Lim-Lee precomputed exponentiation fixed and optimized

Denis Kryskov

Proposed in [1] is a fast method of table-assisted exponentiation. Unfortunately original description and it's narrations such as [2, §9.49] contain error: main formulae is generally incorrect, and hence algorithm sometimes fails to find answer. To the best of author's knowledge, neither the error has been publicly reported, nor a revised algorithm has been presented.

We

- prove the main equation [1, (8)] wrong, by giving counter-example;
- fix the error by restricting parameter choice $b = \left\lceil \frac{a}{v} \right\rceil \longrightarrow b = \frac{a}{v}$, then prove the equation correct;
- optimize the algorithm by relaxing condition $a = \left\lceil \frac{n}{h} \right\rceil \longrightarrow a \geq \left\lceil \frac{n}{h} \right\rceil$;
- formulate the revised method in a general setting (finding exponent in an arbitrary monoid);
- report a successful NVIDIA GPU implementation which outruns sliding-window exponentation [3] (doing 4.1e4 512-bit exponentations/sec) by a factor of 2.9 (GPU speed difference accounted for).

Keywords: Lim–Lee, precomputed exponentation, table-assisted exponentation, NVIDIA, CUDA, GPU, Python, auto-generated code, PTX, monoid, semi-group

References

[1] Lim C.H., Lee P. J. More flexible exponentiation with precomputation // Advances in Cryptology — Crypto 1994, Lecture Notes in Comput. Sci., vol. 839, Springer-Verlag, Berlin. — 1994. P. 95–107.

[2] Cohen H. et al. Handbook of Elliptic and Hyperelliptic Curve Cryptography // Chapman & Hall/CRC. — 2005. — 843 p.

[3] Neves S., Araujo F. On the Perfomance of GPU Public-Key Cryptography // University of Coimbra, Portugal: 2011. — 8 p.