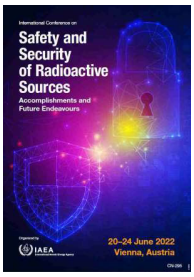


Contribution ID: **9** Type: **Poster**

# Iris Cryptosystem Based on Elliptic Curve Cryptography

*Tuesday, 21 June 2022 16:15 (15 minutes)*

The possibility that radioactive sources could be used for malicious purposes cannot be ruled out in the current global situation. Today, there is a growing concern that terrorist or criminal groups could gain access to high activity radioactive sources and use the sources maliciously. Then, security of radioactive sources has long been a matter of national and international concern. States have agreed to strengthen existing and have established new international legal instruments to enhance nuclear security worldwide.
Based on the basic IAEA guidance, one of the main security pillars for radioactive sources, is that the operator should provide a means of physically controlling access that effectively restrict access to authorized persons only to radioactive sources location, generally by allowing such individuals to temporarily disable physical barriers such as a locked door upon identification of the individual and access authorization.
Biometric technologies become best practice as a sophisticated technology for the identification and authorization of an individual seeking access, that can be used in a standalone or in combination with other traditional identification systems that relay on passwords, ID cards, or personal identification numbers (PINs), attributed to its enhanced accuracy, improved accountability, and a reduction in opportunities for misuse, compared to the traditional identification systems.
However, conventional unprotected biometric schemes are highly vulnerable to numerous privacy and security attacks. To overcome this problem, this paper presents a high-secure biometric authentication system using elliptical curve cryptography (EEC) to protect users'biometric data during storage and transmission. This method guarantees a high degree of privacy/security protection without affecting the performance accuracy compared to unprotected conventional biometric system.
This research mainly will focus on iris authentication as a model but the concepts and solutions can be extended for other biometric authentication methods. Comprehensive experiments on CASIA Iris Image Database V3.0 demonstrate the same performance accuracy with respect to its original counterparts yet which present robust protection against several major privacy/security attacks.

## Country OR Intl. Organization

Egypt

**Primary authors:** ASAKER, ahmed (Egyptian Atomic Energy Authority); Prof. ZAHRAN, Osama (Department of Electronics and Electrical Communication Engineering, Faculty of Electronic Engineering Menoufia University); Prof. ABD EL-SAMIE , Fathi E. (Menoufia University); Prof. AYAD, Nabil (Egyptian Atomic Energy Authority); Dr NASSAR, Sabry (Egyptian Atomic Energy Authority ); Dr ELSHARKAWY, Zeinab F. (Egyptian Atomic Energy Authority)

**Presenter:** ASAKER, ahmed (Egyptian Atomic Energy Authority)

**Session Classification:** Poster Session 1

**Track Classification:** 12. Sustainability and effectiveness of safety and security systems and measures, including emerging technologies