Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 5903
RFC rendue obsolète : 4753
Catégorie : Information
ISSN: 2070-1721

D. Fu, NSA
J. Solinas, NSA
juin 2010

Traduction Claude Brière de L'Isle

Groupes de courbes elliptiques (ECP) modulo un nombre premier pour IKE et IKEv2

Résumé
Le présent document décrit trois groupes de cryptographie à courbe elliptique (ECC, *Elliptic Curve Cryptography*) à utiliser dans les protocole d'échange de clés Internet (IKE, *Internet Key Exchange*) et échange de clés Internet version 2 (IKEv2, *Internet Key Exchange version 2*) en plus des groupes précédemment définis. Ces groupes de courbes se fondent sur l'arithmétique modulaire plutôt que sur l'arithmétique binaire. Ces groupes sont définis pour aligner IKE et IKEv2 avec les autres mises en œuvre et standard de ECC, en particulier les normes du NIST. De plus, les courbes définies ici peuvent fournir une mise en œuvre plus efficace que les groupes ECC précédemment définis. Le présent document rend obsolète la RFC 4753.

Table des matières

1. Introduction

Le présent document décrit les groupes Diffie-Hellman par défaut à utiliser dans IKE et IKEv2 en plus des groupes Oakley inclus dans la [RFC2409] et les groupes additionnels définis depuis [IANA-IKE]. Le présent document suppose que le lecteur est familiarisé avec le protocole IKE et le concept de groupes de Oakley, tel que défini dans la [RFC2409].

La [RFC2409] définit cinq groupes de Oakley standard : trois groupes d'exponentiation modulaire et deux groupes de courbe elliptique sur GF[2^N]. Un groupe d'exponentiation modulaire (768 bits - Groupe 1 de Oakley) est de prise en charge obligatoire pour toutes les mises en œuvre, alors que les quatre autres groupes sont facultatifs. Dix-neuf groupes supplémentaires ont été définis ultérieurement et des valeurs leur ont été allouées par l'IANA. Tous ces groupes supplémentaires sont facultatifs.

L'objet du présent document est d'étendre les options disponibles à ceux qui mettent en œuvre des groupes de courbe elliptique par l'ajout de trois groupes ECP (groupes à courbe elliptique modulo un nombre premier). Les raisons de l'ajout de tels groupes sont les suivantes.

- Les groupes proposés présentent des avantages d'efficacité dans les applications de logiciel car l'arithmétique sous-jacente est une arithmétique d'entier modulo un nombre premier plutôt qu'une arithmétique de champ binaire. (Des avantages de calcul suppémentaires de ces groupes sont présentés dans [GMN].)
- Les groupes proposés encouragent l'alignement avec d'autres normes de courbe elliptique. Les groupes proposés sont parmi ceux qui sont normalisés par le NIST, le groupe pour la normalisation d'une cryptographie efficace (SECG, *Standards for Efficient Cryptography Group*), l'ISO, et l'ANSI. (Voir les détails à la Section 5.)
- Les groupes proposés sont capables de fournir une sécurité cohérente avec la norme de chiffrement évolué (AES, *Advanced Encryption Standard*).

En résumé, du fait des avantages de performance des groupes de courbes elliptiques dans les mises en œuvre de IKE et du besoin d'un alignement avec les autres normes, le présent document définit trois groupes de courbes elliptiques fondés sur une arithmétique modulaire.

Ces groupes étaient à l'origine proposés dans la [RFC4753]. Le présent document change le format de clé partagée produit par un échange Diffie-Hellman utilisant ces groupes. Le format de clé partagée utilisé dans la présente spécification apparaissait antérieurement comme un erratum à la RFC 4753 [Err9], mais certaines mises en œuvre de la RFC 4753 ignoraient l'erratum et nemettaient pas en œuvre la correction. Les mises en œuvre de la RFC 4753 qui incorporent la correction sont interopérables avec les mises en œuvre de la présente spécification. Cependant, il y a de potentiels problèmes d'interopérabilité entre les mises en œuvre de la présente spécification et celles de la RFC 4753 qui ne mettent pas en œuvre la correction provenant de l'erratum. Ces problèmes pourraient être difficiles à détecter et analyser car les deux utilisent le même codet mais la valeur secrète (qui est probablement indisponible au bureau de correction) est calculée différemment. Lorsque des homologues ne sont pas interopérables, l'initiateur ne va jamais recevoir de réponse et va finalement arriver en fin de temporisation.

La Section 9 donne les détails des changements par rapport à la [RFC4753]. Le présent document rend obsolète la RFC 4753 et incorpore l'erratum.

2. Exigences de terminologie

Les mots clés "DOIT" et "DEVRAIT" qui apparaissent dans le présent document sont à interpréter comme décrit dans la [RFC2119].

3. Groupes ECC additionnels

La notation adoptée dans la [RFC2409] est utilisée ci-dessous pour décrire les nouveaux groupes proposés.

3.1 Groupe ECP aléatoire à 256 bits

Les mises en œuvre de IKE et IKEv2 DEVRAIENT prendre en charge un groupe ECP avec les caractéristiques suivantes. La courbe se fonde sur les entiers modulo le nombre premier de Mersenne généralisé p donné par :

p = 2^(256)-2^(224)+2^(192)+2^(96)-1

L'équation de la courbe elliptique est :

y^2 = x^3 - 3 x + b

Taille de champ : 256

Polynome de groupe premier/irréducible :
FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF

Courbe de groupe b :
5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B

Ordre de groupe :
FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551

Le groupe est choisi au hasard de façon vérifiable en utilisant SHA-1 comme spécifié dans [IEEE-1363] à partir du germe :

C49D3608 86E70493 6A6678E1 139D26B7 819F7E90

Le générateur pour ce groupe est donné par g = (gx,gy)
où :
gx : 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296
gy : 4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE CBB64068 37BF51F5

3.2 Groupe ECP aléatoire à 384 bits

Les mises en œuvre de IKE et IKEv2 DEVRAIENT prendre en charge un groupe ECP avec les caractéristiques suivantes. La courbe se fonde sur les entiers modulo le nombre premier de Mersenne généralisé p donné par :

p = 2^(384)-2^(128)-2^(96)+2^(32)-1

L'équation de la courbe elliptique est : y^2 = x^3 - 3 x + b

Taille de champ : 384

Polynome de groupe premier/irréducible :
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE
FFFFFFFF 00000000 00000000 FFFFFFFF

Courbe de groupe b :
B3312FA7 E23EE7E4 988E056B E3F82D19 181D9C6E FE814112 0314088F 5013875A
C656398D 8A2ED19D 2A85C8ED D3EC2AEF

Ordre de groupe :
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF C7634D81 F4372DDF
581A0DB2 48B0A77A ECEC196A CCC52973

Le groupe est choisi au hasard de façon vérifiable en utilisant SHA-1 comme spécifié dans [IEEE-1363] à partir du germe :
A335926A A319A27A 1D00896A 6773A482 7ACDAC73

Le générateur pour ce groupe est donné par g = (gx,gy)
où :
gx : AA87CA22 BE8B0537 8EB1C71E F320AD74 6E1D3B62 8BA79B98 59F741E0 82542A38 5502F25D BF55296C
3A545E38 72760AB7

gy : 3617DE4A 96262C6F 5D9E98BF 9292DC29 F8F41DBD 289A147C E9DA3113 B5F0B8C0 0A60B1CE 1D7E819D 7A431D7C 90EA0E5F

3.3 Groupe ECP aléatoire à 521 bits

Les mises en œuvre de IKE et IKEv2 DEVRAIENT prendre en charge un groupe ECP avec les caractéristiques suivantes. La courbe se fonde sur les entiers modulo le nombre premier de Mersenne généralisé p donné par :

p = 2^(521)-1

L'équation de la courbe elliptique est : y^2 = x^3 - 3 x + b

Taille de champ : 521

Polynome de groupe premier/irréducible :
01FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFF

Courbe de groupe b :
0051953E B9618E1C 9A1F929A 21A0B685 40EEA2DA 725B99B3 15F3B8B4 89918EF1
09E15619 3951EC7E 937B1652 C0BD3BB1 BF073573 DF883D2C 34F1EF45 1FD46B50 3F00

Ordre de groupe :
01FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFA5186 8783BF2F 966B7FCC 0148F709 A5D03BB5 C9B8899C 47AEBB6F B71E9138 6409

Le groupe est choisi au hasard de façon vérifiable en utilisant SHA-1 comme spécifié dans [IEEE-1363] à partir du germe :
D09E8800 291CB853 96CC6717 393284AA A0DA64BA

Le générateur pour ce groupe est donné par g=(gx,gy)
où :
gx : 00C6858E 06B70404 E9CD9E3E CB662395 B4429C64 8139053F B521F828 AF606B4D 3DBAA14B 5E77EFE7 5928FE1D C127A2FF A8DE3348 B3C1856A 429BF97E 7E31C2E5 BD66
gy : 01183929 6A789A3B C0045C8A 5FB42C7D 1BD998F5 4449579B 446817AF BD17273E 662C97EE 72995EF4 2640C550 B9013FAD 0761353C 7086A272 C24088BE 94769FD1 6650

4. Considérations pour la sécurité

Comme le présent document propose des groupes à utiliser dans IKE et IKEv2, beaucoup des considérations de sécurité contenues dans [RFC2409] et [RFC4306] s'appliquent aussi ici.

Les groupes proposés dans le présent document correspondent aux tailles de clés symétriques 128 bits, 192 bits, et 256 bits. Cela permet à l'échange de clés IKE d'offrir une sécurité comparable à celle des algorithmes AES [AES].

5. Alignement avec les autres normes

Le tableau suivant résume l'apparition des trois groupes de courbes elliptiques dans les autres normes.

	Groupe ECP aléatoire de		
Norme	**256 bits**	**384 bits**	**521 bits**
NIST [DSS]	P-256	P-384	P-521
ISO/IEC [ISO-15946-1]	P-256		
ISO/IEC [ISO-18031]	P-256	P-384	P-521
ANSI [X9.62-1998]	Sect. J.5.3, exemple 1		
ANSI [X9.62-2005]	Sect. L.6.4.3	Sect. L.6.5.2	Sect. L.6.6.2
ANSI [X9.63]	Sect. J.5.4,	Sect. J.5.5	Sect. J.5.6 exemple 2
SECG [SEC2]	secp256r1	secp384r1	secp521r1

Voir aussi [NIST], [ISO-14888-3], [ISO-15946-2], [ISO-15946-3], et [ISO-15946-4].

6. Considérations relatives à l'IANA

L'IANA a mis à jour ses registres de groupes Diffie-Hellman pour IKE dans [IANA-IKE] et pour IKEv2 dans [IANA-IKEv2] pour inclure les groupes définis ci-dessus.

Dans [IANA-IKE], les groupes apparaissent comme entrées dans la liste de groupes Diffie-Hellman donnée par description de groupe (classe d'attribut 4).

Les descriptions sont "groupe ECP aléatoire de 256 bits, "groupe ECP aléatoire de 384 bits", et "groupe ECP aléatoire de 521 bits". Dans chaque cas, le type de groupe (classe d'attribut 5) a la valeur de 2 (ECP, groupe de courbe elliptique sur GF[P]).

Dans [IANA-IKEv2], les groupes apparaissent comme entrées dans la liste des valeurs de type de transformation IKEv2 pour le type de transformation 4 (groupes Diffie-Hellman).

Ces entrées ont été mises à jour dans [IANA-IKE] et dans [IANA-IKEv2]. La mise à jour a consisté à changer la référence de la [RFC4753] au présent document.

7. Format des données d'échange de clé ECP

Dans un échange de clé ECP, la valeur publique Diffie-Hellman passée dans une charge utile IKE consiste en deux composants, x et y, qui correspondent aux coordonnées d'un point d'une courbe elliptique. Chaque composant DOIT avoir la longueur en bits donnée par le tableau qui suit :

Groupe Diffie-Hellman	**Longueur du composant en bits**
groupe ECP aléatoire de 256 bits	256
groupe ECP aléatoire de 384 bits	384
groupe ECP aléatoire de 521 bits	528

Cette longueur est appliquée, si nécessaire, en ajoutant des zéros devant la valeur.

La valeur publique Diffie-Hellman est obtenue en enchaînant les valeurs x et y.

La valeur du secret partagé Diffie-Hellman consiste en la valeur x de la valeur Diffie-Hellman commune.

Ces formats devraient être considérés comme spécifiques des courbes ECP et ne sont pas applicables aux courbes EC2N (groupe de courbes elliptiques sur GF[2^N]).

8. Vecteurs d'essai

On donne ci-dessous des exemples de charge utile d'échange de clé IKEv2 pour chacun des trois groupes spécifiés dans ce document.

On note g^n le scalaire multiple du point g par l'entier n ; c'est un autre point sur la courbe. Dans la littérature, le scalaire multiple est normalement noté ng ; la notation g^n est utilisée afin de se conformer à la notation utilisée dans la [RFC2409] et la [RFC4306].

8.1 Groupe ECP aléatoire à 256 bits

L'IANA a alloué la valeur d'identifiant 19 à ce groupe Diffie-Hellman.

On suppose que la clé privée Diffie-Hellman de l'initiateur est :

i : C88F01F5 10D9AC3F 70A292DA A2316DE5 44E9AAB8 AFE84049 C62A9C57 862D1433

Alors la clé publique est donnée par g^i = (gix,giy)
où :
gix : DAD0B653 94221CF9 B051E1FE CA5787D0 98DFE637 FC90B9EF 945D0C37 72581180
giy : 5271A046 1CDB8252 D61F1C45 6FA3E59A B1F45B33 ACCF5F58 389E0577 B8990BB3

La charge utile KEi est la suivante :
00000048 00130000 DAD0B653 94221CF9 B051E1FE CA5787D0 98DFE637 FC90B9EF 945D0C37 72581180
5271A046 1CDB8252 D61F1C45 6FA3E59A B1F45B33 ACCF5F58 389E0577 B8990BB3

On suppose que la clé privée de réponse Diffie-Hellman est :

r : C6EF9C5D 78AE012A 011164AC B397CE20 88685D8F 06BF9BE0 B283AB46 476BEE53

Alors, la clé publique est donnés par g^r = (grx,gry)
où :
grx : D12DFB52 89C8D4F8 1208B702 70398C34 2296970A 0BCCB74C 736FC755 4494BF63
gry : 56FBF3CA 366CC23E 8157854C 13C58D6A AC23F046 ADA30F83 53E74F33 039872AB

La charge utile KEr est comme suit :
00000048 00130000 D12DFB52 89C8D4F8 1208B702 70398C34 2296970A 0BCCB74C 736FC755 4494BF63
56FBF3CA 366CC23E 8157854C 13C58D6A AC23F046 ADA30F83 53E74F33 039872AB

La valeur Diffie-Hellman commune (girx,giry) est :
girx : D6840F6B 42F6EDAF D13116E0 E1256520 2FEF8E9E CE7DCE03 812464D0 4B9442DE
giry : 522BDE0A F0D8585B 8DEF9C18 3B5AE38F 50235206 A8674ECB 5D98EDB2 0EB153A2

La valeur du secret partagé Diffie-Hellman est girx.

8.2 Groupe ECP aléatoire à 384 bits

L'IANA a alloué la valeur d'identifiant de 20 à ce groupe Diffie-Hellman.

On suppose que la clé privée Diffie-Hellman de l'initiateur est :

i : 099F3C70 34D4A2C6 99884D73 A375A67F 7624EF7C 6B3C0F16 0647B674 14DCE655 E35B5380 41E649EE 3FAEF896 783AB194

La clé publique est alors donnée par g^i = (gix,giy) où :

gix : 667842D7 D180AC2C DE6F74F3 7551F557 55C7645C 20EF73E3 1634FE72 B4C55EE6 DE3AC808 ACB4BDB4 C88732AE E95F41AA

giy : 9482ED1F C0EEB9CA FC498462 5CCFC23F 65032149 E0E144AD A0241815 35A0F38E EB9FCFF3 C2C947DA E69B4C63 4573A81C

La charge utile KEi est la suivante .

00000068 00140000 667842D7 D180AC2C DE6F74F3 7551F557 55C7645C 20EF73E3 1634FE72 B4C55EE6 DE3AC808 ACB4BDB4 C88732AE E95F41AA 9482ED1F C0EEB9CA FC498462 5CCFC23F 65032149 E0E144AD A0241815 35A0F38E EB9FCFF3 C2C947DA E69B4C63 4573A81C

On suppose que la clé privée Diffie-Hellman de réppnse est :

r : 41CB0779 B4BDB85D 47846725 FBEC3C94 30FAB46C C8DC5060 855CC9BD A0AA2942 E0308312 916B8ED2 960E4BD5 5A7448FC

Alors la clé publique est donnée par g^r = (grx,gry) où :

grx : E558DBEF 53EECDE3 D3FCCFC1 AEA08A89 A987475D 12FD950D 83CFA417 32BC509D 0D1AC43A 0336DEF9 6FDA41D0 774A3571

gry : DCFBEC7A ACF31964 72169E83 8430367F 66EEBE3C 6E70C416 DD5F0C68 759DD1FF F83FA401 42209DFF 5EAAD96D B9E6386C

La charge utile KEr est la suivante .
00000068 00140000 E558DBEF 53EECDE3 D3FCCFC1 AEA08A89 A987475D 12FD950D 83CFA417 32BC509D 0D1AC43A 0336DEF9 6FDA41D0 774A3571 DCFBEC7A ACF31964 72169E83 8430367F 66EEBE3C 6E70C416 DD5F0C68 759DD1FF F83FA401 42209DFF 5EAAD96D B9E6386C

La valeur commune Diffie-Hellman (girx,giry) est :

girx : 11187331 C279962D 93D60424 3FD592CB 9D0A926F 422E4718 7521287E 7156C5C4 D6031355 69B9E9D0 9CF5D4A2 70F59746

giry : A2A9F38E F5CAFBE2 347CF7EC 24BDD5E6 24BC93BF A82771F4 0D1B65D0 6256A852 C983135D 4669F879 2F2C1D55 718AFBB4

La valeur du secret Diffie-Hellman partagée est girx.

8.3 Groupe ECP aléatoire à 521 bits

L'IANA a alloué la valeur d'identifiant 21 à ce groupe Diffie-Hellman.

On suppose que la clé privée Diffie-Hellman de l'initiateur est :

i : 0037ADE9 319A89F4 DABDB3EF 411AACCC A5123C61 ACAB57B5 393DCE47 608172A0 95AA85A3 0FE1C295 2C6771D9 37BA9777 F5957B26 39BAB072 462F68C2 7A57382D 4A52

La clé publique est alors donnée par g^i = (gix,giy) où :

gix : 0015417E 84DBF28C 0AD3C278 713349DC 7DF153C8 97A1891B D98BAB43 57C9ECBE E1E3BF42 E00B8E38 0AEAE57C 2D107564 94188594 2AF5A7F4 601723C4 195D176C ED3E

giy : 017CAE20 B6641D2E EB695786 D8C94614 6239D099 E18E1D5A 514C739D 7CB4A10A D8A78801 5AC405D7 799DC75E 7B7D5B6C F2261A6A 7F150743 8BF01BEB 6CA3926F 9582

La charge utile KEi est la suivante :
0000008C 00150000 0015417E 84DBF28C 0AD3C278 713349DC 7DF153C8 97A1891B D98BAB43 57C9ECBE E1E3BF42 E00B8E38 0AEAE57C 2D107564 94188594 2AF5A7F4 601723C4 195D176C ED3E017C AE20B664 1D2EEB69 5786D8C9 46146239 D099E18E 1D5A514C 739D7CB4 A10AD8A7 88015AC4 05D7799D C75E7B7D5B6CF226 1A6A7F15 07438BF0 1BEB6CA3 926F9582

On suppose que la clé privée de réponse Diffie-Hellman est :

r : 0145BA99 A847AF43 793FDD0E 872E7CDF A16BE30F DC780F97 BCCC3F07 8380201E 9C677D60 0B343757 A3BDBF2A 3163E4C2 F869CCA7 458AA4A4 EFFC311F 5CB15168 5EB9

La clé publique est alors donnée par g^r = (grx,gry) où :

grx : 00D0B397 5AC4B799 F5BEA16D 5E13E9AF 971D5E9B 984C9F39 728B5E57 39735A21 9B97C356 436ADC6E 95BB0352 F6BE64A6 C2912D4E F2D0433C ED2B6171 640012D9 460F

gry : 015C6822 6383956E 3BD066E7 97B623C2 7CE0EAC2 F551A10C 2C724D98 52077B87 220B6536 C5C408A1 D2AEBB8E 86D678AE 49CB5709 1F473229 6579AB44 FCD17F0F C56A

La charge utile KEr est la suivante :
0000008c 00150000 00D0B397 5AC4B799 F5BEA16D 5E13E9AF 971D5E9B 984C9F39 728B5E57 39735A21 9B97C356 436ADC6E 95BB0352 F6BE64A6 C2912D4E F2D0433C ED2B6171 640012D9 460F015C 68226383

956E3BD0 66E797B6 23C27CE0 EAC2F551 A10C2C72 4D985207 7B87220B 6536C5C4 08A1D2AE BB8E86D678AE49CB 57091F47 32296579 AB44FCD1 7F0FC56A

La valeur Diffie-Hellman commune (girx,giry) est :

girx : 01144C7D 79AE6956 BC8EDB8E 7C787C45 21CB086F A64407F9 7894E5E6 B2D79B04 D1427E73 CA4BAA24 0A347868 59810C06 B3C715A3 A8CC3151 F2BEE417 996D19F3 DDEA

giry : 01B901E6 B17DB294 7AC017D8 53EF1C16 74E5CFE5 9CDA18D0 78E05D1B 5242ADAA 9FFC3C63 EA05EDB1 E13CE5B3 A8E50C3E B622E8DA 1B38E0BD D1F88569 D6C99BAF FA43

La valeur du secret Diffie-Hellman partagé est girx.

9. Changements par rapport à la RFC 4753

La Section 7 (Formats de données d'échange de clé ECP) de la [RFC4753] déclare que
La valeur publique Diffie-Hellman est obtenue en enchaînant les valeurs x et y.
Le format de la valeur du secret partagé Diffie-Hellman est la même que celle de la valeur publique Diffie-Hellman.

Le présent document remplace le second de ces deux paragraphés par ce qui suit :
La valeur du secret partagé Diffie-Hellman consiste en la valeur x de la valeur Diffie-Hellman commune.

Ce changement aligne le format d'échange de clé ECP sur celui utilisé dans les autres normes.

Ce changement apparaissait antérieurement dans un erratum à la RFC 4753 [Err9]. Le présent document rend obsolète la RFC 4753 et incorpore l'erratum.

La Section 8 (Vecteurs d'essais) de la [RFC4753] donne trois exemples d'accords de clé Diffie-Hellman qui utilisent les groupes ECP. Le présent document change le dernier alinéa de chaque paragraphe de la Section 8 pour refléter le nouveau format.

10. Références

10.1 Références normatives

[IANA-IKE] Internet Assigned Numbers Authority. Attributs d'échange de clé Internet (IKE). (http://www.iana.org/assignments/ipsec-registry)

[IANA-IKEv2] Paramètres IKEv2 : http://www.iana.org/assignments/ikev2-parameters

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

[RFC4753] D. Fu, J. Solinas, "Groupes ECP pour IKE et IKEv2", janvier 2007. *(Information) (Remplacée par* RFC5903)

10.2 Références pour information

[AES] U.S. Department of Commerce/National Institute of Standards and Technology, Advanced Encryption Standard (AES), FIPS PUB 197, novembre 2001. (http://csrc.nist.gov/publications/fips/index.html)

[DSS] U.S. Department of Commerce/National Institute of Standards and Technology, Digital Signature Standard (DSS), FIPS PUB 186-2, janvier 2000. (http://csrc.nist.gov/publications/fips/index.html)

[Err9] RFC Errata, Errata ID 9, RFC 4753, <http://www.rfc-editor.org >.

[GMN] J. Solinas, Generalized Mersenne Numbers, Combinatorics and Optimization Research Report 99-39, 1999. (http://www.cacr.math.uwaterloo.ca/)

[IEEE-1363] Institute of Electrical and Electronics Engineers. IEEE 1363-2000, Standard for Public Key Cryptography. (http://grouper.ieee.org/groups/1363/index.html)

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

[ISO-15946-1] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 15946-1: 2002-12-01, Information Technology: Security Techniques: Cryptographic Techniques based on Elliptic Curves: Part 1 - General.

[ISO-15946-2] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 15946-2: 2002-12-01, Information Technology: Security Techniques: Cryptographic Techniques based on Elliptic Curves: Part 2 - Digital Signatures.

[ISO-15946-3] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 15946-3: 2002-12-01, Information Technology: Security Techniques: Cryptographic Techniques based on Elliptic Curves: Part 3 - Key Establishment.

[ISO-15946-4] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 15946-4: 2004-10-01, Information Technology: Security Techniques: Cryptographic Techniques based on Elliptic Curves: Part 4 - Digital Signatures giving Message Recovery.

[ISO-18031] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 18031:2005, Information Technology: Security Techniques: Random Bit Generation.

[NIST] U.S. Department of Commerce/National Institute of Standards and Technology. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, NIST Special Publication Publication 800-56A, March 2006. (http://csrc.nist.gov/CryptoToolkit/KeyMgmt.html)

[SEC2] Standards for Efficient Cryptography Group. "SEC 2 - Recommended Elliptic Curve Domain Parameters, v. 1.0", 2000. (http://www.secg.org)

[X9.62-1998] American National Standards Institute, X9.62-1998: "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm". janvier 1999.

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

[X9.63] American National Standards Institute. X9.63-2001, "Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography". novembre 2001.

Adresse des auteurs

David E. Fu
National Information Assurance Research Laboratory
National Security Agency
mél : defu@orion.ncsc.mil

Jerome A. Solinas
National Information Assurance Research Laboratory
National Security Agency
mél : jasolin@orion.ncsc.mil