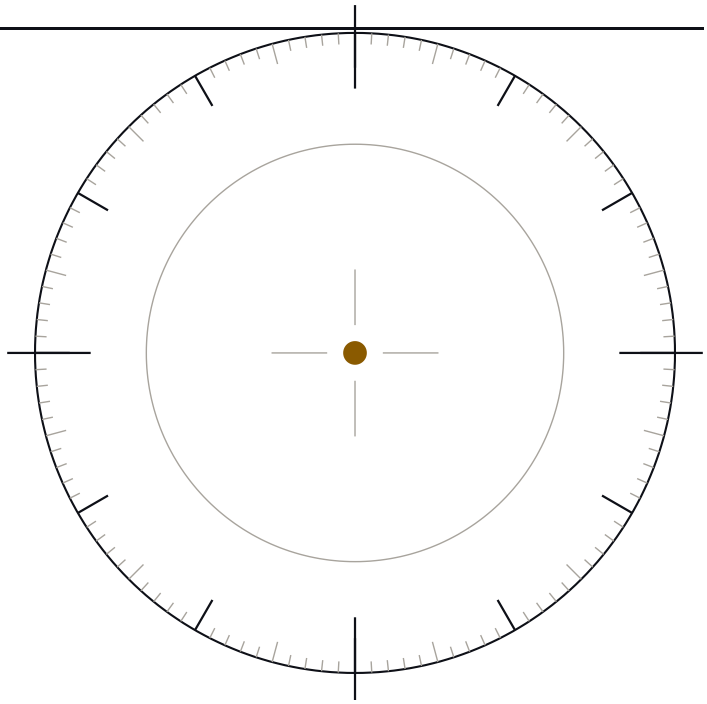
DEEO.AI

FICHE D'ACTUALITÉ · ACCÈS LIBRE



01 · IA

VEILLE IA · FICHE D'ACTUALITÉ · 22 OCTOBRE 2026

Claude a trouvé d'où vient le nombre du cadenas d'Internet

Fiche d'actualité DEEO.AI · Veille IA, hors-série. Situation au 22.10.2026.

PUBLICATION	22 octobre 2026
SITUATION	22.10.2026 · faits vérifiés à cette date
DOMAINE	01 · IA · Intelligence artificielle
VIDÉO	10 min 05, sur deeo.ai et YouTube : la vidéo et la fiche disent la même chose.

Vidéo · 10 min 05
deeo.ai/videos/veille-ia-hs-cadenas/

PARTAGE

Fiche en accès libre : vous pouvez la partager, en citant DEEO.AI.

CHAPÔ

Derrière le petit cadenas de votre navigateur, une formule mathématique très répandue, la courbe P-256, reposait depuis 1997 sur un nombre que personne n'avait su expliquer. Ce nombre avait été fourni par la NSA, l'agence de renseignement américaine, et l'on se demandait s'il cachait un piège. Le 16 octobre 2026, Anthropic a publié la réponse, trouvée par une IA en moins d'une demi-heure : il sortait d'un tirage au sort lancé par l'horloge d'un ordinateur, une nuit d'août 1997. Un piège devient très improbable. La serrure, elle, n'est pas éternelle.

Sources numérotées en fin de fiche, avec leur fiabilité ; les rapprochements faits par DEEO.AI sont signalés comme tels.

EN UNE MINUTE

- **Le nombre mystère** : la courbe P-256, qui sert à signer les certificats des sites web, les clés d'accès sans mot de passe et de nombreuses puces, dérive d'une « graine » de 160 bits fournie par la NSA à la fin des années 1990. Son origine n'avait jamais été expliquée [1] [2].
- **Le soupçon** : en 2013, les documents d'Edward Snowden ont confirmé que la NSA avait poussé un autre standard piégeable, Dual_EC_DRBG. Depuis, les graines des courbes paraissaient suspectes [4] [5].
- **La découverte** : un modèle de recherche interne d'Anthropic (famille Claude) a remarqué que plusieurs graines portaient la signature d'un générateur de hasard banal. En remontant ses tirages, on retrouve l'instant de son lancement : pour P-256, le 16 août 1997 à 1 h 52 min 34 s, heure universelle [1].
- **Ce que ça prouve** : ce n'est ni une faille ni une attaque. Les auteurs sont « plus confiants » que les courbes ont été choisies sans porte dérobée ; ce n'est pas une preuve absolue [1] [3].
- **La suite** : un ordinateur quantique assez grand casserait ces courbes. Les machines actuelles en sont encore très loin, et le monde a commencé à changer de serrures [7] [8] [9].

1. Le cadenas et son nombre mystère

1.1 Quand vous ouvrez un site en « https », votre navigateur vérifie une signature électronique : c'est elle qui fait apparaître le petit cadenas. Ces signatures reposent souvent sur des « courbes elliptiques », des formules mathématiques de la forme $y^2 = x^3 + ax + b$. La plus connue s'appelle **P-**

256. Elle sert aux certificats des sites web, aux clés d’accès sans mot de passe (les *passkeys*) et à de nombreuses puces électroniques ; Filippo Valsorda, cryptographe, la décrit comme présente « partout, y compris dans le matériel » [2].

1.2 Ces courbes figurent dans une liste de l’institut américain des normes, le NIST, publiée en juillet 1999, puis dans sa norme FIPS 186-2 du 27.01.2000 [6]. Chacune dérive d’un nombre de départ, la **graine**. On la passe dans une moulinette mathématique (le hachage SHA-1), et ce qui en sort fixe un paramètre de la courbe. Pour P-256, la graine officielle est `C49D3608 86E70493 6A6678E1 139D26B7 819F7E90`.

1.3 Ces graines ont été fournies par la NSA ; on les attribue à Jerry Solinas, mathématicien de l’agence. Personne n’avait jamais expliqué comment elles avaient été choisies : c’est la combinaison d’un cadenas réglée en usine par le fabricant, sans un mot d’explication.

2. Pourquoi on soupçonnait la NSA

2.1 Le soupçon vient d’une autre affaire. En juin 2006, le NIST normalise **Dual_EC_DRBG**, un générateur de nombres au hasard. En août 2007, deux chercheurs de Microsoft, Dan Shumow et Niels Ferguson, montrent que sa conception peut cacher une porte dérobée : une entrée secrète, pour qui connaît la clé [5].

2.2 Le 05.09.2013, des documents d’Edward Snowden publiés par le New York Times, le Guardian et ProPublica révèlent que la NSA a poussé ce standard. Le NIST le déconseille le 10.09.2013, puis le retire en juin 2015 [5]. Ce qui est établi : la NSA a poussé ce standard, et sa conception permet une porte dérobée. Que cette porte ait été réellement utilisée reste une allégation.

2.3 Depuis, les graines des courbes NIST paraissaient suspectes, elles aussi. En 2014, les chercheurs Bernstein et Lange ont montré qu’un nombre passé dans une moulinette laisse de la marge : en essayant beaucoup de graines, on peut garder celle qui donne une courbe à sa convenance. Koblitz et Menezes en ont fait la synthèse en 2015 [4]. Rien ne montrait un piège, mais rien ne permettait de l’exclure.

3. L'enquête : une prime et une fausse piste

3.1 Le 05.10.2023, Filippo Valsorda lance une prime pour qui retrouvera l'origine des graines : 12 288 dollars, triplés à 36 864 dollars si la somme est versée à une association [2].

3.2 Une piste circulait. Selon des courriels publiés en 2024 par Steve Weis, Jerry Solinas aurait évoqué le hachage d'une phrase pour rire, du genre « Give Bob and Jerry a raise » (« Augmentez Bob et Jerry ») [3]. C'est un souvenir rapporté, pas une preuve. Plusieurs salariés d'Anthropic avaient cherché dans cette direction, en vain [1].

3.3 Steve Weis, qui enquêtait sur les graines depuis 2023, est l'un des dix auteurs de l'article d'Anthropic. Un salarié curieux a posé la question à un modèle de recherche interne de l'entreprise, de la famille Claude, dont le nom n'est pas publié, **sans lui souffler cette piste** [1].

4. La découverte : c'était une heure

4.1 En moins d'une demi-heure, le modèle remarque un détail : plusieurs graines commencent par des zéros. Plus précisément, dans quatre graines sur les dix étudiées, chacun des cinq blocs de 32 bits commence par un 0. C'est la signature d'un générateur de hasard banal de la bibliothèque du langage C de l'époque. Le modèle conclut : « None of them were the results of any hash algorithm at all » (aucune ne sortait d'un hachage) [1].

4.2 Pour comprendre la suite, il faut savoir qu'un ordinateur ne tire pas vraiment au sort. Il suit une recette à partir d'un point de départ : même départ, mêmes tirages, comme un jeu de cartes mélangé deux fois exactement de la même façon. Ici, le point de départ était **l'heure de l'ordinateur**.

4.3 En remontant la recette, on retrouve donc l'instant du lancement. Le modèle a essayé 34 façons de lire les tirages avant de trouver la bonne. Pour P-256, le programme a été lancé le **16 août 1997 à 1 h 52 min 34 s, heure universelle**, et la graine officielle est son **1 842e tirage** [1]. Les chercheurs ont ensuite vérifié le résultat, puis l'ont publié le 16.10.2026.

4.4 Au total, **14 graines** sont expliquées, toutes produites entre mai 1997 et avril 1998. Il y a même une fausse piste amusante : pour quatre autres courbes (les courbes dites « binaires »), l'heure avait été divisée par deux ; lue telle quelle, elle tombe en février 1984, quatorze ans trop tôt ; corrigée, elle donne le 17 avril 1998 [1]. Dans le raisonnement enregistré

du modèle, une phrase : « This is astonishing: it solves the 25-year-old mystery » (« C’est stupéfiant : cela résout le mystère vieux de 25 ans ») [1].

4.5 La prime a été réclamée le 15.10.2026. Filippo Valsorda a refait le calcul de son côté, puis versé les 36 864 dollars à l’ISRG, l’association qui fait fonctionner Let’s Encrypt, l’organisme qui délivre gratuitement les certificats de sites web [3].

5. Ce que ça prouve, et ce que ça ne prouve pas

5.1 Les auteurs sont clairs : « This is not a cryptographic break, new attack, or weakness » (ce n’est ni une faille, ni une nouvelle attaque, ni une faiblesse). En revanche, la découverte « nous rend plus confiants » que les courbes ont été choisies sans porte dérobée [1]. C’est un gain de confiance, pas une preuve.

5.2 Pourquoi plus confiants ? Pour cacher un piège, il faudrait essayer énormément de graines et garder la bonne. Or, selon Valsorda, même en choisissant librement l’heure de départ et le numéro du tirage, il serait resté « à peine 30 bits de liberté », soit environ un milliard de choix : c’est beaucoup trop peu pour viser exprès une courbe piégée, qui serait rare. La méthode de triche imaginée en 2014 est donc écartée [3].

5.3 Des zones d’ombre demeurent, que les auteurs signalent eux-mêmes [1] :

- des tirages valides ont été sautés sans raison connue (pour P-256, le 876e convenait déjà) ;
- on ignore combien de fois le programme a tourné : « Nothing in the numbers shows how many runs there were » ;
- une graine (celle de la courbe B-163) et plusieurs autres paramètres restent inexpliqués.

5.4 Le bilan, à ce jour : le nombre mystère sortait d’un tirage lancé par une horloge ; un piège devient très improbable, sans être exclu par une preuve.

6. La serrure saine, mais pas éternelle

6.1 Cette partie est une mise en contexte de DEEO.AI : Anthropic ne relie pas sa découverte à la menace quantique.

6.2 Dès 1994, le mathématicien Peter Shor a montré qu'un ordinateur quantique assez grand casserait ces courbes, comme le chiffrement RSA. Assez grand, c'est combien ? Selon une estimation de chercheurs de Google publiée le 30.03.2026, moins de 500 000 qubits physiques (les briques de calcul de ces machines) suffiraient pour casser une courbe de cette taille en quelques minutes de calcul [7]. Les plus grosses machines d'aujourd'hui en sont encore très loin.

6.3 Le monde a commencé à changer de serrures. Le NIST a publié le 13.08.2024 trois normes dites « post-quantiques », conçues pour résister à ces machines [8]. Une ébauche de calendrier, publiée le 12.11.2024, propose d'interdire ces courbes après 2035 [9]. Chrome active par défaut un chiffrement hybride post-quantique depuis fin 2024 ; selon Cloudflare (07.04.2026), plus de 65 % du trafic humain qui le traverse est déjà protégé ainsi [10].

6.4 L'IA joue-t-elle un rôle de ce côté aussi ? La même semaine, Anthropic a publié avec des chercheurs de Harvard un article où Claude Mythos 5 a redessiné huit recettes de calcul quantique, et fait mieux que les meilleures publiées sur sept d'entre elles [11]. Ce sont des calculs sur papier, sans essai sur machine, dans un article pas encore relu par d'autres chercheurs ; et Anthropic ne relie pas ces circuits au chiffrement.

7. La question qui reste

7.1 Le cadenas d'Internet cachait-il un piège ? Rien ne le montre, et un piège devient très improbable. Le nombre mystère sortait d'un tirage lancé par une horloge, une nuit d'août 1997.

7.2 Une IA a mis moins d'une demi-heure à résoudre une énigme de plus de vingt-cinq ans. Combien d'autres secrets dorment encore dans nos vieux programmes ?

Sources

Consultées le 22.10.2026. Fiabilité indiquée en italique.

[1] Anthropic (J. Wood, H. de Valence, S. Weis et al., Frontier Red Team), « Claude reveals ECDSA curve origins », https://www.anthropic.com/research/ecdsa-curve-origins , 16.10.2026. *Source primaire (article des auteurs, avec le code et la table des graines).*

[2] Filippo Valsorda, billet annonçant la prime, https://words.filippo.io/seeds-bounty/ , 05.10.2023. *Source primaire (annonce de la prime).*

[3] Filippo Valsorda, billet sur la résolution et le versement de la prime, https://words.filippo.io/seeds-solved/ , octobre 2026. *Source primaire (vérification indépendante et versement de la prime) ; l'estimation de 30 bits est celle de l'auteur.*

[4] N. Koblitz et A. Menezes, « A Riddle Wrapped in an Enigma », https://eprint.iacr.org/2015/1018.pdf , 2015. *Article de recherche (synthèse du débat).*

[5] Dual_EC_DRBG, https://en.wikipedia.org/wiki/Dual_EC_DRBG (chronologie 2006–2015 et références). *Encyclopédie ; dates recoupées avec les sources citées par l'article.*

[6] NIST, FIPS 186-2, « Digital Signature Standard », 27.01.2000, https://csrc.nist.gov/files/pubs/fips/186-2/final/docs/fips186-2.pdf . *Norme officielle.*

[7] R. Babbush, C. Gidney, D. Boneh et al. (Google), estimation des ressources pour une courbe de 256 bits, https://arxiv.org/abs/2603.28846 , 30.03.2026. *Estimation de la source (prépublication).*

[8] NIST, FIPS 203 (et FIPS 204, 205), https://csrc.nist.gov/pubs/fips/203/final , 13.08.2024. *Norme officielle.*

[9] NIST IR 8547 (ébauche), « Transition to Post-Quantum Cryptography Standards », https://csrc.nist.gov/pubs/ir/8547/ipd , 12.11.2024. *Ébauche officielle, non définitive.*

[10] Cloudflare, feuille de route post-quantique, https://blog.cloudflare.com/post-quantum-roadmap/ , 07.04.2026. *Mesure de l'entreprise sur son propre trafic.*

[11] Anthropic, « Designing more efficient quantum circuits with Claude », https://www.anthropic.com/research/designing-efficient-quantum-circuits , 16.10.2026, et A. Gu, A. H. Kemeny, S. F. Yelin, M. D. Lukin et al., https://arxiv.org/abs/2610.22367 . *Source primaire ; estimations simulées, prépublication non relue.*

DEEO.AI cite ces sources et ne garantit pas leurs chiffres ; les estimations et déclarations restent sous la responsabilité de leurs auteurs.

SITUATION	Faits vérifiés au 22.10.2026, sur les sources primaires.
VIDÉO	La vidéo de cette actualité (10 min 05) est sur sa page de deeo.ai : https://deeo.ai/videos/veille-ia-hs-cadenas/
PARTAGE	Fiche en accès libre : vous pouvez la partager, en citant DEEO.AI.
CONTACT	admin@deeo.ai · deeo.ai

DEEO.AI

OBSERVATOIRE DE L'ÉMERGENCE DE L'IA