FAST AND SECURE ELLIPTIC CURVE CRYPTOGRAPHY

X.Fan[1], G.Gong[1], P.Longa[2], B.Schoenmakers[3], F.Sica*[4], A.Sidorenko[5]

[1]Communication Security Lab, Department of Electrical and Computer Engineering, University of Waterloo, Canada; [2]Microsoft Research, Redmond WA, USA; [3]Coding and Crypto Group, Technical University of Eindhoven, The Netherlands; [4]School of Science and Technology, Nazarbayev University, Astana, Kazakhstan; *francesco.sica@nu.edu.kz; [5]Brightsight, The Netherlands

INTRODUCTION.

We survey several advances in the implementation and security design of elliptic curve cryptography. Elliptic curve cryptography is an attractive paradigm of public key cryptography, because it is both secure and lightweight, compared to existing solutions using RSA. For instance, such technology is currently implemented in the encryption of Blackberry smartphones and in the protection of digital data on the Austrian citizenship card (chip card).

RESULTS AND DISCUSSION.

In several works in collaboration, the presenter highlights his recent research in the field of elliptic curve cryptography, both in the implementation of algorithms making use of elliptic curves and in the analysis of their security.

Among the results, we can cite

- An analysis of the four dimensional Gallant-Lambert-Vanstone method to speed up scalar multiplication by a realistic factor of 1.5 [1].
- An efficient method to compress and decompress data arising from multiple points on an (hyper) elliptic curve [2].
- A provable use of elliptic curves in the context of pseudorandom generation of bits [3].
- An improvement of an algorithm due to Cheon to compute discrete logarithms with auxiliary inputs on certain curves [4].

CONCLUSIONS.

The study of elliptic curves in the context of cryptography is less than thirty years old. Thanks to work such as ours, this technology is now sufficiently well understood and reliable to be deployed commercially and endorsed by the United States NSA.

ACKNOWLEDGMENTS.

The presenting author's research is supported by a Nazarbayev University seed grant.

REFERENCES.

1. P. Longa. F. Sica. (2013). Four-dimensional Gallant–Lambert–Vanstone scalar multiplication, Journal of Cryptology, Springer (in press).
2. X. Fan, F. Sica. (2013). Multiple Point Compression on Elliptic and Hyperelliptic Curves, preprint.
3. X. Fan, G. Gong, B. Schoenmakers, F. Sica, A. Sidorenko. (2013). Simultaneous and Secure Bit Extraction on Koblitz Curves, preprint.
4. F. Sica. (2013). Group Action and the Discrete Logarithm Problem, preprint.