Service des admissions et des études
Pôle des études
Bureau des doctorants & hdr
sae@ens.fr

DEFENCE REPORT AT REQUEST OF AN AUTHORIZATION TO HABILITATION (Hdr)

The file of: Duong Hieu Phan
Speciality:

Name of referees: Aggelos Kiayias
Title-quality:
Place of work:

The Defence report (between 1 and 2 pages) established by the referees have to highlight the quality and the originality of the works of the candidate and end in his capacity to lead researches, to supervise PhD students, to manage a research team.

The Defence report can be drafted on separate sheet of paper if all the wanted information above appears in header. The Defence report with the original signature of the reporter has to be send directly, under confidential fold, for the attention of : **Commission HDR- Bureau des doctorants & hdr – 45, rue d'Ulm 75230 PARIS CEDEX 05 – sae@ens.fr**

Reminder: the return of the Defence reports is asked in 4 weeks for Hdr Sciences and in 6 weeks for Hdr Letters after the sending of the file by the candidate.

Dr. Phan's research focus is in cryptographic aspects of digital content distribution. Over the years he has produced a steady flow of excellent work in the area with both novel constructions of encryption schemes with specialized properties that are significant for digital content as well as in the security analysis of such schemes that has taken the form of novel attack concepts. His work has appeared in the top venues of the area such as CRYPTO, Eurocrypt, Asiacrypt and ICALP as well as in widely recognized journals including the IEEE-TIFS and Algorithmica.

Of particular note is the notion of publicly traceable traitor tracing that was introduced by Dr. Phan in a Eurocrypt 2005 article. In this work, the authors introduce a novel type of traceability. Traditionally tracing was considered to be a private state algorithm that is ran by a central authority which is responsible for digital content distribution towards a set of subscribers. Instead, in the public traceability model, it is allowed that tracing is executed by any interested party given the public parameters of the system without jeopardizing overall security. Designing publicly traceable schemes is more difficult than regular systems and Dr. Phan's work paved the way for a number of constructions that followed this path.

(continued on next page)

Signature :

Dr. Phan has also introduced novel attack concepts that have important implicatiosn in the deployment of digital content distribution systems. Specifically, the concept of « Pirates 2.0 » that was introduced in a Eurocrypt 2009 article shows how traitors can collaborate in public without necessarily having a private coordination endpoint. This has some wide implications since it is much more simple to generate large coalitions. Previously large coalitions were considered to be unlikely given that a private coordination endpoint was thought to be necessary for the generation of a pirate decoder.

More recently, Dr. Phan and colleagues intoduced a new traitor tracing scheme that is based on lattices and specifically the k-LWE problem. This new construction enjoys public traceability and is the first construction that non-trivially utilizes advances in lattice based cryptography towards the construction of traitor tracing schemes.

Overall, the work of Dr. Phan is of very high impact in the area of digital content distribution. Moreover, he has shown the capability of collaborating at a national and international level. More recently he has also co-advised the ph.d. thesis of Viet-Cuong Trinh who published a number of papers including one in Asiaccs which is a very good conference in computer security. This demonstrates that Dr. Phan has gained the experience of doctoral supervision as a co-advisor and based on his record I would expect that he will successfully continue to supervise ph.d. students and managing researchers in general.

Signature :