Computing Low-Weight Discrete Logarithms

Ryan Henry, *Indiana University Bloomington*

Joint work with Bailey Kacsmar (University of Waterloo) and Sarah Plosker (Brandon University)

This work deals with the problem of computing discrete logarithms when the radix-b representation of the exponent sought is known to have "low weight" (i.e., only a small number of nonzero digits). Specifically, it proposes and analyzes three new baby-step giant-step algorithms for solving such discrete logarithms in time depending mostly on the radix-b weight (and length) of the exponent. Prior to this work, such algorithms had been proposed for the case where the exponent is known to have low Hamming weight (i.e., the radix-2 case) [4]. The new algorithms (i) improve on the best-known deterministic complexity for the radix-2 case, and then (ii) generalize from radix-2 to arbitrary radixes $b > 1$. When the radix is set to $\lceil \sqrt{q} \rceil$ in a group of order q, all three algorithms reduce to the familiar "textbook" version of baby-step giant-step, as proposed by Dan Shanks back in 1969 [3].

Briefly, the *discrete logarithm (DL) problem* in a multiplicative group $\mathbb{G}$ of order q is the following: Given as input a pair $(g, h) \in \mathbb{G} \times \mathbb{G}$, output an exponent $x \in \mathbb{Z}_q$ such that $h = g^x$, provided one exists. The exponent x is called a *discrete logarithm* of h with respect to the base g and is denoted, using an adaptation of the familiar notation for logarithms, by $x \equiv \log_g h \bmod q$. A longstanding conjecture, commonly referred to as the *DL assumption*, posits that the DL problem is "generically hard"; that is, that there exist infinite families of finite groups with respect to which no (non-uniform, probabilistic) polynomial-time (in $\lg q$) algorithm can solve uniform random instances of the DL problem with inverse polynomial (again, in $\lg q$) probability.

The new algorithms do not refute (or even pose a serious challenge to) the DL assumption. Indeed, although the new algorithms are generic,[1] they do not apply to uniform random DL instances nor do they generally run in polynomial time. Rather, the results demonstrate how, for certain *non-uniform* instance distributions, one can solve the DL problem in time depending on a parameter much smaller than $\lg q$. Specifically, to solve a DL problem instance in which the radix-b representation of the exponent has length m and weight t, the fastest deterministic algorithm evaluates $t\left(\binom{t/2}{m/2} + \mathrm{O}(1)\right)b^{t/2}$ group operations and stores $2\binom{t/2}{m/2}$ group elements in the worst case; for the same problem, the fastest randomized (Las Vegas) algorithm evaluates fewer than $\sqrt{2t}\left(\binom{t/2}{m/2} + \mathrm{O}(1)\right)b^{t/2}$ group operations and stores $\binom{t/2}{m/2}$ group elements, on average.

While a far cry from challenging established cryptographic best practices, the new algorithms are not without practical ramifications. For example, their cryptanalytic utility manifests as devastating attack against some recent Verifier-based Password Authenticated Key Exchange (VPAKE) protocols [1, 2, 5] which—extrapolating from performance measurements obtained using a proof-of-concept Java implementation—renders all three constructions completely insecure in practice.

References

[1] Franziskus Kiefer and Mark Manulis. Zero-knowledge password policy checks and verifier-based PAKE. In *Proceedings of ESORICS 2014 (Pt. II)*, volume 8713 of *LNCS*, pages 295–312, Wrocław, Poland (Sept. 2014).

[2] Franziskus Kiefer and Mark Manulis. Blind password registration for verifier-based PAKE. In *Proceedings of AsiaPKC 2016*, pages 39–48, Xi'an, China (May 2016).

[3] Daniel Shanks. Class number, a theory of factorization, and genera. In *Proceedings of Symposium of Pure Mathematics*, volume 20, pages 415–440, Providence, RI, USA (July–Aug. 1969).

[4] Douglas R. Stinson. Some baby-step giant-step algorithms for the low Hamming weight discrete logarithm problem. *Mathematics of Computation*, 71(237):379–391, 2002.

[5] Xiaoyan Yang, Han Jiang, Qiuliang Xu, Mengbo Hou, Xiaochao Wei, Minghao Zhao, and Kim-Kwang Raymond Choo. A provably-secure and efficient verifier-based anonymous password-authenticated key exchange protocol. In *Proceedings of IEEE TrustCom/BigDataSE/ISPA 2016*, pages 670–677, Tianjin, China (Aug. 2016).

[1] In other words, the algorithms require only black-box oracle access to the group operation (and its inverse) and can, therefore, be run over *any* finite group.