Publicacions més rellevants de la línia de recerca:
Criptografia en entorns computacionalment restringits

Referència: Martínez, S., Valls, M., Roig, C., Miret, J. and Giné, F. A secure elliptic curve-based RFID protocol. *Journal of Computer Science and Technology*, **24(2)** (2009), pp. 309–318.

Abstract: Nowadays, the use of Radio Frequency Identification (RFID) systems in industry and stores has increased. Nevertheless, some of these systems present privacy problems that may discourage potential users. Hence, high confidence and efficient privacy protocols are urgently needed. Previous studies in the literature proposed schemes that are proven to be secure, but they have scalability problems. A feasible and scalable protocol to guarantee privacy is presented in this paper. The proposed protocol uses elliptic curve cryptography combined with a zero knowledge-based authentication scheme. An analysis to prove the system secure and even forward secure is also provided.

Referència: Miret, J., Sadornil, D., Tena, J., Tomàs, R. and Valls, M. On avoiding ZVP-attacks using isogeny volcanoes. WISA 2008 *LNCS* 5379, **12(3)** (2009), pp. 266–277.

Abstract: The usage of elliptic curve cryptography in smart cards has been shown to be efficient although, when considering curves, one should take care about their vulnerability against the Zero-Value Point Attacks (ZVP). In this paper, we present a new procedure to find elliptic curves which are resistant against these attacks. This algorithm finds, in an efficient way, a secure curve by means of volcanoes of isogenies. Moreover, we can deal with one more security condition than Akishita-Takagi method with our search.

Referència: Miret, J., Sadornil, D., Tena, J., Tomàs, R. and Valls, M. Exploiting isogeny cordillera structure to obtain cryptographically good elliptic curves. *Journal of Research and Practice in Information Technology*, **40(4)** (2008), pp. 255–265.

Abstract: The security of most elliptic curve cryptosystems is based on the intractability of the Elliptic Curve Discrete Logarithm Problem (ECDLP). Such a problem turns out to be computationally unfeasible when elliptic curves are suitably chosen. This paper provides an algorithm to

obtain cryptographically good elliptic curves from a given one. The core of such a procedure lies on the usage of successive chains of isogenies, visiting different volcanoes of isogenies which are located in different ℓ–cordilleras.