Dossier de candidature à la qualification aux fonctions de Professeur des Universités

Pour la section 27

Duong Hieu PHAN

Curriculum Vitæ

1 Identification

Nom	PHAN
Prénom	Duong-Hieu
Etat civil	Marié, 36 ans
Date/lieu de naissance	12 juin 1978, à Hanoi, Vietnam
Grade	Maître de conférences, HdR obtenue le 19/11/2014
Section CNU	25
Nationalités	France, Vietnam
E-mail	hieu.phan@univ-paris8.fr ; duong-hieu.phan@ens.fr
Web	http://www.di.ens.fr/users/phan/
Association	IACR - International Association for Cryptologic Research (depuis 2002)

2 Parcours

2007 - présent	**Maître de conférences** LAGA - UMR 7539 (Laboratoire Analyse, Géométrie et Applications) Université Paris 8, Vincennes-Saint Denis Membre associé au Crypto Team, Ecole normale supérieure	
2006 - 2007	**Ingénieur de recherche** France Télécom R&D, Issy-les-Moulineaux	**France**
2005 - 2006	**Post-doc en cryptographie** University College London	**Royaume-Uni**
2002 - 2005	**Doctorat en informatique** Département d'Informatique - École normale supérieure, Paris Directeur de thèse : David Pointcheval	**France**
2001 - 2002	**DEA Algorithmique** Université de Paris 7 – Denis Diderot Stage au département d'Informatique - École normale supérieure	**France**
1996 - 2001	**Diplôme d'Ingénieur** en Technologies de l'Information École Polytechnique de Hanoi	**Vietnam**

3 Activités d'enseignement

2014 – 2015	**Université Paris 8**
	Cours/TD de Master 2 : Cryptographie Avancée 2 (48h TD)
	(Master en co-habilitation avec l'Université Paris 7)
	Cours/TD de Licence : Combinatoire (48h TD)
2013 – 2014	**Université Paris 8**
	Cours/TD de Master 2 : Sécurité prouvable en cryptographie (48h TD)
	Cours/TD de Licence : Combinatoire (48h TD)
2012 – 2013	**Université Paris 8**
	Cours/TD de Master 2 : Sécurité prouvable en cryptographie (48h TD)
	Cours/TD de Licence : Combinatoire (48h TD)
2011 – 2012	**Université Paris 8**
	Cours/TD de Master 2 : Sécurité prouvable en cryptographie (48h TD)
2010 – 2011	**Université Paris 8**
	Cours/TD de Master 2 : Sécurité prouvable en cryptographie (48h TD)
2009 – 2010	**Université Paris 8**
	Cours/TD de Master 2 : Sécurité prouvable en cryptographie (48h TD)
	Cours/TD de Master 1 : Théorie de la complexité (48h TD)
	(Master en co-habilitation avec l'Université Paris 13)
	Cours/TD de Licence : Algèbre linéaire (48h TD)
	Cours/TD de Licence : Combinatoire (48h TD)
2008 – 2009	**Université Paris 8**
	Cours/TD de Master 2 : Sécurité prouvable en cryptographie (48h TD)
	Cours/TD de Master 1 : Théorie de la complexité (48h TD)
	Cours/TD de Licence : Analyse (Séries de fonctions) (48h TD)
2007 – 2008	**Université Paris 8**
	Cours/TD de Master 2 : Sécurité prouvable en cryptographie (48h TD)
	Cours/TD de Master 1 : Théorie de la complexité (48h TD)
	Cours/TD de Licence : Analyse (Séries de fonctions) (48h TD)
	TD de Licence : Mathématiques générales (48h TD)
2004 – 2005	**École polytechnique** (1ère année)
	TD : Les bases de la programmation et de l'algorithmique (40h TD)
2004 – 2005	**ENSTA -** École Nationale Supérieure de Techniques Avancées (2ème année)
	TD : La programmation en C (15h TD)
2003 – 2004	**École polytechnique** (1ère année)
	TD : Les bases de la programmation et de l'algorithmique (40h TD)
2003 – 2004	**ENSTA -** École Nationale Supérieure de Techniques Avancées (2ème année)
	TD : La programmation en C (15h TD)

4 Publications

4.1 Articles après la thèse de doctorat [2006-2014]

[1] **Hardness of k-LWE and Applications in Traitor Tracing**
San Ling, Duong Hieu Phan, Damien Stehlé and Ron Steinfeld.
In Advances in Cryptology – CRYPTO '14, Pages 315-334, LNCS 8616, 2014.

[2] **Black-box Trace&Revoke Codes**
Hung Q. Ngo and Duong Hieu Phan and David Pointcheval.
In Algorithmica, Springer, vol. 67, no. 3, Pages 418-448, 2013.

[3] **Adaptive CCA Broadcast Encryption with Constant-Size Secret Keys and Ciphertexts**
Duong Hieu Phan, David Pointcheval, Siamak F Shahandashti and Mario Strefler
In IJIS - International Journal of Information Security, vol. 12,, no. 4, Pages 251-265, 2013.

Multi-Channel Broadcast Encryption

[4] *Duong Hieu Phan, David Pointcheval and Viet Cuong Trinh*
In ASIACCS 2013, ACM Symposium on Information, Computer and Communications Security, ACM Press, Pages 277-286, 2013

[5] **Optimal Public Key Traitor Tracing Scheme in Non-Black Box Model**
Philippe Guillot, Abdelkrim Nimour, Duong Hieu Phan and Viet Cuong Trinh.
In AFRICACRYPT 2013, LNCS 7918, pages 140-155, Springer-Verlag, 2013.

[6] **Key-Leakage Resilient Revoke Scheme Resisting Pirates 2.0 in Bounded Leakage Model**
Duong Hieu Phan and Viet Cuong Trinh.
In AFRICACRYPT 2013, LNCS 7918, pages 342-358, Springer-Verlag, 2013.

[7] **Generalized Key Delegation for Wildcarded Identity-Based and Inner-Product Encryption**
Michel Abdalla, Angelo De Caro and Duong Hieu Phan
In IEEE-TIFS, IEEE Transactions on Information Forensics & Security, Volume 7 , Issue: 6, Pages 1695 - 1706, 2012.

[8] **Message Tracing with Optimal Ciphertext Rate**
Duong Hieu Phan, David Pointcheval and Mario Strefler
In LatinCrypt' 2012, LNCS 7533, pages 56-77, Springer-Verlag, 2012.

[9] **Decentralized Dynamic Broadcast Encryption**
Duong Hieu Phan, David Pointcheval and Mario Strefler
In SCN' 2012, LNCS 7485, pages 166-183, Springer-Verlag, 2012.

[10] **Security Notions for Broadcast Encryption**
Duong Hieu Phan, David Pointcheval and Mario Strefler
In ACNS' 2011, LNCS 6715, pages 377-394, Springer-Verlag, 2011.
(Best student paper award for Mario Strefler)

[11] **Identity-Based Trace and Revoke Schemes**
Duong Hieu Phan and Viet Cuong Trinh.
In ProvSec' 2011, LNCS 6980, pages 204-221, Springer-Verlag, 2011.

[12] **Traitors Collaborating in Public: Pirates 2.0**
Olivier Billet and Duong Hieu Phan.
In Advances in Cryptology – Eurocrypt '09, Pages 189-205, LNCS 5479, Springer-Verlag, 2009.

[13] **Efficient Traitor Tracing from Collusion Secure Codes.**
Olivier Billet and Duong Hieu Phan.
In Proceeding of ICITS '08 -The 3rd International Conference on Information Theoretic

Security, Pages 171-182, LNCS 5155, Springer-Verlag, 2008.

[14] **A CCA Secure Hybrid Damgaard's ElGamal Encryption.**
Yvo Desmedt and Duong Hieu Phan.
In Proceeding of ProvSec '08, Lecture Notes in Computer Science Vol. 5324, pages 68-92, Springer-Verlag, 2008.

[15] **Hybrid Damgård Is CCA1-Secure under the DDH Assumption.**
Yvo Desmedt, Helger Lipmaa and Duong Hieu Phan.
In Proceeding of CANS '08 -The 7th International Conference on Cryptology and Network Security, Pages 18-30, LNCS 5339, Springer-Verlag, 2008.

[16] **Traitor Tracing with Optimal Transmission Rate.**
Nelly Fazio, Antonio Nicolosi and Duong Hieu Phan.
In Proceeding of ISC '07 - 10th International Conference on Information Security, Pages 71-88, LNCS 4779, Springer-Verlag, 2007.

[17] **Identity-based Traitor Tracing**
M. Abdalla, A.W. Dent, J. Malone-Lee, G. Neven, D.H. Phan and N.P. Smart
In Proceeding of PKC '07 - The International Conference on Theory and Practice of Public-Key Cryptography 2007, Pages 361-376, LNCS 4450, Springer-Verlag, @IACR, 2007.
Traitor Tracing for Stateful Pirate Decoders with Constant Ciphertext Rate
Duong Hieu Phan
In Proceeding of Vietcrypt '06 - International Conference on Cryptography in Vietnam 2006
Volume 4341, Lecture Notes in Computer Science, pp. 354–365, Springer-Verlag, 2006

[18] **Generic Construction of Hybrid Traitor Tracing with Full Public Traceability**
Duong Hieu Phan et Rei Safavi-Naini et Dong Vu Tonien
In Proceeding of ICALP '06 - 33rd International Colloquium on Automata, Languages and Programming
Volume 4052, Lecture Notes in Computer Science, pp. 264–275, Springer-Verlag, 2006

[19] **Public Traceability in Traitor Tracing Schemes**
Hervé Chabanne et Duong Hieu Phan et David Pointcheval
Advances in Cryptology – EUROCRYPT'05
Volume 3376, Lecture Notes in Computer Science, pp. 542–558, Springer-Verlag, 2005

[20] **Optimal Asymmetric Encryption and Signature Paddings**
Benoît Chevallier-Mames et Duong Hieu Phan et David Pointcheval
Proceeding of ACNS '05 : The Third Annual Conference on Applied Cryptography and Network Security
Volume 3494, Lecture Notes in Computer Science, pp. 254–268, Springer-Verlag, 2005

4.2 Articles pendant les années de la thèse de doctorat [2002-2005]

[21] **Public Traceability in Traitor Tracing Schemes**
Hervé Chabanne et Duong Hieu Phan et David Pointcheval
Advances in Cryptology – EUROCRYPT'05
Volume 3376, Lecture Notes in Computer Science, pp. 542–558, Springer-Verlag, 2005

[22] **Optimal Asymmetric Encryption and Signature Paddings**
Benoît Chevallier-Mames et Duong Hieu Phan et David Pointcheval
Proceeding of ACNS '05 : The Third Annual Conference on Applied Cryptography and Network Security
Volume 3494, Lecture Notes in Computer Science, pp. 254–268, Springer-Verlag, 2005

[23] **OAEP 3-Round : A Generic and Secure Asymmetric Encryption Padding**
Duong Hieu Phan and David Pointcheval
Advances in Cryptology – ASIACRYPT ’04.
Volume 3329 of Lecture Notes in Computer Science, pp. 63–77, Springer-Verlag, 2004.

[24] **On the Security Notions for Public-Key Encryption Schemes**
Duong Hieu Phan and David Pointcheval
In Proceeding of SCN ’04 : The Fourth Conference on Security in Communication Networks.
Volume 3352 of Lecture Notes in Computer Science, pp. 33–47, Springer-Verlag, 2004.

[25] **About the Security of Ciphers (Semantic Security and Pseudo-Random Permutations)**
Duong Hieu Phan and David Pointcheval
In Proceeding of SAC ’04 : 11th Annual Workshop on Selected Areas in Cryptography.
Volume 3357 of Lecture Notes in Computer Science, pp. 185–200, Springer-Verlag, 2004.

[26] **Chosen-Ciphertext Security without Redundancy**
Duong Hieu Phan and David Pointcheval
Advances in Cryptology – ASIACRYPT ’03.
Volume 2894 of Lecture Notes in Computer Science, pp. 1–18, Springer-Verlag, 2003.

[27] **A comparison between two methods of security proof**
Duong Hieu Phan and David Pointcheval
In Proceeding of RIVF, pp. 105-110, (2003).

[28] **Some Preliminary Results on the Stableness of Extended F-rule Systems**
Thanh Thuy Nguyen and Duong Hieu Phan and Yamanoi Takahiro
Journal of Advanced Computational Intelligence, Japan, pp. 252–259, Vol.7 No.3, 2003.

4.3 Rapport de recherche

[R1] **Provable Security : Designs and Open Questions**
(rapport rédigé avec les membres du groupe AZTEC, projet ECrypt)
AZTEC Report - European Network of Excellence in Cryptology, July 2005
http://www.ecrypt.eu.org/documents/D.AZTEC.1-1.1.pdf

4.4 Brevets

[B1] **Obtention de valeurs dérivées dépendant d'une valeur maîtresse secrète**
Olivier Billet - Duong Hieu Phan (Demandeur : France Telecom)
Publication: FR2916871 (A1)
Numéro de la demande internationale : PCT/FR2008/050930 du 28.05.2008

[B2] **Système traçable de chiffrement/déchiffrement de données numériques diffusées**
Olivier Billet - Duong Hieu Phan (Demandeur : France Telecom)
Publication: FR2922393 (A1)
Numéro de la demande internationale : PCT/FR2008/051811 du 07.10.2008

4.5 Thèse d'Habilitation à Diriger des Recherches

Titre : Some Advances in Broadcast Encryption and Traitor Tracing
École normale supérieure, novembre 2014

Rapporteurs :

Jean-Sébastien Coron	Professeur à l'University of Luxembourg
Aggelos Kiayias	Associate Professor à l'University of Connecticut, USA
Marc Joye	Chercheur, HdR, Technicolor R&I, USA

Examinateurs :

Michel Abdalla,	Chercheur CNRS, HdR, École normale supérieure
Claude Carlet	Professeur à l'Université Paris 8
Louis Goubin	Professeur à l'Université de Versailles Saint-Quentin-en-Yvelines
David Pointcheval	Directeur de recherche CNRS, École normale supérieure
Jacques Stern	Professeur à l'École normale supérieure

4.6 Thèse de doctorat

Titre : Sécurité et efficacité des schémas cryptographiques
École normale supérieure (avec diplôme de l'École Polytechnique), septembre 2005

Directeur :

David Pointcheval	Directeur de recherche CNRS, École normale supérieure

Président du jury :

Jacques Stern	Professeur à l'École normale supérieure

Rapporteurs :

Antoine Joux	Professeur à l'Université de Versailles St-Quentin en Yvelines
Marc Girault	France Télécom R & D

Examinateurs :

Jacques Patarin	Professeur à l'Université de Versailles St-Quentin en Yvelines
Jean-Marc Steyaert	Professeur à l'École Polytechnique
Guillaume Poupard	Direction Centrale de la Sécurité des Systèmes d'Information
Moti Yung	Professeur à l'Université Columbia, Etats-Unis

5 Encadrement scientifique

5.1 Encadrement de thèse

2009 – 2013 :	Viet-Cuong Trinh, thèse soutenue le 19/12/2013 (co-direction avec Claude Carlet, Professeur à l'Université Paris 8)
2014 – :	Xuan Thanh Do

5.2 Encadrement postdoctoral

2012 – 2013 :	Elizabeth A. Quaglia (co-encadrement avec David Pointcheval)
2011 – 2012 :	Siamak Fayyaz-Shahandashti (co-encadrement avec David Pointcheval)

5.3 Encadrement de Master 2

2012 – 2013 :	Manh-Cuong Ngo, Ecole Polytechnique (co-encadrement avec David Pointcheval)
2011 – 2012 :	Modibo Coulibaly, Université Paris 8 (co-encadrement avec Philippe Guillot)

6 Autres activités

6.1 Comités de programme des conférences internationales

2014	**Asiacrypt 2014** - 20th Annual International Conference on the Theory and Application of Cryptology and Information Security **Africacrypt 2014** - 7th International Conference on Cryptology in Africa
2010	**PKC 2010** - 13th International Conference on Practice and Theory in Public Key Cryptography
2009	**Eurocrypt 2009 -** 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques.
2008	**RIVF 2008** - The 5th IEEE International Conference on Research, Innovation and Vision for the Future
2007	**ProvSec 2007** - International Conference on Provable Security 2007 **WISA** – 7th International Workshop on Information Security Applications
2006	**VietCrypt** – 1st International Conference on Cryptography in Vietnam **InsCrypt 2006** - The 2nd SKLOIS Conference on Information Security and Cryptology
2005	**CISC** – Conference on Information Security and Cryptology 2005

6.2 Responsabilités collectives

General co-Chair (avec Bao Chau Ngo) d'Asiacrypt 2016 à Hanoi, Vietnam
Membre du Steering Committee d'Asiacrypt
Membre du comité consultatif de mathématiques de l'Université Paris 8
Membre du comité d'organisation de la conférence VietCrypt 2006.
Responsable des stages de Master 2 (année 2014-2015)
Responsable des stages de Master 1 (année 2012-2014)
Responsable des travaux d'études de Licence 3 (année 2013-2014)

6.3 Divers

Séminaires invités :	Vietnam Institute for Advanced Study in Mathematics (2014, 2013, 2012) Congrès SMF-VMS de Mathématiques France / Vietnam (2012) Ecole normale supérieure (2012, 2009) Université Paris 13 (2014, 2010), Université Paris 8 (2007, 2014) Université de Caen (2013, 2009, 2007) Université Nationale du Vietnam (2012, 2010) University of Bristol, UK (2006) University College London, UK (2007 et 2006) France Telecom Paris et Caen (2008, 2007) Telecom Paris (2007)
Co-auteurs :	Michel Abdalla (ENS), Olivier Billet (France Telecom), Hervé Chabanne (Sagem), Benoît Chevallier-Mames (Apple), Alexander W. Dent (Royal University, UK), Yvo Desmedt (UCL, UK), Nelly Fazio (IBM, USA), John Malone-Lee (Bristol University, UK), Helger Lipmaa (UCL, UK), San Ling (Nanyang Technological University, Singapore), Gregory Neven (IBM), Antonio Nicolosi (Standford University, USA), Thanh-Thuy Nguyen (Ecole Polytechnique, Vietnam), David Pointcheval (ENS), Nigel Smart (Bristol University, UK), Reihaneh Safavi-Naini (University of Calgary, Canada), Dongvu Tonien (Wollongong University, Australia), Damien Stehlé (ENS Lyon), Ron Steinfeld (Monas University)
Projets	ANR JCJC ROMAnTIC (2012-2016), ANR EnBID (2014-2018) CESAM (Courbes Elliptiques pour la Sécurité des Appareils Mobiles) d'ACI Sécurité Informatique (2003-2006) Provable Security d'ECrypt (European Network of Excellence in Cryptology) (2004-2006) Foresure et Medi@sure, projets de France Telecom R&D (2006-2007)
Responsable de projet	ANR « BEST : Broadcast Encryption for Secure Telecommunication » Projet du période 2010-2014 entre ENS, Thalès, Nagra, CryptoExpert et Université Paris 8 (je suis responsable scientifique pour Paris 8).
Prix/Prime	2009 – PES (Prime d'excellence scientifique) 2000 – 1er prix national d'« Etudiants en recherche scientifique », Vietnam
Concours MdC	2007 – Classé 1er à l'Université de Joseph Fourier (Grenoble), section 27 2007 – Classé 1er à l'Université de Paris 8, section 25 2007 – Classé 1er à l'ENSI Caen, section 26 – 27

Activités de recherches
Sujet : "Protocoles cryptographiques pour la diffusion de données chiffrées"

Mes travaux portent sur un champ de recherche relativement nouveau en cryptographie : la sécurité prouvée. L'objectif principal de ce champ de recherche est d'élaborer des preuves fiables de la sécurité des schémas cryptographiques. La sécurité prouvée comprend deux voies bien distinctes mais très complémentaires qui sont la formalisation des notions de sécurité et la construction des schémas prouvés sûrs.

A la suite d'une thèse de doctorat dont le sujet principal est le chiffrement, je me suis intéressé à la généralisation du chiffrement au cas d'utilisateurs multiples, à savoir la diffusion de données chiffrées. Dans ce modèle, un centre chiffre, puis diffuse les données (chiffrées) à plusieurs destinataires en une seule fois grâce à un canal de diffusion. Du côté des destinataires, chacun dispose d'une clé personnelle (fournie par le centre) qui sert à déchiffrer les données reçues. L'exemple type est la télévision à péage où, en principe, seuls les abonnés disposant d'un décodeur légitime (contenant une clé personnelle) peuvent déchiffrer les données transmises par le centre. Cette généralisation du chiffrement introduit deux nouveaux problèmes au-delà de la confidentialité : comment le centre peut-il identifier les abonnés malhonnêtes (appelés des *traîtres*) qui fabriquent des *décodeurs pirates* (le schéma correspondant est appelé *un schéma de traçage de traîtres*) et comment le centre peut-il révoquer les abonnés malhonnêtes sans avoir besoin de mettre à jour les paramètres du système (le schéma correspondant est appelé *un schéma de révocation*).

Mes recherches abordent à la fois le fondement de la diffusion de données chiffrées et la construction des nouveaux schémas. Elles se concentrent principalement sur les points suivants :

- **Notions de sécurité et modèles d'attaque**: nous avons notamment mis en évidence les relations entre les notions de sécurité face aux différents modèles attaques [10]. Nous avons également proposé un nouveau type d'attaque, appelé Pirates 2.0 [12], et avons montré son impact sur les schémas en pratique (notamment celui utilisé pour les DVD à haute définition)
- **Méthode combinatoire pour la construction de schémas :** nous avons utilisé un certain nombre de types de codes existants pour construire des schémas très efficaces [13, 16, 19] avec une nouvelle fonctionnalité : la traçabilité publique. Nous avons en particulier introduit un nouveau type de code, nommé Trace & Revoke Code [2], qui sert à construire des schémas de traçage de traître et de révocation. Nous avons aussi proposé une nouvelle technique [6] pour rendre les schémas combinatoires plus résistants aux Pirates 2.0.
- **Méthode algébrique fondée sur les couplages sur des courbes elliptiques :** nous avons utilisé les couplages pour construire des schémas efficaces de diffusion de données chiffrées d'une part [5], et introduire une nouvelle catégorie de schémas dont le chiffrement est basé sur l'identité du groupe des destinataires [11, 17] d'autre part. En particulier, notre schéma [3] renforce la sécurité du schéma de Boneh-Gentry-Waters et – en le rendant dynamique – le rend également plus pratique. Ce schéma a notamment été choisi pour être implémenté et testé par Thalès.
- **Méthode algébrique fondée sur les réseaux euclidiens pour la construction de schémas :** Les réseaux euclidiens sont utilisés d'une façon de plus en plus extensive car ils permettent la construction des schémas résistant aux attaques quantiques. Nous avons proposé un schéma de traçage de traîtres [2] dont la sécurité est assurée sous l'hypothèse bien connue de LWE (Learning with errors) et de manière surprenante, notre schéma (multi-destinataire et avec traçabilité) est aussi efficace que le schéma de chiffrement de Regev fondé sur le même problème LWE.

Projet scientifique : Sécurité pour des communications multi-utilisateur

Mon projet scientifique a pour but d'approfondir et d'élargir le sujet de mon HdR au cas plus général de la cryptographie pour des communications multi-utilisateurs. Le choix est motivé par la considération suivante : bien que de nombreux protocoles efficaces existent dans le contexte des communications "one-to-one", dans le cas des communications multi-utilisateurs ("one-to-many", "many-to-many"), la plupart des solutions existant ne sont pas satisfaisantes en pratique.

Ce projet abordera les aspects suivants : formaliser les notions de sécurité requises, construire des schémas efficaces, fournir des preuves de sécurité en réduisant la sécurité des schémas à des hypothèses algorithmiques reconnues difficiles ou à d'éventuelles nouvelles hypothèses algorithmiques et dans ce dernier cas, étudier la difficulté de ces nouvelles hypothèses. Nous nous concentrerons sur le chiffrement mais aussi sur la signature du groupe, le chiffrement fonctionnel, la cryptographie partagée ainsi que les applications qui combinent différentes primitives, notamment le vote électronique. Les principales directions sont :

La sécurité versus l'efficacité : il arrive souvent que l'on doive sacrifier l'efficacité d'un schéma au profit de son niveau de sécurité. Le premier point de ce projet a pour but de rechercher un équilibre entre la sécurité et l'efficacité en fonction des exigences de l'application pratique. Premièrement, nous étudions le compromis (*trade-off*) entre la sécurité et l'efficacité en proposant de nouveaux modèles d'attaque ou de nouvelles notions de sécurité, qui n'atteindraient pas le niveau de sécurité maximal mais qui reflèteraient au mieux les exigences de la pratique. Deuxièmement, nous continuons à améliorer l'efficacité des schémas tout en conservant un niveau de sécurité très élevé, grâce aux techniques récemment développées comme les *non-committing encryption*s et les *lossy trapdoor*. Troisièmement, nous développons un travail en cours pour proposer un schéma de vote électronique qui répondrait mieux aux exigences pratiques en minimisant l'intervention des autorités (via l'introduction d'une nouvelle notion de traçage pour le vote électronique).

Sécurité contre les attaques quantiques : La mise en œuvre éventuelle de machines quantiques rendrait plusieurs schémas cryptographiques vulnérables. Les problèmes algorithmiques demeurant non résolus par les machines quantiques sont à titre d'exemple : le décodage des codes linéaires ; des problèmes sur les réseaux euclidiens, le problème LWE. L'efficacité des schémas qui repose sur ces problèmes est assez limitée. Une direction intéressante, initiée par Lyubashevsky-Peikert-Regev est de considérer le problème LWE dans un anneau d'entiers des extensions cyclytomiques (Ring-LWE). Un de nos objectifs est d'améliorer l'efficacité de notre schéma [1] en nous basant sur Ring-LWE, ce qui est un défi en soi car dans le cas multi-utilisateur, une fois que le pirate obtient une clé, il pourrait générer plusieurs autres clés via les automorphismes d'anneaux. Un autre objectif est de considérer la difficulté du problème LWE dans d'autres extensions algébriques.

La relation entre les primitives : La relation entre les primitives est un axe important qui nous aide à mieux comprendre les difficultés de concevoir ces primitives. Au sein des schémas multi-utilisateurs, il a été démontré que la construction d'un schéma de traçage de traîtres conduit génériquement à la construction d'un schéma de signatures de groupe, et qu'un schéma de traçage de traîtres peut être génériquement construit à partir d'un code résistant aux coalitions et d'un chiffrement symétrique. Les cas inverses ne sont cependant ni infirmés ni confirmés. Il est également intéressant de noter que les relations existent non seulement entre les schémas multi-utilisateurs mais aussi entre un schéma multi-utilisateur et un schéma "one-to-one". Notre objectif est d'étudier plus en détails les relations entre les primitives multi-utilisateurs et les relations entre ces primitives et d'autres primitives plus classiques comme le chiffrement, la signature et l'identification.