Rank Estimation

Vincent Grosso

Rank Estimation

Vincent Grosso *

Definitions

Rank estimation algorithms are evaluation tools that aim to compute the cost of a key recovery using optimal key enumeration algorithms. It allows evaluating the security margins after a divide-and-conquer attack.

Background

At the end of a side-channel attack, an attacker can take advantage of post-processing techniques known as key enumeration to improve the success probabilities of his attack. The rank is the number of master key candidates with higher probabilities than the actual master key k^*:

$$\text{rank}(k^*) = \#\{k, \Pr[K = k] \geq \Pr[K = k^*]\} \quad (1)$$

As shown in the eq. (1), the rank gives the number of keys to test before finding the actual key, i.e. the cost of the post-processing of an attack.

In side-channel attacks and, more generally, divide-and-conquer attacks against cryptographic algorithms, testing all keys should be unfeasible. Enumerating all keys with higher probabilities than the actual key should also be unfeasible to guarantee security margins after an attacker using a certain equipment and number of traces. Key rank estimation algorithms are tools to compute these security margins.

We next consider rank estimation for attacks using a divide-and-conquer approach with independent chunks of the key, i.e. $\Pr[K = (k_1, k_2, \ldots, k_n)] = \Pr[K_1 = k_1] \times \Pr[K_2 = k_2] \times \ldots \times \Pr[K_n = k_n]$.

* Corresponding author
CNRS and Laboratoire Hubert Curien, Saint-Etienne, France
vincent.grosso@cnrs.fr

The first solution to this question was a space carving algorithm Veyrat-Charvillon et al (2013). They then compute the score of a key $k = (k_1, k_2, \ldots, k_n)$ and compare it to the score of the actual key $k^* = (k_1^*, k_2^*, \ldots, k_n^*)$. If $\text{rank}(k) \geq \text{rank}(k^*)$ then all the key $k' = (k_1', k_2', \ldots, k_n')$, such that $\Pr[K_1 = k_1'] \geq \Pr[K_1^* = k_1^*]$ and $\Pr[K_2 = k_2'] \geq \Pr[K_2^* = k_2^*]$ and $\ldots$ and $\Pr[K_n = k_n'] \geq \Pr[K_n^* = k_n^*]$ are also more probable than the actual key. We can then remove a hypercube from the search space. A similar argument can be done if the key evaluated has a lower probability than the actual key. The search space is then reduced, and we have upper and lower bounds on the key rank. The actual rank can be found in complexity smaller than the key enumeration. However, for large rank, the algorithm's time complexity does not allow finding the actual rank and an interval is given.

Methods achieving efficiently tight rank estimation were presented after the seminal work of Veyrat-Charvillon et al. (Martin et al 2015), (Poussier et al 2016), (Bernstein et al 2015). They all use quantization to group keys with close probabilities. In the end, these algorithms also output an interval for the rank that is generally tighter for the same computational time than the Veyrat-Charvillon et al. method. Tighter bounds can be obtained with finer quantization or by using some enumeration in the interval.

These algorithms can recover for each set of traces the rank of the key. The experiment is repeated several times to obtain probability on the security margins. Then security graph can be derived that allows estimating the trade-off between data and post-processing time to mount an attack with a given probability, as illustrated in Fig 1.

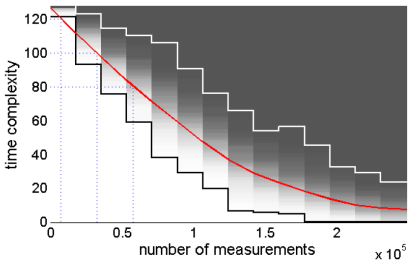

Fig. 1 Example of security graph.

Similar approaches try to evaluate security margins after a side-channel attack but without a key rank estimation algorithm. Indeed, these other approaches use metrics to evaluate the security margins (chunk success rate; chunk guessing entropy,...). They combine the metric result to derive security margin approximation. For example, Duc et al. (Duc et al 2019) and Ye et al. (Ye et al 2014) combine success rate, Choudary et al. Tanasescu et al (2021) use guessing entropy. to derive security margins. While these approaches allow deriving security margins efficiently, they cannot be used to compute the key rank of a single experiment. Actually, as pointed out by Rădulescu et al., the key rank estimation algorithms can be used to estimate the conditional guessing entropy, while other metric estimates (Massey) guessing entropy Radulescu et al (2022).

Application

Rank estimation tools are helpful for security evaluation and thus for evaluation lab.

Open problems and Future directions

Most of the rank estimation tools are designed for symmetric cryptography implementation. Thus they rely on two assumptions that made them efficient: a short master key and independent chunks of the master key. Application to side-channel attacks against asymmetric cryptography implementation may lead to loose bounds.

Cross-References

- Common Criteria
- Divide-and-conquer attack
- Differential–Linear Attack
- Rank estimation
- Side-Channel Attacks

References

Bernstein DJ, Lange T, van Vredendaal C (2015) Tighter, faster, simpler side-channel security evaluations beyond computing power. IACR Cryptol ePrint Arch p 221, URL http://eprint.iacr.org/2015/221

Duc A, Faust S, Standaert F (2019) Making masking security proofs concrete (or how to evaluate the security of any leaking device), extended version. J Cryptol 32(4):1263–1297, DOI 10.1007/s00145-018-9277-0, URL https://doi.org/10.1007/s00145-018-9277-0

Martin DP, O'Connell JF, Oswald E, Stam M (2015) Counting keys in parallel after a side channel attack. In: Iwata T, Cheon JH (eds) Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II, Springer, Lecture Notes in Computer Science, vol 9453, pp 313–337, DOI 10.1007/978-3-662-48800-3_13, URL https://doi.org/10.1007/978-3-662-48800-3_13

Poussier R, Standaert F, Grosso V (2016) Simple key enumeration (and rank estimation) using histograms: An integrated approach. In: Gierlichs B, Poschmann AY (eds) Cryptographic Hardware and Embedded Systems - CHES 2016 - 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings, Springer, Lecture Notes in Computer Science, vol 9813, pp 61–81, DOI 10.1007/978-3-662-53140-2_4, URL https://doi.org/10.1007/978-3-662-53140-2_4

Radulescu A, Popescu PG, Choudary MO (2022) GE vs GM: efficient side-channel security evaluations on full cryptographic keys. IACR Trans Cryptogr Hardw Embed Syst 2022(4):886–905, DOI 10.46586/tches.v2022.i4.886-905, URL https://doi.org/10.46586/tches.v2022.i4.886-905

Tanasescu A, Choudary MO, Rioul O, Popescu PG (2021) Tight and scalable side-channel attack evaluations through asymptotically optimal massey-like inequalities on guessing entropy. Entropy 23(11):1538, DOI 10.3390/e23111538, URL https://doi.org/10.3390/e23111538

Veyrat-Charvillon N, Gérard B, Standaert F (2013) Security evaluations beyond computing power. In: Johansson T, Nguyen PQ (eds) Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, Springer, Lecture Notes in Computer Science, vol 7881, pp 126–141, DOI 10.1007/978-3-642-38348-9_8,

URL https://doi.org/10.1007/978-3-642-38348-9_8

Ye X, Eisenbarth T, Martin W (2014) Bounded, yet sufficient? how to determine whether limited side channel information enables key recovery. In: Joye M, Moradi A (eds) Smart Card Research and Advanced Applications - 13th International Conference, CARDIS 2014, Paris, France, November 5-7, 2014. Revised Selected Papers, Springer, Lecture Notes in Computer Science, vol 8968, pp 215–232, DOI 10.1007/978-3-319-16763-3_13, URL https://doi.org/10.1007/978-3-319-16763-3_13