IEEE P1363.2 Patent Solicitation Letter

October 2006

Open letter re: Patents and Trademarks for IEEE P1363 Working Group

To whom it may concern:

The IEEE P1363 working group "Standard Specifications for Public-Key Cryptography" is developing the standard IEEE P1363.2, “Standard Specifications for Password-Based Public-Key Cryptographic Techniques.” As this standard nears completion, the group requests information on any relevant patents or patent applications. Both U.S. and non-U.S. coverage is of interest.

Under IEEE policy, a working group must take steps to identify such patent coverage, and where coverage may apply, it must solicit a letter from each relevant patent holder assuring that, should optional or mandatory portions of the standard be covered by a given patent, the patent will be licensed in a reasonable and nondiscriminatory manner to users of the standard. Issuance of a standard containing material covered by patents may be delayed pending the delivery of such a letter. Specifics of the IEEE policy are given in IEEE standards documentation.

Your input is therefore requested on whether any patents or patent applications may cover any of the areas of cryptographic technology specified in the current P1363.2 draft, which is posted on http://grouper.ieee.org/groups/1363/passwdPK/index.html. (***Note: the final version of this letter will give the username and password to access the draft). Among the technologies mentioned in the draft are the following:

- Cryptographic primitives based on the discrete logarithm problem, including Diffie-Hellman secret-value derivation (DLSVDP-DH) and Diffie-Hellman secret-value derivation with cofactor multiplication (DLSVDP-DHC). The underlying finite field may be either GF(q) for an odd prime q or GF(2^m) for arbitrary m
- Cryptographic primitives based on the elliptic curve discrete logarithm problem, analogs to the set based on the discrete logarithm problem. Again, the underlying finite field may be either GF(q) for an odd prime q or GF(2^m) for arbitrary m
- Cryptographic schemes derived from the foregoing primitives, based on the use of a weak shared secret (a “password”) in a way that does not expose the secret to offline guessing attacks
- Password-authenticated key retrieval schemes
- Augmented and balanced password-authenticated key agreement schemes
- Random element derivation primitives, for obtaining pseudo-random group elements of known order
- Public key generation primitives

- Password-entangled public key generation primitives
- Secret value derivation primitives that derive a shared secret value from a combination of public and private quantities.
- Key confirmation functions
- Multiplier value creation functions
- Hash functions, including SHA-1 and RIPEMD-160.
- Modular arithmetic, including GF(p) arithmetic.
- GF(2^m) arithmetic, including normal basis representations and polynomial basis representations.
- Elliptic curve point representation, including point compression.
- Techniques described in the following publications:
  - D. Brown & R. Gallant, "The Static Diffie-Hellman Problem", November 15, 2004, preliminary version submitted to Eurocrypt 2005. Available at http://eprint.iacr.org/2004/306/.
  - S. M. Bellovin & M. Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks", Proceedings of the I.E.E.E. Symposium on Research in Security and Privacy, Oakland, May 1992.
  - S. M. Bellovin & M. Merritt, "Augmented Encrypted Key Exchange: a Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise", AT&T Bell Laboratories (c. 1994).
  - V. Boyko, P. MacKenzie & S. Patel, "Provably Secure Password Authenticated Key Exchange Using Diffie-Hellman", Advances in Cryptology - EUROCRYPT 2000, Preneel, B., (Ed.), May 14-18, 2000.
  - FIPS PUB 186-2, "Digital Signature Standard", Federal Information Processing Standards Publication 186-2, U.S. Department of Commerce/National Institute of Standards and Technology, National Technical Information Service, Springfield, Virginia, January 27, 2000 (supersedes FIPS PUB 186-1). Available at http://csrc.nist.gov/fips/.
  - Draft FIPS Draft 186-3, "Digital Signature Standard (DSS)", Federal Information Processing Standards Publication 186-2, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, March 13, 2006. (planned to supersede FIPS PUB 186-2).
  - W. Ford & B. Kaliski, "Server-Assisted Generation of a Strong Secret from a Password", Proceedings of the IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, NIST, Gaithersburg MD, June 14-16, 2000.
  - C. Gentry, P. MacKenzie and Z. Ramzan, "PAKZ+", Contribution to the IEEE P1363 Working Group, August 15, 2005. Available at http://grouper.ieee.org/groups/1363/passwdPK/contributions.html#GMR05b.
  - D. Jablon, "Password Authentication Using Multiple Servers", LNCS 2020: Topics in Cryptology -- CT-RSA 2001, April 8-12, 2001 Proceedings, pp. 344-360, 2001, Springer-Verlag.

- D. Jablon, “Strong Password-Only Authenticated Key Exchange”, Computer Communication Review, ACM SIGCOMM, vol. 26, no. 5, pp. 5-26, October 1996.
- D. Jablon, “Extended Password Key Exchange Protocols Immune to Dictionary Attacks”, Proceedings of the Sixth Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET-ICE ’97) IEEE Computer Society, June 18-20, 1997, Cambridge, MA, pp. 248-255.
- D. Jablon, “B-SPEKE”, Integrity Sciences white paper, September 1, 1999, available at www.integritysciences.com until early 2001.
- D. Jablon, “The SPEKE Password-based Key Agreement Methods”, draft-jablon-speke-02.txt, IETF Internet Draft, October 23, 2003.
- D. Jablon, “SRP-4”, a P1363.2 submission to the IEEE P1363 Working Group, May 9, 2002.
- B. Kaliski, “PKCS #5: Password-Based Cryptography Specification Version 2.0”, IETF RFC 2898, September 2000.
- T. Kwon, “Ultimate Solution to Authentication via Memorable Password”, May 30, 2000. Submission to the IEEE P1363 Working Group, received June 22, 2000. Available at http://grouper.ieee.org/groups/1363.
- T. Kwon, “Authentication and Key Agreement via Memorable Password”, NDSS 2001 Symposium Conference Proceedings, February 7-9, 2001.
- T. Kwon, “Authentication via Memorable Passwords — Revised Submission to IEEE P1363.2”, Submission to the IEEE P1363 Working Group, received October 31, 2002. Available at http://grouper.ieee.org/groups/1363.
- T. Kwon, “Summary of AMP (Authentication and key agreement via Memorable Passwords)”, Contribution to the IEEE P1363 Working Group, received August 22, 2003. Available at http://grouper.ieee.org/groups/1363.
- T. Kwon, “Addendum to Summary of AMP”, Submission to the IEEE P1363 Working Group, received November 20, 2003. Available at http://grouper.ieee.org/groups/1363/passwdPK/contributions.
- T. Kwon, “Revision of AMP in IEEE P1363.2 and ISO/IEC 11770-4”, Contribution to IEEE P1363 Working Group, received June 8, 2005. Available at http://grouper.ieee.org/groups/1363.
- P. MacKenzie, “More Efficient Password-Authenticated Key Exchange”, LNCS 2020: Topics in Cryptology -- CT-RSA 2001, April 8-12, 2001 Proceedings, pp. 361-377, 2001, Springer-Verlag.
- P. MacKenzie, “The PAK suite: Protocols for Password-Authenticated Key Exchange”, a P1363.2 submission to the IEEE P1363 Working Group, April 24, 2002.
- P. MacKenzie, “The PAK Suite: Protocols for Password-Authenticated Key Exchange”, DIMACS Technical Report 2002-46, October 2002.
- R. Perlman & C. Kaufman, “Secure Password-Based Protocol for Downloading a Private Key”, Proceedings of the 1999 Network and Distributed System Security, February 3-5, 1999.

- M. Scott, “MIKE - Mike's Integrated Key Exchange”, Dublin City University, School of Computing, Working Paper CA-1300, November, 2000.
  Available at
  http://www.computing.dcu.ie/research/CA_Working_Papers/wp00.html#1300.
- Y. Wang, “IEEE P1363.2 Submission / D2001-06-21”, [P1363.2-ecsrp-06-21.doc] A contribution by Yongge Wang for P1363.2 giving an elliptic curve version of the SRP protocol, June 21, 2001.
- T. Wu, “The SRP Authentication and Key Exchange System”, IETF RFC 2945, September 2000.
- T. Wu, “SRP-6: Improvements and Refinements to the Secure Remote Password Protocol”, Submission to IEEE P1363 Working Group, October 29, 2002.
- T. Wu, “The Secure Remote Password Protocol”, Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium, San Diego, March 1998, pp. 97-111.

If it is your position that patents or patent applications (either yours or others) cover one of these areas of cryptographic technology, please provide that input to the working group. In the case that patent coverage may apply, the working group will request a letter giving required patent assurances to IEEE. If you have already replied to a previous solicitation by the working group and your position has not changed, it is not necessary to reply again.

The mention of a technology in the standard does not necessarily require a letter giving patent assurances to IEEE. For instance, if a patent covers a particular implementation of a technology (for instance, a specific implementation of modular arithmetic), but the standard does not normatively specify the covered implementation, then patent assurances may not be necessary. However, in the interests of completeness, it would be helpful for the working group to know about the patent.

Input on patent *non-coverage* will also be helpful. If it is your position that no patents or patent applications (either yours or others) cover a particular area of cryptographic technology, please provide that input to the working group. You would of course retain the right later to take a different position, should other information become available. Please be aware that the working group's current draft standard is not yet an IEEE standard and is subject to change.

The working group also requests information about any trademarks that may cover the names of techniques that are defined, used, or mentioned in the standard, which currently include the following:

- PPK, BPKAS-PPK
- PAK, BPKAS-PAK

— SPEKE, BPKAS-SPEKE
— AMP, APKAS-AMP
— BSPEKE,
— BSPEKE2, APKAS-BSPEKE2
— WSPEKE, APKAS-WSPEKE
— PAKZ, APKAS-PAKZ
— SRP,
— SRP3, APKAS-SRP3
— SRP5, APKAS-SRP5
— SRP6, APKAS-SRP6
— PKRS-1,
— DLAPKAS-AMP-CLIENT
— DLAPKAS-AMP-SERVER
— DLAPKAS-BSPEKE2-CLIENT
— DLAPKAS-BSPEKE2-SERVER
— DLAPKAS-PAKZ-CLIENT
— DLAPKAS-PAKZ-SERVER
— DLAPKAS-SRP3-CLIENT
— DLAPKAS-SRP3-SERVER
— DLAPKAS-SRP6-CLIENT
— DLAPKAS-SRP6-SERVER
— DLAPKAS-WSPEKE-CLIENT
— DLAPKAS-WSPEKE-SERVER
— DLBPKAS-PAK-CLIENT
— DLBPKAS-PAK-SERVER
— DLBPKAS-PPK-CLIENT,
— DLBPKAS-PPK-SERVER
— DLBPKAS-PPK-SERVER
— DLBPKAS-SPEKE-CLIENT,
— DLBPKAS-SPEKE-SERVER
— DLPKRS-1-CLIENT
— DLPKRS-1-SERVER
— ECAPKAS-AMP-CLIENT
— ECAPKAS-AMP-SERVER
— ECAPKAS-BSPEKE2-CLIENT
— ECAPKAS-BSPEKE2-SERVER
— ECAPKAS-PAKZ-CLIENT
— ECAPKAS-PAKZ-SERVER
— ECAPKAS-SRP5-CLIENT
— ECAPKAS-SRP5-SERVER
— ECAPKAS-WSPEKE-CLIENT
— ECAPKAS-WSPEKE-SERVER
— ECBPKAS-PAK-CLIENT
— ECBPKAS-PAK-SERVER
— ECBPKAS-PPK-CLIENT,
— ECBPKAS-PPK-SERVER

— ECBPKAS-PPK-SERVER
— ECBPKAS-SPEKE-CLIENT,
— ECBPKAS-SPEKE-SERVER
— ECPKRS-1-CLIENT
— ECPKRS-1-SERVER
— REDP
— SVDP
— PEPKGP
— DLKRBP-1
— ECKRUP-1
— ECKRBP-1
— ECKRUP-1
— DLKRPP-1
— ECKRPP-1
— DLPEPKGP-1
— ECPEPKGP-1
— DLPEPKGP-AMP-SERVER
— ECPEPKGP-AMP-SERVER
— DLPEPKGP-PAK
— ECPEPKGP-PAK
— DLPEPKGP-SPEKE
— ECPEPKGP-SPEKE
— DLPKGP-DH
— ECPKGP-DH
— DLPVDGP-AMP
— ECPVDGP-AMP
— DLPVDGP-BSPEKE2
— ECPVDGP-BSPEKE2
— DLPVDGP-PAKZ
— ECPVDGP-PAKZ
— DLREDP-1
— ECREDP-1
— DLREDP-2
— ECREDP-2
— DLSVDP-AMP-CLIENT
— ECSVDP-AMP-CLIENT
— DLSVDP-AMP-SERVER
— ECSVDP-AMP-SERVER
— DLSVDP-PAK1-CLIENT
— ECSVDP-PAK1-CLIENT
— DLSVDP-PAK2
— ECSVDP-PAK2
— DLSVDP-SPEKE
— ECSVDP-SPEKE
— DLSVDP-WSPEKE-CLIENT
— ECSVDP-WSPEKE-CLIENT

- DLSVDP-WSPEKE-SERVER
- ECSVDP-WSPEKE-SERVER
- DLPEPKGP-SRP3-SERVER
- DLPEPKGP-SRP6-SERVER
- DLPKGP-SRP-CLIENT
- DLPVDGP3-SRP3
- DLPVDGP-SRP3
- DLPVDGP-SRP6
- DLSVDP-SRP3-CLIENT
- DLSVDP-SRP3-SERVER
- DLSVDP-SRP6-CLIENT
- DLSVDP-SRP6-SERVER
- ECPEPKGP-SRP5-SERVER
- ECPKGP-DH
- ECPVDGP-SRP5
- ECSVDP-SRP5-CLIENT
- ECSVDP-SRP5-SERVER
- SHA-1, SHA-256, SHA-384, SHA-512, RIPEMD-160
- MGF1
- KDF, KDF1, KDF2
- KCF, KCF1
- MVCF, MVCF1

Correspondence on this matter should be sent to:

William Whyte,
Chair, IEEE P1363,
NTRU Cryptosystems, Inc.,
35 Nagog Park
Acton
MA 01720

Thank you for your attention.
Sincerely,
William Whyte
Chair, IEEE P1363