AUSTRALIAN RESEARCH COUNCIL
Discovery Early Career Researcher Award
Application for Funding Commencing in 2022

DE

Project ID: DE220100595

First Investigator: Dr Thomas Haines

Admin Org: The Australian National University

Total number of sheets contained in this Application: 41

Information on this form and its attachments is collected in order to make recommendations to the Minister on the allocation of financial assistance under the Australian Research Council Act 2001 and for post award reporting. The information collected may be passed to third parties, including being sent to overseas parties for assessment purposes. It may also be passed to any other Australian Government Department or Agency where required, and noting information contained in this application can be disclosed without consent where authorised or required by law.

Part A - Administrative Summary (DE220100595)

A1. Application Title

(Provide a short title. (Up to 75 characters, approximately 10 words))

Efficient privacy-preserving proofs for secure e-government and e-voting

A2. Person Participant Summary

(Add the DECRA candidate participating in this application.)

Number	Name	Participant Type	Current Organisation(s)
1	Dr Thomas Haines	Discovery Early Career Researcher Award	Norwegian University of Science and Technology

A3. Organisation Participant Summary

(Add the Administering Organisation participating in this application. Refer to the Instructions to Applicants for further information.)

Number	Name	Participant Type
1	The Australian National University	Administering Organisation

A4. Application Summary

(Provide an Application Summary (a paragraph of text which is used by the Minister to consider the application), focusing on the aims, significance, expected outcomes and benefits of this project. Write the Application Summary simply, clearly and in plain English. If the application is successful, the Application Summary will be used to give the general community an understanding of the research. Avoid the use of acronyms, quotation marks and upper case characters. Refer to the Instructions to Applicants for further information. (Up to 750 characters, approximately 100 words))

Electronic systems are becoming increasingly widespread and crucial to social and economic wellbeing. This project aims to ensure that e-government, e-health, e-commerce and e-voting are secure and trustworthy by inventing new ways to verify these systems without infringing privacy. This project expects to use innovative techniques from cryptography to support development of trustworthy systems. Expected outcomes of this project include better support for organisations to build trustworthy systems that will maximise benefit to Australian business and society. This should provide significant commercial, reputational, and societal benefits by avoiding disruptions to the organisations and their clients if and when they are attacked.

A5. List the objectives of the proposed project

(List each objective separately by clicking 'Add answer' to add the next objective. This information will be used for future reporting purposes if this application is funded, including reporting on these objectives in the final report. Objectives are pre-populated into the final report template. (Up to 500 characters, approximately 70 words per objective))

Objective

To assess the applicability of existing cryptographic techniques to provide security in Australian e-government, e-health, e-commerce and e-voting without damaging privacy.

Objective

To optimise the use of the cryptographic techniques to provide trustworthiness and robustness without impacting privacy when deployed.

Objective

To develop the ability to prove the implementations of these techniques to be secure.

Part B - Classifications and Other Statistical Information (DE220100595)

B1. Does this application fall within one of the Science and Research Priorities?

Yes

Science and Research Priority	Practical Research Challenge
Cybersecurity	Secure, trustworthy and fault-tolerant technologies for software applications, mobile services, cloud computing and critical infrastructure.
Cybersecurity	New technologies and approaches to support the nation's cybersecurity: discovery and understanding of vulnerabilities, threats and their impacts, enabling improved risk-based decision making, resilience and effective responses to cyber intrusions and attacks.

B2. Field of Research (FoR)

(Select up to three classification codes that relate to the DECRA candidate's application. Note that the percentages must total 100.)

Code	Percentage
080303 - Computer System Security	60
080203 - Computational Logic and Formal Languages	30
080402 - Data Encryption	10

B3. Socio-Economic Objective (SEO-08)

(Select up to three classification codes that relate to the application. Note that the percentages must total 100.)

Code	Percentage
970108 - Expanding Knowledge in the Information and Computing Sciences	60
890201 - Application Software Packages (excl. Computer Games)	30
940202 - Electoral Systems	10

B4. Interdisciplinary Research

(This is a 'Yes' or 'No' question. If you select 'Yes' two additional questions will be enabled:
1. Specify the ways in which the research is interdisciplinary by selecting one or more of the options below.
2. Indicate the nature of the interdisciplinary research involved. (Up to 375 characters, approximately 50 words))

Does this application involve interdisciplinary research?

Yes

Specify the ways in which the research is interdisciplinary by selecting one or more of the options below.

Methodology
Design

Indicate the nature of the interdisciplinary research involved. (Up to 375 characters, approximately 50 words)

This project will require interdisciplinary research utilising expertise in different areas such as formal methods and cryptography.

B5. Does the proposed research involve international collaboration?

(This is a 'Yes' or 'No' question. If you select 'Yes' two additional questions will be enabled:
1. Specify the nature of the proposed international collaboration by selecting one or more of the options below.
2. Specify the countries which are involved in the international collaboration.)

Yes

B6. What is the nature of the proposed international collaboration activities?

(Select all options from the drop down list which apply to this application by clicking on the 'Add' button each time an option is selected.)

Correspondence: eg email; telephone; or video-conference
Face to face meetings
Attendance at and/or hosting of workshop or conference
Travel to international collaborator: short-term (less than 4 weeks)

B7. If the proposed research involves international collaboration, please specify the country/ies involved.

(Commence typing in the search box and select from the drop-down list the name of the country/ies of collaborators who will be involved in the proposed project. Note that Australia is not to be listed and is not available to be selected from the drop-down list.)

Germany
United States of America
Norway
Belgium
Luxembourg

B8. How many PhD, Masters and Honours that will be filled as a result of this project?

(For reporting purposes, the ARC is capturing the number of Research Students that would be involved if the application is funded. Enter the number of all student places (full-time equivalent - FTE) that will be filled as a result of this project, not just those requested in the budget for funding in the application form.)
Number of Research Student Places (FTE) - PhD

3

Number of Research Student Places (FTE) - Masters

0

Number of Research Student Places (FTE) - Honours

2

Part C - Project Eligibility (DE220100595)

C1. Medical Research

(This is a 'Yes' or 'No' question. Does this application contain content which requires a statement to demonstrate that it complies with the eligible research requirements set out in the ARC Medical Research Policy located on the ARC website?)

No

C2. Medical Research Statement

(Justify why this application complies with the eligible research requirements set out in the ARC Medical Research Policy located on the ARC website. Eligibility will be based solely on the information contained in this application. This is the only chance to provide justification, the ARC will not seek further clarification. (Up to 750 characters, approximately 100 words))

C3. Current Funding

(Does this application request funding for similar or linked research activities, infrastructure or a project previously funded, or currently being funded, with Australian Government funding (from ARC or elsewhere)? This is a 'Yes' or 'No' question. If 'Yes', provide the Project ID(s) and briefly explain how funding this project would not duplicate Australian Government funding or overlap with existing projects.)

No

If yes, provide the Funded Project ID(s)

Briefly explain how funding this project would not duplicate Australian Government funding or overlap with existing projects. (Up to 2000 characters, approximately 285 words)

C4. Other Application(s) for funding

(Are you applying for funding from the Australian Government (ARC or elsewhere) for similar or linked research? This is a 'Yes' or 'No' question. If you answer 'Yes' provide the application ID(s) and briefly explain why more than one application has been submitted and, should all applications be successful, how they will be managed to avoid duplication of Australian Government funding.)

No

If yes, provide the application ID(s)

Briefly explain why more than one application for similar or linked research has been submitted and, should all applications be successful, how they will be managed to avoid duplication of Australian Government funding. (Up to 2000 Characters, approximately 285 words)

Part D - Project Description (DE220100595)

D1. Project Description

(Upload a Project Description as detailed in the Instructions to Applicants and in the required format. Ensure that the Project Description responds to the Assessment Criteria listed in the grant guidelines. (Up to 10 A4 pages))

Uploaded PDF file follows on next page.

PROJECT TITLE

Realising the potential of efficient privacy-preserving proofs for secure e-government, e-health, e-commerce, and e-voting.

PROJECT AIMS AND BACKGROUND

This DECRA project aims to invent new ways to ensure the security of e-commerce, e-government, e-health, and e-voting which avoid negative privacy impacts.

Creating secure and trustworthy systems is a major problem in cybersecurity. Competing simultaneous requirements, for example between privacy and integrity, have historically only been resolved by relying on some party to behave perfectly. However, placing trust not only in the intentions but also in the capability of any private or government organisation to behave perfectly has repeatedly been demonstrated to be problematic; indeed, no rational organisation would accept this onerous burden if it could be efficiently avoided. **Cryptography forms part of the solution by ensuring security through allowing integrity checks which do not unduly effect privacy.**

The security, and specifically integrity, of many systems can be expressed in terms of their output matching some known process on public and private data (Fig. 1)—as I shall reflect on later, the distinction between public and private data is somewhat arbitrary. Such a process can trivially be made verifiable by releasing the private data but obviously this should not be done for privacy reasons. There are cryptographic techniques which can produce proofs that the process was followed; these proofs can then be checked without access to the private data.

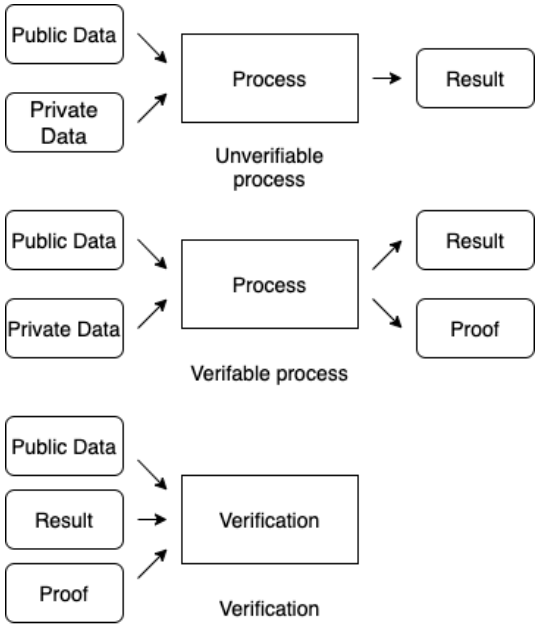

Figure 1. Diagram of an unverifiable process (top). A process which produces a proof that the result is correct (middle) and a verification of that proof (bottom).

The solutions provided by cryptography until recently have had two major downsides which prevented their wide application;

- first, **the computational costs of the solutions did not scale in many applications**.
- Secondly, **there were remaining privacy issues with the techniques** which were not acceptable in some applications.

Recent breakthroughs [12] open up the possibility of resolving both issues. However, **crucial gaps remain** in the understanding of how these techniques can be securely applied in practice.

This project will address these crucial gaps in two related ways. First, I will lead research into how to apply these techniques efficiently and securely (Aims 1 and 2). Secondly, I will conduct research which both increases the rigor of the security proofs for the theoretical solutions while also increasing confidence that the deployed implementations are secure (Aim 3).

Objective: The overarching objective of this project is to develop techniques to enable secure and trustworthy systems in e-commerce, e-government, e-health, and e-voting. Achieving this objective would contribute to **fewer economic and social costs** from these systems failing.

- **Aim 1:** To assess the applicability of existing cryptographic techniques to provide security in Australian e-government, e-health, e-commerce and e-voting without damaging privacy. The crucial question is: *Can the existing techniques provide security within the requirements and processes of existing systems?*
  Outcome Aim 1: New knowledge on the applicability of these techniques.
- **Aim 2:** To optimise the use of the cryptographic techniques to provide trustworthiness and robustness without impacting privacy when deployed.
  Outcome Aim 2: New knowledge on how to best use the techniques in practice.
- **Aim 3:** To develop the ability to prove the implementations of these techniques to be secure. This last aim utilises techniques from formal methods to reduce the gap between theory and practice by proving the security of the implementations.
  Outcome Aim 3: In the long term, improved security and trustworthiness for the systems under consideration.

Aim 3 is expected to have the greatest contribution but Aims 1 and 2 are necessary to achieve this last aim in the most impactful way.

The proposed project addresses two points within the Australian Research Priority of Cybersecurity. Primarily, this project address point three of the priority ***(new technologies and approaches to support the nation's cybersecurity)***. However, the means to achieve this goal covers point two as well ***(developing secure, trustworthy and fault-tolerant technologies).***

Background on cryptographic verification: If we want to do something securely and, particularly, in a transparent and trustworthy manner it is necessary to develop a process which provides sufficient evidence of security. We can imagine such a process as producing a body of evidence which constitutes a proof that some goal was achieved; this goal could be a security objective such as privacy or integrity. Note that in this proposal I inherit a communication problem from formal logic of there being both a formal proof system, and mathematical arguments about that proof system. The term *proof* will most often refer to an object in the formal proof system but it will sometimes refer to mathematical proofs about the proof system.

Consider, for example, health data being released by a country—perhaps about a new virus. It may be the case that a different country is distrustful of the first and would like evidence that the data is correct. However, for privacy reasons it is clear that the evidence of the correctness of the data needs to be carefully constructed. This is the central problem which cryptographic verification seeks to address: How can we show that something is true without revealing too much? In the following I will introduce how this is formalised.

When imagining a proof, it is common to think of a set of logical steps which show that a conclusion follows from the premises. This conception is inherently non-interactive since once the set of steps is written down it can be checked by anybody who knows the logical rules. Interactive proof systems were proposed by Goldwasser, Micali, and Persiano [10,11]; interactive proofs generalise the common conception by allowing the prover and verifier to interact and to be probabilistic in nature rather than deterministic. In addition, they allow the proof system to accept a proof for a false statement provided the chance of this occurring is negligible. This generalisation of the idea of a proof allows a number of interesting properties both in the complexity and "knowledge" of a proof. In all the cases we will be interested in, both the prover and the verifier will be computer programs.

One of the contributions of Goldwasser and colleagues [10,11] was to formally define the "knowledge" contained by a proof. In many applications we desire proofs which contain information beyond the truth of the theorem under consideration, such as the intuition of why it is true. In other applications we may wish to prove something is true without revealing anything other than the truth of the statement—consider for example a whistle blower wanting to show that they hold a certain position within an organisation without revealing their identity. The kind of proof where nothing is revealed expect for the truth of the statement is called a zero-knowledge proof. Zero-knowledge proofs are a major building block in modern cryptography: they underpin the ability to provide verifiable electronic voting without breaking privacy [23], the security of a large proportion of new financial technology (FinTech), and the authentication and confidentiality systems underlying the internet.

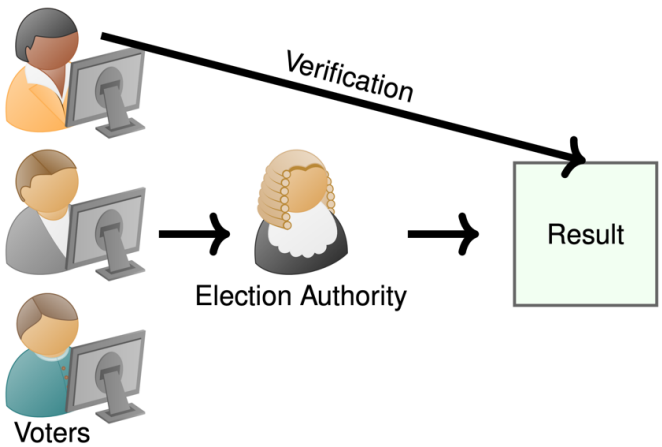

Figure 2. Voters send electronic ballots to an election authority who then announces a tally. The verification arrow represents the way in which voters can check that their vote was included in the tally.

To better understand how this works, consider a simple voting scheme consisting of a set of voters and an election authority (Fig. 2), where each voter votes yes or no. We wish to design a scheme whereby we can check that each of the submitted ballots contain at most one vote and that the election was correctly counted, but which does not "leak" how the voters voted. The basic idea is that the voters encrypt their ballots and the election authority then tallies and announces the result. I will skip over many of the details of how to construct such a scheme and focus only on how to verify the result. The critical point is that the election authority holds the key—to the encryption scheme—used to

decrypt the tally. We want a way for the election authority to prove that they correctly decrypted the tally using their key without revealing the key, which would break the privacy of the submitted ballots. We can do this with a zero-knowledge proof. **E-voting is a very clear example of the need for transparent and trustworthy systems to ensure public trust.** As already mentioned, zero-knowledge proofs are also used in FinTech to secure transactions without impacting privacy and in various authentication systems to prove knowledge of a secret credential without revealing it.

The previous examples in health and voting had a single party who knew the private data. Often in practice no single party knows all the private data, sometimes by law. These cases significantly complicate the use of the techniques since no party has the information required to make a proof. There are several approaches that are common in the literature that try to resolve this problem, but the best approach tends to be very bespoke to the situation. This problem is a significant part of the motivation of Aims 1 and 2.

One interesting aspect of interactive proofs, which has not been utilised until recently, comes from the famous PCP theorem, the proof of which resulted from a line of work by Arora, Feige, Goldwasser, Lund, Lovász, Motwani, Safra, Sudan, and Szegedy [18]. Informally, this theorem says that **interactive proofs can be of constant size regardless of the size of the non-interactive proof.** This opens up significant opportunities for **increasing the computational efficiency** of computer systems by replacing non-interactive proofs with interactive ones. Cryptography also provides methods to securely make interactive proofs non-interactive (under certain computational assumptions) which avoids any inconvenience which would otherwise be incurred because of the interactive proofs. Unfortunately the definition of interactive proofs makes no requirement that the computational complexity of the prover be reasonable (that is to say, polynomial in the size of the input). This means that in practice the techniques may be useless because we are unable to construct a proof in a reasonable time frame; fortunately, efficient provers are possible as I will detail below.

In recent work, for example by Setty [12], proof systems have been developed for algebraic circuits where the prover's work is linear in the complexity of the circuit while maintaining constant time for the verifier. This can be further enhanced by utilising techniques from cryptography which allow the statement to be committed to in constant size regardless of the size of the statement. This allows both the statement and proof transferred to be of constant size. This work is rapidly progressing in the blockchain space [26] where it will significantly ease scalability problems.

Background on formal methods: Formal methods are techniques for **the formal specification, development and verification of software** [25]. There are numerous techniques in formal methods, but for projects related to cryptography two are dominant: model checking and interactive theorem proving. Model checking is a process of building a model of the system and showing that the model has certain properties. This technique is qualitatively different from interactive theorem proving which I will cover in the next paragraph.

In relation to this project I am interested particularly in interactive theorem provers which are tools that allow encoding of mathematically rigorous definitions and algorithms, stating desired properties as theorems to be proved, and interactively proving (machine-checking) that the definitions imply these theorems. Although they provide some automated proof-search facilities, the theorems to be proved invariably require human guidance, so the tools accept directions for using a given finite collection of proof-rules, and only accept a putative proof if the proof-rules are applied correctly. Trust rests upon three pillars:

- first, the code base for interactive theorem provers is usually very small and has been scrutinised by many experts, typically over several decades;
- second, most interactive theorem provers produce a machine-readable proof of the claimed theorem and these proofs can be checked either by hand or by a different interactive theorem prover;
- third, interactive theorem provers typically enjoy extremely rigorous mathematical foundations, which have withstood decades of peer review.

Many interactive theorem provers are able to transliterate (extract) into ML, Haskell, Scheme or OCaml programs.

The main impediment to using interactive theorem proving and code extraction is the rather steep learning curve involving exotic mathematical logic(s) and the associated proof-rules. Consequently, interactive theorem provers have mostly remained in an academic setting, and were rarely considered for real life software engineering. Recent debacles, such as the security bug—called Heartbleed—in the OpenSSL cryptography library, have led companies and researchers to focus on avoiding bugs using formal verification. This has now reached the point where it is gaining momentum in mainstream cryptographic development. Examples include:

- the verification of Google BoringSSL in Coq [19],

- HACL* in F* used in Firefox [20],
- verification of correctness and security of OpenSSL HMAC [15],
- verification of elliptic curve Curve25519 [16],
- and verified side channel security of MAC-then-Encode-then-CBC-Encrypt (MEE-CBC) [17].

Aim 3 of this project makes heavy formal method to prove the security of systems using zero-knowledge proofs. **This level of rigorous security has repeatedly been shown to be necessary by disastrous flaws in practice.** In addition to the list in the previous paragraph, I have personal discovered many serious flaws in deployed scheme [3,5,24]. These formal methods are time consuming to use and hence the project will involve three PhD students, the students will need to have a strong background in logic and formal methods.

INVESTIGATOR/CAPABILITY

This DECRA proposal builds on my extensive research expertise in cybersecurity, specifically the analysis and development of cryptographic protocols and primitives, with a particular focus on holistic analysis.

I have a strong track record focusing on understanding the functionality of cryptographic primitives in their deployed settings [1,3,4,5]. I have also advanced the understanding of the ways in which protocols can provide evidence of the corruption or failure of certain parties, which is a critical issue in many areas of e-governance and e-commerce [1,4,5,6,7,8,9]. Understanding this allows the redesign of protocols to provide strong evidence of either the success or failure of the protocol and hence the certainty of the output.

I have 20 peer-reviewed publications include many first author publications in top venues. I am regularly invited to give talks at universities and to industry groups. My past work has been half related to e-voting, one quarter related to new cryptographic primitives, and the remaining one quarter related to blockchain. The two main areas in which I have analysed and developed cryptographic protocols are electronic voting and cryptocurrencies (blockchain). I am also proficient in machine-verifiable proofs and machine-assisted proof generation, and their applications to cybersecurity. I have spent significant time using the formal methods tools Coq, Tamarin and EasyCRYPT. A number of publications at various top venues, including the ACM Conference on Computer and Communications Security (CCS) and the IEEE Symposium on Security and Privacy (S&P), have resulted from this work [1,3,4].

I have expertise in examining the specification and implementation of deployed electronic voting schemes. These schemes are often inadequately developed and contain bugs which underpin the privacy of votes and the integrity of the election. My work in this area has resulted in numerous critical security disclosures. I played a part in the disclosure related to the system used in the national elections of Switzerland, which has resulted in the system being withdrawn and electronic voting suspended indefinitely. This work was presented at the IEEE Symposium on Security and Privacy (S&P), sometimes referred to as Oakland [3]. As an Australian citizen, I am also a keen participant in the evaluating of electronic voting in Australia. In total, I have contributed to the security of the following electoral systems by involvement either in the design, scrutiny or analysis:

- The sVote system in Switzerland [3]
- The election systems used in the Australian Capital Territory elections
- The iVote system used in the Australian states of New South Wales and Western Australia [24]
- The Zeus system in Greece
- The CHVote system in Switzerland [4]
- The Helios voting system used by the International Association for Cryptographic Research [2]
- The ElectionGuard system by Microsoft used in US elections [21]
- The Verificatum mix net used in numerous national elections [4]

I have contributed to cryptography primarily in the areas of ring signatures, mix nets, and secure key escrow [5,7,8,22]. My work on ring signatures provided much tighter proofs for widely deployed schemes, resulting in much stronger security guarantees in practice. In addition, I was the first to propose an efficient linkable ring signature with forward security. I am one of the leading experts on both the theoretical and practical security of mix nets, which are a crucial building block in numerous privacy-preserving technologies. I have also been active in the development of alternative cryptographic constructions which are secure against quantum computers.

My research in scalable blockchain technologies [9] resulted in the founding of the company Graphchain, spun out by the Norwegian University of Technology, Technology Transfer Network. I continue to consult regularly with industry, government and academia on the capabilities and limitations of blockchain technology.

After completing my PhD, I worked as a research and development manager in an international company (Polyas GmbH) developing cryptographic software (Polyas CORE 3.0) for electronic voting. Consequently, I have experience and expertise at all levels of cybersecurity from industry to academia. I understand the commercial imperatives and practical pressures which so often result in fallible systems. This continues to motivate my research interest in developing the techniques and tools needed to secure real-world systems.

At present I am a postdoctoral fellow on a joint Norway and Luxembourg research council project on electronic voting. My role in the project combines writing security proofs for existing cryptographic electronic voting systems and designing new schemes with a particular focus on long-term security, while also taking in analysis of deployed electronic voting schemes. In the area of long-term security, I have been particularly focused on adapting existing e-voting schemes to provide security if and when large scale quantum computation arrives [5,6].

My various collaborations with researchers at ANU on Coq and cryptography are somewhat orthogonal to my current work in Norway. This is an example of my looking to do interesting research through extending my collaborations. In this case, the collaboration is one of a handful in the world that has expertise in the mathematics of cryptography and the mathematics of formal proofs.

At present I have active research collaborations with leading experts in Germany, USA, Norway, Belgium, Luxembourg and Australia. I am still in regular contact with Prof. Colin Boyd (NTNU), Prof. Xavier Boyen (QUT), and Prof. Vanessa Teague (ANU) who supervised my research training. In addition, I regularly interact with industry partners such as Dr. Tomasz Truderung, the head of research at Polyas GmbH. More recently I have been working with Prof. Rajeev Goré, Prof. Dirk Pattinson, and Prof. Alwen Tiu from ANU; these researchers are experts in formal methods which, among other things, allows high assurance that the cryptographic techniques are correctly implemented. Their expertise aligns with Aim 3 of this project.

My research vision for the proposed DECRA projects involves applying my expertise to a number of "wicked problems" in cybersecurity. I am particularly focused on problems related to the security of cryptographic primitives and protocols in their deployed settings. I am eager to continue to involve and mentor undergraduate, masters and PhD students in security research. My previous mentoring of students has produced impressive results [1,2,4] as would my mentoring of the three PhD students to be recruited to work on this project. If awarded the DECRA, my teaching and service load will be a combined 20% and I will devote 80% of my time to leading this project.

PROJECT QUALITY AND INNOVATION

The verification of the output of a system is a process taking as input the public data, the output and the proof; I will collectively refer to the public data and the output as the statement. One of the unexplored advantages of the new verification techniques, described above, is the ability to hide the statement (Public Data and Result in Fig. 3). At first glance hiding the public data seems counterintuitive; it is, after all, public. In reality the distinction between public and private data depends on the setting. For example, when a service is hacked and the data released, we commonly say that the customers' private data is exposed even though that data is now public. Often, we have systems where data is made publicly available which has an unintended privacy impact, for example "deidentified" data which is often reidentifiable. What I refer to in this section as **hiding the public data should be thought of as introducing a new system which needs to make less data public to enable verification.**

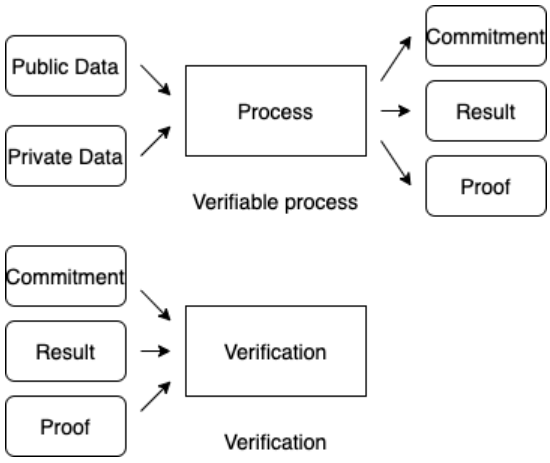

Figure 3. A verifiable process which produces a constant size commitment to the public data.

Consider the case of an election where we wish to prove that the ballots were counted correctly; if we can do this without revealing the ballots this has obvious advantages for privacy. This is one example of a number of applications where the statement being proved contains information that would perhaps be better kept secret, for example in e-health, e-government, e-voting, etc. Even when this information is encrypted, making it public incurs certain risks which various countries have decided are unacceptable; these risks include implementation bugs in the encryption scheme or future breakthroughs in cryptoanalysis revealing the information. Another risk which is of increasing concern is the potential arrival of large-scale quantum computers. The principal aim of my project is to investigate

how these new techniques can be applied to provide secure, trustworthy, and fault-tolerant technologies. **These new technologies will alleviate the current corundum of election management bodies—and others—of either placing the users' privacy or the transparency of the result in jeopardy.**

The use of these techniques is complicated because while they provide efficiency to the party verifying the process, they are still relatively expensive for the party producing the proofs. In many applications no individual should ever have access to the information required to construct the proof, which means if the technique were to be applied directly, the prover would need to be distributed. This could result in an unacceptable slow down. A carefully designed protocol could alleviate these bottlenecks by carefully choosing what facts to prove. This problem motivates Aims 1 and 2 of this proposal.

In addition to the development of new protocols which utilise these techniques in clever ways, additional work is needed to ensure that the techniques are defined sufficiently rigorously and that the deployed implementations match with the rigorous definition. This can be achieved by using interactive theorem provers to formalise and prove the properties of the techniques, and then extracting executable specifications directly from the verified formalisations. This motivates Aim 3.

Project methods: The research methods in this project come from several disciplines; partly they come from mathematics and computer science in the form of mathematical proofs and reductions between algorithms. However, they also draw from IT in designing and evaluating artefacts (systems) to gain knowledge about how to build the artefacts and their properties.

Phase 1: Analysis of existing techniques and requirements (Aim 1: Year 1). At present the techniques are designed mainly for the case where a single party, or small group of parties, knows the secret information required to construct the proof; it is unclear how applicable this is to the existing systems. This first phase will answer the question *Can the existing techniques provide security within the requirements and processes of existing systems?* Answering this question has three major facets: the first is to better understand the capabilities of these techniques. The second is to better understand the requirements of the existing systems and the third is to see how compatible the capabilities and requirements are.

The three facets of this task will be conducted concurrently:

- *The capabilities of the existing techniques will be examined.* The existing techniques are described in the literature; in this facet, I will carefully examine the mathematics of the techniques and their security proofs. This is important to understand not just the techniques as previously described but their fundamental strengths and limitations. It is expected that this task will create new knowledge about the weaknesses of the schemes since I expect to find that some do not deliver the security they promise; that is, I expect to find mistakes in the proofs or definitions. I will also contribute new knowledge about strengths either by generalising existing techniques or repairing vulnerabilities I find in existing techniques.
- *The requirements will be investigated* by a synthesis of the existing literature as well as in collaboration with partners in industry, government, and academia. Translating security requirements of real systems into cryptographic vernacular is difficult and requires a significant degree of discernment and discussion. In this task I will investigate the existing literature on the security requirements of Australian e-government, e-health, e-commerce, and e-voting. It is expected that the literature will raise more questions than it answers and dialogue with partners in industry and government will be required. The ANU Co-Lab with the Australian Signals Directorate (ASD)—which contains The Australian Cyber Security Centre (ACSC) leading the Australian Government's efforts on national cyber security—makes ANU a uniquely suited location to facilitate the success of this facet. **These government and industry links through the ASD and ASCS will be invaluable to this task.**
- *The capabilities of the techniques will be analysed with respect to these requirements.* In this stage I will analysis the degree to which the capabilities of the existing techniques fit the requirements. Since there are multiple ways to use the techniques, this stage is non-trivial and will generate significant knowledge which feeds into Phase 2. The methodology here involves coming up with alternative ways to use the techniques and then rigorously analysing the effectiveness of those methods.

This phase has the deliverable of a systemisation of knowledge suitable for publication at an appropriate venue of international renown, the exact venue depending on the outcome of the research.

This phase will be worked on jointly by myself and PhD student 2. There will be some involvement from PhD student 1 and 3 in so much as knowledge of the systems is required for their work in phase 3.

Phase 2: Optimisation of techniques to better fit requirements (Aim 2: Years 2 & 3). Having in the first phase better understood the current capabilities and requirements, the second phase will work to optimise the techniques to increase their capabilities to meet the requirements.

In the context of cryptography, we call an assumption that a certain party will behave correctly a trust assumption on that party. Trust assumptions are undesirable because if the party behaves incorrectly a system will **not** function securely. Trust assumptions have no inherent correspondence with trust, which is the belief by the public that the parties will behave correctly. Indeed, the less trust assumptions we must make about a system the more trustworthy it is. The differing trust assumptions between the techniques and the requirements suggest that the first phase will discover various gaps between the requirements and capabilities. In this phase, I will investigate how to modify:

- the techniques,
- the use of the techniques,
- and (where possible) the processes/systems to close these gaps.

Essentially, there are many ways to verify something with different trade-offs between efficiency, integrity, and privacy. This phase focuses on constructing many different approaches and comparing their relative strengths. The comparison involves considering both the security (which can be analysed with mathematical rigor) and less concrete properties like practicality. This will result in significant new knowledge about how to best use the techniques to achieve better security. It is expected that several papers will be published at A and A* venues based on this research and the knowledge gained from Facet One of Phase One.

This phase will be worked on jointly by myself and PhD student 2.

Phase 3: Proving the implementation of the techniques correct (Aim 3: Years 2 & 3). The third and most important stage (which will run concurrently with the second stage) involves proving the implementation of these techniques secure using formal methods.

In this stage I will utilise formal methods to prove these techniques, and their implementations, secure. The exact variants of the techniques which I will prove secure, and the exact properties I will prove them to have, will be guided by the outcomes of the first two phases. This stage will use the interactive theorem provers Coq and EasyCrypt, which I have successful used before [1,2,4,21], to formally define and prove the security of the techniques.

In many cases this work involves correctly formalising existing paper proofs inside the interactive theorem prover. This is difficult because the existing paper proofs gloss over difficult points or are simply wrong on certain points. The resulting formal proofs (which are machine checkable) are much harder to construct but provide much greater certainty. In addition, the higher precision in the description of the formal proofs has the additional benefit that the description of the system is executable. That is, there is little or no gap between the system which is proved secure and system which is run; this is in stark contrast to paper-based proofs which are often written with respect to a greatly simplified system. In summary, the work—while relatively straightforward—is laborious and difficult, but crucial to ensuring the security of deployed systems.

I will now describe in several steps how this phase works:

- *Encode the security definitions* inside the interactive theorem prover. There are multiple equivalent ways to encode the security definitions which make little difference to the paper proof but substantially change the difficulty of constructing a machine-checked proof. This stage involves a high degree of thought about how to best encode the definition; the encoded definition itself is a contribution. In addition, encoding the definition inside an interactive theorem prover requires formally specifying the types of data involved; paper proofs, in contrast, normally do not specify the types involved. The process of formally specifying the types is difficult but often reveals weaknesses and flaws in the definition.
- *Encode the techniques* inside the interactive theorem prover. Encoding the techniques involves overcoming many of the same problems as encoding the definitions; the types must be formally specified and the details of the paper scheme must be formalised. Again, this process, while difficult, often discovers flaws or ambiguities in the techniques.
- *Prove that the techniques satisfy the definition* inside the interactive theorem prover. I now encode the proof in the interactive theorem which then machine checks the proofs. The encoding of the proof consists of many small steps which show that the conclusion (security goal) follows for the technique and any assumptions. An example proof is shown in Fig. 4; the lemmas and proofs are on the left. On the right, the theorem prover shows the current goals and the available hypotheses.

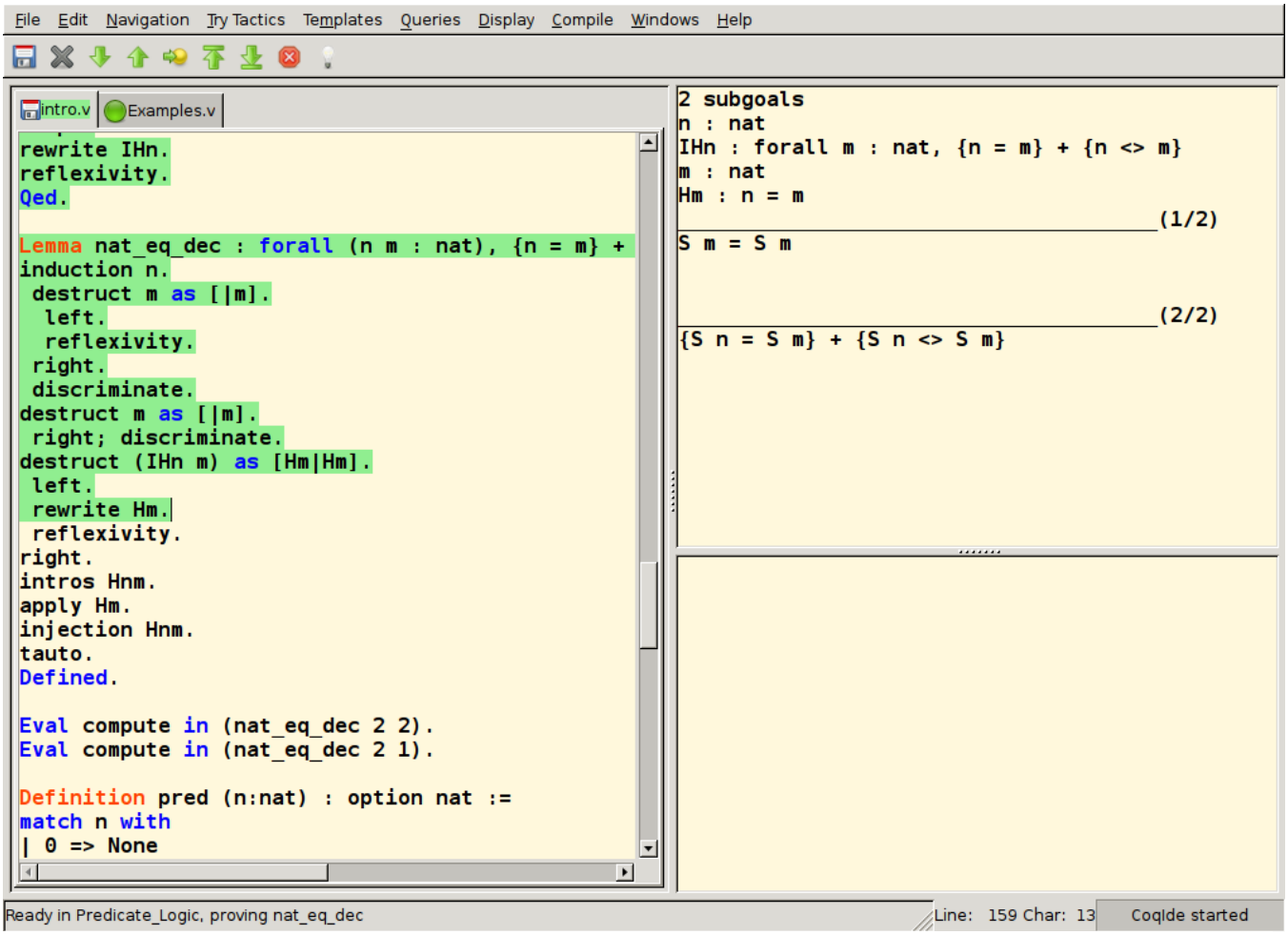

Figure 4. The Coq interactive theorem prover: A proof that for all pairs of natural numbers the numbers are either equal or different. (Screenshot by Matěj Grabovský)

This phase will be worked on jointly by myself and PhD students 1 and 3. The laborious nature of this work necessitates the larger team.

Innovation: *Cybersecurity is increasingly critical both in Australia and internationally*, and cryptography is an important part of cybersecurity. However, at present some of the most promising techniques in cryptography for secure and trustworthy systems are insufficiently developed to be deployed. In this work, I propose to address this by leading research: studying the capabilities and requirements of the techniques and systems respectively, researching how to modify the techniques and systems to increase compatibility, and proving the implementations of the techniques to be secure. The outcomes of this research will be beneficial to both theory and practice, and particularly to the security of deployed systems in e-health, e-commerce, e-voting and e-government.

BENEFIT

As already noted, at present numerous cryptographic techniques have significant potential to seriously improve the trustworthiness and security of computer systems in e-government, e-health, e-commerce, and e-voting. However, they are not deployed; this appears to be because their capabilities do not directly align with the needs of existing systems. For example, the techniques incur privacy risks or otherwise fail to meet the practical requirements. By analysing the requirements and expanding on these new methods so that they do not incur these privacy risks, I can **make systems more trustworthy and secure**. This project has the additional benefit of developing techniques in such a way as to show the implementations are secure. In doing this, I will create new knowledge of significant practical importance. In particular, **this knowledge will support the national priority in cybersecurity of secure and trustworthy systems which are tolerant of faults.**

Economic benefit: This research project will enable more secure systems; this has a direct economic and commercial benefit to the organisations who run these systems, which avoid disruptions if and when these systems are attacked.

In addition to the direct, indirect and reputational costs the organisations **avoid**, the failure of many of these systems would impose significant costs on the customers of the organisation. These costs include **identity theft**, release of personal information, etc.

Social benefit: Many of the systems in e-health, e-government and e-voting require public trust to function; indeed, such trust is critical to the health of our democratic society. Systems which provide strong security in a transparent and trustworthy manner are, therefore, increasingly crucial as we continue to transition to a more digital society. The results of this research will enable the creation of such systems.

FEASIBILITY

The scope of the project is relatively broad. It encompasses both: the machine checking of existing paper proofs which—while complicated—has a relatively low of risk of failure, and the more fundamental research into the nature of these techniques and the best way to apply them.

Track record: I have an outstanding track record in the analysis and development of secure and trustworthy systems. My research has impacted many systems, several being of national importance; my research has been published at the best venues [1,2,3,5,6] and I am highly regarded in my area. I am a recognised expert in both the cryptographic and formal methods techniques required by this project [1,4,21].

Participants: To complete the planned research, I and three PhD students will work together. All students are expected to start in early 2022 (Year 1), complete their respective research components in 2024 and submit in 2025 (Year 3). In addition, two Honours students will work on this project on phase 3 "Proving the implementation of the techniques correct." The large team will ensure adequate manhours to ensure the successful completion of the project.

Table 1: Project timeline

	Year 1				Year 2				Year 3				Personnel
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
Aim 1													CI, PhD2
Aim 2													CI, PhD2
Aim 3													CI, PhD1, PhD3

High-quality research environment: The project does not require any significant laboratory facilities or incur costs other than the candidate's time and the resources required to effectively collaborate with local and international partners, such as travel. The Australian National University, with its excellent track record on research in formal methods, provides an outstanding supportive environment for the candidate and the project. This can be seen from the existing results in related topics produced by the candidate in collaboration with staff from ANU [1,2,5,21]. The environment will also be highly supportive of the HDR students who will work on the project. PhD student 2 will be connected with the domestic and international collaborators already mentioned to develop expertise in the area. PhD students 1 and 3 will benefit from the outstanding expertise at ANU in interactive theorem proving.

One example of the outstanding research environment at ANU—in the area of this proposal—is the Co-Lab collaboration with the Australian Signals Directorate (ASD). This collaborative research environment within ANU conducts complex research into Australia's toughest national security problems; it also fosters the STEM skills and capabilities needed to address the national shortage of expertise in cybersecurity.

The world-class research environment, large team, and my excellent track record will ensure the success of this project.

COMMUNICATION OF RESULTS

The results will be disseminated primarily through publication at leading conferences (CORE A*) in information security such as IEEE Security and Privacy (S&P) and ACM Computer and Community Security (CCS), as well as other (CORE A) conferences such as European Symposium on Research in Computer Security (ESORICS), Computer Security Foundations symposium (CSF) and the leading local venue Australasian Information Security Conference (ACISP). The results will also be communicated through the PhD students' dissertations.

The research artefacts produced by this project (such as Coq code) will be made available on my homepage or on GitHub. In addition, I will continue to consult regularly with industry and government on cybersecurity issues. The ANU commercialisation office with assist with IP management of the techniques created. Furthermore, the ANU College of Engineering and Computer Science's marketing team will assist with public engagement through social media, ANU's website, and public seminars.

REFERENCES

[1] Thomas Haines, Rajeev Goré, and Mukesh Tiwari. Verified verifiers for verifying elections. In 2019 ACM Conference on Computer and Communications Security, CCS 2019, pages 685–702. ACM, 2019.

[2] Thomas Haines, Dirk Pattinson, and Mukesh Tiwari. Verifiable homomorphic tallying for the schulze vote counting scheme. In VSTTE, volume 12031 of Lecture Notes in Computer Science, pages 36–53. Springer, 2019.

[3] Thomas Haines, Sarah J. Lewis, Olivier Pereira, and Vanessa Teague. How not to prove your election outcome. In 2020 IEEE Symposium on Security and Privacy, pages 644–660, 2020.

[4] Thomas Haines, Rajeev Goré, Bhavesh Sharma. Did you mix me? Formally Verifying Verifiable Mix Nets in Electronic Voting. In 2021 IEEE Symposium on Security and Privacy, to appear, 2021.

[5] Thomas Haines, Johannes Müller. SoK: Techniques for Verifiable Mix Nets, In 2020 Computer Security Foundations, CSF 202, pages 49–64. 2020.

[6] Xavier Boyen, Thomas Haines, Johannes Müller. A Verifiable and Practical Lattice-Based Decryption Mix Net with External Auditing, In 2020 European Symposium on Research in Computer Security, ESORICS 2020, pages 336–356. 2020

[7] Xavier Boyen, Thomas Haines. Forward-Secure Linkable Ring Signatures, in 2018 Australasian Conference on Information Security and Privacy, ACISP 2019, pages 245–264, 2018.

[8] Xavier Boyen, Thomas Haines. Forward-Secure Linkable Ring Signatures from Bilinear Maps, in Cryptography, vol. 2, no. 4, pages 35-, 2018.

[9] Xavier Boyen, Christopher Carr, Thomas Haines 2016, 'Blockchain-Free Cryptocurrencies. A Rational Framework for Truly Decentralised Fast Transactions', IACR Cryptol. ePrint Arch., vol. 2016, pp. 871

[10] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems (extended abstract). In STOC, pages291–304. ACM, 1985.

[11] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. SIAM J. Comput., 18(1):186–208, 1989.

[12] Srinath Setty. Spartan: Efficient and general-purpose zksnarks without trusted setup. In CRYPTO (3), volume 12172 of Lecture Notes in Com-puter Science, pages 704–737. Springer, 2020

[13] Erbsen, J. Philipoom, J. Gross, R. Sloan, and A. Chlipala. 2019. Simple High-Level Code for Cryptographic Arithmetic - With Proofs, Without Compromises. In 2019 IEEE Symposium on Security and Privacy, 2019

[14] Jean Karim Zinzindohoué, Karthikeyan Bhargavan, Jonathan Protzenko, and Benjamin Beurdouche. 2017. HACL*: A Verified Modern Cryptographic Library. In 2017 ACM Conference on Computer and Communications Security, CCS 2017, pages 1789–1806. ACM, 2017.

[15] Lennart Beringer, Adam Petcher, Katherine Q. Ye, and Andrew W. Appel. 2015. Verified Correctness and Security of OpenSSL HMAC. In 24th USENIX Security Symposium (USENIX Security 15). USENIX Association, Washington, D.C., 207–221.

[16] Yu-Fang Chen, Chang-Hong Hsu, Hsin-Hung Lin, Peter Schwabe, Ming-Hsien Tsai, Bow-Yaw Wang, Bo-Yin Yang, and Shang-Yi Yang. 2014. Verifying Curve25519 Software. In 2014 ACM Conference on Computer and Communications Security, CCS 2014. ACM, page 299–309.

[17] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, and François Dupressoir. 2016. Verifiable Side-Channel Security of Cryptographic Implementations: Constant-Time MEE-CBC. In Fast Software Encryption, pages 163–184.

[18] Arora Sanjeev, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. 1998. Proof verification and the hardness of approximation problems. In Journal of the ACM (JACM) 45, no. 3 (1998), pages 501-555.

[19] Andres Erbsen, Jade Philipoom, Jason Gross, Robert Sloan, and Adam Chlipala. 2019. Simple High- Level Code for Cryptographic Arithmetic - With Proofs, Without Compromises. In 2019 IEEE Symposium on Security and Privacy, pages 1202-1219, 2020.

[20] Jean Karim Zinzindohoué, Karthikeyan Bhargavan, Jonathan Protzenko, and Benjamin Beurdouche. 2017. HACL*: A Verified Modern Cryptographic Library. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017. ACM, pages 1789–1806.

[21] Thomas Haines, Rajeev Goré, Jack Stodart, 2020. Machine-checking the universal verifiability of ElectionGuard. In Proceedings of the 2020 Nordic Conference on Secure IT Systems, Nordsec 2020, to appear.

[22] Colin Boyd, Xavier Boyen, Christopher Carr, and Thomas Haines, 2016. Key Recovery: Inert and Public', Mycrypt 2017, pages 111–126.

[23] Fen Hao, and Peter YA Ryan. Real-World Electronic Voting: Design, Analysis and Deployment. CRC Press, 2016.

[24] Thomas Haines, 2020. Flaws in the Scytl JavaScript ElGamal implementation. https://folk.ntnu.no/thomaeh/Scytl_js_ElGamal.pdf

[25] Manuel Barbosa, Gilles Barthe, Karthikeyan Bhargavan, Bruno Blanchet, Cas Cremers, Kevin Liao, and Bryan Parno. SoK: Computer-Aided Cryptography." IACR Cryptol. ePrint Arch. 2019: 1393.

[26] Matter Labs, zkSynv, https://zksync.io/

D2. Statement by the Administering Organisation

(Provide a Statement that addresses the relevant criteria as set out in the grant guidelines. The Statement must be signed by the Deputy Vice-Chancellor (Research) or equivalent. (Upload a PDF of up to three A4 pages))

Uploaded PDF file follows on next page.

Australian National University

D2. Statement by the Administering Organisation

Dr. Thomas Haines (DE220100595): *Secure information through interactive proofs for e-government and e-voting*

Dear Expert Assessors, College of Experts and the Australian Research Council,

I provide my unreserved support of Dr Thomas Haines' Discovery Early Career Researcher Award proposal.

Dr Thomas Haines has an impressive research record and impact in the area of this proposal. One of his disclosures saw the Swiss Vote system withdrawn from use in Switzerland's national elections; he is also acknowledged by many top systems and products in cryptography and e-voting for his advice which helped to improve the security and reliability of these systems. These systems include the internationally famous Australian-produced cryptography library BouncyCastle and the verifiable mixnet Verificatum which is used in several national elections around the world. In addition, his research has led to the founding of a spin-off company called Graphchain, based on research resolving scalability constraints in distributed ledger e-commerce.

His 20 peer-reviewed publications include many first author publications in top venues. These publications are based on work which demonstrates strong collaborations both nationally and internationally and have resulted in numerous vulnerability disclosures. Dr Haines' time in industry and academia make him an outstanding candidate to conduct research that will result in substantial real-world impact at a time when government and election cybersecurity is of profound significance to Australia and the world.

Research Environment

The Australian National University (ANU) is a research-intensive university, ranking 1st in Australia and 31st internationally in the QS World University Rankings (2021). The Research School of Computer Science at the ANU is internationally recognised and well placed to support Dr Haines' future research, having been rated a "5" in the most recent Excellence in Research for Australia report in the two fields most related to this research; namely Computer Software (0803) and Computation Theory (0802).

Alignment with research strengths of the ANU

The research focus of Dr Haines' DECRA proposal, improving security and robustness of systems, aligns with the National Science and Research Priority of Cybersecurity. The ANU strategic initiative of collaborating with the Australian Signals Directorate (ASD) - which through the Australian Cyber Security Centre (ACSC) leads the Australian Government's efforts on national cyber security - places ANU at the forefront of this research area. This collaboration with ASD will build a centre of excellence for relevant fundamental research, capacity building, and nurturing the talent Australia needs to secure our national interests. Dr Haines' skills in formally analysing the security of deployed systems will enable ground-breaking research in collaboration with the ASD, the ANU Cyber Institute, and also the Human-Centred Computing group based in the host school.

The proposed research project also aligns strongly with the ANU focus on translational outcomes based on the fundamental research. The ANU already has world leading research in areas which are foundational to cybersecurity, such as formal methods, and Dr Haines is uniquely situated to complement existing expertise to translate this foundational research into implementable security applications for systems currently deployed.

Resources provided to candidate

The Research School of Computer Science strongly supports this proposal whilst noting it has specific and unique contributions to the host School, the collaborative partnership that exists between the Australian Signals Directorate (ASD) and the ANU, and to the information security community more broadly. If the DECRA application is successful, the ANU and the Research School of Computer Science will support the project in following ways:

- The ANU will fund the salary gap of ($46,113) between the DECRA salary funding and the ANU's B3 level salary for the duration of the project.
- The ANU will provide Personal Development (PD) funds for Dr Haines and the students to present at national and international conferences and meet with local and international collaborators at the level of ($19,500) per annum for the duration of the project.
- In addition, the host School will provide each of the PhD students with a ($6,000) professional development allocation.

Within the host school, Dr Haines will receive mentorship from Associate Prof. Alwen Tiu and Prof. Rajeev Goré. In addition, he will also receive mentoring from a diverse senior academic at the ANU via the sector leading ANU NECTAR program for early career academics. To further develop his skills in research management, supervision and teaching, he will be encouraged to make use of the targeted short program of career development, grant writing and University education provided by the ANU for early career researchers.

Opportunities for the DECRA Candidate to demonstrate the level of independence required to be competitive for research and/or research and teaching pathways at the ANU during and after the project

During this award, Dr Haines will also continue to work closely with the business and government communities to increase cybersecurity in Australia. He will be provided with opportunities to supervise research students, strengthen national and international research collaborations, and develop his ongoing research agenda. The Research School of Computer Science is working to develop itself as a leader in cybersecurity research and education in Australia. On a competitive basis, the ANU offers a number of post-DECRA opportunities. However, the resources, experience and outcome provided by a DECRA will greatly benefit Dr Haines' future academic career by allowing him to grow a critical core of cybersecurity experts that will keep Australia at the cutting edge of security technologies.

I am delighted to offer my enthusiastic support of this application on behalf of the Australian National University.

Yours sincerely,

Prof. Nick Birbilis
Deputy Dean
College of Engineering and Computer Science
On behalf of the Deputy Vice-Chancellor (Research and Innovation)

Part E - Project Cost (DE220100595)

E1. What is the proposed budget for your project?

(There are rules around what funds can be requested from the ARC. You must adhere to the scheme specific requirements listed in the grant guidelines. Refer to the Instructions to Applicants for detailed instructions on how to fill out the budget section.)

Total requested budget: $416,400

Year 1

Description	ARC	Admin Org
	Cash	Cash
Total	138,800	65,613
Personnel	134,300	46,113
Dr Thomas Haines (Discovery Early Career Researcher Award)	106,194	46,113
HDR (Higher Degree by Research stipend)	28,106	
Travel	4,500	19,500
ANU funded travel for Dr Haines to visit international collaborator		6,000
ARC funded International Conference Travel	4,500	
ANU funded travel for DR Haines to visit domestic collaborator		3,000
ANU funded travel for HDR students to present at a domestic conference ($2,000) per trip		6,000
ANU funded travel for HDR students to present at international conferences		4,500

Year 2

Description	ARC	Admin Org
	Cash	Cash
Total	138,800	65,613
Personnel	134,300	46,113
Dr Thomas Haines (Discovery Early Career Researcher Award)	106,194	46,113
HDR (Higher Degree by Research stipend)	28,106	
Travel	4,500	19,500
ANU funded travel for Dr Haines to visit international collaborator		6,000
ARC funded International Conference Travel	4,500	
ANU funded travel for DR Haines to visit domestic collaborator		3,000
ANU funded travel for HDR students to present at a domestic conference ($2,000) per trip		6,000
ANU funded travel for HDR students to present at international conferences		4,500

Year 3

Description	ARC	Admin Org
	Cash	Cash

Total	138,800	65,613
Personnel	134,300	46,113
Dr Thomas Haines (Discovery Early Career Researcher Award)	106,194	46,113
HDR (Higher Degree by Research stipend)	28,106	
Travel	4,500	19,500
ANU funded travel for Dr Haines to visit international collaborator		6,000
ARC funded International Conference Travel	4,500	
ANU funded travel for DR Haines to visit domestic collaborator		3,000
ANU funded travel for HDR students to present at a domestic conference ($2,000) per trip		6,000
ANU funded travel for HDR students to present at international conferences		4,500

E2. Justification of funding requested from the ARC

(Fully justify each budget item requested in terms of need and cost. Use the same headings as in the Description column in the above Budget Table of this application. (Upload a PDF of up to four A4 pages and within the required format))

Budget Justification

Uploaded PDF file follows on next page.

Justification of non-salary funding requested from the ARC

The total funding requested from the ARC amounts to $138,800 per annum.

This project does not require the purchase of any special equipment. However, it is heavily reliant on a sizeable research team; this team is partly internal to the project, see personnel below, and partly consists of collaborators. While the standard means of communication with collaborators will be remotely by email and video conference, the collaborations are greatly aided by some in person contact. For this reason, ANU will provide substantial funds to allows such visits. In addition to these visits it is necessary for the wide dissemination of research results to present them at leading conferences. For this reason, funding for three trips to international conferences is requested from the ARC.

Personnel

HDR stipend

This project has three aims, namely: (a) the analysis of the existing techniques and requirements, (b) the optimisation of the techniques to better fit the requirements, and (c) proving the techniques correct. Within these aims there are clearly articulated projects which are ideally scoped for doctoral students; the first is within Aims 1 and 2 while the second and third are within Aims 1 and 3, To ensure the successful completion of the project we need students with a sufficient background in mathematics, logic, and programming. The complexities in the research will require significant time to solve which necessities a large team. Therefore, three HDR students will be required (one with ARC support and two with ANU support).

ANU provides funding for HDR Students 2 and 3 as support in-kind. The request here is for HDR Student 1.

HDR Student 1 will focus on Aims 1 and 3. The candidate will develop the techniques needed to formally prove the security of the implementations of the cryptographic techniques. This work is a crucial part of the project delivering great benefits to both the theory and practice of cybersecurity. However, the work is time intensive hence the need for a large team to successfully complete the project. The HDR Stipend = **$28,106 p.a for 3 years. Total = $84,318.**

Travel

Dr Haines and the students will communicate the results of the project through publication at top conferences in the field of research such as IEEE Security and Privacy (S&P), ACM Computer and Community Security (CCS), European Symposium on Research in Computer Security (ESORICS), and Computer Security Foundations symposium (CSF). In this field, conferences are the most important publication venues; the conferences require that at least one author of every accepted paper registers and attends. The need to attend conferences, which are overwhelming overseas, in order to publish at the most respected venues necessitates the large travel budget of this project.

The collaborative links are much more productive with at least some in-person contact. In some cases, the collaboration requires traveling because the data involved is not allowed to leave a secure premise. The majority of this funding will be provided by ANU; the request here is for three international conference trips. Each conference trip will be approximately one week in length and cost roughly $4,500, including flight ($2,000), registration fees ($1,000), accommodation ($800) and living allowance ($700).

E3. Details of non-ARC contributions

(Provide an explanation of how non-ARC contributions will support the proposed project. Use the same headings as in the Description column in the above Budget Table of this application. (Upload a PDF of up to two A4 pages and within the required format))
Details of Non-ARC Contributions

Uploaded PDF file follows on next page.

E3. Details of non-ARC contributions

CONTRIBUTIONS BY ANU

Personnel
Salary Gap

Dr Haines' ANU level B3 salary is **$152,307 p.a** (including on-costs). ANU will fund a salary gap of **$46,113 p.a** during the project.

Travel
Travel to local and international conferences and to visit collaborators

ANU will provide funding of **$19,500 p.a for 3 years. Total = $58,500** to support Dr Haines and the students to collaborate with international partners and attend conferences for the purpose of reporting research results. It is anticipated that $27,000 of this will be used by Dr Haines and $31,500 used by the students.

ANU will additionally provide a **$6,000** in-kind professional development fund **per student. Total $18,000** to support the students to attend conferences, etc.

It is anticipated that roughly 70% of this funding will be used for international travel and 30% for domestic.

All the trips listed below also include dissemination of research results by giving talks at the respective university or company.

The following trips are planned to visit domestic collaborators:

Two week visit to Associate Prof. Xavier Boyen at the Queensland University of Technology. Purpose: To collaborate on developing efficient zero-knowledge proofs secure against quantum computers. Cost: $3,000, including flight ($500), accommodation ($1500) and living allowance ($1000).
Two week visit to Associate Prof. Vanessa Teague at the Thinking Cybersecurity. Purpose: To collaborate on developing efficient zero-knowledge proofs for use in e-government. Cost: $3,000, including flight ($500), accommodation ($1500) and living allowance ($1000).

The following trips are planned to visit international collaborators:

Two week visit to Prof. Kristian Gjøsteen at the Norwegian University of Science and Technology. Purpose: To collaborate on developing efficient zero-knowledge proofs with a particular focus on the use case of e-voting. Cost: $6,000, including flight ($2,000), accommodation ($2000) and living allowance ($2000).
Two week visit to Prof. Peter Ryan at the University of Luxembourg. Purpose: To collaborate on the application of efficient zero-knowledge proofs in electronic health. Cost: $6,000, including flight ($2,000), accommodation ($2000) and living allowance ($2000).
Two week visit to Dr. Tomasz Truderung at Polyas GmbH. Purpose: To collaborate on the application of efficient zero-knowledge proofs to electronic voting. Cost: $5,000, including flight ($2,000), accommodation ($2000) and living allowance ($1000).

Other Contributions From ANU
HDR stipends supported (in-kind) by ANU

Within the project there are clearly articulated projects which are ideally scoped for doctoral students. A stipend is requested from the ARC for HDR Student 1. ANU provides *(in-kind)* support for HDR Students 2 and 3. HDR student 2 will focus on Aims 1 and 2 and HDR student 3 will focus on Aims 1 and 3. The first candidate will investigate the current state of the art in cryptographic techniques for verifiability and the needs of current systems in e-commerce, e-government, e-health and e-voting while the second and third candidates will work on formally proving the implementations correct in an interactive theorem prover. The HDR Stipends supported by ANU = **$28,106 p.a each for 3 years. Total = $168,636.**

Part F - Participant Details including ROPE (Dr Thomas Haines)

F1. Personal Details

(To update any Personal Details, click on the 'Manage Personal Details' link below. Note this will open a new browser tab. When returning to the form ensure to 'Refresh' the page to capture the changes made to the participant's profile.
Note: The date of birth, country of birth, citizenship, material personal interests and Indigenous status section will not appear in the PDF version of the form and will not be visible to assessors.
Data may be shared with other Commonwealth Entities.
All information contained in Part F is visible to the Administering Organisation on this application.)

Participation Type

Discovery Early Career Researcher Award

Title

Dr

First Name

Thomas

Second Name

Edmund

Family Name

Haines

F2. Current country of residence

(If the DECRA candidate is a Foreign National, they must obtain a legal right to work and reside in Australia.)

Norway

F5. Qualifications

(To update any qualifications, click on the 'Manage Qualifications' link below. Note this will open a new browser tab. When returning to the form ensure to 'Refresh' the page to capture the changes made to the DECRA candidate's profile.)

Conferral Date	AQF Level	Degree/Award Title	Discipline/Field	Awarding Organisation	Country of Award
12/12/2017	Doctoral Degree	Doctor of Philosophy	Information Security	Queensland University of Technology	Australia
11/12/2013	Bachelor Honours Degree,Graduate Certificate, Graduate Diploma	Bachelor of Information Technology (Honours)		Queensland University of Technology	Australia
11/12/2012	Bachelor Degree	Bachelor of Games and Interactive Entertainment (Software Technologies)		Queensland University of Technology	Australia

F6. Research Load (non-ARC Grants and Research)

(Provide details of research funding from non-ARC sources (in Australia and overseas). For research funding from non-ARC sources, list all projects/applications/awards/fellowships awarded or requests submitted involving that participant for funding for the years 2021 to 2025 inclusive.)

Uploaded PDF file follows on next page.

F6. Research Load (non-ARC Grants and Research)

Description (All named investigators on any application or grant/fellowship in which the DECRA candidate is involved, project title, source of support, scheme and round)	**Same Research Area** (Yes/No)	**Support Status** (Requested/Current/Past)	**Application/Project ID** (for NHMRC applications only)	**2021** $'000	**2022** $'000	**2023** $'000	**2024** $'000	**2025** $'000
Secure, Usable and Robust Cryptographic Voting Systems (SURCVS) Norwegian and Luxembourgish Research Councils Prof. Kristian Gjøsteen Prof. Colin Boyd Prof. Peter Y. A. Ryan Prof. Sjouke Mau, 2018	Y	C		450	450			

F7. Currently held ARC Projects

(This information is auto-populated. If you have any concerns with the information recorded here, please contact your Administering Organisation's Research Office.)

F8. What will the DECRA candidate's time commitment be to research activities related to this project?

*(It is a requirement for DECRA candidate to work a minimum of 0.8 full-time equivalent (FTE) of their time on research activities related to the DECRA.
)*

0.8

F9. Eligibility - Relevant Qualification

(Please select the qualification which is most relevant to the application.)

Degree/Award Title	Awarding Organisation	Conferral Date
Doctor of Philosophy	Queensland University of Technology	12/12/2017

F10. Eligibility - Has the DECRA candidate been granted an extension by the Administering Organisation, to the eligibility period due to a significant career interruption as outlined in the grant guidelines?

(If the DECRA candidate's qualification relevant to this application (listed in question F9) was awarded prior to 1 March 2016 and they have had a significant career interruption (as listed in the grant guidelines), the participant will need to seek an extension to the eligibility period through their Deputy Vice-Chancellor (Research).)

No

F11. Eligibility - Select the category of career interruption claimed (more than one may be selected)

*(Choose all types of career interruptions which have been claimed and granted by the DECRA candidate's Deputy Vice-Chancellor (Research).
Select a type of interruption and click 'Add'.)*

F12. Eligibility - What is the total period of extension that the DECRA candidate has claimed?

(Select the period of time which most closely equals the total period of extension claimed.)

F13. Eligibility - Current Research Fellowship or Award funded by other Australian Government agencies

(Do not list Fellowships and Awards granted by the ARC. Only list Fellowships and Awards from other agencies.)
Does the DECRA candidate hold a current Research Fellowship or Award funded by other Australian Government agencies?

No

F14. Eligibility - Project Relinquishment or Application Withdrawal

(ARC grant guidelines specify the limits on the number of applications and projects per named participant. This question will be activated where a DECRA candidate will exceed ARC project limits, if this application is successful.

In this case, while the application can be submitted, project limits must be met under the grant guidelines before the project can start. Project limits can be met by relinquishing existing active project(s), or relinquishing role(s) on existing active projects, or withdrawing application(s) that would exceed the project limits.)

F15. Research Opportunity and Performance Evidence (ROPE) - Current and previous appointment(s) / position(s) - during the past 10 years

(To update any details in this table, click on the 'Manage Employment Details' link in this question. Note this will open in a new browser tab. 'Refresh' the application page when returning to the form to capture changes made to the DECRA candidate's profile.)

Description	Department	Contract Type	Employment Type	Start Date	End Date	Organisation
Postdoctoral Fellow	Department of Mathematical Sciences	Contract	Full Time	02/01/2019	01/12/2021	Norwegian University of Science and Technology
Research and Development Manager		Permanent	Full Time	01/07/2017	31/12/2018	Polyas GmbH

F16. Research Opportunity and Performance Evidence (ROPE) - Career Interruptions

(You must read the ROPE Statement http://www.arc.gov.au/arc-research-opportunity-and-performance-evidence-rope-statement before filling out this section.)
Has the DECRA candidate experienced a significant interruption that has impacted on research opportunity?

Yes

From when

13/12/2017

To when

30/11/2018

FTE of academic interruption

0.4

Interruption Category

Non-research employment

Details

My role as a Research and Development Manager at Polyas GmbH was significantly administrative.

From when

01/12/2018

To when

31/01/2019

FTE of academic interruption

1.0

Interruption Category

Other

Details

Relocation from Germany to Norway

F17. Research Opportunity and Performance Evidence (ROPE) - Details of the DECRA candidate's career and opportunities for research, evidence of research impact and contributions to the field, including those most relevant to this application

(Provide details of the DECRA candidate's career and opportunities. This should not include information presented in the following questions. (Upload a PDF of up to five A4 pages))

Uploaded PDF file follows on next page.

Research Opportunity and Performance Evidence (ROPE)

AMOUNT OF TIME AS AN ACTIVE RESEARCHER

I was awarded my PhD 4 years ago in December 2017. In the period since, I have experienced a total of 6.5 months at 1.0 FTE of career interruptions including both the component of my position in industry which was not research related, and the interruptions in moving from Germany to Norway.

RESEARCH OPPORTUNITIES

I was a PhD student between 2014 and 2017 in information security and applied cryptography. Supervised by Prof. Xavier Boyen, I undertook research into cryptographic techniques which allow trustworthy systems that do not depend on trusted authorities.

After completing my PHD I took an industry position in Germany working for Polyas GmbH, a company which runs secure online elections; Polyas GmbH is one of the leading companies in this space and runs elections for many organisations, including the Gesellschaft für Informatik (GI), a German organization of approximately 20,000 computer science educators, researchers, and professionals. During this time as a research and development manager, my work straddled both internal development within the business (40%) and research (60%). This reduced the time I had for research and publication, but it gave me valuable insight into the reality of the business context which my research impacts. During my time at Polyas, I was intimately involved in developing secure systems. A key part of this involved understanding the research in the area in enough detail to implement it. This process was a major development opportunity which underlined for me the difference between the imprecise paper proofs in the literature and the requirements of practice. Many of the lessons learned during this period inform my current research agenda:

- the analysis of deployed schemes, and
- the use of the deployed formal methods to prove implementations secure.

I also took the initiative during my time in industry to develop and expand my academic links. I held the position at Polyas until the end of 2018 when I moved to the Department of Mathematic Sciences at Norwegian University of Science and Technology (NTNU).

Since starting as a postdoc at NTNU in Norway, I have spent the majority of my time leading research (80%). NTNU has been an excellent place to develop as a research leader with exceptional support for research, international collaborative links and outstanding students. NTNU was ranked first in the world for research collaboration with industry by the Times Higher Education World University Rankings in 2017. My collaboration with industry and government have involved analysing the security of nine different election schemes used in a variety of Government and organisation elections. One of these analyses revealed numerus flaws which ultimately resulted in the Swiss electronic voting system being withdrawn from use.

Through my PhD, time in Industry, and at NTNU, I have accumulated 20 peer-reviewed publications including many first author publications in top venues. These publications are based on work which demonstrates strong collaborations both nationally and internationally and have resulted in numerous serious vulnerability disclosures. As such, I have successfully established a sustained research trajectory with impactful research published at the most respected international venues including IEEE Symposium on Security and Privacy and the ACM Conference on Computer and Communications Security (see [1,2,3] in Ten Career-Best Research Outputs).

I am fortunate to have developed and maintained an excellent network of collaborators and mentors. Through these and other collaborations, I have the opportunity to work on the research problems which need to be solved to enable secure systems in practice.

- I am still in regular contact and collaboration with Prof. Colin Boyd (NTNU), Prof. Xavier Boyen (QUT), and Prof. Vanessa Teague (ANU) who supervised my research training; see [1,5,6,7,10] in Ten Career-Best Research Outputs for examples of results of collaborations after my PhD ended.
- In addition, I received immensely valuable mentorship from Dr. Tomasz Truderung, the head of research at Polyas during my time there; Dr. Truderung has worked in industry for the last five years but before that was one of the leading academics in the study of secure online voting. While I have no joint papers with Dr. Truderung, he was vital in guiding the research which resulted in [2,3] in Ten Career-Best Research Outputs.
- In Norway I have been lucky enough to work with Prof. Kristian Gjøsteen who is leading expert in mathematical cryptography. My collaborations with Prof. Gjøsteen have resulted in several papers.

- More recently I have been working with Prof. Rajeev Goré, Prof. Dirk Pattinson, and Prof. Alwen Tiu from ANU. These professors are experts in formal methods which, among other things, allows high assurance that the cryptographic techniques are correctly implemented. My collaboration with Prof. Tiu on issues with the ACT election system resulted in significant media attention. My collaboration with Prof. Goré and Prof. Pattinson has resulted in papers which have been accepted at top conferences including [2,3,9] in Ten Career-Best Research Outputs. Their expertise aligns with Aim 3 of this project.

During my research career, I have demonstrated a strong capacity for research, an outstanding track record of impact, excellent communication, and high publication productivity. I am well positioned to take advantage of this DECRA to conduct excellent research, with local and international collaborators, which enhances Australia's cybersecurity.

Research mentoring and research facilities

Facilities. The Research School of Computer Science at ANU has an excellent track record of outstanding research, having been ranked 5 out of 5 in Computer Software (0803) and Computation Theory (0802), the two fields most related to this research, in the most recent Excellence in Research for Australia report. A key component of this is the exceptional facilities and support for academics including hosting the National Computational Infrastructure (NCI). As well as the exceptional facilities and support, ANU has terrific pipelines for involving its brilliant students in research. ANU's Co-Lab with the Australian Signals Directorate (ASD) is an incredible resource for myself and the research proposed in this DECRA. ASD through its subsection The Australian Cyber Security Centre (ACSC) leads the Australian Government's efforts on national cyber security. ANU's Co-Lab with ASD is at the forefront of addressing the National Science and Research Priority of Cybersecurity.

Mentoring. Prof. Rajeev Goré will be the principal mentor; he is a world-renowned expert in logic and formal verification. He mentored me through my transition from cryptography into formal methods and is a co-author on two of my top publications. Prof. Alwen Tiu is an expert in logic and computer security; he was among the first in the world to notice a crucial bug in the Apple-Google contact tracing protocol. I have already worked with Prof. Tiu on disclosing flaws in the ACT election system. Prof. Tiu will provide guidance both on the formal methods involved in the project and a wealth of experience in securing deployed systems. Prof. Vanessa Teague has a track record of world-class research into security issues in e-voting and e-government, for example the inadequate deanonymisation of health records in Australia, and insecure e-voting in Australia and internationally. Prof. Teague's expertise in examining e-government, e-health and e-voting in Australia is unmatched and her expertise will greatly aid this project.

Beyond the core mentoring team, the project will also draw upon my extensive collaborative network to deal with particular emerging threats to the security of deployed systems: Prof. Xavier Boyen is a world-renowned cryptographer with a particular specialisation in cryptography secure against adversaries with quantum computers. Prof. Kristian Gjøsteen is a leading expert in e-voting and cryptography secure against quantum computers. Along with these academic partners there is an extensive network of industry and government partners.

RESEARCH ACHIEVEMENTS AND CONTRIBUTIONS

Prizes, honours and awards

- (2019) The security flaws I discovered in the Swiss online voting system for national elections received widespread international media attention and resulted in the system being withdrawn from use; the discovery of the flaws was covered by many leading news outlets. This work was subsequently published as "How not to prove your election outcome" at IEEE Symposium on Security and Privacy.
- (2019) SwissVote Penetration Test. Prize for finding critical error (5,000 Swiss Francs).
- (2016) My paper "VOTOR: conceptually simple remote voting against tiny tyrants" won best paper at the Australasian Information Security Conference (AISC) 2016
- (2016) Travel Awards, Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT) 2016
- (2014) Awarded Postgraduate Research Award scholarship and Higher Degree Research scholarship, Queensland University of Technology, Australia.

Research support income

Since 2017, I have received the following funding:

- Chief Investigator. 2018.1-2018.12, Polyas GmbH (Internal), 'Machine checked e-voting implementations', 25,000 AUD (in kind)
- Chief Investigator. 2017.7-2017.12, Polyas GmbH (Internal), 'E-voting on the blockchain', 10,000 AUD (in kind)

The grants at Polyas were keenly sought after and highly competitive. The application process was very direct and involved convincing senior management of the business value of the research.

Research supervision, mentoring and advice

I have been extensively involved in providing advice to various governments and companies on cybersecurity issues. This involvement has continued through my PhD, time at Polyas GmbH and at NTNU. I primarily advise on the security of cryptography in deployed systems and protocols. This often involves examining source code for deployed systems in order to check for vulnerabilities. I am also involved in communicating the capabilities and limitations of cryptography and advising on the veracity of security claims. This later point is crucial since many government organisations are ill equipped to judge the assertions being made by the vendors looking to win tenders.

I have been actively involved in mentoring research students internationally on topics related to my expertise. Starting during my PhD at QUT, I was involved in teaching a subject called "Understanding Research" for several semesters. Collectively during these semesters, I helped over two hundred Master's students to develop and articulate a research plan. This experience of teaching research as it applies across multiple disciplines was highly formative.

I have been involved in the co-supervision of several students at NTNU and the University of Luxembourg. This has largely consisted of proposing a research direction for a project suitable for inclusion as a chapter in their thesis and then guiding the student through understanding the area and then completing the research. At ANU I have been involved in the co-supervision of a PhD student and several summer scholars. The PhD student, Mukesh Tiwari, has had a paper accepted at ACM Computer and Communication Security (CCS) 2019 based on the work I supervised. One of the summer scholars, Bhavesh Sharma, has had a paper accepted at IEEE Security and Privacy (S&P) 2021, based on the work I supervised.

Invited keynote, speaker addresses and interviews

- Oral presentation, Verified Verifiers for Verifying Election, Cyber Defence Next Generation Technology & Science Conference, 2020
- Poster presentation, Verifiable Homomorphic Tallying for Schulze Vote Counting Scheme, Cyber Defence Next Generation Technology & Science Conference, 2020
- Invited presentation, IT University of Copenhagen, 2020
- Invited presentation, University of Luxembourg, 2020
- Invited speaker, ANU Logic Summer School, 2019
- Invited presentation, Java Users Group Hessen, 2018
- Australian National TV Interview on E-Voting (Channel 7), 2016

Commercial outcomes such as patents, IP licences and resulting benefits

My research has had a significant impact on commercial vendors who have updated their systems based on the vulnerabilities disclosed. This includes the internationally famous Australian-produced cryptography library BouncyCastle which acknowledged a flaw I found in their popular elliptic curve implementation. As well as the verifiable mixnet Verificatum—which is used in several national elections around the world—which acknowledged a flaw in their random element generation. For other examples see Table 1 below.

My research in scalable blockchain technologies (See [8] in Ten Career-Best Research Outputs) resulted in the founding of the company Graphchain, spun out by the Norwegian University of Technology, Technology Transfer Network.

Identifiable benefits outside of academia

The findings of my research undertaken in electronic voting has resulted in changes to electronic voting systems in Australia, Switzerland, and various non-government systems. The cryptography library BouncyCastle, which is used world-wide, was updated based on findings I made.

Other professional activities

Reviewer roles: I have been a reviewer for many conferences and journals such as the Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), and The Cryptographer's Track at the RSA Conference (CT-RSA). I have been a member of the program committee for The International Conference for Electronic Voting since 2018 and I am a program co-chair for the 6th and 7th Workshops on Advances in Secure Electronic Voting.

Professional memberships: I am a member of The International Association for Cryptologic Research (IACR) and an Associate Fellow of the Higher Education Academy (UK).

Community Engagement: I regularly engage with vendors, policy makers and the public on areas relating to my research expertise. I am regularly involved in consultation and the auditing of deployed systems. I also communicate more widely through seminars and media interviews.

Describe how the DECRA candidate's research has led to a significant change or advance of knowledge in their field, and outline how their achievements will contribute to this application.

Contribution to knowledge in electronic voting. My research has been impactful in electronic voting. In addition to the disclosures already mentioned, which led the Swiss Government to withdraw their e-voting system for national elections, I am acknowledged on a number of leading systems for my contributions to their security. The rapid progress of e-voting systems has resulted in an abundance of inadequate solutions in use and a critical shortage of people with the adequate skills to scrutinise the systems. By scrutinising these systems, I have in many cases been able to find critical issues which would have jeopardised either the privacy of the votes or the integrity of the election.

I am also leading the research which is combining formal methods (techniques for the formal specification, development and verification of software) and cryptography to extend security guarantees to the code level; the systems being deployed involve large amount of code which needs to have certain properties for the system to be secure. Manually checking that the code has these properties is infeasible, hence the motivation to use formal methods to achieve guarantees. I have contributed to the theory by proposing new schemes which protect privacy against an adversary with access to a large quantum computer.

My experience in both analysing and securing deployed schemes demonstrates my technical capabilities as well as my ability to constructively engage with government and industry partners. Both the technical capabilities and the collaborative skills will be essential to the success of the research proposed in this application.

- Contributions to practice: My contribution comes both in analysis of existing systems and development of new techniques. I am an acknowledged expert in the analysis of deployed schemes. The following systems have accepted bug reports I have submitted (or been involved in the disclosure of):

Table 1: Security Disclosures in Voting

System	Vulnerability Disclosed
The sVote system in Switzerland (See [1] in Ten Career-Best Research Outputs)	A vulnerability in the processing of ballots which allowed manipulation of outcome without detection by the verification procedure.
The election systems used in the Australian Capital Territory elections	The ballots were posted publicly in the order they were received. This allows a person who knows when you voted relative to them to learn (at least partially) your vote
The iVote system used in the Australian states of New South Wales and Western Australia	Flaws in the implementation of encryption. The system claimed to perform certain security checks which were not implemented.
The Zeus system in Greece	A vulnerability in the processing of ballots which allowed manipulation of outcome without detection by the verification procedure.
The CHVote system in Switzerland	A flaw in the specification of the system which would have allowed manipulation of votes.

The STARVote system in Travis County (Austin) Texas (See [2] in Fully Refereed Conference Rankings)	A flaw in the system which allowed the privacy of ballots to be compromised if one of the trustees was corrupted.

However, while it is possible to find bugs in most systems, it is much harder to check that there are no bugs. This leads into my other contribution to practice, that of formally proving implementations secure. The systems currently impacted by this line of work include:

- The Helios voting system used by the International Association for Cryptographic Research (See [2] in Ten Career-Best Research Outputs)
- The ElectionGuard system by Microsoft used in US elections (See [4] in Fully Refereed Conference Rankings)
- The Verificatum mix net used in numerous national elections (See [3] in Ten Career-Best Research Outputs)
- The CHVote system from Switzerland (See [3] in Ten Career-Best Research Outputs)

This impressive track record directly corresponds to Aim 3 of the research proposed in this application.

- Contributions to theory: I have contributed to theory on a number of issues within e-voting. The main theme has been about how to build practical systems which provide very strong privacy guarantees. (See [10] in Ten Career-Best Research Outputs and [1,3,5,6,8,10] in Fully Refereed Conference Rankings)

Contribution to knowledge in cryptography. My contributions to cryptography are primarily in the areas of ring signatures, mix nets, and secure key escrow. My work on ring signatures provided much tighter proofs for widely deployed schemes, resulting in much stronger security guarantees in practice. In addition, I was the first to propose an efficient linkable ring signature with forward security (See [6,7] in Ten Career-Best Research Outputs). I am one of the leading experts on both the theoretical and practical security of mix nets, which are a crucial building block in numerous privacy-preserving technologies (See [2,3,4,5] in Ten Career-Best Research Outputs and [2,3] in Fully Refereed Conference Rankings). I have been active in the development of alternative cryptographic constructions which are secure against quantum computers. My understanding of cryptography is necessary to analysis and improve existing cryptographic technique as required by Aims 1 and 2 of this proposed research.

Contribution to knowledge in the intersection of formal methods and cryptography. I have been instrumental in bringing the capabilities of formal methods to bear on formally proving e-voting implementations secure, as already noted. However, I have also contributed more widely to formal methods and cryptography by introducing a new paradigm which avoids reasoning about probabilities while still achieving equivalent security guarantees; this significantly eases the difficulty involved in constructing proofs. This paradigm is used in all my work in the area (See [2,3] in Ten Career-Best Research Outputs and [3,4] in Fully Refereed Conference Rankings). In addition, I have used formal methods to derive security guarantees about the theoretical design of systems (See [9] in Ten Career-Best Research Outputs).

Contribution to knowledge about key escrow. Allowing law enforcement access to data in a regulated way without compromising privacy more broadly is difficult. I have contributed several techniques which allow regulated access to data while preserving privacy more broadly (See [9] in Fully Refereed Conference Rankings).

Contribution to knowledge in blockchain. My research was the first to examine a new approach to scalability using directed acyclic graphs (See [8] in Ten Career-Best Research Outputs and [7] in Fully Refereed Conference Rankings). This approach eases the effect of network delay which prevents traditional approaches from increasing throughput without affecting security. This work saw significant attention and was ultimately spun out of the Norwegian University of Technology, Technology Transfer Network as the startup GraphChain.

Contribution to this application

My outstanding track record in the analysis of systems and in proving systems secure aligns directly with the research proposed in this DECRA application. My expertise combines a rare combination of mathematical rigor and real-world impact. I will draw both on my experience and network of collaborators to successfully deliver the proposed research.

F18. Research Opportunity and Performance Evidence (ROPE) - Research Outputs Context

(Research context: Provide clear information that explains the relative importance of different research outputs and expectations in the DECRA candidate's discipline/s. The information should help assessors understand the context of the DECRA candidate's research achievements but not repeat information already provided in this application. It is helpful to include the importance/esteem of specific journals in their field; specific indicators of recognition within their field such as first authorship/citations, or significance of non-traditional research outputs. (Up to 3,750 characters, approximately 500 words))

My discipline differs from many others in that conferences, rather than journals, are the most important publication venues. The most esteemed conferences in my field are IEEE Security and Privacy, ACM Computer and Communication Security and USENIX Security. The next tier includes the European Symposium on Research in Computer Security, IEEE Computer Security Foundations, and the International Conference on Applied Cryptography and Network Security, among others. The field is divided between cryptography, which tends to keep an alphabetic ordering of authors, and wider information security, which tends to list in order of contribution. Most of my publications are in the latter group.

The field highly values research which has direct impact on the security of deployed systems. For instance, analysis of deployed systems and subsequent reporting of vulnerabilities is highly thought of; this analysis often turns up results which are not theoretically interesting (the mistakes are obvious once their presence is realised) and hence much of this research is not published.

F19. Research Opportunity and Performance Evidence (ROPE) – Research Outputs Listing including Ten Career-Best Research Outputs

(Provide a list of research outputs relevant to this application categorised under the following headings: Ten career-best research outputs; Authored books; Edited books; Book chapters; Refereed Journal articles; Fully refereed conference proceedings; Additional research outputs (including non-traditional research outputs). CVs and theses should not be included in this list. The DECRA candidate's ten career-best research outputs should not be repeated under subsequent headings. (Up to 100 research outputs)
Do not include or refer to pre-prints in your application.)
Research Outputs Listing

Generated research output document follows on the next page

Ten Career-Best Research Outputs

[1] * Thomas Haines, Sarah Jamie Lewis, Olivier Pereira, Vanessa Teague 2020, 'How not to prove your election outcome', *IEEE Symposium on Security and Privacy*, pp. 644–660 (Fully Refereed Conference Proceeding)

[2] * Thomas Haines, Rajeev Goré, Mukesh Tiwari 2019, 'Verified Verifiers for Verifying Elections', *ACM Conference on Computer and Communications Security*, pp. 685–702 (Fully Refereed Conference Proceeding)

[3] * Haines, Thomas, Goré, Rajeev & Sharma, Bhavesh 2021, 'Did you mix me? Formally Verifying Verifiable Mix Nets in Electronic Voting', *IEEE Symposium on Security and Privacy* (Fully Refereed Conference Proceeding)

[4] Thomas Haines, Johannes Müller 2020, 'SoK: Techniques for Verifiable Mix Nets', *CSF*, pp. 49–64 (Fully Refereed Conference Proceeding)

[5] Xavier Boyen, Thomas Haines, Johannes Müller 2020, 'A Verifiable and Practical Lattice-Based Decryption Mix Net with External Auditing', *ESORICS (2)*, vol. 12309, pp. 336–356 (Fully Refereed Conference Proceeding)

[6] Xavier Boyen, Thomas Haines 2018, 'Forward-Secure Linkable Ring Signatures', *ACISP*, vol. 10946, pp. 245–264 (Fully Refereed Conference Proceeding)

[7] Xavier Boyen, Thomas Haines 2018, 'Forward-Secure Linkable Ring Signatures from Bilinear Maps', *Cryptogr.*, vol. 2, no. 4, pp. 35 (Refereed Journal Article)

[8] Xavier Boyen, Christopher Carr, Thomas Haines 2016, 'Blockchain-Free Cryptocurrencies. A Rational Framework for Truly Decentralised Fast Transactions', *IACR Cryptol. ePrint Arch.*, vol. 2016, pp. 871 (Additional Research Output)

[9] * Thomas Haines, Dirk Pattinson, Mukesh Tiwari 2019, 'Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme', *VSTTE*, vol. 12031, pp. 36–53 (Fully Refereed Conference Proceeding)

[10] Colin Boyd, Kristian Gjøsteen, Clémentine Gritti, Thomas Haines 2019, 'A Blind Coupon Mechanism Enabling Veto Voting over Unreliable Networks', *INDOCRYPT*, vol. 11898, pp. 250–270 (Fully Refereed Conference Proceeding)

Fully Refereed Conference Proceedings

[1] Colin Boyd, Thomas Haines, Peter B. Rønne 2020, 'Vote Selling Resistant Voting', *Financial Cryptography Workshops*, vol. 12063, pp. 345–359

[2] Thomas Haines, Olivier Pereira, Peter B. Rønne 2020, 'Short Paper: An Update on Marked Mix-Nets: An Attack, a Fix and PQ Possibilities', *Financial Cryptography Workshops*, vol. 12063, pp. 360–368

[3] Gjøsteen, Kristian, Haines, Thomas & Solberg, Morten 2020, 'Efficient mixing of arbitrary ballots with everlasting privacy: How to verifiably mix the PPATC scheme', *Nordsec*

[4] Haines, Thomas, Goré, Rajeev & Stodart, Jack 2020, 'Machine-checking the universal verifiability of ElectionGuard', *Nordsec*

[5] Ehsan Estaji, Thomas Haines, Kristian Gjøsteen, Peter B. Rønne, Peter Y. A. Ryan et al. 2020, 'Revisiting Practical and Usable Coercion-Resistant Remote E-Voting', *E-VOTE-ID*, vol. 12455, pp. 50–66

[6] Thomas Haines 2019, 'Cronus: Everlasting Privacy with Audit and Cast', *NordSec*, vol. 11875, pp. 53–68

[7] Thomas Haines, Clémentine Gritti 2019, 'Improvements in Everlasting Privacy: Efficient and Secure Zero Knowledge Proofs', *E-VOTE-ID*, vol. 11759, pp. 116–133

[8] Xavier Boyen, Christopher Carr, Thomas Haines 2018, 'Graphchain: a Blockchain-Free Scalable Decentralised Ledger', *BCC@AsiaCCS*, pp. 21–33

[9] Thomas Haines, Xavier Boyen 2016, 'VOTOR: conceptually simple remote voting against tiny tyrants', *ACSW*, pp. 32

[10] Colin Boyd, Xavier Boyen, Christopher Carr, Thomas Haines 2016, 'Key Recovery: Inert and Public', *Mycrypt*, vol. 10311, pp. 111–126

[11] Thomas Haines, Xavier Boyen 2016, 'Truly Multi-authority 'Prêt-à-Voter'', *E-VOTE-ID*, vol. 10141, pp. 56–72

Additional Research Outputs

[1] Thomas Haines 2019, 'A Description and Proof of a Generalised and Optimised Variant of Wikström's Mixnet', *CoRR*, abs/1901.08371

[2] Christopher Carr, Colin Boyd, Xavier Boyen, Thomas Haines 2017, 'Bitcoin Unchained', *ERCIM News*, vol. 2017, no. 110

[3] Mukesh Tiwari, Dirk Pattinson, Thomas Haines 2020, 'Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme', Cyber Defence Next Generation Technology & Science Conference (CDNG2020)

[4] Thomas Haines, Rajeev Gore, Mukesh Tiwari 2020, 'Verified Verifiers for Verifying Election', Cyber Defence Next Generation Technology & Science Conference (CDNG2020)

Certification

Certification by the Deputy/Pro Vice-Chancellor (Research) or their delegate or equivalent in the Administering Organisation

I certify that—

- I have read, understood and complied with the *Grant Guidelines for the Discovery Program (2019 edition)*, (grant guidelines) and, to the best of my knowledge all details provided in this application form and in any supporting documentation are true and complete in accordance with the grant guidelines.
- Proper enquiries have been made and I am satisfied that the Discovery Early Career Researcher Award (DECRA) candidate listed in this application meets the requirements specified in the grant guidelines, including having been awarded a PhD on or after 1 March 2016. Where the DECRA candidate has allowable career interruptions, sufficient evidence has been provided to the Administering Organisation and based on this evidence, I certify that the candidate has an award of PhD date together with an allowable period of career interruption (as listed in the grant guidelines) that would be commensurate with an award of PhD date on or after 1 March 2016.
- Where the DECRA candidate holds a research higher degree, that is not a PhD, sufficient evidence has been provided to the Administering Organisation and based on this evidence, I certify that the candidate's qualification meets the level 10 criteria of the *Australian Qualifications Framework Second Edition*.
- I certify that where a DECRA candidate has more than one PhD, the earliest PhD has been selected and meets the eligibility requirements, including having been awarded a PhD on or after 1 March 2016.
- Upon request from the ARC, this organisation will provide evidence to support a career interruption justification in relation to the PhD award date.
- The ARC reserves the right to audit any evidence on which an application is based.
- I will notify the ARC if there are changes to the DECRA candidate after the submission of this application.
- The listed participants are responsible for the authorship and intellectual content of this application, and has appropriately cited sources and acknowledged significant contributions to this application.
- To the best of my knowledge, all personal material interests and Conflicts of Interest relating to parties involved in or associated with this application have been disclosed to the Administering Organisation, and, if the application is successful, I agree to manage all Conflicts of Interest relating to this application in accordance with the *Australian Code for the Responsible Conduct of Research* (2018), the *ARC Conflict of Interest and Confidentiality Policy* located on the ARC website and any relevant successor documents.
- I have obtained the agreement, attested to by written evidence, of all the relevant persons and organisations necessary to allow the project to proceed. This written evidence has been retained and will be provided to the ARC if requested.
- This application complies with the eligible research requirements set out in the *ARC Medical Research Policy*, located on the ARC website.
- This application does not request funding for the same research activities, infrastructure or project previously funded or currently being funded through any other Commonwealth funding.
- If this application is successful, I am prepared to have the project carried out as set out in this application and agree to abide by the terms and conditions of the grant guidelines and the relevant Commonwealth grant agreement.
- The project can be accommodated within the general facilities of this organisation and if applicable, within the facilities of other relevant organisations specified in this application and sufficient working and office space is available for any proposed additional staff.
- All funds for this project will only be spent for the purpose for which they are provided.
- The project will not be permitted to commence until there is an ethics plan in place to ensure that the appropriate clearances or other statutory requirements will be met before the part/s of the project that require those clearances commence.
- I consent, on behalf of all the parties, to this application being referred to third parties, including to overseas parties, who will remain anonymous, for assessment purposes.

- I consent, on behalf of all the parties, to this application being provided to third parties for the purposes of assessment for potential other funding opportunities.
- I consent, on behalf of all the parties, to the ARC copying, modifying and otherwise dealing with information contained in this application for the purpose of conducting the funding round.
- To the best of my knowledge, the Privacy Notice appearing at the top of this form has been drawn to the attention of the DECRA candidate whose personal details have been provided in the Participant section of the application.