Information Sciences 463–464 (2018) 75–85

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

On the asymptotic idealness of the Asmuth-Bloom threshold secret sharing scheme

Constantin Cătălin Drăgan, Ferucio Laurentiu Tiplea*

Department of Computer Science,"Alexandru Ioan Cuza" University of Iași, Romania

ARTICLE INFO

Article history:
Received 25 October 2014
Revised 2 January 2018
Accepted 17 June 2018
Available online 18 June 2018

Keywords:
Secret sharing scheme
Chinese remainder theorem
Entropy
Asymptotic perfectness
Asymptotic idealness

ABSTRACT

The Chinese remainder theorem (CRT) is a fundamental theorem in number theory, widely used in cryptography to design secret sharing schemes. The CRT-based secret sharing schemes proposed so far make use of sequences of pairwise co-prime integers with special properties. The way these sequences are chosen plays a crucial role in the security achieved by the schemes that rely on them. Moreover, the CRT-based secret sharing schemes could achieve at most asymptotic idealness. In this paper we prove that the Asmuth-Bloom threshold secret sharing scheme is asymptotic ideal if and only if it is based on 1-compact sequences of co-primes. Apart from this, a comprehensive analysis of the known variants of the Asmuth-Bloom threshold secret sharing scheme is provided, clarifying the security properties achieved by each of them.

1. Introduction

A $(t+1,n)$-threshold secret sharing scheme $(t+1,n)$-threshold scheme, for short) is a method of partitioning a secret among n users by providing each user with a share of the secret such that any $t+1$ users can uniquely reconstruct the secret by pulling together their shares. If less than $t+1$ shares give no information about the secret, from an information theoretic point of view, then the scheme is called *perfect*. In addition to this, if the share spaces have the same dimension with the secret space, the scheme is called *ideal*.

One of the techniques to construct threshold schemes is based on the Chinese remainder theorem (CRT) [1,2,6–10]. The main idea is to use sequences of pairwise co-prime positive integers with special properties. The shares are obtained by dividing the secret or a secret-dependent quantity by the numbers in the sequence and collecting the remainders.

The CRT-based threshold schemes proposed so far are neither perfect nor ideal. However, they offer some security degree and, in order to study it, Quisquater et al. [9] have introduced the concepts of *asymptotic perfectness* and *asymptotic idealness*. They also proved that the threshold scheme in [6] is asymptotically ideal (and, therefore, asymptotically perfect) provided that it uses sequences of consecutive primes and the secret is uniformly chosen from the secret space. This result was later improved in [2] by showing that the asymptotic idealness of this scheme is achieved for a subclass of *compact sequences of co-primes* [2]. Compact sequences of co-primes capture very well the idea of sequence of numbers of the "same magnitude", and they are much denser than sequences of consecutive primes [2]. Moreover, [2] studies the security of the Asmuth-Bloom threshold scheme [1] and also proposes some asymptotically perfect and ideal variants of it. Another variant of the Asmuth-

* Corresponding author.
E-mail addresses: constantin.dragan@info.uaic.ro (C.C. Drăgan), ferucio.tiplea@uaic.ro (F.L. Tiplea).

https://doi.org/10.1016/j.ins.2018.06.046
0020-0255/

Bloom threshold scheme was proposed in [7] which provides better security than the original Asmuth-Bloom threshold scheme.

This paper comes to complete a series of recent results regarding the security of the CRT-based threshold schemes [2,9,10]. The main result of the paper is a necessary and sufficient characterization of the security of the Asmuth-Bloom threshold scheme (Theorem 1). More precisely, we show that this scheme is asymptotically ideal with respect to the uniform distribution on the secret space if and only of it is based on *1-compact sequences of co-primes* [10]. This result is important from two points of view: first, it closes completely the security problem of the Asmuth-Bloom threshold scheme, and secondly it emphasizes the importance of 1-compact sequences of co-primes in studying the security of the CRT-based secret sharing schemes. Apart from the above main result, our paper makes a comprehensive analysis of the Asmuth-Bloom threshold scheme variants proposed so far, clarifying and discussing the security properties achieved by each of them.

The rest of the paper is organized as follows. The second section discusses the variants of the Asmuth-Bloom threshold scheme met in the literature. The basic security properties a CRT-based threshold scheme should fulfill are recalled in the third section. Moreover, an important result regarding the loss of entropy in a threshold scheme is also obtained. The fourth section establishes our main result regarding the security of the Asmuth-Bloom threshold scheme, while the fifth section clarifies the security of some variant of the Asmuth-Bloom threshold scheme. We conclude in Section 6.

2. The Asmuth-Bloom secret sharing scheme and variations

To facilitate the following description, we first fix the notation and terminology we use. The set of integers is denoted by $\mathbb{Z}$. A positive integer $a > 1$ is a *prime* number if the only positive divisors of it are 1 and a. Given two integers a and b, the notation (a, b) stands for the greatest common divisor of a and b. The integers a and b are called *co-prime* if $(a, b) = 1$, and they are called *congruent modulo* n, denoted $a \equiv b \bmod n$, if n divides $a - b$ (n is an integer too). The notation $a = b \mod n$ means that a is the *remainder* of the integer division of b by n. The set of all congruence classes modulo n is denoted $\mathbb{Z}_n$.

The *Chinese remainder theorem* (CRT) [4] states that, given a finite non-empty set I of positive integers and the integers b_i and m_i for all $i \in I$, the system of congruences

$$x \equiv b_i \bmod m_i, \quad i \in I \tag{1}$$

has a unique solution modulo $\prod_{i\in I} m_i$, provided that m_i and m_j are co-prime for any $i, j \in I$ with $i \neq j$.

One of the main applications of CRT in cryptography is the design of threshold schemes [1,5,6,8]. In this paper we will focus on the threshold scheme in [1] and some of its variants [2,7]. As all of them are based on sequences of positive integers with special properties, we begin with a few notations and definitions regarding them.

A *sequence of co-primes* is a sequence $m_0, m_1, \ldots, m_n$ of pairwise co-prime strictly positive integers, where $n \geq 1$. The *length* of this sequence is $n + 1$.

An *Asmuth-Bloom* $(t + 1, n)$*-threshold sequence of co-primes*, where t and n are two integers with $0 < t + 1 \leq n$, is a sequence of co-primes $m_0, m_1, \ldots, m_n$ which satisfies the following properties:

- $m_0 < m_1 < \cdots < m_n$;
- $\prod_{i=1}^{t+1} m_i > m_0 \prod_{i=0}^{t-1} m_{n-i}$ (this is called the *Asmuth-Bloom constraint*).

Let t and n be integers with $0 < t + 1 \leq n$. The *Asmuth-Bloom* $(t + 1, n)$*-threshold scheme* [1] is defined as follows:

(1) *parameter setup:* consider $m_0, m_1, \ldots, m_n$ an Asmuth-Bloom $(t + 1, n)$-threshold sequence of co-primes. The integers $t, n, m_0, m_1, \ldots, m_n$ are public parameters;
(2) *secret and share spaces:* define the secret space as $\mathbb{Z}_{m_0}$ and the share space of the ith participant as $\mathbb{Z}_{m_i}$, for all $1 \leq i \leq n$;
(3) *secret sharing:* given a secret s in the share space, randomly generate an integer $r \geq 0$ such that $0 \leq s' = s + rm_0 < \prod_{i=1}^{t+1} m_i$. Then, distribute s to the participants by computing $s_i = s' \bmod m_i$ for all $1 \leq i \leq n$ (s_i is the share of the ith participant, known only by him);
(4) *secret reconstruction:* any $t + 1$ distinct shares $s_{i_1}, \ldots, s_{i_{t+1}}$ can uniquely reconstruct the secret s by computing first the unique solution modulo $\prod_{j=1}^{t+1} m_{i_j}$ of the system

$$x \equiv s_{i_j} \bmod m_{i_j}, \quad 1 \leq j \leq t + 1$$

and then reducing it modulo m_0.

The ratio $|\mathbb{Z}_{m_i}|/|\mathbb{Z}_{m_0}|$ is referred to as the *information rate* of the ith participant, for any $1 \leq i \leq n$.

For the sake of simplicity, we will use the terminology "Asmuth-Bloom sequence of co-primes" ("Asmuth-Bloom threshold scheme") instead of "Asmuth-Bloom $(t + 1, n)$-threshold sequence of co-primes" ("Asmuth-Bloom $(t + 1, n)$-threshold scheme") whenever it is not important to mention t and n.

In order to obtain better security properties of the Asmuth-Bloom threshold scheme, several variants of it were proposed (details about their security will be given at the end of Section 3.1):