Applied Kid Cryptography
or
How To Convince Your Children You Are Not Cheating

MONI NAOR[*] YAEL NAOR[†] OMER REINGOLD[‡]

March, 1999

Abstract

In this note, we consider a real life cryptographic problem: how to convince people that you know where Waldo is without revealing information about his location. We propose and discuss methods of solving this problem.

1 Introduction

"Where's Waldo?" is a puzzle book where each page contains a very detailed picture with many different characters (see [9] for "Where's Waldo?" on the WEB). The goal is to find Waldo, a predefined character (and a rather colorful fellow one might add). As the following true story will reveal, in these pictures also lies an interesting cryptographic problem.

Our story involves two of this note's authors. For the sake of anonymity and following a long cryptographic tradition (started in [8] according to [2]) we shall call them Alice and Bob. One day, while Alice and Bob were playing "Where's Waldo?", Alice suddenly claimed: "I know where Waldo is!". Bob responded with a baffling riddle: "Alice, do you know what a liar is?". Worried about her reputation (both as an honest person and as a qualified cryptographer), Alice wondered: "How can I prove to Bob that I know where Waldo is without revealing his location?".

The goal of this note is to offer solutions to the problem Alice was facing. While there are general solutions that allow Alice's computer to prove to Bob's computer a large class of statements without revealing any additional information (see Goldreich [5] for an accessible description of zero-knowledge interactive protocols), these solutions are highly irrelevant in our case. First, for such solutions to be *interesting* and *feasible*, finding Waldo should be *hard* for a computer whereas verifying that he is at a claimed location (with assistance) should be easy. This does not seem to be the case. Moreover, we would like the solution to be carried out between Alice and Bob *themselves*. We do not want to require them to possess sophisticated capabilities (such as being qualified programmers) or to have access to special devices including computers. (See [1] and [3] for examples of different cryptographic problems where non-computerized solutions are discussed.)

[*] Dept. of Computer Science and Applied Math, Weizmann Institute of Science, Rehovot 76100, Israel. E-mail: naor@wisdom.weizmann.ac.il. Supported in part by a grant from the Israel Science Foundation administered by the Israeli Academy of Sciences.

[†] Omanuyot School, Tel-Aviv, Israel. Supported by her parents.

[‡] Dept. of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot 76100, Israel. E-mail: reingold@wisdom.weizmann.ac.il. Supported by a Clore Foundation Fellowship and an Eshkol Post-Doctoral Fellowship.

To conclude, we are looking for a simple solution that does not require complicated computations or non-trivial prior knowledge from the parties and is low-tech in terms of the required resources.

2 Solutions

We now describe two solutions to Alice's problem and discuss their advantage and shortcomings. We note that these are not the only possible solutions. For example, Pinkas and Stopler [7] have suggested solutions that apply to "Where's Waldo?" as well as a large variety of other puzzles. However, their solutions require (off-line) assistance from the manufacturer of the puzzles. The reader is encouraged to come up with additional solutions.

2.1 A Mid-Tech Solution

Let us first slightly violate our low-tech requirement by assuming that Alice and Bob have access to a photocopy machine. In this case, Alice and Bob can perform a very simple protocol: they photocopy the specific "Where's Waldo?" puzzle in question. Alice now cuts out Waldo's image from that copy while Bob is not looking and then shows Bob the image (after hiding or destroying the leftovers). Her ability to do so is certainly a proof that she knows where Waldo is. On the other hand Bob learns nothing (or almost nothing) from the piece he sees (since he is already familiar with Waldo's image).

The obvious disadvantage of this solution (apart from requiring a photocopy machine) is the danger that Alice will cheat by hiding an additional image of Waldo (taken from a different picture) and showing this image (instead of the one in the original picture) to Bob. One way to combat this danger is to require Alice to enter an empty room with nothing on her apart from the picture, scissors, and a match-box. The version for paranoids is to also require a full cavity search. However, it turns out that there is a less invasive method to mend this solution, by using interaction: after photocopying the picture, Bob prints a *random* pattern on its back. Now Alice will be required to show (within a reasonably short time limit) Waldo's image with that specific pattern on its back (a pattern she could not have guessed in advance). Alice should make sure the pattern is regular, so as not to reveal information about the location. An alternative "non-destructive" solution is described below.

2.2 A Low-Tech Solution

The solution described here can be carried out with very simple accessories. Alice and Bob need a large piece of cardboard (at least twice as large as the picture in each dimension) with a small rectangle cut in the middle. In addition, they need paper clips to fix the correct page in the book. To show that she knows where Waldo is, Alice puts the rectangle on top of Waldo while Bob is not looking (to actually execute it Alice should place her finger on Waldo while navigating the cardboard). Bob sees Waldo and at worse learns something about Waldo's immediate surroundings (see Figure 1 for an illustration of Bob's view). However, since the cardboard is large enough to cover the picture (no matter where Waldo is), he learns nothing else about the location of Waldo. Before Bob is completely satisfied Alice must also demonstrate that she has the correct Waldo picture (and hasn't flipped a page). Therefore she should pull the book beneath the cardboard in front of Bob's eyes. This last step should be done with care, so as not reveal information about the place from which she is pulling the book. (At the very least the hole in the cardboard should be covered while the book is pulled out.)

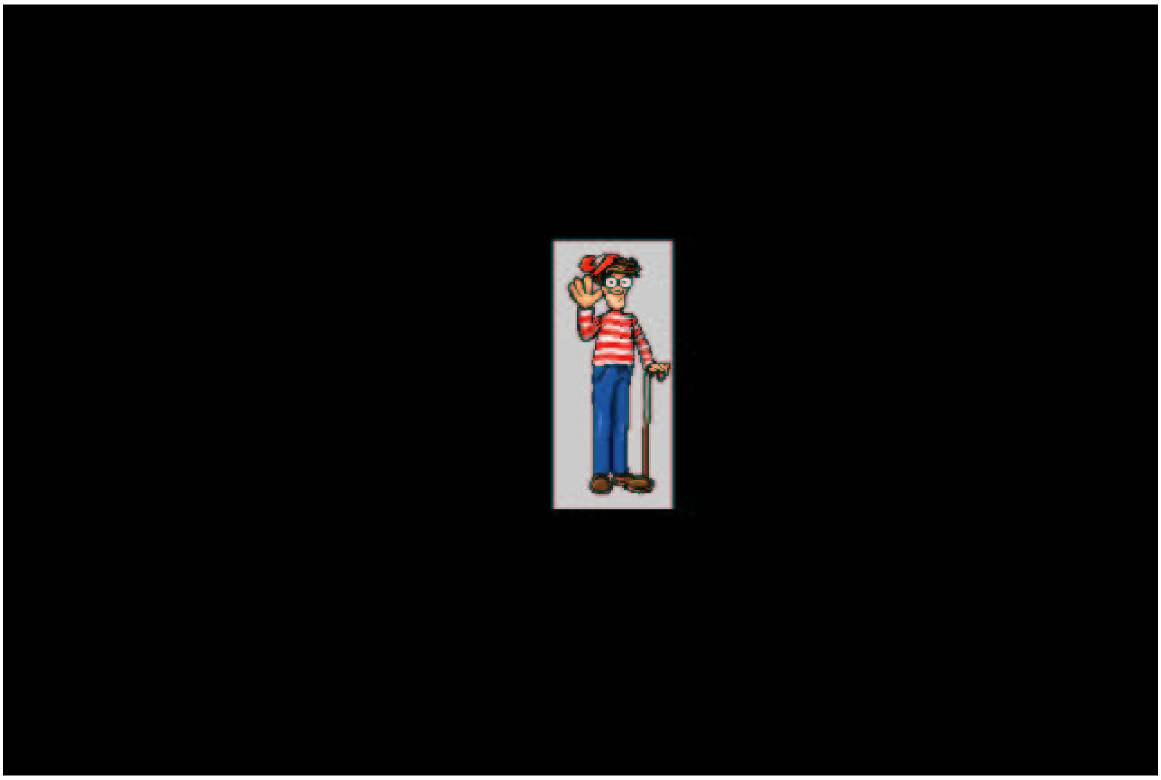

Figure 1: Bob's View

3 Conclusions

We find it interesting that one can demonstrate possession of knowledge without revealing it in a simple "everyday" scenario[1] and without resorting to high technology. Have we learned anything from this? Unlike Fellows and Koblitz [4], we do not claim that this applied kid cryptographic process is particularly educational. It was however very enjoyable to Alice and Bob (and to Carol as well).

Acknowledgments

Our deepest thanks to Waldo for making this note possible. We tried to thank him in person but could not find him.

References

[1] C. Crépeau and J. Kilian, *Discreet solitary games*, Advances in Cryptology - Crypto'93, Lecture Notes in Computer Science, No. 773, Springer Verlag, 1994, pp. 319–330.

[1] Note that previous non-computerized examples [4, 6] were either in the fictional setting of [6] or in the setting of abstract mathematics. Both of these examples hardly describe an everyday scenario. Also note the criticism in [4] regarding the validity of the Ali Baba and the cave story in [6] for demonstrating zero-knowledge.

[2] W. Diffie, *The First Ten Years of Public Key Cryptography*, in **Contemporary Cryptography The Science of Information Integrity**, edited by G. J. Simmons, IEEE Press, 1992.

[3] R. Fagin, M. Naor and P. Winkler, *Comparing Information Without Leaking It*, Communications of the ACM, vol 39, May 1996, pp. 77-85.

[4] M. R. Fellows and N. Koblitz, Kid Crypto, *Advances in Cryptology – Crypto* 92 *Proceedings*, Lecture Notes in Computer Science Vol. 740, E. Brickell ed., Springer-Verlag, 1992.

[5] O. Goldreich, *Randomness, Interactive Proofs, and Zero-Knowledge–A Survey*, in **The Universal Turing Machine: A Half Century Survey**, edited by Rolf Herken, Oxford University Press, 1988, pp. 377–405.

[6] Jean-Jacques Quisquater, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis Guillou, Marie Annick Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, Soazig Guillou and Tom Berson, How to explain zero-knowledge protocols to your children, *Advances in Cryptology – Crypto* 89 *Proceedings*, Lecture Notes in Computer Science Vol. 435, G. Brassard ed., Springer-Verlag, 1989, pp. 628–631.

[7] B. Pinkas and G. Stopler, personal communication.

[8] R. L. Rivest, A. Shamir, and L. M. Adleman, *A method for obtaining digital signature and public key cryptosystems*, Communications of the ACM, vol. 21, Feb 1978, pp. 120–126.

[9] http://www.findwaldo.com/