A Brief Survey of Research Jointly with Jean-Jacques Quisquater

Yvo Desmedt
University College London, UK

Abstract. This paper surveys research jointly with Jean-Jacques Quisquater, primarily the joint work on DES, on exhaustive key search machines, and on information hiding.

1 Introduction

The joint work on, DES is surveyed in Section 2 on exhaustive key search machines in Section 3 and the one on information hiding in Section 4. Other joint work is briefly mentioned in Section 5.

2 Research on DES

Jean-Jacques Quisquater’s first paper at Crypto, was at Crypto 1983 and co-authored by a total of 10 authors [8]. This 32 page paper contained several ideas. A large part of the paper was dedicated to propose alternative representations of DES. The idea of transforming the representation of DES was initiated by Donald Davies [5] when he merged the \( P \) and \( E \) boxes. This part of the paper has been an inspiration for faster software and hardware implementations of DES (see e.g., [9,17,26]). Other parts have not received that much attention. For example, parts of the thesis of Jan Hulsbosch, where included in the paper [9, p. 193]. It improved Marc Davio’s work on pseudocanonical expansion (see [7]) and was used to improve Ingrid Schaumuller-Bichl [27,28] short representations (using EXOR and AND) for the S-Boxes.

One of the alternative presentations in the paper is a 48 bit model which led to a very algebraic representation of DES [9, pp. 184–187]. Although, as we learned in [18], algebra played a major role in breaking Enigma, this or any other algebraic representation of DES has had little influence on the breaking of DES.

Other joint research on DES appeared in particular in [9,14]. The last paper got cited by Biham-Shamir [3].

3 Exhaustive Key Search Machines

Jean-Jacques Quisquater was interested in exhaustive key search machines and alternatives, as is clear from, for example, [21]. This lead to several discussions on how to build an exhaustive key search machine. Jean-Jacques Quisquater considered whether such a machine could be built as a distributed one. A first idea was proposed in 1987 [23]. It
used the idea of putting DES decryption boxes in radio receivers. It focused on how long the computation would be if countries would organize such a distributed exhaustive key search machine (see Table 1).

The presentation [23] was the first academic one suggesting the use of a distributed computer, instead of a parallel one, for cryptanalysis. It predated Lenstra-Manasse [19] by almost 2 years.

Encouraged by Steve White (IBM), the journal version [22] was prepared in 1989. We then realized that the distributed machine had the same problems as identified by NSA and mentioned in 1977 by Diffie-Hellman [16], i.e., some keys might be overlooked and so never found, the machine had a too large Mean Time Between Failures, and it suffered from other problems. The use of random search instead of a deterministic one solved these problems.

Another interesting aspect of the machine is that it uses obfuscation, i.e., it hides its purpose. Moreover, Jean-Jacques Quisquater suggested several other approaches to build such a distributed machine. These were more science fiction and 20 years later cannot be realized yet! Amazingly, these science fiction approaches did appear in the paper [22].

### 4 Information Hiding

In the early stages of the research on Information Hiding, we co-authored three papers on the topic [15][11][12].

In the paper on “Cerebral Cryptography” [15], encryption (embedding) starts from a 2-dimensional picture. Two modified versions are then produced by a computer. To decrypt, the two printed ones are put in a “viewmaster.” In such a device, the viewer sees in 3-D, the original picture. Parts of it have moved up, others moved down. The up and down parts form a letter. So, the decryption is done in the brain. No computer is needed to decrypt.

In the paper on “Audio and Optical Cryptography” [11], a similar effect is created but using sound. The plaintext is binary. The receiver believes the sound is coming from left (1) or right (0). So, decryption is also done in the brain. Both shares are any music, e.g. Beethoven. The optical version uses a Mach-Zehnder interferometer and pictures.