Computing small discrete logarithms using non-exhaustive lookup tables

Vasileios Mavroudis

mavroudisv@cs.ucsb.edu

ABSTRACT

In our previous work [1], we used an additively homomorphic elliptic-curve cryptosystem, based on El Gamal, to compute privacy-preserving statistics for the Tor network [5]. The decryption algorithm of our cryptographic scheme required the computation of a small discrete logarithm (DL). This step should have been trivial, since various algorithms have been proposed (i.e. Pollard's rho) in the past to solve small instances of the DL problem.

However, in our case the discrete logarithms ended up being quite large and a lookup table of precomputed discrete logarithms was proposed as the most time efficient solution. Unfortunately, this resulted in quite large and hard to manage tables.

In this work, we investigate an alternative approach, which has been also been considered in the past [2] [3] [4]. More specifically, we use non-exhaustive lookup tables to assist and speed up the computation of the small discrete logarithms. This approach is combined with one of the traditional DL algorithms to find an acceptable trade-off between speed and the size of tables. Based on our findings, we provide a python implementation of our method, which we also incorporate in Crux [1].

References

[1] Crux: Privacy-Preserving statistics for Tor, https://github.com/mavroudisv/Crux, Retrieved: 11/03/2015

[2] Bernstein, Daniel J., and Tanja Lange. "Computing small discrete logarithms faster." Progress in Cryptology-INDOCRYPT 2012. Springer Berlin Heidelberg, 2012. 317-338

[3] Bernstein, Daniel J., and Tanja Lange. "Non-uniform cracks in the concrete: the power of free precomputation." Advances in Cryptology-ASIACRYPT 2013. Springer Berlin Heidelberg, 2013. 321-340.

[4] Galbraith, Steven, and Pierrick Gaudry. ”Recent progress on the elliptic curve discrete logarithm problem.” Designs, Codes and Cryptography (2015).

[5] Dingledine, Roger, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. Naval Research Lab Washington DC, 2004.