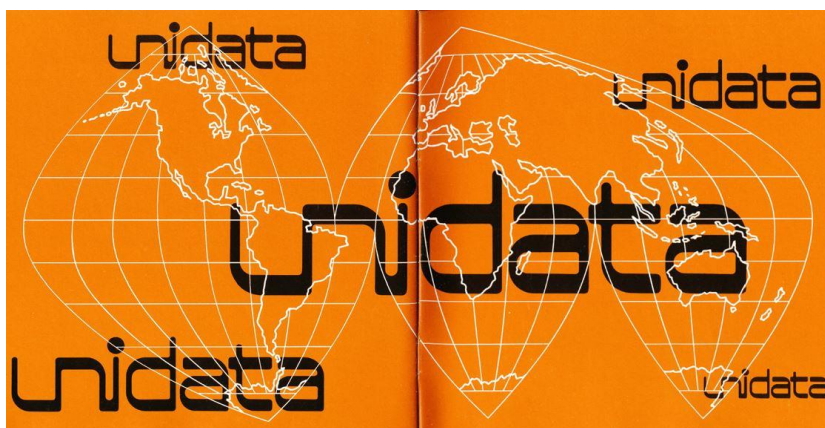


Vers une informatique européenne souveraine

1975 La stratégie **Unidata** 2025

- Une histoire
- Une vision
- Des récits

Témoignage de Jean-Jacques Quisquater



1975 : Le sabordage de l'informatique européenne

2025 : L'émergence d'une souveraineté informatique européenne

**Marie d'Udekem-Gevers
Guy-Noël Maréchal
Roger Roberts**

Partie III : Témoignages

Dans cette partie, notre intention est de donner la parole à des témoins qui présenteront transversalement la vie industrielle et industrielle de l'époque. Ces fragments devraient mieux montrer le contexte, la vie de l'intérieur de la période qui a suivi Unidata jusqu'à nos jours.

Ces fragments montrent aussi l'influence tout à fait significative et de longue durée que le projet de la Machine mathématique IRSIA-FNRS et l'aventure Unidata 7.720 ont eu, au travers des destins de ceux qui y ont collaboré, mais aussi du dynamisme et des opportunités qu'offrait un grand groupe, comme l'était Philips dans les années 60, et de grands hommes qui dirigeaient des équipes et des projets ambitieux et éclectiques. Ces témoignages illustrent aussi le passage de l'analogique au numérique tant sur le plan technique que sociétal.

Nous tenons à remercier le professeur Jacques Neiryck, qui nous a chaudement encouragés de nous exprimer de manière « vécue » via ces témoignages !

Les pistes pour la souveraineté informatique européenne présentées au chapitre 5 découlent directement des expériences, visions, réalisations de ces témoins.

En pratique, chaque témoignage sera introduit sommairement. Les lecteurs désireux de découvrir les témoignages complets pourront le faire en y accédant via un QR Code.

Chapitre 7 : Témoignages de et sur Claude Fosseprez

Chapitre 8 : Témoignage de Guy Maréchal

Chapitre 9 : Témoignage de Jean Voisin

Chapitre 10 : Témoignage de Georges Goeman

Chapitre 11 : Témoignage de Ferdinand de Wasseige

Chapitre 12: Témoignage de Jean-Jacques Quisquater

Chapitre 13 : Témoignage de Bernard Durieux

Chapitre 14 : Témoignage de Roger Roberts

Chapitre 15 : Témoignage de Steny Solitude

1 Témoignage de Jean-Jacques Quisquater

Attention : J'ai organisé le texte qui suit sur base des courriels de JJQ ! Mais, cette transcription ne fut pas aisée, car les propos de JJQ étaient assez bruts. Le texte doit donc être retouché, complété et validé par JJQ ! GNM, 2025-06-18 !

Introduction

Je suis entré chez MBLE en fin 1970 et j'ai quitté en 1991, lorsque Philips a fermé le PRLB !

Ma carrière s'est poursuivie à l'Université Catholique de Louvain [UCL] pour se terminer par l'éméritat en octobre 2010. J'ai continué à être actif, essentiellement dans le domaine de la cryptographie.

Lors de ma prise de pension, j'ai fait un bilan positif de ma vie professionnelle et je me suis dit que j'avais eu bien de la chance grâce à plein de personnes, que je nomme mes fées (et aussi grâce à ma ténacité et ma résilience, et le support constant de ma famille, épouse chouette et enfants). Et aussi de plein de personnes uniques, dévouées, que je n'ai jamais pu vraiment bien remercier ou même mettre en valeur.

Mais, il y a eu aussi quelques rares personnes avec qui je me suis mal entendu ; probablement à cause de leur jalousie, hélas. Et je ne m'attendais pas du tout à cela : je n'ai jamais été jaloux, et personne dans ma famille non plus. Pendant mes études, à tous les niveaux et constamment, j'ai eu la chance de rencontrer de la collaboration.

Lors de ce bilan de vie, je me suis dit que je devais essayer de terminer ma vie en harmonie avec toutes et tous et tenter de lever des quiproquos avec ces personnes qui, par exemple, m'ignoraient. En fait, curieusement, je n'ai eu des problèmes qu'avec des hommes, aucune femme !

Pour illustrer cette difficulté, je puis évoquer mes relations avec Elie Migrom, professeur à l'UCL, qui avait porté mon dossier, son chouette choix, au rectorat UCL après la fermeture de PRLB. Malgré une longue discussion avec lui, je n'ai pas compris pourquoi il m'ignorait après mon éméritat de l'UCL et nous sommes arrivés à un état neutre. C'est son choix !

Dans le domaine de la recherche, les tensions étaient fréquentes, mais ce ne fut jamais le cas avec quelques personnes que je veux citer : Vitold Belevitch, Marc Davio, Jean-Marie Goethals, Jacques Neiryck, Axel van Lamsweerde, Philippe Delsarte.

De même, j'ai eu d'excellents contacts avec Guy Maréchal et son équipe avec qui j'ai marginalement collaboré lors de leur

développement du système d'accès de la télévision numérique DVB, qui était basé sur une des cartes à puce pour laquelle j'avais collaboré avec une des Entreprises du groupe Philips : TRT à Fontenay-aux-Roses.

Mes débuts à PRLB

Je suis rentré chez MBLE Research Lab, devenu plus tard PRLB, le 1er octobre 1970, à 8h15 (important à savoir, j'ai dû attendre jusque 9h pour voir quelqu'un ...) en même temps qu'Axel van Lamsweerde, devenu plus tard professeur à Namur puis à l'UCL.

Nous avions à cette époque deux ordinateurs Electrológica, qui étaient de pure merveille (les seuls ordinateurs cités par Donald Knuth dans sa série bien connue de livres d'informatique). J'ai pas mal utilisé ceux-ci notamment avec le langage APL¹, aussi une pure merveille !

Quand je suis arrivé à PRLB en 1970, je n'avais aucune idée comment cela allait se passer sauf que c'était un endroit chouette où on faisait de la très bonne recherche avec de merveilleux bons

moyens suivant l'avis de Jean Meinget, qui m'avait fort poussé à y aller, et Nicolas Rouche, mon maître de toujours. C'est Jacques Neiryck, directeur adjoint, qui m'avait engagé en l'absence du directeur Vitold Belevitch, ce dernier en année sabbatique, oui cela existait chez Philips et l'on nous avait promis cela aussi. Jacques Neiryck, fondateur aussi de Test-Achats - je suis toujours en contact avec lui - me demande alors d'être top niveau mondial dans mon sujet en 2 ans : oui ! Personne ne m'avait dit alors que c'était lié à Philips, pour moi c'était bien MBLE, un grand souvenir de ma jeunesse et de tous mes bricolages électroniques. À l'époque, tout était très sérieux dans ce labo, trop même : costume, cravate, même, pour certains, un air constipé sans un brin de regard de contact. Avec Axel van Lamsweerde, un ami ayant accompli de bonnes études de licence en math à UCL en // avec les miennes, en ingénieur en math appliquées, arrivé le même jour que moi, nous décidons de changer cela calmement : nous venions sans cravate, avec des cols roulés, et peu à peu, chacun se dérouille et finalement, cela a pris près d'une année au total, à part le directeur et quelques responsables de groupe, plus de cravates sauf lors de la venue de visiteurs.

UNIDATA

Parmi les travaux que j'ai effectués dans mes premières années à PRLB, l'un des plus pénibles fut de collaborer à la finalisation des logiciels de la maquette de développement de la 7•720, l'ordinateur dont Philips était chargé dans le consortium UNIDATA.

Une vraie catastrophe qui m'a coûté plusieurs années de ma vie ...

Jean-Jacques, tu nous a promis (ton courriel du 28 février 2024) une contribution sur les tribulations que l'aventure Unidata a impliqué à PRLB et à toi en particulier.

PRLB

J'ai découvert fort vite que l'ambition des chercheurs les plus anciens était de devenir une sorte de Bell Labs (de l'époque) à la belge et d'en avoir les moyens (voir plus loin, la réalité) et les résultats. Hélas, pour moi, j'ai aussi découvert que ce n'était pas aussi simple : la crise pétrolière de 1973 est arrivée et plus personne n'a été engagé (la promesse était de passer de 50 à 100 chercheurs en 5 ans, jamais tenue). Pendant 10 ans j'ai été le dernier engagé, et il y a eu pourtant des départs. Cette situation de dernier engagé m'a conduit à avoir un comportement de me protéger, en fait, de me rendre indispensable (je n'étais pas le seul). Pour ne pas disparaître, car rien de pareil n'existait alors en Belgique. Avant cela, de 1970 à 1973, j'ai eu une période extraordinaire, en vrai, j'ai publié mon meilleur article mathématique avec Philippe Delsarte, durant la fin de sa thèse, et, vraiment, je suis le seul à avoir publié avec lui, entre 1970 et 1974. Je le remercie vraiment beaucoup pour cela. Cet article fut une collaboration parfaite, moitié-moitié en parfaite harmonie. J'ai toujours gardé de bons contacts avec Philippe depuis lors. Nous avions imaginé d'autres papiers ensemble, mais cela ne s'est pas concrétisé. Philippe a été capté par d'autres.

En effet, les nouvelles étaient alors devenues mauvaises (choc pétrolier de 1973) et le directeur Vitold Belevitch imagine de recycler une partie du labo vers les applications de téléphonie (numérique) pour protéger l'ensemble. Pour cela, nous recevons des cours, pour ceux à recycler, surtout les derniers entrés, dont moi donc. Ces cours de téléphonie étaient donnés par un professeur d'Eindhoven, celui-ci absolument nul, avec des tics verbaux à mourir de rire (tristement). Et, hélas, c'était l'usage à l'époque, pas mal de chercheurs fumaient, y compris surtout Vitold (gros cigares) durant les cours. Horreur ! Pour me protéger de la fumée (je ne fume pas et je suis très sensible à celle-ci) je me réfugie tout à l'arrière de la salle de cours. Et je me demande comment survivre à cela (cela a duré 4 à 5 mois pour des semaines jusqu'à 15 heures de cours ...). Je regarde les revues de notre grande bibliothèque que nous avons et je découvre un article dans IEEE on Computers qui peut s'appliquer aux réseaux téléphoniques et que je crois pouvoir améliorer. Belle excuse ! C'était, vu de loin, le cours donné que j'approfondissais :-). Très vite, j'améliore les résultats (quelle chance !) d'une table de 10x10 entrées dont mon ambition est devenue alors de tout améliorer : pour quelques entrées de la table j'utilise un résultat de

Jean-Marie Goethals et, hélas, pas de chance pour moi, c'était un de ses papiers erronés (cela arrive à tout le monde, sauf à Evariste Galois).

Après correction, les travaux sur ce sujet ont continué et je suis toujours cité dans cette table qui aujourd'hui est de « 10 x 16 », notamment : <https://combgraph.upc.edu/en/resources> et http://combinatoricswiki.org/wiki/The_Degree_Diameter_Problem_for_Bipartite_Graphs.

Concernant les Bell Labs (Murray Hill) que certains chercheurs de PRLB voulaient imiter jusqu'à l'absurde (être bien payé, pour bien faire sa propre recherche, par Philips sans vouloir, surtout pas, être utile et encore moins pratique) , j'ai eu le mot de la fin bien plus tard : non, leurs chercheurs n'y faisaient pas que de la recherche de haut vol avec des applications extraordinaires (transistor ...). En fait, ils répondaient à des demandes bien pratiques de leurs différentes 'Business Units' (après un certain tri quand même). Ils leur donnaient le résultat de leurs recherches, dans un souci d'être utiles avec les meilleures idées possibles, puis ils en faisaient une théorie la plus générale possible, et c'est la partie qu'ils publient, ils étaient aussi d'excellents mathématiciens. Presque personne n'a fait cela à PRLB, proclamant seulement le droit de faire de la "bonne" recherche (sous-entendu alors, pas celle que je faisais moi) sans restriction. Et bien, cela s'est bien planté. Pour eux, se salir les mains, jamais. Cela va (allait) très loin.

La Cryptographie

En 2020, on m'a demandé en France (ce n'est pas la première fois) de décrire mes contributions en carte à puce et la cryptographie. Je ne vais pas détailler cela ici. J'ai eu la grande chance d'être au bon endroit au bon moment et de la saisir avec énergie, avec une excellente préparation et des appuis décisifs. Je ne suis pas le seul à PRLB, Marc Davio et Jean-Marie Goethals en sont aussi : Jean-Marie a eu le génie de comprendre mes suggestions et de présenter le sujet de cryptographie au CA de Philips à Eindhoven. En 1978 il a obtenu que nous soyons le centre de référence pour la cryptographie civile pour tout Philips : Marc a eu plein de bonnes idées en circuits logiques. Mais j'ai donné les idées et même implémenté, en logiciel ou en circuit, tout cela pour les algorithmes cryptographiques DES et le RSA dans la carte à puce Philips (et autres).

J'ai alors découvert que le chef de projet du côté français, qui me téléphonait souvent, en 1985 et après, en me suppliant de trouver la bonne optimisation, car il manquait de place (RAM, ROM, EPROM, ...), s'est attribué au moment même (toutes ?) mes idées devant ses chefs et ses assistants et a obtenu ainsi, notamment, les primes et nominations qui vont avec. Et, donc, les membres du labo d'applis français Philips (TRT,) ont cru qu'il avait tout trouvé. Heureusement, nous (PRLB) avons publié le principal à temps et breveté aussi, ce qui a permis de contrer cela, mais, bien sûr, bien trop tard. Ceci m'a laissé un goût assez amer : et le gars de Philips France, alors un simple exécutant, qui a rouspété il y a 2 ans, était de bonne foi, bien manipulé alors. L'on peut comprendre que cela a renversé le monde dans lequel j'étais. Toute une période extraordinaire de collaboration s'était en fait passée bien autrement que ce que j'avais compris. Hélas ! Ce gars de Philips France m'avait accusé de tirer trop la couverture à moi, alors à PRLB, devant 350 personnes de France, j'ai bien dû nous défendre. Il a bien dû reconnaître que cela c'était passé autrement que ce qu'il avait vu. Bonjour les dégâts. Vraiment, je ne m'attendais pas à celle-là : c'est une des pires de ma vie.

Autre rebond récent : j'ai beaucoup travaillé avec Philips Hambourg, puis devenu NXP, et cela s'est toujours très bien passé (sauf, un peu, avec un gars, physicien, qui ne comprenait rien à la cryptographie et qui, hélas, a été nommé chef du sujet à un moment donné, depuis nous nous sommes réconciliés, ma bonne volonté en action). Philips m'a quitté en 1991. Quelqu'un s'est intercalé entre moi et NXP, je ne sais comment, vers 1993, j'étais alors consultant indépendant, moi à peine nommé à mi-temps à l'UCL au tarif minimum. Et je lui ai raconté récemment le problème du "vol" de mes idées par Philips France en lui demandant s'il était au courant (il travaillait chez Philips France au même endroit que les autres, mais dans un autre service ...). Depuis lors, il ne me parle plus (avant on dînait ensemble à Paris au moins une fois par an) et j'ai

compris récemment, en discutant avec le directeur technique de Philips Hambourg, maintenant à la retraite, que ce quelqu'un avait été chargé (ou s'était chargé plus exactement) de négocier avec moi pour avoir la conception du coprocesseur RSA NXP à un prix forfaitaire très bas (vraiment !) plutôt que de me payer une somme minime par copro (calculez ! il y en a environ 10 milliards de puces à ce jour), NXP a pourtant accepté ceci avec Paul Kocher (presque 3 centimes par copro, je demandais 30 fois moins avec une limite supérieure). Ce quelqu'un a demandé ou reçu (?) je ne sais combien pour avoir négocié cela avec moi alors qu'il se faisait passer pour un ami ... (j'ai assisté à une petite partie de la remise de ses récompenses à Hambourg sans rien comprendre alors). Et je ne suis pas malheureux, loin de là.

À trois, avec Ralf Malzahn et Peter Marissen (ceux-ci pour la partie purement circuit : pour la première version ce fut Peter Klapproth) de Philips Hambourg, nous avons fait un boulot extraordinaire (que je n'ai pu publier en entier, ce qui fait que c'est mal connu et même mal décrit à leurs demandes). À PRLB, Dominique de Waleffe a fourni d'excellents tests et une description parfaite de la machine d'états internes du coprocesseur RSA et Jean-Pierre Bournas (en France, dans un labo d'applications Philips RTC) a programmé avec soin cette machine d'états. Tout a marché du premier coup (hardware et software, sauf un problème de trop haute optimisation, vite contourné). Heureuse collaboration avec des gens honnêtes, mais aussi avec des brouteurs de primes, hélas (je ne l'ai compris que bien plus tard). Les directeurs français de ces projets étaient pour la plupart des personnes extraordinaires et clairvoyantes : André Besse, Jean-Paul Lemarchand, Henri Molko...

Une dernière : en 2021, fête avec un ami les 50 ans de notre arrivée commune à PRLB (fête un an en retard vu le COVID). Nous fêtons cela chaque décade (10 ans). Il est aussi émérite de EPL-ULCLouvain.

Je comprends mieux, grâce à ses descriptions, l'ambiance qu'il y a eu lors de la seule réunion des émérites EPL, en 2022, en présence de la plupart des professeurs qui ont refusé ma venue à l'UCL, à mon insu, et surtout l'absence de mes collègues PRLB (j'en étais le seul présent) qui avaient postulé à l'UCL sans m'inclure pendant que j'essayais de toute part de sauver au moins une partie du labo.

Ce que je ne comprends pas du tout, c'est la durée de ce déni de mon existence : plus de 30 ans que cela dure ! Alors que Vitold Belevitch et Jean-Marie Goethals avaient dit que, grâce à mon travail j'étais de ceux qui avaient longtemps sauvé le labo PRLB et, donc, que je leur avais permis de continuer leurs petits jeux. Je n'invente rien et je n'en croyais pas mes oreilles.

Zero Knowledge

Parmi mes contributions à la cryptographie, il me semble pertinent d'évoquer ma collaboration avec Louis Guillou pour définir un protocole donnant une preuve d'identité à des correspondants sur un réseau, sans divulguer de connaissance à des tiers.

Ici Jean-Jacques, ajoute quelques mots sur ta collaboration avec Louis Guillou et sur les nombreuses applications qui ont émergé.

Conclusion

Pour moi, nous avons alors vécu une période extraordinaire, avec des moyens souvent fabuleux. Si la direction de Philips avait été mieux visionnaire, leurs actionnaires moins âpres à des gains immédiats, Philips aurait pu être aujourd'hui Méta, tous les ingrédients, les compétences y étaient.

Mais bon c'était culturel ! Je connais bien, mon beau-père est né à Eindhoven, et il s'est enfuit avec raison en Belgique...

¹ [https://fr.wikipedia.org/wiki/APL_\(langage\)](https://fr.wikipedia.org/wiki/APL_(langage))