Verifiable Self-Selecting Secret Sharing Based on Elliptic Curves

Hichem Bouchakour Errahmani, Belhadj Bouchaib Center University of Ain Témouchent, Algeria & EEDIS Laboratory, Djilali Liabes University of Sidi Bel Abbes, Algeria
Hind Ikni, Belhadj Bouchaib Center University of Ain Témouchent, Algeria

ABSTRACT

In distributed systems, as any network architecture, cryptography has a vital role in communication security, and sharing a secret represents a jump in this field where the secret depends on a group instead of a single person. In this article, the authors propose a method to share a multi secrets matrix represented by an image, that could be reconstructed without any loss by an access structure over a distributed system. The presented approach has a verifiable property, where each candidate possesses the advantage to verify the validity of his shadow. The security level of the scheme is based on elliptic curve discrete logarithm problem and the opportunity of allowing each side to generate a private sub-secret key for the sharing. The benefit of this method is justified by the absence of information loss and a lower timing results.

KEYWORDS
Discrete Logarithm Problem, Elliptic Curve Cryptography, Image Secret Sharing, Verifiable Secret Sharing

INTRODUCTION

Classical cryptography treats the notions of encryption, decryption, and hashing using secret keys are the actors of the cryptosystem. Those keys represent the security basis of the entire system according to Kerckhoffs principles. On the other hand, the question that could arises in our mind, is how to protect such an important key? Hence, the notion of threshold secret sharing, where the key is distributed over a group of participants in such a way that none of them possesses an information about the secret, but some candidates representing the access structure collaborate at its reconstitution. Several works have contributed to improve secret sharing since the first approach of Adi Shamir, such as verifiable approaches and proactive ones. However, the particularity of contemporary methods lies in the use of elliptic curves, for the reason that they revolutionized cryptosystems security by providing solutions to constraints caused by key size and operations complexity. In this paper, the researchers propose a method of securing visual cryptographic keys by multi secrets sharing scheme with self-selecting of private ones, based on ECDLP. The scheme takes as input an image matrix which represent the secret to share on a server–client network without information loss. In this method, the authors give the participants the capability to verify their received shares without secret reconstruction, to

DOI: 10.4018/IJSI.2020070104

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
prove the validity of the dealer, shadows, and even candidates. The rest of the paper is structured as follows: Section II illustrates preliminaries techniques for a good comprehension of the subject. Section III presents related works for sharing secrets using elliptic curves. Section VI describes steps of the proposed approach. Section V discus results. Finally, section IV concludes and resumes the paper.

**Preliminaries**

In this section, the authors describe basic techniques used for secret sharing with elliptic curves.

**Elliptic Curve**

An elliptic curve $E$ over a finite field $\mathbb{F}_p$ is a set of pairs $(X,Y) \in \mathbb{F}_p^2$ resolving the Equation $Y^2 = X^3 + A \cdot X + B \pmod{p}$ union a particular element called point at infinity noted $O$ such that $A, B \in \mathbb{F}_p$ and $4A^3 + 27B^2 \neq 0 \pmod{p}$ (Paar, 2009) (Figure 1).

![Elliptic curve over R (a) and over Finit Field F_p (b)](image)

Some operations properties over $E(\mathbb{F}_p)$ should be mentioned:

1. Closure: $\forall P, Q \in E$, if $P + Q = R$ then $R \in E$;
2. Associativity: $\forall P, Q, R \in E, (P + Q) + R = P + (Q + R)$;
3. Identity element: $\forall P \in E$, $P + O = O + P = P$;
4. Inverse element: $\forall P(x, y) \in E$, $\exists - P(x, -y) \in E$;
5. Commutativity: $\forall P, Q \in E : P + Q = Q + P ; (X,Y) \in F_p^2 (X,Y) \in F_p^2$.

By inference: $E(\mathbb{F}_p)$ forms an abelian group.

The addition law in $E(\mathbb{F}_p)$ is defined as follows.
A Historical Analysis of the Emergence of Free Cooperative Software Production
www.igi-global.com/chapter/historical-analysis-emergence-free-cooperative/29373?camid=4v1a

A Formal Verification and Validation Approach for Real-Time Databases
www.igi-global.com/chapter/formal-verification-validation-approach-real/29555?camid=4v1a