Key Enumeration

Vincent Grosso

Key Enumeration

Vincent Grosso *

Definitions

Key enumeration algorithms combine the results of different divide-and-conquer attacks to recover the master key. The key enumeration algorithms output the master key candidates that are more likely.

Background

The divide-and-conquer strategy aims to recover the master key by chunks (also called subkey). This is the "divide" part of the attack, which results in a table containing the probabilities for each subkey candidate to be the right guess, as illustrated in Table 1.

Guess	$\Pr[k_0]$	$\Pr[k_1]$	$\Pr[k_2]$	...	$\Pr[k_n]$
0	0.001	0.2	0.032	...	0.0001
1	0.05	0.02	0.002	...	0.002
2	0.01	0.002	0.002	...	0.003
...					
255	0.22	0.2	0.001	...	0.01

Table 1 Example of results after the divide part of a divide-and-conquer attack.

If, for all chunks, the most probable subkeys are correct, then retrieving the master key is trivial. It is more complicated when the master key chunk is not the most probable for at least one chunk. In that case, the master key candidate output by the attack is different from the actual master key. A key enumeration algorithm can be used in that case in order to exploit time and computational power to test more than one key. The second point of key enumeration algorithms is to exploit the non-uniform probability of each candidate.

A key enumeration algorithm outputs the master key candidate according to the probabilities obtained for each

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

chunk. The main issue with this approach is that merging all the result lists is unfeasible, which will lead to a list containing all the possible keys.

Meier and Staffelbach introduced the problem in (Meier and Staffelbach 1991), and the authors propose to draw key candidates randomly following the distribution computed in the divide part of the attack. Then Dichtl suggests using traces in the profiling step to determine an optimal search path (Dichtl 2011), but independent of the attack result. Hence, this solution is optimal on average-case. Veyrat-Charvillon et al. presented the first solution that is optimal for worst-case (Veyrat-Charvillon et al 2012). The Veyrat-Charvillon et al. solution will output the master key candidate from most probable to least probable for each attack. The idea is to sort each candidate list for each subkey and explore paths in high dimensions. Since the lists are sorted, the following key should be at the frontier of the set of keys already tested. The main drawback of this solution is the memory requirement and its sequential processing.

Several solutions have been proposed to solve the memory issue, but these solutions are not optimal anymore but near-optimal. The main idea is to use quantization to reduce the memory requirement. Poussier et al. (Poussier et al 2016) and Martin et al. (Martin et al 2018) quantize the probabilities to be able to compute an approximation of the probabilities of all master key candidates (allowing efficient rank estimation). They use backtracking to test the most probable master key candidates to obtain efficient key enumeration. By playing with the quantification precision parameter, the algorithms can be as near as possible to the optimal one, but with memory issues as Veyrat-Charvillon et al. solution. David and Wool (David and Wool 2017) quantize the candidates by grouping a small number of chunk candidates in a set (also called down-sampling) and then search inside the quantized set before moving to the next quantum set. Based on some assumptions about the distributions of key candidates, it is possible to show that this algorithm is near-optimal. Grouping candidates by sets of size 1, the algorithm is similar to (Veyrat-Charvillon et al 2012). All these solutions take advantage of down-sampling the search space. In (Martin et al 2017) martin et al. show how Grover's algorithm can help reduce key search time in quantum settings by exploiting side-channel advice.

Application

Key enumeration algorithms are generally used in the conquer part of a divide-and-conquer attack. They are primarily used in side-channel settings but can be applied in other contexts. As long as the divide part outputs probability for each chunk candidate and chunks are independent.

Open problems and Future directions

Key enumeration algorithms are useful tools to reduce the data complexity of an attack by exploiting some computational post-processing power. However, the algorithms presented so far are for independent chunks of the master key.

That means attacks that output divide but dependent result (as collision side-channel attacks) can barely take advantage of post-processing.

All presented algorithms take advantage of independent probabilities to have a straightforward ordering of different master key candidates. Combining and comparing the master key candidate scores by an attack, such as single-bit differential power analysis or correlation power analysis, is an open problem.

Cross-References

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

References

David L, Wool A (2017) A bounded-space near-optimal key enumeration algorithm for multi-subkey side-channel attacks. In: Handschuh H (ed) Topics in Cryptology - CT-RSA 2017 - The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14-17, 2017, Proceedings, Springer, Lecture Notes in Computer Science, vol 10159, pp 311–327, DOI 10.1007/978-3-319-52153-4_18, URL https://doi.org/10.1007/978-3-319-52153-4_18

Dichtl M (2011) A new method of black box power analysis and a fast algorithm for optimal key search. J Cryptogr Eng 1(4):255–264, DOI 10.1007/s13389-011-0019-6, URL https://doi.org/10.1007/s13389-011-0019-6

Martin DP, Montanaro A, Oswald E, Shepherd DJ (2017) Quantum key search with side channel advice. In: Adams C, Camenisch J (eds) Selected Areas in Cryptography - SAC 2017 - 24th International Conference, Ottawa, ON, Canada, August 16-18, 2017, Revised Selected Papers, Springer, Lecture Notes in Computer Science, vol 10719, pp 407–422, DOI 10.1007/978-3-319-72565-9_21, URL https://doi.org/10.1007/978-3-319-72565-9_21

Martin DP, Mather L, Oswald E (2018) Two sides of the same coin: Counting and enumerating keys post side-channel attacks revisited. In: Smart NP (ed) Topics in Cryptology - CT-RSA 2018 - The Cryptographers' Track at the RSA Conference 2018, San Francisco, CA, USA, April 16-20, 2018, Proceedings, Springer, Lecture Notes in Computer Science, vol 10808, pp 394–412, DOI 10.1007/978-3-319-76953-0_21, URL https://doi.org/10.1007/978-3-319-76953-0_21

Meier W, Staffelbach O (1991) Analysis of pseudo random sequence generated by cellular automata. In: Davies DW (ed) Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings, Springer, Lecture Notes in Computer Science, vol 547, pp 186–199, DOI 10.1007/3-540-46416-6_17, URL https://doi.org/10.1007/3-540-46416-6_17

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

Veyrat-Charvillon N, Gérard B, Renauld M, Standaert F (2012) An optimal key enumeration algorithm and its application to side-channel attacks. In: Knudsen LR, Wu H (eds) Selected Areas in Cryptography, 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers, Springer, Lecture Notes in Computer Science, vol 7707, pp 390–406, DOI 10.1007/978-3-642-35999-6_25,

URL https://doi.org/10.1007/978-3-642-35999-6_25