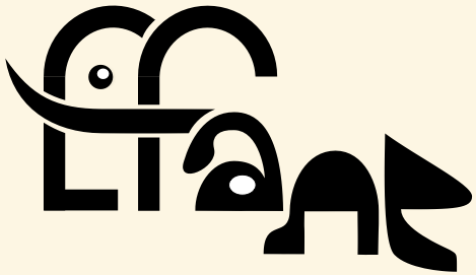
À quoi sert la cryptologie ? – Petit panorama des mathématiques de la cryptologie

2016/01/07 – Inria Bordeaux

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest



Cryptologie à clé publique

Cryptologie :

- Chiffrement ;
- Authenticité ;
- Intégrité.

La cryptologie à clé publique est basée sur une fonction à sens unique (avec trappe)
$\Rightarrow$ chiffrement asymétrique, signatures, preuves sans connaissances...

Applications :

- Militaires ;
- Vie privée ;
- Communications (internet, téléphones...)
- Commerce électronique...

Contexte Historique

- Riche histoire ; chiffrement de messages depuis l'antiquité au moins ;
- Principale application auparavant militaire ;
- Dorénavant la cryptologie joue un rôle essentiel pour garantir la sécurité des communications ;
- Cryptanalyse : déchiffrement d'Énigma par le groupe Ultra (Secret) à Blentchey Park lors de la seconde guerre mondiale ;
- À la fin de la guerre, vente des machines Énigma capturées par les alliés à d'autres pays.

Contexte actuel

- http ://en.wikipedia.org/wiki/PRISM_(surveillance_program) :
  « The Prism program collects stored Internet communications based on demands made to Internet companies» (Microsoft, Yahoo !, Google, Facebook, Paltalk, YouTube, AOL, Skype, Apple...)
- En sus de ce programme d'espionnage, utilisation de virus extrêmement sophistiqués, capables de s'infiltrer dans le firmware des disques durs : Stuxnet, Flame, Equation Group.
- Officiellement pour lutter contre le terrorisme ;
- Mais aussi utilisé pour l'espionnage économique :
  http ://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
- Les États-Unis ne sont pas les seuls à avoir des systèmes de surveillance...
  http ://www.theguardian.com/world/2013/jul/04/france-electronic-spying-operation-nsa

⇒ L'utilisation de la cryptographie est un enjeu de souveraineté nationale !

Quelle cryptographie ?

- Tout système ad-hoc, non basé sur des standards a été cassé (DECSS, GSM, WEP...)
- Utiliser un standard suffit-il ?

Standards :

- NIST workshop to standardize new elliptic curves ;
- IETF CFRG workgroup (Crypto Forum Research Group).

Quelle cryptographie ?

http ://blog.cryptographyengineering.com/2013/09/on-nsa.html

Matthew Green — « The NSA has been :

- Tampering with national standards (NIST is specifically mentioned) to promote weak, or otherwise vulnerable cryptography.
- Influencing standards committees to weaken protocols.
- Working with hardware and software vendors to weaken encryption and random number generators.
- Attacking the encryption used by “the next generation of 4G phones”.
- Obtaining cleartext access to “a major internet peer-to-peer voice and text communications system”
- Identifying and cracking vulnerable keys.
- Establishing a Human Intelligence division to infiltrate the global telecommunications industry.
- decrypting SSL connections.

»

Quelle cryptographie ?

- Tout système ad-hoc, non basé sur des standards a été cassé (DECSS, GSM, WEP...)
- Utiliser un standard suffit-il ?

Standards :

- NIST workshop to standardize new elliptic curves ;
- IETF CFRG workgroup (Crypto Forum Research Group).

⇒ On a besoin d'une cryptographie issue de la recherche publique, conduite par des experts universitaires, en lien avec le milieu économique local.

Protocoles cryptographiques

- Briques de base (primitives), s'appuyant sur des objets mathématiques
- Ces primitives sont combinées pour former des algorithmes/modes opératoires (algorithme de chiffrement, algorithme de signature)
- Ces modes opératoires sont combinés pour former des protocoles (protocole de session TLS, protocole de vote)
- Ces protocoles sont implémentés en logiciel ou matériel
- Puis ils sont utilisés.

Example : De RSA à un algorithme de chiffrement

- RSA permet de chiffrer un message m d'une certaine taille k : $m \longmapsto E(m)$;
- Comment chiffrer un message de longueur arbitraire ?
- Idée naturelle : découper m en messages $m_1 \| m_2 \ldots \| m_d$ de taille k, et poser $E(m) = E(m_1) \| E(m_2) \ldots \| E(m_d)$;
- Problème : RSA est malléable. $E(m \times m') = E(m) \times E(m')$.

$\Rightarrow$ A partir de plusieurs chiffrés on peut en produire plein d'autres ;

- La solution est de chiffrer les blocs m_i avec du padding : $E(m_i \oplus G(r) \| r \oplus H(m_i \oplus G(r))$ où r est aléatoire et H et G sont deux fonctions de hachage (on a une preuve de sécurité).

Example : De RSA à un algorithme de chiffrement

- RSA permet de chiffrer un message m d'une certaine taille k : $m \longmapsto E(m)$;
- Comment chiffrer un message de longueur arbitraire ?
- Idée naturelle : découper m en messages $m_1 \| m_2 \ldots \| m_d$ de taille k, et poser $E(m) = E(m_1) \| E(m_2) \ldots \| E(m_d)$;
- Problème : RSA est malléable. $E(m \times m') = E(m) \times E(m')$.

$\Rightarrow$ A partir de plusieurs chiffrés on peut en produire plein d'autres ;

- La solution est de chiffrer les blocs m_i avec du padding : $E(m_i \oplus G(r) \| r \oplus H(m_i \oplus G(r))$ où r est aléatoire et H et G sont deux fonctions de hachage (on a une preuve de sécurité).

Example : intégrité et chiffrement

- Comment combiner les deux briques de base que sont le chiffrement (Encrypt) et l'intégrité (MAC Message Authentification Code) ;
- Encrypt then MAC ?
- MAC then Encrypt ?
- Encrypt + Mac ?

Example : intégrité et chiffrement

- Comment combiner les deux briques de base que sont le chiffrement (Encrypt) et l'intégrité (MAC Message Authentification Code) ;
- Encrypt then MAC ?
- MAC then Encrypt ?
- Encrypt + Mac ?

Attaques

- Attaques sur les briques de base (très rare) ;
- Attaques sur l'empilement des briques en algorithmes ou protocoles ;
- Attaques sur l'implémentation ;
- Attaques sur l'exécution.

Sécurité

- Briques de base : repose sur des problèmes mathématiques bien identifiés et très étudiés (difficulté de la factorisation, logarithme discret dans les courbes elliptiques)
- Algorithmes et protocoles : si un attaquant peut attaquer le protocole (avec une certaine probabilité p en temps T), alors il peut attaquer une brique de base (avec une certaine probabilité p' en temps T')

Sécurité ?

- Erreur dans les preuves
- Preuves justes mais modèle incorrect
- Modèle correct mais utilisé dans un autre contexte
- Réductions de sécurités inefficaces
- Bug dans les programmes
- Attaques physiques (par canaux cachés) : mesure des impulsions électromagnétiques, du bruit, du temps de calcul, des cache miss

Attaques sur TLS

SSL (Secure Sockets Layer) / TLS (Transport Layer Security)

- Protocole : Renegociation attack / Version rollback attack
- BEAST (attack on Cipher Block Chaining)
- CRIME and BREACH (attack on compression)
- Downgrade attack : FREAK (export grade cryptography), Logjam (precomputation)
- Bugs : Heartbleed (buffer overflow), BERserk, goto fail
- Bogus certificates

Mitigating future loss of private keys : perfect foward secrecy via ephemeral Diffie-Hellman key exchange.

Sécurité !

Preuves formelles

- Des protocoles
- Des implémentations
- Des compilateurs (voir « Reflections on Trusting Trust» de Ken Thomson)
- Du matériel

Implémentation

- En temps constant ;
- Sans branches ;
- Faites par des experts (librairies opensource comme NaCl)

Ne jamais concevoir son propre système cryptographique ad hoc ou sa propre implémentation à moins d'être un expert.

Aléa

- Générer une clé nécessite de l'aléa de qualité
- Aléa matériel ou pseudo-aléa logiciel
- Modèle d'entropie et extracteur d'aléa
- Un aléa de faible qualité peut complètement compromettre un système. (Par exemple si l'aléa dans le système de chiffrement El-Gamal a ses premiers bits prédictables alors la système est cassé)
- Playstation (aléa constant), Clés ssh Debian (aléa = date)
- Instruction RDRAND : instruction Intel retournant un nombre aléatoire grâce à un générateur d'aléa matériel
- Theodore Ts'o : « I am so glad I resisted pressure from Intel engineers to let /dev/random rely only on the RDRAND instruction. To quote from the article below: 'By this year, the Sigint Enabling Project had found ways inside some of the encryption chips that scramble information for businesses and governments, either by working with chipmakers to insert back doors....' Relying solely on the hardware random number generator which is using an implementation sealed inside a chip which is impossible to audit is a BAD idea.»

Aléa

- Générer une clé nécessite de l'aléa de qualité
- Aléa matériel ou pseudo-aléa logiciel
- Modèle d'entropie et extracteur d'aléa
- Un aléa de faible qualité peut complètement compromettre un système. (Par exemple si l'aléa dans le système de chiffrement El-Gamal a ses premiers bits prédictables alors la système est cassé)
- Playstation (aléa constant), Clés ssh Debian (aléa = date)
- Instruction RDRAND : instruction Intel retournant un nombre aléatoire grâce à un générateur d'aléa matériel
- Theodore Ts'o : « I am so glad I resisted pressure from Intel engineers to let /dev/random rely only on the RDRAND instruction. To quote from the article below: 'By this year, the Sigint Enabling Project had found ways inside some of the encryption chips that scramble information for businesses and governments, either by working with chipmakers to insert back doors....' Relying solely on the hardware random number generator which is using an implementation sealed inside a chip which is impossible to audit is a BAD idea.»

Aléa

- Générer une clé nécessite de l'aléa de qualité
- Aléa matériel ou pseudo-aléa logiciel
- Modèle d'entropie et extracteur d'aléa
- Un aléa de faible qualité peut complètement compromettre un système. (Par exemple si l'aléa dans le système de chiffrement El-Gamal a ses premiers bits prédictables alors la système est cassé)
- Playstation (aléa constant), Clés ssh Debian (aléa = date)
- Instruction RDRAND : instruction Intel retournant un nombre aléatoire grâce à un générateur d'aléa matériel
- Theodore Ts'o : « I am so glad I resisted pressure from Intel engineers to let /dev/random rely only on the RDRAND instruction. To quote from the article below: 'By this year, the Sigint Enabling Project had found ways inside some of the encryption chips that scramble information for businesses and governments, either by working with chipmakers to insert back doors....' Relying solely on the hardware random number generator which is using an implementation sealed inside a chip which is impossible to audit is a BAD idea.»

Authentification

La cryptographie (à clé publique) permet de transformer un canal publique un canal authentifié et confidentiel, à partir d'un premier échange authentifié. Comment authentifier ce premier échange ?

- Certificats (TLS)
- Web of trust (GPG)
- Trust on first use (SSH)

Applications cryptographiques : Bitcoin

- Monnaie électronique décentralisée
- Fichier de transaction public (blockchain)
- Signature des transactions par une courbe elliptique
- La vérification de la blockchain (et validation des nouvelles transactions) fabrique de nouveaux bitcoins.

Applications cryptographiques : Vote électronique Belenios

- Confidentialité du vote (partage de secret)
- Résultats corrects (preuves Zero-Knowledge)
- Validation (et confidentialité) de la liste des électeurs

Résumé : importance de la cryptographie

- Chiffrement (pli confidentiel)
- Identification (badge cantine, carte à puce, empreinte digitale)
- Intégrité (clé RIB, scellés)
- Signature (ordre de virement) : identification, intégrité, non-répudiation
- Vie privée, anonymat, argent électronique, vote électronique, certificats, calcul distribué, stockage distribué

Applications : Développement des cartes à puces, commerce électronique, téléphonie mobile, armement, intérieur, sécurité des logiciels, sécurité des réseaux, objets interconnectés

Une opportunité pour les pays en développement

- Réseaux ;
- Objets interconnectés ;
- Puces RFID.

Résumé : importance de la formation en cryptographie

- La conception d'un cryptosystème et son implémentation doit être fait par un expert ;
- Utiliser les standards et les applications open-source mises à disposition par les experts universitaires ;
- Mais ne pas faire confiance aveugle à tous les standards ;
- Il faut des experts locaux pour faire un choix éclairé et le mieux adapté aux besoins spécifiques ;
- Seule la recherche Universitaire permet de rester à la pointe des dernières avancées scientifiques.