INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE
C. J. Mitchell. ,Vol.X, No.Y, pp.*-*.

Challenges in standardising cryptography

Chris J. Mitchell

Information Security Group, Royal Holloway, University of London.
e-mail: me@chrismitchell.net

Abstract—A series of challenges that face effective standardisation of cryptographic techniques are discussed. In many cases these challenges are illustrated with case studies, primarily focussing on experience within ISO/IEC JTC 1/SC 27/WG 2, the international standards committee responsible for developing standards for cryptographic methods. Priorities for improving the effectiveness of the standards-making process are also highlighted.

1. Introduction

There is no doubt that standards have an important part to play in implementing and managing security. Within the field of cryptography, a vital technology for implementing security, standards have played a leading role in developments for around 40 years, i.e. since the dawn of its widespread commercial use. A detailed discussion of cryptographic standardisation up to 2005 can be found in Dent and Mitchell, [1].

However, as we discuss in this paper, there are many challenges to ensuring that cryptographic standards are as effective as they should be. Describing the nature of these challenges forms the main content of this paper. In many cases examples are given from recent standards development work.

The remainder of this paper is structured as follows. A brief and rather selective history of cryptographic standardisation is given in section 2. This is followed in section 3 by the main content of the paper, namely a review of some of the most serious challenges that face the standardisation process. The paper concludes with a number of remarks relevant to the future of standardisation 4.

2. Cryptographic standardisation

Standards have played a major role in cryptographic developments for over 40 years. In the 1970s, the US National Bureau of Standards (NBS), which later became the National Institute for Standards and Technology (NIST), requested proposals for a block cipher to become a US federal standard. This was implicit recognition that cryptography was becoming a vital technology for more than just the military and government classified applications. IBM made a proposal which, after modifications proposed by the NSA, in 1977 became the hugely important and influential DES algorithm [2]. DES, whilst now insecure in single key mode, remains in widespread use in multiple key mode.

*Manuscript received June 6, 2016; revised ***.*

Shortly after DES became a US federal standard, a number of parallel standards were published showing how to use the DES algorithm. Most important these included:

- methods for encrypting data to protect its confidentiality, i.e. the *modes of operation*, [3];
- techniques for generating a *Message Authentication Code (MAC)*, a type of checksum or *tag* appended to data which guarantees its integrity and origin [4], [5].

DES was initial standardised only for US federal government use. However, DES soon became a US national standard (published by ANSI), [6], and a de facto international standard for the protection of banking communications. Modes of operation and MAC standards were similarly published by ANSI, [7], [8], and also internationally by ISO/IEC [9], [10], [11].

On the international stage, in the early 1980s a committee was established specifically to address security standardisation: ISO/TC 97 (Information technology) established SC 20, dealing with cryptography. One of its earliest projects was to standardise DES, but, as discussed below, this failed. However, other work succeeded. When, at the beginning of the 1990s, ISO/TC 97 was merged with its parallel IEC committee to become ISO/IEC JTC 1, SC 20 was reformed and expanded in scope to become SC 27, dealing with all aspects of Information security (including cryptography). Today, SC 27[1], has five working groups (WGs), of which one, WG 2, is responsible for cryptography standards.

As mentioned in the previous paragraph, efforts in the late 1980s to produce an international standard for DES failed. In fact, the ISO DES standard was almost published, but was blocked for political reasons at the very last moment. Encryption (but not MACs and other cryptographic methods) was still a technology some governments wished to control. For this reason it was decided at the time that SC 27 was formed that its scope would explicitly exclude standardising encryption algorithms. This did not prevent the development of a range of standards covering a range of other techniques, and, in the early 2000s, the decision to exclude encryption was overturned. Today, a wide range of encryption algorithms are the subject of international standards (see, for example, ISO/IEC 18033, [12], [13], [14], [15]).

Indeed, SC 27/WG 2 has published, and continues to maintain, a wide range of standards for cryptographic techniques, including:

- encryption algorithms (including asymmetric schemes (ISO/IEC 18033-2, [13]), block ciphers (ISO/IEC 18033-3, [16]) and stream ciphers (ISO/IEC 18033-4, [15]));
- modes of operation for block ciphers (ISO/IEC 10116, [17]);
- MAC techniques (ISO/IEC 9797 parts 1–3, [18], [19], [20]);
- hash functions (ISO/IEC 10118 parts 1–4, [21], [22], [23], [24]);
- digital signatures (ISO/IEC 9796 parts 2 and 3, [25], [26] and ISO/IEC 14888 parts 1–3, [27], [28], [29]);
- authenticated encryption (ISO/IEC 19772, [30]);
- authentication and key management protocols (ISO/IEC 9798 parts 1–6, [31], [32], [33], [34], [35], [36], and ISO/IEC 11770 parts 1–4, [37], [38], [39], [40]);
- random bit and random prime generation (ISO/IEC 18031, [41], and 18032, [42]);
- lightweight cryptography (ISO/IEC 29192 parts 1–4, [43], [44], [45], [46]); and
- privacy enhancing technologies (ISO/IEC

1. See http://www.din.de/en/meta/jtc1sc27

20008 parts 1 and 2, [47], [48] and ISO/IEC 20009 parts 1 and 2, [49], [50]).

Despite these practical successes, many challenges remain, as we discuss in the remainder of this paper.

3. Challenges to standardisation

We now review some of the most serious challenges that the standardisation process continues to face.

3.1. Drafting and maintenance

Cryptographic algorithm standards are intended to specify a range of aspects of a technique, including:

- how to implement an algorithm;
- in what circumstances the algorithm should be used; and
- how parameters/options for an algorithm should be chosen.

However, they are not intended to be textbooks — in particular, they are not concerned with *why* particular aspects of a scheme are designed the way they are. After all, a software developer or protocol designer does not need to know such information; if they want to know more they can read a textbook or take a course on cryptography! Typically a standard will provide references to books and papers providing further information on the standardised techniques.

In the author's view, standards should be as simple and as easy to use as possible. Perhaps surprisingly, this is an area academics writing standards often really struggle with, as they instinctively want to explain *why*, and as a result they risk making standards unnecessarily long and complex. Indeed, writing an easy-to-use standard is a highly non-trivial exercise, and certainly something worth thinking about as an art in itself.

Perhaps the most serious challenge of all is merely to do with the fact that published standards need to be maintained, particularly in a fast-moving area like cryptography. As the list in the previous section makes clear, there are many published standards, and there are a limited number of experts prepared to give up their time for the often rather unglamorous work of updating and correcting draft standards.

Legacy, i.e. the need to maintain compatibility with existing deployed systems, is one of the bugbears of security, and this very much holds for standards development. In some cases SC 27/WG 2 has had to retain undesirable techniques or options in standards because they remain in wide use; typically a retained technique of this type will be one that is not suitable for general use but remains secure if used appropriately. Such a technique needs to be clearly marked as deprecated for new applications. Of course, there are obvious hazards in leaving such techniques in standards, but in practice there is little choice. Of course, if such a technique becomes completely insecure, then there is no alternative but to remove it from the standard as speedily as possible.

One example of such a deprecated technique arises in ISO/IEC 9797-1, [18], the ISO/IEC standard for MACs computed using a block cipher in a variant of Cipher Block Chaining (CBC) mode, so called CBC-MACs. When computing a CBC-MAC, the data meeds to be divided into fixed length blocks — as a result the last block of data often needs to be 'padded'. Historically this was done using a string of all zeros. This technique remains secure if the message length is known to the recipient by independent means, e.g. if the message length is fixed — otherwise it is insecure. Thus this padding

method should only be used with great care and its use is deprecated. However it is still specified in the latest edition of ISO/IEC 9797-1 (as padding method 1 of clause 6.3.2) because of the huge legacy of applications which employ this technique.

3.2. Revising standards

If a security weakness is found in a standardised algorithm, protocol or procedure, this needs to be fixed (to remove the algorithm or amend the advice on its use). Historically, SC 27/WG 2 has been receptive to news of problems and reasonably quick to act. However, acting has typically meant simply amending the standard. That is, unless a user of the standard regularly checks the ISO website[2] they would have no way of knowing that a change has occurred. This needs to change, and SC 27/WG 2 has recently developed procedures for informing the wider community of issues in existing standards as soon as possible after they have been identified. We briefly mention two recent examples of where such changes have needed to be made.

A few years ago, it became clear that almost all the authentication and key management protocol standards had a specification problem [51]. Many of the protocol messages are specified as being made up of the concatenation of various fields, input to a crypto-primitive. However, 'concatenation' was not really specified. It could be interpreted to mean simply taking two bit strings and joining them together to make a longer bit string. In some cases such an implementation could give rise to security issues. It was therefore necessary to amend all the affected standards (various parts of the ISO/IEC 9798 and ISO/IEC 11770 series) to make it clear that concatenation implied an encoding method which was uniquely and unambiguously decodable. SC 27/WG 2 created and published six corrigenda to fix this problem, all within 12 months.

ISO/IEC 19772, [30] is concerned with authenticated encryption. One of the six mechanisms in this standard is 'generic encrypt-then-MAC', i.e. allowing authenticated encryption to be instantiated by encryption then MAC computation using arbitrary (secure) algorithms. It was recently pointed out by Namprempre, Rogaway and Shrimpton, [52] that the standard as specified is insecure, since it did not mandate the inclusion of the Initialisation Vector used for the encryption process within the scope of the MAC. A (quite complex) corrigendum was written and published by WG 2 of SC 27 within 12 months, [53], to address this problem.

3.3. Timing

In some cases SC 27/WG 2 has tried to standardise techniques when there are no suitable candidates. For example, SC 27/WG 2 started work on ISO/IEC 10118-3 (dedicated hash-functions) before NIST's Secure Hash Algorithm (SHA) was published, when the only obvious candidates were MD4, [54], and MD5, [55]. As work started on this new standard in the early 1990s, it was made clear by participating experts that MD4 and MD5 were not suitable for standardisation. Fortunately SHA/SHA-1, [56], was published just at the right time, and was duly included in the first edition of ISO/IEC 10118-3, [57].

However, whilst there are dangers of standardising too early, there are also dangers of being too late. SC 27 is only now standardising key derivation techniques: ISO/IEC 11770-6 is currently out for FDIS ballot, [58], and should be published in late 2016. As a result there are many slightly different techniques in use (including in SC 27 standards), a potential major problem for future implementers trying to maintain compatibility between systems.

2. See http://www.iso.org/iso/home.html

3.4. Variation

As Tanenbaum famously said: 'The nice thing about standards is that there are so many of them to choose from', [59]. Cryptography standards have been, and continue to be, produced by many different bodies, including both national organisations (e.g. NIST, ANSI, DIN, BSI, etc.), and international bodies (such as ISO/IEC, IEEE, IETF, ITU-T, and ETSI). Too often these standards overlap and even conflict with one another, making life very challenging for standards users. Arguably even the ISO/IEC standards contain too many choices; for example, ISO/IEC 18033-3, [16], contains as many as seven different block ciphers: four 64-bit ciphers and three 128-bit schemes.

The issue of trying to minimise the set of standardised techniques has been discussed widely — see, for example, [60]. An internal standing document has been established within SC 27/WG2 to try to help ensure that only algorithms of genuine value to users are added to the catalogue of standardised techniques, [61].

3.5. Adoption

One major practical problem with ISO/IEC standards is that they are not freely available. Indeed they are rather expensive to buy. As a result they are widely ignored. Too often, IETF RFCs, many of which are not in any sense standards, are treated as the authoritative source for cryptographic technology. This is despite the fact that the process for adopting an ISO/IEC standard is far more rigorous than that used to decide whether an RFC should be promulgated.

There are many reasons why ISO/IEC standards are not always adopted. One is that they cost money, as discussed before. However, many parties seem possessed by an irrepressible desire to invent their own techniques, independently of any already existing standards. IETF is a prime example — the US influence is strong, and possibly as a result international standards are regarded as rather irrelevant. Perhaps more surprisingly, ETSI, with apparently good relations with ISO, insists on designing its own algorithms in its specialist cryptography committee SAGE[3] rather than joining forces with SC 27. Historically, the banking community have also tended to write their own standards.

This diversification of algorithm standards can have very damaging consequences. As mentioned before, MD5 (a hash function) was not standardised by ISO/IEC for sound security reasons. However, it was published by the IETF in an RFC, [55]. This has led to its very widespread (and continuing) use, despite the fact it is insecure. Indeed there are known real-world attacks, notably including the Flame malware, [62], which have exploited its use.

Although this is not necessarily the fault of the standards, there are many examples of implementations which have been found not to follow standards correctly — see, for example, [63], [64], [65]. This is perhaps not so much a problem for algorithm standards, but is certainly an issue for random number generation (as needed for cryptographic keys). It may also be a problem for some aspects of key management and authentication. This seems to be a cultural issue amongst the developer community. To try to minimise the chance of this happening, it is incumbent on developers of standards to make them as clear and precise as possible, and not burdened with unnecessary detail.

3.6. Reputation

The recent Snowden revelations, as discussed by Landau, [66], [67], have damaged the reputation of

3. See https://portal.etsi.org/TBSiteMap/sage

the cryptography standards bodies. As described below, it seems that a random bit generation algorithm of dubious security (known as Dual_EC_DRBG) were included in national (NIST) and international (ISO/IEC) standards.

Dual_EC_DRBG is a random bit generation technique. Following a parallel NIST standard, it was included in ISO/IEC 18031, [41], along with a set of 'recommended parameters'. Only because of Snowden did the world suddenly realise that the technique had originally been designed to allow the scheme to be broken if the parameters are chosen carefully (but only by the chooser of the parameters). Moreover, the 'recommended parameters' were of unknown provenance. As soon as this became known, SC 27/WG 2 issued a press release warning about this issue, and shortly afterwards a corrigendum was published, [68], removing Dual_EC_DRBG from the standard.

Whilst the offending technique has now been de-standardised, this potentially damages trust long-term. Indeed, two lightweight block ciphers, SIMON and SPECK, were recently submitted by the US national body (ANSI) for possible standardisation by ISO/IEC SC 27/WG 2 as part of its evolving lightweight cryptography standard, ISO/IEC 29192. Despite having desirable efficiency properties, and having been subject to widespread scrutiny, adoption is currently being blocked — mainly because of suspicion of the US.

3.7. Intellectual property and commercial issues

Some standards bodies prohibit standardisation of patent-protected schemes. ISO/IEC, however, allows this, as long as fair and non-discriminatory terms are agreed by the intellectual property (IP) owner. Enforcing this relies on the standards committee learning whether or not algorithms proposed for standardisation are protected. As a side issue, it is interesting to note that apparently minor crypto-related features of the 3G mobile standards which were patent-protected during the standards-writing process have meant that 'late' entrants to the mobile phone market (e.g. Apple) have had to make huge payments to the IP owners.

Many of the experts attending the standards committees are employees of companies with commercial interests in what is or is not standardised. As a result, the schemes that are standardised are sometimes influenced by commercial preferences. This is perfectly legitimate — if you attend, you get a say — but it may not always be desirable in a global sense. Academics can play an important role in challenging what look like poor decisions, as they are often unencumbered by commercial considerations.

As mentioned earlier in this talk, efforts to make DES an international standard in the 1980s foundered under US government pressure. However, triple DES is now part of ISO/IEC 18033-3, [16]. It remains primarily for commercial/legacy reasons — it is certainly significantly weaker than the key length would lead a user to expect. However, because it is in wide use, de-standardising it would cause major real-world problems. It is interesting to see what the impact will be of recent work showing 2-key triple DES is even weaker than previously thought [69].

3.8. Political issues

Just like companies with IP portfolios to exploit, governments, who often fund standards committee attendees, may wish to promote technologies which favour individual nation states. One reason is that if technologies are standardised then it is acceptable to list them in requirements specifications under WTO rules. This can lead to nations trying to get

national standards made international — this can, in turn, exacerbate the problem of excessive numbers of standardised algorithms.

4. Concluding remarks

The development of novel cryptographic techniques and their assessment and cryptanalysis is primarily down to academia, at least for non-government use. This means academic expertise is vital to the standardisation process in SC 27/WG 2 and elsewhere. Involvement at the national level typically costs nothing — national bodies shadowing the work of SC 27, and making contributions to the work, exist worldwide. Participation in international meetings as a national delegate is also possible.

On the relatively rare occasions defects are identified in standards, SC 27/WG 2 needs to be more active in promulgating these issues. Historically, WG 2 simply amended the standard concerned, and felt this was enough. However, this neglects the users who may have implemented the standard, and who are unaware of the changes. Only recently has SC 27/WG 2 developed procedures to let the wider world know when issues (such as Dual_EC_DRBG) are identified.

Sometimes standards development can take far too long. However, it is possible to go from start to finish with an ISO/IEC standard in less than three years; however, it often takes more like five! Greater involvement by experts is key to getting the job done in a timely way, and this includes those editing new standards.

Many academics are wary of being involved in standardisation as the payback is not easily defined — specifically, no publications arise directly and it is sometimes hard to get research grant funding to support involvement. However, as someone with nearly 30 years of involvement in standardisation, I know there are many potential benefits. Writing a standard often makes you think about things you might not otherwise worry about, and this can lead to new research. Also, standards development can lead to fruitful interactions with industry experts, and hence to joint research projects and/or consultancy. Above all else, there is huge intrinsic satisfaction in making academic work accessible and usable by the wider world.

Unfortunately, there are many examples of real world systems and products where it seems that development engineers and protocol designers have assumed they know better than cryptographers, and in particular than writers of standards. For example, developers sometimes design their own cryptographic algorithm or ignore vital parts of a security protocol because the rationale for their inclusion is not obvious (and hence they are wrongly deemed unnecessary). One might reasonably wonder what is it about cryptography that makes a non-expert assume they know as much as an expert. The answer is far from clear, but it is a hugely serious problem.

One way of reducing the risk of problems of the above type is to get as many people as possible involved in the standards process, and to try to ensure the main messages about standards implementation are promulgated as widely as possible. To this end, as a long-term standards contributor, I would like to appeal to everyone who cares about the correct use of cryptography to think about getting involved in crypto standards development. Standards represent a vitally important bridge between theory and practice. For those of us from academia, standards are our chance to communicate in simple terms what our research results indicate should happen.

Despite all the challenges described above, SC 27 has a pretty good track record — so far! Very few standardised schemes have needed to be significantly modified or removed, despite a standards

portfolio going back 30 years. However, for this to remain true requires that the cryptographic community, in academia and industry, continues to participate in and contribute to the standards development and management processes.

References

[1] A. W. Dent and C. J. Mitchell, *User's Guide to Cryptography and Standards*. Artech House, Boston, MA, 2005.

[2] *National Bureau of Standards (NBS) Federal Information Processing Standards (FIPS) Publication 46—Data Encryption Standard (DES)*, National Technical Information Service, Springfield, Va., April 1977.

[3] *National Bureau of Standards (NBS) Federal Information Processing Standards (FIPS) Publication 81—DES modes of operation*, National Technical Information Service, Springfield, Va., December 1980.

[4] *ANSI X9.19, Financial institution retail message authentication*, American Bankers Association, Washington, DC, August 1986.

[5] *ANSI X9.9–1986 (revised), Financial institution message authentication (wholesale)*, American Bankers Association, Washington, DC, April 1986.

[6] *ANSI X3.92–1981, Data Encryption Algorithm*, American National Standards Institute, New York, 1981.

[7] *ANSI X3.106–1983, Data Encryption Algorithm—Modes of operation*, American National Standards Institute, New York, 1983.

[8] *ANSI X9.52–1998, Triple Data Encryption Algorithm — Modes of operation*, American National Standards Institute, New York, 1998.

[9] *ISO 8372: 1987, Information Processing — Modes of operation for a 64-bit block cipher algorithm*, International Organization for Standardization, Genève, Switzerland, 1987.

[10] *ISO/IEC 9797: 1989, Data cryptographic techniques—Data integrity mechanism using a cryptographic check function employing a block cipher algorithm*, International Organization for Standardization, Genève, Switzerland, December 1989.

[11] *ISO/IEC 10116: 1991, Information Processing — Modes of operation for an n-bit block cipher algorithm*, International Organization for Standardization, Genève, Switzerland, 1991.

[12] *ISO/IEC 18033-1:2005, Information technology — Security techniques — Encryption Algorithms — Part 1: General*, International Organization for Standardization, Genève, Switzerland, 2005.

[13] *ISO/IEC 18033-2:2006, Information technology — Security techniques — Encryption Algorithms — Part 2: Asymmetric Ciphers*, International Organization for Standardization, Genève, Switzerland, 2006.

[14] *ISO/IEC 18033-3:2010, Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*, 2nd ed., International Organization for Standardization, Genève, Switzerland, 2010.

[15] *ISO/IEC 18033-4:2011, Information technology — Security techniques — Encryption Algorithms — Part 4: Stream Ciphers*, 2nd ed., International Organization for Standardization, Genève, Switzerland, 2011.

[16] *ISO/IEC 18033-3:2010, Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*, 2nd ed., International Organization for Standardization, Genève, Switzerland, 2010.

[17] *ISO/IEC 10116: 2006, Information technology — Security techniques — Modes of operation for an n-bit block cipher*, 3rd ed., International Organization for Standardization, Genève, Switzerland, 2006.

[18] *ISO/IEC 9797–1, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*, 2nd ed., International Organization for Standardization, Genève, Switzerland, 2011.

[19] *ISO/IEC 9797-2:2011, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function*, 2nd ed., International Organization for Standardization, Genève, Switzerland, May 2011.

[20] *ISO/IEC 9797-3:2011, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 3: Mechanisms using a universal hash-function*, International Organization for Standardization, Genève, Switzerland, 2011.

[21] *ISO/IEC 10118-1:2000, Information technology — Security techniques — Hash-functions — Part 1: General*, 2nd ed., International Organization for Standardization, Genève, Switzerland, June 2000.

[22] *ISO/IEC 10118-2:2010, Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher*, 3rd ed., International Organization for Standardization, Genève, Switzerland, October 2010.

[23] *ISO/IEC 10118–3, Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*, 3rd ed., International Organization for Standardization, Genève, Switzerland, 2004.

[24] *ISO/IEC 10118-4:1998, Information technology — Security techniques — Hash-functions — Part 4: Hash-functions using modular arithmetic*, International Organization for Standardization, Genève, Switzerland, December 1998.

[25] *ISO/IEC 9796-2:2010, Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*, 3rd ed., International Organization for Standardization, Genève, Switzerland, December 2010.

[26] *ISO/IEC 9796-3:2006, Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms*, 2nd ed., Inter-

national Organization for Standardization, Genève, Switzerland, September 2006.

[27] *ISO/IEC 14888-1:2008, Information technology — Security techniques — Digital signatures with appendix — Part 1: General*, 2nd ed., International Organization for Standardization, Genève, Switzerland, April 2008.

[28] *ISO/IEC 14888-2:2008, Information technology — Security techniques — — Digital signatures with appendix — Part 2: Integer factorization based mechanisms*, 2nd ed., International Organization for Standardization, Genève, Switzerland, April 2008.

[29] *ISO/IEC 14888-3:2016, Information technology — Security techniques — — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*, 3rd ed., International Organization for Standardization, Genève, Switzerland, March 2016.

[30] *ISO/IEC 3rd CD 19772, Information technology — Security techniques — Authenticated encryption mechanisms*, International Organization for Standardization, Genève, Switzerland, June 2007.

[31] *ISO/IEC 9798-1:2010, Information technology — Security techniques — — Entity authentication — Part 1: General*, 3rd ed., International Organization for Standardization, Genève, Switzerland, June 2010.

[32] *ISO/IEC 9798-2:2008, Information technology — Security techniques — — Entity authentication — Part 2: Mechanisms using symmetric encipherment algorithms*, 3rd ed., International Organization for Standardization, Genève, Switzerland, December 2008.

[33] *ISO/IEC 9798-3:1998, Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature algorithms*, 2nd ed., International Organization for Standardization, Genève, Switzerland, 1998.

[34] *ISO/IEC 9798–4:1999, Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function*, 2nd ed., International Organization for Standardization, Genève, Switzerland, 1999.

[35] *ISO/IEC 9798-5:2009, Information technology — Security techniques — — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques*, 3rd ed., International Organization for Standardization, Genève, Switzerland, December 2009.

[36] *ISO/IEC 9798-6:2010, Information technology — Security techniques — — Entity authentication — Part 6: Mechanisms using manual data transfer*, 2nd ed., International Organization for Standardization, Genève, Switzerland, November 2010.

[37] *ISO/IEC 11770-1:2010, Information technology — Security techniques — — Key management — Part 1: Framework*, 2nd ed., International Organization for Standardization, Genève, Switzerland, November 2010.

[38] *ISO/IEC 11770-2:2008, Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*, 2nd ed., International Organization for Standardization, Genève, Switzerland, 2008.

[39] *ISO/IEC 11770-3:2015, Information technology — Security techniques — — Key management — Part 3: Mechanisms using asymmetric techniques*, 3rd ed., International Organization for Standardization, Genève, Switzerland, August 2015.

[40] *ISO/IEC 11770–4:2006, Information technology — Security techniques — Key management — Part 4: Mechanisms based on weak secrets*, International Organization for Standardization, Genève, Switzerland, 2006.

[41] *ISO/IEC 18031:2011, Information technology — Security techniques — Random bit generation*, 2nd ed., International Organization for Standardization, Genève, Switzerland, 2011.

[42] *ISO/IEC 18032:2005, Information technology — Security techniques — — Prime number generation*, International Organization for Standardization, Genève, Switzerland, January 2005.

[43] *ISO/IEC 29192-1:2012, Information technology — Security techniques — Lightweight cryptography — Part 1: General*, International Organization for Standardization, Genève, Switzerland, 2012.

[44] *ISO/IEC 29192-2:2012, Information technology — Security techniques — Lightweight cryptography — Part 2: Block ciphers*, International Organization for Standardization, Genève, Switzerland, 2012.

[45] *ISO/IEC 29192-3:2012, Information technology — Security techniques — Lightweight cryptography — Part 3: Stream ciphers*, International Organization for Standardization, Genève, Switzerland, September 2012.

[46] *ISO/IEC 29192-4:2013, Information technology — Security techniques — Lightweight cryptography — Part 4: Mechanisms using asymmetric techniques*, International Organization for Standardization, Genève, Switzerland, May 2013.

[47] *ISO/IEC 20008-1:2013, Information technology — Security techniques — Anonymous digital signatures — Part 1: General*, International Organization for Standardization, Genève, Switzerland, December 2013.

[48] *ISO/IEC 20008-2:2013, Information technology — Security techniques — Anonymous digital signatures — Part 2: Mechanisms using a group public key*, International Organization for Standardization, Genève, Switzerland, November 2013.

[49] *ISO/IEC 20009-1:2013, Information technology — Security techniques — Anonymous entity authentication — Part 1: General*, International Organization for Standardization, Genève, Switzerland, July 2013.

[50] *ISO/IEC 20009-2:2013, Information technology — Security techniques — Anonymous entity authentication — Part 2: Mechanisms based on signatures using a group public key*, International Organization for Standardization, Genève, Switzerland, November 2013.

[51] L. Chen and C. J. Mitchell, "Parsing ambiguities in authentication and key establishment protocols," *Journal of Electronic Security and Digital Forensics*, vol. 3, pp. 82–94, 2010.

[52] C. Namprempre, P. Rogaway, and T. Shrimpton, "Reconsidering generic composition," in *Advances in Cryptology — EUROCRYPT 2014 — 33rd Annual International Conference on the*

Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11–15, 2014. Proceedings, ser. Lecture Notes in Computer Science, P. Q. Nguyen and E. Oswald, Eds., vol. 8441. Springer-Verlag, Berlin, 2014, pp. 257–274.

[53] *ISO/IEC 19772:2009/Cor 1:2014, Information technology — Security techniques — Authenticated encryption mechanisms — Corrigendum 1*, International Organization for Standardization, Genève, Switzerland, September 2014.

[54] R. L. Rivest, *RFC 1320, The MD4 Message-Digest Algorithm*, Internet Engineering Task Force, April 1992.

[55] ——, *RFC 1321, The MD5 Message-Digest Algorithm*, Internet Engineering Task Force, April 1992.

[56] *Federal Information Processing Standard Publication 180 (FIPS PUB 180): Secure Hash Standard (SHS)*, U.S. Department of Commerce / National Institute of Standards and Technology (NIST), Gaithersburg, MD, October 1993.

[57] *ISO/IEC 10118–3, Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*, International Organization for Standardization, Genève, Switzerland, 1998.

[58] *ISO/IEC FDIS 11770-6, Information technology — Security techniques — Key management — Part 1: Key derivation*, International Organization for Standardization, Genève, Switzerland, May 2016.

[59] A. S. Tanenbaum, *Computer networks*, 2nd ed. Prentice-Hall, Upper Saddle River, NJ, 1988.

[60] C. J. Mitchell, "Choosing algorithms to standardise," Department of Mathematics, Royal Holloway, University of London, Tech. Rep. RHUL-MA-2012-14, June 2012, available at http://www.ma.rhul.ac.uk/techreports.

[61] *ISO/IEC JTC 1/SC 27 N14020: SC 27/WG 2 Standing Document 5 — Process for inclusion and deletion of Cryptographic Mechanisms*, International Organization for Standardization, Genève, Switzerland, April 2014, available at http://www.din.de/en/meta/jtc1sc27/downloads.

[62] K. Munro, "Deconstructing Flame: the limitations of traditional defences," *Computer Fraud & Security*, vol. 2012, pp. 8–11, 2012.

[63] J. P. Degabriele and K. G. Paterson, "Attacking the IPsec standards in encryption-only configurations," in *Proceedings: 2007 IEEE Symposium on Security and Privacy (S&P 2007), 20–23 May 2007, Oakland, California, USA*. IEEE Computer Society Press, Los Alamitos, California, 2007, pp. 335–349.

[64] S. Fahl, M. Harbach, T. Muders, M. Smith, L. Baumgärtner, and B. Freisleben, "Why Eve and Mallory love Android: An analysis of Android SSL (in)security," in *ACM Conference on Computer and Communications Security, CCS '12, Raleigh, NC, USA, October 16–18, 2012*, T. Yu, G. Danezis, and V. D. Gligor, Eds. ACM, 2012, pp. 50–61.

[65] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov, "The most dangerous code in the world: Validating SSL certificates in non-browser software," in *ACM Conference on Computer and Communications Security, CCS '12, Raleigh, NC, USA, October 16–18, 2012*, T. Yu, G. Danezis, and V. D. Gligor, Eds. ACM, 2012, pp. 38–49.

[66] S. Landau, "Making sense from Snowden: What's significant in the NSA surveillance revelations," *IEEE Security & Privacy*, vol. 11, no. 4, pp. 54–63, 2013.

[67] ——, "Highlights from making sense of Snowden, Part II: What's significant in the NSA revelations," *IEEE Security & Privacy*, vol. 12, no. 1, pp. 62–64, 2014.

[68] *ISO/IEC 18031:2011/Cor 1:2014, Information technology — Security techniques — Random bit generation — Corrigendum 1*, International Organization for Standardization, Genève, Switzerland, September 2014.

[69] C. J. Mitchell, "On the security of 2-key triple DES," February 2016, arXiv:1602.062298 [cs.CR], http://arxiv.org/abs/1602.06229.