Exhibit A

PATENT INVALIDITY CONTENTIONS FOR U.S. PATENT NO. 6,563,928

U.S. Patent No. 6,563,928
Title: STRENGTHENED PUBLIC KEY PROTOCOL
Filed: April 1, 1999
Issued: May 13, 2003

Identification and Date of Relevant Prior Art (P.R. 3-3(a)):

U.S. Patent No. 5,442,707 to Miyaji
Title: METHOD FOR GENERATING AND VERIFYING ELECTRONIC SIGNATURES AND PRIVACY COMMUNICATION USING ELLIPTIC CURVES
Filed: September 27, 1993
Published: August 15, 1995

Publication: Neal Koblitz, "A Course in Number Theory and Cryptography," Springer-Verlag New York, Inc. (1994).

Publication: G. Agnew, R. Mullin and S. Vanstone, "An implementation of elliptic curve cryptosystems over F2155", IEEE Journal on Selected Areas in Communications, 11, p. 804-813 (1993).

Publication: Andreas Bender, Guy Castagnoli, "On the implementation of elliptic curve cryptosystems", Proceedings on Advances in Cryptology, p.186-192 (July 1989).

Publication: C. Gunther, "An Identity-Based Key-Exchange Protocol", Eurocrypt '89, LNCS 434, pp. 29-37, Springer-Verlag (1990).

Publication: C. Schnorr, "Efficient Signature Generation by Smart Cards", J. Cryptology, 4, p. 161-174 (1991).

Publication: Dr. Alfred J. Menezes, Dr. Mingua Qu and Dr. Scott Vanstone, "IEEE P1363 Standard, Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography, Part 6: Elliptic Curve Systems (Draft 2)," dated October 30, 1994, published at least as early as November 1, 1994.

Basis of Invalidity(P.R. 3-3(b)):

Asserted claim 61, and the claim from which it depends, claim 53, are invalid as anticipated under 35 U.S.C. § 102(e) by U.S. Patent No. 5,442,707 to Miyaji (the "'707 Patent"), because the '707 patent discloses each step in the method of claims 53 and 61. Claims 53 and 61 are also invalid as obvious under 35 U.S.C. § 103 over the '707 Patent.

Claim 53 is also invalid as anticipated under 35 U.S.C. § 102(b) over Neal Koblitz, “A Course in Number Theory and Cryptography” (“A Course in Number Theory and Cryptography”) because A Course in Number Theory and Cryptography discloses each step in the method of claim 53. Claim 53 is also invalid as obvious under 35 U.S.C. § 103 over A Course in Number Theory and Cryptography.

Asserted claim 61, and the claim from which it depends, claim 53, are also invalid as anticipated under 35 U.S.C. § 102(b) by G. Agnew, R. Mullin and S. Vanstone, "An implementation of elliptic curve cryptosystems over F2155" (“Agnew, Mullin and Vanstone Article”) because the Agnew, Mullin and Vanstone Article discloses each step in the method of claims 53 and 61. Claims 53 and 61 are also invalid as obvious under 35 U.S.C. § 103 over the Agnew, Mullin and Vanstone Article.

Asserted claim 61, and the claim from which it depends, claim 53, are also invalid as anticipated under 35 U.S.C. § 102(b) by Andreas Bender and Guy Castagnoli, “On the implementation of elliptic curve cryptosystems” (“Bender and Castagnoli Article”) because the Bender and Castagnoli Article discloses each step in the method of claims 53 and 61. Claims 53 and 61 are also invalid as obvious under 35 U.S.C. § 103 over the Bender and Castagnoli Article.

Asserted claim 61, and the claim from which it depends, claim 53, are also invalid as anticipated under 35 U.S.C. § 102(b) by C. Gunther, "An Identity-Based Key-Exchange Protocol" (“Gunther Article”) and C. Schnorr, "Efficient Signature Generation by Smart Cards" (“Schnorr Article”) because the Gunther Article and the Schnorr Article disclose each step in the method of claims 53 and 61 (the Gunther Article is effectively incorporated by reference in the Schnorr Article). Claims 53 and 61 are also invalid as obvious under 35 U.S.C. § 103 over the Gunther Article and the Schnorr Article. The Schnorr article itself provides the motivation to combine it with the Gunther Article by expressly referencing the Gunther Article.

Asserted claim 61, and the claim from which it depends, claim 53, are also invalid as anticipated under 35 U.S.C. § 102(b) by IEEE P1363 Standard, Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography, Part 6: Elliptic Curve Systems (Draft 2),” by Dr. Alfred J. Menezes, Dr. Mingua Qu, and Dr. Scott Vanstone, (the “IEEE P1363 Oct. 1994 Draft”), because the IEEE P1363 Oct. 1994 Draft discloses each step in the method of claims 53 and 61. Claims 53 and 61 are also invalid as obvious under 35 U.S.C. § 103 over the IEEE P1363 Oct. 1994 Draft.

Invalidity Chart (P.R. 3-3(c)):

U.S. Patent No. 6,563,928	**Exemplary Cites to U.S. 5,442,707 to Miyaji et al.**
	Exemplary Cites to "A Course in Number Theory and Cryptography" by Neal Koblitz, published in 1994.
	Exemplary Cites to "An implementation of elliptic curve cryptosystems over F2155" by Agnew, 6,563,928 Mullin and Vanstone published in 1993.
	Exemplary Cites to "On the implementation of elliptic curve cryptosystems" by Bender and Castagnoli published in 1999.
	Exemplary Cites to "An Identity-Based Key-Exchange Protocol" by Gunther published in 1990.
	Exemplary Cites to "Efficient Signature Generation by Smart Cards" by Schnorr published in 1991.
	Exemplary Cites to the IEEE P1363 Oct. 1994 Draft.
53. A method of establishing a session key for encryption of data between a pair of correspondents comprising the steps of	**U.S. 5,442,707 to Miyaji et al.** at Col. 1:49-60; 2:11-17.[1]
	A Course in Number Theory and Cryptography at p. 181**.**
	Agnew, Mullin and Vanstone Article at p. 804, 812.
	Bender and Castagnoli Article at p. 188.
	Gunther Article at p. 33.
	Schnorr Article at p. 162.

[1] This document uses the notation "x:a-b" to refer to column x, lines a- b within a patent.

U.S. Patent No. 6,563,928	**Exemplary Cites to U.S. 5,442,707 to Miyaji et al.**
	Exemplary Cites to "A Course in Number Theory and Cryptography" by Neal Koblitz, published in 1994.
	Exemplary Cites to "An implementation of elliptic curve cryptosystems over F2155" by Agnew, 6,563,928 Mullin and Vanstone published in 1993.
	Exemplary Cites to "On the implementation of elliptic curve cryptosystems" by Bender and Castagnoli published in 1999.
	Exemplary Cites to "An Identity-Based Key-Exchange Protocol" by Gunther published in 1990.
	Exemplary Cites to "Efficient Signature Generation by Smart Cards" by Schnorr published in 1991.
	Exemplary Cites to the IEEE P1363 Oct. 1994 Draft.
	IEEE P1363 Oct. 1994 Draft at 6.1.1, pp. 6-7.
one of said correspondents selecting a finite group G,	**U.S. 5,442,707 to Miyaji et al.** at col. 6:47-63.
	A Course in Number Theory and Cryptography at p. 181**.**
	Agnew, Mullin and Vanstone Article at p. 804.
	Bender and Castagnoli Article at p. 188, 189.
	Gunther Article at p. 30, 31, 33.
	Schnorr Article at p. 162.
	IEEE P1363 Oct. 1994 Draft at 6.1.1 p. 6, 6.8 pp. 13-14.

U.S. Patent No. 6,563,928	Exemplary Cites to U.S. 5,442,707 to Miyaji et al.
	Exemplary Cites to "A Course in Number Theory and Cryptography" by Neal Koblitz, published in 1994.
	Exemplary Cites to "An implementation of elliptic curve cryptosystems over F2155" by Agnew, 6,563,928 Mullin and Vanstone published in 1993.
	Exemplary Cites to "On the implementation of elliptic curve cryptosystems" by Bender and Castagnoli published in 1999.
	Exemplary Cites to "An Identity-Based Key-Exchange Protocol" by Gunther published in 1990.
	Exemplary Cites to "Efficient Signature Generation by Smart Cards" by Schnorr published in 1991.
	Exemplary Cites to the IEEE P1363 Oct. 1994 Draft.
establishing a subgroup S having an order q of the group G,	**U.S. 5,442,707 to Miyaji et al.** at col. 7:3-5.
	A Course in Number Theory and Cryptography at p. 181; p. 184.
	Agnew, Mullin and Vanstone Article at p. 812.
	Bender and Castagnoli Article at p. 189.
	Schnorr Article at p. 161, 162.
	IEEE P1363 Oct. 1994 Draft at 6.1.1, p. 6, 6.8, p. 13.
determining an element .alpha. of the subgroup S to generate greater than a predetermined	**U.S. 5,442,707 to Miyaji et al.** at col. 7:8-14**.**

U.S. Patent No. 6,563,928	Exemplary Cites to U.S. 5,442,707 to Miyaji et al.
	Exemplary Cites to "A Course in Number Theory and Cryptography" by Neal Koblitz, published in 1994.
	Exemplary Cites to "An implementation of elliptic curve cryptosystems over F2155" by Agnew, 6,563,928 Mullin and Vanstone published in 1993.
	Exemplary Cites to "On the implementation of elliptic curve cryptosystems" by Bender and Castagnoli published in 1999.
	Exemplary Cites to "An Identity-Based Key-Exchange Protocol" by Gunther published in 1990.
	Exemplary Cites to "Efficient Signature Generation by Smart Cards" by Schnorr published in 1991.
	Exemplary Cites to the IEEE P1363 Oct. 1994 Draft.
number of the q elements of the subgroup S	**A Course in Number Theory and Cryptography** at p. 181; p. 184.
	Agnew, Mullin and Vanstone Article at p. 804.
	Bender and Castagnoli Article at p. 189, 190.
	Schnorr Article at p. 162.
	IEEE P1363 Oct. 1994 Draft at 6.1.1, p. 6, 6.8, p.13.
and utilising said element .alpha. to generate a session key at said one correspondent.	**U.S. 5,442,707 to Miyaji et al.** at col. 2:34 - col. 3:19; 7:8-14.
	A Course in Number Theory and Cryptography at p. 181.

U.S. Patent No. 6,563,928	Exemplary Cites to U.S. 5,442,707 to Miyaji et al.
	Exemplary Cites to "A Course in Number Theory and Cryptography" by Neal Koblitz, published in 1994.
	Exemplary Cites to "An implementation of elliptic curve cryptosystems over F2155" by Agnew, 6,563,928 Mullin and Vanstone published in 1993.
	Exemplary Cites to "On the implementation of elliptic curve cryptosystems" by Bender and Castagnoli published in 1999.
	Exemplary Cites to "An Identity-Based Key-Exchange Protocol" by Gunther published in 1990.
	Exemplary Cites to "Efficient Signature Generation by Smart Cards" by Schnorr published in 1991.
	Exemplary Cites to the IEEE P1363 Oct. 1994 Draft.
	Agnew, Mullin and Vanstone Article at p. 804.
	Bender and Castagnoli Article at p. 188, 189.
	Gunther Article at p. 33.
	IEEE P1363 Oct. 1994 Draft at 6.1.1, p. 6.
61. A method according to claim 53 wherein said subgroup is selected to have an order that is to be a function of the product of a pair of primes r,r' and said element .alpha. is a generator of a subgroup of an order of one of said primes r,r'.	**U.S. 5,442,707 to Miyaji et al.** at col. 7:.3-5**;** 7:8-14.
	Agnew, Mullin and Vanstone Article at p. 812, 813.

U.S. Patent No. 6,563,928	**Exemplary Cites to U.S. 5,442,707 to Miyaji et al.**
	Exemplary Cites to "A Course in Number Theory and Cryptography" by Neal Koblitz, published in 1994.
	Exemplary Cites to "An implementation of elliptic curve cryptosystems over F2155" by Agnew, 6,563,928 Mullin and Vanstone published in 1993.
	Exemplary Cites to "On the implementation of elliptic curve cryptosystems" by Bender and Castagnoli published in 1999.
	Exemplary Cites to "An Identity-Based Key-Exchange Protocol" by Gunther published in 1990.
	Exemplary Cites to "Efficient Signature Generation by Smart Cards" by Schnorr published in 1991.
	Exemplary Cites to the IEEE P1363 Oct. 1994 Draft.
	Bender and Castagnoli Article at p. 189-190.
	Schnorr Article at p. 162.
	IEEE P1363 Oct. 1994 Draft at 6.1.1, p. 6, 6.8 p. 13.

Basis of Invalidity (P.R. 3-3(d)):

Claims 53 and 61 are also invalid under 35 U.S.C. § 112, ¶ 2, because the phrases "the q elements" and "greater than a predetermined number of the q elements" are vague and indefinite.