Recherche en informatique au LORIA

Factorisation d'entiers: quelle sécurité pour les clefs RSA?

Pierrick Gaudry

LORIA
Université de Lorraine – CNRS – INRIA

La sécurité informatique au LORIA

- LORIA = Laboratoire Lorrain de Recherche en Informatique et ses Applications. Plus de 400 personnes, dont 160 chercheurs permanents.
- Associé au CNRS, à l'INRIA et à l'Université de Lorraine.
- Thèmes de recherche variés, des plus théoriques aux plus appliqués.
- Environ 25 chercheurs permanents travaillent sur la sécurité informatique.
- Encore plus si l'on rajoute des thèmes voisins tels que les réseaux, ou la sûreté des logiciels.

Axes de recherche

- Virologie, étude des logiciels malveillants.

  [équipe CARTE]
- Vérification formelle de protocoles.

  [équipe CASSIS]
- Primitives cryptographiques.

  [équipe CARAMEL]
- Management, monitoring d'Internet.

  [équipe MADYNES]

Une plateforme : le Laboratoire Haute Sécurité.

Des applications transverses : vote électronique, réseaux sociaux pair-à-pair.

Des liens avec l'industrie et les agences gouvernementales : ANSSI, DGA, Gendarmerie Nationale, Thalès, Alcatel-Lucent, Symantec, Cisco, Ingenico.

Le cryptosystème RSA

Enjeu majeur en SI : être certain de l'identité de l'interlocuteur. (e.g. faux mail, faux site web, etc)

Point de départ de nombreuses attaques !

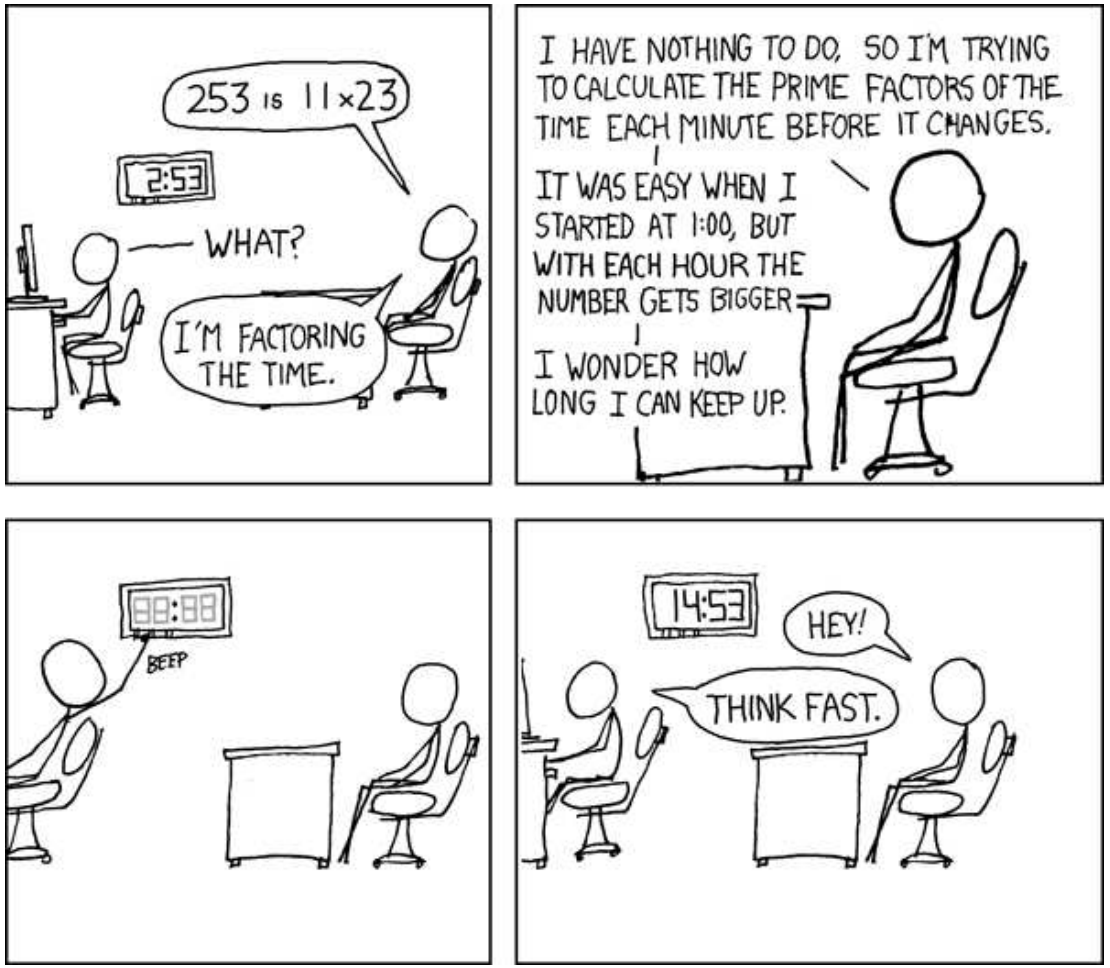
Une solution : cryptographie à clef publique ; signature numérique.

[attention : le terme "signature" est ambigu ; beaucoup de notions implicites associées]

Système le plus fréquemment utilisé actuellement : RSA.

La sécurité repose sur la difficulté présumée de la factorisation d'entiers.

Factorisation d'entiers



- Facile : fabriquer de grands nombres premiers, les multiplier.
- Difficile : retrouver les facteurs premiers d'un grand nombre.

Difficile comment ?

Important de quantifier le temps que prendrait la factorisation d'une clef RSA : permet de choisir la taille.

Exple : d'après le site `http://www.keylength.com`, si l'on souhaite que la meilleure attaque nécessite 2^{128} opérations élémentaires, il faut prendre une clef RSA entre 3000 et 4500 bits selon les sources.

Approche théorique : factoriser N par la méthode du crible algébrique nécessite

$$\exp\left(\left(\left(\frac{64}{9}\right)^{1/3}+o(1)\right)(\log N)^{1/3}(\log\log N)^{2/3}\right).$$

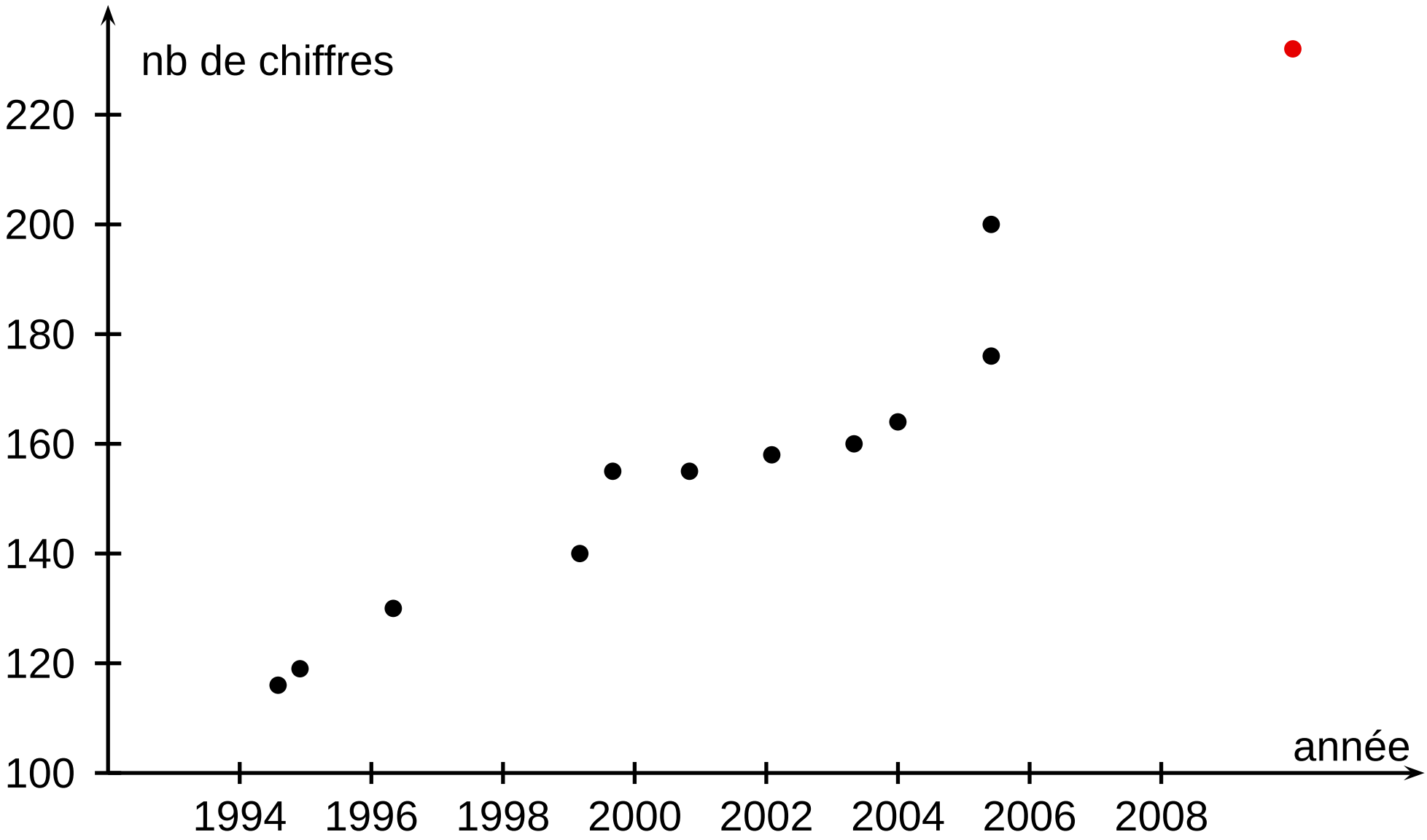
De la théorie à la pratique

Problèmes avec l'estimation théorique :

- Ne prend en compte que le temps de calcul, pas le temps de communication ; or l'algorithme tel qu'analysé nécessite trop de mémoire pour être implanté tel quel.
- Nombreuses améliorations pratiques de l'algo, peu quantifiable dans la formule théorique.
- L'analyse est de toute façon heuristique (conjectures mathématiques bien plus forte que l'hypthèse de Riemann).

Nécessité de faire des expériences.

Historique des précédents records



Calcul record RSA-768

- Nombre issu d'un défi lancé par la compagnie RSA en 1991.
  - Les facteurs premiers ont été volontairement oubliés ;
  - $50\,000$ de dollars de récompense ; mais clos en 2007.
- De nombreux partenaires :
  - EPFL (Suisse)
  - NTT (Japon)
  - CWI (Pays-Bas)
  - Nancy (+ clusters Grid5000, partout en France)
- Temps de calcul : équivalent de ≈ 1700 années ;
- Parallélisme : 2 ans et demi.
- Algorithme utilisé très complexe.

Résultat (décembre 2009)

RSA768 =

$$123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3$$

=

$$334780716989568987860441698482126908177047949837137685689124313889828837938780022876147116525317430877378144679994893674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7$$

*

$$367460436667995904282446337996279526322791581643430876426760322838157396665112792333734171433968102700927987363089 17$$

Quelques conséquences

- Ne plus utiliser de clefs RSA de 768 bits. (en usage dans les cartes bancaires au début des années 2000)
- A permis de raffiner l'estimation pour RSA-1024. Il faudrait environ 1000 fois plus de temps ;
- Quelques avancées algorithmiques (en particulier, meilleure distribution de la phase d'algèbre linéaire).