MULTIPLE POINT COMPRESSION ON CURVES

X. Fan[1], A. Otemissov[2], F. Sica[2*], A. Sidorenko[3]

1) Communication Security Lab, Department of Electrical and Computer Engineering, University of Waterloo, Canada; 2) School of Science and Technology, Nazarbayev University, Astana, Kazakhstan; *francesco.sica@nu.edu.kz; 3) Brightsight, The Netherlands

Introduction. Point compression is an essential technique to save bandwidth and memory when deploying elliptic curve based security solutions in wireless communication systems. Normally, a point would be stored by its two coordinates *(x,y),* which are finite field elements. Alternatively, one can store only *x* and recover *y* by computing a square root. We show that one can improve the decompression (i.e. finding y) when *n* points are stored simultaneously, by saving only n+1 field elements.

Figure 1. Real construction process.

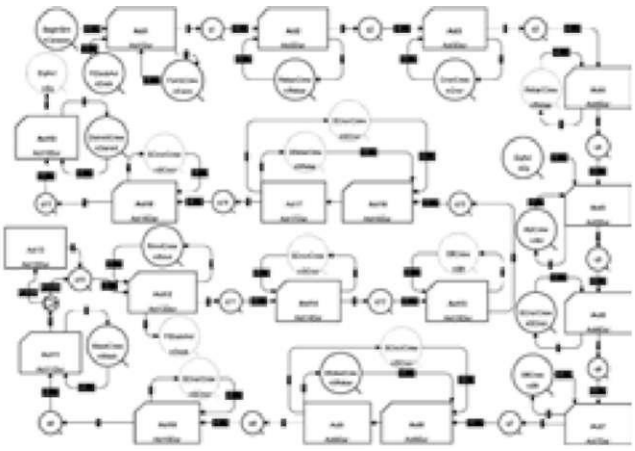

Figure 2. Developed simulation model.

Methods. We use linear algebra methods, following [1]. This allows us to compute all the y coordinates of the n points in a constant number of field operations (independently of the field).

Results and discussion. We extend the results of [1], originally valid for n=2 and 3, to 4 and 5 points explicitly and to any value of *n* asymptotically. The corresponding article [2] has been submitted to the conference Public Key Cryptography 2015, one of the top conferences in the area, with typically around 20% acceptance rate.

Conclusions. Multiple point compression is an important feature to improve the implementation of elliptic curve cryptography. This can be extended to other curves, in particular hyperelliptic curves, with divisors represented in Mumford form.

Acknowledgments. Dr. Francesco Sica is supported by a Nazarbayev University seed grant. We thank Changbo Chen for discussions about Grobner bases.

References.

1. M. Khabbazian, T. A. Gulliver, and V. K. Bhargava. Double point compression with applications to speeding up random point multiplication. *IEEE Trans. Computers,* 56(3):305-313, 2007.
2. X. Fan, A. Otemissov, F. Sica and A. Sidorenko, Multiple Point Compression on Curves, submitted to PKC 2015.