Email This Letter

06 December 2006

Bob Davis
Summit Computer System, Inc.
22685 Summit Road
Los Gatos, CA 95033-9310
bob@scsi.com

Re: P1363.1 - Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices

Dear Bob:

I am pleased to report that on 06 December 2006 the IEEE-SA Standards Board approved the extension request of the above-referenced project until 31 December 2007.

If you should have any further questions, please contact me at +1 732 562 6003 or by email at s.hampton@ieee.org.

Sincerely,

Sherry Hampton
Administrator, Governance
Standards Activities
Phone +1 732 562 6003
FAX +1 732 875 0695
Email: s.hampton@ieee.org

CC: wwhyte@ntru.com

IEEE-SA Standards Board Extension Request

Revised 23 June 2004

1. Date of Request: 12-Sep-06

2. Assigned Project Number: P1363.1

3. Project Title: Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices
a. Name of Working Group (WG): Standard Specifications for Public-Key Cryptography
b. Name of Working Group Chair: William Whyte
c. Name of Sponsoring Society and Committee: Computer/Microprocessors and Microcomputers
d. Name of Sponsoring Committee Chair: Bob David

4. Contact Information (Contact should be the person who will answer any questions concerning this extension request):
a. Name: William Whyte
b. Telephone: +1 978 844 5208
c. FAX: +1 978 264 0103
d. EMAIL: wwhyte@ntru.com

5. Statement of why an extension is required. This should include a description of what the working group has accomplished and what remains to be accomplished, along with the reasons why the work was unable to be completed in the allotted timeframe Standard is almost complete and is currently undergoing working group ballot and sponsor ballot invitation. Completion was delayed because additional security results about the techniques in the standard had to be taken into account, requiring additional consideration.

6. History
a. What date was the PAR first approved? 7-Dec-00
b. What date did you begin writing the first draft? 7-Dec-00
c. How many people are actively working on the project? 10
d. How many times a year does the working group meet:
   1. In person? 1
   2. Via teleconference? 6
e. How many times a year is a draft circulated to the working group via electronic means? 2

7. Document Progress
a. What percentage of the Draft is stable? 98%
b. How many significant work revisions has the Draft been through? 8

8. Project Plan
(Item #8a is only for projects that have been balloted. If your draft has not yet gone to ballot, please go to Item #8b)

a. Balloting History - Provide history of all IEEE Sponsor ballots under this project::

1st Ballot Close date (or scheduled close):
1st Ballot Draft Number:
1st Ballot results (% affirmative, %negative, %abstain):

2nd Ballot Close date (or scheduled close):
2nd Ballot Draft Number:
2nd Ballot results (% affirmative, %negative, %abstain):

(Add additional entries for ballots as needed):

When do you estimate that the final IEEE Sponsor ballot will be completed?
When do you expect to submit the proposed standard to RevCom?

b. For projects that have not yet begun Sponsor ballot, please answer the following:

When will IEEE sponsor balloting begin? `1-Dec-06`
When do you estimate that the final IEEE Sponsor ballot will be completed? `1-Mar-07`
When do you expect to submit the proposed standard to RevCom? `1-Apr-07`

9. Future Adoptions

- If this is a new document, will it be adopted (in part or in whole) by another national, regional or international organization? No If yes, which organization?
- If this is a revision of an existing document, has this document been adopted by the IEC, ISO, ETSI, SCC, etc? Choose One If yes, which organization?

10. Additional Extensions

a. Is this the first request for an extension? No (If yes, please do not go any further. You have completed the form.)
b. If not, when was the previous extension approved? `8-Dec-04`

After completion of this form, please e-mail this to the NesCom Administrator at nescom-admin@ieee.org. Confirmation of submittal will be sent on receipt of this request.

Email This Letter

13 December 2004

Bob Davis
Summit Computer System, Inc.
22685 Summit Road
Los Gatos, CA 95033-9310
bob@scsi.com

Re: P1363.1 - Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices

Dear Bob:

I am pleased to report that on 08 December 2004 the IEEE-SA Standards Board approved the extension request of the above-referenced project until 31 December 2006.

If you should have any further questions, please contact me at 732-562-6367 or by email at j.haasz@ieee.org.

Sincerely,

Jodi Haasz
Program Manager
International Stds Programs and Governance
Standards Activities
Phone +1 732 562 6367
FAX +1 732 875 0695
Email: j.haasz@ieee.org

cc: wwhyte@ntru.com

IEEE-SA Standards Board Extension Request

Revised 23 June 2004

1. Date of Request: 8-Jul-04

2. Assigned Project Number: P1363.1

3. Project Title: Standard Specifications for Password-Based Public-Key Cryptographic Techniques
a. Name of Working Group(WG): P1363
b. Name of Working Group Chair: William Whyte
c. Name of Sponsoring Society and Committee: MSC
d. Name of Sponsoring Committee Chair: Bob Davis

4. Contact Information (Contact should be the person who will answer any questions concerning this extension request):
a. Name: William Whyte
b. Telephone: 508 878 4585
c. FAX: 781 418 2532
d. EMAIL: wwhyte@ntru.com

5. Statement of why an extension is required. This should include a description of what the working group has accomplished and what remains to be accomplished, along with the reasons why the work was unable to be completed in the allotted timeframe The working group has made progress in standardizing the techniques known of at the time the PAR was approved. However, new research has made it possible to obtain improved security and efficiency for the technologies under consideration. It has taken time to integrate this new research into the document, but it should be possible to move quickly in the second half of 2004 to finish the integration and move the document to ballot.

6. History
a. What date was the PAR first approved? 7-Dec-00
b. What date did you begin writing the first draft? 7-Dec-00
c. How many people are actively working on the project? 10
d. How many times a year does the working group meet:
   1. In person? 2
   2. Via teleconference? 4
e. How many times a year is a draft circulated to the working group via electronic means? 1 to 2

7. Document Progress
a. What percentage of the Draft is stable? 70%
b. How many significant work revisions has the Draft been through? 4

8. Project Plan

(Item #8a is only for projects that have been balloted. If your draft has not yet gone to ballot, please go to Item #8b)

a. Balloting History - Provide history of all IEEE Sponsor ballots under this project::

1st Ballot Close date (or scheduled close):
1st Ballot Draft Number:
1st Ballot results (% affirmative, %negative, %abstain):

2nd Ballot Close date (or scheduled close):
2nd Ballot Draft Number:
2nd Ballot results (% affirmative, %negative, %abstain):

(Add additional entries for ballots as needed):

When do you estimate that the final IEEE Sponsor ballot will be completed?
When do you expect to submit the proposed standard to RevCom?

b. For projects that have not yet begun Sponsor ballot, please answer the following:

When will IEEE sponsor balloting begin? March 2005
When do you estimate that the final IEEE Sponsor ballot will be completed? June 2005
When do you expect to submit the proposed standard to RevCom? September 2005

9. Future Adoptions

- If this is a new document, will it be adopted (in part or in whole) by another national, regional or international organization? No If yes, which organization?
- If this is a revision of an existing document, has this document been adopted by the IEC, ISO, ETSI, SCC, etc)? If yes, which organization?

10. Additional Extensions

a. Is this the first request for an extension? Yes (If yes, please do not go any further. You have completed the form.)
b. If not, when was the previous extension approved?

After completion of this form, please e-mail this to the NesCom Administrator at nescom-admin@ieee.org. Confirmation of submittal will be sent on receipt of this request.

Jodi Haasz

12/13/00 01:20 PM

To: don@lexmark.com
cc: paul@4Links.co.uk, jrosello@estec.esa.nl, asinger@ntru.com
Subject: PAR Approvals

13 December 2000

Forrest Wright
C18L/035-3
Lexmark Int'l
Dept. C14/035-3
740 New Circle Road
Lexington, KY 40511

Re	P1355.2	Standard for SpaceWire - Links, Nodes, Routers and Networks
	P1363.1	Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices
	P1363.2	Standard Specification for Password-Based Public-Key Cryptographic Techniques
	P1579	Standard for Parallel 10 Gb/s Signaling (LiteLink)

Dear Mr. Wright:

I am pleased to inform you that on 7 December 2000 the IEEE-SA Standards Board approved the above referenced projects until December 2004. Copies of the files are attached in .pdf format.

Now that your projects have been approved, please forward a roster of participants involved in the development of these projects. This request is in accordance with the IEEE-SA Operations Manual, Clause 5.1.2f under *Duties of the Sponsor* which states:

"Submit annually to the IEEE Standards Department an electronic roster of individuals participating on standards projects"

Attached is an Excel spreadsheet for your convenience. Please forward these lists to me via e-mail at j.haasz@ieee.org no later than 1 March 2001.

At the bottom of this e-mail, please find URLs which you may find useful in the development of your proposed standard and in submitting your final draft for approval. Written responses from all committees/organizations listed on the PAR as proposed coordination must be included with the final draft when it is submitted.

If coordination is effected by common membership, i.e., a person on the standard's developing committee who is also a member of the committee/organization specified on the PAR for coordination, there must be a document included with the final draft from that coordinating body which states that person is authorized to represent it. We strongly recommend that a copy of your draft be sent to this office for review prior to the final voting by the working group to allow for a quick review by the editorial staff before sponsor balloting.

If you should have any further questions or would like to receive this information in paper, please contact me at 732-562-6367 or by email at j.haasz@ieee.org.

Sincerely,

Jodi Haasz
Senior Administrator, Standards Board

PS - The information in the .pdf file is viewable in Adobe Reader, version 3.0 or higher. If you do not have this software, please go to http//www.adobe.com/prodindex/acrobat/readstep.html#reader to download the free version.

****

Standards Process-at-a-Glance
http//standards.ieee.org/resources/glance.html - A quick-reference site useful to any standards developer.

IEEE Standards Style Manual
http//standards.ieee.org/guides/style/index.html - Guidelines that establish style and format requirements for the preparation of proposed IEEE standards.

IEEE Standards Companion
http//standards.ieee.org/guides/companion/index.html - An overall view of the standards process; what to do, what to avoid, lessons learned, and sample forms.

Implement Plan for Metric Policy 9.20
http//standards.ieee.org/announcements/metric.html - Information on when, why and how the plan will be implemented and what exceptions exist.

Leading a Standards Development Group
http//standards.ieee.org/faqs/ltpres.html#q1 - A free training session offered by staff to make the most of the standards process. After attending, you will have a great understanding of

- the need for due process and consensus
- how to submit PARs and Drafts
- the "legal" aspects (copyrights, trademarks, patents)
- how staff can help you

Standards Coordinating Committee 10
http//standards.ieee.org/faqs/SCC10.html - An explanation of the importance of coordinating with the IEEE Dictionary (SCC10) as is mandated on the PAR form.

Balloting Information
http//standards.ieee.org/resources/glance_at_balloting.html


Sample Roster.xls


1355-2.pdf


1363-1.pdf


1363-2.pdf


1579.pdf

IEEE-SA Standards Board Project Authorization Request (PAR) Form (2000-Rev 1)

Note: For use with help hyperlinks offline, download guide.html and par2000.html into the same directory. **After completing and saving this form, please send the form as an e-mail attachment to the NesCom Secretary. Please don't forget to fax the signature page.**

Instructions for Downloading the PAR Form

Please click on a year to view the submittal deadlines for the year 2000 and the year 2001.

---

1. Sponsor Date of Request	2. Assigned Project Number	3. PAR Approval Date
[2000 Oct 27]	[P1363.1]	**7 December 2000**

Copyright release must be submitted with appropriate signatures by FAX (1-732-562-1571)}

[X] PAR Signature Page on File {IEEE Staff to check box}

---

4. Project Title, Recorder and Working Group/Sponsor for this Project

Document type and title: {Place an X in only one option below}

- [X] **Standard for**{document stressing the verb "shall"}
- [..] **Recommended Practice for**{document stressing the verb "should"}
- [..] **Guide for** {document in which good practices are suggested}

Title: [Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices]

Name of Working Group (WG): [IEEE P1363 Working Group]

Name of Official Reporter (usually the WG Chair) who must be an SA member as well as an IEEE/Affiliate Member: [Ari Singer]

IEEE-Standards Staff has verified that the Official Reporter (or Working Group Chair) is an IEEE and an IEEE-SA member: [X] (Staff to check box)

Contact Information:

Telephone [(781) 221-1306] FAX: [(781) 221-0117]

E-mail: [asinger@ntru.com]

Name of Working Group Chair (if different than Reporter): [...]

IEEE-Standards Staff has verified that the Working Group Chair is an IEEE and an IEEE-SA member: [...] (Staff to check box)

Contact Information:

Telephone	[...]	FAX:	[...]
E-mail:	[...]		

Name of Sponsoring Society and Committee: [Microprocessor Standards Committee (

Name of Committee Sponsor Chair: [Don Wright]

IEEE-Standards Staff has verified that the Sponsor is an IEEE and an IEEE-SA member: [X] (Staff to check box)

Contact Information:

Telephone	[(859) 232-4808]	FAX:	[(603) 963-8352]
E-mail:	[don@lexmark.com]		

---

5. Type of Project

a. Is this an update to an existing PAR? [NO]

If YES, indicate PAR Number/Approval Date [P####-YEAR]
If YES, is this project in ballot now? [yes/no]
[Indicate changes/rationale for revised PAR in Item #16. This should be no more than 5 lines.]

b. Choose one from the following:

[X] New Standard
[...] Revision of existing Standard {number and year} [...]
[...] Amendment (Supplement) to an existing standard {number and year} [...]
[...] Corrigenda to an existing standard {number and year} [...]

---

6. Life Cycle

[X] Full Use (5-year life cycle)
[...] Trial Use (2-year life cycle)

---

7. Balloting Information

Choose one from the following:

[X] Individual Sponsor Balloting
[...] Entity Sponsor Balloting
[...] Mixed Balloting (combination of Individual and Entity Sponsor Balloting)

Expected Date of Submission for Initial Sponsor Ballot: [January 2003]

---

8. Fill in Projected Completion Date for Submittal to RevCom [June, 2003]

---

9. Scope of Proposed Project:

[Specifications of common public-key cryptographic techniques based on hard problems over lattices supplemental to those considered in IEEE 1363 and IEEE P1363a, including mathematical primitives for secret value (key) derivation, public-key encryption, identification and digital signatures, and cryptographic schemes based on those primitives. Specifications of related cryptographic parameters, public keys and private keys. Class of computer and communications systems is not restricted.]

---

10. Purpose of Proposed Project:

[The transition from paper to electronic media brings with it the need for electronic privacy and authenticity. Public-key cryptography offers fundamental technology addressing this need. Many alternative public-key techniques have been proposed, each with its own benefits. The IEEE 1363 Standard and P1363a project have produced a comprehensive reference defining a range of common public-key techniques covering key agreement, public-key encryption and digital signatures from several families, namely the discrete logarithm, integer factorization, and elliptic curve families.

IEEE P1363.1 will specify cryptographic techniques based on hard problems over lattices. These techniques may offer tradeoffs in operating characteristics when compared with the methods already specified in IEEE 1363-2000 and draft P1363a. It is also intended that P1363.1 provide a second-generation framework for the description of cryptographic techniques, as compared to the initial framework provided in 1363-2000 and draft P1363a.

It is not the purpose of this project to mandate any particular set of public-key techniques or security requirements (including key sizes) for this or any family. Rather, the purpose is to provide: (1) a reference for specification of a variety of techniques from which applications may select, (2) the relevant number-theoretic background, and (3) extensive discussion of security and implementation considerations so that a solution provider can choose appropriate security requirements for itself.]

---

11. Intellectual Property {Answer each of the questions below}

Are you aware of any patents relevant to this project?

[Yes] {Yes, with detailed explanation below / No}
[As with Std 1363-2000 and its first amendment, P1363a, it is anticipated that certain techniques and methods of implementation of techniques included in P1363.1 may be covered by claims in patents and patent applications. It is the intention of the working group to seek out reasonable and non-discriminatory licensing from all parties that claim to have intellectual property rights on techniques included in P1363.1. It is also the policy of the working group (as with the IEEE) to favor non-patented techniques when equivalent to patented techniques. This treatment of patent issues is consistent with the policies implemented by the working group for Std 1363-2000 and P1363a.] {Explanation}

Are you aware of any copyrights relevant to this project?

[No] {Yes, with detailed explanation below / No}
[...] {Explanation}

Are you aware of any trademarks relevant to this project?

[Yes] {Yes, with detailed explanation below / No}
[As with Std 1363-2000 and its first amendment, P1363a, it is anticipated that there may be certain techniques included in P1363.1 that are trademarked. As before, it is the intention of the working group to either receive permission to use trademarked names or to choose technique names carefully so as not to infringe on any trademarks.] {Explanation}

Are you aware of any registration of objects or numbers relevant to this project?

[No] {Yes, with detailed explanation below / No}
[...] {Explanation}

---

12. Are you aware of any other standards or projects with a similar scope?

[No] {Yes, with detailed explanation below / No}
[...] {Explanation}

---

13. International Harmonization

Is this standard planned for adoption by another international organization?
[??] {Yes/No/?? if you don't know at this time}
If Yes: Which International Organization [...]
If Yes: Include coordination in question 15 below
If No: Explanation [...]

---

14. Is this project intended to focus on health, safety or environmental issues?

[No] {Yes/No/?? if you don't know at this time}
If Yes: Explanation [...]

---

15. Proposed Coordination/Recommended Method of Coordination

Mandatory Coordination

SCC 10 (IEEE Dictionary)	by **DR**	{Circulation of **DR**afts}
IEEE Staff Editorial Review by	by **DR**	
SCC 14 (Quantities, Units and Letter symbols)	by **DR**	

Coordination requested by Sponsor:

[..... by [...] {circulation of **DR**afts/**LI**aison memb/**CO**mmon memb} .....]

[..... by [...] {circulation of **DR**afts/**LI**aison memb/**CO**mmon memb} .....]

[..... by [...] {circulation of **DR**afts/**LI**aison memb/**CO**mmon memb} .....]

[..... by [...] {circulation of **DR**afts/**LI**aison memb/**CO**mmon memb} .....]

Coordination Requested by Others:

[...] {added by staff}

16. Additional Explanation Notes: {Item Number and Explanation}

[...]{If necessary, these can be continued on additional pages}

The PAR Copyright Release and Signature Page must be submitted by FAX to 732-562-1571 before this PAR will be sent on for NesCom and Standards Board approval.