

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	09/10/2009	Reviewer Reference:	2XET82
-------------------	------------	---------------------	--------

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 programme described in the proposal is interesting and extends work that the applicant has been conducting over the last few years.

The subject matter is of some independent interest, although possibly most interesting because of its potential applications.

The proposal is timely - this is definitely the right time to conduct this work.

This proposal is ambitious in parts. Indeed it would appear to take the applicant into areas where he has not yet demonstrated full capability (the design of cryptographic primitives). On the other hand it is also slightly unambitious in that it is largely based on "keeping on going" from his thesis work. I think this balance is reasonable.

The methodology is largely fair, although there are some claimed outcomes whose methodology is not particularly well-explained in the proposal, making this hard to judge in places. However in research of this type it is reasonable to leave some "leaps of faith" since if the full methodology was already known then much of the work would already have been done.

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.

There is no doubt that the applicant is well-versed in dissemination processes and has very good ideas for continuing to do this. There is a healthy travel and collaboration budget. The involvement in the international standards process provides an ideal dissemination tool for relevant results, although it does also provide a potential "conflict of interest" since the candidate will clearly be keen to include his own research.

I felt that some of the publication outlets such as "Crypto" and "Asiacrypt" were rather ambitious, since the candidate has yet to demonstrate capability in the type of research required to be accepted at these highly competitive venues.

The proposal identified many potential beneficiaries. These are all possible, but I felt that the proposal tried rather "too hard" in this respect to convince us that the results of this research will be "ground breaking". I agree that there is potential, but I am not as convinced as the applicant of the significance of this impact.

Potential impact has been demonstrated

Not at all

Adequately

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

The candidate is very capable, of that there is no doubt. His current publication record is very good, although not outstanding. I note however that there are several works in progress, so it is probably too early in his research career to make general judgements. He has good potential.

The academic environment in Oxford is suitable for parts of this research. The candidate has identified areas where he needs to seek expertise elsewhere, such as cryptographic design and security proof modelling. The collaborators he has named are excellent and will be of great value to him. It was not fully clear to me whether the high expectations of the short visits to these partners are realistic, but I am convinced that they are appropriate partners.

I remain slightly concerned about whether the applicant has the cryptographic pedigree to deliver on the claimed research outcomes concerning design of primitives. However funding this project may well provide the environment in which he can grow and achieve these.

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

Not appropriate

Adequate

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 management plan seemed reasonable and the travel budget extremely healthy.

The one query I have on this aspect of the proposal is the inclusion of funds to engage in the standardisation meetings. While this activity is commended and is related to the project, it is not strictly research. It was also unclear what time component the applicant plans to spend on editing the relevant standard (this can be a very time consuming task). I am supportive of this work, but I would have liked to see some reference to the co-ordination of this work within the project plan.

The level of planning and justification of resources is

Unacceptable

Adequate

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

The applicant has incorporated a suitable time period spent in quality overseas institutions, as required under the call.

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

I think this is a strong proposal from a good candidate.

The good points are the potential of the candidate, the breadth of the research, the strong collaborators and the potential impact of the research.

The weak points are the lack of cryptographic experience and the lack of clarity on the real impact of the research (much is claimed).

The proposal document is very confidently written, perhaps slightly over-confidently. Confidence is often a good quality in a researcher, but there is a slight danger that this research plan is rather "self-centred" and "over-hyped".

I am broadly supportive of this proposal and think the results could be very interesting. I would have made the case slightly more carefully if I had written it myself. In particular I don't think the proposal ever makes an attempt to explain the application (the letter of support provides a bit more detail!) I'd say there is a 70% chance that this research described will have a broad impact, 30% chance that digest functions don't turn out to be very significant, but that is a just my own "hunch". So why not spend a few years finding out?

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

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

Cryptography, information security
