### UCL STUDENT AND REGISTRY SERVICES

Research Degrees

Student Records

## Examiners’ Joint Report for a PhD Candidate

**Candidate: Jonathan Bootle**

*(Please enter full name and title)*

**Student Number: 14091295**

*(Please enter student number if known)*

**Examination:** PhD

**Thesis Title: Designing efficient zero-knowledge proofs in the ideal linear model**

*(Please enter complete thesis title)*

**Date of Oral Examination:**  Wed 6 Feb 2019

**Supervisor present? Yes**  **/ No**

*(If yes, please enter the supervisor’s name here)*: Prof. Jens Groth

**Please Note:** Section B should be completed, giving the grounds on which the joint decision is based. This report should be submitted together with the preliminary reports to Research Degrees, Assessment and Student Records within two weeks of the oral examination. Signed and dated original reports should be sent by post to:

Research Degrees

Student Records

Student and Registry Services

UCL

Gower Street

London, WC1E 6BT

|  |  |
| --- | --- |
| **Section A: Summary of Examination Result** |  |
| **The examiners confirm** that they have examined the thesis submitted by the candidate and have also examined the candidate orally on the subject of the thesis and on subjects relevant to the thesis.    **The examiners confirm** that they have satisfied themselves that the candidate, as evidenced by the thesis and the Viva, can communicate with the scholarly community about their areas of expertise. | |
| **The examiners report that they have satisfied themselves that the thesis:**   |  |  | | --- | --- | | ***Please check the box against the relevant items***   1. is genuinely the work of the candidate 2. forms a distinct and significant contribution to knowledge of the subject   iii) affords evidence of originality: a) by the discovery of new facts and/or b) by the exercise of  independent critical power   1. is an integrated whole and presents a coherent argument 2. gives a critical assessment of the relevant literature 3. gives the method of research and its findings 4. gives discussion of those findings and how they advance the study of the subject 5. demonstrates deep and synoptic understanding of the field of study, including objectivity, autonomy and the capacity for judgement in a complex situation 6. is satisfactory as regards literary presentation 7. includes a satisfactory bibliography and references 8. demonstrates research skills relevant to the thesis 9. is of a standard to merit publication in whole, in part or in revised form |  |   Please comment in Section B below and provide feedback if you are not satisfied in any of the above.  **Please continue overleaf….** | |

|  |
| --- |
| **The examiners report that they have determined ONE of the following:** |
| **1.** The candidate has met the criteria for a **PhD** without the need for corrections and **can be awarded the PhD** |
| **2.** The candidate **is required** to make **specified amendments** to the examiners’ satisfaction **within three months.**  **(If ticked please complete section C)**    Name of person nominated to check the minor corrections: **­­­­­** Prof G Danezis  Address: University College London (g.danezis@ucl.ac.uk)  Post Code: -  ***\* The person* *nominated to check the amendments can either confirm the required amendments have been made satisfactorily by email (***[***researchdegrees@ucl.ac.uk***](mailto:researchdegrees@ucl.ac.uk)***) or by using the Certification of Minor Amendments form available from:*** [***www.ucl.ac.uk/srs/academic-manual/research-degrees/documents/minor\_amendments.doc***](http://www.ucl.ac.uk/srs/academic-manual/research-degrees/documents/minor_amendments.doc) |
| **3.** The candidate is permitted to **re-enter** for the above degree and **to resubmit the thesis** **in a revised form** **within a period not exceeding eighteen months.** (A further oral examination is at the discretion of the examiners)  **NB: This result is not applicable for a resubmitted thesis.**  **Oral Examination? Yes**  **No**  **To Be Confirmed** |
| **4.** Thecandidate has met the criteria as outlined in the regulations and guidelines for examiners and be **awarded the degree of M.Phil.** |
| **5.** The candidate is required to make **specified minor amendments** to the examiners’ satisfaction **within three months** for the award of the degree of **M.Phil.**  **(If ticked please complete section C)**  Name of person nominated to check the minor corrections:  Address:  Post Code:  ***\* The person nominated to check the amendments can either confirm the required amendments have been made satisfactorily by email (***[***researchdegrees@ucl.ac.uk***](mailto:researchdegrees@ucl.ac.uk) ***) or by using the Certification of Minor Amendments form available from:*** [***www.ucl.ac.uk/srs/academic-manual/research-degrees/documents/minor\_amendments.doc***](http://www.ucl.ac.uk/srs/academic-manual/research-degrees/documents/minor_amendments.doc) |
| **6.** Thecandidate is permitted to **enter** **for the degree of M.Phil and** **to re-present the thesis** in a revised form **within twelve months.** (A further oral examination is at the discretion of the examiners)  **Oral Examination? Yes  No  To Be Confirmed** |
| **7.** Thecandidate has **not fulfilled the requirements for a PhD or M.Phil** (Such a candidate will not be permitted to re-enter this thesis for examination). |
| **Section B: Examiners’ Joint Report of the Viva**  This section of the report should be completed by the examiners and should give the grounds on which the joint decision is based, including feedback on any of the criteria for the degree which have not been satisfied. |
| The examination started with Jonathan giving a short presentation about the work in the thesis. First he presented a motivation and properties of zero-knowledge, and also a genealogy of zero knowledge models. There was a question about abstracting other types of proofs, such as on lattices, and we had a conversation about how the model could be extended to those constructions.  We then continued discussing how the thesis represents a mix between designing protocols in the model, extending the model, and designing protocols outside the ILC model. He then presented 2/3 concrete examples, namely Schnoor / bit commitment, and how they map to the general ILC model. He then described how the IMC model is implemented using codes. We discussed whether there is something special about what hash is used. He also explained why the use of codes, rather than DL, is cool and has impact – in that zkp do not require public key related assumptions.  He also discussed how to prove the security of the protocols, and how the compilation step, allows for nearly straight-line extraction to prove soundness. We also had a discussion on why straight line extraction gives better concrete security bounds as compared to rewinding. This also has an impact on implementing protocols against quantum capable adversaries.  He also presented DL compilation, and also the logN argument construction that falls outside the ILC model. We also discussed how that compression technique can be used in other settings. We also discussed the Bullet proof constructions, and the relative intellectual contribution of this and earlier work. The final contribution presented is about boosting the soundness of protocols in small fields. And had a Q&A about the meaning of this extension and its applications.  We then opened the discussion for questions from the examiners.  First we discussed the relation of the material in the thesis, with the fully dynamic group signature schemes. The attack in the paper discussed was about a participant joining then leaving the group, and as a result some of the key material would leak. The attacked showed that the model had weaknesses. Even though this was a contrived attacks, this highlighted the weakness of the foundations of the model.  We then asked why chose the contribution around the ILC model as an axis to present his contribution, rather than another axis based on his research. We also expanded on whether that now he has designed a number of protocols, he has insights about automatically generate proofs. We had a discussion about the costs and the future potential of this approach. We also discussed about machine checking. Finally we discussed bounds on the potential efficiency benefits, which are limited since the hand crafted protocols are close to the theoretical limit.  On chapter 3 we discussed the difficulty of understanding the ILC model. And whether there is a way of specifying the model in a more formal / programmatic way. This would also support better the chapter on compilation.  **(1) ASK: We asked the candidate to include the example of using the ILC model for either a simple Schnor proof, or a bit commitment proof. Either could be used to highlight why ILC is a natural formalization. And also highlight ILC is your core contribution, and highlight it as a chapter.**  **(2) ASK: Provide a more formal definition of the ILC model in code / pseudo code, following or in contrast with previous works. Possibly separate ILC into separate chapter to highlight it as key contribution.**  Mention potential limitations against expected poly time adversaries, following the conversation in the viva and ways to refine them (use the Markov inequality, etc.).  We also had a discussion (page 74) on the definition of a “non-uniform” adversary. In this case it probably needs to be ppt rather than non-uniform. We also discussed definition 3 (page 56) and definition 57. Re-order potentially 3.3.1 and 3.3.2. Parameters “n” and “s”. Also look at references to figures (missing), and clarify that the lemmas are yours and what their role will be.  The definition for polynomial commitment seems to be generic in any polynomial is a bit strange, and it is worth noting this in terms of the formalization of security there, and in relation to earlier definitions. In particular you can relate the material here with oblivious polynomial evaluation. Also clarify what the “first oracle execution” is defined. (Page 83).  **(3) ASK: Clean up the section on polynomial evaluation; and explain that it may not fit into the previous definitions. Link it instead in previous literature on polynomial evaluation.**  What is the important of having full-rank and matrices of fewer rows than columns? (Maybe specify). In the argument 6.3 clarify what are P and Q, and illustrate with simple initial example.  We had a discussion about the general difficulty of following proofs in cryptography. Jonathan shared reflections on proving concrete protocols, but there might be opportunities also for parameterized proofs over all polynomials. Potentially one could prove some properties about the compilation, and then separate proofs for specific protocols.  What is the relevance of the 3-move vs 5-move protocols if the protocols will end up being non-interactive? In practice the 5-move protocol might be more practical, in the non-interactive setting. However, it led to corner cases about the model, and therefore is important to present. Maybe concrete parameters could be better, or quantum resistant protocols could be better in fewer rounds.  What are the practicalities of turning non-interactive, protocols from code based compilation. This is apparently OK since the space of the choice of commitments is very large. The security parameters are also practical.  What is the relation between the opening of commitments and known results that show that opening some commitments may leak information about others. How comes this is not a problem in these proofs.  What protocols have you implemented? The low-depth circuit proofs have been prototyped. Lugero and Bullet proofs are deployed. Toy implementations were done in Python.  ---  **Discussion between examiners:** Overall the examiners are satisfied with the work, and suggest minor corrections (option 2), specifically on the 3 items highlighted in bold in the text above. |
| **Section C**: **Examiners’ Request for Minor Amendments**: The following section **should** be completed where the examiners have determined that minor amendments are required. Examiners should select **one** of the following: |
| **i)** The examiners confirm that the candidate has been provided with **a list of minor** amendments **or an annotated thesis** either immediately after the oral or within two weeks of the oral examination and has been asked to **send the amended thesis for confirmation to the person nominated to check the corrections:**  **\***  **ii)** The candidate has **already** made the minor amendments required to the satisfaction of **designated checker**: |
| **Section D: Examiners’ Signature Confirming Result of the Examination**  **Declaration:** We confirm this is the joint examiners’ report for the above name candidate. |
| Signed: Date:  (Please print name)  Signed: Date:  (Please print name)  Signed: \* Date:  (Please print name)  If electronic signatures are to be used, these must be the image of a hand written signature. We cannot accept a typed name in place of a signature.  ***( \* Only for use in the exceptional cases when UCL has approved the appointment of a third examiner)*** |