La thèse après la prépa (?)

Joël Felderhoff
Doctorant en informatique
INRIA Lyon, ENS de Lyon, LIP

Mon parcours

- Bac S en 2014
- Prépa Lycée Massena (MPSI, MP)
- ENS de Lyon (math) intégré en 2016
- Licence + Master d'Info
- Squat des cours de Math
- Début thèse en 2021

Les Écoles Normales Supérieures

- Fondées au moment de la Révolution **pour former les enseignant·es et les chercheur·euses**.
- 4 en France : Paris, Saclay, Lyon, Rennes
- Accessible concours ou dossier

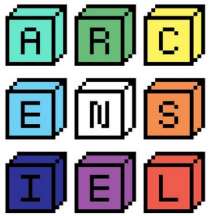
Formation classique :

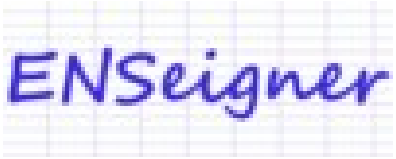
- L3
- M1
- M2 recherche / Agrégation
- Projet Long de Recherche / M2 recherche

Pourquoi faire une ENS ?

- T’as envie de faire de la science de manière plus poussée qu’en école d’ingé.
- T’as pas envie de suivre des cours de management.
- Tu veux poursuivre un parcours plus universitaire.
- Tu te destines à l’enseignement.
- T’as encore envie de réfléchir au futur (attention à l’engagement décénal !).
- T’as envie d’être payé pendant tes études (concours).

La vie à l'ENS de Lyon





La thèse (en France)

- Après un M2 (ou équivalent).
- On est encadré par un·e chercheur·euse, pendant ~3 ans.
- CIFRE (avec un entreprise) : on fait des aller-retour dans l'entreprise
- Académique (INRIA, CNRS, ED…) : on travaille dans un labo.
- Mais aussi : formation, enseignement, médiation…

Et après la thèse (en informatique) ?

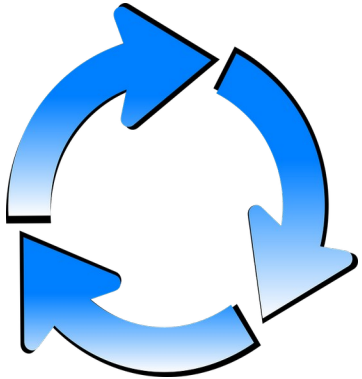
Recherche académique :

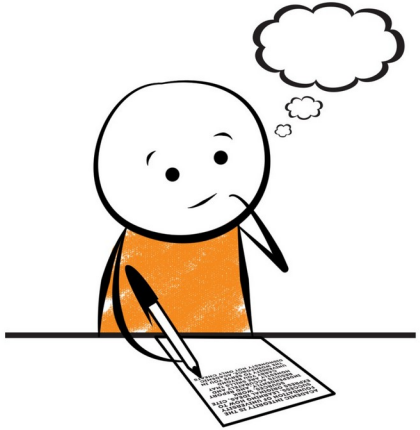
- 1-3 ans de post-doc.
- Poste permanent :
  Chargé·e de recherche /
  Maître·sse de conférence /
  Ingénieur·e de recherche.
- Directeur·ice de recherche /
  Professeur·e.

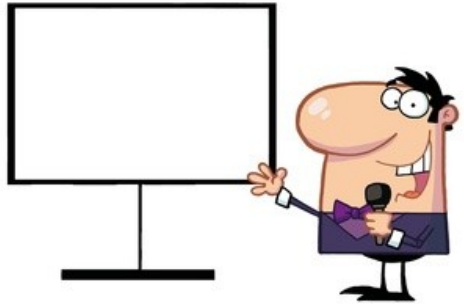
Sinon :

- Enseignement dans le secondaire (lycée, prépa).
- Grands Corps de l'État (Mines, Pont, DGA).
- Instituts publics (ANSII, ...).
- R&D dans le privé.
- Totalement autre chose.

La recherche ça marche comment ?







Un papier de recherche (en crypto)

Paper 2023/1370

Ideal-SVP is Hard for Small-Norm Uniform Prime Ideals

Joël Felderhoff, Inria Lyon, École Normale Supérieure de Lyon
Alice Pellet-Mary, Institut de Mathématiques de Bordeaux, Centre National de la Recherche Scientifique, Inria Bordeaux - Sud-Ouest Research Centre
Damien Stehlé, École Normale Supérieure de Lyon, CryptoLab, Inc.
Benjamin Wesolowski, École Normale Supérieure de Lyon, Centre National de la Recherche Scientifique, UMPA

Abstract

The presumed hardness of the Shortest Vector Problem for ideal lattices (Ideal-SVP) has been a fruitful assumption to understand other assumptions on algebraic lattices and as a security foundation of cryptosystems. Gentry [CRYPTO'10] proved that Ideal-SVP enjoys a worst-case to average-case reduction, where the average-case distribution is the uniform distribution over the set of inverses of prime ideals of small algebraic norm (below $d^{O(d)}$ for cyclotomic fields, here d refers to the field degree). De Boer et al. [CRYPTO'20] obtained another random self-reducibility result for an average-case distribution involving integral ideals of norm $2^{O(d^2)}$.

In this work, we show that Ideal-SVP for the uniform distribution over inverses of small-norm prime ideals reduces to Ideal-SVP for the uniform distribution over small-norm prime ideals. Combined with Gentry's reduction, this leads to a worst-case to average-case reduction for the uniform distribution over the set of \emph{small-norm prime ideals}. Using the reduction from Pellet-Mary and Stehl\'e [ASIACRYPT'21], this notably leads to the first distribution over NTRU instances with a polynomial modulus whose hardness is supported by a worst-case lattice problem.

6 NTRU with polynomial modulus

The main result of this section is Corollary 6.3. It gives a distribution over NTRU instances with small modulus q that is hard on average, under the worst-case id-HSVP hardness assumption.

Definition 6.1 ([PS21, Def. 3.1 and 3.4]). *Let $\gamma \geq \gamma' \geq 1$ be real numbers. Let $q \geq 2$ be an integer.*

- *A (γ, q)-NTRU instance is an element $h \in \mathcal{O}_K/q\mathcal{O}_K$ such that there exists $(f, g) \in \mathcal{O}_K \setminus \{(0,0)\}$ verifying $f = h \cdot g \bmod q$ and $\|f\|, \|g\| \leq \sqrt{q}/\gamma$.*
- *The (γ, γ', q)-NTRU problem asks, given a (γ, q)-NTRU instance h, to find $(f, g) \in \mathcal{O}_K \setminus \{(0,0)\}$ verifying $f = h \cdot g \bmod q$ and $\|f\|, \|g\| \leq \sqrt{q}/\gamma'$.*
- *Let D be a distribution over (γ, q)-NTRU instances. The (D, γ, γ', q)-NTRU problem asks to solve (γ, γ', q)-NTRU for an instance sampled from D, with non-negligible probability (over the choice of the instance and the internal randomness of the algorithm).*

Note that in this work we are only interested in the vector version of NTRU from [PS21]. We let `IdealToNTRU` denote [PS21, Alg. 4.1]. It takes as input a basis of an integral ideal $\mathfrak{a}$ and a modulus q and outputs an instance of (γ, q)-NTRU whose solution is related to a short non-zero vector of $\mathfrak{a}$. The following result is a consequence of [PS21, Le. 4.3], whose proof is very similar to [PS21, Th. 4.1]. We provide a proof for the sake of completeness.

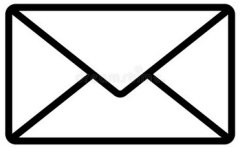
Theorem 6.2 (Adapted from [PS21, Th. 4.1]). *Let $\gamma \geq \gamma' \geq 1$ be real numbers, $q \geq 2$ be an integer, and*

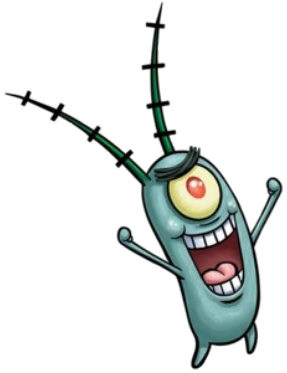
$$N = \frac{1}{2^{d+2}} \cdot \left(\frac{\sqrt{q}}{\gamma \cdot d^{1.5} \cdot \delta_K \cdot \Delta_K^{1/(2d)}} \right)^d .$$

Let $\mathfrak{a}$ be an integral ideal of norm in $[N, 2^{d+2} \cdot N]$ and $h = \texttt{IdealToNTRU}(\mathfrak{a}, q)$. Then h is a (γ, q)-NTRU instance. If (f, g) is a solution to (γ, γ', q)-NTRU on instance h, then g is a solution to γ_{HSVP}-id-HSVP for instance $\mathfrak{a}$, where $\gamma_{\mathrm{HSVP}} = \gamma/\gamma' \cdot 4d^{1.5} \cdot \delta_K$.

Further, `IdealToNTRU` runs in time polynomial in its input size and in $\log \Delta_K$.

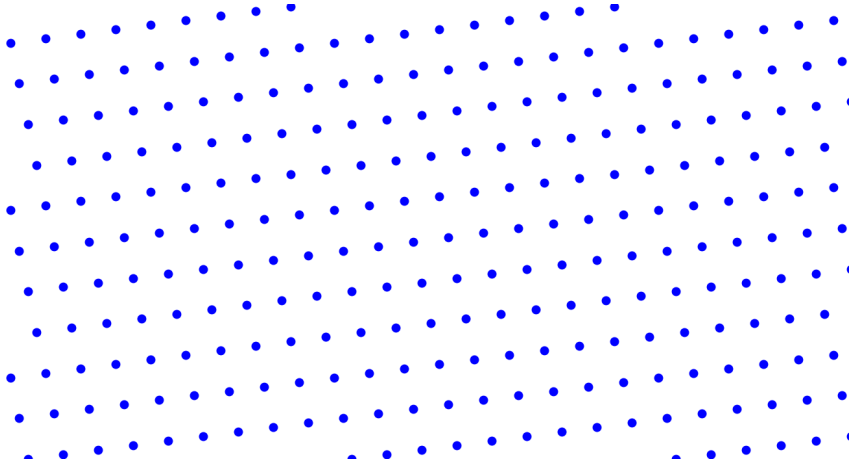
Mon sujet de recherche : la cryptographie



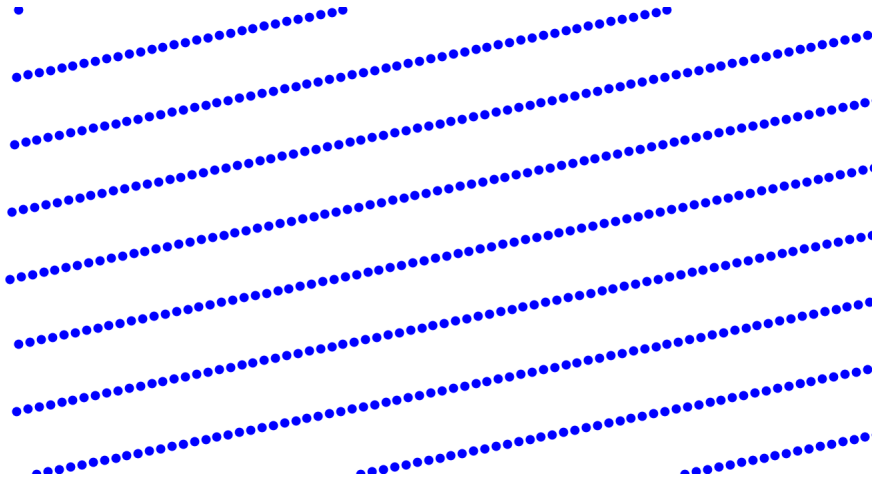


Les réseaux euclidiens

$$B \in \mathbb{Z}^{n \times n} \qquad \mathcal{L}(B) = \{B \cdot x, \quad x \in \mathbb{Z}^n\}$$

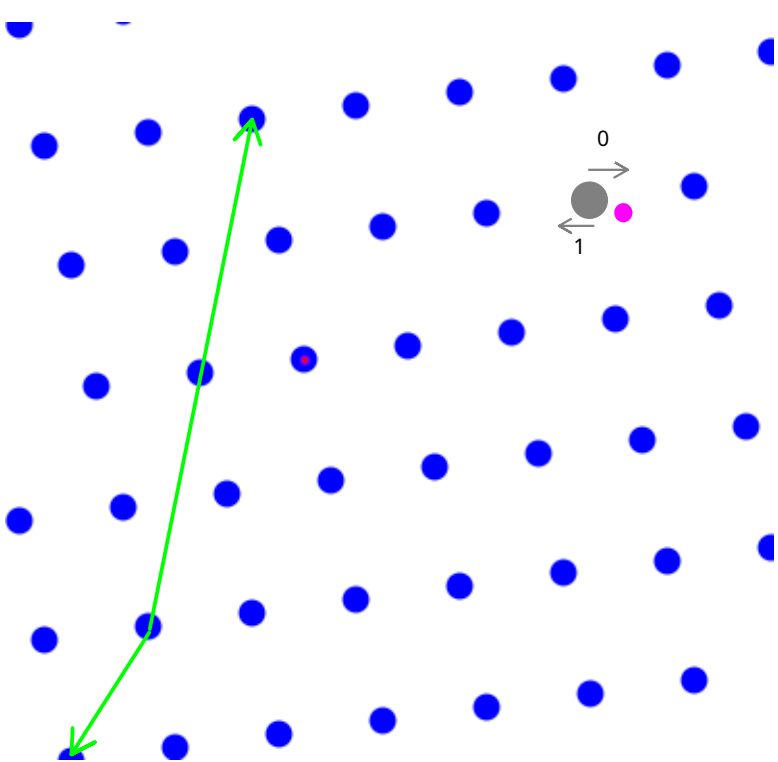


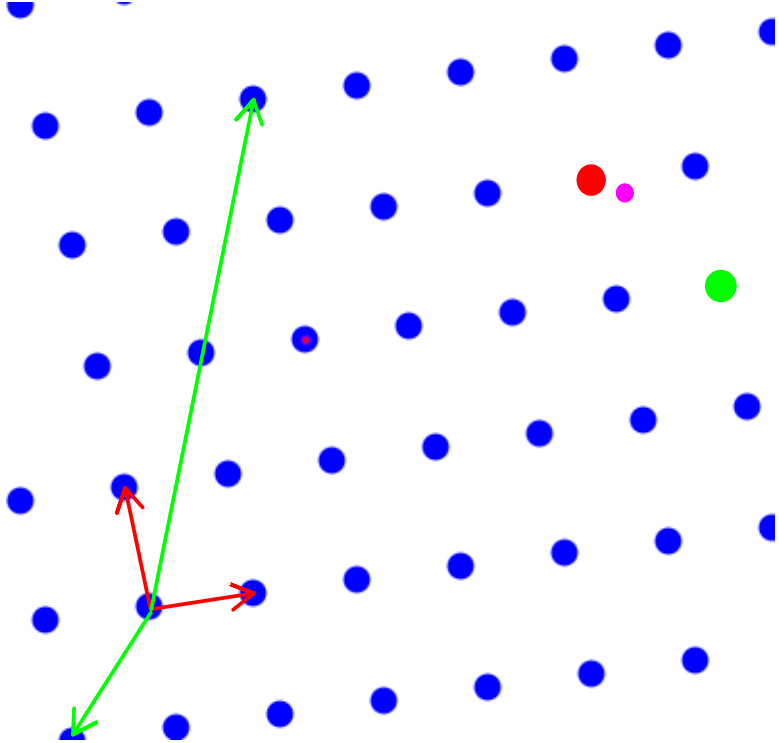
$$B = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$



$$B = \begin{pmatrix} 1 & 1 \\ 2 & 30 \end{pmatrix}$$

La cryptographie à base de réseaux euclidiens





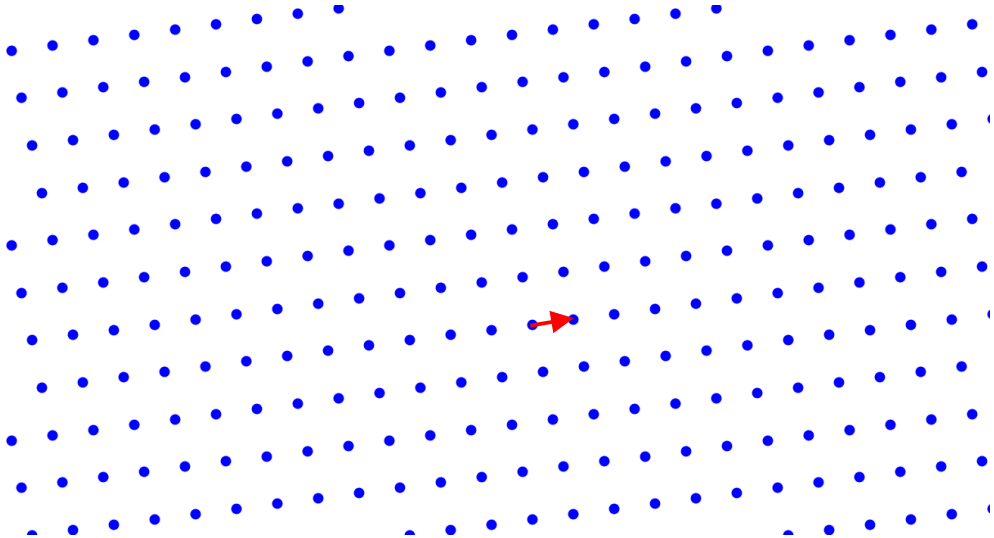
Les maths associées

Shortest Vector Problem :

Je vous donne $B \in \mathbb{Z}^{n \times n}$

Trouvez $x \in \mathbb{Z}^n \setminus \{0^n\}$

tel que $\|B \cdot x\|$ petit.

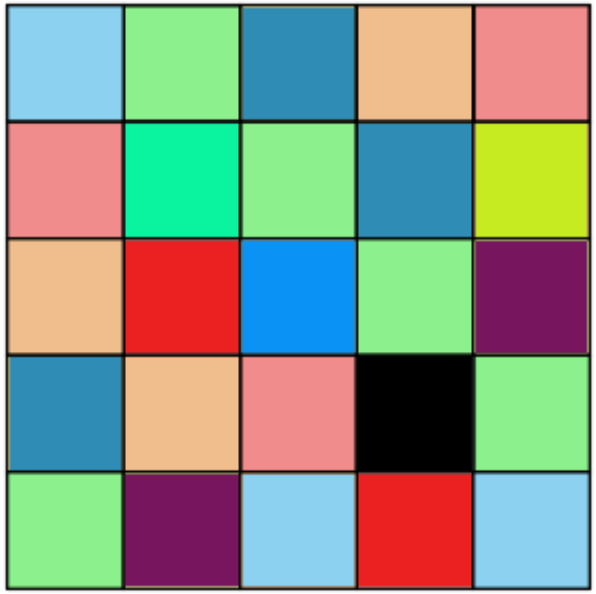


Ça devient très dur quand la dimension est grande.
(meilleur algo en $O(2^n)$).

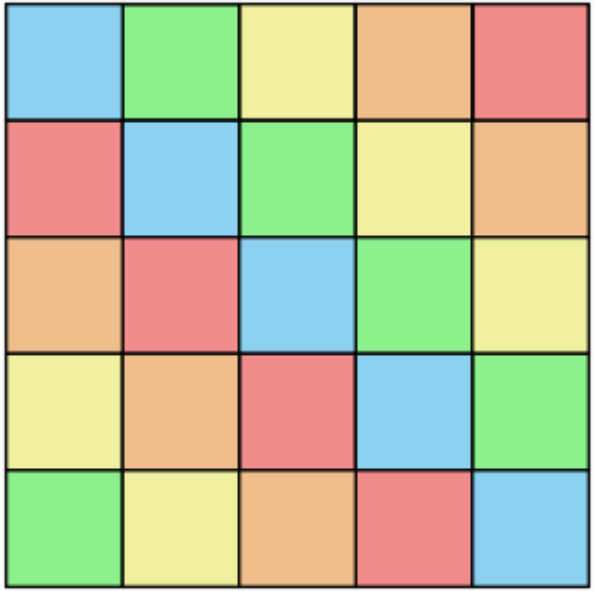
Maintenant qu'on a un problème dur, on fait quoi ?

«Si jamais tu casses mon code, tu casses aussi le problème dur.
Sauf que le problème dur est dur.
Donc tu casses pas le code»

Des matrices plus sympas



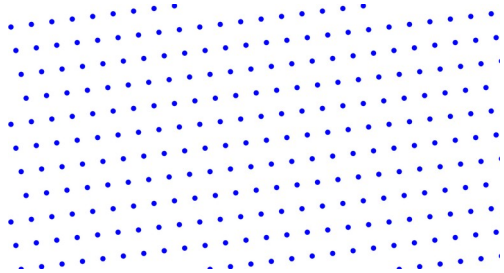
Matrice quelconque

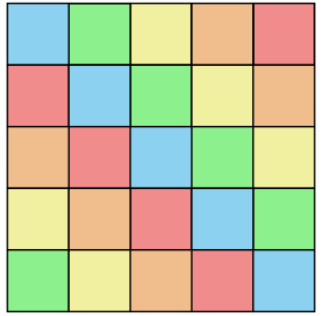


Matrice circulante

Et soudain… de l’algèbre

$\mathcal{O}_K = \{P(e^{2i\pi/p}), \quad P \in \mathbb{Z}[X]\}$ est un anneau (+, x)

$(3 + e^{2i\pi/p} + e^{2i(p-1)\pi/p}) \cdot \mathcal{O}_K$ =  =



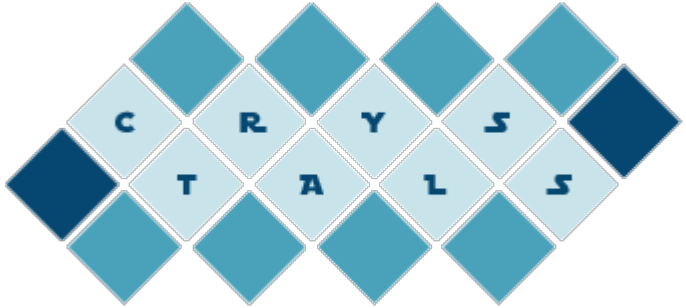
Idéal

Réseau euclidien

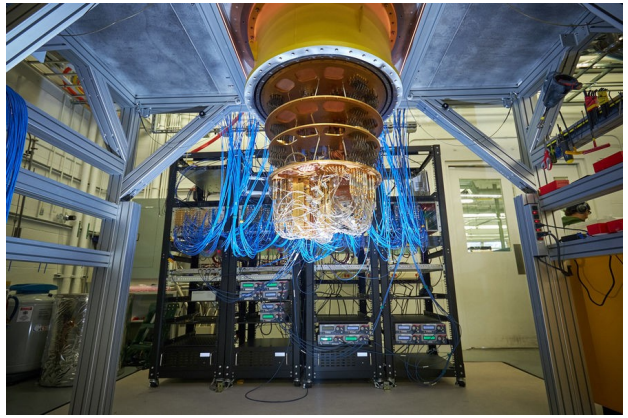
Matrice «circulante »

Et aussi : calculs plus rapides, plein de jolies maths à faire…

Utilisé pour de vrai !



NIST
National Institute of Standards and Technology



Processeur quantique de Google (2021)

Photo par Rocco Ceselin

Les trucs de prépa que j'utilise encore

- Toute l'analyse réelle de sup' (dérivée, intégration, fonctions usuelles…).
- L'analyse asymptotique (petit o, grand O)
- L'algèbre générale (groupes, anneaux, polynômes, corps) et linéaire (e.v., matrices…).
- Les probabilités.
- Les limites de fonctions (de temps en temps).
- L'algorithmique.

NB : je suis pas (du tout) bon partout !

De la science pour le plaisir

- **3 Blue 1 Brown** : math + physique + informatique
  https://www.youtube.com/@3blue1brown
- **Michael Penn** : problèmes de math « type prépa »
  https://www.youtube.com/@MichaelPennMath
- **Sebastian League** : Coding Adventure
  https://www.youtube.com/@SebastianLague
- **El jj** : maths plus accessible
  https://www.youtube.com/@ElJj

Des trucs qui aident en prépa (je pense)

- Faites des trucs à coté de la prépa (sport, musique, regarder des séries, jeux vidéos, sorties…).
- Gardez des relations hors prépa (famille, amour, amitié…).
- Se reposer est une composante **indispensable** du travail.
- Vous êtes pas plus débiles que les élèves des « grandes prépa parisiennes ».
- Si vous voulez intégrer, vous allez pouvoir le faire.

Et aussi…

- Votre santé est plus importante que vos concours.
- La santé mentale c’est **aussi** de la santé.
- Si ça va pas ne restez pas seul·e (amis, parents, profs, internet).
- Attention à l’alcool.

3114
LE NUMÉRO NATIONAL DE PRÉVENTION DU SUICIDE

Nightline
FRANCE

Merci beaucoup pour votre attention !