A New Method for Solving Polynomial Systems with Noise over $\mathbb{F}_2$ and Its Applications in Cold Boot Key Recovery*

Zhenyu Huang and Dongdai Lin

State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
{huangzhenyu,ddlin}@iie.ac.cn

Abstract. The family of Max-PoSSo problems is about solving polynomial systems with noise, and is analogous to the well-known Max-SAT family of problems when the ground field is $\mathbb{F}_2$. In this paper, we present a new method called ISBS for solving the family of Max-PoSSo problems over $\mathbb{F}_2$. This method is based on the ideas of incrementally solving polynomial system and searching the values of polynomials with backtracking. The ISBS method can be combined with different algebraic methods for solving polynomial systems, such as the Gröbner Basis method or the Characteristic Set (CS) method. By combining with the CS method, we implement ISBS and apply it in Cold Boot attacks. A Cold Boot attack is a type of side channel attack in which an attacker recovers cryptographic key material from DRAM relies on the data remanence property of DRAM. Cold Boot key recovery problems of block ciphers can be modeled as Max-PoSSo problems over $\mathbb{F}_2$. We apply the ISBS method to solve the Cold Boot key recovery problems of AES and Serpent, and obtain some experimental results which are better than the existing ones.

Keywords: polynomial system with noise, Max-PoSSo, Cold Boot attack, boolean equations, Characteristic Set method, AES, Serpent.

1 Introduction

Solving polynomial system with noise, which means finding an optimal solution from a group of polynomials with noise, is a fundamental problem in several areas of cryptography, such as algebraic attacks, side-channel attacks and the cryptanalysis of LPN/LWE-based schemes. In computation complexity field, this problem is also significant and called the maximum equation satisfying problem [7,14]. In the general case, this problem is NP-hard even when the polynomials are linear. In [1], the authors classified this kind of problems into three categories:

* This work was in part supported by National 973 Program of China under Grants No. 2013CB834203 and No. 2011CB302400, the National Natural Science Foundation of China under Grant No. 60970152 and the "Strategic Priority Research Program" of the Chinese Academy of Sciences under Grant No. XDA06010701.
Max-PoSSo, Partial Max-PoSSo, and Partial Weighted Max-PoSSo, and called them the family of Max-PoSSo problems. Moreover, they presented a model by which they can convert the Cold Boot key recovery problems of block ciphers into the family of Max-PoSSo problems. The Cold Boot key recovery problems originated from a side channel attack which is called the Cold Boot attack\cite{8}. In a Cold Boot attack, an attacker with physical access to a computer is able to retrieve sensitive information from a running operating system after using a cold reboot to restart the machine from a completely “off” state. The attack relies on the data remanence property of DRAM to retrieve memory contents which remain readable in the seconds to minutes after power has been removed. Furthermore, the time of retention can be potentially increased by reducing the temperature of memory. Thus, data in memory can be used to recover potentially sensitive information, such as cryptographic keys. Due to the nature of the Cold Boot attack, it is realistic to assume that only decayed image of the data in memory can be available to the attacker, which means a fraction of memory bits will be flipped. Therefore, the most important step of the Cold Boot attack is recovering the original sensitive information from the decayed data.

In the case of block cipher, the sensitive information is the original key, and the decayed data is likely to be the round keys, which are generated from the origin key by the key schedule operation. Thus the Cold Boot key recovery problem of block cipher is recovering the origin key from the decayed round keys. Intuitively, every bit of round keys corresponds to a boolean polynomial equation with the bits of origin key as its variables. Then all bits of these round keys correspond to a boolean polynomial system. However, because of the data decay this polynomial system has some noise. In general case, these polynomials can be seen as random ones, so a random assignment may satisfy about half of them. If the percentage of the decayed bits is smaller than 50%, an assignment satisfying the maximum number of these polynomials may be equal to the origin key with high probability. By this way, we can model the Cold Boot key recovery problem of block cipher as the Max-PoSSo problem over $\mathbb{F}_2$, which is finding the optimal solution of a polynomial system with noise.

As mentioned before, the general Max-PoSSo problem over $\mathbb{F}_2$ is NP-hard. A natural way of solving Max-PoSSo problems over $\mathbb{F}_2$ is converting them into their SAT equivalents and then solve them by Max-SAT solvers. However, this method has a disadvantages that the original algebraic structure is destroyed. In \cite{1}, the authors converted the Max-PoSSo problems over $\mathbb{F}_2$ into mixed integer programming problems, and used the MIP solver SCIP to solve them. They presented some experimental results about attacking AES and Serpent. Their attack result about Serpent is a new result, and they showed that comparing with generic combinatorial approach their attack is much better.

The main contribution of this paper is that we propose a new method called ISBS for solving the family of Max-PoSSo problems over $\mathbb{F}_2$. The basic idea of ISBS is searching the values of polynomials. Precisely speaking, given a polynomials system with noise $\{f_1, f_2, \ldots, f_m\}$, we try to solve polynomial systems $\{f_1 + e_2, f_2 + e_2, \ldots, f_m + e_m\}$, where $\{e_1, e_2, \ldots, e_m\}$