Conception d'un chiffrement symétrique par blocs

Marion Videau

1 Introduction

La cryptographie se définit comme un ensemble de procédés visant à protéger une information contre toute forme d'utilisation malveillante par des tiers. Elle recouvre donc plusieurs fonctionnalités dont les principales sont le chiffrement et la signature. Cette présentation concerne la définition et les principaux critères de conception d'un algorithme de chiffrement symétrique.

Un algorithme de chiffrement transforme, grâce à une donnée secrète appelée *clé*, un message dit *texte clair* en un *texte chiffré* destiné à n'être lisible que du destinataire légitime. Pour ce faire, on dispose de deux grandes familles d'algorithmes, les algorithmes à clé secrète, dits aussi symétriques, et les algorithmes à clé publique, ou asymétriques. Les systèmes à clé secrète, les plus anciens, nécessitent le partage du secret entre les interlocuteurs. Les systèmes à clé publique datant de 1976 apportent une solution au partage de la clé. Le destinataire possède une clé dite *privée* connue de lui seul, lui permettant de lire tout message chiffré grâce à sa clé *publique*, connue de tous. Cependant, le problème de la gestion des clés se pose alors en d'autres termes et ces systèmes n'apportent pas une solution définitive dans la mesure où leur lenteur les rend inaptes au chiffrement en ligne. C'est pourquoi la plupart des applications utilisent des systèmes hybrides comprenant un chiffrement asymétrique pour l'échange de la clé secrète et un système symétrique pour le chiffrement des données.

2 Étude d'un algorithme de chiffrement

Hormis les contraintes de vitesse ou de mémoire qui pèsent sur un algorithme de chiffrement, le problème essentiel qui se pose est de pouvoir assurer un niveau de sécurité suffisant au système. Afin d'en évaluer la sécurité, on est amené à faire des hypothèses sur les conditions d'une éventuelle attaque visant à retrouver soit le message d'origine soit la clé de chiffrement. On doit en outre qualifier, voire quantifier, le contexte de l'attaque. On considère tout d'abord qu'on doit faire reposer la confidentialité d'un échange sur le seul secret de la clé. L'expérience prouve en effet qu'il est illusoire de compter sur le secret d'un algorithme qui se trouvera toujours être éventé à plus ou moins longue échéance. On pose donc comme principe qu'un attaquant a à sa disposition toutes les spécifications du système.

On définit en outre divers contextes d'attaques dont principalement celles à chiffré seul, à clair connu et à clair choisi, pour lesquelles l'attaquant dispose respectivement de quelques chiffrés ou de certains couples clairs-chiffrés, soit quelconques, soit correspondant à des clairs de son choix. Enfin, l'attaquant peut aussi tenter de retrouver la clé par *recherche exhaustive*, c'est-à-dire par énumération de l'ensemble des clés possibles pour le système. Si la clé est choisie aléatoirement parmi les mots de k bits, l'attaque nécessite en moyenne 2^{k-1} déchiffrements. Compte tenu de l'état actuel de la technologie, on recommande une taille de clé supérieure à 80 bits. En général, on quantifie la faisabilité d'une attaque par le nombre d'opérations de déchiffrement à effectuer. On considère que pour être sûr, un système ne doit pas permettre des attaques donc le coût est significativement inférieur à celui de la recherche exhaustive.

3 Le chiffrement itératif par blocs

On peut considérer un système de chiffrement *par blocs* comme une permutation d'un mot de n bits en un autre mot de n bits, la permutation étant indexée par une clé de k bits.

Il s'agit d'un système qui divise le texte clair en blocs de taille fixe (en général 64 ou 128 bits) puis les chiffre successivement avec la même clé. Le chiffré est ensuite obtenu par application d'un mode opératoire paliant la faiblesse d'une simple concaténation de blocs.

L'idée générale d'un chiffrement *itératif* est de réaliser un algorithme à partir d'unités élémentaires de chiffrement qui répétées un nombre suffisant de fois produiront un chiffrement cryptographiquement plus résistant qu'une unité isolée. Cette technique a été formalisée au début des années 70 par Horst Feistel. Les notions fondamentales utilisées sont tirées de l'article fondateur de Claude Shannon, *The communication theory of secrecy systems* [1], où sont traitées les bases mathématiques d'un système de communication chiffrée, à partir de la théorie de l'information. Ont été dégagées en particulier les notions de diffusion et de confusion.

La confusion permet de rendre inextricables les liens entre le message clair, la clé et le message chiffré. La diffusion assure la propagation de l'information contenue dans le texte clair et la clé dans tous les bits du texte chiffré.

Les itérations d'une unité élémentaire de chiffrement, ou fonction interne paramétrée par une sous-clé dérivée de la *clé maître*, permettent de répartir les permutations de manière satisfaisante parmi l'ensemble des permutations des mots de n bits afin que les liens entre le clair, le chiffré et la clé soient suffisamment inextricables.

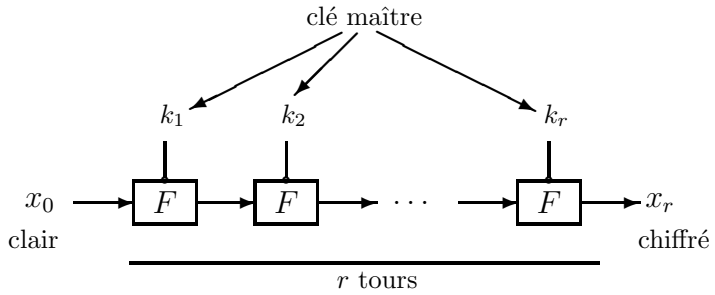

FIG. 21 – *Chiffrement itératif par blocs*

4 Détails de la fonction itérée

Les algorithmes itératifs par blocs se répartissent essentiellement en deux grandes familles suivant la structure de la fonction interne F : la structure de Feistel et la structure substitution-permutation. Elles s'illustrent dans les deux standards successifs de chiffrement à clé secrète : le DES choisi en 1977 et l'AES en 2000.

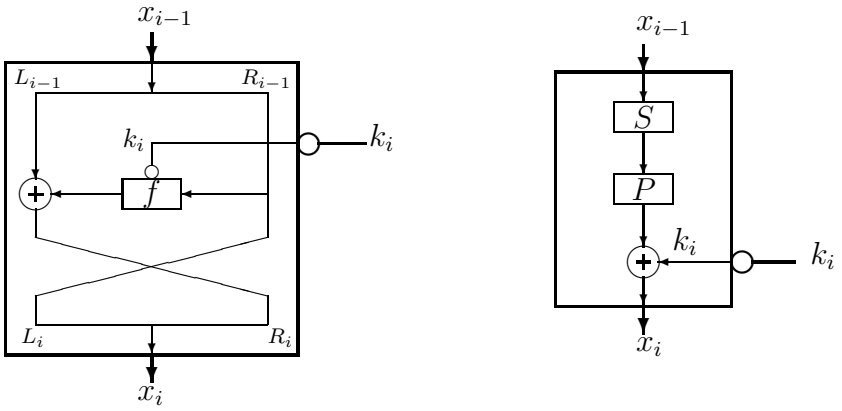

FIG. 22 – *Fonction itérée : à gauche d'un schéma de Feistel, à droite d'un réseau substitution-permutation*

Les chiffrements itératifs par blocs ne possèdent pas de théories mathématiques complètes permettant de se prononcer définitivement quant à leur sécurité. La fiabilité de tels systèmes se mesure d'abord en terme de résistance contre des cryptanalyses connues. L'effort essentiel de formalisation a porté sur les propriétés des fonctions F assurant la meilleure résistance aux deux principales attaques génériques : la cryptanalyse différentielle présentée par Biham et Shamir en 1991 [2] et la cryptanalyse linéaire due à Matsui en 1993 [3]. Les caractéristiques relevées ont conduit au concept de *sécurité démontrable* [4]. Les fonctions présentant des propriétés de résistance optimale contre ces deux types de cryptanalyses sont les fonctions *presque parfaitement non-linéaires* et les fonctions *presque-courbes*.

Ces fonctions sont alors dotées de structures algébriques fortes, exploitables dans d'autres attaques. Il est donc important de pouvoir énoncer de nouveaux critères de sécurité concernant les fonctions utilisées dans des chiffrements itératifs par blocs.

Références

[1] *Shannon (C.E.)* , Communication theory of secrecy systems. Bell System Technical Journal, **28** (1949), pp. 656-715.

[2] *Biham (E.) et Shamir (A.)*, Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, vol.4, **1** (1991), pp. 3-72.

[3] *Matsui (M.)*, Linear cryptanalysis method for DES cipher. Advances in Cryptology - EUROCRYPT'93, LNCS, **765**, pp. 386-397. Springer-Verlag, 1994.

[4] *Nyberg (K.) et Knudsen (L.R.)*, Provable security against differential cryptanalysis. Advances in Cryptology - CRYPTO'92, LNCS, **740**, pp. 566-574. Springer-Verlag, 1993.

Marion Videau
INRIA Projet CODES
Domaine de Voluceau, BP 105
78153 LE CHESNAY Cedex, FRANCE
`Marion.Videau@inria.fr`
http://www-rocq.inria.fr/codes/Marion.Videau/