Chapter 13
A 3D-Cellular Automata-Based Publicly-Verifiable Threshold Secret Sharing

Rosemary Koikara
Kyungpook National University, South Korea

Eun-Joon Yoon
Kyungil Univeristy, South Korea

Anand Paul
Kyungpook National University, South Korea

ABSTRACT

In secret sharing, a secret is distributed between various participants in a manner that an authorized group of participants in the appropriate access structures can recover this secret. However, a dealer might get corrupted by adversaries and may influence this secret sharing or the reconstruction process. Verifiable secret sharing (VSS) overcomes this issue by adding a verifiability protocol to the original secret sharing scheme. This chapter discusses a computationally secure publicly verifiable secret sharing scheme constructed using the three-dimensional cellular automata (3D CA). The initial configuration of the 3D CA is the secret. The following configurations are devised to be the shares distributed among the participants. Update mechanisms and various rules make it hard for an adversary to corrupt or duplicate a share. To make it even more efficient, the authors added a verifiability layer such that a dealer posts a public share and a private share to each shareholder. The NIST test suite has been used to calculate the randomness of the shares.

INTRODUCTION

Securing information that is flowing on the Internet has become crucial in the past few years. There has been an escalation in the amount of cyber-crime when it comes to an organization's privacy or an individual's privacy. Cryptographic algorithms like DES (Diffie, & Hellman, 1977) and RSA (Rivest,

DOI: 10.4018/978-1-5225-9611-0.ch013

Shamir, & Adleman, 1978) have been used for encrypting data using keys. However, here the security of information lies in the safety of the keys. Key-management techniques were developed to solve this issue. Secret sharing was one of the techniques that emerged mainly for key management though it has many other applications.

Secret sharing (SS) is composed of two algorithms – the secret sharing algorithm and the reconstruction algorithm. In SS, a dealer generates shares and then distributes them to various participants who then become shareholders. The shares generated are then used to reconstruct the secret. The concept of secret sharing was first formulated independent of each other by Shamir (1979) and Blakley (1979) in 1979. The SS scheme developed were $\left(k,n\right)$-threshold SS schemes in which a secret $\mathcal{S}$ is divided among n shareholders such that at least k or more shareholders are required to reconstruct the secret correctly. It is not feasible to reconstruct the secret if $k-1$ or fewer shares are present. Polynomial arithmetic operations and interpolation form the basis of Shamir's Scheme. The goal was to take k points and guarantee that a unique polynomial with those points exists. The interpolation of the missing points corresponding to the polynomial is made possible. Blakley's scheme, on the other hand, was based on hyperplane intersections instead of polynomial interpolation.

The shareholders in SS belong to various subsets of participants called the access structure. Suppose, $\mathcal{A}$ is the access structure, then $\mathcal{A}$ determines the mechanism to share and reconstruct the secret. "Any subset in $\mathcal{A}$ can reconstruct the secret from its shares, and any subset not in $\mathcal{A}$ cannot reveal any information about the secret" (Beimel, 2011). Depending upon the access structure, there can be many SS schemes. A hierarchical threshold SS scheme that had a hierarchical access structure was proposed by Tassa (2007). This scheme was based on Birkhoff interpolation and could share one secret.

Shamir's SS scheme among other commonly used SS mechanisms can be used to distribute only one secret. However, the secret messages are not always small, and they may be huge on certain occasions (Capocelli, Santis, Gargano, & Vaccaro, 1991). There has to be a technique to share more than one secret message among shareholders. In ref. (He, & Dawson, 1994; Blundo, De Santis, Di Crescenzo, Gaggia, &Vaccaro, 1994), multi-secret sharing schemes were proposed. These schemes as mentioned earlier use were based on Shamir's schemes.

Numerous research has been carried out in the field of SS (Benalo, & Leichter, 1990; Ito, Saito, & Nishizeki, 1989; Simmons, 1991; Brickell, 1989; Karchmer, &Wigderson, 1993; Bertilsson, & Ingemarsson, 1992). Shamir's SS scheme is the most widely researched SS technique. Researchers have also proposed different techniques. Mignotte (1982) and Asmuth and Bloom (1983) proposed to use the Chinese Remainder Theorem (CRT) to share the secret. It was later pointed out by Kaya and Selçuk (2008) that Mignotte's and Asmuth-Bloom's schemes are not safe against dishonest dealers. A dealer can distribute inconsistent shares to the shareholders, and the schemes cannot prevent that. Kaya et al. proposed a Verifiable Secret Sharing (VSS) scheme based on the CRT and the RSA assumption. Goyal and Kumar (2018) introduced an SS scheme for general access structures such that if an adversary tampers with any or all of the shares, either the original secret is reconstructed or lost.

Cellular automata (CA) have also been used to design SS algorithms. A CA is an arrangement of cells. The state of each cell depends on the states of neighboring cells and is updated with time. An update mechanism and rules govern the approach used to make the change in the state of each cell. The same update rule is used to synchronously modify the states of the cells across the CA. A CA may be of various dimensions: one dimensional (1D), two dimensional (2D) or three dimensional (3D). The use of 3D-CA in a SS scheme increases the complexity of a third party to attack the system.