IEEE P1363.1 pre-sponsor-ballot comments

Contents

1. IEEE Mandatory Editorial Coordination Letter

```
> -----Original Message-----
> From: L.Perry@ieee.org [mailto:L.Perry@ieee.org]
> Sent: Monday, August 25, 2008 11:50 AM
> To: Whyte, William
> Cc: M.Zaman@ieee.org
> Subject: IEEE P1363.1/D10: Mandatory Editorial Coordination
>
>
> William,
>
> Attached to this e-mail, please find the pre-ballot Mandatory Editorial
> Coordination (MEC) review of P1363.1/D10.  The required legal changes
> has been incorporated into the attached document.
>
> Please note that the items in SECTION I need to be addressed before the
> document can move to Sponsor ballot.  These items include changes to
> the following:
>
>
> *    Copyright statement
> *    Matching the draft title to the PAR
>
>
> Please take note of the third ACTION item listed under Normative
> references and bibliography in SECTION II.  Although these changes are
> not required before the start of the ballot, you will need to clarify
> and cite normative references in text before completing your ballot (so
> it is best to do this now).
>
> As you will see in the attached MEC document, I sometimes refer to
> specific clauses/subclauses of the 2007 version of the IEEE Standards
> Style Manual. For your reference, you can access the style manual at
> the following URL:
> http://standards.ieee.org/guides/style/2007_Style_Manual.pdf
> <http://standards.ieee.org/guides/style/2007_Style_Manual.pdf> .
```

>
> Please share with me any questions that you have regarding the MEC.
> Otherwise, an IEEE-SA editor will again review the draft once it is at
> Sponsor ballot.
>
> Best regards,
>
> Lisa

25 August 2008

RE: Pre-ballot Mandatory Editorial Coordination (Pre-ballot MEC) of P1363.1/D10

Dear William:

I have reviewed Draft 10 of IEEE P1363.1™, and I have the following comments. Please note that this review has been organized into three sections and uses the "language of standards" to communicate necessary requirements (shall) of the IEEE-SA standards process versus those issues that are voluntary (should) in nature.

Section I: Items/issues that *shall* be resolved before the ballot begins

The draft cannot be balloted or recirculated until these issues are resolved. Your Staff Liaison will review the updated draft for compliance prior to upload of the PDF for ballot.

Section II: Items/issues that *shall* be resolved before the final recirculation

These issues have to be resolved and viewed by balloters. The items will be checked for completion by the Project Editor during the Sponsor ballot, then checked by the Review Committee (RevCom) of the IEEE-SA Standards Board (IEEE-SASB), and will impact approval unless rectified.

Section III: Recommended changes

Recommended changes may be editorial or format-related. Although these changes are unlikely to impact approval of the project by the IEEE-SASB, they represent the next steps that your Staff Editor will make in the preparation of your draft for publication. This information may be useful to you, particularly if you are going to go through a recirculation ballot or otherwise need to edit your draft.

Working groups who wish to have a draft that is very close to the published document may want to implement these changes. However, the comments should not affect the approval of the standard.

Please note that professional editing takes place once the document has been approved and, as such, this MEC does not address all of the editorial items that will be reviewed then (i.e., punctuation, grammar, formatting).

The following comments are derived from the *IEEE Standards Style Manual*. The complete *IEEE Standards Style Manual*, in viewable/downloadable format, can be found at:

http://standards.ieee.org/guides/style/2007_Style_Manual.pdf

SECTION I: Items/issues that *shall* be resolved before the ballot begins

Copyright permissions

ACTION: If any figures, tables, or text were derived or obtained from sources other than the Working Group itself, please obtain and supply copyright permission from the appropriate sources.

- If applicable, all copyright permission for excerpted text, tables, and figures shall be submitted to the IEEE prior to the start of ballot. If there are missing permission response letters, please submit them immediately to me (l.perry@ieee.org).

  Prior to sending them to me, please ensure that the following are included in each response letter you obtain from the copyright owner:

  - The permission response is on company letterhead (where applicable) or the original email from the copyright owner should be forwarded to me if the individual is the copyright owner (rather than a company)
  - Permission has to be granted
    - For world rights use of the material in the standard (either modified or unmodified, as requested by you)
    - To modify and reprint in all future revisions and editions of the standard
    - For use in all media known or hereinafter known

  If the above information is not included in the response letters sent to you, you will need to request revised letters from the copyright owner. Please inform me if the copyright owner does not agree to grant permission for these items.

  Sample permission request and response letters are available at the following Internet location:

  http://standards.ieee.org/guides/style/annexd.html

Copyright statement

ACTION: Replace "<year>" with "2008" in the copyright statement on the first page and also in the footer at the bottom of each page.

Draft title

ACTION: Please revise the title as shown on the PAR. (Change the title globally by using the Required Info button on the IEEE Word template toolbar.)

- The draft title shall match the title on the latest Project Authorization Request (PAR) form found at http://standards.ieee.org/board/nes/approved.html.

  "Draft Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices"

SECTION II: Items/issues that *shall* be resolved before the final recirculation

Legal review

Comment [LMP1]:

ACTION: Draft 10 of IEEE P1363.1 was submitted for legal review. The required changes follow this paragraph. **You may incorporate the legal comments either 1) before balloting or 2) after the start of balloting, which will require a recirculation of the resulting legal changes.**

Required Revisions

Definition 3.92 – Statistically Unique

Please revise the second sentence (page 8) as follows to avoid providing a "guarantee:"

"… the process that governs the selection of this element is such ~~provides a guarantee~~ that, for any integer ..."

Clause 4.4 – Algorithm specification conventions

Please revise the penultimate sentence of this clause (page 12, line 8) as follows to avoid the use of the absolute term "always:"

"… perform the operations using any sequence of steps that consistently ~~always~~ produces the same output as the sequence in this standard."

Clause 8.3 – Encoding Methods (page 24, line 18)

Please revise the first sentence to avoid an unnecessary "guarantee:"

"Before a message is encrypted, it must be processed to provide ~~guarantee~~ certain desirable security properties ..."

Clause A.1.4 – Lattice Reduction Algorithms

Please remove the "guarantee" language as follows (page 40, line 25):

"... runs in polynomial time and ~~is guaranteed to~~ returns a nonzero vector ..."

and (page 40, line 29)

"The BKZ-LLL algorithm with block size ß ~~is guaranteed to~~ finds a nonzero vector ..."

Clause A.3.4.2 – Combinatorial Strength in the hybrid case (page , line)

Please revise line 24 on page 50 as follows to avoid unnecessary suggestion of absolute safety:

"However, to protect ~~for safety~~ against an improved reduction algorithm that would let an attacker ..."

Trademarks or service marks

ACTION: Please address the use of trademarks in the draft, if applicable.

- References to commercial equipment or products in a standard shall be generic and shall not include trademarks or other proprietary designations. Where a sole source exists for essential equipment or materials, it is permissible to supply the name of the trademark owner in a footnote. The proper use guidelines for trademarks shall be determined by the trademark owner. Trademark owners must grant written permission before their trademarks may be referenced in a standard.

Registration objects

ACTION: Please address the registration of objects, if applicable.

- If the draft contains a registration of objects (for additional information, visit the IEEE Standards Web site at http://standards.ieee.org/regauth/index.html), the working group shall submit the document to the IEEE Registration Authority (IEEE-RA) for mandatory coordination (submit to a.n.weaver@ieee.org for review). The text containing the registration information should be highlighted in the draft and the clause should be noted in the email. If the working group believes that the draft may potentially contain a registration of objects or if the working group would like information about setting up a registration, contact the IEEE-RA as early as possible to prevent a delay in approval by the IEEE-SA Standards Board.

Patents

ACTION: I noticed that the base document, IEEE Std 1363-2000 has patent letters of assurance (LoA) on file. Does a patent LoA exist for this standard? If so, then 1) the LoA should be provided to the PatCom administrator (patcom@ieee.org) as soon as possible and 2) the patents paragraph shall be replacing with the following text:

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. A patent holder or patent applicant has filed a statement of assurance that it will grant licenses under these rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses. Other Essential Patent Claims may exist for which a statement of assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Verbs (shall, must, will)

ACTION: A text search resulted in the following: 29 instances of *shall*, 35 instances of *must*, and 63 instances of *will*. **Please review usage of the verbs detailed below and address accordingly. Consider changing *must* to *shall* where appropriate** (see 13.1 of the *IEEE Standards Style Manual* for more information).

- Standards are documents with mandatory requirements and are generally characterized by the use of the verb ***shall***.

  "The word ***shall*** is used to indicate mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (**shall** equals **is required to**).

  The use of the word ***must*** is deprecated and shall not be used when stating mandatory requirements; ***must*** is used only to describe unavoidable situations.

  The use of the word ***will*** is deprecated and shall not be used when stating mandatory requirements; ***will*** is only used in statements of fact."

Normative references and bibliography

ACTION: Please update the text that introduces the normative reference clause with the following paragraph (For more information about references, see 10.4.2 of the *IEEE Standards Style Manual*.):

> "The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated referenced, the latest edition of the referenced document (including any amendments or corrigenda) applies."

ACTION: **Please consider the dates of the publications.** (For more information about references, see 10.4.2 of the *IEEE Standards Style Manual*.)

- Dated and/or undated references are allowed in standards. Using undated references helps eliminate the burden of continuous updates to align standards as they are revised, while ensuring that the most up-to-date information on technologies and statutes is referenced (when appropriate). Dated references can be used in certain circumstances, such as when a high degree of specificity is needed (e.g., when citing tables, figures, and text of a normative reference). (See 10.4.1 of the *IEEE Standards Style Manual*.)

ACTION: **The normative references are not cited within the body of the document.** Please consider that documents listed in the references clause shall also be cited within the body of the document. If references are not cited normatively, they should be stored in an informative bibliography (annex).

- Citation as a normative references

  “References are those normative documents that contain material that must be understood and used to implement the standard. Thus, referenced documents are indispensable when applying the standard. Each reference shall be cited, and the role and relationship of each referenced document shall be explained in the body of the standard. (See 10.4.1 of the *IEEE Standards Style Manual.*)

Graphics

ACTION: **Please ensure that the backgrounds of the figures that you submit are as light as possible.**

ACTION: Please consider that figures should be black and white. **If the figures are in color, the color must not be required for proper interpretation of the figures since the print-version of the standard will print in black and white.** (See existing Figure 5 through Figure 8 of Annex A)

ACTION: Please include a legend, if necessary for interpretation, for existing Figure 5 in Annex A.

ACTION: Please supply the graphics as TIFF files that are separate from the Word document. If possible please also supply the source file for the graphics. (In other words, please supply the figure in the native file format from the program where it was created. We will archive this file so it is available for future updates to the standard.)

Mathematical expressions

ACTION: **Please ensure consistency in the presentation of equations and math in text** (see 17.3 of the *IEEE Standards Style Manual*). **For example, in item i3) through i7) of Algorithm 16, change** $\mathrm{i}_{\mathrm{cur}}$ **to** i_{cur}**.**

- The general rules regarding the use of upright and italic text in equations are as follows:

  — Quantity symbols (including the symbols for physical constants), subscripts or superscripts representing symbols for quantities, mathematical variables, and indexes are set in italic text.

  — Unit symbols, mathematical constants, mathematical functions, abbreviations, and numerals are set in upright text.

ACTION: **Change multidots and asterisks to multiplication signs in equations and inline math (e.g, see 3.6 birthday paradox and the Note of 7.3.1)** (see 17.3 of the *IEEE Standards Style Manual*)**.**

- A multiplication sign (×), rather than the letter “x” or a multidot (·), should be used to indicate multiplication of numbers and numerical values, including those values with units (e.g., 3 cm × 4 cm).

Definitions

ACTION: **Some terms are not actual definitions, e.g., 3.53 lattice-based polynomial public key encryption, and should be moved into an acronyms and abbreviations subclause as 3.2** (see 10.6 of the *IEEE Standards Style Manual*)**.**

- If the standard makes extensive use of acronyms or abbreviations, a subclause within the definitions clause may be provided. If acronyms and abbreviations are included in the definitions clause, the clause title should be “Definitions, acronyms, and abbreviations.” Subclauses 3.1 and 3.2 would be titled “Definitions” and “Acronyms and abbreviations,” respectively.
- The acronyms and abbreviations subclause is not meant to take the place of the definitions clause. If a definition is needed, the term should be added to the definitions clause as well. Acronyms and abbreviations, followed by the full term only, should be listed in alphanumeric order.

ACTION: If adding subclause 3.2, perhaps you can integrate some of the abbreviated terms from the informal table of existing 5.1.

Please note that additional corrections to the *normative references* and *bibliography, mathematical expressions, definitions, and table/figure numbering* are listed in Section III.

SECTION III: Recommended changes

Internet citations

ACTION: **Please move all non-IEEE URLs to footnotes** (e.g., reference to http://csrc.nist.gov/CryptoToolkit/Hash.html). We cannot guarantee that these URLs will always work, so per style, outside URLs are placed in footnotes rather than the normative part of the standard. The URL should be the most stable location whenever possible to avoid inadvertent or intentional changes that would affect the site name, i.e., you would use the index to the page rather than the page itself.

Definitions

ACTION: **Reword 3.80 salt size to the following rule:**

- Each definition should be a brief, self-contained description of the term in question and shall not contain any other information, such as **requirements** and elaborative text.

ACTION: **In 3.27 encryption primitives, reword according to the following rule:**

- The term should not be used in its own definition.

Table/figure numbering

ACTION: **Tables and figures should be referenced in text by the words *Table* or *Figure* and their numbers only** (e.g., “see Table 1”).

ACTION: **Renumber figures and tables appropriately in Annex A of the draft (e.g., the first figure in Annex A should be identified as “Figure A.1”).**

- Figures included in annexes should carry the identifying letter of the annex in which they appear, followed by a period.

Normative references and bibliography

ACTION: **Please add *The Authoritative Dictionary of IEEE Standards Terms* to the bibliography.**

ACTION: **Review bibliographic citations in text.**

- In text, bibliographical references should be referenced using the author’s name, organization, or product designation followed by the bibliography number in square brackets. For example,

> See Cantone et al. [B1] or see *Handbook of Standard Terminology for the Power Sources Industry* [B4] or see IEEE Std C37.23™-2003 [B20].

Mathematical expressions

ACTION: **If appropriate, please number equations in the draft according to the following rules** (see 17.2 of the *IEEE Standards Style Manual*):

- If the standard contains more than one equation, then equations of key importance should be numbered consecutively in parentheses at the right margin. Derivations of equations or examples where values are substituted for variables need not be numbered.
- An equation should be cited in the text by the word *Equation* and its number only [e.g., "see Equation (1)"], unless given in an annex [e.g., "see Equation (A.1)"].

ACTION: **In item i) of Algorithm 17, should the ">=" be changed to "≥"?**

ACTION: **Is there a reason for the unformatted math in existing Table 2 through Table 13? If not, please make the math consistent with the rest of the draft.**

Body clause numbering in text (see 11.1 of the *IEEE Standards Style Manual*):

- Clauses and subclauses should be divided into further subclauses only when there is to be more than one subclause. In other words, clauses and subclauses should not be broken down into further subclauses if another subclause of the same level does not exist. For example, Clause 1 should not have a subclause 1.1 unless there is also a subclause 1.2.

ACTION: **Consider combining clause/subclause titles to avoid the hanging subclause of 5.1.** For example, 5. Mathematical conventions—Notation and abbreviated terms.

ACTION: **Consider changing 8.3 as follows to avoid the hanging paragraph and subclause:**

> **8.3 Encoding Methods**
>
> **8.3.1 General**
>
> Before a message is encrypted, it must be processed to guarantee certain desirable security properties such as semantic security. In this clause, the auxiliary methods for manipulating data for the encryption scheme are listed. These currently consist of specific methods for generating the blinding polynomial r.
>
> **8.3.2 Blinding Polynomial Generation Methods (BPGM)**
>
> **8.3.2.1 General**
>
> In order to provide plaintext awareness, a blinding polynomial generation method (BPGM) shall be used to generate a blinding polynomial r from the padded message pm. This clause contains two BPGMs. The first utilizes the standard polynomial convolution method, and the second utilizes the optimized polynomial convolution method.
>
> **8.3.2.2 lbp-bpgm-3**
>
> The blinding polynomial r shall be generated deterministically from the message m and the random value b using a pseudo-random number generator.

General style

ACTION: **Move the names of contributors to the draft in the Introduction to appear after the working group list in the Participants section.**

ACTION: I reviewed the base document (IEEE Std 1363-2000) and algorithms are not numbered. **Delete algorithm numbering. Also format the algorithms in text instead of in text boxes.**

ACTION: For future standards, please use the document template found on the IEEE Standards website, which contains the correct IEEE copyright notice:

http://standards.ieee.org/resources/development/writing/templates.html

Please note that the following are next steps for this project.

a) After you have implemented this review, create the PDF that will be used for ballot (remember that the draft number shall be rolled to reflect that changes have been made to this document, e.g., P1363.1™/Dx+1).

b) Upon completion of the invitation to ballot, upload the PDF that will be used for ballot to http://standards.ieee.org/resources/development/balloting/startballot.html.

c) Note that compliance with items in Section I will be reviewed by the Staff Liaison when you upload the PDF to the URL in item b). The Project Editor will not review your draft until the Ballot MEC, which occurs during the Sponsor ballot review.

d) The RevCom MEC will occur after you submit the final balloted draft to RevCom. At that time you will also be required to submit the document source file. If the figures are not native FrameMaker graphics, each graphic shall be submitted as a separate TIFF file following the requirements outlined in Clause 16 of the *IEEE Standards Style Manual.*

Thank you for the opportunity to review this draft. If you have any queries about the comments in this mandatory editorial coordination, please contact me via email (l.perry@ieee.org).

Best regards,

Lisa Perry
Project Editor
IEEE Standards Association

cc: Malia Zaman
Program Manager, Technical Program Development

2. 1363.1 editor’s response to IEEE MEC

Hi Lisa,

Thanks for the MEC feedback. Here are my comments / responses. Please find attached copies of 1363.1 that implement those comments that I've had time to implement so far: one copy is clean, one is change-tracked.

SECTION 1:

ACTION: If any figures, tables, or text were derived or obtained from sources other than the Working Group itself, please obtain and supply copyright permission from the appropriate sources.

RESPONSE: no figures, tables or text were derived from sources other than the Working Group.

ACTION: Replace “<year>” with “2008” in the copyright statement on the first page and also in the footer at the bottom of each page.

RESPONSE: I've done this, but I recommend that in future versions of the template this is done automatically.

ACTION: Please revise the title as shown on the PAR.

RESPONSE: The PAR says "Draft Standard Specification for <title>". The draft says "Draft Standard for <title>". I'm happy to change the title of the draft to the one specified in the PAR, but I note that the PAR title doesn't conform to current IEEE convention (ie, current convention is simply "Draft Standard for", while the document is "Draft Standard Specification for"). Will this cause trouble at RevCom and should we instead change the PAR?

==========================

SECTION 2:

Legal review:

I accept all comments. I have implemented all suggested changes exactly, with the exception of the following:

Clause 4.4 – Legal review suggested
“… perform the operations using any sequence of steps that consistently produces the same output as the sequence in this standard.”

I have instead written
“… perform the operations using any sequence of steps that produces the same output as the sequence in this standard.”

Trademarks or service marks:

The only trademarks or service marks that we are aware of appear in the titles of papers in the bibliography. We have given these paper titles verbatim; ie, in these paper titles the trademarks have no "TM" or "(R)" attached, and we have not added TM or (R) in the bibliography.

Registration of objects:

There is no registration of objects.

Patent LoA:

NTRU Cryptosystems, Inc., needs to provide a LoA. We will provide this shortly.

I have modified the document as requested.

Verbs:

I have ensured that all musts refer to unavoidable situations (except for the musts that appear in the IEEE boilerplate at the front of the document).

One "will" appears in the Purpose -- is this acceptable or should we change the Purpose?

Other than that, I have eliminated the use of "will" other than in statements of fact.

Normative references and bibliography:

I have changed the references to undated.

I'm not sure how to reference normative references. My understanding is:
* Normative references are listed in Clause 2
* They are also listed in the bibliography
* In the standard text, they are also referred to by their bibliography number.

I've tried to conform to this. If I could make a suggestion, I think it would be easier to understand if the bibliography reference appeared in Clause 2 alongside the name of the normative reference, e.g.

  FIPS 180, Name of document, [B22]

That makes it easier for a reader to cross-reference and determine if a reference is normative or informative.

Graphics: I will resolve these before submission to RevCom.

Mathematical expressions: I will resolve these before submission to RevCom.

Definitions:

ACTION: Some terms are not actual definitions, e.g., 3.53 lattice-based polynomial public key encryption

Response: I have rephrased 3.53 so that it is a definition. It'd be useful if you could identify the other terms that you consider not to be definitions.

ACTION: If adding subclause 3.2, perhaps you can integrate some of the abbreviated terms from the informal table of existing 5.1.

Response: This seems like a good idea. I moved the acronyms from the table in 5.1 to a new clause 3.2, and kept only the mathematical notation in 5.1.

=========

RECOMMENDED CHANGES:

Internet citations: Please move all non-IEEE URLs to footnotes: Accepted and will implement before submission to RevCom.

Definitions:

ACTION: Reword 3.80 salt size...

Response: Accepted. Introduced a separate definition for "salt" and then defined "salt size" as the size of the salt.

ACTION: In 3.27 encryption primitives, reword...

Response: Accepted. Reworded.

Table/figure numbering

ACTION: Tables and figures should be referenced in text by the words Table or Figure and their numbers only (e.g., “see Table 1”).
ACTION: Renumber figures and tables appropriately in Annex A of the draft (e.g., the first figure in Annex A should be identified as “Figure A.1”).

Response: Accepted. Will implement before submission to RevCom.

Normative references and bibliography:

ACTION: Please add The Authoritative Dictionary of IEEE Standards Terms to the bibliography.

Response: Accepted

ACTION: Review bibliographic citations in text.

Response: Accepted. Will implement before submission to RevCom.

Mathematical expressions:

ACTION: If appropriate, please number equations in the draft according to the following rules

Response: Accepted. Will implement before submission to RevCom.

ACTION: In item i) of Algorithm 17, should the “>=” be changed to “≥”?

Response: Accepted.

ACTION: Is there a reason for the unformatted math in existing Table 2 through Table 13? If not, please make the math consistent with the rest of the draft.

Response: There is no reason for the unformatted math. I've fixed this.

Body clause numbering in text:

ACTION: Consider combining clause/subclause titles to avoid the hanging subclause of 5.1.

Response: Agree.

ACTION: Consider changing 8.3 as follows to avoid the hanging paragraph and subclause [...]

Response: Agree.

General style:

ACTION: Move the names of contributors to the draft in the Introduction to appear after the working group list in the Participants section.

Response: Agree, implemented.

ACTION: I reviewed the base document (IEEE Std 1363-2000) and algorithms are not numbered. Delete algorithm numbering. Also format the algorithms in text instead of in text boxes.

Response: Agree, implemented.

ACTION: For future standards, please use the document template found on the IEEE Standards website, which contains the correct IEEE copyright notice

Response: Will do.

Cheers,

William

3. Comments from Paulo Barreto

I'd like to point out a few things that need attention in the current draft should the project go on.

1. Section 2, line 9: the current version of the ISO/IEC standard is ISO/IEC 10118-3:2004, and the NIST standard has a new draft, FIPS 180-3, since June 2007.

2. Section 3.92, line 14: the final equation "L)!nL .˜to n!(n" is rather unclear.

3. Section 6.3.3.4, algorithm 4: the ring name should be Z_p[X]/(X^N - 1), not Zp[X]/(XN – 1).

4. Reference FIP95 occurs several times, but is not defined.

5. The tern "trinary" seems somehwat unusual compared to "ternary," and in fact the dictionaries I have define the former as meaning the same as the latter (the converse is not true).

6. There seem to be inconsistencies in the treatment of binary vs. "trinary" algebraic structures; for instance, primitive OS2BREP is declared on p. 14 but not defined anywhere (to be sure, I wonder if binary rings are actually used), and the handling of ternary quantities is mixed with higher-level operations like encryption and decryption rather than confined to dedicated primitives.

Best regards,

Paulo Barreto.

4. 1363.1 editor’s response to Paulo Baretto

Hi Paulo,

Thanks for the notes. Here are some responses:

> 1. Section 2, line 9: the current version of the ISO/IEC standard is
> ISO/IEC
> 10118-3:2004, and the NIST standard has a new draft, FIPS 180-3, since
> June 2007.

Yes: We don't need to refer to 10118, and IEEE recommends that we don't include version numbers on normative references, so I've changed the reference to simply be to FIPS 180 (with most up-to-date version number implied).

> 2. Section 3.92, line 14: the final equation "L)!nL .˜to n!(n" is
> rather unclear.

I would describe it as baffling... I've removed that last sentence.

> 3. Section 6.3.3.4, algorithm 4: the ring name should be Z_p[X]/(X^N -
> 1), not
> Zp[X]/(XN – 1).

This seems to be fixed already -- I don't see the error in my copy.

> 4. Reference FIP95 occurs several times, but is not defined.

This was supposed to be a reference to FIPS-180. Fixed by putting FIPS-180 in the bibliography and referring to it by its bibliography reference.

> 5. The tern "trinary" seems somehwat unusual compared to "ternary," and
> in fact
> the dictionaries I have define the former as meaning the same as the
> latter (the
> converse is not true).

Accepted. Changed to "Ternary" throughout.

> 6. There seem to be inconsistencies in the treatment of binary vs.
> "trinary"
> algebraic structures; for instance, primitive OS2BREP is declared on p.
> 14 but
> not defined anywhere (to be sure, I wonder if binary rings are actually
> used),
> and the handling of ternary quantities is mixed with higher-level
> operations

> like encryption and decryption rather than confined to dedicated
> primitives.

I agree that this is inconsistent, and will think about whether it should be addressed. I don't think this needs to be fixed before we go to sponsor ballot.

Cheers,

William