

MATHÉMATIQUES

Les standards cryptographiques du XXI^e siècle : AES et IEEE-P1363

Franck LEPRÉVOST (*Université Paris 6/université Grenoble 1*)

1. Introduction

L'UNE DES PRINCIPALES QUESTIONS de notre époque, tant du point de vue économique, sociologique que politique est : les consommateurs vont-ils rejoindre le cyberspace ? Va-t-on abandonner le fameux « merci de bien vouloir mettre la dinde (Noël approche à l'heure où nous écrivons ces lignes) dans mon panier » des marchés pour le « put it in the basket » des pages WEB ? La notion de commerce électronique est en train de s'établir. Cependant, les usagers potentiels rechignent encore à passer des ordres d'achat ou de vente online. La principale raison invoquée est le manque de sécurité technologique qu'ils ressentent, auquel s'ajoute un flou juridique gênant.

Nous donnons dans cet article un survol panoramique des concepts qui sous-tendent ces questions. Nous nous contenterons donc ici de présenter succinctement, dans la partie **2**, les enjeux et dispositions juridiques européennes concernant la cryptographie : la cryptographie est l'étude des techniques mathématiques relatives aux aspects de sécurité de l'information, telles celles concernant la confidentialité, l'intégrité ou l'authentification des données ou de leur origine. Les algorithmes utilisés se séparent en deux groupes : les cryptosystèmes symétriques ou à clef secrète et les cryptosystèmes asymétriques ou à clef publique. Une des contributions les plus importantes de la cryptographie à clef publique est la notion de signature électronique. Nous décrivons dans la partie **3** la philosophie sous-jacente aux cryptosystèmes à clef secrète. L'algorithme certainement le plus utilisé à l'heure actuelle est DES (Data Encryption Standard). Cet algorithme a été très longtemps soutenu politiquement, bien que les experts aient très tôt émis des réserves concernant son niveau de sécurité : à juste titre sait-on désormais (voir 3.2). Cela a eu comme conséquence que le NIST (National Institute for Standards and Technology) a demandé à la communauté cryptographique internationale de faire des propositions pour son successeur AES (Advanced Encryption Standard). Nous décrivons aussi bien les propriétés que l'AES doit remplir ainsi que les premiers résultats sur les candidats. La partie **4** décrit l'idée générale des algorithmes à clef publique. Parmi ceux-ci, RSA (d'après les noms des auteurs Rivest, Shamir et Adleman) est le plus couramment utilisé. Cet algorithme n'a pas été cassé jusqu'ici. Cependant, des faiblesses ont été mises en évidence dans certaines implémentations.

Malgré l'utilisation importante de RSA, des alternatives existent, telles celles basées sur les courbes elliptiques définies sur les corps finis. C'est le but du projet IEEE-P1363 de standardiser les algorithmes RSA, Diffie-Hellman et les algorithmes à base de courbes elliptiques. Dans la partie **5**, nous décrivons la technologie sous-jacente des signatures électroniques et présentons une nouvelle activité, à savoir celle d'autorité de certification. La partie **6** décrit ce que le futur de la cryptographie pourrait être. Si Dieu joue aux dés, des ordinateurs quantiques existeront et tous les algorithmes à clef publique utilisés actuellement succomberont à des attaques quantiques. En contrepartie, une théorie de la cryptographie quantique existe. Sa mise en pratique permettra l'implémentation d'algorithmes de cryptage absolument incassables.

L'objet du présent article est à la fois ambitieux et modeste : ambitieux par la variété des thèmes qu'il aborde et modeste par la profondeur accordée à chacun. Une étude, plus satisfaisante aussi bien pour le novice que l'expert, nécessiterait un (voire des) ouvrage(s) complet(s). Néanmoins, nous avons décidé d'illustrer notre propos en donnant quelques détails concernant les algorithmes de chiffrement symétrique DES, de chiffrement à clef publique RSA et de signature électronique à l'aide des courbes elliptiques. Le lecteur aura donc un panorama assez vaste et un guide vers des lectures plus complètes.

2. Enjeux et dispositions juridiques européennes

2.1. Enjeux

Les enjeux sont multiples. Nous en avons présenté un dès l'introduction de cet article. A titre d'illustration de notre propos, nous en privilégions ici un autre dont la grande presse s'est fait l'écho. Un article du *Figaro* ([17]) a rappelé aux lecteurs français l'existence du réseau Echelon (depuis le 21 novembre 1998, date de la première version de notre article, on peut trouver dans la presse internationale de très nombreux articles sur Echelon). Il s'agit d'un réseau satellitaire chargé d'écouter environ 100 millions de communications (téléphones, fax, emails) par mois. Sur des critères de mots-clés, ces messages sont retenus ou rejetés. Les messages retenus sont envoyés aux USA, où ils sont étudiés par le gouvernement américain. Il est aisé d'imaginer ce que la concurrence peut faire des informations glanées de la sorte au détriment des entreprises européennes (il est à noter que la Grande-Bretagne joue la main dans la main avec les USA sur ce réseau...). Le lecteur pense-t-il que le scénario imaginaire suivant soit fantaisiste : une entreprise européenne X décide de compléter son réseau international en achetant une entreprise Y japonaise, dont les produits et compétences s'intègrent parfaitement à la stratégie de X . X envoie donc un email, un fax ou passe un coup de fil à la filiale japonaise de Lazard Frères pour qu'ils approchent la société Y et fassent une étude financière de Y . Carte blanche leur est donnée à hauteur de 25 millions de dollars. Comme des chiffres très importants ont été utilisés, cette communication est interceptée par Echelon. En cette période de soldes en Asie, toute opportunité sur ce continent est à étudier, bien entendu y compris par l'entreprise américaine Z qui évolue sur le même marché que X . Si Z est bien informée par le réseau (un état cache-t-il des informations stratégiques aux entreprises qu'il finance ?), elle est libre

de faire une offre de 30 millions de dollars (les USA ne sont pas pingres, et savent mettre le prix pour satisfaire leurs besoins...) à *Y*, via Merrill Lynch par exemple. Un tel scénario, dont l'auteur tient expressément à préciser qu'il n'est que purement imaginaire, aurait de multiples conséquences :

– *X* a perdu une opportunité peut-être unique de s'étendre à l'international. Et bien évidemment, *X* a perdu de l'argent (transferts de fonds vers le Japon, frais de consultants de Lazard Frères, frais d'étude au siège, etc).

– Pour affaiblir encore davantage *X*, *Z*, toujours très bien informé, attend que les tractations entre *X* et *Y* soient très avancées. En effet, *X* doit payer le travail fait par Lazard Frères et chaque heure passée est une heure payée. *Z* a également profité de l'étude réalisée par Lazard (envoyée par email au siège européen de *X*), sans déboursier un cent. Ses frais engagés dans cette transaction sont minimes, puisque Merrill Lynch n'intervient en réalité que pour conclure l'affaire. *Z*, décidément très motivé, peut également recourir à la désinformation, en envoyant des mails à *Y* très déroutants et signés apparemment par *X*. Cela ajoute au discrédit de *X* aux yeux de *Y*.

Un scénario qui, lui, n'est pas imaginaire, est le manque à gagner de 30 milliards de francs qu'a subi Airbus Industrie lorsque le contrat historique avec l'Arabie Saoudite en 1994 ne lui a pas été attribué au profit, très déroutant, de McDonnell-Douglas. Un autre est tristement fourni par la firme allemande Enercon, qui a supprimé 300 emplois à la suite d'un acte d'espionnage industriel dû à la concurrence américaine. Que l'on se rassure : des exemples intra-européens d'espionnage industriel existent également...

Avant d'aborder les solutions techniques à ces problèmes (englobés à l'heure actuelle sous le concept d'intelligence économique), il est utile de savoir si leur utilisation est légale et donc de voir ce qu'il en est des dispositions juridiques relatives à la sécurité des systèmes d'information au niveau communautaire.

2.2. Dispositions juridiques européennes

L'objet ici n'est pas de donner un rapport exhaustif des dispositions de chacun des pays de la communauté en ce qui concerne la sécurité des systèmes d'information. Il est davantage de chercher à dégager les orientations communautaires dans ce domaine. A ce titre deux textes existent.

Le premier [7] est une communication de la DGXIII de la commission européenne placée sous la direction de Martin Bangemann. La nécessité de communications sécurisées y est soulignée, les solutions techniques aux problèmes d'authentification et d'intégrité (signatures électroniques) et de communications sécurisées (cryptographie) y sont présentées¹ et annoncent le document [8].

Le second [8] est une proposition de directive qui porte seulement sur les signatures électroniques. La communauté internationale a pris bonne note de cette proposition (voir [14]). Son principal impact concerne le commerce électronique, puisqu'elle a pour but de préciser au niveau communautaire la notion de signature électronique pour lui conférer le même statut juridique qu'une signature manuelle. Cette proposition nécessite l'approbation des 15 nations

¹ L'auteur a relevé de multiples erreurs dans la partie technique (voir [18]).

européennes pour acquérir force de loi. Même s'il s'agit d'harmoniser les législations des pays membres relatives aux signatures électroniques, il n'est pas certain que cette directive suffise à évacuer le risque de législations nationales divergentes. Un aspect positif est qu'une date limite est donnée : les états membres doivent prendre les mesures nécessaires pour se conformer avec la directive pour le 31 décembre 2000 (Article 13-1).

3. Cryptographie à clef secrète : AES

La cryptographie à clef secrète se sépare en deux catégories : les Stream Ciphers et les Blocks Ciphers. Nous nous intéressons ici seulement aux Blocks Ciphers.

3.1. Description de la cryptographie à clef secrète (Block Ciphers)

Un message est coupé en blocs de longueur N bits. A l'aide d'une clef secrète K de longueur L , on encode chaque bloc B . On récupère en sortie $A(K, B)$, où A désigne dans cette partie l'algorithme utilisé. Le réceptionnaire doit décoder $A(K, B)$ pour chaque bloc B . Il utilise pour cela la même clef secrète K . Il lui suffit alors de « recoller » les blocs B les uns aux autres pour récupérer le message original. Ces méthodes s'exposent à (au moins) deux problèmes :

- Comment est-ce que les intervenants se communiquent la clef secrète K ?
- Dans un réseau à n participants, il faut $n(n-1)/2$ clefs secrètes, ce qui pose des problèmes naturels de stockage et de sécurité.

3.2. DES : état de l'art

L'algorithme symétrique le plus utilisé actuellement est sans aucun doute DES. Il a été reconnu en 1977 comme FIPS (Federal Information Processing Standard), sous le numéro FIPS 46-2. DES utilise une clef de longueur 56 bits. Il y a donc 2^{56} clefs possibles. Les blocs, eux, ont une longueur de 64 bits.

En pratique, DES fonctionne de la manière suivante (voir [22], p. 252-256) : le chiffrement se fait sur 16 tours ; à partir de la clef K de 56 bits, on construit 16 clefs $(K_i)_{1 \leq i \leq 16}$ de 48 bits (une par tour). Pour chaque tour, on construit des S -boxes $S = (S_1, \dots, S_8)$. Les S_j sont des applications de substitution qui prennent 6 bits en entrée et renvoient 4 bits en sortie. Le bloc initial de 64 bits est divisé en deux moitiés de 32 bits : L_0 (L =left=gauche) et R_0 (R =right=droite). Chaque tour suit le même schéma : il prend en entrée 32 bits : L_{i-1} et R_{i-1} du tour précédent et produit de nouveau 32 bits L_i et R_i de la manière suivante :

$$L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus f(R_{i-1}, K_i),$$

où \oplus désigne XOR (l'exclusive-OR, qui obéit aux règles suivantes : $0 \oplus 1 = 1 \oplus 0 = 1$ et $0 \oplus 0 = 1 \oplus 1 = 0$), et $f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$. Ici E est une fonction fixée qui étend R_{i-1} de 32 bits à 48 bits, et P une permutation fixée sur 32 bits. Une permutation initiale IP des bits précède le premier tour. Après le dernier tour, les moitiés gauche et droite sont échangées et le texte est permuté bit-à-bit par IP^{-1} . Le déchiffrement suit le même algorithme avec la même clef K , mais simplement les sous-clefs sont appliquées dans le sens inverse.

DES a très longtemps profité du soutien politique des USA. Robert S. Litt (Principal Associate Deputy Attorney General) par exemple assurait encore le 17 mars 1998 ([5], p. 1-3), que le FBI n'avait aucune possibilité technologique et financière de décoder un message codé avec un algorithme symétrique dont la clef secrète a une longueur égale à 56 bits. Il complétait sa démonstration en déclarant que 14 000 PC Pentium durant 4 mois seraient nécessaires pour réaliser cela (voir également les déclarations de Louis J. Freeh (Directeur du FBI) et de William P. Crowell (Deputy Director de la NSA, [5], p. 1-2)).

Cependant, la Electronic Frontier Foundation a construit un DES-Cracker et l'a présenté durant la Rump-Session de Crypto'98 à Santa Barbara. On trouve la description de cette machine (valeur 250 000 dollars, design inclus) dans [5]. Mieux : il est expliqué comment scanner les plans de la machine, afin de reproduire une machine analogue (pour un prix maximal de 200 000 dollars, puisqu'il est inutile de repayer pour le design) à domicile. Cette machine est en mesure de trouver une clef secrète DES en 4 jours en moyenne. Cela a des conséquences politiques et diplomatiques : en effet, il semble accessible financièrement à toutes les nations de décoder les archives codées en DES qu'elle auraient pu constituer au cours des années. Pour le présent et le futur, il est désormais nécessaire de considérer comme peu sûrs tous les systèmes basés sur DES. En pratique, il est suggéré d'utiliser aujourd'hui au moins Triple-DES (mais là encore, il faut faire très attention...). Conscient de ces risques concernant DES, le NIST a demandé à la communauté cryptographique de réfléchir au successeur : AES.

3.3. AES

Les caractéristiques voulues de AES sont les suivantes : l'algorithme est un algorithme à clef secrète de type Block Cipher, il doit pouvoir accepter des combinaisons clefs-blocs de longueurs 128 – 128, 192 – 128 et 256 – 128 Bits. Les algorithmes utilisés dans AES seront libres de royalties et cela au niveau mondial. L'algorithme doit également être suffisamment flexible, par exemple pour autoriser d'autres combinaisons (blocs de longueur 64 Bits), efficace pour différentes plates-formes et applications (processeurs à 8-Bits, Réseaux ATM, communications satellitaires, HDTV, B-ISDN, etc.) et doit pouvoir être utilisé comme Stream Cipher, générateur de MAC, Pseudo-Random Number Generator, etc.

Ces multiples conditions ont été énoncées au cours du Pre-Round 1 (janvier 1997-juillet 1998) initié par le NIST. Le premier congrès AES s'est déroulé le 20 août 1998 (juste avant Crypto'98). A cette occasion ont été présentés les 15 (parmi 21) candidats retenus : CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOK197, MAGENTA, MARS, RC6, RIJNDAEL, SAFER+, SERPENT et TWOFISH. À l'issue de ce congrès, la discussion concernant les 15 candidats a immédiatement commencé ([15], [4], [21], [9], [10] et [28]). Le second congrès AES a eu lieu les 22-23 mars 1999 à Rome (juste avant le sixième Fast Software Encryption Workshop), et a terminé le Round 1.

Le 9 août 1999, le NIST a ouvert le Round 2 (qui se poursuivra jusqu'en mai 2000) et annoncé les 5 finalistes : MARS, RC6, RIJNDAEL, SERPENT et TWOFISH. La troisième conférence AES se tiendra du 13 au 14 avril 2000 à New

York, juste après le Fast Software Encryption Workshop 2000. Au cours de ce congrès, l'analyse technique des finalistes sera présentée et discutée. Cette analyse se poursuit actuellement, éventuellement jusqu'en automne 2000, même si les résultats des évaluations hardware des finalistes sont disponibles depuis le 15 mai 2000. Dès lors que le vainqueur sera connu, après une dernière période d'examen de six à neuf mois supplémentaires, cet algorithme sera proposé comme FIPS. Il est prévu que l'AES devienne un FIPS vers 2001.

4. Cryptographie à clef publique : IEEE-P1363

4.1. Description de la cryptographie à clef publique

Contrairement aux algorithmes à clef secrète, les algorithmes à clef publique nécessitent 2 clefs par utilisateur. Étant donné un algorithme (voir ci-dessous pour cela), Alice (resp. Bob) choisit une clef secrète x_A (resp. x_B) et publie (par exemple dans un annuaire) une clef publique y_A (resp. y_B). Bob encode son message M avec y_A et l'envoie à Alice. Seule Alice peut, avec sa clef secrète x_A , décoder le message.

Les algorithmes à clef publique sont basés sur des problèmes mathématiques :

- Factorisation de grands entiers : RSA et Rabin-Williams.
- Problème du Log Discret : DSA (Digital Signature Algorithm), échange de clef de Diffie-Hellman, méthode de codage de El Gamal et signature électronique de El Gamal, de Schnorr et de Nyberg-Rueppel.
- Problème du Log Discret pour les courbes elliptiques : les analogues des algorithmes ci-dessus pour les courbes elliptiques. On considère une courbe elliptique E définie sur un corps fini, tels \mathbf{F}_p ou \mathbf{F}_{2^n} . Il est essentiel de pouvoir calculer rapidement le nombre de points rationnels de la courbe elliptique sur le corps fini considéré. En général, on utilise pour cela une méthode due à Schoof-Elkies-Atkin (dénommée SEA depuis). Dans certains cas (courbes de Koblitz ou courbes à multiplication complexe), ce nombre est très aisément calculable.

Nous illustrons notre propos en décrivant la méthode de chiffrement et déchiffrement RSA ([27]). Il y a trois étapes : création des clefs, chiffrement et déchiffrement.

(i) Création de clefs pour le chiffrement. Chaque entité A procède de la manière suivante :

- (i.1) A génère deux grands nombres premiers p, q , distincts de taille comparable.
- (i.2) A calcule le module $n = pq$ et $\psi = (p - 1)(q - 1)$.
- (i.3) A choisit e tel que $1 < e < \psi$ et $\text{pgcd}(e, \psi) = 1$.
- (i.4) A calcule (par l'algorithme d'Euclide) l'unique d tel que $1 < d < \psi$ et $ed \equiv 1 \pmod{\psi}$.
- (i.5) La clef publique de A est (n, e) . La clef secrète de A est d .

(ii) Chiffrement. B chiffre le message m pour le destinataire A :

- (ii.1) B récupère la clef publique (n, e) de A .
- (ii.2) B représente le message comme un entier $m \in [0, n - 1]$.

(ii.3) B envoie $c = m^e \pmod n$ à A .

(iii) Déchiffrement : A calcule $m = c^d \pmod n$.

Il est aisé de vérifier que cet algorithme est correct. En effet, comme $ed \equiv 1 \pmod{\psi}$, il existe k tel que $ed = 1 + k\psi$. Si $\text{pgcd}(m, p) = 1$, alors le (petit) théorème de Fermat montre que $m^{p-1} \equiv 1 \pmod p$, et donc

$$m^{1+k(p-1)(q-1)} \equiv m \pmod p.$$

Si $\text{pgcd}(m, p) = p$, l'équation ci-dessus est également vérifiée, car chaque membre est nul modulo p . Par conséquent, dans tous les cas, on a

$$m^{ed} \equiv m \pmod p.$$

De la même manière, on a $m^{ed} \equiv m \pmod q$. Comme $p \neq q$, on a donc

$$m^{ed} \equiv m \pmod n,$$

et donc $c^d \equiv (m^e)^d \equiv m \pmod n$.

Les cryptosystèmes à clef publique sont sujets à des attaques :

– Factorisation de grands entiers : on utilise la méthode ECM (Elliptic Curve Factoring Method) de H. Lenstra pour trouver les petits facteurs (P. Montgomery a trouvé ainsi le 27 novembre 1995 un nombre premier de 47 décimales, soit 157 bits, qui factorise un entier de 135 décimales, soit 449 bits). A l'heure actuelle, on utilise QFS (Quadratic Field Sieve). Par cette méthode, A. Lenstra et al. ont factorisé en 1994 un nombre de 129 décimales, soit 429 bits et ainsi résolu un défi lancé en 1977 par la société RSA ou NSF (Number Field Sieve). Par cette méthode, A. Lenstra et al. ont factorisé en 1996 un nombre de 130 décimales, soit 432 bits pour trouver les gros facteurs. A l'heure actuelle, il ne faut plus considérer 512 bits comme cryptographiquement sûrs.

Par ailleurs, une faiblesse a été trouvée dans l'implémentation de PKCS # 1 v. 1 ([2]) : Avec 300 000 à 2 millions d'attaques de type Chosen-Ciphertext, les serveurs de type SSL (v. 3.0) n'offrent plus de sécurité raisonnable. Ce problème est résolu dans PKCS # 1, v. 2.

– Problème du Log discret : pour résoudre ce problème, on peut utiliser la méthode du calcul d'indices (ce que font Weber, Demy et Zayer pour résoudre le Log Discret pour p premier de longueur 248 bits) ou encore la méthode NSF.

– Problème du Log discret pour les courbes elliptiques : si on travaille dans le groupe d'ordre m engendré par $P \in E(\mathbf{F}_q)$, les résultats de [25] imposent que m soit premier. Une attaque bien connue est la méthode ρ de Pollard (voir [26]). Elle peut d'ailleurs être parallélisée. Il y a également des restrictions sur les courbes à considérer : le nombre de points de la courbe elliptique considérée sur \mathbf{F}_p ($p > 3$) doit être différent de $p + 1$ (courbes elliptiques supersingulières) et de p (courbes elliptiques anormales).

Remarque : à la place du groupe des points rationnels de courbes elliptiques définies sur un corps fini, on peut également utiliser d'autres groupes adaptés du point de vue cryptographique, par exemple les variétés jacobiniennes de courbes (convenablement choisies) de genre ≥ 2 définies sur des corps finis. Dans ce contexte, on dispose également de variétés abéliennes à multiplication complexe

ou réelle, pour lesquelles il est (relativement) aisé de déterminer le nombre de points rationnels.

4.2. Cryptographie symétrique ou à clef publique : que choisir ?

A ce stade, le lecteur est maintenant parfaitement au courant des techniques de cryptographie symétrique et de celles relevant de la cryptographie à clef publique. La question naturelle est : que choisir ? Réponse : tout !

En effet, pour communiquer un document de manière sécurisée sur un canal ouvert (Internet), la solution consiste à combiner les deux techniques. Par exemple, Alice vivant à Paris veut envoyer par mail un rapport de 15 pages à Bob qui habite Londres. Il est hors de question pour Alice d'aller à Londres remettre une clef secrète d'AES à Bob. Si elle choisissait cette méthode coûteuse, autant qu'elle remette directement le document. Alice et Bob pourraient bien entendu choisir de communiquer à l'aide des techniques de la cryptographie à clef publique, comme décrit plus haut. Seulement le problème est que le chiffrement est environ 1000 fois plus lent pour ces techniques que pour les cryptosystèmes à clef secrète. La solution la plus pratique est la suivante :

- Alice envoie un message K de 128 bits à Bob à l'aide de la cryptographie à clef publique. L'utilisation des techniques à clef publique se justifie, car la taille du message à transmettre est très courte (128 bits dans notre cas). A ce stade, Alice et Bob partagent le secret K .

- Comme convenu de manière standard entre eux, K est la clef secrète d'un algorithme à clef secrète, tel AES.

- Alice et Bob oublient la technologie à clef publique. Pour la suite de leurs communications, ils utilisent AES avec la clef K pour communiquer. C'est ainsi qu'Alice peut maintenant envoyer son document de 15 pages à Bob pour le prix d'une communication téléphonique au lieu d'un aller-retour en première classe sur British Airways (Alice, voulant que son document et elle-même arrivent à bon port, aurait bien évidemment choisi en conséquence sa compagnie aérienne).

Encore faut-il que les systèmes d'Alice et Bob soient compatibles : le but des démarches de standardisation décrites ci-dessous est précisément de favoriser l'harmonie des communications.

4.3. IEEE-P1363 et autres standards

Le projet P1363 a commencé en 1993 sous l'égide du comité de standardisation de l'IEEE. Il a pour but d'améliorer les communications entre plusieurs familles de cryptosystèmes à clef publique : RSA, El Gamal, Diffie-Hellman et courbes elliptiques. Depuis la fin de 1996, l'ensemble des techniques considérées par P1363 est relativement stable et regroupé dans un document ([24]).

Le document [24] est formé d'une partie principale et d'annexes.

La partie principale est scindée en 14 sections.

- La section 1 est un survol général.
- La section 2 fournit des références pour les autres standards (voir plus bas).
- La section 3 définit les termes utilisés dans le document.

- La section 4 donne un survol des types de techniques cryptographiques utilisées dans le document.
- La section 5 donne des conventions mathématiques utilisées dans ce standard, ainsi que leurs notations et représentations. Elle précise également les formats à utiliser ainsi que les primitives pour les conversions des types de données.
- Les sections 6, 7, 8, 9, 10 et 11 définissent les trois familles de techniques cryptographiques évoquées en 4.1.
- La section 12 définit les méthodes de codage pour la signature et le chiffrement.
- La section 13 définit les fonctions d'obtention des clefs pour les schémas d'échanges de clefs de la section 9.
- La section 14 définit des fonctions auxiliaires qui supportent les techniques des sections 12 et 13.

Les six annexes ne sont données qu'à titre d'information et portent sur les considérations suivantes : l'annexe A concerne les rappels de théorie des nombres nécessaires, l'annexe B les concepts de conformité, l'annexe C ceux de rationalité, l'annexe D les considérations de sécurité, l'annexe E les formats et l'annexe F une bibliographie.

Le standard (draft version 7) a été révisé par un groupe d'experts de l'IEEE Standards Association : ce groupe a commencé son travail vers le 15 janvier 1999 et remis ses premières conclusions en mars 1999. Le draft version 9 a été accepté par le ballot group. Néanmoins, un certain nombre de votes ont été négatifs et le groupe d'expert a répondu aux commentaires. Suite à des attaques sur certains protocoles, le processus a subi un certain retard. Finalement, le draft version 13 a été adopté comme standard IEEE en février 2000.

Le standard IEEE-P1363 a une interactivité très importante avec d'autres standards, tels par exemple ANSI X9.42, ANSI X9.62, ANSI X9.63 de l'industrie bancaire. Les techniques décrites dans ces standards sont nécessaires à la mise en place d'autres protocoles, comme X509 ([12]) et S-MIME ([13]) par exemple.

Des techniques supplémentaires peuvent être trouvées dans le projet P1363A, que nous ne discutons pas ici. Disons seulement que l'Europe, en l'occurrence la Technische Universität Berlin, a accueilli du 15 au 17 mars 2000 le groupe de travail planchant sur ce projet.

Cette rencontre a été co-organisée par l'auteur, membre du groupe d'experts en charge de l'évaluation des normes P1363 et P1363A et par Rüdi Seiler, doyen du département de mathématiques de la TUB et directeur de la société Algovision (cotée à l'EASDAQ). Cette rencontre a été un succès : la participation a été double de celle des rencontres analogues aux USA avec en particulier des représentants des sociétés IBM, RSA, Certicom, Pitney, NTRU, Deutsch Telekom, Smartring, Wave communication, NTT et des universités de Paris, Berlin, Braunschweig, Bonn, Toronto.

5. Signatures électroniques

Les signatures électroniques (ou digitales) sont utilisées pour prouver l'authenticité et l'intégrité des données. A la différence d'une signature manuelle, elles dépendent du document à signer.

5.1. Description du schéma de signature d'El Gamal pour les courbes elliptiques

Étant donné $P \in E(\mathbf{F}_p)$ d'ordre l premier, Alice veut signer le document M . Tout d'abord, Alice se donne deux fonctions f_1 et f_2 . La fonction f_1 applique tout message M vers $\mathbf{Z}/l\mathbf{Z}$: par exemple, une fonction f_1 convenable consiste à numériser M , à le couper en morceaux de taille l , et additionner les morceaux modulo l . La fonction f_2 envoie tout élément $R \in \langle P \rangle$ dans $\mathbf{Z}/l\mathbf{Z}$: par exemple, il suffit de concaténer les coordonnées de R et de réduire modulo l . Alice choisit au hasard $x \in \{1, \dots, l\}$ secret et publie $Y = x.P \in \langle P \rangle$.

(i) Création de la signature de M : Alice choisit $k \in \{1, \dots, l-1\}$ au hasard et calcule $R = k.P \in \langle P \rangle$. Alice calcule ensuite s tel que $f_1(M) = x.f_2(R) + ks \pmod{l}$. La signature d'Alice du document M est le couple (R, s) .

(ii) Vérification de la signature : si l'équation

$$f_1(M).P = f_2(R).Y + s.R$$

est vérifiée dans $\langle P \rangle$, alors la signature est valide. Trouver la clef secrète revient à résoudre dans $\langle P \rangle$ l'équation en x

$$f_1(M).P = (x.f_2(R)).P + s.k.P,$$

ce qui revient à chercher à résoudre le problème du log discret dans $\langle P \rangle$.

5.2. Description de la technologie

En pratique, pour des raisons de rapidité, on ne signe pas (au sens strict du mot) un fichier, mais le résultat donné par l'application d'une fonction de hachage à ce fichier. Une fonction de hachage est une fonction qui prend en entrée (input) un fichier de n'importe quelle taille et génère une sortie (output) de taille fixée. Pour les besoins de la cause, nous prenons l'exemple de la fonction (européenne) RIPEMD-160, pour laquelle la taille en sortie est de 160 bits. Une bonne fonction de hachage doit satisfaire à diverses propriétés (impossibilité technique de fabriquer une pré-image ou encore one-way function, résistance aux collisions, etc). En l'état actuel des connaissances, c'est le cas de RIPEMD-160.

Les différentes étapes typiques de constitution de la signature électronique d'un document peuvent être décrites comme suit (il y a d'autres choix possibles) :

- Une paire unique de clefs cryptographiques (pour la technologie à clef publique) est fournie à Alice (ou générée par elle).
- Avec RIPEMD-160, Alice hache son message M et récupère un output MD (comme Message Digest).

- Alice signe MD avec sa clef secrète, via un algorithme de signature électronique. La signature électronique S consiste en le résultat de cette opération.
- Alice ajoute S au message M et envoie le tout électroniquement à Bob.

De son côté, Bob reçoit le message $M + S$ de Alice. Il veut vérifier l'authenticité de l'origine de ce message.

- Bob sépare M de S . Il applique de nouveau RIPEMD-160 à M et récupère un output MD .
- Bob utilise la clef publique d'Alice pour vérifier que S est bien la signature électronique de MD émanant de Alice. S'il n'y a aucune altération (tous les bits sont égaux), alors il sait que les données n'ont pas été altérées après la signature.
- Bob reçoit un certificat d'une autorité de certification (ou de Alice elle-même). Ce certificat confirme la signature digitale sur les données de Alice. Le certificat contient la clef publique, le nom (ou pseudonyme) d'Alice (éventuellement d'autres informations) et le tout est signé digitalement par l'autorité de certification.

Remarque : Pour d'autres aspects et applications, le lecteur peut consulter [16] et [20].

5.3. Autorités de certification

Dans la partie précédente, on a vu le rôle crucial joué par les autorités de certification (CA). Il s'agit d'un secteur d'activités complètement nouveau. Nous décrivons ici en quoi il consiste.

La tâche centrale du CA est d'authentifier le possédant et les caractéristiques d'une clef publique de sorte à ce qu'elles soient considérées comme de confiance. Une fois que le CA est persuadé que ces critères sont satisfaits, un certificat est généré contenant cette clef et d'autres détails. Ce certificat est lui-même signé digitalement par le CA (et donc avec la clef secrète du CA) pour établir la corrélation avec le possesseur de la clef. Si le CA publie sa clef publique, alors une vérification automatique est possible par tout récipiendaire. Cependant, il est nécessaire que le récipiendaire du certificat fasse confiance au CA. Toutes les parties doivent donc faire confiance au CA. Il résulte de cela que plusieurs catégories de certificats peuvent être concus. Par exemple la clef publique d'un CA peut être signée digitalement par un autre CA et donner naissance ainsi à une hiérarchie de CA. Une clef publique peut aussi être certifiée par plusieurs CA.

Un exemple de certificat est donné ci-dessous :

- Nom ou pseudonyme du signataire.
- Nom du CA.
- Clef publique du signataire.
- Algorithme, type de clef.
- Profession, position dans une organisation, qualifications, documents officiels relatifs au signataire.
- Limites juridiques.
- Confirmation de la révélation des vrais interlocuteurs (en cas de pseudonymes) en cas de conflit.

– Date d’expiration du certificat.

6. Dieu joue-t-il aux dés ?

Peter Shor de AT & T Bell Labs a remporté en août 1998 le Prix Nevanlinna, qui lui a été remis au cours de l’*International Congress of Mathematicians* à Berlin. Il est l’un des fondateurs de la cryptanalyse quantique (la cryptanalyse est l’activité qui consiste à « casser » des algorithmes cryptographiques). Il a développé des méthodes basées sur la physique quantique pour factoriser en temps polynomial de grands nombres ([29]) ou pour résoudre le problème du Log Discret, également lorsqu’il est formulé dans le cadre général des variétés abéliennes ([30]). Les travaux de Shor faisant l’objet d’un article de la *Gazette* ([19]), nous n’entrons pas ici dans les détails de ces résultats.

Malgré cela, IEEE-P1363 reste actuel : ces algorithmes de Shor nécessitent un ordinateur quantique puissant. Selon l’avis de Shor lui-même ([30]), on ne disposera d’un coprocesseur quantique (et rien que cela !) au plus tôt dans 10 ans, et cela bien que le département recherche (DARPA) du Pentagone investisse annuellement 5 millions de dollars dans ce projet. Un projet européen analogue existe : neuf groupes de recherche se sont unis dans le Quantum Information European Research Network (et se sont d’ailleurs réunis du 24 au 26 septembre 1998 au cours de l’*International Workshop on Physics of Quantum Information*). Imaginons qu’un tel ordinateur quantique existe dans 30, 40 ou 100 ans : le jour même où un tel ordinateur quantique existera, il rendra obsolète la cryptographie à clef publique décrite dans la section 4. Le pigeon voyageur pourra-t-il se réjouir d’un rebond de carrière ?

Une théorie de la cryptographie quantique existe, plus précisément du partage quantique de clefs ([1], voir [3] pour une bibliographie sur le sujet). Elle constitue donc une alternative à la cryptographie à clef publique. La problématique est similaire à celle exposée dans la partie 4.2 : Alice et Bob veulent de nouveau partager un secret commun qu’ils pourront alors utiliser comme clef secrète d’un protocole symétrique (comme AES). S’ils utilisent seulement une ligne téléphonique, ils n’ont d’autre recours que d’utiliser la cryptographie à clef publique. Si leur communication est écoutée par un attaquant muni d’un ordinateur quantique puissant, ils sont exposés aux attaques évoquées plus haut. Cependant, si en plus ils ont une fibre optique à disposition sur laquelle ils peuvent transmettre des états quantiques, ils peuvent utiliser la cryptographie quantique. Par exemple Alice transmet des états choisis aléatoirement dans un ensemble d’états quantiques non orthogonaux (par exemple $V_0, V_1, \frac{1}{\sqrt{2}}(V_0 + V_1), \frac{1}{\sqrt{2}}(V_0 - V_1)$). Nous n’entrons pas dans les détails ici et renvoyons à [19] pour les notations, qui ne sont données ici qu’à titre d’illustration). Bob lit les états soit dans la base $\{V_0, V_1\}$ ou dans la base $\{\frac{1}{\sqrt{2}}(V_0 + V_1), \frac{1}{\sqrt{2}}(V_0 - V_1)\}$, de nouveau choisie aléatoirement. A l’aide d’un protocole spécial sur le canal classique, Alice et Bob peuvent décider des états sur lesquels ils sont d’accord dans la base de mesure. Ils doivent être d’accord pour environ la moitié des états. Chacun de ces états fournit un bit de la clef secrète. Un attaquant qui écoute la conversation n’a gagné à peu près aucune information, puisqu’il ne sait pas dans quelle base les états sont transmis et que

toute information qu'il capture entraîne un dérangement des états (au moins 1/4 des orientations des polarisations des photons sont modifiées), ce que Alice et Bob notent immédiatement en mesurant certains de leurs états au lieu de les utiliser comme éléments de la clef secrète. Ils peuvent également sacrifier certains des bits pour s'assurer que l'attaquant ne gagne aucune information sur les bits restants de la clef, sur laquelle ils s'accordent alors.

Si la théorie remonte à 1982-84 ([1]), les années 1990 ont vu les premières réalisations (voir [11] pour cet historique). En 1990-92 une première expérimentation à l'air libre sur une longueur de 30 cm a été initiée par IBM. En 1993-95, DRA et British Telecom ont réalisé une expérience sur fibres optiques sur une longueur de 10 à 30 km. En 1996, Swiss Telekom a réalisé de telles expériences sur une fibre de 23 km sous le lac Léman. En 1997, Los Alamos National Lab a mené à bien de telles expériences sur une fibre optique de 48 km et en 1998 à l'air libre sur une longueur de 1 km.

7. Conclusion

Nous avons décrit succinctement dans cet article certains des enjeux et risques que recèle la sécurité des systèmes d'information. L'unité de mesure financière de ces enjeux est le milliard de dollar ou d'euro (il est à noter qu'une devise se porte mieux que l'autre, tout du moins en ce moment...). L'unité de mesure politique est le secret d'Etat. Du point de vue communautaire, l'impact économique est la santé des entreprises européennes. Nous avons donné un aperçu très partiel malheureusement des orientations juridiques communautaires et des solutions technologiques.

A un moment où il est légitime de s'interroger sur les débouchés offerts par un DEA et/ou un doctorat en mathématiques, il nous paraît important de souligner que la sécurité des systèmes d'informations est un domaine riche d'opportunités pour notre discipline.

En effet, ce domaine fait appel à des connaissances très fines en ce qui concerne le traitement du signal (watermarking et information hiding), la réduction des réseaux (algorithmes LLL, etc.) ou encore les opérateurs de Hecke!

Nous utilisons ces dernières lignes pour signaler le bulletin de presse du Department of Commerce US du 13 janvier 2000, où est décrite la suppression quasi-totale des restrictions à l'exportation des logiciels cryptographiques américains. Jusqu'alors, l'Europe pouvait espérer un marché égal à la planète moins les USA, puisque les USA n'autorisaient à l'exportation que des solutions à faible sécurité (40 bits) et restreignaient très fortement les importations des produits dans ce domaine. Ce n'est désormais plus le cas. Il sera donc à l'avenir d'autant plus recommandé de se méfier des solutions proposées, afin d'échapper autant que faire se peut aux trap-doors, comme celles qu'avaient eu la surprise de découvrir les 500 000 utilisateurs suédois de Lotus — en particulier plusieurs ministères — il y a quelques années...

Références

- [1] *C. H. Bennett, G. Brassard* : Quantum cryptography : public key distribution and coin tossing, in Proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (1984).
- [2] *D. Bleichenbacher* : Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS # 1, Advances in Cryptology-Crypto'98, LNCS 1462, Springer (1998)
- [3] *G. Brassard* : Quantum cryptography : a bibliography, SIGACT News 24 : 3 (1993). Une version plus récente est accessible online à <http://www.iro.umontreal.ca/~crepeau/Biblio-QC.html>
- [4] *CAESar Project* : <http://www.dice.ucl.ac.be/crypto/CAESAR/caesar.html>
- [5] *Electronic Frontier Foundation* : Cracking DES, Secrets of Encryption Research, Wiretap Politics & Chip Design, O'Reilly (1998)
- [6] *T. El Gamal* : A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory **31**, p. 469-472 (1985)
- [7] *European Commission, Directorate-General XIII* : Communication from the commission to the European parliament, the council, the economic and social committee and the committee of the regions ensuring security and trust in electronic communications. Towards a European framework for digital signatures and encryption (1997)
- [8] *European Commission, Directorate-General XIII* : Proposal for a European parliament and council directive on a common framework for electronic signatures (1998)
- [9] *B. Gladman* : AES Algorithm Efficiency.
http://www.seven77.demon.co.uk/cryptography_technology/Aes/
- [10] *L. Granboulan* : Analysis. <http://www.dmi.ens.fr/~granboul/recherche/AES.html>
- [11] *P. Guillot* : Crypto quantique pour le partage de clefs. Texte de conférence au séminaire IC5 (Séminaire d'information sur le codage, la cryptographie, la complexité, la compression et le calcul formel) de la direction générale pour l'Armement (5/6/1998)
- [12] IETF-PKIX, *Public-Key Infrastructure (x509)* : <http://www.ietf.org/html.charters/pkix-charter.html>
- [13] IETF-S/MIME, *Mail Security (smime)* : <http://www.ietf.org/html.charters/smime-charter.html>
- [14] *International Herald Tribune* : EU unveils a draft law for internet, p. 17 (19/11/1998)
- [15] *L. Knudsen, V. Rijmen* : Block Cipher Lounge.
<http://www.iu.uib.no/~larsr/aes.html>
- [16] *M. Kutter, F. Leprévost* : Symbiose von Kryptographie und digitalen Wasserzeichen : effizienter Schutz des Urheberrechtes digitaler Medien, à paraître dans le Tagungsband des 6. Deutschen IT-Sicherheitskongress des BSI (1999)
- [17] *Le Figaro* : Article de C. Doré et J. Fleury (19-20/9/1998)
- [18] *F. Leprévost* : Lettre à la DGXIII (en préparation, novembre 1998)
- [19] *F. Leprévost* : Peter Shor, Prix Nevanlinna 1998. *La Gazette des mathématiciens* **81** (1999)
- [20] *F. Leprévost, M. Kutter, T. Ebrahimi* : Efficient copyright protection of multimedia data through the combination of cryptography and digital watermarking. En préparation (1999-2000)
- [21] *H. Lipma* : Efficiency Testing table. <http://home.cyber.ee/helger/aes/>
- [22] *A. J. Menezes, P. C. van Oorschot, S. A. Vanstone* : Handbook of applied cryptography, CRC Press (1996)
- [23] NIST AES *Home Page* : http://csrc.nist.gov/encryption/aes/aes_home.htm
- [24] IEEE-P1363 : <http://grouper.ieee.org/groups/1363/index.html>
- [25] *S. Pohlig, M. Hellman* : An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance, IEEE Transactions on Information Theory **24**, p. 106-110 (1978)
- [26] *J. Pollard* : Monte Carlo methods for index computation mod p , Maths. Comp. **32**, p. 918-924 (1978)
- [27] *R. L. Rivest, A. Shamir, L. M. Adleman* : A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM **21**, p. 120-126 (1978)

- [28] *B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson* : Performance comparisons of the AES candidates.
<http://www.counterpane.com/AES-performance.html>
- [29] *P. Shor* : Quantum Computing, Proceedings of the International Congress of Mathematicians, Berlin, Documenta Mathematica, Journal der Deutschen Mathematiker-Vereinigung (1998)
- [30] *P. Shor* : Communication personnelle (1998)

Solutions exactes et solutions approchées d'équations polynomiales

François Loeser (Université Paris 6)

1. – Préliminaires et présentation du problème

ON CONSIDÈRE dans ce texte des systèmes d'équations polynomiales à coefficients dans le corps \mathbb{C} des nombres complexes. Un tel système correspond à la donnée de r polynômes F_1, \dots, F_r appartenant à l'algèbre $\mathbb{C}[x_1, \dots, x_m]$ des polynômes en m variables à coefficients complexes. On note $Z(F)$ l'ensemble des solutions dans \mathbb{C}^m du système

$$(F) = \begin{cases} F_1(x_1, \dots, x_m) = 0 \\ \dots \\ F_r(x_1, \dots, x_m) = 0. \end{cases}$$

Une partie de \mathbb{C}^m de la forme $Z(F)$ est appelée *sous-ensemble algébrique* de \mathbb{C}^m .

On peut également s'intéresser aux séries qui sont solutions du système (F) . Plus précisément, on considère l'ensemble des m -uplets de séries formelles, ou « arcs formels »,

$$x_i(t) = \sum_{j \in \mathbb{N}} a_{i,j} t^j,$$

avec $a_{i,j}$ appartenant à \mathbb{C} , qui sont solutions du système (F) , c'est-à-dire telles que les séries $F_k(x_1(t), \dots, x_m(t))$ obtenues par substitution soient identiquement nulles pour $1 \leq k \leq r$. On note $Z_\infty(F)$ ce sous-ensemble de $\mathbb{C}[[t]]^m$. On pourrait aussi considérer les séries convergentes qui sont solutions du système (F) , mais, pour ce qui nous concerne ici, la recherche de solutions convergentes est essentiellement équivalente à celle de solutions formelles, au vu du résultat suivant de M. Artin :

Théorème 1.1 ([1]). *Soit $(x_1(t), \dots, x_m(t))$ un m -uplet de séries formelles solution du système (F) . Pour tout entier $n \geq 0$, il existe un m -uplet de séries convergeant au voisinage de l'origine, $(\tilde{x}_1(t), \dots, \tilde{x}_m(t))$, solution du système (F) , et vérifiant*

$$x_i(t) \equiv \tilde{x}_i(t) \pmod{t^{n+1}},$$

pour $1 \leq i \leq m$.

Comment trouver les solutions séries formelles du système (F) ? L'approche naturelle consiste à procéder par approximations successives : à partir d'une solution approchée donnée, disons modulo t^{n+1} , c'est-à-dire d'un m -uplet de séries formelles $(x_1(t), \dots, x_m(t))$ telles que les séries $F_k(x_1(t), \dots, x_m(t))$ obtenues par substitution soient toutes divisibles par t^{n+1} , on cherche à construire une solution modulo t^{n+2} . Comme le fait d'être une solution approchée modulo t^{n+1} ne dépend clairement pas des termes d'ordre $\geq n+1$ apparaissant dans les

séries $x_i(t)$, il sera plus commode de considérer les solutions approchées modulo t^{n+1} comme des éléments de $(\mathbb{C}[t]/t^{n+1}\mathbb{C}[t])^m$, via le morphisme de troncation

$$\tau_n : \mathbb{C}[[t]]^m \rightarrow (\mathbb{C}[t]/t^{n+1}\mathbb{C}[t])^m.$$

Pour $n' \geq n$, on dispose également d'un morphisme de troncation

$$\tau_{n',n} : (\mathbb{C}[t]/t^{n'+1}\mathbb{C}[t])^m \rightarrow (\mathbb{C}[t]/t^{n+1}\mathbb{C}[t])^m.$$

Bien entendu, on a une identification naturelle $\mathbb{C}[t]/t^{n+1}\mathbb{C}[t] \simeq \mathbb{C}^{n+1}$. On note $Z_n(F)$ le sous-ensemble de $(\mathbb{C}[t]/t^{n+1}\mathbb{C}[t])^m$ formé des solutions approchées de (F) modulo t^{n+1} . Pour une solution approchée modulo t^{n+1} , se relever en une vraie solution est par définition équivalent à être dans l'image de $Z_\infty(F)$ par τ_n ; de même se relever en une solution approchée modulo $t^{n'+1}$ équivaut à être dans l'image de $Z_{n'}(F)$ par $\tau_{n',n}$. On remarquera que, avec nos notations, $Z_0(F)$ s'identifie naturellement à $Z(F)$.

Il est important de remarquer que, en général, une solution approchée modulo t^{n+1} ne se relève pas nécessairement en une solution approchée modulo t^{n+2} . En effet, considérons le système F composé uniquement de l'équation à 2 variables $x_1^2 - x_2^3 = 0$: le couple $(x_1(t) = t, x_2(t) = t)$ est une solution approchée modulo t^2 qui n'admet aucun relèvement en une solution approchée modulo t^3 (et encore moins en une vraie solution !). Ceci est lié au fait que l'origine est un point singulier de la courbe d'équation $x_1^2 - x_2^3 = 0$ dans \mathbb{C}^2 ; plus généralement, pour F quelconque, l'obstruction à relever les solutions approchées provient des points singuliers de $Z(F)$, c'est-à-dire des points au voisinage desquels $Z(F)$ n'est pas une variété analytique complexe.

En théorie, il est facile de tester si une solution approchée modulo t^{n+1} se relève ou non modulo $t^{n'+1}$: on part d'une solution approchée $(x_1^0(t), \dots, x_m^0(t))$ modulo t^{n+1} , vue comme m -uplet de polynômes de degré $\leq n$, on considère un m -uplet $(x_1(t), \dots, x_m(t))$ de polynômes de degré $\leq n'$ se projetant sur $(x_1^0(t), \dots, x_m^0(t))$, et on développe les séries $F_i(x_1(t), \dots, x_m(t))$ à l'ordre n' . La condition pour ces séries d'être nulles à l'ordre n' se traduit par un nombre fini d'équations polynomiales portant sur les $m(n - n')$ coefficients indéterminés. Le relèvement existe si et seulement si ce système admet une solution dans $\mathbb{C}^{m(n-n')}$.

D'après le résultat fondamental suivant, dû à M. Greenberg, pour savoir si une solution approchée modulo t^{n+1} se relève en une **vraie** solution, il suffit de savoir si elle se relève en une solution approchée modulo $t^{\gamma(n)+1}$, avec $\gamma(n)$ un entier $\geq n$ ne dépendant que de n et de (F) , ce qui peut être vérifié par la méthode précédente.

Théorème 1.2 ([6]). *Pour tout entier $n \geq 0$, il existe un entier $\gamma(n) \geq n$, ne dépendant que de (F) , tel que*

$$\tau_n(Z_\infty(F)) = \tau_{\gamma(n),n}(Z_{\gamma(n)}(F)).$$

De plus, il est possible de choisir la fonction $n \mapsto \gamma(n)$ majorée par une fonction affine de n .

L'objet de ce petit texte est d'essayer de raconter des résultats obtenus récemment sur la façon dont les ensembles $\tau_n(Z_\infty(F))$ varient avec n .

2. – Interlude : parties constructibles et semi-algébriques

En général, la projection d'un sous-ensemble algébrique de \mathbb{C}^m n'est pas nécessairement algébrique. Ainsi la projection sur l'une des droites de coordonnées de l'hyperbole d'équation $x_1x_2 - 1$ dans \mathbb{C}^2 est égale à $\mathbb{C} \setminus \{0\}$, qui n'est certainement pas un sous-ensemble algébrique de \mathbb{C}^2 . Pour pallier cette difficulté on introduit la notion de sous-ensemble *constructible* de \mathbb{C}^m . La famille des sous-ensembles constructibles de \mathbb{C}^m , $\mathcal{S}(\mathbb{C}^m)$, est la plus petite famille de parties de \mathbb{C}^m contenant les sous-ensembles algébriques qui soit stable par intersection et réunion finie et passage au complémentaire (c'est la sous-algèbre de Boole de l'ensemble des parties de \mathbb{C}^m engendrée par les sous-ensembles algébriques). Autrement dit, un sous-ensemble constructible de \mathbb{C}^m est décrit par un ensemble fini de conditions de la forme $F_i = 0$ et $G_j \neq 0$ avec F_i et G_j des polynômes à coefficients complexes. D'après un théorème de C. Chevalley (en fait une version "moderne" de la théorie classique de l'élimination), l'image d'une partie constructible par une application polynomiale est toujours constructible : on a $\pi(\mathcal{S}(\mathbb{C}^m)) \subset \pi(\mathcal{S}(\mathbb{C}^{m'}))$ pour toute application polynomiale $\pi : \mathbb{C}^m \rightarrow \mathbb{C}^{m'}$. Considérons des parties constructibles Z et Z' de \mathbb{C}^m et $\mathbb{C}^{m'}$ respectivement. On dit que Z et Z' sont *strictement isomorphes* s'il existe une application rationnelle (c'est à dire dont les composantes sont des fractions rationnelles) $F : Z \rightarrow Z'$ qui soit bijective et d'inverse F^{-1} également rationnelle. Avec cette définition, l'hyperbole d'équation $x_1x_2 - 1$ dans \mathbb{C}^2 est strictement isomorphe à $\mathbb{C} \setminus \{0\}$. S'il existe des partitions finies $A_i, i \in I$ et $A'_i, i \in I$ de Z et Z' respectivement en parties constructibles telles que, pour tout $i \in I$, A_i soit strictement isomorphe à A'_i , on dit que Z et Z' sont *isomorphes*.

Le théorème de Chevalley reste valable lorsque \mathbb{C} est remplacé par un corps algébriquement clos quelconque. En général, pour K un corps et m un entier ≥ 0 , on note $\mathcal{S}(K^m)$ la plus petite sous-algèbre de Boole de l'ensemble des parties de K^m contenant les parties algébriques de K^m (c'est à dire définies par des équations polynomiales à coefficients dans K), telle que $\pi(\mathcal{S}(K^m))$ soit contenu dans $\mathcal{S}(K^{m'})$ pour toute application polynomiale $\pi : K^m \rightarrow K^{m'}$. On remarquera que, nécessairement, les parties $Z_{F,n}$ définies par la condition « $F(x)$ est une puissance n -ième dans K », avec F un polynôme en m -variables à coefficients dans K , et n un entier ≥ 2 , doivent appartenir à $\mathcal{S}(K^m)$. Lorsque $K = \mathbb{R}$, il résulte du théorème de Tarski-Seidenberg que $\mathcal{S}(\mathbb{R}^m)$ est exactement l'algèbre de Boole engendrée par les parties de la forme $Z_{F,2}$, c'est à dire définies par la condition $F \geq 0$, avec F un polynôme à coefficients réels. Les éléments de $\mathcal{S}(\mathbb{R}^m)$ sont appelés parties semi-algébriques de \mathbb{R}^m . Ce sont les sous-ensembles décrits par un nombre fini de conditions de la forme $F_i = 0, G_j \geq 0$ et $H_k \neq 0$ avec F_i, G_j et H_k des polynômes à coefficients réels.

Bien que cela soit moins connu, il existe d'autres corps pour lesquels les ensembles $\mathcal{S}(K^m)$ admettent une description agréable. Considérons, par exemple, le corps \mathbb{Q}_p des nombres p -adiques, pour p un nombre premier. C'est le complété de \mathbb{Q} pour la norme p -adique $|x| = p^{-v_p x}$. Ici $v_p x$ désigne la valuation p -adique de x , c'est-à-dire l'exposant de p dans la décomposition en facteurs premiers de x . On convient que 0 a pour valuation ∞ . Il résulte d'un théorème de Macintyre que $\mathcal{S}(\mathbb{Q}_p^m)$ est alors exactement l'algèbre de Boole engendrée par les $Z_{F,n}$. Pour se convaincre que les parties algébriques de \mathbb{Q}_p^m appartiennent

bien à cette algèbre de Boole, on remarquera que, si F est un polynôme à coefficients dans \mathbb{Q}_p , F s'annule en un point a de \mathbb{Q}_p si et seulement si $pF^2(a)$ est un carré. Les éléments de $\mathcal{S}(\mathbb{Q}_p^m)$ sont appelés semi-algébriques par analogie avec le cas réel. La démonstration originelle de Macintyre [7] utilisait la théorie des modèles et une démonstration élémentaire (sans logique) du théorème de Macintyre a été ultérieurement donnée par Denef [3].

Retournons maintenant à l'objet de cet exposé, à savoir les séries formelles. On considère le corps des fractions $K = \mathbb{C}((t))$ de l'anneau des séries formelles $\mathbb{C}[[t]]$. Les éléments de K sont de la forme $f = \sum_{i \in \mathbb{Z}} a_i t^i$ avec $a_i = 0$ pour $i \ll 0$. On note $\text{ord}(f)$ l'ordre d'une telle série f , à savoir le plus petit i tel que a_i soit non nul et on pose $\text{in}(f) = a_{\text{ord}(f)}$. Lorsque f est la série nulle, on convient que $\text{ord}(f) = \infty$ et que $\text{in}(f) = 0$. Il résulte maintenant d'un théorème de Pas [9] que les éléments de $\mathcal{S}(K^m)$ appartiennent à l'algèbre de Boole engendrée par les parties définies par les conditions du type suivant

$$(2.1) \quad \text{ord}F(x(t)) \geq \text{ord}G(x(t)) + \ell$$

$$(2.2) \quad \text{ord}F(x(t)) \equiv \ell \pmod{d}$$

$$(2.3) \quad F(\text{in}(G_1(x(t))), \dots, \text{in}(G_q(x(t)))) = 0$$

portant sur un m -uplet $x(t)$ d'éléments de K . Ici F , G et les G_i sont des polynômes à coefficients dans K , d ainsi que ℓ sont des entiers. Si dans la définition de $\mathcal{S}(K^m)$ on ne considère que les parties algébriques de K^m définies par des équations polynomiales à coefficients dans \mathbb{C} et des images de tels ensembles par des applications polynomiales à coefficients dans \mathbb{C} , on obtient une sous-algèbre de Boole $\mathcal{S}_0(K^m)$ de $\mathcal{S}(K^m)$. Il résulte également du théorème de Pas que les éléments de $\mathcal{S}_0(K^m)$ appartiennent à l'algèbre de Boole engendrée par les parties définies par les conditions du type (2.1), (2.2), (2.3) avec maintenant F , G et les G_i des polynômes à coefficients dans \mathbb{C} et non plus dans $K = \mathbb{C}((t))$. Les éléments de cette algèbre de Boole seront appelés ensembles semi-algébriques.

3. – L'anneau universel associé aux ensembles constructibles

Il est possible de construire un anneau universel \mathcal{M} à partir des ensembles constructibles de la façon suivante. À toute partie constructible Z de \mathbb{C}^m (ici m est variable), on associe un symbole $[Z]$. On considère le quotient du groupe abélien libre engendré par ces symboles par les relations

$$[Z] = [Z'] \quad \text{si } Z \text{ est isomorphe à } Z'$$

et

$$[Z \cup Z'] = [Z] + [Z'] - [Z \cap Z'].$$

On obtient ainsi un groupe abélien que l'on note \mathcal{M} et que l'on munit d'une structure d'anneau en posant $[Z][Z'] = [Z \times Z']$. On remarquera que l'unité est donnée par la classe d'un point. L'anneau \mathcal{M} est universel dans le sens suivant : toute application F qui à un ensemble constructible Z associe un élément $F(Z)$ d'un anneau A qui ne dépend que de la classe d'isomorphisme de Z , est de plus additive (elle vérifie $F(Z \cup Z') = F(Z) + F(Z') - F(Z \cap Z')$) et multiplicative (elle vérifie $F(Z \times Z') = F(Z)F(Z')$) se factorise nécessairement à travers

\mathcal{M} . Un exemple de telle application est donné par la caractéristique d'Euler-Poincaré $\chi : \mathcal{M} \rightarrow \mathbb{Z}$, mais on peut en construire beaucoup d'autres. En fait, l'anneau \mathcal{M} n'est pas encore tout à fait celui que l'on va utiliser. Appelons \mathbb{L} la classe de la droite affine \mathbb{C} dans \mathcal{M} . On va considérer l'anneau \mathcal{M}_{loc} obtenu en inversant formellement l'élément \mathbb{L} . En termes techniques c'est l'anneau localisé $\mathcal{M}[\mathbb{L}^{-1}]$. On a un morphisme naturel d'anneaux $\mathcal{M} \rightarrow \mathcal{M}_{\text{loc}}$, mais a priori il n'est pas injectif : en effet deux éléments de \mathcal{M} ont même image dans \mathcal{M}_{loc} s'il deviennent égaux après multiplication par une puissance adéquate de \mathbb{L} . Grosso modo regarder les ensembles constructibles dans \mathcal{M} revient à les considérer « à découpage près », tandis que les regarder dans \mathcal{M}_{loc} revient à les considérer « à découpage et stabilisation par un espace affine près ».

4. – Les énoncés

Après tous ces détours, il est maintenant temps de revenir à notre question première : comment les ensembles $\tau_n(Z_\infty(F))$ varient-ils avec n ?

Pour cela commençons par remarquer que $\tau_n(Z_\infty(F))$ est une partie constructible de

$$(\mathbb{C}[t]/t^{n+1}\mathbb{C}[t])^m \simeq \mathbb{C}^{(n+1)m}.$$

En effet, par le théorème de Greenberg 1.2, $\tau_n(Z_\infty(F))$ est l'image par une application polynomiale d'un ensemble algébrique et est donc constructible d'après le théorème de Chevalley. On peut donc considérer la classe $[\tau_n(Z_\infty(F))]$ de $\tau_n(Z_\infty(F))$ dans l'anneau \mathcal{M}_{loc} . Formons la série génératrice

$$P(T) := \sum_{n \in \mathbb{N}} [\tau_n(Z_\infty(F))] T^n$$

dans l'anneau $\mathcal{M}_{\text{loc}}[[T]]$.

On a le résultat de rationalité suivant :

Théorème 4.1 ([4]). *Dans l'anneau $\mathcal{M}_{\text{loc}}[[T]]$, la série génératrice $P(T)$ est égale à une combinaison linéaire à coefficients dans l'anneau de polynômes $\mathcal{M}_{\text{loc}}[T]$ de séries de la forme $(1 - \mathbb{L}^a T^b)^{-N}$, avec a dans \mathbb{Z} , b et N dans $\mathbb{N} \setminus \{0\}$.*

Une conséquence de ce résultat est que les $\tau_n(Z_\infty(F))$ ont un comportement asymptotique particulièrement simple : pour n assez grand ils vérifient une relation linéaire de récurrence à coefficients dans \mathcal{M}_{loc} .

Ceci ne nous dit toutefois rien sur la valeur de $\tau_n(Z_\infty(F))$ pour n très grand. En fait, on va voir que, convenablement renormalisés, les $\tau_n(Z_\infty(F))$ ont une limite quand $n \rightarrow \infty$. Pour pouvoir parler de limite, il faut tout d'abord disposer d'une topologie. Pour cela on va considérer la dimension virtuelle des éléments de \mathcal{M}_{loc} : pour tout entier m dans \mathbb{Z} , on note F^m le sous-groupe abélien de \mathcal{M}_{loc} engendré par les fractions de la forme $[S]\mathbb{L}^{-i}$ avec S de dimension complexe $\leq -m + i$; les éléments de F^m sont ceux de dimension virtuelle $\leq -m$: plus m est grand, plus F^m est petit. Ceci permet de munir \mathcal{M}_{loc} d'une structure topologique (uniforme, pour les puristes) compatible avec la structure d'anneau et on peut considérer l'anneau complété $\widehat{\mathcal{M}}$, introduit par M. Kontsevich.

Théorème 4.2 ([4]). *Si $Z(F)$ est non vide et de dimension complexe r , alors la suite $n \mapsto [\tau_n(Z_\infty(F))]_{\mathbb{L}}^{-(n+1)r}$ est de Cauchy dans \mathcal{M}_{loc} et a une limite non nulle $\mu(Z_\infty(F))$ dans $\widehat{\mathcal{M}}$.*

Concrètement, ce résultat affirme que, à un facteur affine « trivial » près, les ensembles $\tau_n(Z_\infty(F))$ ont une limite virtuelle quand $n \rightarrow \infty$. Il est en fait possible de donner des « formules » pour cette limite, pour lesquelles nous renvoyons à [4].

5. – L’analogie avec le p -adique

Heuristiquement les énoncés des théorèmes 4.1 et 4.2 ont été découverts par analogie avec le cas p -adique. Par définition l’anneau \mathbb{Z}_p des entiers p -adiques est le complété de \mathbb{Z} pour la norme p -adique. C’est aussi l’ensemble des éléments de \mathbb{Q}_p de norme p -adique ≤ 1 . Les éléments de \mathbb{Z}_p s’écrivent de façon unique comme des séries $\sum_{i \in \mathbb{N}} a_i p^i$ avec a_i dans $\{0, \dots, p-1\}$. On voit ainsi apparaître une analogie naturelle entre les séries formelles et les entiers p -adiques, le nombre premier p correspondant à la variable t . Il est de plus clair à partir de cette écriture que $\mathbb{Z}_p/p^i \mathbb{Z}_p$ est isomorphe à $\mathbb{Z}/p^i \mathbb{Z}$ pour tout i . Considérons maintenant un système (F) d’équations polynomiales comme celui du début de ce texte, mais dont les coefficients appartiennent à \mathbb{Z}_p au lieu d’appartenir à \mathbb{C} . Notons $Z(F)(\mathbb{Z}_p)$ la partie de \mathbb{Z}_p^m formée des solutions du système à coefficients dans \mathbb{Z}_p . Dans cette situation l’analogie de l’ensemble des tronqués $\tau_n(Z_\infty(F))$ est tout simplement l’image de l’ensemble $Z(F)(\mathbb{Z}_p)$ dans $(\mathbb{Z}_p/p^i \mathbb{Z}_p)^m$. Comme $(\mathbb{Z}_p/p^i \mathbb{Z}_p)^m$ est un ensemble fini, il en est de même de l’image de $Z(F)(\mathbb{Z}_p)$, et la seule chose raisonnable à faire est d’étudier son cardinal que l’on note N_i .

Le résultat de rationalité suivant, dont le théorème 4.1 est l’analogie, est dû à J. Denef et répond à une question posée par J.-P. Serre.

Théorème 5.1 ([2]). *La série de Poincaré $Q(T) := \sum_{i \in \mathbb{N}} N_i T^i$ est le développement en série d’une fraction rationnelle.*

Quant au théorème 4.2, il est l’analogie du résultat suivant de J. Oesterlé :

Théorème 5.2 ([8]). *Si $Z(F)(\mathbb{Z}_p)$ est non vide et de dimension r , alors la suite $n \mapsto N_n p^{-(n+1)r}$ a une limite non nulle dans \mathbb{R} .*

6. – Les ingrédients

La preuve du théorème 5.1 utilise de façon essentielle que la série de Poincaré $Q(T)$ est égale, à un grain de sel près, à l’intégrale

$$(6.1) \quad Z(s) := \int_{\mathbb{Z}_p^m} d(x, Z(F)(\mathbb{Z}_p))^{-s}.$$

Ici \mathbb{Z}_p^m est muni de la mesure de Lebesgue, dont la construction dans le cas p -adique est similaire, en bien plus simple, à celle du cas réel, $d(x, Z(F)(\mathbb{Z}_p))$ désigne la distance de x à $Z(F)(\mathbb{Z}_p)$ et s est relié à T par la relation $T = p^{-s}$. On voit apparaître avec l’intégrale $Z(s)$ les deux ingrédients essentiels de la preuve du théorème 4.1 qui sont

- l'utilisation de l'intégration pour la mesure de Lebesgue
- l'utilisation de la fonction distance d .

Déjà dans le cas complexe, la fonction distance à un ensemble algébrique n'est pas en général polynomiale, mais seulement semi-algébrique (au sens que son graphe est un ensemble semi-algébrique réel). De même, dans le cas p -adique, le graphe de la fonction distance est semi-algébrique.

La démonstration des théorèmes 4.1 et 4.2 procède par analogie avec le cas p -adique. Un rôle clé est ainsi joué par la théorie des ensembles semi-algébriques sur $\mathbb{C}((t))$, qui est un analogue de la théorie des ensembles semi-algébriques p -adiques, ainsi que par un analogue géométrique de l'intégration p -adique, l'intégration motivique. Pour développer cette théorie de l'intégration motivique on construit une mesure μ , qui à une partie semi-algébrique Z de $\mathbb{C}[[t]]^m$ associe un élément $\mu(Z)$ de $\widehat{\mathcal{M}}$, de la façon suivante : on démontre, par une preuve analogue à celle du théorème 5.2, que la suite $n \mapsto [\tau_n(Z)]\mathbb{L}^{-(n+1)m}$ est de Cauchy dans \mathcal{M}_{loc} (ce qui donne essentiellement le théorème 4.2) ; le volume motivique $\mu(Z)$ est égal à la limite de cette suite dans $\widehat{\mathcal{M}}$. Cette mesure permet également d'intégrer des fonctions « semi-algébriques » et en particulier d'exprimer la série de Poincaré $P(T)$ en fonction d'un analogue de l'intégrale $Z(s)$ définie en (6.1). Pour démontrer la rationalité de $P(T)$ on peut alors suivre la stratégie de la preuve du théorème 5.2, qui utilise de façon essentielle le théorème de résolution des singularités d'Hironaka et la formule de changement de variable dans les intégrales. Dans le présent contexte l'analogue de la formule de changement de variable se ramène à un énoncé purement géométrique démontré dans [4].

Remarque. Supposons que les polynômes F_i soient à coefficients rationnels. Les coefficients de la série $P(T)$ sont alors des classes de parties constructibles définies par des équations à coefficients rationnels et on peut considérer leur nombre de points dans le corps fini à p éléments \mathbb{F}_p , au moins pour presque tout nombre premier p . On pourrait imaginer qu'en procédant ainsi il soit possible de récupérer les séries $P_p(T)$, au moins pour presque tout nombre premier p , à partir de la série $P(T)$. En fait il n'en est rien ; il est cependant possible (cf. [5]), mais cela demande plus de travail, de construire une autre série de Poincaré, de nature arithmétique celle-ci, vérifiant une telle propriété de spécialisation.

Références

1. M. Artin, *On the solutions of analytic equations*, Invent. Math. **5**(1968), 277–291.
2. J. Denef, *The rationality of the Poincaré series associated to the p -adic points on a variety*, Invent. Math. **77** (1984), 1–23.
3. J. Denef, *p -adic semi-algebraic sets and cell decomposition*, J. Reine Angew. Math. **369** (1986), 154–166.
4. J. Denef, F. Loeser, *Germes of arcs on singular algebraic varieties and motivic integration*, Inv. Math. **135** (1999), 201–232.
5. J. Denef and F. Loeser, *Definable sets, motives and p -adic integrals*, preprint octobre 1999, math/9910107.
6. M. Greenberg, *Rational points in Henselian discrete valuation rings*, Inst. Hautes Études Sci. Publ. Math. **31** (1966), 59–64.
7. A. Macintyre, *On definable subsets of p -adic fields*, J. Symbolic Logic **41** (1976), 605–610.

8. J. Oesterlé, *Réduction modulo p^n des sous-ensembles analytiques fermés de \mathbb{Z}_p^N* , Invent. math. **66** (1982), 325–341.
9. J. Pas, *Uniform p -adic cell decomposition and local zeta functions*, J. reine angew. Math. **399** (1989), 137–172.

Rectificatif à l'article de H. Darmon intitulé : « La Conjecture de Shimura-Taniyama-Weil est enfin démontrée¹ »

Yves HELLEGOUARCH (Université de Caen)

LE PRÉSENT RECTIFICATIF concerne un point de cet article dont l'importance est plus historique que mathématique et qui peut se résumer par une question : qui a inventé les « courbes de Frey » ?

Dans son article, H. Darmon semble donner une réponse en écrivant que « C'est Frey qui a eu l'idée d'associer à une solution non triviale (a, b, c) de l'équation $x^p + y^p = z^p$ une courbe elliptique $E_{a,b,c}$ (appelée maintenant « courbe de Frey ») donnée par l'équation $y^2 = x(x - a^p)(x + b^p)$ ».

Comme le reconnaît H. Darmon lui-même, la formulation de cette phrase est « fâcheuse » car elle suggère que c'est Frey qui, le premier, a eu cette idée. Or si une chose est bien claire, c'est que ce n'est pas Frey qui a **le premier** utilisé cette construction et remarqué **le premier** les étranges propriétés de faible ramification de la p -torsion de cette courbe (qui font douter de l'existence de celle-ci).

Voici, par exemple, le contenu d'une lettre que Jean-Pierre Serre m'a adressée le 16 janvier 1986 et qui pose la question :

Dans votre thèse, vous aviez utilisé la courbe elliptique

$$E_{a,b,c} \quad y^2 = x(x - a^p)(x - c^p)$$

associée à une solution $a^p + b^p = c^p$ de l'équation de Fermat, et vous aviez étudié les propriétés de ramification de ses points de division par p .

*Vous savez peut-être que cette construction a été reprise tout récemment par G. Frey. Si l'on combine cette idée avec certaines **conjectures** sur les formes modulaires \pmod{p} que j'avais faites vers 1974, on trouve une contradiction (ce qui démontre Fermat! mais hélas **modulo** mes conjectures).*

Je vous écris, d'abord pour vous raconter ces développements récents (qui peuvent vous intéresser), et puis aussi pour vous demander des références sur la courbe $E_{a,b,c}$: où apparaît-elle pour la première fois ? Est-ce dans votre thèse, ou chez Demjanenko ? Ou ailleurs ? Pouvez-vous avoir l'obligeance de me renseigner ?

¹ *Gazette des mathématiciens* n° 83 (janvier 2000).

En fait l'origine de cette construction ne peut être postérieure à 1969 puisque je l'avais exposée oralement aux Journées Arithmétique de Bordeaux, qui avaient eu lieu cette année-là, dans le but de prouver que l'un des points d'ordre p de la courbe $E_{a,b,c}$ engendrait une extension de \mathbb{Q} non ramifiée en p lorsque p divise abc . L'argument que j'avais utilisé était faux et Jean-Pierre Serre (qui était présent à l'exposé) l'avait aussitôt démolé. C'est la raison pour laquelle les courbes $E_{a,b,c}$ ont été supprimées dans ma contribution aux Comptes-Rendus de ces Journées Arithmétiques. La première utilisation que j'ai faite de ces courbes apparaît (pour les initiés) dans une note aux CRAS de 1971 [1]. Cette utilisation est détaillée dans ma thèse [2] et résumée dans un article aux Acta Arithmetica [3]. Mon article aux Acta Arithmetica est cité en 1977 dans [4] et ma thèse l'est en 1982 dans [5], ce qui montre que la communauté mathématique avait bien pris connaissance de cette construction.

Le lecteur remarquera que je n'ai pas répondu à toutes les questions posées dans la lettre de Jean-Pierre Serre. En effet je n'avais trouvé le modèle de cette construction précise dans aucun document antérieur à 1969, mais il serait présomptueux de ma part d'en conclure que l'origine de cette construction ne se trouve pas dans des documents que je ne connaissais pas.

Ce qui est clair est que la recherche de l'origine de cette construction est un point historique intéressant.

Bibliographie

- [1] Y. HELLEGOUARCH, *Points d'ordre fini sur les courbes elliptiques*; CRAS Paris, t. 273, 540-43, 1971.
- [2] Y. HELLEGOUARCH, *Courbes elliptiques et équations de Fermat*; Thèse, Besançon, 1972.
- [3] Y. HELLEGOUARCH, *Points d'ordre $2p^h$ sur les courbes elliptiques*. Acta Arith. XXVI, 253-263, 1975.
- [4] G. FREY, *Some remarks concerning points of finite order on elliptic curves over global fields*, Arkiv f. Math. 15, 1-19, 1977.
- [5] G. FREY, *Rationale Punkte auf Fermatkurven und getwisteten Modulkurven*. J. Reine u. Angew. Math. 33, 185-191, 1982.