

**COMPLIANCE WITH THE DATA PROTECTION ACT 1998**

In accordance with the Data Protection Act 1998, the personal data provided on this form will be processed by EPSRC, and may be held on computerised database and/or manual files. Further details may be found in the **guidance notes**

# PostDoctoral Research Fellowship Peer Review

EPSRC Reference: EP/H026886/1

Document Status: With Council

## Postdoctoral Fellowships 2010

**Applicant Details**

Applicant	Mr long hoang nguyen	Organisation	University of Oxford
-----------	----------------------	--------------	----------------------

**Title of Research Project**

NOVEL AUTHENTICATION FOR COMPUTER SECURITY

**Review Information**

Response Due Date	05/10/2009	Reviewer Reference:	YG4BFY
-------------------	------------	---------------------	--------

**Research Council Contact Details**

EPSRC Administration Contact: Miss Teresa Andow	Email: <a href="mailto:teresa.andow@epsrc.ac.uk">teresa.andow@epsrc.ac.uk</a>	Telephone: 01793 444584
---	---	-------------------------

**Quality**

Please comment on the degree of excellence of the proposal, making reference to:

- (1) The novelty, relationship to the context, and timeliness;
- (2) The ambition, adventure, and transformative aspects identified;
- (3) The appropriateness of the proposed methodology.

(For multi-disciplinary proposals please state which aspects of the proposal you feel qualified to assess)

Long Nguyen is proposing to work on novel security protocols that use a lightweight notion of hashing - i.e. digests. These are more akin to pin numbers in that they are short. Because of their brevity, these functions lack some of the properties that are so beloved of cryptographers - they are not collision resistant. They are not non-invertible. But we do have ambiguity - many messages will hash to the same value. In their favour they are short (4 - 5 digits long) and hence can be entered by a user - or verified by the user. This does seem to be a useful contribution to user-centric cryptography.

There is an interesting mix of security proofs and user interaction which I have not seen elsewhere.

There is currently considerable debate amongst the crypto community on the subject of hashing. Consequently this work is timely.

I am not sure that the work is particularly risky - a lot seems to be implementational in nature. Indeed the ideas seem to build upon ideas in Long NGuyen's D.Phil thesis - so I suspect a long of the ideas "simply" need fleshing out.

*The excellence of this proposal has been demonstrated*

<input type="checkbox"/> Not at all	<input checked="" type="checkbox"/> Adequately	<input type="checkbox"/> Fully
-------------------------------------	--	--------------------------------

**Impact**

Please comment on the extent to which the proposal shows the potential impact of the project, making reference to:  
 (1) The relevance and appropriateness of any beneficiaries or collaborators;  
 (2) Whether appropriate routes and resources have been identified for dissemination and knowledge exchange.

The (external) collaborators seem eminently suitable. I had a concern that there would be insufficient support within the group however a lot of the prior work was performed in cooperation with Professor Bill Roscoe - who, hopefully, will be available to support this activity.

No major concerns about knowledge exchange. A minor concern - there does seem to be a desire to patent aggressively. This can have the effect of killing off interest in a new cryptographic technique. i.e. be an obstacle to adoption.

*Potential impact has been demonstrated*

<input type="checkbox"/> Not at all	<input type="checkbox"/> Adequately	<input checked="" type="checkbox"/> Fully
-------------------------------------	-------------------------------------	---

**Applicant**

Please comment on the applicant's ability to deliver the proposed project, making reference to:  
 (1) Appropriateness of the track record of the applicant(s);  
 (2) Balance of skills of the project team, including academic collaborators

Mr Long Nguyen seems to have a good academic track record. His DPhil research was in the same area, so there is no reason to believe he will not produce good quality results.

The research will also be performed within the same group he was in whilst working towards his DPhil - so he should enjoy the same level of support.

*The applicant's track record and ability to deliver this project is*

<input type="checkbox"/> Not appropriate	<input type="checkbox"/> Adequate	<input checked="" type="checkbox"/> Appropriate
--	-----------------------------------	---

**Resources and Management**

Please comment on the effectiveness of the proposed planning and management and on whether the requested resources are appropriate and have been fully justified.

The planning seems adequate. The work has been broken into 7 milestones. It was not clear how these milestones would be marked (formal meeting with persons unknown? publication of results? ...)

The resources seem adequate to the task.

One small question ... I was a little surprised to see a line item for work permit/visa costs. I presume that is the normal procedure.

*The level of planning and justification of resources is*

<input type="checkbox"/> Unacceptable	<input checked="" type="checkbox"/> Adequate	<input type="checkbox"/> Good
---------------------------------------	--	-------------------------------

**Proposal Assessment**

Please comment on the extent to which this proposal meets each of the criteria laid out in the call document not already covered by your previous answers

No problems here.

*This proposal meets the call criteria*

<input type="checkbox"/> Partially	<input type="checkbox"/> Broadly	<input checked="" type="checkbox"/> Strongly
------------------------------------	----------------------------------	--

**Overall Assessment**

Please summarise your view of this proposal

This work seems to be an extension of the candidates D.Phil thesis. He will be continuing to work within the same group - and so should receive the same level of support as before.

Since the finding of collisions in MD5, ... there has been a lot of interest (academic and industrial) in the design of hash functions with provable properties. This work should add to that debate.

The area of research is of interest to both industry and academia. I welcome the intention to consider the user as an active agent within this research - too often the goal is for security perfection whatever the discomfort level of the user. Realising the user is apt to make typing mistakes ... is an interesting usability twist. I also like the idea that we are being adult about the notion of "good enough". for example, protocols where the user/attacker is only going to get one chance to get a value right.

The security "theorists" will welcome more cryptographic primitives with proven properties. The security "engineers" will welcome them if they are efficient, flexible and user-friendly.

I am not so convinced about the means of dissemination. It seems a little too introverted. ("...exchange ideas with many other researchers...")

*My judgement is that:*

- 1) *This proposal is scientifically or technically flawed*
- 2) *This proposal does not meet one or more of the assessment criteria*
- 3) *This proposal meets all assessment criteria but with clear weaknesses*
- 4) *This is a good proposal that meets all assessment criteria but with minor weaknesses*
- 5) *This is a strong proposal that broadly meets all assessment criteria*
- 6) *This is a very strong proposal that fully meets all assessment criteria*

*My confidence level in assessing this is:*

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	2	3	4	5	6

<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Low	Medium	High

### **Reviewer Expertise**

*Please indicate your areas of expertise that are relevant to your assessment. Take care not to reveal your identity to the applicant.*

I am a senior researcher in an industrial research laboratory. I have worked in the area of cryptography since 2001. My areas of interest include hash based cryptography, elliptic curve cryptography and quantum cryptography.