UNIVERSITÉ DE LYON

ENS DE LYON

Rapport de soutenance d'une thèse de doctorat de l'Université de Lyon opérée par l'Ecole Normale Supérieure de Lyon

Présentée par Mme Ida TUCKER, le 19/10/2020

Sur le sujet de thèse : Chiffrement fonctionnel et signatures distribuées fondés sur des fonctions de hachage à projection, apport des groupes de classe.

Nom	Signature
M. Michel ABDALLA	
M. Ivan DAMGARD	
M. Fabien LAGUILLAUMIE	
Mme Shweta AGRAWAL	
Mme Carla RAFOLS SALVADOR	
M. Guilhem CASTAGNOS	
M. Pierre-Alain FOUQUE	

During her PhD thesis defense, Ida Tucker presented her work in the area of functional encryption and distributed signatures and the benefit of class groups. The presentation was excellent and pedagogical and highlighted the breath and depth of her results.

During her defense, Ida focused on her main results regarding the new and very interesting class group assumptions, which have nice and innovative applications in cryptography and their usage in security proofs to build advanced secure cryptosystems. Her results are expected to have great impact because the generic framework she designed can also be instantiated with other more classical cryptographic assumptions such as Discrete Logarithm or Factorization.

After the presentation, Ida Tucker convincingly answered all the questions asked by the committee about both specific technical points and general aspects of the topic. She showed that she masters her research subject and she has interesting directions for her future works.

For all these reasons, the committee is convinced that Ida Tucker has all the qualities to become an outstanding researcher or professor and decides to confer upon her the PhD degree in Computer Science of Université de Lyon operated by the École Normale Supérieure de Lyon.

Le président signe le rapport de soutenance, qui est contresigné par l'ensemble des membres du jury présents
Si un membre est présent en visioconférence, l'indiquer à la place de la signature.

L'original signé de ce document doit être transmis **au Bureau du 3ème cycle de l'ENS de Lyon - Bureau D2.**
Descartes - BP 7000 - 69342 Lyon cedex 07.

ECOLE NORMALE SUPERIEURE DE LYON