

*Il est conseillé de joindre ce document au dossier transmis
aux rapporteurs désignés par le Conseil National des Universités*

DÉCLARATION DE CANDIDATURE À LA QUALIFICATION
AUX FONCTIONS DE PROFESSEUR DES UNIVERSITÉS,
POUR LA SECTION 27-Informatique
(Campagne 2015)
1ère demande

Je soussigné(e) M.

Nom de famille : PHAN

Nom d'usage : PHAN

Prénom : DUONG HIEU

Date et lieu de naissance : 12/06/1978 - HANOI-VIETNAM

Nationalité : Française

Adresse postale et électronique à laquelle seront acheminées toutes les correspondances
9, RUE DE L'ABREUVOIR BAT. 2 / APP. 2063
Code postal : 92400 Ville : COURBEVOIE Pays : FRANCE Téléphone : 0659139197 Télécopie : +33 9 58 44 18 28 Adresse électronique : duong-hieu.phan@ens.fr

Date de création de la candidature

22/09/2014 à 15:09

Date de dernière modification de la candidature

20/10/2014 à 22:10

Titres universitaires français :

Habilitation à diriger des recherches

Diplôme au titre duquel la qualification est demandée : HDR

Titre : Some Advances in Broadcast Encryption and Traitor Tracing

Date de soutenance : 19/11/2014

Lieu de la soutenance : ECOLE NORMALE SUPERIEURE

Mention :

Directeur : DAVID POINTCHEVAL

Composition du jury : MARC JOYE

MICHEL ABDALLA

CLAUDE CARLET

JACQUES STERN

JEAN-SEBASTIEN CORON

AGGELOS KIAYIAS ET LOUIS GOUBIN

Liste des étabs et labos d'exercice :

LAGA, UMR 7539, Université Paris 8, Université Paris 13 (membre permanent)

DI ENS, UMR 8548, Ecole normale supérieure (membre associé)

Activités en matière d'enseignement :

Cours/TD de Master 2: Cryptographie avancée

Cours/TD de Master 1: Théorie de la Complexité

Cours/TD de Licence: Combinatoire, Algèbre linéaire, Analyse

TD: Les bases de la programmation et de l'algorithmique

TD: Programmation en C

Co-direction de thèse de V.C. Trinh (soutenue en 2013)

Co-encadrement post-doctoral de E.A. Quaglia et S. Shahandashti.

Encadrement de stages de M2, M1.

Thème de recherche et mots clés :

Mes travaux portent sur la cryptographie, en particulier la sécurité prouvée. L'objectif principal est d'élaborer des preuves fiables de la sécurité des protocoles cryptographiques. Cela consiste à formaliser les notions de sécurité, à examiner la difficulté des problèmes algorithmiques et à construire des protocoles munis de preuves de sécurité.

Mots clés: cryptographie, algorithmique, protocol

Activités en matière d'administration et autres responsabilités collectives :

Responsable des stages de Master 2 (2014 - 2015)

Responsable des travaux d'études de Licence 3 (2013 - 2014) et Master 1 (2012 - 2014)

Membre du Jury de Master

Membre suppléant du comité consultatif

Membre du "Steering Committee" d'Asiacrypt

Membres de plusieurs comités de programme des conférences internationales (Eurocrypt, Asiacrypt, PKC,...)

déclare faire acte de candidature à la qualification.

Fait à Paris le 22/09/2014

Signature

