Attaque par padding court de Coppersmith

Clara Do et Juliette Paumelle

1 Attaque par padding court et Attaque de Franklin Reiter

1.1 Attaque de Franklin-Reiter

Si Bob envoie à Alice les chiffrés de deux messages différents M_1, M_2, mais reliés par une fonction linéaire telle que $M_1 \equiv f(M_2) \pmod N$, alors un attaquant peut retrouver ces messages. Cette attaque fonctionne pour des petites clés publiques e. Comme l'attaque se déroule en temps quadratique selon e, on ne peut pas prendre cette clé trop grande.

Théorème 1. *Soit et $\langle N, e\rangle$ la clé publique d'un système RSA. Soient $M_1 \neq M_2 \in \mathbb{Z}_N^*$ tels que $M_1 \equiv f(M_2) \pmod N$ pour une fonction linéaire polynomiale $f = ax + b \in \mathbb{Z}_N[x]$ avec $b \neq 0$. Alors, si on connaît $\langle N, e, C_1, C_2, f\rangle$, on peut retrouver M_1, M_2 en temps quadratique en $\log(N)$ et e.*

Proof. Comme $C_1 \equiv M_1^e \pmod N$, on sait que M_2 est une racine du polynôme $g_1(x) = f(x)^e - C_1 \in \mathbb{Z}_N[x]$. De même, M_2 est une racine du polynôme $g_2(x) = x^e - C_2 \in \mathbb{Z}_N[x]$. Le facteur linéaire $x - M_2$ divise donc ces deux polynômes. Ainsi, il suffit d'utiliser l'algorithme d'Euclide étendu pour trouver le pgcd de g_1 et g_2. Si ce pgcd est linéaire, on a trouvé M_2. Il suffit ensuite d'appliquer la fonction modulo N pour retrouver M_1.

Pour $e = 3$, le pgcd est nécessairement linéaire. En effet, $x^3 - C_2$ n'a qu'une seule racine et g_2 ne peut pas diviser g_1 donc le pgcd est nécessairement linéaire.

Pour $e > 3$, le pgcd est presque toujours linéaire. Ce n'est que pour quelques rares triplets M_1, M_2 et f que le pgcd n'est pas linéaire et, dans ces cas, l'attaque ne réussit pas. □

1.2 Attaque par padding court

Généralement, personne ne penserait à envoyer des messages reliés, du moins pas intentionnellement. Cependant, cette attaque permet d'en exécuter une autre sur des messages utilisant le padding. Cette fois-ci, l'attaquant intercepte le message de Bob pour Alice. Comme Bob ne reçoit pas de réponse, il renvoie le message à Alice. Comme il remplit aléatoirement son message, les deux chiffrés sont différents, mais le clair est le même. Ainsi, si on ne fait pas attention à la méthode pour rajouter des données aléatoirement, on peut tout de même retrouver les messages chiffrés.

Théorème 2. *Soit $\langle N, e\rangle$ la clé publique d'un système RSA où N est de taille n bits. Soit $m = \lfloor \frac{n}{e^2} \rfloor$. Soit $M \in \mathbb{Z}_N^*$ un message de taille au plus $n - m$ bits. On pose $M_1 = 2^m M + r_1$ et $M_2 = 2^m M + r_2$ avec r_1 et r_2 distincts et $0 < r_1, r_2 < 2^m$. Si on connaît $\langle N, e\rangle$ et les chiffrés C_1, C_2, on peut retrouver efficacement M.*

Proof. On pose $g_1(x, y) = x^e - C_1$ et $g_2(x, y) = (x + y)^e - C_2$. Lorsque $y = r_2 - r_1$, ces deux polynômes ont une racine commune qui est M_1. Autrement dit, $\Delta = r_2 - r_1$ est la racine du résultant $h(y) = res_x(g_1, g_2) \in \mathbb{Z}_n[y]$. Le degré de h est au plus e^2. De plus, $\mid \Delta \mid < 2^m < N^{\frac{1}{e^2}}$. Ainsi, Δ est une petite racine de h modulo N et on peut efficacement la retrouver en utilisant le théorème de Coppersmith.

Une fois qu'on connaît Δ, il nous suffit d'utiliser l'attaque de Franklin-Reiter pour M_1 et donc M. □

2 Théorème de Coppersmith

Théorème 3. ***(Coppersmith)*** *Soit N un entier et $f \in \mathbb{Z}[x]$ un polynôme unitaire de degré d. Soit $X = N^{\frac{1}{d}-\epsilon}$ avec $\epsilon > 0$. Alors, étant donnés (N, f), un attaquant peut trouver efficacement tous les entiers $\mid x_0 \mid < X$ tels que $f(x_0) \equiv 0 \pmod N$.*

Soient $N \in \mathbb{Z}$ et $X = N^{\frac{1}{d}-\epsilon}, \epsilon > 0$.

Le théorème de Coppersmith nous dit qu'on peut trouver toutes les petites racines modulaires $\mid x_0 \mid < X$ d'un polynôme f de degré d, $f(x_0) \equiv 0 \pmod N$. Pour cela, on souhaite passer à un autre polynôme h qui a les mêmes racines que f mais dans les entiers, c'est-à-dire $h(x_0) = 0$. En effet, il est plus simple de chercher des racines dans les entiers que des racines modulaires.

Or, d'après le lemme de Howgrave-Graham, si on arrive à construire h de degré d_h tel que $\| h(xX) \| < \frac{N}{\sqrt{d_h}}$, alors toutes les racines x_0 telles que $h(x_0) \equiv 0 \pmod N$ sont des racines dans $\mathbb{Z}$. En voici la preuve :

Lemme 4. ***(Howgrave-Graham)*** *Soit $h(x) \in \mathbb{Z}[x]$ un polynôme de degré d et soit $X \in \mathbb{N}^*$. On suppose que $\| h(xX) \| < \frac{N}{\sqrt{d}}$. Si pour $\mid x_0 \mid < X$, $h(x_0) \equiv 0 \pmod N$, alors $h(x_0) = 0$ dans $\mathbb{Z}$.*

Proof.

Soient $h(x) = \sum_{i=0}^{d} a_i x^i$ et $\mid x_0 \mid < X$. Alors on a :

$$\mid h(x_0) \mid = \mid \sum_{i=0}^{d} a_i x_0^i \mid < \sum_{i=0}^{d} \mid a_i x_0^i \mid < \sum_{i=0}^{d} \mid a_i X^i \mid$$

Or, l'inégalité de Cauchy-Schwartz nous dit, pour tout $(a, b) \in \mathbb{R}^2$:

$$\left(\sum_k a_k b_k \right)^2 \leq \sum_k a_k^2 \sum_k b_k^2$$

Alors, en posant $a_k = 1$ et $b_k = \mid a_i X^i \mid$, on obtient :

$$\left(\sum_k \mid a_i X^i \mid \right)^2 \leq \sum_k 1 \sum_k \mid a_i X^i \mid^2 \leq d. \sum_k \mid a_i X^i \mid^2 = d. \| h(xX) \|^2$$

Ainsi, en supposant que $\| h(xX) \| < \frac{N}{\sqrt{d}}$, on a :

$$\mid h(x_0) \mid \leq \sqrt{d}. \| h(xX) \| < N$$

Donc si $h(x_0) \equiv 0 \pmod N$, alors on a nécessairement $h(x_0) = 0$.

□

On va donc chercher à construire $h \in \mathbb{Z}[x]$ tel que $h = gf$ avec $g \in \mathbb{Z}[x]$ et ayant une norme plus petite que N. Cela revient à chercher une combinaison linéaire entière dans la base $\{f, xf, x^2 f, \ldots, x^r f\}$, pour $r > 0$, ayant une norme inférieure à N. En effet, un polynôme divisible par f aura les mêmes racines que f.

Cependant, la majoration est trop petite et il est rare de trouver une telle combinaison linéaire entière non-triviale.

exemple...

Pour résoudre ce problème, il faut agrandir la dimension du réseau.

Or, on peut observer que si $f(x_0) \equiv 0 \pmod N$, alors $\forall k \in \mathbb{N}$ $f(x_0)^k \equiv 0 \pmod{N^k}$. Autrement dit, $\exists l \in \mathbb{Z}$ tel que $f(x_0) = lN$, d'où $f(x_0)^k = (lN)^k = l^k N^k$.

Soit m fixé, on définit alors les polynômes suivants :

$$g_{u,v}(x) = x^u N^{m-v} f(x)^v$$

Alors, $\forall 0 \leq v \leq d-1, \forall 0 \leq v \leq m$:

$$g_{u,v}(x_0) = x_0^u N^{m-v} f(x_0)^v = x_0^u N^{m-v} l^v N^v = x_0^u N^m l^v$$

On a donc la relation : $g_{u,v}(x_0) \equiv 0 \pmod{N^m}$. Comme $f(x_0) \equiv 0 \pmod{N}$, alors $f(x_0)^v N^{m-v} \equiv 0 \pmod{N^m}$. Ainsi, tous les polynômes $g_{u,v}(x)$ partage la même racine x_0 modulo N^m. De plus, comme $f(x)$ est un polynôme unitaire et de degré d, alors $g_{u,v}(x)$ est de degré exactement $u + vd$ avec comme coefficient dominant N^{m-v}.

On doit maintenant trouver une combinaison linéaire entière $h(x)$ dans la base engendrée par les polynômes $g_{u,v}(x)$ telle que $\parallel h(xX) \parallel$ est inférieure à N^m.

Or, l'algorithme LLL nous assure que pour un réseau $\mathcal{L}$ de dimension n, il existe un vecteur h tel quel $\parallel h \parallel \leq 2^{\frac{n-1}{4}} det(\mathcal{L})^{\frac{1}{n}}$.

Théorème 5. *Soient un réseau $\mathcal{L}$ de dimension n, $\mathcal{B} = (b_1, \ldots, b_n)$ une de ses bases, LLL-réduite. Alors on a :*

$$\parallel b_1 \parallel \leq 2^{\frac{n-1}{4}} det(\mathcal{L})^{\frac{1}{n}}$$

Proof. Pour prouver ce résultat, on doit utiliser l'orthogonalisation de Gram-Schmidt et d'autres résultats dus à la réduction LLL. On en fait la preuve plus loin. □

On va donc construire un réseau $\mathcal{L}$ de dimension n de façon à trouver un vecteur h qui nous convienne. Cette construction nous donnera les conditions sur m pour trouver les petites racines modulaires de f.

$$\begin{array}{cc}
 & \begin{array}{cccccccccccc} 1 & x & \cdots & x^{d-1} & \cdots & x^{dv} & \cdots & x^{(v+1)d-1} & \cdots & x^{dm} & \cdots & x^{(m+1)d-1} \end{array} \\
\begin{array}{c} g_{0,0} \\ g_{1,0} \\ \vdots \\ g_{d-1,0} \\ \vdots \\ g_{0,v} \\ \vdots \\ g_{d-1,v} \\ \vdots \\ g_{0,m} \\ \vdots \\ g_{d-1,m} \end{array} & \left(\begin{array}{cccccccccccc}
N^m & & & & & & & & & & & \\
 & N^m X & & & & & & & & & & \\
 & & \ddots & & & & & & & & & \\
 & & & N^m X^{d-1} & & & & & & & & \\
* & * & \cdots & * & \ddots & & & & & & & \\
* & * & \cdots & * & \ldots & N^{m-v} X^{dv} & & & & & & \\
\vdots & \vdots & \ldots & \vdots & \vdots & \ldots & \ddots & & & & & \\
* & * & \cdots & * & \ldots & * & \cdots & N^{m-v} X^{(d+1)v-1} & & & & \\
* & * & \cdots & * & \ldots & * & \cdots & * & \ddots & & & \\
* & * & \cdots & * & \ldots & * & \cdots & * & \ldots & X^{dm} & & \\
\vdots & \vdots & \ldots & \vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \ldots & \ddots & \\
* & * & \cdots & * & \ldots & * & \cdots & * & \vdots & * & \cdots & X^{(m+1)d-1}
\end{array}\right)
\end{array}$$

On vient de construire la matrice des polynômes $g_{u,v}(xX)$ dans la base $(1, \ldots, x^{(m+1)d-1})$. On considère le réseau $\mathcal{L}$ généré par cette matrice. Cette matrice étant triangulaire inférieure, son déterminant est $det(\mathcal{L}) = N^{\frac{m(m+1)d}{2}} X^{\frac{n(n-1)}{2}}$ où $n = d(m+1)$ et est la dimension de $\mathcal{L}$.

Grâce à l'algorithme LLL, on sait qu'il existe $h(x)$ tel quel

$$\parallel h(xX) \parallel \leq 2^{\frac{n-1}{4}} det(\mathcal{L})^{\frac{1}{n}} = 2^{\frac{n-1}{4}} N^{\frac{m(m+1)d}{2n}} X^{\frac{n-1}{2}}$$

De plus, nous savons $h(x_0) \equiv 0 \pmod{N^m}$. Si $\parallel h(xX) \parallel \leq \frac{N^m}{\sqrt{n}}$, alors on peut appliquer le résultat de Howgrave-Graham et trouver toutes les petites racines $\mid x_0 \mid < N^m$ telles que $h(x_0) = 0$ dans $\mathbb{Z}$. Il ne reste plus qu'à trouver les conditions sur m.

Proof. (Coppersmith)

On construit le réseau $\mathcal{L}$ comme expliqué précédemment. On sait alors qu'il existe un vecteur h tel que

$$\parallel h(xX) \parallel \leq 2^{\frac{n-1}{4}} det(\mathcal{L})^{\frac{1}{n}} = 2^{\frac{n-1}{4}} N^{\frac{m(m+1)d}{2n}} X^{\frac{n-1}{2}}$$

Une condition suffisante pour trouver ses petites racines dans $\mathbb{Z}$ d'après Howgrave-Graham est que

$$2^{\frac{n-1}{4}} N^{\frac{m(m+1)d}{2n}} X^{\frac{n-1}{2}} < \frac{N^m}{\sqrt{n}}$$

ce qui donne

$$X < 2^{-\frac{1}{2}} n^{-\frac{1}{n-1}} N^{\frac{2m}{n-1} - \frac{m(m+1)d}{n(n-1)}}$$

Comme $2^{-\frac{1}{2}} n^{-\frac{1}{n-1}} > \frac{1}{2}$ pour $n > 6$, on peut prendre la condition diminuée :

$$X < \frac{1}{2} N^{\frac{2m}{n-1} - \frac{m(m+1)d}{n(n-1)}} < 2^{-\frac{1}{2}} n^{-\frac{1}{n-1}} N^{\frac{2m}{n-1} - \frac{m(m+1)d}{n(n-1)}}$$

De plus, comme $n = d(m+1)$, on a

$$\frac{2m}{n-1} - \frac{m(m+1)d}{n(n-1)} = \frac{2m}{d(m+1)-1} - \frac{m}{d(m+1)-1} = \frac{m}{d(m+1)-1}$$

On souhaite avoir

$$\frac{m}{d(m+1)-1} \geq \frac{1}{d} - \epsilon$$

D'où

$$m \geq \frac{d - 1 + \epsilon d - \epsilon d^2}{\epsilon d^2}$$

Or

$$\frac{d - 1 + \epsilon d - \epsilon d^2}{\epsilon d^2} \leq \frac{1+\epsilon}{\epsilon d} = \frac{1}{\epsilon d} + \frac{1}{d}$$

Il suffit donc de prendre $m = \lceil \frac{1}{\epsilon d} + \frac{1}{d} \rceil$ et on a $X < \frac{1}{2} N^{\frac{1}{d} - \epsilon} < N^{\frac{1}{d} - \epsilon}$.

$\square$

On peut ainsi trouver toutes les petites racines modulaires $\mid x_0 \mid < X$ d'un polynôme f de degré d, $f(x_0) \equiv 0 \pmod{N}$. En effet, sachant qu'on a réussi à les transformer en racines dans $\mathbb{Z}$ pour un autre polynôme, il suffit d'utiliser les méthodes classiques dans $\mathbb{Z}$.

3 Réseaux et algorithme LLL

3.1 Réseaux

Définition 6. ***(Réseau)*** *Soit $n < m$ deux entiers positifs. Soient $b_1, \ldots, b_n \in \mathbb{R}^m$ n vecteurs linéairement indépendants. Alors, un réseau $\mathcal{L}$ engendré par $\{b_1, \ldots, b_n\}$ est l'ensemble de toutes les combinaisons linéaires entières de $b_1, \ldots, b_n$, c'est-à-dire*

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} x_i b_i \mid x_1 \in \mathbb{Z} \right\}$$

L'ensemble $\{b_1, \ldots, b_n\}$ est une base du réseau $\mathcal{L}$ et sa dimension est $dim(\mathcal{L}) = n$.

Théorème 7. *Si $(b_1, \ldots, b_n)$ et $(d_1, \ldots, d_k)$ sont des bases d'un réseau $\mathcal{L}$ (c'est-à-dire que ce sont des familles libres qui engendre $\mathcal{L}$) alors $n = k$ et il existe une matrice M de dimension $n \times n$ à coefficients entiers et de déterminant ± 1 telle que $(b_1, \ldots, b_n) = (d_1, \ldots, d_k) \times M$.*

3.2 Orthogonalisation de Gram-Schmidt

Définition 8. ***Matrice de Gram*** *Soit $(b_1 \dots b_n)$ une base d'un réseau $\mathcal{L}$. La matrice de Gram correspondante est $M = (m_{i,j})_{1\leq i,j\leq n}$ une matrice $n \times n$, avec $\forall 1 \leq i,j \leq n m_{i,j} =< b_i, b_j >$ ($< x, y >$ étant le produit scalaire de x et y).*

On note le déterminant de la matrice de Gram de $(b_1 \dots b_n)$:
$\Delta(b) = det_{1\leq i,j\leq n} < b_i, b_j >$.

Les matrices de Gram des bases d'un réseau $\mathcal{L}$ ont toutes le même déterminant $\Delta(b)$. Le déterminant du réseau $\mathcal{L}$ est donc $\sqrt{\Delta(b)}$

Définition 9. ***Norme Euclidienne*** *Soit $v = \sum_{i=1}^{n} x_i b_i$ un vecteur d'un réseau $\mathcal{L}$. On définit la norme suivante:*
$\| v \| = (\sum_{i=1}^{n} x_i^2)^{\frac{1}{2}}$

Étant donné une base $\mathcal{B} = (b_1, \dots, b_n)$ d'un réseau $\mathcal{L}$, l'orthogonalisation de Gram-Schmidt retourne un ensemble orthogonal $(b_1^*, \dots, b_n^*)$ tel que le déterminant de $\mathcal{L}$ soit: $\prod_{i=1}^{n} \| b_i^* \|$

Pour cela, on a la récurrence suivante:
$b_1^* = b_1$
$\forall i \geq 2$: $b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_i^*$ avec pour $1 \leq j < i, \mu_{i,j} = \frac{< b_i, b_j^* >}{b_j^*, b_j^*}$

3.3 Réduction LLL

Soient $\mathcal{B} = (b_1, \dots, b_n)$ une base d'un réseau $\mathcal{L}$ et $\mathcal{B}^* = (b_1^*, \dots, b_n^*)$ sa base orthogonale associée par l'orthogonalisation de Gram-Schmidt.

Soit pour $1 \leq j < i, \mu_{i,j} = \frac{< b_i, b_j^* >}{b_j^*, b_j^*}$.

Définition 10. ***Forme LLL-réduite***
$\mathcal{B}$ est dit sous forme LLL-réduite si:
Pour $1 \leq i < j \leq n, |\mu_{i,j}| \leq \frac{1}{2}$
Pour $1 \leq i \leq n$, $\frac{3}{4} \| b_{i-1}^* \|^2 \leq \| b_i^* + \mu_{i,i-1} b_{i-1}^* \|^2$

Théorème 11. *Soient un réseau $\mathcal{L}$ de dimension n, $\mathcal{B} = (b_1, \dots, b_n)$ une de ses bases, LLL-réduite et $\mathcal{B}^* = (b_1^*, \dots, b_n^*)$ sa base orthogonale associée.*

1. *$\forall 1 \leq i \leq j \leq n, \| b_i \|^2 \leq 2^{j-1} \| b_j^* \|^2$*
2. *$det(\mathcal{L}) \leq \prod_{i=1}^{n} \| b_i \| \leq 2^{\frac{n(n-1)}{4}} det(\mathcal{L})$*
3. *$\| b_1 \| \leq 2^{\frac{n-1}{4}} det(\mathcal{L})^{\frac{1}{n}}$*

Proof. 1. $(b_1, \dots, b_n)$ étant une base LLL-réduite, on a alors:
$\frac{3}{4} \| b_{i-1}^* \|^2 \leq \| b_i^* \|^2 + |\mu_{i,i-1}|^2 \| b_{i-1}^* \|^2 \leq \| b_i^* \|^2 + \frac{1}{4} \| b_{i-1}^* \|^2$
d'où: $\| b_i^* \|^2 \geq \frac{1}{2} \| b_{i-1}^* \|^2$
donc $\forall 1 \leq i \leq j \leq n \| b_j^* \|^2 \geq 2^{i-j} \| b_i^* \|^2$

Soient i et j tels que $1 \leq i \leq j \leq n$ alors on a :

$\| b_i \|^2 = \| b_i^* + \sum_{k=1}^{i-1} \mu_{i,k} b_k^* \|^2$

$= \| b_i^* \|^2 + \sum_{k=1}^{i-1} |\mu_{i,k}|^2 \| b_k^* \|^2$

$\leq 2^{j-i} \parallel b_j^* \parallel^2 + \frac{1}{4} \sum_{k=1}^{i-1} 2^{j-k} \parallel b_j^* \parallel^2$

$\leq \parallel b_j^* \parallel^2 (2^{j-i} + \frac{1}{4} \sum_{k=1}^{i-1} 2^{j-k})$

$\leq \parallel b_j^* \parallel^2 (2^{j-i} + \frac{1}{4}(2^{j-i} - 2^{j-i+1}))$

$\leq \parallel b_j^* \parallel^2 (2^{j-2} + 2^{j-i-1})$

$\leq 2^{j-1} \parallel b_j^* \parallel^2$

2. On sait que $det(\mathcal{L}) = \prod_{i=1}^{n} \parallel b_i^* \parallel$.

   De plus $b_1 = b_1^*$ et $\forall i \geq 2 b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_i^*$. $\sum_{j=1}^{i-1} \mu_{i,j} b_i^* > 0$ donc $\forall 1 \leq i \leq n b_i \geq b_i^*$.

   On a donc $det(\mathcal{L}) \leq \prod_{i=1}^{n} \parallel b_i \parallel$.

   Pour tout $1 \leq i \leq n$ on a $\parallel b_i \parallel \leq 2^{\frac{i-1}{2}} \parallel b_i^* \parallel$.

   En multipliant toutes ces inégalités on obtient:

   $\prod_{i=1}^{n} \parallel b_i \parallel \leq \prod_{i=1}^{n} 2^{\frac{i-1}{2}} det(\mathcal{L})$

   Or $\prod_{i=1}^{n} 2^{\frac{i-1}{2}} = \frac{1}{4} 2^{\sum \prod_{k=0}^{n-1} k} = 2^{\frac{n(n-1)}{4}}$

   Donc on a l'inégalité souhaitée.

3. Soit $i = 1$ et $1 \leq j \leq n$ alors: $\parallel b_1 \parallel \leq 2^{\frac{j-1}{2}} \parallel b_j^* \parallel$.

   D'où $\prod_{i=1}^{n} \parallel b_1 \parallel \leq \prod_{j=1}^{n} 2^{\frac{j-1}{2}} det(\mathcal{L})$

   $\prod_{i=1}^{n} \parallel b_1 \parallel \leq 2^{\frac{n(n-1)}{4}} det(\mathcal{L})$

   On a alors: $\parallel b_1 \parallel \leq 2^{\frac{n-1}{4}} det(\mathcal{L})^{\frac{1}{n}}$

□

Bibliographie

[1] Dan Boneh, *Twenty Years of Attacks on the RSA Cryptosystem*, Notice of the AMS, 1999.

[2] Don Coppersmith, *Small Solutions to Polynomial Equations and low Exponent RSA Vulnerabilities*, , 1997.