DENCRYPT

Opinion on Dynamic Encryption

Vincent Rijmen

May 22, 2017

Dynamic Encryption [1] is proposed by Knudsen as a method to strengthen the security of a cryptosystem against mathematical cryptanalysis. The core idea of the method is the following. The encryption function consists of a base cipher together with a dynamic encryption layer which is generated at random at the beginning of the encryption process.

Although at first sight the approach of Dynamic Encryption might violate Kerckhoffs' principle —which has to be satisfied by any modern cryptosystem—, this does not necessarily have to be the case. If each of the possible ciphers is secure by itself, and would remain secure even if its description would be known to the adversary, then Kerckhoffs' principle remains satisfied.

There are different ways to realise Dynamic Encryption in practice. The realisations proposed in [1, 2] all start from one base cipher or a small set of base ciphers. They cascade some ciphers in variable order, cascade one cipher with parts from other ciphers or with an extra layer with a definition that depends on the key, or they modify some components from a base cipher, e.g. the S-box of AES. All these realisations guarantee that the security of dynamic encryption against cryptanalysis is at least the security of the base cipher.

We conclude that the method of dynamic encryption is sound and secure according to the state of art in cryptology.

References

[1] Lars R. Knudsen. Dynamic Encryption. *Journal of Cyber Security, Vol. 3*, 357-370, 2015.

[2] Dencrypt. Dynamic Encryption Reference code.

Vincent Rijmen, professor at University of Leuven, Belgium, is the author of the Advanced Encryption Standard (AES), the world's de facto standard for strong encryption.