An Algorithm for Solving the LPN Problem and Its Application to Security Evaluation of the HB Protocols for RFID Authentication

Marc P.C. Fossorier[1], Miodrag J. Mihaljević[2,4], Hideki Imai[3,4], Yang Cui[5], and Kanta Matsuura[5]

[1] University of Hawaii, Department of Electrical Engineering, Honolulu, USA
[2] Mathematical Institute, Serbian Academy of Sciences and Arts, Belgrade, Serbia
[3] Chuo University, Faculty of Science and Engineering, Tokyo, Japan
[4] Research Center for Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan
[5] University of Tokyo, Institute of Industrial Science (IIS), Tokyo, Japan

Abstract. An algorithm for solving the "learning parity with noise" (LPN) problem is proposed and analyzed. The algorithm originates from the recently proposed advanced fast correlation attacks, and it employs the concepts of decimation, linear combining, hypothesizing and minimum distance decoding. However, as opposed to fast correlation attacks, no preprocessing phase is allowed for the LPN problem. The proposed algorithm appears as more powerful than the best one previously reported known as the BKW algorithm proposed by Blum, Kalai and Wasserman. In fact the BKW algorithm is shown to be a special instance of the proposed algorithm, but without optimized parameters. An improved security evaluation, assuming the passive attacks, of Hopper and Blum HB and HB$^+$ protocols for radio-frequency identification (RFID) authentication is then developed. Employing the proposed algorithm, the security of the HB protocols is reevaluated, implying that the previously reported security margins appear as overestimated.

Keywords: cryptanalysis, LPN problem, fast correlation attacks, HB protocols, RFID authentication.

1 Introduction

In [12] (following the prior work of Hopper and Blum [10]), two shared-key authentication protocols have been proposed and analyzed. Their extremely low computational cost makes them attractive for low-cost devices such as radio-frequency identification (RFID) tags. The first protocol (called the HB protocol) is proven secure against a passive (eavesdropping) adversary, while the second (called HB$^+$) is proven secure against the stronger class of active adversaries. Security of these protocols is based on the conjectured hardness of the "learning parity with noise" (LPN) problem (see [3], for example). In [13], the security of the HB and HB$^+$ protocols under parallel/concurrent executions has been proven.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 48–62, 2006.

The underlying paradigm of the HB protocol is the following. Suppose Alice and a computing device C share an k-bit secret $\mathbf{x}$, and Alice would like to authenticate herself to C. Then C selects a random challenge $\mathbf{a} \in \{0,1\}^k$ and sends it to Alice. Alice computes the binary inner-product $\mathbf{a} \cdot \mathbf{x}$, then sends the result back to C. Finally, C computes $\mathbf{a} \cdot \mathbf{x}$, and accepts the single round authentication if Alice's parity bit is correct. In a single round, someone imitating Alice who does not know the secret $\mathbf{x}$ will guess the correct value $\mathbf{a} \cdot \mathbf{x}$ half the time. By repeating for r rounds, Alice can lower the probability of naively guessing the correct parity bits for all r rounds to 2^{-r}. However, an eavesdropper capturing $O(k)$ valid challenge-response pairs between Alice and C can quickly calculate the value of $\mathbf{x}$ through Gaussian elimination. To prevent revealing $\mathbf{x}$ to passive eavesdroppers, Alice can inject noise into her response. Alice intentionally sends the wrong response with constant probability $p \in (0, 1/2)$. Then C authenticates Alice's identity if fewer than pr of her responses are incorrect.

Suppose that an eavesdropper, i.e., a passive adversary, captures q rounds of the HB protocol over several authentications and wishes to make the impersonation. The goal of the adversary in this case is equivalent to the core problem investigated in this paper. This problem is known as the learning parity in the presence of noise, or LPN problem. It is shown in [12] that the security of the both HB and HB$^+$ protocols against the passive attack depends on the hardness of LPN problem.

On the other hand, the results reported in [9] have recently shown a man-in-the-middle attack on the HB$^+$ protocol. However, the arguments given in [12] and [13] limit the impact of such attack.

Accordingly, this paper is focused only to the LPN problem and the passive attacking of HB and HB$^+$ protocols.

Motivation for the Work. Despite certain differences, both the LPN problem and the underlying problem of fast correlation attack can be viewed as the problem of solving an overdefined system of noisy linear equations. However, it appears that the currently reported approaches for solving the LPN problem do not take into account the approaches developed for fast correlation attacks. Accordingly, a goal of this work is to consider employment of fast correlation attack approaches for solving the LPN problem. Another motivation of this work is the security re-evaluation of the HB protocol for RFID authentication as its security level appears as a direct consequence of the LPN problem hardness.

Summary of the Contributions. This paper proposes a generic algorithm for solving the LPN problem. The proposed algorithm originates from the recently proposed advanced fast correlation attacks and it employs the following concepts: decimation, linear combining, hypothesizing and decoding. However, as opposed to fast correlation attacks, no preprocessing can be performed, which introduces an additional constraint. The following main characteristics of the proposed algorithm have been analytically established: (i) average time complexity; and (ii) average space complexity. The proposed algorithm has been compared with the best previously reported one, namely the BKW algorithm, and its advantages for solving the LPN problem have been pointed out. The proposed algorithm has been applied