Editorial

We are pleased to present a Special Issue on Formal Methods and Cryptography, based on papers presented at the 2011 CryptoForma workshop at Limerick, and other submitted papers on this theme.

In the 1990s, formal methods were successfully applied to security protocols, using e.g. CSP or Isabelle. Modern cryptography based security protocols can be analysed using such techniques, but they and their corresponding notions of security likely also contain probabilistic and complexity-theoretic aspects which require different abstractions and proof methods. CryptoForma (<http://www.cryptoforma.org.uk>), a Network of Excellence funded by the UK Engineering and Physical Sciences Research Council, brings together formal methods researchers and cryptologists, from academia and industry, aiming to find the right abstractions and methods for modelling, analysing, and verifying cryptographic protocols and primitives. The network was originally funded to run from 2009 to 2012, and received renewed funding to continue until 2015. Its activities include informal meetings (some 3 per year, typically attended by around 50 researchers from 10+ UK universities, industry, and other European countries), co-organisation of the FOSAD summer school (<http://www.sti.uniurb.it/events/fosad/>), and international workshops co-located with major conferences. The 2011 workshop was co-located with FM at Limerick. The call for papers for this associated special issue asked for research papers, e.g. following on from the workshop presentations. However, it also invited tutorials and surveys, to explain the problems in this research area and the current state of their solutions to the wider formal methods audience as represented in the Formal Aspects of Computing readership. The resulting issue does indeed contain papers in all those categories. All submissions were reviewed by experts from within and outside the CryptoForma network, with CryptoForma members Steve Schneider and Eerke Boiten as editors.

“Inductive study of confidentiality: for everyone” by Giampaolo Bella is a tutorial on the inductive method as developed by Paulson and others, using the Isabelle theorem prover. It explains how, assuming a basic set of Computer Science skills, one can successfully analyse protocols using Isabelle, focusing on confidentiality properties in two different threat models.

The other proven successful formal method for security already mentioned above, CSP, is the main analysis tool in two papers in this special issue. In “Cryptographic protocols with everyday objects” by James Heather, Steve Schneider and Vanessa Teague, protocols are modelled and analysed that use coins, dice, and other everyday objects to achieve typical security aims—instead of using computers. An important area where formal methods play an essential role in increasing public confidence is electronic voting. “Verifying anonymity in voting systems using CSP” by Murat Moran, James Heather and Steve Schneider considers the modelling of two voting systems in CSP, different notions of anonymity for such systems, and how these can be formalised and verified.

A common criticism of formal methods approaches to protocol verification is that they remain at a too high level of abstraction, analysing formal specifications which may be too far removed from actual implementations for the results to be fully relevant. However, good progress has been made in recent years with the verification of actual implementations in code of security protocols. “Formal verification of security protocol implementations: a survey” by Matteo Avalle, Alfredo Pironti and Riccardo Sisto presents and contrasts recent approaches in this area. One such approach is presented in “Safe abstractions of data encodings in formal security protocol models” by Alfredo Pironti and Riccardo Sisto, in this case with respect to data encoding. This aspect is generally abstracted away for tractability in protocol analysis, but it must be done in an appropriate way if a secure abstract protocol is to remain secure in implementation. The paper identifies sufficient conditions, which are straightforward to check, on implementations of encoding and decoding to ensure that they are appropriate in this way.

Morgan’s possibilistic “shadow semantics” was an important step forward in the application of formal methods to security, by including the preservation of secrecy in a notion of refinement. “Abstractions of non-interference security: probabilistic versus possibilistic” by T. S. Hoang, A. K. McIver, L. Meinicke, C. C. Morgan, A. Sloane and E. Susatyo continues this line of work by relating it to a probabilistic framework developed subsequently, and characterising which proofs and theorems in the possibilistic world can be promoted into the probabilistic context.

We are grateful to ‘Formal Aspects of Computing’ for allowing us to publish this collection of papers in the journal; to the participants and reviewers of the workshop, and to the reviewers involved in selecting the papers.

Eerke Boiten
Steve Schneider