Information Processing Letters 114 (2014) 299–303

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

A necessary and sufficient condition for the asymptotic idealness of the GRS threshold secret sharing scheme

Ferucio Laurenţiu Ţiplea *, Constantin Cătălin Drăgan [1]

Department of Computer Science, Alexandru Ioan Cuza University of Iaşi, Romania

ARTICLE INFO

Article history:
Received 8 April 2013
Received in revised form 2 September 2013
Accepted 21 January 2014
Available online 23 January 2014
Communicated by V. Rijmen

Keywords:
Cryptography
Secret sharing scheme
Chinese Remainder Theorem
Entropy
(Asymptotic) perfectness
(Asymptotic) idealness

ABSTRACT

The study of the asymptotic idealness of the Goldreich–Ron–Sudan (GRS, for short) threshold secret sharing scheme was the subject of several research papers, where sufficient conditions were provided. In this paper a necessary and sufficient condition is established; namely, it is shown that the GRS threshold secret sharing scheme is asymptotically ideal under the uniform distribution on the secret space if and only if it is based on *1-compact sequences of co-primes*.

1. Introduction

The Chinese Remainder Theorem (CRT) is a very useful tool in many areas of theoretical and practical cryptography. One of these areas is the theory of threshold secret sharing schemes. 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. Several threshold schemes based on CRT are known [1–3]. These schemes 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 secret can be reconstructed by some sufficient number of shares by using CRT.

In order to study the security of the CRT-based threshold secret sharing schemes, Quisquater et al. [4] have introduced the concepts of *asymptotic perfectness* and *asymptotic idealness*, and proved that the Goldreich–Ron–Sudan (GRS) threshold scheme in [3] is asymptotically ideal (and, therefore, asymptotically perfect) under the uniform distribution on the secret space, provided that it uses sequences of consecutive primes. This result was later improved [5] by showing that the asymptotic idealness of this scheme is achieved not only for the class of sequences of consecutive primes but also for a larger class of sequences of co-primes, namely for the class of (t,Θ)-compact sequences of co-primes, where t defines the scheme threshold and Θ is any arbitrary real number in the interval $(0,1)$.

1.1. Contribution

Compact sequences of co-primes were introduced in [5] in an attempt to formalize the idea of sequences of positive integers of the "same magnitude" [3]. Both sequences of consecutive primes and (t,Θ)-compact sequences of co-primes are particular cases of compact sequences of

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

[1] Supported by the European Social Fund in Romania, under the responsibility of the Managing Authority for the Sectoral Operational Programme for Human Resources Development 2007–2013 [Grant POSDRU/CPP 107/DMI 1.5/S/78342].

0020-0190/$ – see front matter
http://dx.doi.org/10.1016/j.ipl.2014.01.008

co-primes [5]. Moreover, compact sequences of co-primes are much denser than sequences of consecutive primes [5]. Therefore, the results in [4] and [5] show that the GRS threshold scheme is asymptotically ideal under the uniform distribution on the secret space if it is based on some subclasses of the class of compact sequences of co-primes. In this context, the question is whether these results can be extended to the entire class of compact sequences of co-primes. Our paper answers this question. We introduce first the class of 1-compact sequences of co-primes as an extension of the class of compact sequences of co-primes and then we show that the GRS threshold scheme is asymptotically ideal under the uniform distribution on the secret space if and only if it is based on 1-compact sequences of co-primes.

We believe that our result is important from two points of view: first, it closes completely the security problem of the GRS threshold scheme, and secondly it emphasizes the importance of 1-compact sequences of co-primes in studying the security of the CRT-based threshold secret sharing schemes. Moreover, as far as we are concerned, this is the first time a necessary and sufficient condition for the asymptotic idealness of a CRT-based threshold secret sharing scheme is established.

2. The main result

In this section we recall the GRS threshold scheme [3] and then we prove our main result, namely that the GRS threshold scheme is asymptotically ideal under the uniform distribution on the secret space if and only if it is based on 1-compact sequences of co-primes.

2.1. The GRS scheme

Throughout this paper, $\mathbb{Z}$ stands for the set of integers. For two integers a and b, (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 set of all congruence classes modulo n is denoted $\mathbb{Z}_n$. A positive integer $a>1$ is a *prime* number if the only positive divisors of it are 1 and a.

The *Chinese Remainder Theorem* (CRT, for short) [6] states that the system of congruences

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

where I is a finite non-empty set of positive integers and b_i and m_i are integers for all $i\in I$, has a unique solution modulo $\prod_{i\in I} m_i$, if 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 is in the design of threshold secret sharing schemes [1–3]. Given t and n positive integers with $0<t+1\leqslant n$, the GRS $(t+1,n)$-threshold scheme in [3] is defined as follows:

(1) *Parameter setup*: consider $m_0<m_1<\cdots<m_n$ a *sequence of co-primes* (that is, $m_0,m_1,\ldots,m_n$ are pairwise co-prime strictly positive integers in increasing order). The integers $t,n,m_0,m_1,\ldots,m_n$ are public parameters;

(2) *Secret and share spaces*: define the *secret space* as being $\mathbb{Z}_{m_0}$ and the *share space* of the ith participant as being $\mathbb{Z}_{m_i}$, for all $1\leqslant i\leqslant n$;

(3) *Secret sharing*: given a secret s in the secret space, share it by $s_i=s' \bmod m_i$, for all $1\leqslant i\leqslant n$, where s' is the unique solution modulo $m_0\prod_{i=1}^{t} m_i$ of the system

$$x\equiv r_i \bmod m_i,\quad 0\leqslant i\leqslant t,$$

where $r_0=s$ and r_i is randomly chosen from $\mathbb{Z}_{m_i}$ for all $1\leqslant i\leqslant t$;

(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

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

and then reducing it modulo m_0.

The correctness of the reconstruction step above is as follows: by solving the system of congruences from the step (4) one obtains the unique solution s' modulo $\prod_{j=1}^{t+1} m_{i_j}$. As $\prod_{j=1}^{t+1} m_{i_j} > m_0\prod_{i=1}^{t} m_i$ and s' is a solution to the system of congruences from the step (3) too, one obtains $s=s' \bmod m_0$.

2.2. Asymptotic idealness

Given the GRS $(t+1,n)$-threshold scheme, a sequence $m_0<m_1<\cdots<m_n$ of co-primes, and a non-empty set $I\subseteq\{1,\ldots,n\}$, consider X and Y_I two random variables associated to the secret space $\mathbb{Z}_{m_0}$ and to the combined share space $\prod_{i\in I}\mathbb{Z}_{m_i}$, respectively. For any $y_I\in\prod_{i\in I}\mathbb{Z}_{m_i}$, define the *loss of entropy with respect to* y_I [4], denoted $\Delta(y_I)$, by

$$\Delta(y_I)=H(X)-H(X|Y_I=y_I),$$

where $H(X)$ stands for the entropy of X and $H(X|Y_I=y_I)$ stands for the entropy of X conditioned by $Y_I=y_I$.

The GRS $(t+1,n)$-threshold scheme is called *asymptotically perfect* [4] if for any non-empty subset $I\subseteq\{1,\ldots,n\}$ with $|I|\leqslant t$ and for any $\epsilon>0$ there exists $m\geqslant 0$ such that for any sequence $m_0<m_1<\cdots<m_n$ of co-primes with $m_0\geqslant m$, the following hold:

- $H(X)\neq 0$;
- $|\Delta(y_I)|<\epsilon$, for any $y_I\in\prod_{i\in I}\mathbb{Z}_{m_i}$.

The GRS $(t+1,n)$-threshold scheme is called *asymptotically ideal* [4] if it is asymptotically perfect and for any $\epsilon>0$ there exists $m\geqslant 0$ such that for any sequence $m_0<m_1<\cdots<m_n$ of co-primes with $m_0\geqslant m$ and any $1\leqslant i\leqslant n$ the following holds:

$$\frac{|\mathbb{Z}_{m_i}|}{|\mathbb{Z}_{m_0}|}<1+\epsilon.$$

$|\mathbb{Z}_{m_i}|/|\mathbb{Z}_{m_0}|$ is called the *information rate* of the ith participant.

Remark 1. One can easily see that the constraint "for any $\epsilon>0$" in the concepts of asymptotic perfectness and idealness can be equivalently replaced by "for any $0<\epsilon<1$".