Cryptologie : le projet NESSIE

Sélection des meilleures primitives cryptographiques, bilan et perspectives

Louis Granboulan

Le projet NESSIE, financé par l'Union européenne sous le numéro IST-1999-12324, avait pour objectif principal la sélection d'un portefeuille de primitives cryptographiques, à recommander aux industriels européens. Ce projet s'est terminé en avril 2003 et de nombreux enseignements peuvent être tirés de ses résultats.

Nous présentons plus en détail les objectifs, méthodes et résultats de NESSIE, puis nous décrirons les perspectives qu'on peut déduire de NESSIE, en particulier quant à l'état de l'art en cryptographie, et quant au long chemin qu'il reste à faire pour que la sécurité des systèmes d'information soit assurée avec une confiance élevée.

Sélectionner un portefeuille de primitives cryptographiques

Qu'est une primitive cryptographique ?

Définition

La cryptologie est une composante essentielle de la sécurité des systèmes d'information. C'est la science qui étudie les méthodes (mathématiques) permettant d'obtenir confidentialité, intégrité et authenticité. On distingue la cryptographie, qui est la conception de méthodes cryptologiques, et la

LCN, volume 4, n° 3-4/2003, pages 73 à 86

cryptanalyse, qui y recherche des failles. On distingue aussi les protocoles cryptographiques, où plusieurs interlocuteurs communiquent, et les primitives cryptographiques, qui sont les briques servant à construire les protocoles.

La cryptologie est déjà une science ancienne, utilisée depuis longtemps par les militaires et les diplomates, mais l'avènement de l'informatique en a révolutionné les fondements (Stern, 1998). De plus, l'invention de la cryptographie asymétrique (Diffie *et al.*, 1976) (Rivest *et al.*, 1978) permet d'étendre les domaines d'application de la cryptologie. Contrairement à la cryptographie symétrique qui suppose l'existence d'un secret partagé par les interlocuteurs, la cryptographie asymétrique permet d'obtenir confidentialité, intégrité et authenticité même en l'absence de toute convention secrète préalable.

Exemples : les primitives cryptographiques étudiées par NESSIE

– Chiffrement de flot. C'est une primitive symétrique pour la confidentialité, qui consiste principalement en la génération d'une suite de bits parfaitement aléatoire en apparence.

– Chiffrement par bloc. C'est une autre primitive symétrique pour la confidentialité, qui sert à chiffrer un message de taille fixe (le bloc).

– Fonction de hachage cryptographique. C'est une fonction en apparence injective, qui fabrique un condensé de taille fixe à partir d'un message quelconque.

– Authentification de message (MAC). C'est une primitive symétrique qui fabrique un condensé à partir d'un message et d'une clé secrète.

– Chiffrement asymétrique. Il s'agit ici de décrire un algorithme public permettant de chiffrer un message, tel que seul le détenteur de la clé secrète soit capable de le déchiffrer.

– Signature numérique. Il s'agit ici de décrire un algorithme public permettant de vérifier une signature d'un message, tel que seul le détenteur de la clé secrète soit capable d'avoir engendré une signature valide.

– Authentification. Il s'agit de prouver son identité en prouvant la connaissance d'un secret sans révéler aucune information sur ce secret.

La normalisation de primitives cryptographiques

Puisque les primitives cryptographiques servent de fondation à toutes les constructions cryptographiques, la sécurité des systèmes d'information repose donc de façon essentielle sur l'hypothèse que les primitives

cryptographiques utilisées apportent une sécurité suffisante. Mais l'analyse d'une primitive cryptographique dans le but d'en déterminer la sécurité est un travail d'une grande technicité. C'est pour cela qu'il est habituellement conseillé d'utiliser des primitives ayant été incluses dans une norme.

Le plus ancien exemple de primitive cryptographique normalisée est le chiffrement par bloc DEA (*Data Encryption Algorithm*) inclus dans le DES (*Data Encryption Standard*) qui a été publié par le gouvernement américain (NBS, 1977). Le gouvernement américain a ensuite publié la description de la fonction de hachage SHA (NIST, 1993) et de la signature DSA (NIST, 1994). Mais un gros défaut de ces normes est que leur évaluation n'a pas été faite de façon ouverte et publique. En particulier, les services secrets américains (NSA) ont participé à la conception de ces algorithmes, ce qui peut diminuer la confiance qu'on leur porte.

Conscient de ce problème, et aussi à cause des faiblesses du DES, le NIST a lancé en 1997 un appel à successeur pour le DES, qui a abouti en 2000 au choix de l'algorithme Rijndael pour être l'AES (NIST, 2001). L'évaluation des candidats AES a été faite de façon ouverte et publique, pour répondre aux critiques du DES, mais en même temps la conception des successeurs de SHA a été confiée à la NSA…

C'est donc à la fois pour ne pas dépendre de normes américaines et pour avoir accès à des algorithmes dont l'évaluation est publique que l'Europe et le Japon ont mis en route vers 1999 respectivement le projet NESSIE et le projet CRYPTREC. Aucun n'est à proprement parler un effort de normalisation, car l'un et l'autre ne font qu'émettre des recommandations. De plus, le projet NESSIE ayant une durée de vie limitée (il s'est terminé fin avril 2003), il n'est pas prévu de mise à jour de ses recommandations.

De nombreuses autres initiatives de normalisation de primitives cryptographiques existent. On peut mentionner les normes ISO 9796, ISO 9797, ISO 9798, ISO 10118, ISO 14888, ISO 15946, ANSI X9.19, ANSI X9.30, ANSI X9.31, ANSI X9.62, ANSI X9.71, FIPS 198, IEEE 1363.

Les spécificités de NESSIE

La principale particularité de NESSIE est la façon dont l'évaluation des primitives cryptographiques a été faite. Les membres du consortium NESSIE (cf. tableau 1) ont été choisis pour leurs compétences techniques. Un panel d'industriels (cf. tableau 2) a aidé le consortium à déterminer les besoins des principales industries utilisant des normes cryptographiques. En plus, l'ensemble des chercheurs en cryptographie et des industriels concernés a été régulièrement invité à contribuer à l'évaluation des primitives. Tous les

documents produits dans le cadre de l'évaluation faite par NESSIE ont été publiés sur la page web du projet, à l'exception évidemment des brouillons.

En comparaison, l'évaluation faite par le NIST pour la sélection de l'algorithme de l'AES reposait entièrement sur les participations volontaires de chercheurs extérieurs et sur le travail d'évaluation fait par la NSA, dont les conclusions ont été gardées secrètes.

Katholieke Universiteit Leuven	Belgique
Ecole Normale Supérieure	France
Royal Holloway, University of London	Royaume-Uni
Siemens AG	Allemagne
Technion – Israel Institute of Technology	Israël
Université Catholique de Louvain-la-Neuve	Belgique
Universitetet i Bergen	Norvège

Tableau 1. Membres du consortium NESSIE

La seconde particularité de NESSIE apparaît dans le choix des algorithmes devant être évalués. Ont été incluses toutes les catégories de primitives cryptographiques pour lesquelles un besoin industriel existait et pour lesquelles l'état de l'art était suffisamment étoffé pour envisager une recommandation valable une dizaine d'années. Un appel à soumissions a été publié, avec la possibilité de faire des modifications mineures à mi-parcours (fin 2001). Puisque NESSIE n'est pas l'émanation d'un gouvernement cherchant à sélectionner des algorithmes pour son usage (contrairement à CRYPTREC ou aux travaux du NIST), il n'y avait aucune obligation de sélectionner l'un des algorithmes soumis, si aucun ne respectait les critères de sécurité et de performances explicités dans l'appel à soumissions. Il se trouve qu'aucune primitive de chiffrement de flot n'a été sélectionnée.

Certaines catégories de primitives étudiées par NESSIE ont fait l'objet de subdivisions, correspondant principalement à des niveaux de sécurité différents. En particulier, une catégorie *chiffrement de blocs de 64 bits* a été incluse, bien que cette petite taille de blocs puisse être une faiblesse (ce qui est l'une des raisons pour lesquelles le successeur du DES – 64 bits – est l'AES – 128 bits). C'est la réponse à une demande de l'industrie, pour des raisons de compatibilité avec des produits contenant DES.

Algorithmic Research	Israël
Amtec SpA	Italie
Baltimore Tech.	Irlande
Cryptomathic	Danemark
Deutsche Telecom	Allemagne
Entrust Techn.	Suisse et Canada
Ericsson Radio Systems	Suède
Europay Intern.	Belgique
Gemplus	France
Hewlett-Packard Labs	Royaume-Uni
Isabel	Belgique
KPN Research	Pays-Bas
NDS	Israël
Nokia	Finlande
Oberthur	France
RSA Labs	Suède et Etats-Unis
Security Design Int.	Royaume-Uni
STMicroelectronics	France et Italie
S.W.I.F.T.	Belgique
Telenor Research	Norvège
Telsy Elettronica	Italie
Thalès	France
Thomson	France
Utimaco Safeware	Belgique et Allemagne
Vodaphone	Royaume-Uni
Zaxus	Royaume-Uni

Tableau 2. Panel d'industriels associés à NESSIE

Déroulement de NESSIE

Soumission des primitives

L'appel à soumissions a été publié en mars 2000, les soumissions devant être reçues avant septembre 2000. Ce délai assez court a permis que soient

soumises des primitives existantes, plus quelques-unes développées spécifiquement en fonction des critères de NESSIE. Les contraintes formelles du dossier de soumission étant légères, le consortium NESSIE a reçu une cinquantaine d'algorithmes à évaluer. Les graphiques ci-dessous montrent que les soumissions venaient du monde entier, et que les concepteurs des algorithmes étaient très majoritairement employés dans l'industrie. On peut en déduire que l'ensemble des primitives cryptographiques évaluées par NESSIE est représentatif de l'état de l'art du domaine.

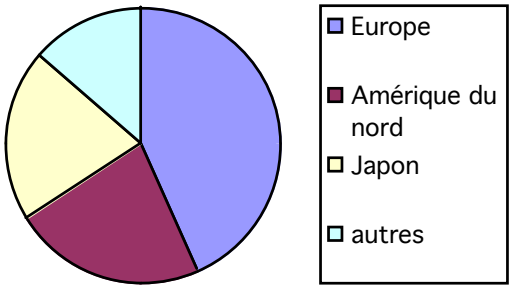

Figure 1. Origine géographique des soumissions à NESSIE

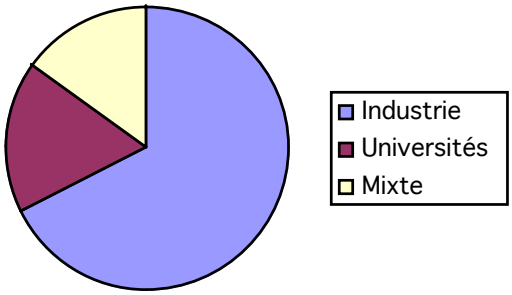

Figure 2. Statut des concepteurs des soumissions à NESSIE

Parmi les catégories de primitives demandées par NESSIE, deux n'ont pas reçu de soumission. Il s'agit des chiffrements de flot autosynchrones, et des familles de fonctions pseudo-aléatoires. La première catégorie

vraisemblablement parce que, malgré leur importance historique, les systèmes de chiffrement de flot autosynchrones n'ont pas suffisamment d'applications industrielles. La seconde catégorie vraisemblablement par manque de maturité de la recherche sous-jacente. Il était possible de préciser au moment de la soumission qu'une certaine primitive n'est prévue que pour certains environnements spécifiques. C'est en particulier le cas de la signature SFLASH, destinée aux cartes à puce à bas coût.

En novembre 2000, un colloque de présentation des soumissions à été organisé par NESSIE à Louvain. Outre la présentation des algorithmes par leurs inventeurs, les premiers résultats obtenus par le consortium NESSIE ont été exposés. En particulier, plusieurs soumissions (de chiffrements par bloc) avaient été déjà cassées.

Ce fait est très important, car il montre que malgré tout le savoir-faire acquis par la communauté cryptographique à l'occasion de la sélection d'AES (qui se terminait mi-2000), la conception de primitives cryptographiques reste difficile. Cela suffit à justifier l'évaluation publique d'algorithmes normalisés, par opposition à l'utilisation d'algorithmes secrets.

Première phase d'évaluation

La première phase d'évaluation s'est déroulée de septembre 2000 à juin 2001. Toutes les soumissions ont été étudiées du point de vue de la sécurité, des performances, de la flexibilité, et aussi des aspects liés à la propriété intellectuelle.

La composition du consortium NESSIE n'incluant pas de juriste spécialisé dans les questions de propriété intellectuelle, l'évaluation faite par NESSIE dans ce domaine s'est limitée à deux aspects : demander à la personne soumettant une primitive de s'engager à informer NESSIE et le public sur tous les éléments de propriété intellectuelle en rapport avec la soumission dont ils peuvent avoir connaissance ; afficher régulièrement de façon concise ces informations, et demander des commentaires. De plus, NESSIE a fait pression de façon informelle sur les personnes ayant soumis des algorithmes pour que celles-ci allègent le plus possible les contraintes d'utilisation liées à la propriété intellectuelle.

Du point de vue des performances et de la flexibilité, une étude théorique de chaque primitive a été menée, qui a permis une comparaison exhaustive, et qui a été publiée (NESSIE Deliverable D14). Ce document inclut aussi un recensement des implémentations existantes, principalement sur divers modèles de PC, cartes à puce ou FPGA. En outre, l'étude faite par NESSIE a

aussi isolé quelques erreurs de conception de certaines primitives de cryptographie asymétrique, qui en pénalisaient les performances, en particulier sur de longs messages.

Du point de vue de la sécurité, chaque primitive a été étudiée, et de nombreuses faiblesses ont été trouvées. Tous ces résultats ont été publiés (NESSIE Deliverable D13 et rapports). Diverses comparaisons entre les primitives d'une même catégorie ont été faites.

Le résultat de cette première phase d'évaluation a été présenté à un colloque organisé en septembre 2001 à Londres. Plus d'une vingtaine d'articles scientifiques concernant les primitives soumises à NESSIE y ont été exposés, dont les deux tiers écrits par des extérieurs à NESSIE. Avec plus d'une centaine de participants, dont de nombreux industriels, ce colloque a permis aux membres de NESSIE de valider l'approche du projet et de proposer une première sélection.

Seconde phase d'évaluation

Une première sélection a été présentée de façon informelle au colloque de Londres, et a servi de base de travail pour de nouvelles interactions avec les personnes ayant soumis les primitives. En effet, non seulement la moitié des primitives a été rejetée au terme de la première phase d'évaluation, à cause de failles dans leur sécurité ou d'une comparaison défavorable par rapport à d'autres primitives, mais la plupart des primitives retenues a fait l'objet d'une ou plusieurs améliorations (*tweaks*).

C'est en février 2002 qu'a été publiée par NESSIE la sélection des primitives étudiées pendant la seconde phase (NESSIE Deliverable D18). Les études commencées pendant la première phase ont été affinées, et publiées en novembre 2002 (NESSIE Deliverable D20 et NESSIE Deliverable D21), à l'occasion du troisième colloque NESSIE, à Munich.

La seconde phase d'évaluation s'est terminée au moment du quatrième colloque NESSIE, en février 2003 à Lund, où les versions finales des documents D20 et D21 ont été présentées, et où la composition du portfolio de primitives sélectionnées par NESSIE a été annoncée.

Sélection

Un grand soin a été donné par les membres du consortium à la justification de leurs décisions, afin de prouver l'exhaustivité et l'objectivité de leur travail d'évaluation. La composition du portfolio NESSIE reflète

assez fidèlement l'état de l'art en matière de primitives cryptographiques. En voici les détails.

– Quatre chiffrements par blocs ont été sélectionnés, deux d'entre eux pour une taille de bloc de 128 bits (Rijndael et Camellia), un pour 64 bits (Misty1) et un pour 256 bits (Shacal-2). Tous ces algorithmes sont utilisables gratuitement et librement, reposent sur des techniques cryptographiques éprouvées, et ont d'excellentes performances. Cela montre la maturité du domaine. Quelques bons algorithmes (IDEA et RC6) ont été rejetés à cause de problèmes de propriété intellectuelle.

– Aucun chiffrement de flot n'a été sélectionné. Bien que certaines soumissions résistent encore largement à toutes les attaques envisageables à moyen terme, aucune n'atteint le niveau de sécurité demandé par NESSIE.

– Quatre fonctions de hachage cryptographique ont été sélectionnées (Whirlpool, SHA-256, SHA-384 et SHA-512). Ce sont toutes les fonctions étudiées par NESSIE dans cette catégorie. Il est difficile de savoir si cela est dû à une grande maturité dans la conception de fonctions de hachage, ou à un manque de techniques de cryptanalyse. Néanmoins, on peut remarquer que toutes ces fonctions de hachage sont en fait des modes d'utilisation de chiffrement par blocs, et profitent donc du savoir-faire dans ce domaine.

– Quatre techniques d'authentification de message ont été sélectionnées (UMAC, TTMAC, EMAC et UMAC). Ce sont toutes les fonctions étudiées par NESSIE dans cette catégorie. Les mêmes réserves que pour la catégorie ci-dessus s'appliquent. A noter que UMAC a une preuve formelle de sécurité. De plus, ces quatre techniques ont des profils de performance très différents, et s'utilisent donc dans des contextes différents.

– Trois systèmes de chiffrement asymétriques ont été sélectionnés (PSEC-KEM, RSA-KEM et ACE-KEM). Chacun a une preuve formelle de sécurité. Certains ont de meilleures performances pour la taille minimale acceptable des paramètres de sécurité, mais les hypothèses relatives à leur sécurité sont difficilement comparables si on se place à performances égales. Tous utilisent la description KEM-DEM récemment proposée (Shoup, 2001).

– Trois systèmes de signature numérique ont été sélectionnés (RSA-PSS, ECDSA et SFLASH). Les deux premiers sont déjà classiques (quoique ce sont souvent d'autres variantes moins sûres de RSA qui sont utilisées), le troisième quant à lui est atypique, car SFLASH est destinée aux cartes à puce à bas coût. La faible marge de sécurité de cet algorithme fait que contrairement aux autres, il n'est pas recommandé si on cherche une sécurité à moyen terme (5 à 10 ans) mais uniquement si les contraintes d'implantation empêchent l'utilisation de l'un des autres.

– Le système d'identification soumis à NESSIE a été sélectionné (GPS). A part un défaut corrigé à mi-parcours, cette primitive à d'excellentes performances, et une bonne preuve formelle de sécurité.

– Contrairement aux cryptosystèmes symétriques, les cryptosystèmes asymétriques dépendent presque tous d'un paramètre particulier, ayant une influence majeure sur la sécurité et les performances (taille de module de factorisation secrète ou taille de la courbe elliptique par exemple). Les recommandations de NESSIE sur le sujet bénéficient de l'expérience des erreurs du passé, où cette « taille de clé » a souvent été choisie trop courte pour la durée de vie du produit. C'est pour cela que sont recommandés un minimum de 1536 bits pour la factorisation et 160 bits pour les courbes elliptiques.

Interactions avec d'autres efforts de normalisation

Au début de son existence, NESSIE a interagi avec le NIST en fournissant des commentaires destinés à aider au choix de l'AES. Plus tard, NESSIE a participé à l'étude de modes d'opération de chiffrements par bloc, et à l'étude des techniques d'authentification de messages. En revanche, le NIST n'a pas participé aux travaux de NESSIE.

L'interaction de NESSIE avec le groupe appointé par l'ISO pour normaliser les systèmes de chiffrement asymétriques a été très fructueuse. De même, l'interaction de NESSIE avec CRYPTREC a apporté beaucoup à chacun des deux.

Primitives cryptographiques : quel bilan déduire des résultats de NESSIE ?

Maturité, preuves et modèles

L'exemple des systèmes de chiffrement de flot montre que pour certaines primitives cryptographiques pourtant étudiées depuis longtemps la communauté des industriels et des chercheurs n'est pas capable de concevoir un algorithme respectant des critères de sécurités stricts définis à l'avance. Ceci est probablement dû à une prise de risque trop élevée, la sécurité étant sacrifiée pour obtenir d'excellentes performances, mais c'est aussi sûrement dû à des lacunes dans la théorie de la conception de tels systèmes.

Quant aux systèmes de chiffrement par blocs, la sélection d'AES puis les travaux de NESSIE ont montré qu'il existait des techniques permettant de

construire de bons systèmes, mais que même des cryptographes expérimentés faisaient couramment des erreurs (par exemple le défaut de la première version de KHAZAD et ANUBIS). De plus, l'absence de preuve formelle de sécurité reposant sur une hypothèse simple laisse ces systèmes à la merci de nouveaux types d'attaque (Courtois *et al.*, 2002 ; Murphy *et al.*, 2002).

Quant aux primitives de cryptographie asymétrique, l'expérience de NESSIE a montré qu'il n'était pas rare que les preuves de sécurité soient inexactes (Stern *et al.*, 2002 ; Granboulan, 2002), et la plupart des soumissions à NESSIE ont dû être modifiées afin d'en améliorer performances et flexibilité.

La flexibilité des primitives cryptographiques est un paramètre très important pour la sécurité, car si la primitive n'a pas été étudiée dans toute sa flexibilité, il est possible qu'une implantation ne respecte pas les spécifications et qu'une grosse faille de sécurité apparaisse (Mantin *et al.*, 2001).

On peut déduire des résultats de NESSIE que, parmi les catégories incluses dans l'appel à soumissions, un effort doit être fait par les chercheurs et les industriels pour définir des primitives sûres et efficaces dans les deux catégories : chiffrement de flot et génération de familles de fonctions pseudo-aléatoires. La première de ces deux catégories fait d'ailleurs l'objet de nombreux projets en cours de mise en route.

Autres primitives

Certaines catégories de primitives cryptographiques n'ont pas été étudiées par NESSIE. Pour la plupart d'entre elles, c'est parce qu'il s'agit de primitives appelées à être intégrées dans des protocoles cryptographiques plus complets, et la sécurité de la primitive peut difficilement être isolée du reste du protocole. C'est par exemple le cas des techniques d'échange de clé, qui font partie des primitives considérées par CRYPTREC, ou des preuves de connaissance à divulgation nulle.

Mais il existe des primitives dont les fonctionnalités pourraient trouver de nombreuses applications, et qui n'ont pas été étudiées par NESSIE. C'est en particulier le cas des systèmes asymétriques « basés sur l'identité » pour lesquels la clé privée est déduite de la clé publique par une autorité de confiance, et qui peuvent dans certains cas éviter le déploiement d'une infrastructure de clés publiques (PKI). Trop peu de candidats existent dans ce domaine pour qu'une comparaison permette de sélectionner les meilleurs.

Protocoles et modes d'utilisation

Un vaste champ de la cryptographie n'était pas couvert par NESSIE. Il s'agit de tout ce qui est protocoles cryptographiques et modes d'utilisation des primitives.

Les techniques d'étude de la sécurité des protocoles cryptographiques sont variées, et aucune n'est actuellement satisfaisante. Tandis que certains utilisent des « méthodes formelles » qui permettent une analyse semi-automatique des protocoles compliqués, au prix d'approximations où nichent parfois des failles de sécurité, d'autres font une analyse détaillée de protocoles simples, en risquant d'introduire des erreurs dans des démonstrations compliquées. Dans ce domaine, il reste encore beaucoup de théorie à inventer, et l'analyse des protocoles est encore de l'artisanat.

Quant aux modes d'utilisation des primitives, qui peuvent être vus comme des protocoles très simples, un certain savoir-faire existe, en particulier en ce qui concerne les modes d'opération des systèmes de chiffrement par bloc. Mais les groupes de travail organisés autour du NIST depuis fin 2000 pour mettre à jour la norme FIPS 81 montrent que sur ce sujet aussi, un consensus est difficile à obtenir (Joux, 2003 ; Bellare *et al.*, 2003).

Conclusion

La cryptologie, nécessaire à la sécurité des systèmes d'information, est un domaine où la recherche de ces dernières années a fait progresser l'état de l'art au point d'envisager la mise au point de normes, performantes, flexibles et sûres, pour que la cryptographie puisse être utilisée dans un grand nombre d'applications. Néanmoins, même en ce qui concerne les primitives *a priori* les plus faciles à normaliser, le grand âge du DES (utilisé dans les cartes bancaires), les faiblesses de A5/1 (chiffrement du GSM) ou la mauvaise utilisation de RC4 dans le Wi-Fi montrent qu'une coopération internationale et une évaluation publique faisant intervenir les chercheurs du domaine sont nécessaires. NESSIE est un exemple d'effort unissant universitaires et industriels pour trier le bon grain de l'ivraie.

Le portfolio de primitives cryptographiques sélectionnées par NESSIE est une première étape dans la sécurisation des systèmes. Néanmoins, non seulement les domaines non couverts par NESSIE n'ont pas la maturité suffisante pour pouvoir être normalisés, mais les travaux de NESSIE ont montré qu'un domaine apparemment ancien et bien étudié, celui des

chiffrements de flot, nécessite de nouvelles recherches avant de pouvoir être considéré comme mûr.

De plus, de nouvelles applications apparaissent (calcul distribué sur des serveurs *a priori* hostiles) ou mûrissent (vote électronique), qui demandent de nouvelles primitives cryptographiques et de nouveaux modèles de sécurité. Le travail accompli par les cryptologues est certes très avancé, mais il reste encore de nombreux problèmes à résoudre.

Bibliographie

Bellare M., Rogaway P., Wagner D., *EAX : A Conventional Authenticated-Encryption Mode*, 2003, http://eprint.iacr.org/2003/069/

Courtois N., Pierprzyk J., « Cryptanalysis of Block Cipher with Overdefined Systems of Equations », *Proceedings of Asiacrypt'02*, LNCS 2501, Springer, 2002, P. 267-287.

CRYPTREC (Evaluation of Cryptographic Techniques), http://www.ipa.go.jp/security/enc/CRYPTREC/

Diffie W., Hellman M., « New directions in cryptography », *IEEE transactions on Information Theory*, vol. IT-22, 1976, P. 644-654.

Granboulan L., « How to repair ESIGN », *Proceedings of SCN'02*, LNCS 2576, Springer, 2002.

Joux A., « Cryptanalysis of the EMD mode of operation », *Proceedings of Eurocrypt'03*, LNCS 2656, Springer, 2003, P. 1-16.

Mantin I., Shamir A., « A practical attack on broadcast RC4 », *Proceedings of FSE'01*, LNCS 2355, Springer, 2001, P. 152-164.

Murphy S., Robshaw M., « Essential algebraic structure within the AES », *Proceedings of Crypto'02*, LNCS 2442, Springer, 2002, P. 1-16.

NESSIE (New European Schemes for Signature, Integrity and Encryption), http://www.cryptonessie.org/

NESSIE Selection, http://www.cryptonessie.org/deliverables/decision-final.pdf

NESSIE Deliverables, http://www.cryptonessie.org/deliverables/

NESSIE Reports, http://www.cryptonessie.org/reports/

NESSIE Submissions, http://www.cryptonessie.org/workshop/submissions.html

NESSIE Tweaks, http://www.cryptonessie.org/tweaks.html

NBS (National Bureau of Standards), Data Encryption Standard (DES), FIPS 46, 1977.

NIST (National Institute of Standards and Technology), Secure Hash Standard (SHS), FIPS 180, 1993.

NIST (National Institute of Standards and Technology), Digital Signature Standard (DSS), FIPS 186, 1994.

NIST (National Institute of Standards and Technology), Advanced Encryption Standard (AES), FIPS 197, 2001.

NIST (National Institute of Standards and Technology), Modes of operation, http://csrc.nist.gov/encryption/modes/

Rivest R., Shamir A., Adleman L., « A Method for Obtaining Digital Signatures and Public-Key Cryptosystems », *Communications of the ACM*, vol. 21, n° 2, 1978, p. 120-126.

Shoup V., *A proposal for an ISO standard for public key encryption (version 2.0)*, 2001, http://eprint.iacr.org/2001/112/

Stern J., *La science du secret*, Paris, Editions Odile Jacob, 1998.

Stern J., Pointcheval D., Malone-Lee J., Smart N., « Flaws in applying proof methodologies to signature schemes », *Proceedings of Crypto'02*, LNCS 2442, Springer, 2002, p. 93-110.