HAI906I : Introduction à la sécurité prouvée en cryptographie

Fabien Laguillaumie (fabien.laguillaumie@umontpellier.fr)

I.U.T
MONTPELLIER-SETE

Introduction

Cryptologie = science du secret et de la confiance

- Oded Goldreich (Weizmann Institute of Science) :

  « Cryptography is concerned with the construction of schemes that withstand any abuse : Such schemes are constructed so to maintain a desired functionality, even under malicious attempts aimed at making them deviate from their prescribed functionality. »

Introduction

Cryptologie = science du secret et de la confiance

Dans la vraie vie :

- Internet :
  - sites bancaires
  - sites de vente en ligne
  - site d'enchères
  - ...

Introduction

Dans la vraie vie :

- Carte à puce
  - cartes de paiements
  - carte vitale

Introduction

Dans la vraie vie :

- Signature électronique (`http://www.ssi.gouv.fr`)

La signature électronique permet, à l'aide d'un procédé cryptographique, de garantir l'intégrité du document signé et l'identité du signataire.

L'écrit électronique signé électroniquement peut être reconnu comme preuve en justice. L'ANSSI a publié un mémento visant à dresser le cadre juridique autour de la signature électronique. Partant d'un rappel sur le contexte législatif, il expose, au jour d'aujourd'hui, le cadre technique défini pour la mise en œuvre d'une signature électronique présumée fiable au sens du décret 2001-272 sur la signature électronique.

Pour l'ensemble du vocabulaire utilisé dans ce document il est conseillé de se référer à la FAQ « Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ».

Le procédé de signature électronique est présumé fiable, au sens du décret 2001-272 sur la signature électronique, si :

- la signature électronique est sécurisée ;
- elle est créée par un dispositif sécurisé de création de signature, c'est à dire par un dispositif certifié conforme aux exigences de l'article 3. I du décret conformément à la procédure de "Certification de conformité des dispositifs de création de signature électronique" ;
- et la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié. Les certificats délivrés par des "prestataires de services de certification électronique qualifiés" sont présumés qualifiés.

Introduction

Dans la vraie vie :

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Signature électronique
Point de situation

Memento

Version 0.94
25.08.04

I.U.T MONTPELLIER-SETE

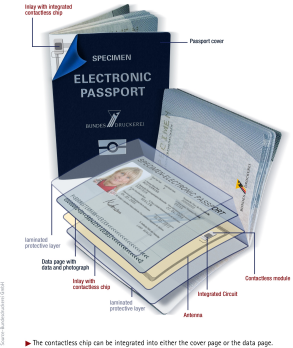
UNIVERSITÉ MONTPELLIER

Introduction

Cryptologie = science du secret et de la confiance

Dans la vraie vie :

- RFID (**R**adio-**F**requency **ID**entification)



Introduction

Cryptologie = science du secret et de la confiance

Dans la vraie vie :

I.U.T MONTPELLIER-SETE

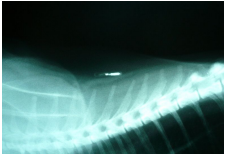
UNIVERSITÉ MONTPELLIER

Introduction

Cryptologie = science du secret et de la confiance

Dans la vraie vie :

- identification animale



- identification VIP

I.U.T MONTPELLIER-SETE

UNIVERSITÉ MONTPELLIER

Introduction

Cryptologie = science du secret et de la confiance

Dans la vraie vie :

Introduction

Cryptologie = science du secret et de la confiance

Dans la vraie vie :

Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars

Aurélien Francillon, Boris Danev, Srdjan Čapkun
Department of Computer Science
ETH Zurich
8092 Zurich, Switzerland
{aurelien.francillon, boris.danev, srdjan.capkun}@inf.ethz.ch

I.U.T MONTPELLIER-SETE

UNIVERSITÉ MONTPELLIER

Introduction

Dans la vraie vie :

- Télé payante
  - décodeur
  - pay-tv

Introduction

Dans la vraie vie :

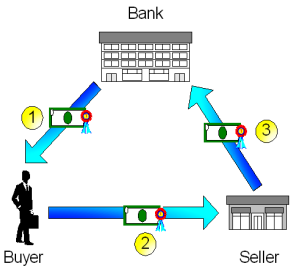
- Télécommunications
  - GSM
  - Wifi

- Hybrid fixed/mobile phone enabling communications both over fixed (PSTN, ISDN, VoIP) and mobile (Quadri-Band GSM, GPRS Class 10, EDGE, UMTS) telecom networks
- Vocoders ensuring secure and high-quality speech : STANAG 4591 (2.4 kbps) and G.728 (16 kbps)
- Security level : High Grade (up to French « SECRET DÉFENSE »)

Introduction

Dans la vraie vie :

- Paiement
  - porte-monnaie électronique
  - cryptocurrency
  - e-cash



Introduction

Récemment :

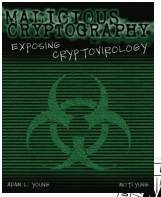
Affaire Snowden : comment la NSA déjoue le chiffrement des communications

Le Monde.fr | 05.09.2013 à 23h28 • Mis à jour le 06.09.2013 à 19h14

Abonnez-vous à partir de 1 € | Réagir | Classer | Partager

Recommander | Envoyer | 1 695 personnes le recommandent.

Les désormais célèbres documents d'Edward Snowden, l'ancien consultant de l'Agence de sécurité nationale (NSA), viennent d'éclaircir une facette encore



I.U.T MONTPELLIER-SETE

MONTPELLIER

Introduction

SEARCH

The New York Times

EDITORIAL
Leaving the E.U. Would Hurt Britain's Economy

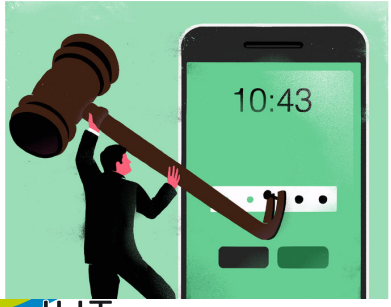
CHARLES M. BLOW
The End of American Idealism

PAUL KRUGMAN
When Fallacies Collide

The Opinion Pages | OP-ED CONTRIBUTORS

When Phone Encryption Blocks Justice

By CYRUS R. VANCE Jr., FRANÇOIS MOLINS, ADRIAN LEPPARD and JAVIER ZARAGOZA AUG. 11, 2015



François Molins: "Les nouveaux téléphones rendent la justice aveugle"

Actualité | Société | Propos recueillis par Emmanuel Paquette et Eric Pelletier, publié le 02/09/2015 à 08:57

521 partages | Partager | Tweeter | Partager | 2 réactions

LIBÉRATION

TRIBUNE

Sécurité informatique : tous connectés, tous responsables

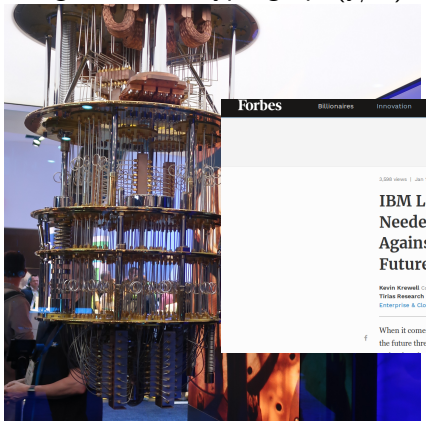
Par Guillaume Poupard, Directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) — 21 janvier 2019 à 08:19 (mis à jour le 22 janvier 2019 à 12:31)

PARTAGER | TWEETER

I.U.T MONTPELLIER-SETE

Introduction

Google News : cryptograph(y/ie)



Forbes Billionaires Innovation Leadership Money Consumer Industry

IBM Lattice Cryptography Is Needed Now To Defend Against Quantum Computing Future

Kevin Krewell, Contributor
Tirias Research, Contributor Group
Enterprise & Cloud

When it comes to securing data, it is not too early to start anticipating the future threat of quantum computing. Today's cryptographic

CYBERSÉCURITÉ

Protection des données : débattre pour résoudre la «crise de confiance»

Par Amaelle Guiton — 30 janvier 2018 à 11:40

PARTAGER TWEETER

9TO5Mac

IT NETWORK Dark Reading Network Computing About Us Adver

DARKReading Join us live at Interop

Authors Slideshows Video Tech Library University Radio Calendar Black Hat News

ANALYTICS ATTACKS / BREACHES APP SEC CAREERS & PEOPLE CLOUD ENDPOINT IoT MOBILE OPERATIONS

ATTACKS/BREACHES

1/22/2019 02:30 PM

The Fact and Fiction of Homomorphic Encryption

The approach's promise continues to entice cryptographers and academics. But don't expect it to help in the real world anytime soon.

Ameesh Divatia Commentary

Connect Directly

The history of homomorphic encryption stretches back to the late 1970s. Just a year after the RSA public-key scheme was developed, Ron Rivest, Len Adleman, and Michael Dertouzos published a report called "On Data Banks and Privacy Homomorphisms." The paper detailed how a loan company, for example, could use a cloud provider (then known as a commercial time-

I.U.T MONTPELLIER-SETE

Introduction

Le cœur de la crypto :

- échange de clés
- sécurité des communications (confidentialité, intégrité)

Introduction

Le cœur de la crypto :

- échange de clés
- sécurité des communications (confidentialité, intégrité)

mais encore

- signatures numériques
- communications anonymes
- protocoles : vote, e-cash, enchères, interrogation anonyme de BD

Introduction

Le cœur de la crypto :

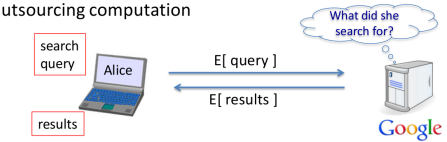
- échange de clés
- sécurité des communications (confidentialité, intégrité)

mais encore

- signatures numériques
- communications anonymes
- protocoles : vote, e-cash, enchères, interrogation anonyme de BD

et la magie :

- preuves à divulgation nulle de connaissance
- multi-party computation (thm : c'est possible !)
- calculs secrets délégués



I.U.T MONTPELLIER-SETE

Multiparty computation

- Alice et Bob ont eu un premier rendez-vous
- Ils veulent savoir s'il y en aura un second

  mais...

  ils ne veulent pas se prendre une veste en direct !

- Ils vont jouer à un jeu à l'issue duquel, la seule information connue sera la possibilité d'un second rendez-vous ou pas.

I.U.T MONTPELLIER-SETE

UNIVERSITÉ MONTPELLIER

Multiparty computation

- Alice et Bob ont eu un premier rendez-vous
- Ils veulent savoir s'il y en aura un second

mais...

ils ne veulent pas se prendre une veste en direct !

- Ils vont jouer à un jeu à l'issue duquel, la seule information connue sera la possibilité d'un second rendez-vous ou pas.

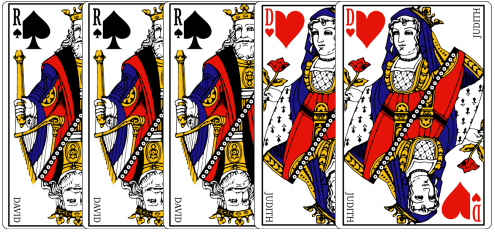
Après le premier rendez-vous :

- Alice sait si elle veut un second rendez-vous
- Bob sait si il veut un second rendez-vous
- et c'est tout !

IUT MONTPELLIER-SÈTE

UNIVERSITÉ MONTPELLIER

Multiparty computation



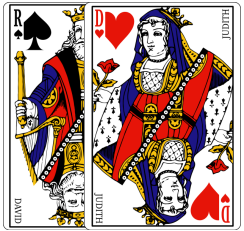
I.U.T
MONTPELLIER-SETE

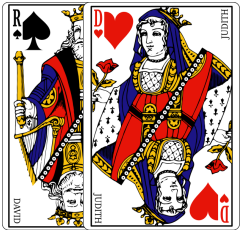
UNIVERSITÉ MONTPELLIER

Multiparty computation

Dans ce jeu :

- Un **roi** de ♠ est face cachée sur la table
- Alice et Bob reçoivent un **roi** et une **reine**
- Bob pose ses cartes face cachée par dessus le **roi** de ♠
  - si il veut un second rendez-vous : **reine** au dessus
- Alice pose ses cartes face cachée sur le dessus du paquet
  - si elle veut un second rendez-vous : **roi** sur le dessus

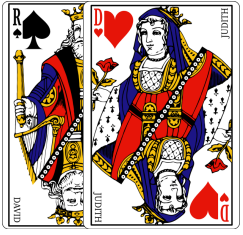




Multiparty computation

Dans ce jeu :

- Un **roi** de ♠ est face cachée sur la table
- Alice et Bob reçoivent un **roi** et une **reine**
- Bob pose ses cartes face cachée par dessus le **roi** de ♠
  - si il veut un second rendez-vous : **reine** au dessus
- Alice pose ses cartes face cachée sur le dessus du paquet
  - si elle veut un second rendez-vous : **roi** sur le dessus



Multiparty computation

Dans ce jeu :

- Un **roi** de ♠ est face cachée sur la table
- Alice et Bob reçoivent un **roi** et une **reine**
- Bob pose ses cartes face cachée par dessus le **roi** de ♠
  - si il veut un second rendez-vous : **reine** au dessus
- Alice pose ses cartes face cachée sur le dessus du paquet
  - si elle veut un second rendez-vous : **roi** sur le dessus

MONTPELLIER-SETE

Multiparty computation

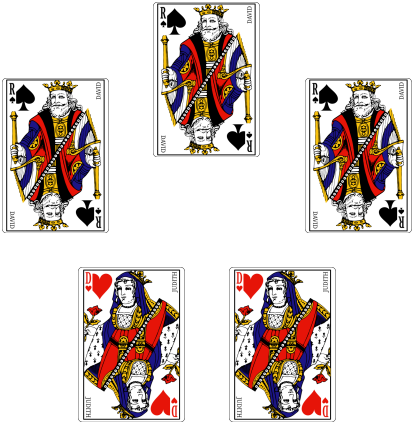
Dans ce jeu :

- Un **roi** de ♠ est face cachée sur la table
- Alice et Bob reçoivent un **roi** et une **reine**
- Bob pose ses cartes face cachée par dessus le **roi** de ♠
  - si il veut un second rendez-vous : **reine** au dessus
- Alice pose ses cartes face cachée sur le dessus du paquet
  - si elle veut un second rendez-vous : **roi** sur le dessus

- Alice et Bob coupent

Multiparty computation

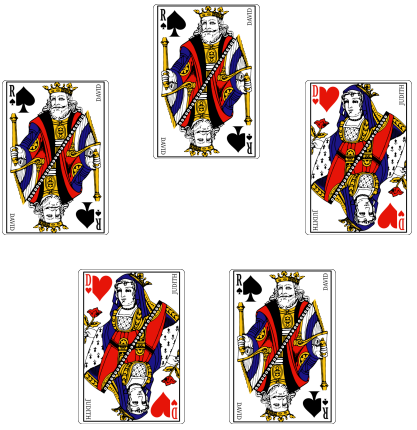
- Si les reines sont côte à côte : Alice et Bob sont amoureux !



Multiparty computation

- Si les reines sont côte à côte : Alice et Bob sont amoureux !
- Sinon :

  Rien n'est révélé si les reines ne sont pas côte à côte

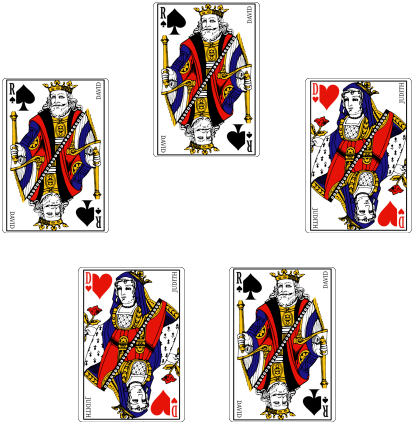


Multiparty computation

- Si les reines sont côte à côte : Alice et Bob sont amoureux !
- Sinon :

  Rien n'est révelé si les reines ne sont pas côte à côte

  i.e., on ne sait pas si seul l'un des deux n'aime pas l'autre, ou aucun ne s'aiment



I.U.T MONTPELLIER-SETE

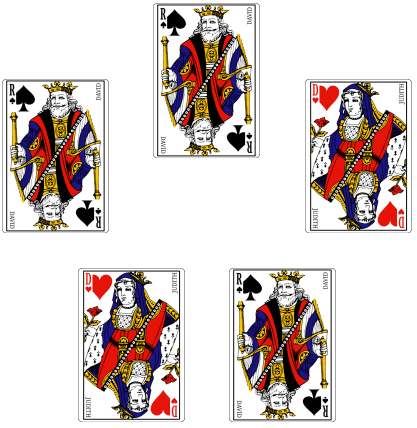
UNIVERSITÉ MONTPELLIER

Multiparty computation

- Si les reines sont côte à côte : Alice et Bob sont amoureux !
- Sinon :

  Rien n'est révélé si les reines ne sont pas côte à côte

  i.e., on ne sait pas si seul l'un des deux n'aime pas l'autre, ou aucun ne s'aiment
- fonction "**et**"



I.U.T MONTPELLIER-SETE

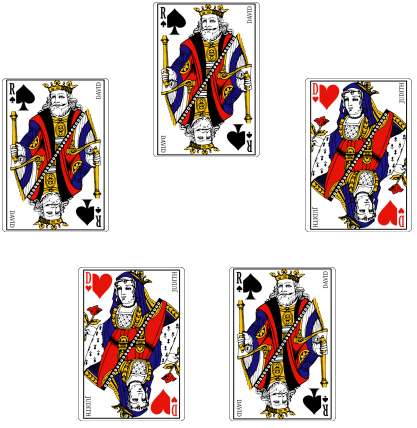
UNIVERSITÉ MONTPELLIER

Multiparty computation

- Si les reines sont côte à côte : Alice et Bob sont amoureux !
- Sinon :

  Rien n'est révélé si les reines ne sont pas côte à côte

  i.e., on ne sait pas si seul l'un des deux n'aime pas l'autre, ou aucun ne s'aiment



- fonction "**et**"

Multiparty computation : calcule une fonction de sorte à ce qu'une entrée secrète ne soit pas révélée aux autres parties

(**attention :** de l'information peut se déduire du résultat de la fonction)

Introduction

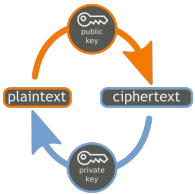
- Cryptographie = conception de protocoles sûrs

  confidentialité - authenticité - integrité

- Cryptographie à clé publique :

  - Concept : Diffie & Hellman '76

  - Le secret est secret
    $\rightsquigarrow$ une information publique est nécessaire



$$sk \longleftrightarrow pk$$

  - Premières réalisations :
    - RSA '78 — factorisation
    - McEliece'78 — décodage de codes correcteurs d'erreurs
    - Elgamal '84 — logarithme discret dans $(\mathbb{F}_q)$
    - Koblitz / Miller '85 — logarithme discret sur des courbes elliptiques

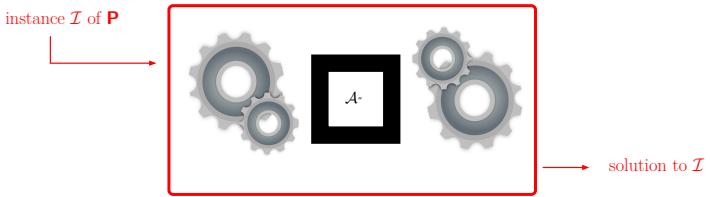
I.U.T MONTPELLIER-SETE

Introduction

Que signifie « sûrs » ? dépend de l'application

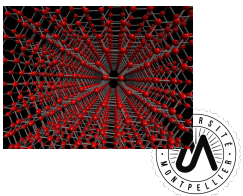
- $\rightsquigarrow$ *modèle de sécurité* d'une primitive cryptographique
- $\rightsquigarrow$ *preuve* de sa sécurité (insécurité ?)

prouver = réduire un problème difficile **P** à une attaque contre le schéma ″



- Exhiber des problèmes "difficiles" :
  - problèmes NP difficiles (*e. g.*, euclidean lattices)
  - problèmes arithmétiques : logarithme discret, factorisation

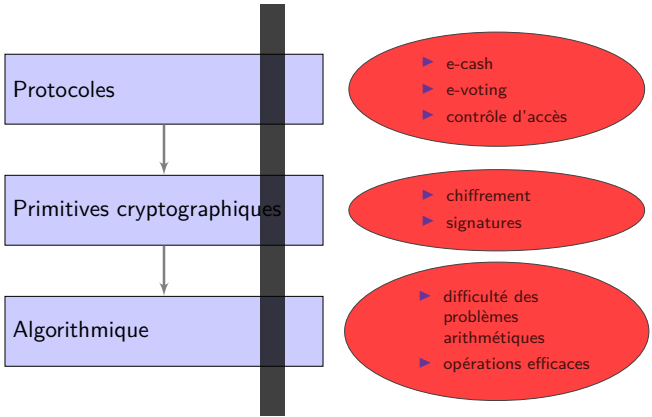
$N = p \times q$



I.U.T MONTPELLIER-SETE

Introduction

Cryptographie à clé publique :

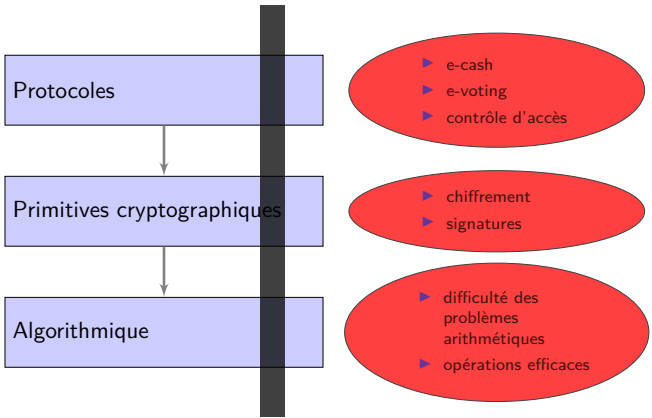


I.U.T MONTPELLIER-SETE

UNIVERSITÉ MONTPELLIER

Introduction

Cryptographie à clé publique :



Introduction

Cryptologie :

- Cryptographie :
  - conception de systèmes cryptographiques
  - étude (preuve) de leur sécurité
  - amélioration des performances

- Cryptanalyse :
  - mise en défaut des systèmes cryptographiques
  - attaque des problèmes algorithmiques sous-jacents
  - observation des “canaux auxiliaires”

Introduction

Objectifs :

- confidentialité : garantir que le contenu d'une communication (ou d'un fichier) n'est pas accessible à tout autre personne que le destinataire légitime
- authenticité : s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication (ou d'un fichier)
- intégrité : s'assurer que le contenu d'une communication (ou d'un fichier) n'a pas été modifié de façon malveillante

Introduction

Objectifs :

- confidentialité : garantir que le contenu d'une communication (ou d'un fichier) n'est pas accessible à tout autre personne que le destinataire légitime

  $\rightsquigarrow$ chiffrement

- authenticité : s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication (ou d'un fichier)

- intégrité : s'assurer que le contenu d'une communication (ou d'un fichier) n'a pas été modifié de façon malveillante

Introduction

Objectifs :

- confidentialité : garantir que le contenu d'une communication (ou d'un fichier) n'est pas accessible à tout autre personne que le destinataire légitime

  $\rightsquigarrow$ chiffrement

- authenticité : s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication (ou d'un fichier)

  $\rightsquigarrow$ identification/signature

- intégrité : s'assurer que le contenu d'une communication (ou d'un fichier) n'a pas été modifié de façon malveillante

Introduction

Objectifs :

- confidentialité : garantir que le contenu d'une communication (ou d'un fichier) n'est pas accessible à tout autre personne que le destinataire légitime

  $\rightsquigarrow$ chiffrement

- authenticité : s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication (ou d'un fichier)

  $\rightsquigarrow$ identification/signature

- intégrité : s'assurer que le contenu d'une communication (ou d'un fichier) n'a pas été modifié de façon malveillante

  $\rightsquigarrow$ hachage/signature

Introduction

Cyptographie à clé publique

on ne s'échange plus de clé : on la publie !

$\rightsquigarrow$ chaque utilisateur possède un couple

$$(sk, pk)$$

où pk est publique et sk est gardée secrète

$$sk \ \mathcal{R} \ pk$$

il est "*difficile*" de retrouver sk à partir de pk.

New Directions in Cryptography. W. Diffie and M. E. Hellman, IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp 644–654.

Sécurité prouvée

- Pour se convaincre de la sécurité d'un schéma :
  - exhiber une attaque : le système est prouvée non-sûr
    $\rightsquigarrow$ si on n'en trouve pas ?
  - Système de Chor et Rivest [1] : attaque [2] définitive après 10 ans de vie

- *Prouver* la sécurité du schéma

- Preuve *réductionniste* (théorie de la complexité) dans le "modèle standard"

- Une preuve fournit une réduction entre la résolution d'un problème difficile et une attaque contre le protocole

1. *A knapsack-type public-key cryptosystem based on arithmetic in finite fields*. B. Chor and R.L. Rivest, IEEE IT, 34(5) : 901–909 (1988)
2. *Cryptanalysis of the Chor-Rivest cryptosystem*. S. Vaudenay, Proc. of Crypto'98, Springer LNCS Vol. 1462, 243–256 (1998)

IUT MONTPELLIER-SETE

UNIVERSITE MONTPELLIER

Sécurité Prouvée

- Sécurité prouvée
  - Défintion d'un modèle de sécurité
  - Réduction (polynomiale) à une hypothèse minimale (ex. fonction à sens unique)
    $\rightsquigarrow$ résultats théoriques

> La sécurité prouvée garantit qu'un protocole est asymptotiquement sûr, *i.e.*, que toute attaque polynomiale échoue pour des clés suffisamment grandes

- Sécurité exacte (ou pratique)
  - Rendre la réduction la plus fine possible
    i.e., à partir d'une attaque, on peut construire un algorithme qui casse le schéma sous-jacent avec la même probabilité de réussite.

> La sécurité exacte donne une réduction explicite pour fixer la taille des clés pour une sécurité concrète

Sécurité Prouvée

- Hypothèses calculatoires
  - Peu de cryptosystèmes sont “inconditionnellement” sûrs
  - Exemples :
    - existence de fonction à sens-unique
    - difficulté de la factorisation
    - difficulté du calcul d'un logarithme discret
    - difficulté du problème DDH
    - ...
  - Hypothèses supplémentaires
    - modèle de l'oracle aléatoire
    - modèle du chiffrement idéal
    - modèle générique
  - Un attaquant contre un cryptosystème donne lieu à un algorithme de factorisation en $2^{25}k^{10}$
    - $k = 1024 \rightsquigarrow 2^{125}$ opérations
    - or NFS a besoin de 2^{200} opérations pour factoriser...

Sécurité Prouvée

Input : the vector $\overrightarrow{x}_{\tilde{\ell}+\tilde{m}} = (x_1, \ldots, x_{\tilde{\ell}+\tilde{m}})$ whose components are pairwise distinct elements of $(\mathbb{Z}/p\mathbb{Z})^\star$ which define the polynomials

$$f(X) = \prod_{i=1}^{\tilde{\ell}} (X + x_i) \text{ and } g(X) = \prod_{i=\tilde{\ell}+1}^{\tilde{\ell}+\tilde{m}} (X + x_i),$$

the values

$$\begin{cases} g_0, g_0^{\gamma}, \ldots, g_0^{\gamma^{\tilde{\ell}+\tilde{t}-2}}, \quad g_0^{\kappa\cdot\gamma\cdot f(\gamma)}, & \text{(I.1)} \\ g_0^{\omega\gamma}, \ldots, g_0^{\omega\gamma^{\tilde{\ell}+\tilde{t}-2}}, & \text{(I.2)} \\ g_0^{\alpha}, g_0^{\alpha\gamma}, \ldots, g_0^{\alpha\gamma^{\tilde{\ell}+\tilde{t}}}, & \text{(I.3)} \\ h_0, h_0^{\gamma}, \ldots, h_0^{\gamma^{\tilde{m}-2}}, \quad h_0^{\kappa\cdot g(\gamma)} & \text{(I.4)} \\ h_0^{\omega}, h_0^{\omega\gamma}, \ldots, h_0^{\omega\gamma^{\tilde{m}-1}}, & \text{(I.5)} \\ h_0^{\alpha}, h_0^{\alpha\gamma}, \ldots, h_0^{\alpha\gamma^{2(\tilde{m}-\tilde{t})+3}} & \text{(I.6)} \end{cases}$$

where $\kappa, \alpha, \gamma, \omega$ are unknown random elements of $(\mathbb{Z}/p\mathbb{Z})^\star$, and finally an element $T \in \mathbb{G}_T$.

Output : a bit b.

The problem is correctly solved if the output is $b = 1$ when $T = e(g_0, h_0)^{\kappa\cdot f(\gamma)}$ or if the output is $b = 0$ when T is a random value from $\mathbb{G}_T$.

IUT MONTPELLIER-SETE

UNIVERSITÉ MONTPELLIER

Introduction

Email du 7 janvier 2010 :

We are pleased to announce the factorization of RSA768, the following 768-bit, 232-digit number from RSA's challenge list :

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3.

The factorization, found using the Number Field Sieve (NFS), is :

334780716989568987860441698482126908177047949837137685689124313889828837938780022876147116525317430877378144679994893674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7

EPFL (Suisse), NTT (Japon), Univ. Bonn (Allemagne), INRIA (France), Microsoft (USA), CWI (Pays-Bas)

I.U.T MONTPELLIER-SETE

UNIVERSITÉ MONTPELLIER

Introduction

Email du 7 janvier 2010 :

We are pleased to announce the factorization of RSA768, the following 768-bit, 232-digit number from RSA's challenge list :

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3.

The factorization, found using the Number Field Sieve (NFS), is :

334780716989568987860441698482126908177047949837137685689124313889828837938780022876147116525317430877378144679994893674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7

×

EPFL (Suisse), NTT (Japon), Univ. Bonn (Allemagne), INRIA (France), Microsoft (USA), CWI (Pays-Bas)

Introduction

- « *We spent half a year on 80 processors on polynomial selection. [...] the sieving, which was done on many hundreds of machines and took almost two years. On a single core 2.2 GHz AMD Opteron processor with 2 GB RAM per core, sieving would have taken about fifteen hundred years. [...] Preparing the sieving data for the matrix step took a couple of weeks on a few processors, the final step after the matrix step took less than half a day of computing, but took about four days of intensive labor because a few bugs had to be fixed.* »

- « *[...]* 192796550 $\times$ 192795550-*matrix of total weight* 27797115920 *(thus, on average* 144 *non-zeros per row)[...]* »

- « *[...] it is not unreasonable to expect that 1024-bit RSA moduli can be factored well within the next decade by an academic effort such as ours [...]* »

- « *Thus, it would be prudent to phase out usage of 1024-bit RSA within the next three to four years* »

I.U.T MONTPELLIER-SETE

UNIVERSITÉ MONTPELLIER

Mécanismes cryptographiques - Règles et recommandations,
Rev. 1.20, ANSSI , 01/2010.

RègleCléSym-1. La taille minimale des clés symétriques utilisées jusqu'en 2020 est de 100 bits.

RègleCléSym-2. La taille minimale des clés symétriques devant être utilisées au-delà de 2020 est de 128 bits.

RecomCléSym-1. La taille minimale recommandée des clés symétriques est de 128 bits.

RègleAlgoBloc-1. Pour un algorithme de chiffrement ne devant pas être utilisé après 2020, aucune attaque nécessitant moins de $Nop = 2^{100}$ opérations de calcul doit être connue.

RègleAlgoBloc-2. Pour un algorithme de chiffrement utilisé au-delà de 2020, aucune attaque nécessitant moins de $Nop = 2^{128}$ opérations de calcul doit être connue.

RecomAlgoBloc-1. Il est recommandé d'employer des algorithmes de chiffrement par bloc largement éprouvés dans le milieu académique.

Factorisation

RégleFact-1. La taille minimale du module est de 2048 bits, pour une utilisation ne devant pas dépasser l'année 2020.

RégleFact-2. Pour une utilisation au-delà de 2020, la taille minimale du module est de 4096 bits.

RègleFact-3. Les exposants secrets doivent être de même taille que le module.

RègleFact-4. Pour les applications de chiffrement, les exposants publics doivent être strictement supérieurs à $2^{16} = 65536$.

RecomFact-1. Il est recommandé, pour toute application, d'employer des exposants publics strictement supérieurs à $2^{16} = 65536$.

RecomFact-2. Il est recommandé que les deux nombres premiers p et q constitutifs du module soient de même taille et choisis aléatoirement uniformément.

Introduction

Quelques ordres de grandeur

- sécurité : $\geq 2^{100}$
- nombre d'atomes dans l'univers : $10^{80} \sim 2^{265}$
- taille d'un module RSA : 1024 bits $\sim 2^{1024} \sim 10^{310}$
- taille d'une clé AES : 256 bits
- Core 2 Quad (Penryn) - 3,2 GHz : 2×24200 MIPS[1]
  $1\,000\,000 \sim 2^{20}$
  2^{35} opérations en 1 seconde
  Recherche exhaustive sur 2^{80} : $2^{80}/2^{35} = 2^{45}$ secondes

Introduction

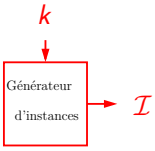
Quelques ordres de grandeur

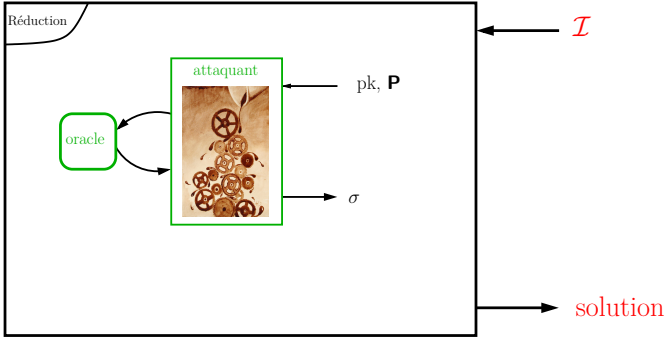
- sécurité : $\geq 2^{100}$
- nombre d'atomes dans l'univers : $10^{80} \sim 2^{265}$
- taille d'un module RSA : 1024 bits $\sim 2^{1024} \sim 10^{310}$
- taille d'une clé AES : 256 bits
- Core 2 Quad (Penryn) - 3,2 GHz : 2×24200 MIPS[1]
  $1\,000\,000 \sim 2^{20}$
  2^{35} opérations en 1 seconde
  Recherche exhaustive sur 2^{80} : $2^{80}/2^{35} = 2^{45}$ secondes

  $\rightsquigarrow$ 1114925 années

[1] le nombre de millions d'instructions complétées par le microprocesseur en une seconde

Sécurité Prouvée





I.U.T MONTPELLIER-SETE

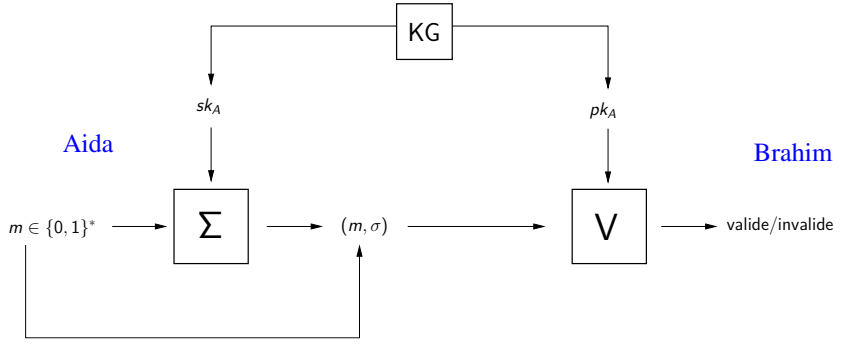
UNIVERSITÉ MONTPELLIER

Sécurité des schémas de signatures.

Signature

- La signature électronique émule la signature manuscrite.
- Elle doit dépendre du message.
- Elle vérifie les propriétés suivantes :
  - authenticité de la source
  - intégrité
  - résistance à une contrefaçon
  - vérification universelle
  - non-répudiation

Signature



Définition des buts et des moyens d'un *forgeur* $\mathcal{F}$.

Signature

Sécurité d'un schéma de signatures

Définition des buts et des moyens d'un *forgeur* $\mathcal{F}$.

- *cassage total* : $\mathcal{F}$ retrouve la clé secrète du signataire,
- *forge universelle* : $\mathcal{F}$ peut signer n'importe quel message,
- *forge sélective* : $\mathcal{F}$ peut signer *un* message de son choix,
- *forge existentielle* : $\mathcal{F}$ peut générer un couple message/signature valide.

Signature

Sécurité d'un schéma de signatures

Définition des buts et des moyens d'un *forgeur* $\mathcal{F}$.

- *cassage total* : $\mathcal{F}$ retrouve la clé secrète du signataire,
- *forge universelle* : $\mathcal{F}$ peut signer n'importe quel message,
- *forge sélective* : $\mathcal{F}$ peut signer *un* message de son choix,
- *forge existentielle* : $\mathcal{F}$ peut générer un couple message/signature valide.

- une *attaque sans message* : $\mathcal{F}$ ne connaît que *pk*
- une *attaque à messages connus* : $\mathcal{F}$ a accès à une liste de couples message/signature de ce signataire,
- une *attaque à messages choisis* : $\mathcal{F}$ obtient des signatures de messages de son choix.

Fonctions de hachage

Definition

Soit $\ell \in \mathbb{N}$.

Une fonction $h : \{0,1\}^* \longrightarrow \{0,1\}^\ell$ est une fonction de hachage si

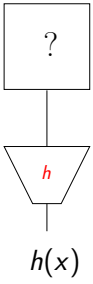
- h est à sens unique (résistante à la préimage)
  [étant donné $h(x)$ trouver x' tel que $h(x') = h(x)$ est difficile]
- h est résistante à la seconde préimage
  [étant donné x et $h(x)$, trouver $x' \neq x$ tel que $h(x') = h(x)$ est difficile]
- h est résistante aux collisions
  [trouver x et x', $x \neq x'$, tels que $h(x) = h(x')$ est difficile]

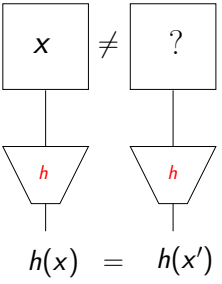
h crée une "empreinte" (un haché) de m.

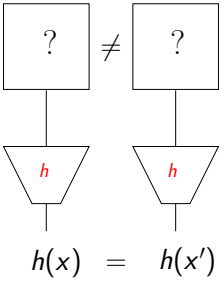
I.U.T MONTPELLIER-SETE

UNIVERSITÉ MONTPELLIER

Fonctions de hachage







Complexité : 2^{ℓ} 2^{ℓ} $2^{\ell/2}$

I.U.T MONTPELLIER-SETE

UNIVERSITÉ MONTPELLIER

Signature

Définition

Soit $k \in \mathbb{N}$. Un schéma de signatures $\mathcal{S}$ est un quadruplet

$$(Setup, KeyGen, Sign, Verify)$$

---

où

- $\mathcal{S}.Setup$ *est une PPTM prenant en entrée k dont la sortie est appelée paramètres publics et notée* $\mathbf{P}$

$$\mathcal{S}.Setup(k) = \mathbf{P}$$

- $\mathcal{S}.KeyGen$ *est une PPTM prenant en entrée des paramètres publics et dont la sortie est un couple (pk, sk) de clés publique et privée*

$$\mathcal{S}.KeyGen(\mathbf{P}) = (pk, sk)$$

Signature

Définition

Soit $k \in \mathbb{N}$. Un schéma de signatures $\mathcal{S}$ est un quadruplet

$$(Setup, KeyGen, Sign, Verify)$$

- $\mathcal{S}.Sign$ *est une PPTM prenant en entrée des paramètres publics, un message et une clé privée. Sa sortie est une chaîne binaire appelée signature*

$$\mathcal{S}.Sign(\mathbf{P}, m, sk) = \sigma$$

- $\mathcal{S}.Verify$ *est une PPTM prenant en entrée des paramètres publics, une clé publique, un message et une chaîne binaire. Elle renvoie un bit qui vaut 0 si la signature est invalide, et 1 sinon.*

$$\mathcal{S}.Verify(\mathbf{P}, pk, m, \sigma) \in \{0, 1\}$$

I.U.T MONTPELLIER - SETE

UNIVERSITÉ MONTPELLIER

Signature

Définition

Soit $k \in \mathbb{N}$. Un schéma de signatures $\mathcal{S}$ est un quadruplet

$$(Setup, KeyGen, Sign, Verify)$$

---

et tel que

$$\forall k \in \mathbb{N},$$
$$\forall \mathbf{P} = \mathcal{S}.Setup(k),$$
$$\forall (pk, sk) = \mathcal{S}.KeyGen(\mathbf{P}),$$
$$\forall m \in \{0,1\}^*,$$
$$\forall \sigma = \mathcal{S}.Sign(\mathbf{P}, m, sk)$$

alors

$$\mathcal{S}.Verify(\mathbf{P}, pk, m, \sigma) = 1$$

I.U.T MONTPELLIER-SETE

UNIVERSITÉ MONTPELLIER

Signature

Modèle de sécurité :

- La notion de sécurité la plus forte est la

  la résistance à une forge existentielle
  dans une attaque à messages choisis

- Existential forgery in a chosen message attack : EF-CMA

S. Goldwasser, S. Micali, R. L. Rivest : A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. SIAM J. Comput. 17(2) : 281-308 (1988)

Signature : modèle de sécurité

Définition (EF-CMA)

Soit $k \in \mathbb{N}$ et l'expérience aléatoire suivante :

Experiment $\mathbf{Exp}^{\mathsf{ef-cma}}_{\mathcal{S},\mathcal{F}}(k)$

$params = \mathcal{S}.Setup(k)$

$(pk, sk) = \mathcal{S}.KeyGen(params)$

$(m^\star, \sigma^\star) \leftarrow \mathcal{F}^{\Sigma}(params, pk)$

Retourne 1 *si* $\mathcal{S}.Verify(params, pk, m^\star, \sigma^\star) = 1$ *et* $\sigma^\star$ *ne provient pas de* Σ

0 *sinon*

On définit le succès de $\mathcal{F}$ *comme*

$$Succ^{ef\text{-}cma}_{\mathcal{S},\mathcal{F}}(k) = \Pr\left[\mathbf{Exp}^{\mathsf{ef-cma}}_{\mathcal{S},\mathcal{F}}(k) = 1\right].$$

Un schéma de signature est dit résistant aux forges existentielles dans une attaque à messages choisis si toute PPTM a un succès négligeable dans cette expérience.

RSA textbook

- RSA.Setup$(k) = \{k\}$
- RSA.KeyGen(k) :
  - p et q sont deux grands premiers tels que $2^{\lfloor k/2 \rfloor - 1} \leq p, q \leq 2^{\lfloor k/2 \rfloor} - 1$
  - $N = pq$
  - e et d sont deux entiers premiers à $\varphi(N) = (p-1)(q-1)$ tels que

$$ed = 1 \mod \varphi(N)$$

  - Finalement
    - (N, e) est la clé publique pk
    - (d, p, q) est la clé secrète sk

- RSA.Sign$(k, m, (d, p, q))$:

$$\sigma = m^d \mod N$$

- RSA.Verify$(k, (N, e), m, \sigma)$:

$$\sigma \text{ valide} \iff m = \sigma^e \mod N$$

I.U.T MONTPELLIER-SETE

UNIVERSITÉ MONTPELLIER

RSA textbook

Sécurité

- Est-il EF-CMA ?
- Est-il EF-KMA ?
- Est-il EF-NMA ?
- Est-il SF-CMA ?
- Est-il TB-NMA ?

RSA textbook

Sécurité

- Est-il EF-CMA ? non
- Est-il EF-KMA ?
- Est-il EF-NMA ?
- Est-il SF-CMA ?
- Est-il TB-NMA ?

RSA textbook

Sécurité

- Est-il EF-CMA ? non
- Est-il EF-KMA ? non
- Est-il EF-NMA ?
- Est-il SF-CMA ?
- Est-il TB-NMA ?

I.U.T MONTPELLIER-SETE

UNIVERSITÉ MONTPELLIER

RSA textbook

Sécurité

- Est-il EF-CMA ? non
- Est-il EF-KMA ? non
- Est-il EF-NMA ? non
- Est-il SF-CMA ?
- Est-il TB-NMA ?

RSA textbook

Sécurité

- Est-il EF-CMA ? non
- Est-il EF-KMA ? non
- Est-il EF-NMA ? non
- Est-il SF-CMA ? non
- Est-il TB-NMA ?

RSA textbook

Sécurité

- Est-il EF-CMA ? non
- Est-il EF-KMA ? non
- Est-il EF-NMA ? non
- Est-il SF-CMA ? non
- Est-il TB-NMA ?