CURRICULUM VITAE DETAILLE
DETAILED CURRICULUM VITAE

Nom/*Last Name* : Augot Prénom/*First Name* : Daniel
Date et lieu de naissance/*Date and place of birth* : 15/03/1966, Auch (France)
Nationalité/*Citizenship* : Fran,is Sexe/*Sex* : M
Adresse postale/*Mailing address* : Daniel Augot
4, rue du val d'Orsay
91400 Orsay
N° de téléphone/*Telephone* : (+33) 01 39 63 58 71
Adresse électronique/*E-mail* : Daniel.Augot@inria.fr
Page Web personnelle/*Web page* : http://www-rocq.inria.fr/secret/Daniel.Augot/

1.Diplômes/*DIPLOMAS*

Doctorat(s)/*Ph.D.(s)* :
– Étude algébrique des mots de poids minimum des codes cycliques, méthodes d'algèbre linéaire sur les corps finis. Soutenue le 2 Décembre 1993, à l'université Paris VI, devant le jury constitué de Daniel Lazard, Philippe Flajolet, Maurice Mignotte, Jacques Wolfmann, Thomas Ericson, Pascale Charpin, Paul Camion, avec la mention trés honorable et les félicitations du jury.

Habilitation à Diriger des Recherches (HDR) :
– Décodage des codes algébriques et cryptographie. Soutenue le 7 juin 2007,'a l'université PARIS VI, devant le jury constitué de Patrick Fitzpatrick, Daniel Lazard, Amin Shokrollahi, Philippe Flajolet, François Morain, Nicolas Sendrier et Annick Valibouze.

Autres diplômes (à partir du niveau maîtrise)/***Other diplomas*** *(Master's and higher)* :
– Agrégation de mathématiques (1988) ;
– DEA Langages, algorithme et programmation, à l'université Paris VI, mention TB (1989).

2.Parcours Professionnel/*Professionnal history*

Statut et fonction/*Position and statute* : Chargé de recherche 1ère classe dans l'équipe SECRET
Etablissement/*Institution* : Centre de Recherche INRIA Paris-Rocquencourt
Date d'entrée en fonction/*Start* : 10/93

FORMATION ET PARCOURS PROFESSIONNEL/*TRAINING AND PROFESSIONAL HISTORY*

Établissements français ou étrangers	Fonctions et statuts (salarié, boursier, etc.)	Dates		Observations *REMARKS*
INSTITUTIONS French or foreign	*POSITIONS AND STATUS*[1] *(employee, fellow, etc.)*	d'entrée en fonction *Start*	de cessation de fonction *End*	
ENS Fontenay-aux Roses	Éléve professeur stagiaire	09/85	08/87	
ENS Lyon/Section St Cloud	Éléve professeur stagiaire	09/87	09/89	
Paris VI	Allocataire moniteur normalien	10/89	07/91	
École Polytechnique	Service national	08/91	07/92	
Paris VI	Allocataire moniteur normalien	08/92	09/93	
INRIA Rocquencourt	Chargé de recherche 2ème classe	10/93	12/95	
INRIA Rocquencourt	Chargé de recherche 1ère classe	01/96		

[1] *For each position, indicate grade or rank. For example, for a tenured civil service position, indicate the branch and rank,*

3. Développements technologiques : Description de Logiciel ou Autre Réalisation/ *Technology development : Description of Software or Other Realization*

1. (2000) J'ai implémenté, en `Aldor` (anciennement `Axiom`, anciennement `Scratchpad II`) l'algorithme de Sudan pour les codes géométriques dits *hermitiens*.
2. (2002) J'ai implémenté l'algorithme de Sudan de décodage des codes de Reed-Solomon en `C`. J'ai utilisé cet algorithme dans le cadre d'un contrat avec Canal+, pour analyser un algorithme de chiffrement développé en interne à Canal+.
3. Dans le cadre du projet européen Aquarelle (1995-1998), j'ai réalisé, avec Caroline Fontaine, un prototype de système client-serveur pour l'obtention des clés paramétrisant un algorithme de marquage des images. Nous avons implémenté un client capable d'uploader des images vers un serveur (implanté aussi) pour faire vérifier le watermark (conformément au protocole DHWM que nous avions défini à l'époque). Nous avons utilisé le protocole HTTP pour la couche réseau, Motif pour l'interface graphique, et GMP pour les grands entiers. Ce prototype a fait l'objet d'une démonstration aux représentants de la Commission Européenne.
4. Dans le cadre de l'ACI SERAC, une implantation du protocole de mise en accord de clé proposé avec Bhaskar a été faire. Cette implantation a été faite dans le cadre du simulateur réseau NS2, pou étudier l'impact des pertes réseau sur la composition de groupes sécuriés.

4. Transferts technologiques résultant de la recherche/ *Technology transfer of research result*

Contrats industriels.

1. Aquarelle 1995-1997, coordonné par Alain Michard. Aquarelle était un projet de Recherche et Développement soutenu par le programme « Applications Télématiques » du cinquième PCRD de l'Union Européenne. Il s'agissait de mettre un place un système de diffusion et de partage de l'information présente dans le patrimoine culturel européen. Il a été mis en place un consortium européen regroupant des institutions culturelles, des éditeurs, des entreprises industrielles technologiques, et des laboratoires de recherche.

   Les partenaires culturels étaient très attentifs au problème de la protection des droits d'auteurs. J'ai contribué au livrable D5.4 « IPR protection for multimedia assets », et avec Caroline Fontaine, nous avons défini un protocole de gestion de clés pour le marquage d'images. Le groupe TELE (Benoit Macq) de l'université catholique de Louvain a été sous-contractant, en fournissant un algorithme de marquage d'image. Nous avons réalisé un prototype intégrant la gestion des clés et l'algorithme de Louvain.
2. Canal+, février-juin 2002. Expertise, avec Anne Canteaut, d'un algorithme de chiffrement symétrique développé en interne à Canal+. Dans ce cadre, j'ai utilisé mon implémentation de l'algorithme de Sudan, pour essayer de trouver des approximations de l'algorithme de Canal+.
3. Banque de France, décembre 2003-mars 2004. Étude de la possibilité de mettre un authentifiant cryptographique, variable, sur chaque billet, dépendant de données imprimées invisibles sur chaque billet.

Contrats de recherche.

1. ARC INRIA Courbes (1999-2001(: projet rassemblant le LIX (François Morain), Limoges (Iwan Duursma), et le projet CODES, en courbes algébrique et théorie des nombres, pour le codage et la cryptographie.
2. CRAC I (2000-2003) et II (2002-2005) : premières ACI Cryptologie, soutien aux équipes d'excellence.
3. ACI PolyCrypt : 2001-2004 : avec le projet Spaces (Jean-Charles Faugère, Guillaume Hanrot) et le LACO de l'université de Limoges (Philippe Gaborit) : étude des systèmes polynomiaux intervenant dans les systèmes cryptographiques. C'est dans ce cadre que Jean-Charles Faugère a cassé le cryptosystème HFE.

---

for a private sector position or non-tenured position in a public institution, indicate the nature of the work contract, etc.

4. ECRYPT – Réseau d'excellence européen (NoE) en cryptologie. Je suis intervenu dans le laboratoire virtuel STVL (Symmetric Techniques Virtual Labs).
5. ACI SERAC, 2004-2007 : models and protocols for SEcuRity in wireless Ad hoC networks. Avec Farid Naït-Abdesselam de l'USTL (Université des Sciences et Techniques de Lille), Jean Leneutre du GET (Groupe des Ecoles des Télécommunications) et managée par Caroline Fontaine. L'INRIA est présente avec Codes, Tanc et HiperCom qui proposent des algorithmes et des protocoles cryptographiques adaptés aux réseaux Ad Hoc.
6. 2006- ANR EDHASH : Evaluation and Design of cryptographic HASH functions. Avec l'UVSQ (Antoine Joux). À la suite des attaques de Wang sur les principales fonctions de hachage cryptographiques, il faut des fonctions de remplacement. Nous travaillons à l'étude et la généralisation de la cryptanalyse de Wang, ainsi qu'à la construction d'une nouvelle fonction, à partir de celle que j'ai construite avec M. Finiasz et N. Sendrier.
7. 2008- Offre de maturation technologique (OMT Digiteo) CryptoNet : Proof-of-concept of security in ad-hoc networks using elliptic curves. Dans le projet TANC en collaboration avec Hipercom, développement d'une implantation standard de la cryptologie à base de courbes elliptiques, avec mise en place de PKIs, et peut-être de protocole de mise en accord de clé de groupe.

5. Encadrement d'activités de recherche/*Supervision of research activities*

Thèse de Lancelot Pecquet : Décodage en liste des codes géométriques Co-encadrée avec Pascale Charpin, soutenue le 18 décembre 2001. J'ai assuré toute la direction scientifique. Cette thèse a été consacrée à l'étude et à l'implantation des algorithmes de Sudan et Guruswami-Sudan, pour décoder les codes de Reed-Solomon et les codes géométriques. Ces algorithmes consitutent une percée fondamentale en codage : ils permettent de décoder beaucoup mieux les codes ultra-classiques que sont les codes de Reed-Solomon, qui sont employés partout. Lancelot Pecquet a contribué à améliorer la complexité algorithmique de ces algorithmes.
Lancelot Pecquet est maintenant maître de conférence à l'université de Poitiers.

Thèse de Cédric Tavernier : Testeurs, problèmes de reconstruction univariés et multivariés, et application à la cryptanalyse du DES Co-encadrée avec Pascale Charpin, soutenue le 15 janvier 2004. J'ai assuré toute la direction scientifique à 50%.
Cédric Tavernier a étudié le pendant « multivarié de l'algorithme de Sudan », c'est-à-dire le décodage des codes de Reed-Muller, en se basant sur l'algorithme de Goldreich et Levin. Ce décodage peut aussi être vu comme un algorithme d'approximation par des polynômes. Cédrix Tavernier a appliqué cet algorithme à la sortie de l'algorithme de chiffrement DES, obtenant ainsi de nouvelles équations permettant la cryptanalyse linéaire de Matsui.
Cédric Tavernier travaille aujourd'hui dans le laboratoire de cryptographie de Thalès Communication.

Thèse de Magali Bardet : Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie Co-encadrée (50%) avec Jean-Charles Faugère, soutenue le 8 décembre 2004.
Partie codes de la thèse : beaucoup de codes n'ont pas d'algorithme de décodage dédié (au contraire des codes BCH par exemple). Il est toutefois possible de les décoder en résolvant des systèmes d'équations algébriques que l'on résout avec des outils de calcul de bases de Gröbner. Il est apparu que les algorithmes de base de Gröbner sont efficaces grâce à de nouvelles mises en équation plus pertinentes. Dans la partie sur la cryptographie de la thèse, Magali Bardet a étudié la complexité des algorithmes de calcul de bases de Gröbner, avec application au cryptosystème HFE.
Magali Bardet est maintenant maître de conférences à l'université de Rouen.

Thèse de Raghav Bhaskar : Cryptographic protocols for Ad Hoc networks Co encadrée (80%) avec Valérie Issarny, soutenue le 26 juin 2006.
Le sujet de départ était la sécurisation du système de fichiers AdHocFS, développé dans le projet Arles. Il a semblé immédiatement intéressant d'élaborer une solution à base de protocoles de mise en accord de clés, qui sont une généralisation à n utilisateurs du protocole de Diffie-Hellman. Nous avons au bout du compte produit une contribution dans ce domaine, qui est meilleure à de nombreux points de vue que l'existant. Enfin au delà du monde parfait de la cryptogaphie, il a été proposé une *vraie* mise en œuvre de ce procole, à travers une collaboration avec HiperCom (Paul Mühlethaler et Cédric Adjih) : du point de vue l'applicabilité aux réseaux, notre protocole est le meilleur.
Raghav Bhaskar est maintenant PostDoc à Microsoft Research, Bangalore.

Stages
- Stage de Rajesh Kumar, 2007. Implantation du protocole de mise en accord de clé multi-utilisateurs dans le contexte du simulateur réseau NS2. Coencadré avec Cédric Adjih d'Hipercom.
- Stage de Frank Giton, Master Cryptographie/Codage/Calcul de l'université de Limoges : *étude de l'algorithme cyclotomique de Fedorenko*, septembre 2007. Fedorenko a proposé en 2006 une optimisation très agressive de la transformée de Fourier, basée sur la notion de base normale, efficace dès les petites tailles. Le but du stage était de comprendre l'algorithme et de l'implanter.
- Stage d'AlexanderZeh, Diplôme d'ingénieur de l'ENST Paris : *généralisation de l'équation clé de Roth et Ruckenstein*, février 2008. On oppose généralement le décodage par syndrome au décodage par interpolation. En 2000, Roth et Ruckenstein ont synthétisé les deux approches, en produisant une « équation clé » pour l'algorithme de Sudan. Le but du stage est de produire une équation clé pour l'algorithme de Guruswami-Sudan.

6. Enseignement/ *Teaching*

1. TD de Caml en license d'informatique à Paris VI (Thèrese Hardin enseignant) en 2000-2001. Ce module a ensuite été arrété. Je me suis investi dans ce cours à cause de l'intérêt que j'avais pour le projet Focal.
2. TD de java à l'École polytechnique en 2001.
3. Cours de codes correcteurs d'erreurs dans le DEA Algorithmique, Paris VI, 2001-2004, 20 heures partagées avec Jean-Pierre Tillich. Ce DEA a été intégré dans le Master MPRI :
4. Master MPRI (Master Parisien de Recherche en Informatique), 2004-2008, où j'enseigne toujours (51 heures, partagées avec Jean-Charles Faugère et Jean-Pierre Tillich). Ce dernier cours permet de développer les liens entre algorithmes de calcul formel.
5. Cours de cryptologie dans le DEA Informatique Fondamentale et Applications de l'université de Marne-la-Vallée (2003-2005). Devenu le Mastère Informatique Recherche où j'enseigne toujours (2005-2007).
6. En 2007 et en 2008, Travaux dirigés de cryptographie en Java à l'École Polytechnique, avec Andreas Enge, correspondants au cours de Majeure de François Morain.

7. Diffusion de l'information scientifique/ *Dissemination of scientific knowledge*

1. Cours de cryptographie (six heures) avec Anne Canteaut, à destination d'ingénieurs réseaux, organisé par FNET (Association pour la promotion de l'Internet en France) en 1995.
   J'ai aussi fait ce cours de cryptographie devant les ingénieurs ITA de Rocquencourt (1996).
2. Dans le cadre du séminaire Aristote (`http://www.aristote.asso.fr/`), lors de la journée « La sécurité des réseaux : sommes nous toujours protégés ? », du 20 Janvier 2000, j'ai fait un exposé intitulé « Cryptosystèmes, algorithmes et longueur de clés ».
   J'ai aussi présenté ce thème au séminaire groupe OSSIR (Observatoire de la Sécurité des Systèmes d'information et des Réseaux, `http://www.ossir.org/`) en Octobre 1999 .

3. J'ai présenté les travaux avec Hipercom sur le Diffie-Hellman généralisé aux rencontres INRIA-Industrie du 11 octobre 2007, sur le thème de la sécurité.

Articles :

1. Daniel Augot. Les travaux de M. Sudan sur les codes correcteurs d'erreurs. *Gazette des Mathematiciens*, 98, October 2003.
2. Daniel Augot. Madhu Sudan's work on error-correcting codes. *European Mathematical Society Newsletter*, 51 :8–10, March 2004. `http://www.emis.de/`.

8. Collaborations, mobilité/*Collaborations, visits*

Mobilité géographique Séjour à Sherbrooke (Québec) : Juillet-Août-Septembre 1994. Visite de Bernard Courteau, étude des codes correcteurs d'erreur géométriques.

Mobilité thématique 1995-1997, Protection des droits d'auteurs dans le cadre du projet européen Aquarelle, coordonné par Alain Michard. Ce projet à grande échelle visait à construire un système multimédia distribué pour unifier et présenter le patrimoine culturel européen. J'ai étudié, avec Caroline Fontaine, les solutions à base de *watermarking* pour protéger les ayants droits des images diffusées par ce système. Cela m'a amené à comprendre les outils utilisés (Z39.50 –outil de base de données employés par les grandes bibliothèques– SGML, bases de données hétérogènes).

9. Responsabilités collectives/*Responsibilities*

1. Comité de lecture des colloques WCC 99, 01, 03, 05 (Workshop on Coding and Cryptography).
2. Édition des actes des colloques WCC 99, 01, 03.
3. Co-Chair, avec Nicolas Sendrier de WCC 2007.
4. Comité de lecture de ICPSS (International Conference on Polynomial System Solving, Paris, Novembre 2004).
5. Editeur, avec Ludovic Perret et Jean-Charles Faugère d'un numéro spécial de Journal of Symbolic Computation, sur le thème "Gröbner Bases Techniques in Cryptography and Coding Theory" (2007-2008).
6. Membre du comité de programme des journées C2 2008 (Codage et Cryptographie). Webmestre du site et du seveur de soumission (`http://C2-2008.inria.fr/C2`).

Responsable permanent du projet Codes jusqu'en décembre 2007.
Jurys de thèse (hors des thèsards que j'ai encadrés) :

1. Gaëtan Haché (Construction effective des codes géométriques, 1996, Paris VI),
2. Caroline Fontaine (Contribution à la recherche de fonctions booléennes hautement non linéaires, et au marquage d'images en vue de la protection des droits d'auteur, 1998, Paris VI),
3. Mireille Fouquet (Anneau d'endomorphismes et cardinalité de courbes elliptiques : aspects algorithmiques, 2001, École Polytechnique),
4. Daniele Raffo (Security Schemes for the OLSR Protocol for Ad Hoc Networks, Paris VI, 2005).
5. Andrew Brown EPFL 2007 (Codes, graphs and graph based codes), rapporteur.

Direction de l'ARC (Action de Recherche Concertée de l'INRIA) « Arc Courbes » (LIX, Limoges, Codes).

Formulaire 6/*Form 6*

LISTE COMPLÈTE DES PUBLICATIONS[2]
COMPLETE PUBLICATION LIST[3]

Nom/*Last name*: Augot Prénom/*First name*: Daniel

Most relevant publications on `http://www-rocq.inria.fr/secret/Daniel.Augot/articlesDR2.html`

Articles dans des revues avec comité de lecture

1. Daniel Augot, Pascale Charpin, and Nicolas Sendrier. Sur une classe de polynômes scindés de l'algèbre $F_{2^m}[Z]$. *Comptes Rendus de l'Académie des Sciences*, 312 :649–751, 1991.
2. Daniel Augot, Pascale Charpin, and Nicolas Sendrier. Studying the locator polynomial of minimum weight codewords of BCH codes. *IEEE Transactions on Information Theory*, 38(3) :960–973, 1992. `http://ieeexplore.ieee.org/xpls/abs\_all.jsp?arnumber=135638`.
3. Daniel Augot and Paul Camion. Forme de Frobenius et vecteurs cycliques. *Comptes rendus de l'Académie des Sciences*, 318 :183–188, 1993.
4. Daniel Augot and Nicolas Sendrier. Idempotents and the BCH bound. *IEEE Transactions on Information Theory*, 40(1) :204–207, January 1994.
5. Daniel Augot. Description of minimum weight codewords of cyclic codes by algebraic systems. *Finite Fields Appl.*, 2(2) :138–152, 1996.
6. Daniel Augot and Françoise Lévy dit Véhel. Bounds on the minimum distance of the duals of BCH code. *IEEE Transactions on Information Theory*, 1996.
7. Daniel Augot and Paul Camion. On the computation of minimal polynomials, cyclic vectors and Frobenius forms. *Linear Algebra and its Applications*, 260 :61–94, 1997.
8. Daniel Augot, Jean-Marc Boucqueau, Jean-François Delaigle, Caroline Fontaine, and Eddy Goray. Secure delivery of images over open networks. *Proceedings of the IEEE*, 87(7) :2605–2614, November 1999.
9. Daniel Augot and Lancelot Pecquet. A Hensel lifting to replace factorization in list-decoding of Algebraic-Geometric and Reed-Solomon codes. *IEEE Transactions on Information Theory*, 46(7) :2605–2614, November 2000.
10. Daniel Augot, Raghav Bhaskar, Valerie Issarny, and Daniele Sacchetti. A three round authenticated group key agreement protocol for adhoc networks. *Pervasive and Mobile Computing*, 3(1) :36–52, 2007. `http://www.sciencedirect.com/science/article/B7MF1-4KTVPCX-1/2/69e95fcd%91a4ec5a8dc05ed06301def`
11. Daniel Augot, Magali Bardet, and Jean-Charles Faugère. On the decoding of cyclic codes with the newton's identities. *Journal of Symbolic Computation*, page : 29 pages, 2008. Special Issue on Gröbner Bases Techniques in Cryptography and Coding Theory.
12. Daniel Augot, Emanuele Betti, and Emmanuela Orsini. *An Introduction to cyclic codes.* Springer, 2007. soumis.
13. Daniel Augot and Mikhail Stepanov. *A note on the generalisation of the Guruswami-Sudan list decoding algorithm to Reed-Muller codes.* Springer, 2007. soumis.

[2] Les publications les plus significatives devront être consultables sur la page web du candidat.

[3] *Most relevant publications have to be available for consultation via the web page of the applicant.*

Articles longs dans des conférences internationales avec comité de lecture

1. Daniel Augot, Pascale Charpin, and Nicolas Sendrier. Weights of some binary cyclic codes throughout the Newton's identities. In Gérard Cohen and Pascale Charpin, editors, *Eurocode 90*. Springer-Verlag, 1990.
2. Daniel Augot. A deterministic algorithm for computing a normal basis in a finite field. In *Eurocodes 94*, Abbaye de la Bussière, France, 1994.
3. Daniel Augot, Jean-Francois Delaigle, and Caroline Fontaine :. A scheme for managing watermarking keys in the Aquarelle multimedia distributed system. In Jean-Jacques Quisquater, Yves Deswarte, Catherine Meadows, and Dieter Gollmann, editors, *ESORICS*, number 1485 in Lecture Notes in Computer Science. Springer-Verlag, 1998.
4. Daniel Augot and Caroline Fontaine. Key issues for watermarking digital images. In *SPIE, EUROPTO - Conference on Electronic Imaging : Processing, Printing, and Publishing in Color, EUROPTO*, pages 176–185, Zürich, Suisse, 1998.
5. Daniel Augot and Matthieu Finiasz. A public key encryption scheme based on the polynomial reconstruction problem. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003*, number 2656 in Lecture Notes in Computer Science, pages 229–240. Springer-Verlag, 2003.
6. Daniel Augot, Matthieu Finiasz, and Nicolas Sendrier. A family of fast syndrome based cryptographic hash functions. In Ed Dawson and Serge Vaudenay, editors, *Progress in Cryptology - Mycrypt 2005 : First International Conference on Cryptology in Malaysia*, number 3715 in Lecture Notes in Computer Science, pages 64–83. Springer-Verlag, 2005.
7. Raghav Bhaskar, Daniel Augot, Valérie Issarny, and Daniele Sacchetti. An efficient group key agreement protocol for ad hoc networks. In *WOWMOM '05. IEEE Workshop on Trust, Security and Privacy in Ubiquitous Computing*, Taormina, Italy, 2005.
8. Daniel Augot, Mostafa El-Khamy, Robert J McEliece, Farzad Parvaresh, Mikhail Stepanov, and Alexander Vardy. List decoding of Reed-Solomon product codes. In *Proceedings of the Tenth International Workshop on Algebraic and Combinatorial Coding Theory, Zvenigorod, Russia*, pages 210–213, September 2006.
9. Daniel Augot, Magali Bardet, and Jean-Charles Faugère. On formulas for decoding binary cyclic codes. In *IEEE Internation Symposium on Information Theory (ISIT 2007)*, Nice, France, 2007. `http://www-rocq.inria.fr/secret/Daniel.Augot/decode_cyclique.pdf`.

Résumés courts dans des conférences internationales avec comité de lecture

1. Daniel Augot, Pascale Charpin, and Nicolas Sendrier. On the minimum weight of some binary BCH codes. In *IEEE Internation Symposium on Information Theory*, page 7, Budapest, Hungary, 1991.
2. Daniel Augot. Algebraic characterization of minimum weight codewords of cyclic codes. In *IEEE International Symposium on Information Theory 94*, Trondheim, Norway, June 1994.
3. Daniel Augot and Françoise Lévy dit Véhel. Bounds on the minimum distance of the duals of BCH codes. In *IEEE International Symposium on Information Theory*, Trondheim, Norway, 1994.
4. Daniel Augot. Algebraic equations for minimum weight codewords of many codes. In *International Conference on Finite Field and Applications*, Glasgow, Scotland, 1995.
5. Daniel Augot. Newton's identities for minimum codewords of a family of alternant codes. In *IEEE International Symposium on Information Theory (ISIT 95)*, Whistler, Canada, 1995.
6. Daniel Augot. Algebraic solutions of Newton's identities for cyclic codes. In *Proceedings of the 1998 Information Theory Workshop*, Killarney, Irland, 1998.
7. Daniel Augot. A parallel version of a special case of the Sudan decoding algorithm. In *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*, Lausanne, 2002.

8. Daniel Augot, Magali Bardet, and Jean-Charles Faugère. Efficient decoding of (binary) cyclic codes above the correction capacity of the code using Gröbner bases. In *IEEE International Symposium on Information Theory*, Yokohama, Japan, 2003.
9. Raghav Bhaskar, Daniel Augot, Cédric Adjih, Paul Mühlethaler, and Saadi Boudjit. AGDH (Asymmetric Group Diffie Hellman) an efficient and dynamic group key agreement protocol for Ad Hoc networks. In *NTMS 2007, International Conference on New Technologies, Mobility and Security*, 2007. **Poster**, extended abstract on `http://www-rocq.inria.fr/secret/Daniel.Augot/AdHocGKA-NTMS07.pdf`.

Conférences internationales

1. Daniel Augot and Nicolas Sendrier. Idemptotents and the BCH bound. In *Sixth Joint Swedish -Russian International Workshop on Information Theory*, Mölle, 1993.
2. Daniel Augot. Computing normal bases in finite fields. In Jacques Calmet, editor, *Rhine Workshop on Computer Algebra*, Karlsruhe, 1994.
3. Daniel Augot. Computing Groebner bases for finding codewords of small weight. In *The 2nd IMACS Conference on Applications of Computer Algebra*, Linz, Austria, 1996.
4. Daniel Augot. Protection des droits et marquage d'image. In *Electronic Imaging and The Visual Arts (EVA'96)*, 1996.
5. Daniel Augot and Anne Canteaut. Cryptologie pour la sécurité des communications. In *CARI 98, colloque africain de recherche en informatique*, Dakar, Sénégal, 1998.
6. Nicolas Sendrier, Daniel Augot, Matthieu Finiasz, and Pierre Loidreau. Diversity in public key cryptography using coding theory and related problems. In *STORK cryptography workshop*, Bruges, Belgium, november 2002. workshop préparatoire du réseau d'excellence E-CRYPT.
7. Daniel Augot, Magali Bardet, and Jean-Charles Faugère. Decoding cyclic codes with algebraic systems. In Luxembourg Belgian (BMS), Dutch (KWG) and French (SMF) Mathematical Societies, editors, *Joint BeNeLuxFra Conference in Mathematics*, May 2005.
8. Daniel Augot, Matthieu Finiasz, and Nicolas Sendrier. A family of fast syndrome based cryptographic hash functions. In European Network of Excellence in Cryptology ECRYPT, editor, *Ecrypt Conference on Hash Functions, Krakow, Poland*, Krakow, Poland, 2005. `http://www.ecrypt.eu.org/stvl/hfw/`.
9. Daniel Augot and Mikhail Stepanov. Decoding Reed-Muller codes with the Guruswami-Sudan's algorithm. In *The Claude Shannon workshop on Coding and Cryptography*, Cork, Ireland, May 2006.
10. Daniel Augot and Mikhail Stepanov. Decoding Reed-Muller codes with the Guruswami-Sudan's algorithm. In *Workshop D1 : Groebner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics, within the Special Semester on Groebner Bases at RICAM and RISC*, Linz, Austria, 2006. `http://www.ricam.oeaw.ac.at/specsem/srs/groeb/schedule_D1.html`.
11. Daniel Augot. Multivariate generalizations of the Guruswami-Sudan list decoding algorithm. In *Oberwolfach workshop on Coding Theory*, 2007. **Invited**.
12. Daniel Augot, Magali Bardet, and Jean-Charles Faugère. On the Newton's identities for decoding cyclic codes with Gröbner bases. In *The Claude Shannon workshop on Coding and Cryptography*, Cork, Ireland, May 2007.

Rappors techniques et de recherche

1. Daniel Augot, Pascale CHarpin, and Nicolas Sendrier. Studying the locator polynomials of minimum weight codewords of BCH codes. Technical Report 1488, INRIA, July 1991. `http://www.inria.fr`.
2. Daniel Augot and Paul Camion. The minimal polynomials, characteristic subspaces, normal bases and the Frobenius from. Technical Report 2006, INRIA, 1993. `http://www.inria.fr`.
3. Daniel Augot and Caroline Fontaine. D5.4 : IPR protection for multimedia assets, 1997.

4. Daniel Augot and Lancelot Pecquet. An alternative to factorization : a speedup for Sudan's decoding algorithm and its generalization to algebraic-geometric codes. Technical Report 3532, INRIA, Octobre 1998. `http://www.inria.fr`.
5. Daniel Augot, Magali Bardet, and Jean-Charles Faugère. Efficient decoding of (binary) cyclic codes beyond the correction capacity of the code using Gröbner bases. Technical Report 4652, INRIA, Novembre 2002. `http://www.inria.fr`.
6. Daniel Augot, Matthieu Finiasz, and Pierre Loidreau. Using the trace operator to repair the polynomial reconstruction based cryptosystem, presented at eurocrypt 2003. Cryptology ePrint Archive, Report 2003/209, 2003. `http://eprint.iacr.org/`.
7. Daniel Augot, Matthieu Finiasz, and Nicolas Sendrier. A fast provably secure cryptographic hash function. `eprint.iacr.org`, 2003.
8. Daniel Augot, Matthieu Finiasz, and Nicolas Sendrier. A family of fast syndrome based cryptographic hash functions. Technical Report 5592, INRIA, Juin 2005. `http://www.inria.fr`.
9. Daniel Augot, François Morain, Caroline Fontaine, Jean Leneutre, Stéphane Maag, Anna Cavalli, and Farid Naït-Abdesselam. Review of vulnerabilities in mobile ad-hoc networks : trust and routing protocols views. Technical report, ACI SERAC, 2005. Internal delivrable de l'action concertée incitative SERAC.
10. A. Canteaut (Ed.), D. Augot, A. Biryukov, A. Braeken, C. Cid, H. Dobbertin, H. Englund, H. Gilbert, L. Granboulan, H. Handschuh, M. Hell, T. Johansson, A. Maximov, M. Parker, T. Pornin, B. Preneel, M. Robshaw, and M. Ward. Open research areas in symmetric cryptography and technical trends in lightweight cryptography. Technical report, Réseau d'excellence européen ECRYPT, 2005.
11. Raghav Bhaskar, Paul Mühlethaler, Daniel Augot, Cédric Adjih, and Saadi Boudjit. Efficient and dynamic group key agreement in Ad Hoc networks. Technical Report RR-5915, INRIA, 2006. `http://hal.inria.fr/inria-00071348`.
12. Anne Canteaut (ed.), D. Augot, C. Cid, H. Englund, H. Gilbert, M. Hell, T. Johansson, M. Parker, T. Pornin, B. Preneel, and M. Robshaw. Ongoing research areas in symmetric cryptography. Technical report, Réseau d'excellence européen ECRYPT, Mars 2007. `http://www.ecrypt.eu.org/documents/D.STVL.5-1.1.pdf`.

Colloques nationaux

1. Daniel Augot. Introduction à la cryptologie des courbes elliptiques. In *27ème École de printemps d'informatique théorique, Codage et cryptographie*, Batz-sur-mer, France, 1999.
2. Daniel Augot. Algorithme de décodage de sudan et cryptanalyse. In *Journées nationales de calcul formel*, CIRM, Luminy, 20-24 janvier 2003 2003.
3. Daniel Augot. Chiffrement et signature. In *École des Jeunes Chercheurs an Algorithmique et Calcul formel*. Institut Gaspard Monge, laboratoire d'Informatique, 31 mars - 4 avril 2003.
4. Daniel Augot. Application des algorithmes de décodage par interpolation en cryptanalyse. In *Journées nationales du GDR Informatique Mathématique 2007*, Institut Henri Poincaré, 2007.

Articles dans des revues sans comité de lecture

1. Daniel Augot. Protection of intellectual property rights related to images. *ERCIM News*, April 1998. `http://www.ercim.org`.
2. Daniel Augot. Les travaux de M. Sudan sur les codes correcteurs d'erreurs. *Gazette des Mathematiciens*, 98, octobre 2003.
3. Daniel Augot. Madhu Sudan's work on error-correcting codes. *European Mathematical Society Newsletter*, 51 :8–10, March 2004. `http://www.emis.de/`.

Édition de comptes rendus

1. Daniel Augot and Claude Carlet, editors. *Workshop on Coding and Cryptography*, Paris, France, 1999. INRIA.
2. Daniel Augot and Claude Carlet, editors. *Workshop on Coding and Cryptography*, Paris, France, January 2001. ESAT.
3. Daniel Augot, Pascale Charpin, Tor Helleseth, Gregor Leander, and Nicolas Sendrier, editors. *Design, Codes and Cryptography, WCC2007 Special Issue on Coding and Cryptography.* Springer, 2008. In Memory of Hans Dobbertin.
4. Daniel Augot, Pascale Charpin, and Grigory Kabatianski, editors. *Workshop on Coding and Cryptography*, Versailles, France, March 2003. ESAT.
5. Daniel Augot, Nicolas Sendrier, and Jean-Pierre Tillich, editors. *Workshop on Coding and Cryptography*, Versailles, France, 2007. INRIA.

Diplômes

1. Daniel Augot. *Étude algébrique des mots de poids minimum des codes cycliques, méthodes d'algèbre linéaire sur les corps finis.* PhD thesis, Université Pierre et Marie Curie, Paris VI, 1993.
2. Daniel Augot. *Décodage des codes algébriques et cryptographie* HDR, Université Pierre et Marie Curie, Paris VI, 2007.

Most relevant publications on `http://www-rocq.inria.fr/~augot/articlesDR2.html`