

Trustworthy voting systems

Case for support

Summary Governments all over the world are investing in electronic voting, but experiences in the USA and in the UK have shown that there are immense obstacles to be overcome before we can have secure and usable systems. The project aims to develop and implement robust voter-verifiable electronic voting systems that are usable in real large-scale elections. We will also conduct user trials, and we will develop and extend techniques for analysis and verification of voting systems. To achieve these aims, we will work with the UK Ministry of Justice, which is charged with modernising UK elections, as well as two commercial election systems providers, namely Election Reform Services and Opt2Vote. We are also partnered with influential US organisations and individuals.

1 Previous Research Track

1.1 Newcastle University

Professor Peter Ryan has over 20 years of experience in cryptography, information assurance and formal verification. He pioneered the application of process calculi to modelling and analysis of secure systems and is one of the developers, along with Steve Schneider and others, of the groundbreaking CSP and model-checking approach to the analysis of security protocols. He has published extensively on cryptography, cryptographic protocols, security policies, mathematical models of computer security and, most recently, high assurance voting systems. He is the creator of the Prêt à Voter verifiable voting scheme [7, 16]. Peter Ryan sits on or has sat on the programme committees of several prestigious security conferences, notably: IEEE Security and Privacy, IEEE Computer Security Foundations Workshop, the European Symposium on Research in Computer Security (ESORICS), Workshop on Issues in Security (WITS). He was chair of WITS'04 and co-chair of ESORICS'04, co-chair of Frontiers of Electronic Elections (FEE) 2005, chair Workshop on Trustworthy Elections (WOTE) 2007. Since 1999 he has been the chair of the ESORICS Steering Committee.

Newcastle University School of Computing Science has been active in research into techniques for designing dependable information systems for over 30 years. More recently it has established an international profile in security and information assurance. Currently the School hosts a major research group in dependability and the Centre for Software Reliability. Two long running significant research actions are: the Interdisciplinary Research Collaboration in Dependability (DIRC) and the EU FP7 DEPLOY NoE. Key areas of expertise encompass rigorous design, fault tolerance, system architectures, integration of components, diversity, dependability concepts, security, information assurance, cryptography, requirements, traceability, safety cases, modelling socio-technical systems, verification tools.

1.2 University of Birmingham

Dr Mark Ryan is a Reader in the School of Computer Science. He is known for his work on applications of logic in computer science, and for his successful book in that area [14], now in its second edition. His recent work is on analysis and verification of security protocols [20, 4, 3, 6], including electronic voting protocols [21, 18]. He has also worked on verification of access control systems [15]. Mark Ryan is on the programme committee of several international security and verification conferences, including 12th International Symposium on Temporal Representation and Reasoning (TIME 2005), International Colloquium on Theoretical Aspects of Computing (2005, 2006), Foundations of Computer Security (FCS'05, FCS-ARSPA'07), Computer Security Foundations (CSF 2006, 2008), ICALP track C (2007), SecCo (2007). He was co-chair of the International Conf. on Feature Interactions in 2005.

The University of Birmingham School of Computer Science is internationally leading in modelling and analysis of distributed systems, and of security systems in particular. The School is currently investing in computer security, having begun offering an M.Sc. in Computer Security (started October 2006) which has proved successful, and having appointed two new lecturers in that area in the last year. The School has a

thriving research environment following its rapid research-led expansion in the last ten years, having c.50 research students, c.30 research fellows, and 36 academic staff, six regular seminar series, and a research committee with a budget of £70,000 to support non-project research travel.

1.3 University of Surrey

Dr James Heather is a Lecturer in Computing at the University of Surrey. He is active in computer security, and in the last few years has been focused on issues relating to secure electronic voting. In particular, his recent work centred around adapting Prêt à Voter to deal securely with elections run by Single Transferable Vote [30]. Over the last twelve months, James led a team from Surrey and Newcastle in designing and building the first working implementation of Prêt à Voter, and entered the system for VoComp, an international voting systems competition held in Portland, Oregon, and funded by the National Science Foundation. The system attracted a good deal of interest from the judges and from the electoral officials at VoComp¹, and was awarded the ‘Best Design’ prize and second place overall. James has also published work on the formal analysis of security protocols [32], mainly using the process algebra CSP to prove correctness of the protocols [33], and on an embedding of CSP into the PVS theorem prover [31]. He is on the program committee of several major international conferences, including the IEEE Symposium on Computer Security Foundations (CSF), and the Workshop On Trustworthy Elections (WOTE).

Professor Steve Schneider joined the University of Surrey as Professor of Computing and Head of Department in 2004, having previously been at Royal Holloway. He has worked on formal methods and concurrency theory for 20 years, and on their applications to security since 1995 [36, 28, 32, 27]. He is a co-author of the Prêt à Voter secure electronic voting system [7], and has since been working on further development of the system design [16], and on other aspects of e-voting. He is head of the e-voting research group at Surrey, which led the implementation of Prêt à Voter that won ‘Best Design’ and came second overall at the VoComp 2006 Universities Voting System Competition. He has written well-received books in the area of concurrency theory [22] and its application to security protocol modelling and analysis [17] (coauthored with Peter Ryan and others). He has served as programme

chair for the IEEE Computer Security Foundations Workshop 2001 and 2002, and general co-chair of Formal Aspects in Security and Trust (FAST) since 2004, as well as serving on numerous security and formal methods conference committees. He is a member of IFIP WG1.7 (Theoretical foundations of security analysis and design) and WG1.8 (concurrency theory).

The University of Surrey Department of Computing is in the 5* Faculty of Engineering and Physical Sciences. The Department currently comprises 16 full-time academics, and is growing as a result of strategic investment by the University, following a recent move to newly refurbished premises in 2006 at a cost of £750K. The Department is involved in a variety of externally funded projects, with support received from EPSRC, EU, NHS, and private industry, and provides a well-founded research environment. The University has a tradition of innovation and exploitation of research, with one of the most successful University spin-out companies in the UK, and will provide the ideal environment for exploiting the potential of this project.

2 Background

Electronic voting has the potential to provide more efficient elections with higher voter participation, better accuracy and lower costs, compared to current manual methods. A properly designed and engineered system could also offer much better security properties than current manual systems, such as vote-privacy even in the face of untrusted election authorities, and voter-verification, namely the ability of voters to check that their vote has been correctly counted in the declared outcome. Governments the world over have been trialling and deploying electronic voting systems, including in the USA, UK, Canada, Brazil, the Netherlands and Estonia.

Unfortunately, the potential benefits have turned out to be very hard to realise. There has been controversy surrounding the voting machines supplied by Diebold, a major USA supplier, ever since 2003 when the source code of the machines was leaked on the internet. A damning analysis produced by computer scientists at Johns Hopkins University [23] concluded that the Diebold system is far below even the most minimal security standards applicable in other contexts. They showed that voters without any insider privileges can cast unlimited votes without being detected by any mechanisms within the voting terminal software.

¹vocomp.org

In more recent developments in 2007, the Secretary of State for California commissioned “top to bottom” reviews of the four electronic voting systems certified for use in the state, namely, those supplied by Diebold, Sequoia, Hart Inter-Civic, and Elections Systems and Software. The reviews [8], published in August 2007, describe a catalogue of vulnerabilities, including the susceptibility of the machines to viruses that propagate from voting machine to voting machine and between voting machines and the election management system, and that could maliciously cause votes to be recorded incorrectly or miscounted. In response to these reports, the State of California decertified all four electronic voting machines on 3 August 2007. Other states have followed California’s lead. For example, Colorado decertified all their voting machines in December 2007, and Ohio in early 2008, leaving the situation quite uncertain for the presidential elections this year.

A similar situation, albeit less extreme, exists in the UK, where the May 2007 elections included five local authorities that piloted a range of e-voting solutions. The Electoral Commission report [25] found that implementation and security risk was “significant and unacceptable”, and has recommended that no further e-voting should take place until a sufficiently secure and transparent e-voting solution is available.

The causes of this disastrous situation are on several levels. Superficially, many of the problems reported in California’s ‘top to bottom’ review are fixable, such as their use of deprecated cryptography and poor programming practices. However, the report also describes ‘weaknesses-in-depth’ – architecturally unsound systems, in which even as known flaws are fixed, new ones are discovered. These systems can only be made secure by complete re-engineering. More fundamentally, the USA and the UK reports both raise the question of trustworthiness: a system as fundamental to a core principle of our civilisation, namely democracy, must be able to provide exceptionally high levels of assurance and auditability in order to be accepted.

Voter verification A key principle for modern trustworthy elections is the idea that voters should be able after the election to check that their vote was correctly counted; and that any observer, whether a voter or not, should be able to verify that the declared outcome reflects the votes cast. This voter verification principle aims to remove the reliance on having to trust the equipment suppliers and programmers; voting systems should produce auditable results, so

that all stakeholders can obtain proof that the declared outcome reflects the intention of the voters. End-to-end verifiability of this sort is the only way to restore public confidence and provide a long-term solution to the problems being faced in the USA and elsewhere.

Producing such systems is immensely challenging, however. Understood naively, the requirement of voter verifiability appears to be in conflict with that of ballot secrecy. It is possible to achieve both properties together, but doing so and obtaining a usable system which is understandable by all voters and maximises convenience and accessibility appears to be very difficult.

Early work in electronic voting has produced a plethora of cryptography-based voting systems [1, 13, 2, 5, 24] that take various trade-off positions by satisfying certain subsets of the functional requirements. These systems have helped immensely to clarify the desired properties and understand the trade-offs. However, many people believe that the fact that they require client-side cryptography makes them impractical for use on a national scale. Therefore, interest has grown in schemes that don’t involve client-side cryptography.

Currently, the leading proposals that offer end-to-end verifiability without requiring client-side cryptography include Prêt à Voter [7, 16], designed by two of the current applicants; PunchScan [12]; and VoteHere [26]. These are excellent starting points for this research project, but none of them is yet mature enough to be used in a mission-critical, large-scale setting. The requirements of voting systems need to be identified and properly defined, and they need to be analysed and refined according to those requirements. They need to be extended with recovery strategies for dealing with disputes or failures. The possibility of including votes from non-standard sources in a disciplined and secure way needs to be added. Trials need to be carried out.

3 Programme of work

As mentioned, Prêt à Voter, PunchScan and VoteHere represent excellent starting points, but there are still many conceptual and practical issues to be resolved. This includes formalising the requirements, such as voter verifiability, coercion-resistance, and fairness, and developing techniques for proving that system designs satisfy those requirements. Designing a voting system is not a purely technical problem, however: a mathematically perfect system that is not usable and does not command voter confidence is not a

viable solution. The human/computer interface and other sociological factors are paramount in a voting system, because we cannot rely on users gaining familiarity with it by everyday use. Robust implementations and medium-scale user trials are also essential, in order to test and refine the system. Therefore, our aims in this project are:

3.1 Aims and objectives

1. Develop and extend the design of robust voter-verifiable electronic voting systems.
2. Implement a system and conduct a user-trial.
3. Develop and extend techniques for analysis and verification of voting systems.

3.2 Work plan

The work packages are divided into three streams, corresponding to the three aims of the project. Each stream is led by one of the three sites (see diagram), and each work package is allocated a number of person-months from each site (again, see diagram).

3.2.1 Design of robust electronic voting systems

WP1.1 Identifying and defining the requirements There are many requirements set out for electronic voting systems, such as vote privacy, eligibility enforcement, coercion-resistance, and voter verifiability. These are not binary yes/no properties; for example, ThreeBallot [35] doesn't reveal how you voted but could reveal statistical information about how a group voted. Therefore, we will define properties in a variety of strengths; e.g., privacy can be defined probabilistically [21], or in varying strengths probabilistically [11]. Depending on exactly how the requirements are specified, they may be in conflict with each other, and there are trade-offs to be resolved. Additionally, there are non-functional requirements, such as usability, robustness, recoverability, inclusivity, voter acceptability, which again have to be balanced with other requirements when they are in conflict. We will obtain a taxonomy of requirements and their definitions.

WP1.2 Evaluating and further developing existing systems This work package will evaluate existing systems in the light of the taxonomy produced by WP1.1, and will establish precisely what areas need to be addressed. We will investigate how to resolve the problems that existing

systems have, and improve any areas of concern that can be improved. We will also identify weaknesses that are inherent to the design of existing systems and that therefore cannot be resolved.

We will also improve the functionality of existing systems by establishing what tallying strategies can in principle be handled, and how such strategies can be incorporated into the systems. Different tallying methodologies sometimes need radically different approaches to handling decryption of the votes in order to maintain provable correctness while minimising unnecessary information flow; for instance, STV is best handled by lazy decryption [30], whereas Condorcet is best dealt with by splitting the vote into multiple ordered pairs at a very early stage so that the different pairwise rankings within the same vote can be decoupled.

WP1.3 Handling multiple voting methods

One of the attractions of electronic voting to election officials is the possibility of increasing election turnout by including several voting channels, such as internet voting, postal voting, and possibly voting by mobile phone or TV. Additionally, one can consider channels designed to assist voters with special needs, e.g., disabled voters, technically challenged voters, and low-motivation voters. These extra channels introduce additional difficulties for voter verifiability, and additional threats to other security properties.

We will analyse these methods and corresponding threats, and establish whether it is possible to incorporate these methods into the system without compromising security. In some cases, it might be that there is an unavoidable trade-off between accessibility and security. For instance, it is difficult to see how coercion resistance can be maintained if votes can be cast in an unsupervised environment where a coercer might insist on being physically present.

We will introduce hooks into our basic systems to allow such supplementary channels, and define parameters and usage boundaries in such a way that the security properties of the core system are maintained, and the security compromises for non-standard voting methods are properly understood.

WP1.4 Designing recovery strategies Prêt à Voter has well-defined mechanisms for the detection of errors or corruption. But recovery mechanisms and strategies have not been explored. The purpose of the WP is to define the error modes and explore effective recovery strategies for various patterns detected of errors/corruption.

It is essential to define appropriate responses to errors and define how they are handled. In particular, clear procedures must be defined as to what action voters should take if they detect problems, and how they should report these problems, and how they will be resolved. Prêt à Voter allows the possibility of revoking ballot anonymity, with the cooperation of a threshold set of tellers. We need to define circumstances under which it might be necessary to revoke the anonymity of certain ballots in the event of fraud, along with checks and balances to prevent abuse of such a capability.

3.2.2 Development of techniques for analysis and verification of voting systems

WP2.1 Threat models A bewildering array of threats to voting systems has been identified [29, 34], since voting systems operate in a highly hostile environment: voters may try to circumvent the system, the system may try to cheat voters, coercers may try to influence voters, and officials may try to manipulate the outcome. In conjunction with WP1.1, we will identify, classify and prioritise the threats from different sources, e.g. voters and other external parties, system administrators, system designers and implementers, equipment providers. These results will be used to inform the implementation and the verification threads.

WP2.2 Formalisation of systems and properties We will formalise the properties identified in WP1.1 and the systems of WP1.2, in appropriate frameworks. Exactly which frameworks we will use has not yet been decided. Process calculi such as the applied pi calculus are obvious candidates because of promising results so far [18, 21], but they are not adequate for systems with inherent probabilistic choice, such as Prêt à Voter where the mixnets are probabilistic. It may be possible to find appropriate abstractions of the probabilistic elements, or it may be necessary to use calculi that handle probabilities directly, such as [10, 9]. The calculi will allow us to express reachability-type properties (such as vote secrecy, eligibility enforcement, fairness) as well as equivalence-type properties (vote privacy, coercion resistance). Formalising the property of voter verification is likely to be a particular challenge because of its complex interaction with privacy, and if successful, it will be a significant contribution of the project.

WP2.3 Development of verification algorithms and methods We will verify the prop-

erties formalised in WP2.2 against the systems considered there. This will involve developing new verification algorithms and methods. We can build on existing work developing symbolic methods for the applied pi calculus [19], which is designed to lead to better algorithms for determining reachability and equivalence properties. We also aim to verify the properties of the recovery strategies defined in WP1.4, and propose improvements.

3.2.3 Implementation and user-trial of a voting system

WP3.1 Usability trial 1 and its consequences This workpackage will involve conducting a usability study of the existing Prêt à Voter prototype. A company specialising in usability analysis (quite likely *Flow Interactive*, a London-based user-experience research consultancy) will be engaged to recruit ten participants for the study; the participants will be asked to perform a specific task, and then be given a chance to talk about the experience during an hour-long one-to-one interview with a consultant. Some users will be asked to vote for a particular candidate; some will be asked to audit a ballot form. They will then be given the opportunity to check their votes or audit receipts on the web site.

Conducting this trial will enable us to discover what inadequacies there are with the prototype system: for example, are the participants able to understand the feedback that the system provides after they have voted?

The trial will also give us insight into participants' trust in the system, and whether they believe that the system really does keep their vote secret, and really does protect against modification of the cast votes. We will also be looking to gauge participants' trust in cryptographically secured voting in general.

Results of this initial study will be useful for identifying and defining the requirements of a trustworthy voting system in WP1.1, and will also inform the analysis of threat models in WP2.1. Ultimately, it will inform development of the full system in WP3.2.

WP3.2 Implementation core We will implement the system designed in WP1.2, and construct a full, working system, using results from WP2.1. Throughout this workpackage, we will be guided by information gained from Usability trial 1 in WP3.1.

The implementation we provide will be made freely available, along with the associated source code, to enable any third parties who wish to do

so to analyse the system and to extend it where appropriate. The aim throughout will be to create portable code, so that it can be easily compiled and run on a wide variety of systems.

The system will be decoupled into two distinct parts: a back end, which receives votes and processes them appropriately; and a front end, which deals with interpreting the voter's input and transmitting the encrypted vote to the back end. This decoupling will make it possible to add further front ends in WP3.4 to deal with other voting methods.

WP3.3 Usability trial 2 and its consequences When the full system has been built, we will run a similar study to that of WP3.1, to elicit detailed feedback on usability of the system. Again, we will ask participants to perform specific tasks with the system, and then afterwards to discuss the voting experience. The usability company from WP3.1 will once more be engaged to recruit participants and organise and conduct the interviews.

Usability trial 2 will involve testing two variants of the new system, to discover which is more readily acceptable to voters. A key difference between the two variants will be in the handling of *auditing*: in one variant, auditing will be performed by voters, as in the prototype system; in the other variant, independent auditors will be called on to perform this task, and voters need not do any auditing of their own.

Again, as with Usability trial 1, we will require feedback on participants' suggestions concerning what parts of the system are confusing or difficult to use, or could be improved, as well as participants' beliefs about the claimed properties of the system, and about cryptographically secured voting in general.

WP3.4 Further implementation The system built in WP3.2 will now be extended and refined. We will make changes in the light of the feedback from Usability trial 2 (WP3.3). We will also now have results from the verification workpackage (WP2.3), which we will use to inform and implement improvements.

We will build further front end modules to enable us to support the other voting methods identified and considered in WP1.3; this will make the system accessible to those who are unable to vote using traditional methods. The work on recovery strategies (WP1.4) will also be incorporated into our improved implementation, so that the system will be able to react to and recover from malfunction or external attack.

WP3.5 Full trial and evaluation When the implementation has been completed and thoroughly tested, we will run a trial by holding an election using the system. This is likely to be a Student Union government election. At the end of the election, we will make public all of the necessary information for voters and candidates to be able to verify the results and run audits on the machines involved in vote collection and tallying.

Testing resolving of disputes will involve instructing several 'disruptive' voters, unknown to the poll workers, who will be given various tasks to complete, such as presenting a fake voting receipt and attempting to use it to challenge the integrity of the system. Recoverability from failure or compromise will be tested by deliberately introducing failure-prone or rogue components into the system.

We will draw on the expertise of colleagues in Public Policy and Sociology at Surrey and Newcastle to assist in designing a questionnaire for voters, poll workers, mystery shoppers and candidates to complete. The results of this questionnaire, along with the experience of running the full trial, will be useful for evaluating the success of the project.

4 Management

The project will be led (and managed locally at each university) by Peter Ryan, Mark Ryan, and James Heather. The three threads of design, verification and implementation will be led by the universities of Newcastle, Birmingham and Surrey respectively. Most of the WPs are a collaborative effort of all three universities, as detailed in the Plan. We will hold two full project meetings each year (Spring and Autumn), which all project members are required to attend. The Autumn meeting will be accompanied by a Workshop, consisting of paper presentations by members of the project. In years 1 and 3 this will be one-day, while in years 2 and 4 it will be a two-day event including presentations from external researchers. This may be combined with FEE/WOTE, the main workshops in voting, depending on negotiations with their steering committees.

We also plan to have an advisory board consisting of the six external partners (detailed below) and the project investigators. Its brief is to advise us on scientific and technical issues that arise in the running of the project. It will meet two or three times during the course of the project.

4.1 Partners and collaborations

Recognising the importance of ensuring relevance to and take-up by the beneficiaries of our research, we will collaborate with the following organisations and individuals (see accompanying letters of support). We have selected five organisations to work with us, three from the UK and two from the USA. Each one of them will be a member of our Advisory Board which will advise us and overview the running of the project.

Ministry of Justice The Electoral Policy Division in the UK Ministry of Justice is responsible for modernising the UK electoral processes. As indicated in their letter, they will provide the project with guidance on government policy and requirements. They will benefit from the design and verification outputs of our research.

Opt2vote Opt2vote is a UK company providing services and expertise in all areas of election management. They specialise in designing and delivering election solutions. Their products and services include both paper-based and electronic voting (including by internet and telephone). They have welcomed our research and have offered to look at their client needs at the time of our trials with a view to our running a trial with one of their clients.

Electoral Reform Services The Electoral Reform Society (founded 1884) is a lobby organisation that promotes fair elections in the UK and worldwide. It is concerned with all aspects of the election process. In 1988 it created a subsidiary company called Electoral Reform Services, which is now the world's leading independent supplier of election services. Its expertise is recognised by the UN and in UK Acts of Parliament. Each year it helps about 1000 different organisations hold elections, with voter populations ranging from 100 to one million. ERS will advise us about trials and, if possible at the time, they will help us run trials, as mentioned in their letter.

Professor Ron Rivest, MIT Rivest is a computer scientist of international standing and recipient of the ACM Turing Award (2002, joint with Adleman and Shamir). He is also a member of the Technical Guidelines Development Committee of the Election Assistance Commission (EAC) in the USA, an organisation charged by the US government with serving as a national resource for administering federal elections. As indicated in his letter, Rivest will join our Advisory Board which will offer guidance on US policy and requirements.

He will also help disseminate our verification and usability findings via the EAC.

CalTech/MIT Voting Technologies Project

Professor Mike Alvarez is an eminent Professor of Political Science at CalTech and co-director of the CalTech/MIT Voting Technologies Project (VTP). He has made major contributions to the science of voting and is the author of several books in the field, most recently *Election Fraud: Detecting and Deterring Electoral Manipulation*. His achievements in the field were recognised by his being included in the 2004 "Scientific American 50" list. He has indicated in the accompanying letter of support that he is happy to serve on the advisory board and is keen to foster collaboration between the VTP and this project.

National Institute of Standards and Technology (NIST)

Founded in 1901, NIST is a non-regulatory federal agency within the US Department of Commerce. NIST's mission is to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. NIST is keen to advise us and help disseminate our results.

5 Relevance to Beneficiaries

The project will develop secure, appropriate, and usable electronic voting systems. The beneficiaries we envisage are:

- Society at large;
- UK Government and UK election providers. We are partnered with the Ministry of Justice and with two commercial providers, but all other departments and organisations will also have access to all our outputs.
- Other researchers in computer security and in electronic voting world-wide.

5.1 Dissemination and exploitation

Our dissemination will be by all the standard routes appropriate to this kind of project.

- Papers in journals and conferences. These will include the specialist workshops in electronic voting, WOTE and FEE, as well as more general computer security fora such as *Journal of Computer Security*, ESORICS, CSF, IEEE Security and Privacy, ACM CCS. We are currently in discussion about founding a new journal in voting sciences.

- Via trials, held if appropriate in collaboration with Opt2Vote or Electoral Reform Services.
- Via our partners.
- Via project workshops (see Section 4)
- Naturally, we will maintain a project website with all relevant output, including all our source code which will be available under an appropriate open source licence.

References

- [1] A. Fujioka, T Okamoto, and K Ohta. A practical secret voting scheme for large scale elections. AUSCRYPT 1992, LNCS volume 718 of pages 244-251. Springer, 1992.
- [2] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In Proc. of Workshop on Privacy in the Electronic Society (WPES'05), ACM Press, 2005.
- [3] A. Mukhamedov and M. D. Ryan. Fair Multi-party Contract Signing using Private Contract Signatures. Information and Computation, in print 2008.
- [4] A. Mukhamedov and M. D. Ryan, On Anonymity with Identity Escrow. Proc. Third international Workshop on Formal Aspects in Security and Trust (FAST2005). LNCS 3866, pages 235-243.
- [5] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo. Providing receipt-freeness in mixnet-based voting protocols. In Proc. of Information Security and Cryptology (ICISC'03), LNCS volume 2971, pages 245-258. Springer, 2004.
- [6] B. Smyth, L. Chen, and M. D. Ryan, Direct Anonymous Attestation: ensuring privacy with corrupt administrators. F. Stajano et al. (eds.), Proceedings of the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks, pp. 218-231, LNCS 4572, Springer-Verlag 2007.
- [7] D. Chaum, P. Y. A Ryan and S. A. Schneider. A practical, voter-verifiable election scheme. ESORICS'05, LNCS volume 367, pages 118-139. Springer, 2005.
- [8] D. Wagner, D. Wallach, M. Blaze, M. Bishop, and others. Four documents reviewing the source code of the Diebold, Sequoia, and Hart InterCivic systems; and four documents describing the results of "Red Team" testing of those systems. Available at www.sos.ca.gov/elections/elections.vsr.htm.
- [9] K. Chatzikokolakis, C. Palamidessi. A Framework to Analyze Probabilistic Protocols and its Application to the Partial Secrets Exchange. Theoretical Computer Science, to appear.
- [10] K. Chatzikokolakis, C. Palamidessi. Making Random Choices Invisible to the Scheduler. Proc. CONCUR 2007.
- [11] K. Chatzikokolakis, C. Palamidessi. Probable Innocence Revisited.
- [12] K. Fisher, R. Carback, A. Sherman, Punchscan: Introduction and System Definition of a High-Integrity Election System. Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE), 2006.
- [13] M. Hirt and K. Sako. Efficient receipt-free voting based on homomorphic encryption. Eurocrypt'00, LNCS volume 1807, pages 539- 556. Springer, 2000.
- [14] M. Huth and M. D. Ryan, Logic in Computer Science: Modelling and Reasoning about Systems. Second Edition with major revisions and updates. Cambridge University Press, 2004. 427 pages.
- [15] N. Zhang, D. P. Guelev, and M. Ryan. Synthesising Verified Access Control Systems through Model Checking. Journal of Computer Security, 2007.
- [16] P. Y. A Ryan and S. A. Schneider. Prêt à Voter with re-encryption mixes. ESORICS, 2006.
- [17] Peter Y A Ryan, Steve Schneider, Michael Goldsmith, Gavin Lowe, Bill Roscoe, Modelling and analysis of security protocols, Addison-Wesley 2001.
- [18] S. Delaune, S. Kremer and M. Ryan. Coercion-resistance and Receipt-freeness in Electronic Voting. In 19th Computer Security Foundations Workshop (CSFW), IEEE Comp. Soc. Press, 2006.
- [19] S. Delaune, S. Kremer and M. Ryan. Symbolic bisimulation for the applied pi calculus. Submitted, 2007.
- [20] S. Kremer and M. D. Ryan. Analysing the vulnerability of protocols to produce known-pair and chosen-text attacks. Proceedings of the 2nd International Workshop on Security Issues in Coordination Models, Languages, and Systems (SecCo 2004), ENTCS 128(5), 87-104, 2004.
- [21] S. Kremer and M. D. Ryan. Analysis of an Electronic Voting Protocol in the Applied Pi Calculus. In Proceedings of the European Symposium on Programming (ESOP'05), LNCS 3444, pages 186-200. Springer Verlag, 2005.
- [22] Steve Schneider, Concurrent and real-time systems: the CSP approach, Wiley 1999.
- [23] T. Kohno, A. Stubblefield, A. D. Rubin, D. S. Wallach, Analysis of an Electronic Voting System. IEEE Symposium on Security and Privacy, Oakland, 2004.
- [24] T. Okamoto. Receipt-free electronic voting schemes for large scale elections. In Proc. 5th Int. Security Protocols Workshop, LNCS volume 1361, pages 25-35. Springer, 1997.
- [25] The Electoral Commission. Key Issues and Conclusions of the May 2007 Electoral Pilot Schemes.
- [26] Votehere documents, Accessed February 2008. <http://votehere.com/documents.php>.
- [27] R. Delicata and S. Schneider. A formal approach for reasoning about a class of Diffie-Hellman protocols. In *Formal Aspects of Security and Trust*, LNCS, 2005.
- [28] R. Delicata and S. Schneider. Temporal rank functions for forward secrecy. In *18th IEEE Computer Security Foundations Workshop*, 2005.
- [29] A. Gumbel. Steal this vote!, 2005. Nation Books.
- [30] J. Heather. Implementing STV securely in Prêt à Voter. In *Proceedings of the 20th IEEE Symposium on Computer Security Foundations*, 2007.
- [31] J. Heather and K. Wei. Where next for formal methods? In *Proceedings of the 14th International Workshop on Security Protocols*, Cambridge, UK, 2006.
- [32] J. A. Heather, G. Lowe, and S. A. Schneider. How to avoid type flaw attacks on security protocols. 2003.
- [33] J. A. Heather and S. A. Schneider. To Infinity And Beyond, or Avoiding the infinite in security protocol analysis. In *21st ACM Symposium on Applied Computing*, Dijon, France, Apr. 2006.
- [34] C. Karlof, N. Sastry, and D. Wagner. Cryptographic voting protocols: A systems perspective. In *USENIX Security Symposium*, number 3444, pages 186-200. Springer-Verlag, 2005.
- [35] R. L. Rivest and W. D. Smith. Three voting protocols: Threeballot, vav, and twin. In *EVT'07: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop*, Berkeley, CA, USA, 2007. USENIX Association.
- [36] S. Schneider. Verifying authentication protocols in CSP. *IEEE Transactions in Software Engineering*, 24(9), 1998.