Choosing algorithms to standardise

Chris J. Mitchell
Information Security Group
Royal Holloway, University of London
me@chrismitchell.net

24th July 2012

Abstract

The developers of the ISO/IEC standard on encryption, ISO/IEC 18033, are facing a dilemma. To maximise interoperability and make life as simple as possible for developers, the smallest possible number of algorithms should be standardised; however, despite this, there seems to be an inexorable growth in the number of standardised algorithms. We put this problem into historical context, and review efforts to devise ways of restricting the numbers of standardised algorithms dating back to the beginning of the development of ISO/IEC 18033. We then consider how and why these efforts have proved inadequate, leading to an almost uncontrollably large number of standardised algorithms. Finally, we discuss recent efforts to address this situation, which appear to have ramifications not only for ISO/IEC but for almost any body seeking to standardise a set of general purpose techniques.

1 Introduction

The sad but true quote 'The nice thing about standards is that you have so many to choose from' is due to Andrew Tanenbaum [32]. This applies to encryption just as much as any other technology. There are almost as many encryption standards, both de facto and de jure, as there are algorithms to choose from.

Nevertheless, the potentially positive role of a well-written and well-used standard is clear — the use of poor choices for encryption algorithms is widely believed to be the source of a huge number of security vulnerabilities [31], and so broad adoption of a sound standard would greatly improve matters. Over the last decade or so, and with this is mind, one such series of standards, ISO/IEC 18033 [11, 13, 15, 19], has been developed.

From the beginning of its development, experts in the committee responsible for its drafting (ISO/IEC JTC1/SC27/WG2) were aware of the possible danger of ISO/IEC 18033 becoming nothing more than a large catalogue of known algorithms, rather than a carefully selected set of algorithms recommended for wide use. As a result, in the introductory part (ISO/IEC 18033-1 [11]) a list of 'criteria for inclusion of ciphers in ISO/IEC 18033' was included, one objective for which was to try to minimise the number of standardised schemes. The inclusion of these criteria has only had very limited success in reducing the number of standardised algorithms — for example, ISO/IEC 18033-3 [15] (concerned with block ciphers) contains a total of seven different algorithms, and there seems to be constant pressure for the standard to be expanded to include new algorithms.

With this in mind, over the last couple of years work has been ongoing on 'beefing up' these criteria, to try to end this proliferation. In this article we review this work and consider the likely outcome, as well as possible implications for the general notion of standardising specific algorithms (of all types); we also note the possible wider applicability of such criteria. Additional inputs to the standardisation process are sought from all interested parties.

The reminder of the article is structured as follows. In section 2 we briefly review the history of encryption standardisation. This is followed in section 3 by a discussion of possible ways of deciding what should, and should not, be standardised. In section 4 we then consider the recent (failed) efforts to include the Russian block cipher GOST in ISO/IEC 18033-3. More recent efforts to produce a more rigorous set of selection criteria are discussed in section 5, followed by concluding remarks in section 6.

2 Standards for encryption

Encryption standardisation in the public domain dates back to the 1970s, when the National Bureau of Standards (NBS) in the US decided to create a standard for use by federal government bodies when procuring security products. Of course, there were, no doubt, closed 'standards' in use long before this, e.g. as employed by military alliances, but this is beyond the scope of this paper.

As has been widely documented (see, for example, Meyer and Matyas [27]), to achieve its goal the NBS launched a competition to select a standard algorithm. IBM was the only entrant and, after some modifications, IBM's submission became the still very widely used Data Encryption Standard (DES) block cipher, defined in the NBS Federal Information Processing Standard (FIPS) 46 [30].

From the very beginning, the relatively short (56-bit) key length of DES gave rise to concerns about its security (see Diffie and Hellman [3]). More recently, both software and hardware attacks taking advantage of this property have been demonstrated [1, 4]. As a result, triple DES, involving three iterations of DES using two or three keys, was introduced as a more secure yet backwards compatible alternative; triple DES was included in an updated version of the original standard, as issued by the National Institute for Standards and Technology (NIST), the successor body to NBS [28].

Whilst it remains very widely used, triple DES was always only a stopgap solution, since it is relatively inefficient and it needs to be used with care to avoid cryptanalytic attacks. As a result, following another competition, in 2001 NIST adopted the Advanced Encryption Standard (AES) algorithm as a replacement for both DES and triple DES [29].

Whilst DES, triple DES and AES have been very widely used, they were originally national rather than international standards. Many other nations have adopted national standards, although they have been much less influential internationally, and we do not consider them further here — the main focus of this paper is on international standardisation and, more specifically, ISO/IEC standards.

Within ISO, work on standards for cryptographic techniques goes back to the early 1980s. One of the first projects within SC20, the cryptography sub-committee of ISO TC97, was to make the DES algorithm into an international standard. Work on this progressed successfully until the very final stage — after a successful final ballot of member bodies, adoption of DES as an ISO standard was blocked for political reasons within the organisational structure of ISO itself. Following this, and for the same reasons, a decision was made to abandon any attempts within ISO to standardise encryption techniques, although work continued on standards for other cryptographic methods, including digital signatures, message authentication codes (MACs), key management schemes, and authentication protocols. Standards on all these technologies were, and continue to be, produced.

Despite the decision to abandon standardisation of encryption, it was nevertheless felt that a standardised naming scheme for encryption techniques was needed, e.g. for algorithm negotiation in communications protocols. This gave rise to the notion of the ISO register of cryptographic algorithms, intended as an agreed list of algorithms, each with a unique name. The form of the register, and the procedures for inclusion in it, were standardised in ISO/IEC 9979 [9][1]. However, inclusion in the register was not intended to indicate that an algorithm is recommended for use, or has met any minimum set of criteria for security — it simply functioned as a way of naming schemes. Eventually a total of 24 algorithms were included in the register.

[1] Although now defunct, the register is still online at `www.ISO-register.com`

By 2000, the political climate had changed sufficiently for the ISO standardisation of encryption algorithms to become possible. As a result, ISO/IEC JTC1/SC27 (the successor committee to TC97/SC20), started work on what became a four-part standard on encryption techniques, ISO/IEC 18033. This standard, which forms the main focus of this article, has the following coverage.

- Part 1, [11], is an introductory part, and provides definitions for the subsequent parts which specify algorithms. Most significantly from the perspective of this paper, it contains an annex entitled 'Criteria for inclusion of ciphers in ISO/IEC 18033', which we discuss in greater detail in section 3.
- ISO/IEC 18033-2, [13], is concerned with asymmetric encryption.
- The third part, [15], covers block ciphers. Modes of operation for block ciphers, i.e. standardised ways to use block ciphers for encryption, are described in a separate standard, ISO/IEC 10116 [12].
- Finally, part 4, [19], specifies stream cipher techniques.

Of course, although it forms the main focus of this paper, ISO/IEC 18033 is not the only international encryption standard. For example, the IEEE P1363 committee has developed a series of standards for asymmetric cryptography [5, 7, 8, 6], including encryption techniques. The RSA company has also developed a series of specifications for the use of public key techniques, known as the PKCS specifications[2].

In addition there are a wide range of sector-specific encryption standards, including for the GSM, 3GPP and LTE mobile networks, and for use in banking applications. Finally, national and regional efforts have been put in place to try to evaluate cryptographic techniques, including ECRYPT and ECRYPT II[3] in Europe, and CRYPTREC[4] in Japan.

For a more detailed review of the history of encryption standardisation up to 2004, see chapter 4 of Dent and Mitchell [2].

3 Criteria for standardisation — a history

From the very beginning of the ISO/IEC 18033 standardisation effort in 2000, the danger of the standard ending up like the register was recognised. That is, there was widespread concern that the standard should not consist

[2]See `http://www.rsa.com/rsalabs/node.asp?id=2124`

[3]See `http://www.ecrypt.eu.org/`

[4]See `http://www.cryptrec.go.jp/english/`

of a long list containing everyone's favourite algorithm, but should instead contain a short list of algorithms recommended for widespread use.

As a result, the very first working draft of what would become ISO/IEC 18033-1 [10] contained a list of 'Criteria for inclusion of algorithms in this standard'. The intention was to devise a list of properties necessary for an algorithm to be included in the standard, with the goal of trying to reduce the number (and improve the quality) of the standardised algorithms. This list was included in the main body of the draft, making the criteria *normative* (i.e. mandatory) and not just *informative* (i.e. advisory). The text given in the 1st working draft was as follows.

> The algorithms included in subsequent parts of this international standard have been selected from the large variety of encryption algorithms published and in use. The exclusion of particular algorithms does not imply that these algorithms are insecure. The algorithms specified represent a small set of algorithms chosen according to the following criteria (where the order of presentation of the criteria is not of significance).
>
> The evaluation will be made with respect to the following aspects of the algorithm.
>
> 1. The *security* of the algorithm, i.e. selected algorithms must be resistant to cryptanalytic attack. The existence of a proof of security will be regarded as a significant argument in favour of an algorithm, depending on the security model and the proof assumptions. The nature of any evaluations will also be of great importance, especially those conducted by widely recognised evaluation organisations.
> 2. The *performance* of the algorithm on a variety of typical platforms. This will include not only issues such as time and space efficiency, but also whether or not it has characteristics that give it advantages over other techniques.
> 3. The nature of any *licensing issues* affecting the algorithm.
> 4. The *maturity* of the algorithm. The maturity of the algorithm will be evaluated in terms of how extensively it has been used, how widely any analysis has been published, how much the algorithm has been scrutinised, and whether or not the algorithm has already been adopted by another standards organisation.
> 5. The existing *level of use* of the algorithm. Unless other considerations over-ride such a decision, algorithms that are de facto standards are to be favoured over less well-used algorithms.

6. In general, the *number* of algorithms to be standardised in each part of this international standard should be as small as possible. Two exceptions to this rule exist.
   (a) Where two algorithms have different characteristics, e.g. n-bit block ciphers with different values of n or ciphers with widely differing computational and space implementation requirements, and both sets of characteristics have practical significance, ciphers of both types are likely to be standardised.
   (b) It is generally desirable to have available standard ciphers based on different fundamental principles, such that if one cipher becomes vulnerable to cryptanalytic attack, another algorithm has a good chance of remaining secure.

Making such a list normative was controversial; some nations preferred deleting the list altogether. As a compromise it was eventually agreed to include the list (in modified form) in an annex to ISO/IEC 18033-1, making it informative. The final text of this annex [11] is as reproduced below.

> The ciphers included in subsequent parts of ISO/IEC 18033 have been selected from the large variety of such techniques published and in use. The exclusion of particular ciphers does not imply that these techniques are insecure. The ciphers specified represent a small set of techniques chosen according to the following criteria (where the order of presentation of the criteria is not of significance).
>
> Evaluations are made with respect to the following aspects of the cipher.
>
> 1. The *security* of the cipher, i.e. selected algorithms must be resistant to cryptanalytic attack. The existence of a proof of security is regarded as a significant argument in favour of a cipher, depending on the security model and the proof assumptions. The nature of any evaluations is also of great importance, especially those conducted by widely recognised evaluation organisations.
> 2. The *performance* of the cipher on a variety of typical platforms. This includes not only issues such as time and space efficiency, but also whether or not it has characteristics that give it advantages over other techniques.
> 3. The nature of any *licensing issues* affecting the cipher.

4. The *maturity* of the cipher. The maturity of the cipher is evaluated in terms of how extensively it is used, how widely any analysis has been published, and the level to which the cipher has been scrutinised.
5. The degree to which the cipher is *endorsed* by a recognised organisation (e.g. a standards body, government security agency, etc.), or is under investigation and/or analysis for endorsement by such a body.
6. The existing level of *adoption* of the cipher. Unless other considerations over-ride such a decision, ciphers that are de facto standards are to be favoured over less well-used techniques.
7. In general, the *number* of ciphers to be standardised in each part of of ISO/IEC 18033 should be as small as possible. Two exceptions to this principle exist.
   (a) Where two ciphers have different characteristics, e.g. n-bit block ciphers with different values of n or ciphers with widely differing computational and space implementation requirements, and both sets of characteristics have practical significance, ciphers of both types are likely to be standardised.
   (b) It is generally desirable to have available standard ciphers based on different fundamental principles, such that if one cipher becomes vulnerable to cryptanalytic attack, another cipher has a good chance of remaining secure.

It is interesting to note that apart from a few small wording changes, the text of the criteria did not change much over the four years during which the standard went from first draft to published version. The main change was to replace 'level of use' with 'degree of endorsement'. It seems reasonable to conclude that the general tone, and rather vague wording, of the criteria met with general approval.

While the criteria have proved useful in considering which algorithms should be standardised, they have been far from successful in restricting the number of standardised schemes (despite criterion 7 in the above list). ISO/IEC 18033-2 [13] contains a total of six public key encryption schemes (together with three data encapsulation mechanisms), the second edition of ISO/IEC 18033-3 [15] specifies seven different block ciphers, and the latest version of ISO/IEC 18033-4 [19] contains five stream cipher schemes. Recently the situation has been exacerbated by the publication of a four-part standard on 'lightweight' cryptographic techniques, ISO/IEC 29192 [20, 23, 24, 25],

covering block ciphers, stream ciphers and asymmetric techniques. The lightweight block cipher standard, ISO/IEC 29192-2 [24], contains a further two block ciphers, and the lightweight stream cipher standard, ISO/IEC 29192-3 [25], contains three stream ciphers. That is, when combined with ISO/IEC 18033, there are a total of nine ISO/IEC standard block ciphers and eight standard stream ciphers.

Ideally, one might imagine a scenario where the numbers of standardised algorithms was perhaps not much more than half the above numbers, which would still allow for some degree of choice. Perhaps the major problem with the ISO/IEC standardisation process is that it is much easier to include a new algorithm into a draft standard than it is to remove it once it is there.

Recently, and rather belatedly, SC27/WG2 has decided that the situation is becoming such that the reputations of ISO and IEC could be damaged if the list of standardised algorithms is permitted to continue to grow in length. We will consider in section 5 how progress is being made in this direction. However, we first consider recent events which will continue to inform the debate about how to choose algorithms for standards.

4 GOST — to standardise or not to standardise?

Concerns regarding the fact that the standard was in danger of becoming a catalogue containing a large number of algorithms, rather than a small number of carefully scrutinised and recommended algorithms, were exposed during the long and painful discussions regarding the possible ISO adoption of the GOST cipher. GOST 28147-89 [33] is a Russian national standard block cipher, the origins of which date back to the 1970s.

In April 2009, a proposal to include the GOST block cipher in ISO/IEC 18033-3 was circulated [14]. Much of the discussion about whether or not to include the algorithm centered around the criteria given in ISO/IEC 18033-1. Arguably the algorithm met all the criteria, although there was considerable resistance to the idea of adopting the algorithm, since it was seen as being both outdated in design and rather inefficient.

After almost two years of discussions, the decision eventually came to a vote, the result of which was not to standardise GOST [21]. The discussion was finally swung by the appearance of a paper by Isobe [26], describing an attack against GOST significantly faster than a brute force attack[5]. Whilst far from practical, it was felt that the existence of such an attack meant that GOST should not be standardised; however, this is going beyond what is stated in the criteria, since the attack in no way threatens the security of

[5]Since this paper has been published, other attacks on GOST have been described, although none are in any sense practical.

the scheme. This decision suggests that the criteria need to be made more explicit, so that it is made explicit that algorithms which are clearly less secure than they are designed to be should not be standardised.

5 Recent developments

Over and above the GOST discussions, concerns about the number of algorithms being standardised had been growing within SC27 for some time, and this came to head during the SC27/WG2 meeting in Berlin in October 2010. The ECRYPT II project had submitted a fairly strongly worded liaison statement to SC27/WG2 [17] criticising the apparent policy of making ISO/IEC standards into catalogues of algorithms rather than carefully selected recommendations. The liaison statement contained the following warning.

> Finally, we would like to stress the difficulty of creating stable cryptographic standards. If a standard includes an algorithm, that is subsequently broken, it becomes urgent to update the standard, lest users lose confidence in the standard. Special care has to be taken in order to avoid too frequent updating or amendment of standards because algorithms have been broken. Furthermore, the usefulness of a standard with more than a few ciphers is questionable, since it impedes rather than enhances interoperability.
>
> Therefore, standards should not just be collections of algorithms that are unbroken at the time of submission. The selection of which algorithms to include in a standard must be performed with great diligence, and only algorithms that offer sufficient confidence in their security in the long term should be considered. Such confidence can only be obtained once an algorithm reaches a certain level of maturity through extensive evaluation and analysis.

It is not surprising that a long and heated debate about this liaison statement took place in Berlin. The main conclusions of this debate are reported in the meeting report [16], in which the following statement is made.

> [The liaison statement from ECRYPT II] had a recommendation regarding the choice of encryption algorithms for inclusion in our standards. It also said that ISO should not merely have a collection of ciphers but rather have fewer ciphers and choose them carefully. Liaison officer from ECRYPT II attended the meeting and pointed out that many years ago a cipher register

> was kept instead of a standard on ciphers, and that the current standard was growing into something similar to a register again, except that it was called a standard.
>
> The general consensus seemed to be that WG2 experts did agree with ECRYPT II that care should be taken in choosing the encryption algorithms, but no consensus could be reached by the meeting as to the criteria to be used to choose the best ciphers as well as the number of ciphers, and it was agreed that a study period should be established in WG2 to investigate the selection criteria.
>
> There were concerns within the delegates present regarding the ongoing project and the impact that the establishment of a study period has on the progressing of these projects at the meeting. Everyone at the WG2 meeting seemed to be in agreement that the study period should not disrupt the current projects and that it should be conducted independently of them. A number of questions which must be included in the call for contributions were set up by the experts during the meeting.
>
> Therefore, it was agreed to establish a study period on the criteria for standardization of encryption algorithms. At this stage this study period will focus only on encryption algorithms and may be broadened in a next stage to include other mechanisms. It was also agreed to send out a call for contributions with the questions.

As can be seen from the meeting report, this very serious matter was dealt with by setting up a committee! Of course, to be fair, this is pretty well the only measure that a standards committee can take.

The initial call for contributions to this study period [18] asked a total of eight questions, as follows.

1. What is the appropriate number of algorithms that should be in the ISO/IEC 18033 standards?
2. During the selection process, as well as in the ECRYPT II liaison statement, some terms are often used for selection criteria. There does not seem to be consensus on how to define these criteria exactly.
    - What are appropriate definitions of 'The algorithm should be widely known'?
    - What are appropriate definitions of 'The algorithm should be sufficiently analysed'?

- What should the criteria be to define 'The algorithm should be sufficiently mature for standardisation'?

3. Should ISO/IEC documents address different levels of security, e.g. low security, medium security, high security? If so, please provide suggested levels.

4. Do you have any research available regarding the use of algorithms published in SC 27 standards within your country or the world? If so, please provide such research to this study period.

5. What do you think should be the selection criteria to standardise algorithms in SC27/WG2?

6. What is your opinion regarding the algorithms currently included in the standards as set out in 1. above.

7. The ECRYPT II liaison statement listed the following algorithms for consideration for inclusion into the SC 27 standard (possibly 29192-3 or 18033-4). Please formulate an opinion on which cipher(s) you support for inclusion in the SC27/WG2 standard.

8. Is there anything else you want to contribute to the study period regarding how algorithms should be selected for inclusion in SC27/WG2 standards?

In the ensuing 18 months, not all these questions have been addressed satisfactorily, but the study period is nevertheless having some effects. In particular, it has been decided to revise ISO/IEC 18033-1 to both strengthen and clarify the selection criteria, and also to make them normative as opposed to informative.

This has been implemented in the current (2nd) working draft of the revised version of ISO/IEC 18033-1 [22]. The annex containing the criteria has been made normative, and has been expanded considerably to contain three main parts, as follows.

- The first part specifies 'Minimum qualification criteria for addition of ciphers'. It states that 'In order for a cipher to be considered for inclusion in subsequent parts of this International Standard ... [it] ... shall comply with the following requirements'. These requirements are as follows.

  a) *Minimum security strength*: All ciphers submitted shall have [a] minimum security strength of 128 bits. Additionally the only known cryptanalytic attacks against the cipher shall not be faster than generic attacks against the cipher.

b) *Public domain*: The cipher description shall have been published for a minimum period of 3 years in the public domain. [Examples of acceptable publication venues are also listed].

c) *Cryptanalysis*: Prior to inclusion a cipher shall have cryptanalysis papers published in peer reviewed journals or conferences such as those listed in b).

d) *Industry adoption*: Robust evidence shall be provided of commercial applications using the ciphers and possible world-wide deployments of the applications.

e) *Performance*: Performance measurements occur on many different vectors such as bits/cycle, bits/watt, bits/security level. Robust evidence shall be provided that the cipher offers better performance on the performance vectors that are optimised for the intended applications [than] existing ciphers already in the standard.

- The second part specifies 'Guidelines used for considering encryption algorithms'. These are very similar to the criteria given in the first edition of the standard [11], as listed in section 3 above.

- The third part specifies 'Guidelines for security of cryptanalytic attack'. These guidelines attempt to specify the types of attack that apply to various types of cipher, including in particular asymmetric ciphers, block ciphers and stream ciphers.

Some of this wording (notably that in the third part above) will change significantly in the 3rd working draft, due to be produced by July 2012. However, it is hoped that the wording can be finalised by the end of 2012, and the revised standard published in late 2013.

Although a more specific and normative set of criteria is clearly helpful, unfortunately its effects look set to be limited to what is standardised in the future. Reducing the number of algorithms already standardised is extremely difficult unless, of course, serious vulnerabilities are discovered in any of these algorithms.

This leads naturally to a topic discussed at the meeting of SC27/WG2 held in Stockholm in May 2012, namely criteria for the *removal* of algorithms from standards. The criteria we have developed to date only apply to the inclusion of new algorithms. Clearly any criteria for removal need to be rather different. That is, whilst imperfections in algorithms may preclude their adoption as new schemes, if such imperfections are discovered after standardisation then they are unlikely to necessitate removal of the algorithm from the standard unless there are potential practical security implications. For example, triple DES is standardised in ISO/IEC 18033-3;

although it has known shortcomings, it nevertheless continues to offer useful level of security in practice (if used with care) and hence has not been removed from ISO/IEC 18033-3, at least for the time being. It is hoped that, during 2012, criteria for removal can be developed and added to the draft of ISO/IEC 18033-1. This should clarify the procedures for managing standardised algorithms.

More generally, whilst clarified and strengthened criteria will be of value in managing the portfolio of standardised algorithms, they are certainly not a panacea. The criteria need to be applied rigorously and with appropriate care. Moreover, since no criteria are bullet-proof, the process relies on national member bodies of ISO/IEC, and their delegates to SC7/WG2 meetings, exerting some discipline and self-restraint in the schemes that they propose for standardisation. In the past, it appears that some algorithms have been proposed for reasons more of personal or national pride, rather than because anyone expects them to be widely used. It could be argued that the committee needs to be more robust when addressing national proposals.

Finally, whatever the final results of the deliberations are, it is to be hoped that the results are of wider applicability than simply to ISO/IEC encryption algorithm standards. We have focussed on encryption here simply because this is where some of the greatest problems have been encountered to date, and because this is the area that SC27 is currently wrestling with. There are two obvious areas in which such criteria (perhaps suitably modified) could be applied. Firstly, there are a variety of standards covering cryptographic techniques other than encryption, e.g. digital signature and MAC algorithms, where very similar problems of algorithm proliferation have arisen. Secondly, it would be interesting if other standardisation bodies could consider whether they too might take steps to reduce the number of cryptographic techniques that they standardise.

6 Concluding remarks

As we have discussed, to maximise interoperability and make life as simple as possible for developers, the smallest possible number of algorithms should be standardised; however, despite this, there seems to be an inexorable growth in the number of standardised algorithms. This problem has been put into historical context, and recent efforts to put in place procedures to limit the number of standardised algorithms have been reviewed.

The problem is clearly a difficult one, and a complete solution has not yet been devised. Inputs are sought to the evolving effort to develop criteria for the adoption and retention of standardised cryptographic algorithms.

References

[1] M. Curtin and J. Dolske. A brute force seach of DES keyspace. *;login: — The Magazine of the USENIX Association*, May 1998. also available from `http://www.interhack.net/pubs/des-key-crack/`.

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

[3] W. Diffie and M. Hellman. Exhaustive cryptanalysis of the NBS data encryption standard. *IEEE Computer*, 10(6):74–84, June 1977.

[4] J. Gilmore. *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design*. O'Reilly, 1998.

[5] IEEE Standards Association, US. *1363-2000 — IEEE Standard Specifications for Public-Key Cryptography*, 2000.

[6] IEEE Standards Association, US. *1363a-2004 — IEEE Standard Specifications for Public-Key Cryptography — Amendment 1: Additional Techniques*, 2004.

[7] IEEE Standards Association, US. *1363.1-2008 — IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices*, 2008.

[8] IEEE Standards Association, US. *1363.2-2008 — IEEE Standard Specification for Password-Based Public-Key Cryptographic Techniques*, 2008.

[9] International Organization for Standardization, Genève, Switzerland. *ISO/IEC 9979: 1999, Information technology — Security techniques — Procedures for the registration of cryptographic algorithms*, 2nd edition, 1999.

[10] International Organization for Standardization, Genève, Switzerland. *ISO/IEC JTC1/SC27 N2723, ISO/IEC 1st WD 18033-1, Information technology — Security techniques — Encryption Algorithms — Part 1: General*, February 2001.

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

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

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

[14] International Organization for Standardization, Genève, Switzerland. *ISO/IEC JTC1/SC27 N7629, Russian NB NWI Proposal on Amendment 1 to ISO/IEC 18033-3:2005*, April 2009.

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

[16] International Organization for Standardization, Genève, Switzerland. *ISO/IEC JTC1/SC27 N9167, Report of the 41st meeting of SC 27/WG 2*, November 2010.

[17] International Organization for Standardization, Genève, Switzerland. *ISO/IEC JTC1/SC27 N9332, ECRYPT II liaison statement regarding ECRYPT II position on stream ciphers*, September 2010.

[18] International Organization for Standardization, Genève, Switzerland. *ISO/IEC JTC1/SC27 N9429, Call for contributions (questionnaire) to the SC 27/WG 2 study period on criteria for the standardization of encryption algorithms*, October 2010.

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

[20] International Organization for Standardization, Genève, Switzerland. *ISO/IEC DIS 29192-4, Information technology — Security techniques — Lightweight cryptography — Part 4: Mechanisms using asymmetric techniques*, December 2011.

[21] International Organization for Standardization, Genève, Switzerland. *ISO/IEC JTC1/SC27 N10130, Summary of voting on document SC 27 N10068 — A 60-day letter ballot on Russian block cipher GOST*, August 2011.

[22] International Organization for Standardization, Genève, Switzerland. *ISO/IEC JTC1/SC27 N10427, Text for ISO/IEC 2nd WD 18033-1 (Revision)*, December 2011.

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

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

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

[26] T. Isobe. A single-key attack on the full GOST block cipher. In A. Joux, editor, *Fast Software Encryption — 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13–16, 2011, Revised Selected Papers*, volume 6733 of *Lecture Notes in Computer Science*, pages 290–305. Springer-Verlag, Berlin, 2011.

[27] C. H. Meyer and S. M. Matyas. *Cryptography: A new dimension in computer data security.* John Wiley and Sons, New York, 1982.

[28] National Institute of Standards and Technology (NIST), Gaithersburg, MD. *Federal Information Processing Standards Publication 46-3 (FIPS PUB 46-3): Data Encryption Standard*, October 1999.

[29] National Institute of Standards and Technology (NIST), Gaithersburg, MD. *Federal Information Processing Standards Publication 197 (FIPS PUB 197): Specification for the Advanced Encryption Standard (AES)*, November 2001.

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

[31] K. Petkov. Overcoming programming flaws: Indexing of common software vulnerabilities. In *InfoSecCD '05: Proceedings of the 2nd annual conference on Information security curriculum development*, pages 127–134. ACM, New York, 2005.

[32] A. S. Tanenbaum. *Computer Networks.* Prentice-Hall PTR, 4th edition, 2007.

[33] I. A. Zabotin, G. P. Glazkov, and V. B. Isaeva. *GOST: Gosudarstvennyi Standard 28147-89: Cryptographic Protection for Data Processing Systems: Cryptographic Transformation Algorithm.* Government Committee of the USSR for Standards, 1989.