Efficient Format-preserving-encryption with 2-round Feistels

Lab.: LJK, Grenoble
Topic: Cryptography
Adviser: Pierre Karpman, Pierre.Karpman@univ-grenoble-alpes.fr

Context

A block cipher $\mathscr{E} : \mathscr{K} \times \mathscr{M} \to \mathscr{M}$ is a family of invertible mappings indexed by a key. That is, $\forall k \in \mathscr{K}, \mathscr{E}(k,\cdot) : \mathscr{M} \to \mathscr{M}$ is bijective. As digital information is represented and processed in binary, the most natural choice for $\mathscr{K}$ and $\mathscr{M}$ is to take them of the form $\{0,1\}^\kappa$ and $\{0,1\}^n$, i.e. binary strings of length κ and n, respectively. This is for instance the case of the ubiquitous AES block cipher, which has $\kappa \in \{128, 192, 256\}$ and $n = 128$.

Most of the time, a cipher such as the AES is all that is needed to encrypt the data at hand. Any binary file m can be padded to m' of length multiple of 128, on which AES (with a suitable mode of operation) is called. However, in some specific contexts, it may be the case that the original message is from a "special" domain, and one wishes to encrypt into exactly the same domain, and not an embedding into binary strings. For instance, this domain $\mathscr{M}$ could be taken to be the set of valid social security numbers (SSN), meaning that one wishes to encrypt a valid SSN into *again* a valid SSN. The term *format preserving encryption* (FPE) is usually used to denote schemes satisfying such conditions.

Objectives

A generic way to design an FPE scheme is to use a Feistel construction instantiated with a "usual" block cipher, for instance the AES. A recent NIST Special Publication introduces two such schemes, named FF1 and FF3 [NIS16]. The goal of this work is to study the potential usefulness of a closely related but nonetheless distinct approach, based on *All-Or-Nothing-Transforms* (AONT) [Riv97]. Roughly speaking, an AONT is a randomized public bijective mapping $\mathscr{T} : \mathscr{R} \times \mathscr{M} \to \mathscr{M}$ such that for any non-injective $\theta : \mathscr{M} \to \mathscr{M}$, $\theta \circ \mathscr{T}(r, x)$ does not a priori reveal anything about x. An AONT can be used to implement a mode of operation for long messages (say on $N \times 128$ bits) by 1) computing the transformed message $y := \mathscr{T}(x)$; 2) encrypting 128 bits of y with a conventional block cipher. This process was in particular described by Jakobsson & al. [JSY99] in 1999. The same year, Boyko showed that the OAEP padding scheme of Bellare and Rogaway is an AONT, for some proper formalization of the concept [Boy99]. OAEP uses a simple two-round Feistel structure, and can be instantiated for many domains.

The goal of this work is to study the potential of a "scramble-then-encrypt" approach to design an efficient FPE scheme. The idea is to observe that the OAEP Feistel structure is somewhat similar to the one of FF1 or FF3, but needs much fewer rounds as it does not need itself to provide confidentiality. One could thus hope to improve the performance over the state of the art by adopting such an hybrid approach. Note that because OAEP itself is expanding, it cannot be used directly in an FPE. It will thus be necessary to define an appropriate variant and to analyse its security.

Skills

A candidate should have a strong interest for research and good programming experience in C. Prior knowledge of cryptography is not necessary, but an interest for the field is.

References

[Boy99] Victor Boyko. On the Security Properties of OAEP as an All-or-Nothing Transform. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 503–518. Springer, 1999.

[JSY99] Markus Jakobsson, Julien P. Stern, and Moti Yung. Scramble All, Encrypt Small. In Lars R. Knudsen, editor, *Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings*, volume 1636 of *Lecture Notes in Computer Science*, pages 95–111. Springer, 1999.

[NIS16] NIST. Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38G, March 2016.

[Riv97] Ronald L. Rivest. All-or-Nothing Encryption and the Package Transform. In Eli Biham, editor, *Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings*, volume 1267 of *Lecture Notes in Computer Science*, pages 210–218. Springer, 1997.