970s and went unacknowledged until well after the war, and beyond his own death in 1954. Some of Turing's techniques *were* ultimately shared more widely in 1950, when his assistant from the wartime efforts, Jack Good, published a book titled 'Probability and the Weighing of Evidence' [6]. Moreover, in 1979, Good went on to directly comment on Turing's use of Bayesian methods in codebreaking [7], but this was still in general terms compared to what would later be released through declassification.

In more recent times, Turing's works across various disciplines have been retrospectively collated into several volumes by different authors, with examples being *The Collected Works of A.M.Turing* from 2001 (split into four volumes, addressing *Mechanical Intelligence*, *Morphogenesis*, *Pure Mathematics*, and *Mathematical Logic* respectively), and *The Essential Turing* from 2004. Within these it is possible to see some aspects of the work that he documented, but even here the works are not complete. Indeed, it is notable that key elements relating to his work in cryptology were released in 2012 [8] and so had no opportunity to be reflected in the earlier compendia.

Specifically, 2012 saw the release of 'The Applications of Probability to Cryptography' [9], and a shorter companion piece entitled 'Paper on the Statistics of Repetitions' [10], which described how the mathematical analysis based on probability could help to determine which key values were more likely. Originally dating from around 1941, the longer paper (44 pages) presented a cryptanalysis approach based on the Factor Principle (Bayes's Theorem) and prior probabilities, which then illustrated its application to a series of four 'Straightforward Cryptanalytic Problems' of increasing difficulty (namely the Vigenère cipher, a letter subtractor problem, a theory of repeats, and transposition ciphers). The shorter paper (eight pages) was the focus on the repetition aspect, providing an alternate version of the theory of repeats section in the longer paper. Those interested in a detailed discussion of the work are referred to the commentary paper by Zabell, which appeared in *Cryptologia* in the same year [11].

Given that cryptology itself had significantly advanced by the time Turing's works were declassified, in the intervening period, from the academic perspective, his works were simply not there to be cited. So, while Turing made significant contributions to the cryptanalysis work of his era, the extent to which he can be seen and directly *credited* as an influence on later work is limited by the fact that the work could not be openly published at the time, and by the time it emerged in the public domain the work in the crypto domain had moved on significantly. Such hidden innovation has parallels elsewhere in cryptography, with the subsequent work of James Ellis on secure non-secret encryption [12] (undertaken in 1970) remaining classified, while public key cryptography being publicly credited to the independent but slightly later work of Diffie and Hellman published in 1976 [13]. The fact of the earlier work remained classified until 1997, which is notably a much shorter period than the ~71 years for which Turing's 'applications of probability' work remained unreleased.

Viewed through the lens of modern academic study, Turing's cryptology work is therefore somewhat obscured. For example, attempting to look for related entries against his author name in popular indexes such as Scopus and Google Scholar quickly reveals that there is nothing in terms of publication titles that directly pertain to his crypto work (although 'cryptography' is prominently listed amongst the topic areas at the head of his posthumous Google Scholar profile page). Listing the most cited authors with 'cryptography' amongst their Google Scholar keywords finds Turing being prominently placed (eighth at the time of writing), but this listing is simply based upon total citations, and his positioning is traceable to his work in other areas such as machine intelligence and mathematics. Indeed, Turing's seminal work on machine intelligence, first published in 1950 in *Mind* [14], and subsequently republished in various other sources, is appropriately highly cited (with almost 25 000 citations on Google Scholar at the time of writing).

So, in terms of our modern-day fascination with research metrics, citation counts, h-indices, and their ilk, Turing's contribution would not be getting him very far. Which ultimately says more about the value of metrics than it does about Turing's work!

4. CONCLUSION

At the end of the war, General Dwight D. Eisenhower wrote to the head of the British Secret Intelligence Service to recognize and thank them for the codebreaking work undertaken at Bletchley. It had, he said, '*saved thousands of British and American lives and, in no small way, contributed to the speed with which the enemy was routed and eventually forced to surrender*' [15]. Of course, although not addressed to them, this recognition is in significant part due to the efforts of Turing and his colleagues. As with many other artefacts relating to Turing's cryptanalysis work, this letter—written in 1945—was not made public until 2016.

Ultimately, then, it is fair to say that Turing's main contribution to cryptology transcends the academic. It was the practical nature of his work, and the context to which it was applied that delivered the most impact. The work on ENIGMA and Tunny codebreaking is widely believed to be fundamental in shortening the duration of the war by 2 years. Thus, saving many thousands of lives in the process. In short, Turing's cryptology work continues to affect lives today through the very fact that they had the opportunity to occur. Viewed from this perspective, it is perhaps one of the best impact cases we will ever see.

FUNDING

None declared.

REFERENCES

1. TNMOC. The Turing-Welchman Bombe nd; The National Museum of Computing. https://www.tnmoc.org/bombe (18 August 2024, date last accessed).
2. Copeland J. Alan Turing: the codebreaker who saved 'millions of lives'. *BBC News*, 19 June 2012 2012. https://www.bbc.com/news/technology-18419691 (18 August 2024, date last accessed).
3. Erskine R. NAVAL ENIGMA ciphers nd. uboat.net. https://uboat.net/technical/ENIGMA_ciphers.htm.
4. Turing AM, Bayley D. Report on speech secrecy system DELILAH, a technical description compiled by A. M. Turing and Lieutenant D. Bayley REME, 1945–1946 *Cryptologia*. 2012;**36**:295–340. https://doi.org/10.1080/01611194.2012.713803 (18 August 2024, date last accessed).
5. Turing AM. Mathematical theory of ENIGMA machine 1940; available from https://archive.org/details/TuringMathTheoryEnigma/mode/2up (18 August 2024, date last accessed).
6. Good IJ. *Probability and the Weighing of Evidence* 119. London: Griffin, 1950.
7. Good IJ. Studies in the history of probability and statistics: XXXVII A. M. Turing's statistical work in World War II *Biometrika*. 1979;**66**:393–396. https://doi.org/10.1093/biomet/66.2.393.
8. Vallance C. Alan Turing papers on code breaking released by GCHQ. *BBC News*, 19 April 2012 2012. https://www.bbc.co.uk/news/technology-17771962 (18 August 2024, date last accessed).
9. Turing AM. The applications of probability to cryptography 2012; unpublished paper, c. 1941, UK National Archives, HW 25/37.
10. Turing AM. Paper on the statistics of repetitions 2012; unpublished paper, c. 1941, UK National Archives, HW 25/38.
11. Zabell S. Commentary on Alan M. Turing: the applications of probability to cryptography *Cryptologia*. 2012;**36**:191–214. https://doi.org/10.1080/01611194.2012.697811 (18 August 2024, date last accessed).
12. Ellis JH. *The Possibility of Secure Non-Secret Digital Encryption*Available from1970. https://cryptocellar.org/cesg/possnse.pdf (18 August 2024, date last accessed).
13. Diffie W, Hellman M. New directions in cryptography *IEEE Trans Inf Theory*. 1976;**22**:644–654. https://doi.org/10.1109/TIT.1976.1055638.
14. Turing AM. Computing machinery and intelligence *Mind*. 1950;**LIX**:433–460. https://doi.org/10.1093/mind/LIX.236.433.
15. Kirka D. British codebreakers show Eisenhower letter on their success. The Washington Times 15 March 2016 2016. https://www.washingtontimes.com/news/2016/mar/15/british-codebreakers-show-eisenhower-letter-on-the/ (18 August 2024, date last accessed).