SÉCURITÉ DU GÉNÉRATEUR DE BLUM BLUM SHUB. PARTIE I

par

Robert Rolland

1. Introduction

Soit N un entier de Blum (c'est-à-dire un produit de deux nombres premiers p et q congrus à 3 modulo 4) ayant k bits On définit à partir d'un germe X_0 la suite $X_i = X_{i-1}^2 \mod n$, et enfin $x_i = \mathrm{lsb}(X_i) = X_i \mod 2$. Ce générateur pseudo-aléatoire est le générateur BBS (de Blum Blum Shub). Dans la suite nous allons étudier la sécurité d'un tel générateur.

2. Sécurité du générateur de Blum Blum shub

2.1. Rappel sur le problème de la résiduosité quadratique. — Soit N un entier. On rappelle qu'un résidu quadratique modulo N est le carré d'un nombre modulo N. Afin d'éviter un certain nombre de cas où la situation dégénère, on appellera $\mathbf{Q}_N$ l'ensemble des résidus quadratiques $x^2 \mod N$ tels que $\gcd(x, N) = 1$. Dans la suite par abus de langage, si on ne précise rien, un résidu quadratique modulo N sera un élément de $\mathbf{Q}_N$.

Le problème de la résiduosité quadratique est le suivant : étant donné un nombre $1 \leq a < N$, déterminer si a est un carré modulo N ou non.

Dans le cas où $N = p$ est premier, on peut résoudre ce problème en temps polynomial en la taille de p par le calcul du symbole de Legendre

$\left(\frac{a}{p}\right)$. On sait dans ce cas que a est un résidu quadratique modulo p, si et seulement si son symbole de Legendre est 1.

En revanche si N est un nombre composé dont on ignore la factorisation, on ne dispose d'aucun algorithme polynomial en la taille de N pour résoudre le problème de la résiduosité quadratique. On peut calculer en temps polynomial le symbole de Jacobi de a, qui généralise le symbole de Legendre, mais celui-ci ne nous donne plus une réponse qui permette de conclure. On sait bien que si ce symbole de Jacobi n'est pas 1, et si a est premier avec le module N, alors a n'est sûrement pas un résidu quadratique. Mais contrairement au cas d'un module premier, si le symbole de Jacobi est 1, on ne peut pas en déduire que a est un résidu quadratique.

Supposons que $N = pq$ où p et q sont deux nombres premiers distincts. Si on connait la factorisation de N alors le problème de la résiduosité quadratique se résout en temps polynomial en cherchant tout simplement si $a \mod p$ et $a \mod q$ sont des résidus quadratiques par le calcul de leurs symboles de Legendre. Si on ne connait pas la factorisation de N on ne sait pas résoudre le problème en temps polynomial. On pourrait donc se demander si réciproquement, la résolution du problème de la résiduosité quadratique permet de factoriser N. Pour le moment on ne sait rien de tel.

Un autre problème du même secteur est celui de l'extraction d'une racine carrée modulaire. Plus précisément, sachant qu'un nombre a est un résidu quadratique, comment déterminer un nombre b tel que $b^2 = a \mod N$? Cette fois-ci, on peut montrer que ce problème est polynomialement équivalent au problème de la factorisation (si on autorise l'utilisation d'algorithmes de réductions probabilistes de Las Vegas).

2.2. Les entiers de Blum. — Un entier de Blum est un entier N qui est le produit de deux nombres premiers distincts congrus à 3 modulo 4. Soit x un résidu quadratique modulo N qui n'est ni multiple de p ni multiple de q. Alors x admet 4 racines carrées modulo N. L'intérêt des entiers de Blum, c'est que dans ce cas on peut affirmer que parmis ces 4 racines carrées, il en existe une et une seule qui est elle-même un résidu quadratique (voir l'annexe 3).

Remarque 2.1. — Soit N un entier de Blum, X un élément de symbole de Jacobi 1 et $Y = X^2 \mod N$ son carré modulo N. Par construction $Y \in \mathbf{Q}_N$, et posséde donc 4 racines carrées dont deux ont pour symbole de Jacobi 1 : ce sont X et $-X$. Une et seulement une des deux valeurs X et $-X$, est dans $\mathbf{Q}_N$. En outre X et $-X$ ont des parités différentes. Autrement dit, si on disposait d'un algorithme capable de déterminer avec une probabilité de succès non négligeable, à partir de Y, quelle est la parité de la racine carrée qui est elle même un carré, on pourrait déterminer avec la même probabilité de succès si X est un carré ou non.

2.3. Détails sur la sécurité de la résiduosité quadratique. — Définissons le problème exact de la résiduosité quadratique et sa sécurité supposée. Nous nous placerons dans le cadre de la sécurité asymptotique probabiliste (cf. [**1**]).

Nous allons noter $\mathbf{J}_N^+$ l'ensemble des entiers $a > 0$ de symbole de Jacobi $\left(\frac{a}{N}\right)$ valant 1.

Remarque 2.2. — Le nombre d'éléments de $\mathbf{J}_N^+$ est donné par :

$$\#\mathbf{J}_N^+ = \frac{1}{2}(N - (p+q) + 1).$$

On sait que :

$$\mathbf{Q}_N \subset \mathbf{J}_N^+,$$

et que :

$$\#\mathbf{Q}_N = \frac{\#\mathbf{J}_N^+}{2} = \frac{1}{4}(N - (p+q) + 1).$$

Rappelons qu'on prend pour N un entier de Blum, en conséquence l'application g_N de $\mathbf{Q}_N$ dans lui même définie par :

$$g_N(x) = x^2 \mod N$$

est une bijection.

Soit k, la taille de l'entier N, qui va nous servir de paramètre de sécurité. On dispose d'un algorithme probabiliste polynomial en k, $\mathcal{G}$, qui étant donné en entrée le paramètre de sécurité k, construit au hasard un environnement de travail, c'est-à-dire dans notre cas, un entier de Blum N de taille k, et par conséquent la fonction g_N d'élévation au carrée modulo N. On note Γ_k l'ensemble des environnements possibles.

Soit $\mathcal{A}$ un algorithme probabiliste polynomial en k, dont l'entrée est le paramètre de sécurité k, le nombre N et un élément a de $\mathbf{J}_N^+$ et la sortie un bit b dont on espère qu'il détermine avec succès si a est un élément de $\mathbf{Q}_N$ ou non.

On considère les expériences :

$\mathbf{Expt}_{\mathcal{G}}^{\mathbf{res}}(\mathcal{A}, k)$
$(N, g_N) \leftarrow \Gamma_k$
$X \leftarrow \mathbf{J}_N^+$
$X \leftarrow g_N(X)$
$b \leftarrow \mathcal{A}(k, N, X)$
retour b
Fin.

$\widetilde{\mathbf{Expt}}_{\mathcal{G}}^{\mathbf{res}}(\mathcal{A}, k)$
$(N, g_N) \leftarrow \Gamma_k$
$X \leftarrow \mathbf{J}_N^+$
$b \leftarrow \mathcal{A}(k, N, X)$
retour b
Fin.

L'avantage de l'attaquant $\mathcal{A}$ est défini par :

$$Adv_{\mathcal{G}}^{res}(\mathcal{A}, k) = \left| Prob\left(\mathbf{Expt}_{\mathcal{G}}^{\mathbf{res}}(\mathcal{A}, k) = 1\right) - Prob\left(\widetilde{\mathbf{Expt}}_{\mathcal{G}}^{\mathbf{res}}(\mathcal{A}, k) = 1\right)\right|$$

***Hypothèse 1* (Difficulté de la résiduosité quadratique)**
Le problème de la résiduosité quadratique est sûr, c'est-à-dire que pour tout attaquant polynomial $\mathcal{A}$ et pour tout entier m :

$$\lim_{k \to +\infty} k^m \, Adv_{\mathcal{G}}^{res}(\mathcal{A}, k) = 0.$$

Autrement dit tout attaquant polynomial a un avantage qui est une fonction négligeable du paramètre de sécurité k.

2.4. Les algorithmes d'extrapolation. — En s'appuyant sur l'étude faite dans [**1**, théorème 8.2 et §9], on sait que la sécurité d'un système de générateurs pseudo-aléatoires dépend du succès ou non d'un extrapolateur à gauche qui prédit « le bit précédent ». Soit k le paramètre de sécurité, N_k un entier de Blum de taille k et f_{N_k} le générateur pseudo-aléatoire définie par :

$$f_{N_k} : Q_{N_k} \to \{0,1\}^{l(k)},$$

où pour tout $X_0 \in Q_{N_k}$ le calcul de $f_{N_k}(X_0)$ se fait de la façon suivante.

(1) La bijection g_{N_k} de Q_{N_k} dans lui même définie par $g_{N_k}(X) = X^2 \mod N_k$ permet de calculer $X_1 = g_{N_k}(X_0), \cdots X_{l(k)} = g_{N_k}(X_{l(k)-1})$.
(2) chaque X_i donne un bit $x_i = X_i \mod 2$.
(3) $f_{N_k}(X_0) = (x_1, x_2, \cdots, x_{l(k)})$.

Lemme 2.3. — *Soit $s \in [1, l(k)]$ et $\mathcal{B}_s$ un algorithme probabiliste polynomial qui étant donnés les bits $(x_s, \cdots, x_{l(k)})$ prédit le bit x_{s-1} avec un avantage non négligeable. Alors si on fournit en entrée de cet algorithme probabiliste polynomial, les $l(k) - s$ bits $(y_1, y_2, \cdots, y_{l(k)-s})$ d'un $f_{N_k}(Y_0)$, il prédit le bit $y_0 = Y_0 \mod 2$ avec le même avantage non négligeable.*

Démonstration. — Du fait que g_{N_k} est une bijection, la loi de probabilité du terme calculé $X_s \in Q_{N_k}$, est la même que la loi de probabilité du terme tiré au sort dans Q_{N_k} qui sert de germe X_0. □

Pour démontrer que le générateur BBS est sûr, nous montrerons que s'il existe un extrapolateur probabiliste polynomial qui prédit le bit x_0 avec un avantage non négligeable, alors, il existe un algorithme probabiliste polynomial qui possède un avantage non négligeable pour résoudre le problème de la résiduosité quadratique.

Soit donc $\mathcal{B}$ un algorithme polynomial probabiliste, dont les entrées sont $k, N_k, (y_1, y_2, \cdots, y_r)$ et dont l'avantage de prédiction du bit y_0 n'est pas une fonction négligeable de k. Construisons l'algorithme $\mathcal{A}$ dont les entrées sont (k, N_k, X) où $X \in \mathbf{J}_k^+$ et qui sort un bit.

$\mathcal{A}(k, N_k, X)$
  $Y_0 \leftarrow X$
  pour $i = 1$ à $i = l(k)$
    $Y_i = Y_{i-1}^2 \mod N$; $y_i = Y_i \mod 2$
  fin pour
  $y_0 = \mathcal{B}(k, N_k, (y_1, \cdots, y_r))$
  $b = (y_0 = Y_0 \mod 2)$
  retour b
Fin.

Compte tenu de la remarque 2.1, on voit que l'algorithme $\mathcal{A}$ ainsi construit, a un avantage $Adv_{\mathcal{G}}^{res}(\mathcal{A}, k)$ non négligeable pour le problème de

la résiduosité quadratique. Compte tenu de l'hypothèse 1, on en conclut que le générateur BBS est sûr.

Le résultat qu'on a obtenu a été démontré en s'appuyant sur la sécurité supposée du problème de la résiduosité quadratique.

3. Annexe arithmétique

Soit N un produit de deux nombres premiers distincts p et q. Le théorème des restes chinois nous dit que l'application qui à x associe le couple $(x \mod p, x \mod q)$ est un isomorphisme d'anneaux :

$$\mathbb{Z}/N\mathbb{Z} \sim \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

On peut donc considérer tout élément $x \in \mathbb{Z}/N\mathbb{Z}$ comme l'élément $(x_p = x \mod p, x_q = x \mod q)$.

Un élément $x = (x_p, x_q)$ tel que $\gcd(x, n) = 1$ est un résidu quadratique si et seulement si x_p est un résidu quadratique non nul dans $\mathbb{Z}/p\mathbb{Z}$ et x_q un résidu quadratique non nul dans $\mathbb{Z}/q\mathbb{Z}$.

Soit α un élément primitif dans $\mathbb{Z}/p\mathbb{Z}$. Un élément primitif α n'est sûrement pas un carré sinon par le petit théorème de Fermat on aurait $\alpha^{(p-1)/2} = 1$ ce qui contredirait la primitivité de α. Le symbole de Legendre de α est donc -1. Remarquons que $\alpha^{(p-1)/2} = -1$. Donc le symbole de Legendre de (-1) est $(-1)^{(p-1)/2}$.

Si $p \equiv 3 \mod 4$, alors $(p-1)/2$ est impair et le symbole de Legendre de (-1) est -1. En conséquence, dans ce cas, le symbole de Legendre de $-x$ est l'opposé du symbole de Legendre de x.

Voici donc ce qu'il se passe au niveau des racines carrées modulo un entier de Blum N.

Soit $x \in \mathbf{Q}_N$ un résidu quadratique modulo N tel que $\gcd(x, N) = 1$. Notons, comme indiqué précédemment, $x = (x_p, x_q)$. Le nombre x_p est un résidu quadratique modulo p de racines carrées y_p et $-y_p$. On supposera que y_p est parmis les deux racines y_p et $-y_p$ celle qui a $+1$ pour symbole de Legendre. De même, x_q a eux racines carrées modulo q qu'on notera y_q et $-y_q$, et on supposera que le symbole de Legendre de y_q est 1.

Le nombre x a 4 racines carrées : $(y_p, y_q), (y_p, -y_q), (-y_p, y_q), (-y_p, -y_q)$. Les deux racines carrées $y = (y_p, y_q)$ et $-y = (-y_p, -y_q)$ ont pour symbole de Jacobi 1. Les deux autres ont pour symbole de Jacobi -1. $y = (y_p, y_q)$ qui a ses eux composantes y_p et y_q qui sont des carrés est la seule racine carrée de x à être elle même un carré.

Références

[1] Robert Rolland, Sécurité des générateurs pseudo-aléatoires, notes téléchargeables depuis le site http ://www.acrypta.fr

---

22 mars 2008

R. Rolland, Institut de Mathématiques de Luminy, Campus de Luminy, Case 907, 13288 MARSEILLE Cedex 9 • *E-mail :* robert.rolland@acrypta.fr
Url : http://www.acrypta.fr/~rolland