34

Cryptanalyse différentielle du DES en 16 rounds

Adi Shamir
The Weizmann Institut of Science, Rehovot

[résumé par Abalo Baya]

DES (Data Encryption Standard) est sans doute le cryptosystème le plus connu et le plus utilisé dans un grand nombre de transactions civiles. Développé par IBM et adopté par NBS (National Bureau of Standards) dans les années 70, ce cryptosystème a résisté à toutes les attaques publiées jusqu'à présent. L'auteur développe ici une cryptanalyse différentielle des cryptosystèmes à n rounds en général et du DES en particulier.

1 Cryptosystèmes à n rounds

Un cryptosystème à n rounds est une fonction cryptographiquement forte basée sur n itérations d'une fonction cryptographiquement faible. Chaque itération est appelée *round* . La fonction itérée (fonction round) est fonction du résultat du round précédent et d'une sous-clé de la clé de codage. La fonction round est habituellement basée sur des S-boîtes, des permutations de bits, des opérations arithmétiques et de l'opération "ou exclusif" (notée par $\oplus$ ou XOR). Les S-boîtes sont des tables de transformation non-linéaire d'un petit segment de bits en un autre petit segment de bits. Les permutations de bits permettent de réarranger les sorties des S-boîtes de telle sorte que les entrées des S-boîtes d'un round proviennent des sorties d'un maximum de S-boîtes du round précédent. L'opération XOR sert à faire le brassage de la sous-clé et du message. Dans la plupart des applications, l'algorithme de codage est supposé connu alors que la clé de codage reste secrète.

Un exemple type de cryptosystème à n rounds ($n = 16$) est le DES. Chacune des clés du DES a 56 bits tandis que les messages en ont 64. La principale partie de la fonction round est une fonction F dont l'argument est un couple (m_1, K_s), où m_1 est une séquence de 32 bits et où K_s est une clé de 48 bits calculés à partir de la clé de codage. L'entrée m_1 de 32 bits est transformée (par un extenseur) en une séquence m_2 de 48 bits. On fait ensuite le XOR de K_s et de m_2. Le résultat de l'opération XOR est transformé par 8 S-boîtes en une séquence m_3 de 32 bits et la sortie de F est obtenue par permutation des bits de m_3. La spécification complète du DES est exposée dans [7].

2 Cryptanalyse différentielle du DES

Une littérature extensive sur le DES a été publiée depuis son adoption par le NBS en 1977. Mais aucune cryptanalyse faisant mieux qu'une recherche exhaustive sur 2^{55} clés (on dit que la complexité de l'attaque est de 2^{55}) n'a pu être réalisée. Ce manque de progrès sur l'amélioration de la complexité concernant la cryptanalyse du DES en 16 rounds a conduit beaucoup de chercheurs à analyser des versions simplifiées du DES et en particulier des versions du DES en moins de 16 rounds. Ainsi Chaum et Evertse [5] ont développé une attaque de complexité 2^{54} sur le DES en 6

rounds et ils ont démontré qu'une telle attaque ne pouvait pas être appliquée à un DES de plus de 7 rounds. Par ailleurs l'attaque de Davies [6], de complexité 2^{40} sur un DES en 8 rounds, est moins efficace sur un DES en 16 rounds qu'une simple recherche exhaustive. La première version [1] de la cryptanalyse différentielle est efficace sur un DES ne dépassant pas 15 rounds et la version actuelle [4] "casse" le DES en 16 rounds avec une complexité strictement inférieure à 2^{55}.

La cryptanalyse différentielle est une attaque avec choix de message en clair, l'outil essentiel de cette attaque étant le concept de "paires de messages encryptés" : une paire de messages encryptés est une paire résultant du codage de deux messages ayant une différence spécifique. Fondamentalement, la cryptanalyse différentielle est une méthode qui analyse *l'effet des différences* des paires de messages *sur les différences* des messages encryptés résultant. De telles différences sont utilisées pour attribuer des probabilités aux valeurs possibles des clés, ce qui permet de retenir uniquement les clés les plus probables. Pour la cryptanalyse du DES, la différence spécifique choisie est le XOR de deux messages en clair. En fait on génère un nombre suffisant de paires de messages en clair donnant lieu à des XOR intermédiaires spécifiés par une caractéristique convenablement choisie (voir [1] pour la définition de caractéristique). L'analyse partielle ou totale de ces messages en clair permet d'obtenir les clés les plus probables. Une recherche exhaustive sur ces clés conduit *presque toujours* à la clé secrète désirée. La table suivante résume les résultats obtenus. La dernière colonne de cette table reporte les complexités atteintes dans la première version [1] de la cryptanalyse différentielle.

Nb. de rounds	nb. de messages choisis	nb. de messages analysés	complexité de de l'analyse	complexité trouvée dans [1]
8	2^{14}	4	2^{9}	2^{16}
9	2^{24}	2	2^{32}	2^{26}
10	2^{24}	2^{14}	2^{14}	2^{15}
11	2^{31}	2	2^{32}	2^{36}
12	2^{31}	2^{21}	2^{21}	2^{43}
13	2^{39}	2	2^{32}	2^{44}
14	2^{39}	2^{29}	2^{51}	2^{51}
15	2^{47}	2^{7}	2^{37}	2^{52}
16	2^{47}	2^{36}	2^{37}	2^{58}

Table 1 : Résultats de la cryptanalyse différentielle du DES.

Références

[1] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991. The extended abstract appears in Advances in Cryptology, proceedings of CRYPTO 90.

[2] E. Biham and A. Shamir. Differential cryptanalysis of Feal and N-Hash. Technical report CS91-17, The Weizmann Institute of Science, 1991. The extended abstract appears in Advances in Cryptology, proceedings of CRYPTO 91.

[3] E. Biham and A. Shamir. Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer. Technical report CS91-18, The Weizmann Institute of Science, 1991. The extended abstract appears in Advances of Cryptology, proceedings of CRYPTO 91.

[4] E. Biham and A. Shamir. Differential cryptanalysis of the full 16-round DES. Preprint, December 1991.

[5] D. Chaum and J.-H. Evertse. Cryptanalysis of DES with a reduced number of rounds, Sequences of linear factors in block ciphers. In *Advances in Cryptology*, pages 192–211, 1985. Proceedings of CRYPTO 85.

[6] D. W. Davies. Private communication.

[7] National Bureau of Standards. Data encryption standard. *FIPS*, 46, January 1977. U. S. Department of Commerce.