ROYAL HOLLOWAY UNIVERSITY OF LONDON

Recent developments in cryptographic standards

Chris Mitchell
Head of Department

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Where are we?
- New types of encryption
- Multi-party computation
- Lightweight cryptography
- Post-quantum cryptography
- The future

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Where are we?
- New types of encryption
- Multi-party computation
- Lightweight cryptography
- Post-quantum cryptography
- The future

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Focus of talk

- There are many bodies worldwide developing crypto standards.
- Well-known examples include:
  - **NIST** in US (e.g. SHA hash function standards, AES block cipher, various modes of operation)
  - **ETSI** and **3GPP** algorithm standards for mobile;
  - **IETF** RFCs have included crypto algorithms.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

ISO/IEC JTC 1/SC 27

- The main focus of this talk is the set of crypto standards developed by Working Group 2 (WG 2) of SC 27.
- SC 27 is a large and very active international standards committee concerned with general purpose security and privacy standards.
- SC 27 has five working groups:
  - WG 1 focusses on the core 27000 series security management standards;
  - WG 2 is responsible for crypto standards;
  - WG 3 looks after security evaluation criteria;
  - WG 4 supplements the work of WG 1 on security management;
  - WG 5 is concerned with privacy and identity management.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

ISO/IEC JTC 1/SC 27 WG 2

- WG 2 has well over 30 years of history of developing crypto standards.
- Published standards include:
  - ISO/IEC 9797 (3 parts); on MACs;
  - ISO/IEC 9798 (6 parts) on authentication protocols;
  - ISO/IEC 10118 (4 parts) on hash functions;
  - ISO/IEC 11770 (7 parts) on key establishment protocols;
  - ISO/IEC 14888 (3 parts) on digital signatures;
  - ISO/IEC 18370 (2 parts) on blind signatures;
  - ISO/IEC 18033 (7 parts) on encryption.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Ongoing work

- Existing standards are regularly reviewed, and also often amended to include new techniques offering advantages over previously standardised schemes.
- In a few cases it has also been necessary to remove schemes no longer sufficiently secure (e.g. the OCB2 mode of operation and the Dual_EC_DRBG method for random bit generation).
- In this talk I will mainly focus on new standards.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Where are we?
- New types of encryption
- Multi-party computation
- Lightweight cryptography
- Post-quantum cryptography
- The future

ROYAL HOLLOWAY UNIVERSITY OF LONDON

ISO/IEC 18033

- This multipart encryption standard currently has 7 parts, covering:
  - asymmetric encryption (Part 2);
  - block ciphers (Part 3);
  - stream ciphers (Part 4);
  - identity-based ciphers (Part 5);
  - (partially) homomorphic encryption (Part 6); and
  - tweakable block ciphers (Part 7).
- Actually, Part 7 is not quite finished – it should be published later in 2022.

ISO/IEC 18033-8

- A new part (Part 8) is currently at an early stage of development (second working draft) covering fully homomorphic encryption schemes.
- Such algorithms allow both addition and multiplication operations to be performed on encrypted data.
- The four schemes included in the current draft are:
  - Brakerski-Gentry-Vaikuntanathan (BGV);
  - Brakerski-Fan-Vercauteren (BFV);
  - Cheon-Kim-Kim-Song (CKKS);
  - Chillotti-Gama-Georgieva-Izabachene (CGGI).
- The security of all four schemes relies on the difficulty of the Ring Learning With Errors (RLWE) problem, so it is hoped they will be post-quantum-secure.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Where are we?
- New types of encryption
- Multi-party computation
- Lightweight cryptography
- Post-quantum cryptography
- The future

ROYAL HOLLOWAY UNIVERSITY OF LONDON

ISO/IEC 4922

- A three-part standard (ISO/IEC 4922) is being developed on secure multi-party computation.
- Secure multiparty computation enables the output of a function to be computed while keeping the individual inputs provided by different parties secret.
- It is a valuable tool to improve privacy in situations where computations need to be outsourced, or multiple stakeholders must cooperate.
- In essence, it is a scheme which emulates the functionality of a trusted third party that takes the private inputs of individual players, computes an agreed function, and disseminates the output privately to relevant parties.

ISO/IEC 4922-1

- Part 1 of the new standard (DIS ballot ended in April '22) is introductory (called *General*).
- Most of the multipart crypto standards have an introductory part as Part 1.
- Defines key ideas.
- Discusses parameters for secure multiparty computation, and also describes security properties of poractical schemes.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

ISO/IEC 4922-2

- Part 2 (2nd CD ballot very soon) covers mechanisms based on secret sharing.
- Secret sharing mechanisms (standardised in ISO/IEC 19592) allow a secret to be shared amongst *n* parties so that any *k* of them can recover the secret (for specified *k* and *n*).
- In secure multiparty computation based on secret sharing, a message is shared among participants.
- Each party computes a function on its message share and thereby obtains a share of the function output.
- The output can be obtained using a subset of the output shares.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

ISO/IEC 4922-3

- Part 3 (at a very early stage) covers mechanisms based on garbled circuits.
- Choices for mechanisms to standardise have not yet been made, so it is difficult to say more at this stage.
- Expert meetings are being held regularly online.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Where are we?
- New types of encryption
- Multi-party computation
- Lightweight cryptography
- Post-quantum cryptography
- The future

ROYAL HOLLOWAY UNIVERSITY OF LONDON

ISO/IEC 29192

- ISO/IEC 29192 is a multipart standard (currently 7 parts) covering a wide range of crypto functions designed to be *lightweight*.
  - ISO/IEC 29192-2: Block ciphers (2019, 2nd edn.);
  - ISO/IEC 29192-3: Stream ciphers (2012);
  - ISO/IEC 29192-4: Asymmetric schemes (2013);
  - ISO/IEC 29192-5: Hash functions (2016);
  - ISO/IEC 29192-6: MACs (2019);
  - ISO/IEC 29192-7: Broadcast authentication (2019).

ROYAL HOLLOWAY UNIVERSITY OF LONDON

ISO/IEC 29192-8

- A new part (Part 8) on *Authenticated encryption* is now nearing completion – voting on the FDIS ballot closes this month.
- It standardises a stream-cipher-based scheme called Grain-128A, dating back to 2011.
- This is an improved version of a scheme called Grain-128 which was broken.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Where are we?
- New types of encryption
- Multi-party computation
- Lightweight cryptography
- Post-quantum cryptography
- The future

ROYAL HOLLOWAY UNIVERSITY OF LONDON

NIST study

- I'm sure many of you are familiar with the ongoing project run by NIST to select quantum-computing-proof asymmetric algorithms.
- SC 27 is essentially waiting for this project to complete before deciding which algorithms it will standardise.
- These will, I expect, be added to the relevant multipart standards.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

ISO/IEC 14888-4

- One exception is provided by work on ISO/IEC 14888-4 (currently at CD ballot stage).
- This draft standard contains hash-based signatures.
- Such signatures are quantum-computer-proof, and are generally well-accepted.
- It was therefore felt that it was appropriate to standardise them even before the NIST process has completed.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Where are we?
- New types of encryption
- Multi-party computation
- Lightweight cryptography
- Post-quantum cryptography
- The future

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Further developments

- It is hard to predict what the next developments will be.
- I suspect that, once the NIST process has terminated, adopting a complete set of post-quantum asymmetric algorithms and protocols will take several years and significant effort.
- However, I am sure that other work will continue in parallel.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Your chance to contribute

- Here in the UK, inputs to the work of SC 27 are led by the British Standards Institute, which runs a committee (IST/33) which mirrors the work of SC 27.
- It has five sub-committees, (IST/33/1-IST/33/5) mirroring the work of WG 1 - WG 5 of SC 27.
- New members wishing to help further the development of security standards are welcome to participate.