Network Working Group
Internet-Draft
Intended status: Informational
Expires: February 28, 2013

J. Merkle
secunet Security Networks
M. Lochter
Bundesamt fuer Sicherheit in der Informationstechnik (BSI)
August 27, 2012

Using the ECC Brainpool Curves for IKEv2 Key Exchange
draft-merkle-ikev2-ke-brainpool-00

Abstract

This document specifies the use of the ECC Brainpool elliptic curve groups for key exchange in the Internet Key Exchange version 2 (IKEv2) protocol.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 28, 2013.

Copyright Notice

Table of Contents

1. Introduction

In RFC 5639 [RFC5639], a new set of elliptic curve groups over finite prime fields for use in cryptographic applications was specified. These groups, denoted as Brainpool curves, were generated in a verifiably pseudo-random way and comply with the security requirements of relevant standards from ISO [ISO1] [ISO2], ANSI [ANSI1], NIST [FIPS], and SecG [SEC2].

While the ASN.1 object identifiers defined in RFC 5639 allow usage of the ECC Brainpool curves in certificates and certificate revocation lists, their utilization for key exchange in IKEv2 [RFC4306] requires the definition and assignment of additional transform IDs in the respective IANA registry. Furthermore, the encoding of the key exchange payload and derivation of the shared secret are defined, because previous RFCs specified this encoding only for the curves proposed therein.

2. IKEv2 Key Exchange using the ECC Brainpool Curves

2.1. Diffie-Hellman Group Transform IDs

In order to use the Brainpool curves for key exchange within IKEv2, the Diffie-Hellman Group Transform IDs (Transform Type 4) listed in the following table are to be registered with IANA [IANA-IKE2]. The parameters associated with these curves are defined in RFC 5639 [RFC5639].

Curve	Transform ID
brainpoolP160r1	TBD1
brainpoolP160t1	TBD2
brainpoolP192r1	TBD3
brainpoolP192t1	TBD4
brainpoolP224r1	TBD5
brainpoolP224t1	TBD6
brainpoolP256r1	TBD7
brainpoolP256t1	TBD8

brainpoolP320r1	TBD9
brainpoolP320t1	TBD10
brainpoolP384r1	TBD11
brainpoolP384t1	TBD12
brainpoolP512r1	TBD13
brainpoolP512t1	TBD14

Table 1

Test vectors for the groups defined by the Brainpool curves are provided in Appendix A

2.2. Key Exchange Payload and Shared Secret

RFC4306 [RFC4306] only specifies the use of MODP groups and GF[2^N] elliptic curve groups for Diffie-Hellman key exchange with IKEv2. For Diffie-Hellman groups of elliptic curves defined over prime fields (ECP Diffie-Hellman groups), however, the format of key exchange payloads and the derivation of a shared secret has thus far not been specified generally but on a group-by-group basis. To accomodate for different bandwidth limitations, for the groups defined in this document, two different methods for encoding the key exchange payload, compressed and uncompressed, are specified.

In an ECP key exchange, the Diffie-Hellman public value passed in a KE payload consists of two components, x and y, corresponding to the coordinates of an elliptic curve point. Each component MUST be computed from the corresponding coordinate using the FieldElement-to-OctetString conversion method specified in [SEC1] and MUST have bit length as indicated in Table 2. This length is enforced by the FieldElement-to-OctetString conversion method, if necessary, by prepending the value with zeros.

Curves	Bit lengths
brainpoolP160r1 or brainpoolP160t1	160
brainpoolP192r1 or brainpoolP192t1	191
brainpoolP224r1 or brainpoolP224t1	224
brainpoolP256r1 or brainpoolP256t1	256
brainpoolP320r1 or brainpoolP320t1	320
brainpoolP384r1 or brainpoolP384t1	384
brainpoolP512r1 or brainpoolP512t1	512

Table 2

From these components, the key exchange payload MUST be computed using one of the two following encodings.

1. Uncompressed. This method equals the method specified in RFC 5903 [RFC5903] for the ECP curves proposed therein. The key exchange payload is defined as the concatenation of the x and y coordinates. Using this method, the bit length of the key

exchange payload is twice the bit length of each component listed in Table 2. If a peer receives a key exchange payload for an ECC Brainpool curve having twice the bitlength indicated for that curve in Table 2, it MUST assume that the uncompressed encoding has been used.

2. Compressed. The key exchange payload is defined as x. Using this method, the bit length of the key exchange payload equals the bit length of each component listed in Table 2. If a peer receives a key exchange payload for an ECC Brainpool curve having the bitlength indicated for that curve in Table 2, it MUST assume that the compressed encoding has been used.

The Diffie-Hellman shared secret value MUST be computed from the x coordinate of the Diffie-Hellman common value using the FieldElement-

to-OctetString conversion method specified in [SEC1] and MUST have bit length as indicated in the Table 2. The parties MUST verify that the Diffie-Hellman common value is not the "point at infinity", i.e. that the shared secret derived contains non-zero octets.

When compressed encoding is used, computation of the Diffie-Hellman common value, and hence, of the shared secret value from the x-coordinate transmitted in the key exchange payload requires recovery of a correspoding y-coordinate. Since there are up to two possible points on the elliptic curve having a given x-coordinate, the recovered y-component is not unique. However, as explained in [RFC6090], any of the two y-coordinates corresponding to the x-value transmitted in the key exchange payload can be used to compute the Diffie-Hellman common value.

3. Security Considerations

The level of security provided by the authentication method in IKEv2 and the symmetric enryption and message integrity protection in IPSEc should roughly match or exceed the level provided by the group chosen for key exchange. RFC 5639 gives guidance in selection symmetric key sizes and hash functions for the ECC Brainpool curves. Furthermore, the security considerations of [RFC4306] apply as well.

4. IANA Considerations

Before this document can become an RFC, IANA is required to update the Transform Type 4 (Diffie-Hellman Group Transform) IDs in its Internet Key Exchange Version 2 (IKEv2) Parameters registry [IANA-IKE2]. In particular, numbers are to be assigned to the 14 groups specified in Table 1. Another I-D is being submitted for publication as RFC [BP_IKE] requesting assignment for the same groups in the corresponding registry for IKEv1; in order to keep the registries for IKEv1 and IKEv2 in accordance, it is advisable to assign the same values in both registries.

5. Intellectual Property Rights

Although, the authors have no knowledge about any intellectual property rights which cover the general usage of the ECP groups defined herein, implementations based on these domain parameters may require use of inventions covered by patent rights. In particular, the compressed encoding method for the key exchange payload defined in Section 2.2 may by covered by patents.

6. References

6.1. Normative References

[IANA-IKE2] Internet Assigned Numbers Authority, "Internet Key Exchange Version 2 (IKEv2) Parameters", <http://www.iana.org/assignments/ikev2-parameters>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC5639] Lochter, M. and J. Merkle, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation", RFC 5639, March 2010.

6.2. Informative References

[ANSI1] American National Standards Institute, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANSI X9.62, 2005.

[FIPS] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", FIPS PUB 186-2, December 1998.

[BP_IKE] Harkins, D., "Brainpool Elliptic Curves for the IKE Group Description Registry", draft-harkins-brainpool-ike-groups-00 (work in progress), August 2012.

[ISO1] International Organization for Standardization, "Information Technology - Security Techniques - Digital Signatures with Appendix - Part 3: Discrete Logarithm Based Mechanisms", ISO/IEC 14888-3, 2006.

[ISO2] International Organization for Standardization, "Information Technology - Security Techniques - Cryptographic Techniques Based on Elliptic Curves - Part 2: Digital signatures", ISO/IEC 15946-2, 2002.

[RFC5903] Fu, D. and J. Solinas, "Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2", RFC 5903, June 2010.

[RFC6090] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", RFC 6090, February 2011.

[SEC1] Certicom Research, "Elliptic Curve Cryptography", Standards for Efficient Cryptography (SEC) 1, September 2000.

[SEC2] Certicom Research, "Recommended Elliptic Curve Domain Parameters", Standards for Efficient Cryptography (SEC) 2, September 2000.

Appendix A. Test Vectors

This section provides some test vectors for example Diffie-Hellman key exchanges using each of the curves defined in Section 2 . In all of the following sections the following notation is used:

d_A: the secret key of party A

x_qA: the x-coordinate of the public key of party A

y_qA: the y-coordinate of the public key of party A

d_B: the secret key of party B

x_qB: the x-coordinate of the public key of party B

y_qB: the y-coordinate of the public key of party B

x_Z: the x-coordinate of the shared secret that results from completion of the Diffie-Hellman computation

y_Z: the y-coordinate of the shared secret that results from completion of the Diffie-Hellman computation

The field elements x_qA, y_qA, x_qB, y_qB, x_Z, y_Z are represented

as hexadecimal values using the FieldElement-to-OctetString conversion method specified in [SEC1].

A.1. 160 Bit Curves

Curve brainpoolP160r1

dA = 8BF7BC5CBE8AC8B34940C2C5652D6AE4EC9F53CE

x_qA = 651DA24C7FF64DD863F8F650E53F07B8EC943C39

y_qA = D1C68C656E44034D0DAD60A1589FD49594E7C2A4

dB = B6F7160F0DE61CCEAAC528A32BD7AD942E8017B2

x_qB = DF9F259AEA6DFA1F28B16B8FEC52044CC1DFBA35

y_qB = DF72AEA65A5E3EF69166DA161ABE00FC9C81C4D0

x_Z = D78792AC4CBE3390DDD6557060066BC25579CA97

y_Z = 3A3DAB50421585FB9DE9D87BB3BBBAFE3379A571

Twisted Curve brainpoolP160t1

dA = A1FED74247778596E0FFEA292DF215D291FB8A6A

x_qA = 1CDBF3D03C8CE04183600B99F80661129AB17B64

y_qA = 5FF702E42CFEB890329439CD9594FB26D52CDCC5

dB = A98B640213F32546F7A527EA7C75EACDADC001AB

x_qB = D7FB21ED2FD367B21B663C77ECD233FE97B7B39B

y_qB = A475B6F2BDB551A8303262814C2A5B1F3C77009C

x_Z = 87BFBDB38B161DA82C7696F80403610213419FF5

y_Z = 51D2ECA90C28ACBD7162A7700EB7FD3D60D9722B

A.2. 192 Bit Curves

Curve brainpoolP192r1

dA = 4B32E699290E3F052A99C7F0CFFD1C5707898015C743FE2A

x_qA = 31DB86048351629CFCA68541D65D909A0F1DC8E77AC440B2

y_qA = 7FB2925E1FDC609CF2252F0469836BA4F216ADF8A812893D

dB = 6916B2A336B3305A256238EA2BAB549D9C893F47D07964B8

x_qB = 15B795C67C5E47510116B0DE419C45835C209AE77D971536

y_qB = 0D1ADD9881EF6115EDF5B5CEF854B42E435CD9260A5719FB

x_Z = B946A6914877922A40F6D588D47FC7D44691C346FD384570

y_Z = AAD4E9CBC5BB6C7C308A95F445287580A09EBC93624FB24E

Twisted Curve brainpoolP192t1

dA = BA0D8C324347CD29B6EBC40540A4EB46C293F18E799E4748

x_qA = 29541AD06E6BC4C3CF28D7D0A505037D527A165889AF2646

y_qA = 0222140F457C044F5F585E5943A7411BCF7B95676C938E9C

dB = 479499E64FF4F30A5F4F08B1A451A113B166A32328ED549B

x_qB = 885FC460B907C9F7C1CF91C7C6AD3BF6343F381D06139021

y_qB = 704257DFF34C99B623FE6DF24A2719B9D5901285519977EB

x_Z = 1C6BE551CA60C6D24AF434915A381FBDC9EC934F4DB73257

y_Z = 110BA8C4446A689F1A526087DF8A9A620F75286F36B07014

A.3. 224 Bit Curves

Curve brainpoolP224r1

dA = 39F155483CEE191FBECFE9C81D8AB1A03CDA6790E7184ACE44BCA161

x_qA = A9C21A569759DA95E038704118426144032 7AFE33141CA04B82DC92E

y_qA = 98A0F75FBBF61D8E58AE5511B2BCDBE8E549B31E37069A2825F590C1

dB = 6060552303899E2140715816C45B57D9B42204FB6A5BF5BEAC10DB00

x_qB = 034A56C550FF88056144E6DD56070F54B0135976B5BF77827313F36B

y_qB = 75165AD99347DC86CAAB1CBB579E198EAF88DC35F927B358AA683681

x_Z = 1A4BFE705445120C8E3E026699054104510D119757B74D5FE2462C66

y_Z = BB6802AC01F8B7E91B1A1ACFB9830A95C079CEC48E52805DFD7D2AFE

Twisted Curve brainpoolP224t1

dA = B9324E65766C765036E8AFBD2611864C195F893B9256F40AA23B2738

x_qA = 3DA543100518A53531EBB3D1C14514C13EECA0A78CE92E71E2546FC1

y_qA = 67580D56C0C89AF632911B3F99934CA2AB154E7E6F5E47CB2980E084

dB = C9452FA256A710BEA19DFE6C7B4A848F82C2586BB815909B0C8099D6

x_qB = 5DC490CFBD576B1DAC7462BE6B567CA371A108BBCD3609F0C33C679B

y_qB = 8FBBAB24A248B676DF9D739478ABCCD593169297F2DEC2552C3F8DA0

x_Z = 62F1A83BE792608C1D2AAFB229779B47D3F88B1EE2F9686E8CD8EF3C

y_Z = B7F4B16BE902487127A605FED0069CB451CC56E0F9186B462D8BDD04

A.4. 256 Bit Curves

Curve brainpoolP256r1

dA =
81DB1EE100150FF2EA338D708271BE38300CB54241D79950F77B063039804F1D

x_qA =
44106E913F92BC02A1705D9953A8414DB95E1AAA49E81D9E85F929A8E3100BE5

y_qA =
8AB4846F11CACCB73CE49CBDD120F5A900A69FD32C272223F789EF10EB089BDC

dB =
55E40BC41E37E3E2AD25C3C6654511FFA8474A91A0032087593852D3E7D76BD3

x_qB =
8D2D688C6CF93E1160AD04CC4429117DC2C41825E1E9FCA0ADDD34E6F1B39F7B

y_qB =
990C57520812BE512641E47034832106BC7D3E8DD0E4C7F1136D7006547CEC6A

x_Z =
89AFC39D41D3B327814B80940B042590F96556EC91E6AE7939BCE31F3A18BF2B

y_Z =
49C27868F4ECA2179BFD7D59B1E3BF34C1DBDE61AE12931648F43E59632504DE

Twisted Curve brainpoolP256t1

dA =
67CF7C2A6537E1E135C131B06958D388B97AC6173A2E669103A6F55EFCA51726

x_qA =
356AEB7B004AD59A48E46373BF2D413A52987BF8FE7073729AB56920C4B2FFE1

y_qA =
791116DEA74A3724F84F68ED3E18F01E3B9ABD90A26E38028322066FD7A09BAF

dB =
A74E29848D27882B6B7817694CC82EE81330AF856F243939B5F8B57CE59FD7EC

x_qB =
7D9FD6B1FAAF13C9C34DD8D713E9759D7A0F7E34206B8566C8D771C02871A702

y_qB =
45A49EDEBA249C9DBB0FE8B42CF4765650DB68C84B4BD467BE151E6D6C60F5C1

x_Z =
A0AF0A63DE5579343129183FF958582A19D63DDBAAA91E07536421DEAB1064AF

y_Z =
78162E9FB4E2E0CA1F7B30ED51685864F9AB1B59E40E0E8DA046D4E897A77DD7

A.5. 320 Bit Curves

Curve brainpoolP320r1

dA = 7CD9C454BA907F7617E262A7FD73764C4A3157C13F82279EF9F062BE5D49A
8E390B66A4DCEDFA867

x_qA = BC43666C00E4B943FE1C785DD8AA842A42AB54B0B49819F960F77694193
CD3AFA71B6B3C826C7734

y_qA = 69E998892C0764468023C8E3A7B8F219A1446042BE175D4476B2FDFD85B
22EAD2F29101A1242A578

dB = B832A73DA5F671E80D87F09372544801F6812224B19A4BC1B37AA7DB0842E
6DD3CA11DE0F802BFED

x_qB = B1246229429354D1D687BCA48BCCD6FC733B146DAC03642A0AD4B896F5D
8BCBD2F4BCA16776E4526

y_qB = A41683898F9A76EF36EA2DC7B74D419E55CF3664721890D6A2B2FB8CEB7
C113167ED137A358EE37F

x_Z = 730314D906B2F21DC11BE05031B028D665696BEEC7139328CDF70C718BE5
D208659BB96743A88067

y_Z = C338B5B7A3FB62EDE9BAA9C06DF9BC36D4B5F0D35EFDF79249913E6DC4DB
6DBC7BA9B74E59C840F1

Twisted Curve brainpoolP320t1

dA = 61ACFDF3C9C0E50B6ED58EC6B2750725D90C94D368EFA665B8800AFF31F21
9AF39DA188ABAD9D6BC

x_qA = 4DEABAB307DDD924E302EFABC15E4BC588FE67ECF92F03B918E5F4AE43B
62FFDE0F115015D9AD732

y_qA = 6E312549C939A9FCCD17D454B9212A39F670D4738B175EE5755A5BAAFF6
D94992A5EA7541250E8FA

dB = CDF6A4032DA09679DDE13D74F12C0F2E838D4CBE062E65CDDB595799EDA4C
22D3A69A4794DD4B032

x_qB = B3B33997A7047C32F2FCBC76960FFD71910316177E059AE77FFDE107722
C6B05D019A71AE7FCEA05

y_qB = 2D97625CB68013D900C169FD1336FC27A5531F0F54461AD91E38C49584D
8ECCDE3AE66BA4D1E7D29

x_Z = 13FB6B5E601AB1FAD84210E087EAE185F8CDC6D54EF63CF62950D0DA3437
4BEF4DE4998E9A87263A

y_Z = 6A969AE380DC0B22A0112F602DE3188EE2DE14EA453A2F5D2963CAF11CA9
AEFEE241C7038411C27C

A.6. 384 Bit Curves

Curve brainpoolP384r1

dA = 1E20F5E048A5886F1F157C74E91BDE2B98C8B52D58E5003D57053FC4B0BD6
5D6F15EB5D1EE1610DF870795143627D042

x_qA = 68B665DD91C195800650CDD363C625F4E742E8134667B767B1B47679358
8F885AB698C852D4A6E77A252D6380FCAF068

y_qA = 55BC91A39C9EC01DEE36017B7D673A931236D2F1F5C83942D049E3FA206
07493E0D038FF2FD30C2AB67D15C85F7FAA59

dB = 032640BC6003C59260F7250C3DB58CE647F98E1260ACCE4ACDA3DD869F74E
01F8BA5E0324309DB6A9831497ABAC96670

x_qB = 4D44326F269A597A5B58BBA565DA5556ED7FD9A8A9EB76C25F46DB69D19
DC8CE6AD18E404B15738B2086DF37E71D1EB4

y_qB = 62D692136DE56CBE93BF5FA3188EF58BC8A3A0EC6C1E151A21038A42E91
85329B5B275903D192F8D4E1F32FE9CC78C48

x_Z = 0BD9D3A7EA0B3D519D09D8E48D0785FB744A6B355E6304BC51C229FBBCE2
39BBADF6403715C35D4FB2A5444F575D4F42

y_Z = 0DF213417EBE4D8E40A5F76F66C56470C489A3478D146DECF6DF0D94BAE9
E598157290F8756066975F1DB34B2324B7BD

Twisted Curve brainpoolP384t1

dA = 820B55599BA830FB45BD280FE20D32F9A114F6E2EA4F9AC1D5EBE67F7C0B1
A0506413A4B49E372A56620454FC0735481

x_qA = 0C1C3E48C8072055EC617DECC3B5F6EE2566CBB16E9EAB2E8D839AB6E98
1FCF13B2EDF86E27877B1AF99D8F2280BEA76

y_qA = 3365AC30C33AABB342C6FC30C2E3C0AAC15E4D521633185899687742188
F96588C03DE656BD308C1906F67B033981603

dB = 3DF90919D4970788047B1FA0FBB716546ECF2A784CDD9CA53D5101B5BCA1A
7CCAD7A7180B4C9F9D7D2A8F24E2B5936BD

x_qB = 4C3949372FF295B6708C4180F6CF3616CA8BDF7CC792BAB582C27EC42EE
FF0E563F2512B592438616E45D01309A06C0C

y_qB = 1C43A48648C857189D9F2799B06F8253DF1BA8187622EDBF5C2C4A34164
22877E7A2056FE6165271899DDD86DEC2CBC7

x_Z = 8549A7BC6523128176322B295F5806971F9C2B6C10A6595D252CCA4B404E
940BDB193AE0AB664959DBE638C8BB75A55E

y_Z = 0C9D339F9ECA04924E2B73619DB30CADAF344AAB15938D4EE4E9DC7A81A4
66A1CDC0D4C422DC75A5333DE8F226E9707C

A.7. 512 Bit Curves

Curve brainpoolP512r1

dA = 16302FF0DBBB5A8D733DAB7141C1B45ACBC8715939677F6A56850A38BD87B
D59B09E80279609FF333EB9D4C061231FB26F92EEB04982A5F1D1764CAD5766542
2

x_qA = 0A420517E406AAC0ACDCE90FCD71487718D3B953EFD7FBEC5F7F27E28C6
149999397E91E029E06457DB2D3E640668B392C2A7E737A7F0BF04436D11640FD0
9FD

y_qA = 72E6882E8DB28AAD36237CD25D580DB23783961C8DC52DFA2EC138AD472
A0FCEF3887CF62B623B2A87DE5C588301EA3E5FC269B373B60724F5E82A6AD147F
DE7

dB = 230E18E1BCC88A362FA54E4EA3902009292F7F8033624FD471B5D8ACE49D1
2CFABBC19963DAB8E2F1EBA00BFFB29E4D72D13F2224562F405CB80503666B2542
9

x_qB = 9D45F66DE5D67E2E6DB6E93A59CE0BB48106097FF78A081DE781CDB31FC
E8CCBAAEA8DD4320C4119F1E9CD437A2EAB3731FA9668AB268D871DEDA55A54731
99F

y_qB = 2FDC313095BCDD5FB3A91636F07A959C8E86B5636A1E930E8396049CB48
1961D365CC11453A06C719835475B12CB52FC3C383BCE35E27EF194512B7187628
5FA

x_Z = A7927098655F1F9976FA50A9D566865DC530331846381C87256BAF322624
4B76D36403C024D7BBF0AA0803EAFF405D3D24F11A9B5C0BEF679FE1454B21C4CD

1F

y_Z = 7DB71C3DEF63212841C463E881BDCF055523BD368240E6C3143BD8DEF8B3
B3223B95E0F53082FF5E412F4222537A43DF1C6D25729DDB51620A832BE6A26680
A2

Twisted Curve brainpoolP512t1

dA = 7938A373E32ECDCB3A88B725531EF0A41165904FDE02879EE738FE81B3B87
A4F5730A8EB5FBA650609D7A5979099F058500EB160D3557D69B90FB2BAFE8AA3B
4

x_qA = 587335843CF88ACBC4110DD3711E21238280FD9D6BCDCB5F5AC8DB599D3
77DE168AA32276FB068A3EF05EE61021668EC7C5BB1DDB96E392F6AC5C03F4A7C6
05A

y_qA = 501E2C43716E3F5D6D2F5960A33ECD2BA2D812AFB76B8C158E6E25FD37F
82EE7299E2E64BCB39C0B739A5493C99615E62AE79C8719E40DDD9B7A44D990C73
683

dB = 5538DF5451063E1CE7351C1A750C29D38FA2348F2FA097A1DB75D24AC8F83
D8F13ED009F02621F6A0E3796101FB1EC9F1890B66635DDCEB5EF1ED083A28CF01
2

x_qB = A6400A41B64FCD6E451DD3B42B0247B24596118058B4DF8E34EC3EC33B1
9CDCF5A9B2ECA4F1DB2D58C2AFD047550996CA361FCA8497233AF8C0F406FD9FC0

CD1

y_qB = 7B7DB683F90DE91F3814139CC83E0693FED68A302458CA7690BA66067E3
C963EB4D073F72723E01E05B6D0484D80FBE2EE830DB1F8F0B58570E5D8342267B
2DE

x_Z = 540789E4BA46DD1925ED37A9FCAFC927A3FE264F924FDA130790B1429AA2
449C6FDFF21EC506672E2E9E1DB3D69B04461FFB1736D7E7F7764BE4BDD9F8D271
B1

y_Z = 37C113154C495B136D495B6864EC85C31AC46C19E3131E736D1C0B42BC00
B05452AF0AB408B244ED0B4B3ECB65634C603829C72396D8D6072DE5663935DD89
5F

Authors' Addresses

Johannes Merkle
secunet Security Networks
Mergenthaler Allee 77
65760 Eschborn
Germany

Phone: +49 201 5454 3091
EMail: johannes.merkle@secunet.com

Manfred Lochter
Bundesamt fuer Sicherheit in der Informationstechnik (BSI)
Postfach 200363
53133 Bonn
Germany

Phone: +49 228 9582 5643

EMail: manfred.lochter@bsi.bund.de