Cryptographie Asymétrique : Description d'un nouveau cryptogramme

Rémy Aumeunier
remy.aumeunier@libertysurf.fr

Amateur

Résumé En cryptographie asymétrique, l'un des principaux défis consiste à définir un point d'arrêt. Le schéma qui suit est basé sur une propriété mathématique qui n'est pas utilisée, à ma connaissance, dans ce contexte. Alice crée une fonction qui offre une infinité de solutions, puis sachant que 2 entiers différents ne peuvent pas avoir la même partie décimale dans leur racine nième, cette propriété lui permet de retrouver le choix de son correspondant.

1 Introduction

Le chiffrement asymétrique est apparu en 1976[1], avec la publication d'un ouvrage sur la cryptographie publié par Whitfield Diffie et Martin Hellman ; mais aussi par $RalphMerkle$[2] à la même époque. Le cryptosystème asymétrique utilise 2 clefs : une clef publique et une clef privée, ou secret. Lorsque 2 personnes (nommées par convention Alice et Bob) veulent échanger des informations via un canal ouvert ou public, Alice publie une clef publique, Bob code son message avec la clef public d'Alice et met à disposition d'Alice le résultat du chiffrement. Puis Alice avec sa clef privée récupère les informations codées par Bob.

1.1 État de l'art

Les algorithmes de cryptographie asymétrique peuvent être regroupés en 3 grandes familles. Les plus connus sont les cryptogrammes de type RSA. Cet algorithme a été décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman. Il y a aussi les cryptogrammes à courbe elliptique proposés de manière indépendante, par $NealKoblitz$[4] et $VictorMiller$[3] en 1985. Une courbe elliptique est un cas particulier de courbe algébrique avec laquelle on peut faire une addition, ce qui permet de définir un échange de clés de type Diffie-Hellman. Enfin, le chiffrement El Gamal qui est un algorithme de cryptographie asymétrique fondé sur le problème du logarithme discret créé par l'Égyptien Taher Elgamal, doctorant de l'université de Stanford.

2 Présentation du schéma cryptographique

Alice crée une clef publique avec $a_1 \in \mathbb{D}, a_2 \in \mathbb{N}$ telle que

$$clefPubliqueAlice = a_1 + \sqrt{a_2}$$

Bob à partir de la clefPubliqueAlice va créer une clefPubliqueBob avec $b_1, b_2 \in \mathbb{N}$ telle que

$$clefPubliqueBob = (clefPubliqueAlice - b_1)^2 + \sqrt{b_2}$$

puis Alice recherche un entier par force brute ou recherche exhaustive en faisant varier $x_{Alice} \in \mathbb{N}$ dans

$$clefPubliqueBob = (clefPubliqueAlice - b_1)^2 + \sqrt{b_2}$$

$$clefPubliqueBob = (a_1 + \sqrt{a_2} - b_1)^2 + \sqrt{b_2}$$

$$clefPubliqueBob = a_1^2 + a_2 + b_1^2 + 2.a_1.\sqrt{a_2} - 2.b_1.(a_1 + \sqrt{a_2}) + \sqrt{b_2}$$

sss $x_{Alice} = b_1$ alors

$$(clefPubliqueBob - (a_1^2 + a_2 + b_1^2 + 2.a_1.\sqrt{a_2} - 2.b_1.(a_1 + \sqrt{a_2})))^2 = b_2 \in \mathbb{N}$$

3 Unicité de la partie décimale d'une racine carré

Démonstration de l'unicité de la partie décimale d'une racine carré

$$n = (\sqrt{n})^2 = (e + d)^2 e \in \mathbb{N}, d \in \mathbb{D}, n = (e + d)^2 = (e^2 + 2.e.d + d^2)$$

$$e^2 \in \mathbb{N}, (2.e.d + d^2) \in \mathbb{D}$$

$$n_1 = (e_1 + e + d)^2 = e_1^2 + e_1.e + e_1.d + e.e_1 + e^2 + e.d + d.e_1 + d.e + d^2$$

$$n_1 = (e_1 + e + d)^2 = n + e_1^2 + 2.e_1.e + 2.e_1.d$$

$$n, n_1, e_1^2, 2.e.e_1 \in \mathbb{N}, 2.e_1.d \in \mathbb{D}$$

ce qui implique que 2 entiers différents ne peuvent pas avoir la même partie décimale dans leur racine carré, sauf si elle est nulle, bien sûr.

4 La problématique de la troncature

Il est possible que deux entiers différents partagent une même valeur dans leur partie décimale, suite à une troncature de leur racine carré.

$$\sqrt{6} = 2.4494 \quad \sqrt{8363} = 91.4494 \quad \sqrt{10292} = 101.4494$$

Pour ne pas être confronté à cette problématique, je vais imposer à Bob une quantité de décimale plus importante que la quantité de chiffres qui compose la partie entière de la racine carré. Cette simple règle va me garantir le rang de l'occurrence de la partie décimale. Si je considère l'ensemble de toutes les racines qui partage une même partie dans leur partie décimale .

4.1 Démonstration :

$$x, x_1, n, n_1, n_x \in \mathbb{R}, d \in \mathbb{D} \quad x_1 > x$$

$$\sqrt{x} = n + d \quad x = (n+d)^2 = (n^2 + 2.n.d + d^2)$$

$$\sqrt{x_1} = (n+n_1)+d \quad x_1 = ((n+n_1)+d)^2 = ((n+n_1)^2 + 2.d.(n+n_1) + d^2)$$

$$x_1 - x = ((n+n_1)^2 + 2.d.n + 2.d.n_1 + d^2) - (n^2 + 2.n.d + d^2)$$

$$x_1 - x = ((n+n_1)^2 - n^2 + 2.d.n_1)$$

comme $(x_1 - x) \in \mathbb{R}$ cela implique $(2.d.n_1) \in \mathbb{R}$ et donc n_1 est au minimum de la forme $n_1 = n_x.10^{NbDecimales(d)}$ Ceci garanti à Alice l'unicité de sa solution et le rang de l'occurrence de la partie décimale. Dit différement, si je considère l'ensemble de toutes les racines carres et que parmis cet ensemble, je prends une racine tronquée de la forme $xxx.yyyyyyy$ je suis sûr et certain que c'est la première fois que l'occurence $.yyyyyyy$ apparaît dans les parties décimales. Par contre, si la racine carré est de la forme $xxxxxxxxxx.yyyyyyy$ je ne peux pas être certain que c'est la première fois que $.yyyyyyy$ apparaît dans les parties décimales d'une racine carré et cela quelque soit la méthode de troncature,

5 Unicité de la solution trouvée par Alice

Alice à partir de la $clefPubliqueBob$ va donc rechercher les solutions possible par force brute ou recherche exhaustive en faisant varier x_{Alice} dans sa clefs privée $(a_1^2 + a_2 + b_1^2 + 2.a_1.\sqrt{a_2} - 2.b_1.(a_1 + \sqrt{a_2})) \in \mathbb{D}$

5.1 Explication ,Mise en lumiére ,Démonstration :

sss $b_1 = x_{Alice}$ alors

$$clefPriveAlice = (a_1^2 + a_2 + x_{Alice} + 2.a_1.\sqrt{a_2} - 2.x_{Alice}.(a_1 + \sqrt{a_2}))$$

$$(clefPubliqueBob - clefPriveAlice)^2 = b_2$$

ce point d'arrêt est unique parce qu'il n'existe pas deux racines de nombre entier qui ont la même partie décimale,dans le contexte précédemment décrit

6 Étude de la sécurité, attaques possibles

il existe plussieur clefPubliqueAlice possible

$$clefPubliqueAlice = a_1 + \sqrt{a_2}$$

et plussiuer solution possible

$$(clefPubliqueBob - clefPriveAlice)^2 = b_2 \in \mathbb{N}$$

7 Inconvénient, amélioration à apporter

La recherche de toutes les solutions par Alice jusqu'à la bonne est d'une lenteur désespérante. Il doit être possible de mettre en musique le point d'arrêt dans un autre schéma cryptographique qui permette une recherche plus rapide pour Alice

8 Licence et droit de propriété intellectuelle

Domaine public ou libre de toute contrainte ou notion de propriété.

9 Recommandation, mise en garde

Compte tenu du fait que la création d'un schéma de cryptographie asymétrique est l'une des choses les plus difficiles auxquelles je me suis retrouvé confronté, je vous conseille vivement la plus grande prudence. Autrement dit, je ne suis pas censé réussir à ce jeu, donc ...

Références

1. ↑ W. Diffie and M.E. Hellman, Multiuser cryptographic technics, Proceedings of AFIPS National Computer Conference, 109-112, 1976
2. ↑ A.J. Menezes, P.C Van Oorschot, S.A. Vanstone, Handbook of applied cryptography, CRC Press, 1997, p. 47
3. ↑ V. Miller, « Use of elliptic curves in cryptography », dans CRYPTO, n°85, 1985.
4. ↑ Neal Koblitz, « Elliptic curve cryptosystems », dans Mathematics of Computation, n°48, 1987, p.203–209