

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:	U178P3
-------------------	------------	---------------------	--------

Research Council Contact Details

EPSRC Administration Contact: Miss Teresa Andow	Email: teresa.andow@epsrc.ac.uk	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)

The research proposal is in the general area of cryptography, which is an important and fast-moving interdisciplinary research area. Nguyen, in his thesis, has identified a new cryptographic building block (namely, a "digest") which is an alternative to a hash function in cryptographic protocols which include some human involvement (i.e., are not entirely performed by computers). Exploiting the human involvement is an important concept which could become commonplace in real-world security applications (we already see this with CAPTCHAs). Nguyen seems to have identified an important set of ideas and is well placed to investigate them further. Hence the novelty, ambition and potential reward are high.

The obvious way to design a digest is to apply a cryptographic hash function and truncate the output. This is what other authors do. It is natural to study whether more efficient solutions exist and it should be relatively straightforward to apply the existing literature on hash functions (which is large) to this problem. Hence this part of the proposal is rather incremental. The proposal is stronger in the less theoretical topics, such as "new authentication".

Nguyen is ideally suited to study these ideas further, and has identified appropriate collaborators to help him develop this subject. The research proposal is detailed and contains a number of specific goals. Most of these continue work already done by him so there is a good chance that these goals can be achieved. The proposal states that he will take month-long visits to Leuven (Belgium), EPFL (Switzerland) and Xerox PARC (USA). It will be extremely beneficial to the applicant to visit these groups. The experts there will be able to assist the resolution of the goals of the proposal. I did not see any letters of support from these institutions, which is a pity, but I know these groups and am confident that visits to these institutions will be worthwhile.

The excellence of this proposal has been demonstrated

<input type="checkbox"/> Not at all	<input type="checkbox"/> Adequately	<input checked="" 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 proposal clearly emphasises that the work, although theoretical, has many potential applications. The applicant is doing all the right things to ensure that these ideas are adopted by industry. In particular, he has become involved in international standardisation and is in discussion with representatives of industry. In general, the proposal is very strong in this area.

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*

Nguyen has performed excellent research in his PhD. He has ambition to work on important topics in research and is clearly independent and well motivated. His number of publications is above average for a good student at his level in theoretical cryptography.

The proposal lists some excellent collaborators, who are appropriate for this project: Leuven, EPFL and Xerox are centers of excellence and visits to these institutions will have a positive influence on the success of the research.

In all, the applicant is well-qualified to perform the research.

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 fine. The resources are appropriate, though I am surprised that people still ask for both a laptop and desktop these days.

The level of planning and justification of resources is

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

Generally I think the proposal matches the call. One issue is of course that the applicant is staying in the institution of his PhD. This is obviously a concern, when it might have been more appropriate to move to Royal Holloway or Bristol. However, as I have mentioned, the proposal includes three visits of one month duration each to leading international groups and this will be very beneficial. Also, the applicant is clearly working hard to increase his network of collaborators and to learn from other groups, so I am satisfied that the fellowship is still worth funding.

The fellowship will certainly assist Nguyen in establishing an independent research career, and I have little doubt that he will be successful in this.

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 is a strong proposal. Novel ideas of potentially major impact (both theoretical and in the real world) are to be studied. The research is timely and the applicant is ideally suited to perform this work.

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

<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" 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 work in public key cryptography and related mathematics. I am not an expert in real-world applications and so my opinions on this part of the proposal are less insightful.