Résumé

Dans Eurocrypt 1991, un cryptosystème HNSM basé sur l'itération d'une fonction chaotique est proposé. Il semble que sa linéarité et qu'une concentration des messages chiffrés aux bords de l'intervalle constituent des faiblesses. Une attaque est proposée par Biham, qui toutefois reste exponentielle. Ensuite dans Eurocode 1992, S. Harari et P.Liardet proposent le cryptosystème HARALIA basé sur une fonction non-linéaire, ayant de meilleures propriétés ergodiques et de répartition que HNSM.

Dans ce rapport, les deux systèmes sont placés dans un contexte plus général appelé H-système. Une étude approfondie des diverses propriétés mathématiques et informatiques de HARALIA est faite, et les paramètres exacts d'application sont étudiés. On propose de nombreuses attaques et améliorations. L'une de ces attaques est aussi efficace que celle de Biham. Un H-système peut-être amélioré pour éviter cette attaque. Malgré cela, une faiblesse particulière de HARALIA permet une toute autre attaque de même complexité. Cela donne un critère de sécurité pour tous les H-systèmes.

Abstract

In Eurocrypt 1991, a cryptosystem HNSM using iteration of chaotic maps is introduced. It's linearity and concentration at the edges of ciphertext space seems to be weak points. An attack is proposed by Biham, however remaining exponential. Then in Eurocode 1992, S.Harari and P.Liardet introduce a cryptosystem called HARALIA, based on non linear function which have better ergodic and distribution properties.

In this work two systems are regarded in more general framework of H-systems we introduce. Several close mathematical and computational properties and exact implementing conditions of HARALIA are regarded. Différent attacks and improvements are introduced. One attack is as good as Biham's one. An H-system can be improved to avoid this attack. Yet a particular weakness of HARALIA allow a différent attack of the same complexity. It gives a criterion for designing strongest H-systems.

1 Introduction.

Derrière tout problème, aussi abstrait soit-il, il y a une histoire...

C'est vers 465 avant Jésus-Christ, que la tekhnê rhétorike, ou l'art de la parole, voit le jour au plein centre de la Méditerranée, dans la capitale de la Grande Grèce, Syracuse. Elle est apparue dans un contexte où la démocratie, la nécessité de faire des preuves dans de nombreux procès, le besoin de convaincre, et de raisonner avait fait du verbe l'arme la plus redoutable qui soit. La faculté de langage, la communication, la parole et donc aussi le raisonnement, sera désormais l'art martial le plus noble de tous.

La rhétorique se trouvera vite défigurée par des Sophistes, et c'est à partir de là que Socrate part à la conquête de la vérité. La science occidentale est née.

De l'autre côté du globe et dans une autre époque, au 17-ème siècle, au Japon, le pays des samouraï, les shôgun Tokugawa imposent la paix pendant près de deux siècles, fait sans précédent dans l'histoire. C'est alors que, dans un immense fleurissement culturel et intellectuel les grands maîtres des arts martiaux traditionnels continuent à s'entraîner. Vite, on remarque que cette pratique prolonge la vie, calme les conflits et développe la personnalité permettant d'atteindre une efficacité réelle et non-violente dans la résolution des problèmes de la vie quelle que soit leur nature. Plus tard, ils se réuniront dans Butokukai (littéralement: l'art d'arrêter la lance) et ils fonderont l'art martial suprême, le Ju Jitsu Butokukai, synthèse hautement structurée et rationnelle de tous les arts martiaux existants. Une philosophie de haute valeur éthique et pratique y est associée.

Après la deuxième guerre mondiale la libre concurrence, la compétitivité et le besoin d'efficacité de la société moderne, ont achevé ce développement. Désormais la capacité d'agir, de combattre, de se défendre contre les agressions de toutes sortes, le courage et l'initiative font partie de la vie quotidienne, de notre langage, de notre civilisation.

Rien n'explique mieux le développement actuel de la cryptologie, que ces croisements et rapprochements qui se sont opérés au cours de l'histoire, entre d'une part la communication, la preuve, la science, et d'autre part la défense, l'art martial, l'efficacité.

Dans toute problématique de cryptologie on retrouve ces deux aspects. Dans la cryptanalyse on parle des attaques, qui sont des actions visant à enfreindre la sécurité du système, et il vaut mieux qu'elles soient connus de la science et des utilisateurs d'un système, plutôt que d'être découvertes plus tard et utilisées dans des buts peu honnêtes. La cryptographie sert à se défendre contre ses attaques, et atteindre en même temps un but précis de communication au sens large.

Ainsi, dans la cryptographie classique il est question de communiquer, sans être espionné. Dans l'authentification, on se défend contre les intrus qui pourraient altérer une communication. Dans la signature numérique il s'agit de prouver, ou plutôt de convaincre de son identité et de se défendre contre des imposteurs. Dans la problématique des preuves à divulgation nulle, il s'agit de prouver ou de convaincre de posséder une donnée sensible, et de ne donner à l'autre aucune chance de s'en emparer.

Bien d'autres problèmes semblables existent encore, et il y a autant de préoccupations pour les cryptologues que de façons d'être malhonnête, de violer l'intégrité des personnes, d'enfreindre la loi, ou simplement de tricher au jeu...

Depuis Socrate, la science a progressé à grand pas, et aujourd'hui avec le développement de l'informatique elle a fini par faire de la cryptographie, (jadis réservée aux militaires et diplomates), une nécessité quotidienne pour chacun de nous.

Le développement même de la science, peut-être vu comme un long processus de décryptage des lois de la nature. Il est fondé sur le fait que la réalité est plus complexe que les lois de la physique, et chacune d'elles laisse d'innombrables traces, et indices qui se répètent et qui finissent par se faire remarquer, non sans difficulté. La cryptanalyse et la créativité scientifique sont fondées sur la même capacité d'induction que nous avons tous. Pourtant dans la science occidentale on s'était concentré sur des événements **reproductibles** et répétitifs, en ignorant ceux qui ne le sont pas toujours. Par exemple la créativité, une communication, et même le fait de prouver quelque chose sont des expériences, qui ne se reproduisent jamais de la même façon.

En même temps, dans l'Orient une autre science qui prend en charge pré-

cisément ces événements non reproductibles existe depuis plus de 40 siècles. Cachée sous un langage poétique du Ying et du Yang, la science taoïste des changements nous offre une autre cryptanalyse de la nature. En effet, tout comme il est possible en cryptanalyse de déchiffrer un message sans connaître la clef secrète, il est également possible de prévoir le déroulement des événements dans tout système complexe sans connaître les lois précises qui le gouvernent.

Dans la cryptographie à clef secrète classique, on regarde habituellement les systèmes dont le codage est reproductible, tels que DES. Dans ce rapport on regardera uniquement des cryptosystèmes dont le codage n'est presque jamais **reproductible**, à cause du hasard introduit, et dont la sécurité est basée précisément sur ce non-déterminisme. La cryptographie probabiliste [BRA,STI] en est un exemple mais à clef publique. Dans ce rapport on va se restreindre à des cryptosystèmes non-déterministes à clef secrète.

Deux cryptosystèmes semblables s'affronteront ici.

Comme par hasard, le premier, le HARALIA avait été conçu précisément au bord de la Méditerranée, le deuxième, le HNSM au Japon.
Le système français était jusque là censé être plus fort que le japonais. Dans ce travail, nous montrons que ce n'est pas forcément le cas.

On n'a jamais été assez prudent en cryptographie.

Maintenant l'histoire va s'arrêter et les chiffres et des symboles mathématiques remplaceront les mots.

Par contre dans la partie qui suivra, je me permettrai d'interposer la plus stricte théorie et les intuitions qui lui donnent un sens, afin d'obtenir une vision originale de l'état actuel de fondements de la cryptographie, et placer le HARALIA dans ce contexte.

Une discussion de la notion d'entropie est faite dans le but de l'étendre à des phénomènes **non-reproductibles** et improbables.

Dans la partie 4, on étudiera un certain cadre commun qui est appelé H-système, puis on fera connaissance avec HARALIA et HNSM. On verra aussi l'attaque la plus rudimentaire.

Après, le HARALIA en particulier, mais aussi toutes les H-systèmes seront soumis à des rudes épreuves.

Dans la cinquième partie, une étude élémentaire, mais détaillée de propriétés de la fonction utilisée dans HARALIA sera faite. Dans la partie qui suivra, des propriétés beaucoup moins évidentes de cette fonction liées a l'uniformité et la répartition des messages chiffrés seront étudiées, et on commencera à en déduire des attaques.

La partie 7 est consacrée à un phénomène général qui apparaîtra dans tout les H-systèmes, la convergence, mais qui n'a pas joué le rôle espéré dans la cryptanalyse.

Dans la partie 8 une étude complexe et non triviale permet de donner des valeurs précises de paramètres d'utilisation de HARALIA, et également certaines mesures de divulgation de l'information et de redondance.

Tout le savoir des parties précédentes sera employé dans la partie 9, dans le but de cryptanalyse de HARALIA. On introduira un cadre général qui permet plusieurs attaques, en fonction des informations particulières sur la fonction du H-système donnée.

Une attaque, appelée l'attaque des extrémités, montrera que HARALIA peut être cassé avec la même complexité $\sqrt{2^n}$, que celle de l'attaque de Biham pour le HNSM, malheureusement toujours exponentielle.

Une amélioration applicable dans tous les H-systèmes sera proposée.

Malgré cela, le système HARALIA, même après cette amélioration, possède une certaine propriété de monotonicité en fonction de la clef qui permet de concevoir une autre attaque de même complexité. Le HNSM possède cette propriété, et il semble qu'on pourrait étendre l'attaque à HNSM et à d'autres cryptosystèmes qui la satisfont.

À ce jour, le HNSM paraît aussi fort que HARALIA, pour les attaques développés dans ce travail. Toutefois le HNSM reste très suspect à cause de ses autres faiblesses, dont la linéarité et une concentration de messages chiffrés autour de 1 et 0.

L'absence de cette propriété de monotonicité, évoquée plus haut, devra désormais être exigée de tout H-système.