Sylvain Heraud <avavrin@gmail.com>

A propos de la fonction d'Icart

10 messages

Sylvain Heraud <sylvain.heraud@gmail.com> **Wed, Nov 17, 2010 at 13:18**
To: thomas.icart@gmail.com, jscoron@gmail.com

Bonjour,

J'ai une question à propos de la fonction d'Icart, je suis en these sur la formalisation en Coq de primitive cryptographique (Certicrypt) et on s'intéresse à vos travaux.

Dans vos papier, la fonction f(u) renvoie le point infini de la courbe si u = 0 et un point de la courbe sinon.
et son inverse renvoie les solutions d'une équation de dégrée 4.

J'aimerai prouver la double équivalence suivante,
pour tout u et g, si u est dans (finv g) <-> f u = g
avec l'hypothèse que mon algorithme qui me résout les equation de dégréé 4 a la meme propriété pour tout x in u (solve4 pol) <-> pol u = 0
(où pol est un polynome)

J'ai un problème, car je ne trouve pas d'information quand on passe le point infini à finv,
pour le moment je renvoie l'élément neutre du corps (pour coller avec le f(0) = infini)

Mais la double implication si dessus est fausse car si 0 se trouve dans les solutions de l'équation, alors f(0) serait un point de la courbe et pas le point infini

la première solution qui me parait brutale serait de supprimer l'élément neutre de l'ensemble des solutions.

Sinon dire que 0 est solution signifie que a = 0, et si on ajoute l'hypothèse a<>0 il y aurait une contradiction se qui terminerait la preuve.

Je voulais savoir se que ca faisait d'ajouter l'hypothèse a<>0 ? Sachant qu'on a l'hypothèse sur a et b pour SWU ?

Je vous remercie

Cordialement

Sylvain

Thomas Icart <thomas.icart@gmail.com> **Wed, Nov 17, 2010 at 15:12**
To: Sylvain Heraud <sylvain.heraud@gmail.com>
Cc: jscoron@gmail.com

Bonjour,

Alors dans le papier http://eprint.iacr.org/2009/226.pdf, page 5 il y a les systemes d'equations qui prouvent l'equivalence. Je vais repondre plus en details au reste.

Le 17 novembre 2010 13:18, Sylvain Heraud <sylvain.heraud@gmail.com> a écrit :

> Bonjour,
>
> J'ai une question à propos de la fonction d'Icart, je suis en these sur la formalisation en Coq de primitive cryptographique (Certicrypt) et on s'intéresse à vos travaux.
>
> Dans vos papier, la fonction f(u) renvoie le point infini de la courbe si u = 0 et un point de la courbe sinon.
> et son inverse renvoie les solutions d'une équation de dégrée 4.
>
> J'aimerai prouver la double équivalence suivante,

> pour tout u et g, si u est dans (finv g) <-> f u = g
> avec l'hypothèse que mon algorithme qui me résout les equation de dégréé 4 a la meme propriété pour tout x in u (solve4 pol) <-> pol u = 0 (où pol est un polynome)
>
> J'ai un problème, car je ne trouve pas d'information quand on passe le point infini à finv,
> pour le moment je renvoie l'élément neutre du corps (pour coller avec le f(0) = infini)

Tu vas avoir du mal a passer le point a l'infini a finv, vu que l'expression de finv est en coordonnes affine, et que comme son nom l'indique, le point a l'infini n'est pas definit pour ces coordonnes.

> Mais la double implication si dessus est fausse car si 0 se trouve dans les solutions de l'équation, alors f(0) serait un point de la courbe et pas le point infini
>
> la première solution qui me parait brutale serait de supprimer l'élément neutre de l'ensemble des solutions.
>
> Sinon dire que 0 est solution signifie que a = 0, et si on ajoute l'hypothèse a<>0 il y aurait une contradiction se qui terminerait la preuve.

En fait tu touches un point particulier. f(0) n'est pas le point a l'infini si a = 0. Dans ce cas precis, f(0) = ((-b)^(1/3), 0).

> Je voulais savoir se que ca faisait d'ajouter l'hypothèse a<>0 ? Sachant qu'on a l'hypothèse sur a et b pour SWU ?

En fait, ca fait 2 preuves differentes, une pour a <> 0 et une pour a = 0. Note que pour a =0, l'element neutre n'est pas dans l'image de f.

J'espere que ca repond a tes questions.

Thomas

> Je vous remercie
>
> Cordialement
>
> Sylvain

Sylvain Heraud <sylvain.heraud@gmail.com> **Wed, Nov 17, 2010 at 15:19**
To: Benjamin Gregoire <Benjamin.Gregoire@sophia.inria.fr>

[Quoted text hidden]

Sylvain Heraud <sylvain.heraud@gmail.com> **Wed, Nov 17, 2010 at 16:35**
To: Thomas Icart <thomas.icart@gmail.com>
Cc: jscoron@gmail.com

Merci de ta réponse, mais j'ai pas tout compris.

2010/11/17 Thomas Icart <thomas.icart@gmail.com>

> Bonjour,
>
> Alors dans le papier http://eprint.iacr.org/2009/226.pdf, page 5 il y a les systemes d'equations qui prouvent l'equivalence. Je vais repondre plus en details au reste.
>
> Le 17 novembre 2010 13:18, Sylvain Heraud <sylvain.heraud@gmail.com> a écrit :
>
> > Bonjour,
> >
> > J'ai une question à propos de la fonction d'Icart, je suis en these sur la formalisation en Coq de primitive cryptographique (Certicrypt) et on s'intéresse à vos travaux.

> Dans vos papier, la fonction f(u) renvoie le point infini de la courbe si u = 0 et un point de la courbe sinon.
> et son inverse renvoie les solutions d'une équation de dégrée 4.
>
> J'aimerai prouver la double équivalence suivante,
> pour tout u et g, si u est dans (finv g) <-> f u = g
> avec l'hypothèse que mon algorithme qui me résout les equation de dégréé 4 a la meme propriété pour tout x in u (solve4 pol) <-> pol u = 0 (où pol est un polynome)
>
> J'ai un problème, car je ne trouve pas d'information quand on passe le point infini à finv,
> pour le moment je renvoie l'élément neutre du corps (pour coller avec le f(0) = infini)

Tu vas avoir du mal a passer le point a l'infini a finv, vu que l'expression de finv est en coordonnes affine, et que comme son nom l'indique, le point a l'infini n'est pas définit pour ces coordonnes.

Ok, c'est juste un problème de Coq ou tu dois tout définir, et mon type (élément de groupe) est soit le point infini, soit un point sur la courbe, (mais c'est pas un gros problème) c'est plus la suite qui me pose probleme

> Mais la double implication si dessus est fausse car si 0 se trouve dans les solutions de l'équation, alors f(0) serait un point de la courbe et pas le point infini
>
> la première solution qui me parait brutale serait de supprimer l'élément neutre de l'ensemble des solutions.
>
> Sinon dire que 0 est solution signifie que a = 0, et si on ajoute l'hypothèse a<>0 il y aurait une contradiction se qui terminerait la preuve.

En fait tu touches un point particulier. f(0) n'est pas le point a l'infini si a = 0. Dans ce cas precis, f(0) = ((-b)^(1/3), 0).

Dans le papier page 4, on a "For u = 0, we fix f_(a,b)(0) = O (l'element neutre de la courbe)
Et dans ma définition du groupe sur les courbes, mon élément neutre c'est le point à l'infini !
Mais la tu me dis que f(0) est un point de la courbe, ((-b)^(1/3), 0)).

En tout cas merci de répondre à mes questions !

> Je voulais savoir se que ca faisait d'ajouter l'hypothèse a<>0 ? Sachant qu'on a l'hypothèse sur a et b pour SWU ?

En fait, ca fait 2 preuves differentes, une pour a <> 0 et une pour a = 0. Note que pour a =0, l'element neutre n'est pas dans l'image de f.

J'espere que ca repond a tes questions.

Thomas

> Je vous remercie
>
> Cordialement
>
> Sylvain

Sylvain Heraud <sylvain.heraud@gmail.com> **Wed, Nov 17, 2010 at 16:47**
To: Thomas Icart <thomas.icart@gmail.com>
Cc: jscoron@gmail.com

OK désolé je crois avoir compris, la fin de ton mail

si a <> 0 alors f(0) = infini (et j'ai pas de problème pour ma preuve car j'ai l'hypothèse a <> 0)
si a = 0 alors f(0) est une point de la courbe

donc le papier traite le cas a <> 0 en disant que f(0) = O

C'est bien ca ?

Sylvain

2010/11/17 Sylvain Heraud <sylvain.heraud@gmail.com>
[Quoted text hidden]

Thomas Icart <thomas.icart@gmail.com> **Wed, Nov 17, 2010 at 16:51**
To: Sylvain Heraud <sylvain.heraud@gmail.com>
Cc: jscoron@gmail.com

Le 17 novembre 2010 16:47, Sylvain Heraud <sylvain.heraud@gmail.com> a écrit :

> OK désolé je crois avoir compris, la fin de ton mail
>
> si a <> 0 alors f(0) = infini (et j'ai pas de problème pour ma preuve car j'ai l'hypothèse a <> 0)
> si a = 0 alors f(0) est une point de la courbe
>
> donc le papier traite le cas a <> 0 en disant que f(0) = O
>
> C'est bien ca ?

Voila tout a fait! Ok c'est une legere erreur... ;-)

Thomas
[Quoted text hidden]

Sylvain Heraud <sylvain.heraud@gmail.com> **Wed, Nov 17, 2010 at 16:52**
To: Thomas Icart <thomas.icart@gmail.com>
Cc: jscoron@gmail.com

Ok merci en tout cas !

Sylvain
[Quoted text hidden]

Sylvain Heraud <sylvain.heraud@gmail.com> **Wed, Nov 24, 2010 at 14:53**
To: Thomas Icart <thomas.icart@gmail.com>

Bonjour,

Bon désolé, mais j'ai encore une question :/

Petit rappel !
A=0 => f(0) = ((-b)^(1/3), 0))
A<>0 => f(0) = inf
et f(u) = f_papier(u)

Pr contre pour finv(x,y)
déjà il faut que (x,y) soit dans l'image de f !
si A<>0 on utilise la preuve du papier, (les solutions sont les solutions de $u^4 - 6u^2x + 6uy - 3A = 0$)

si on veut monter que tout u,g si u est dans finv g alors f u = (x, y)

le problème c'est que quand A = 0 et u=0
l'équation $u^4 - 6u^2x + 6uy - 3A = 0$ se simplifie en 0 =0
donc on perd les informations sur x et y
et on peut pas prouver que f u = ((-b)^(1/3), 0)) = (x, y)

J'ai l'impression que finv est aussi différant quand A=0, mais j'ai pas envi de faire n'importe quoi
par exemple si on doit résoudre un équation de la forme $a.u^4 + b.u^3 + c.u^2 + d.u + y = 0$
ca regarde le problème pour le y, car si on a u=0 on sait que y = 0

[Quoted text hidden]

Thomas Icart <thomas.icart@gmail.com> **Wed, Nov 24, 2010 at 15:03**
To: Sylvain Heraud <sylvain.heraud@gmail.com>

Bonjour,

Pour A=0,
le polynome, c'est :
u^3 - 6ux + 6y =0

(au cas ou, c'est les solution de y = u x + v avec v = - u ^3 / 6)

donc oui le polynome est different, et il est meme de degre 3.
Thomas

Le 24 novembre 2010 14:53, Sylvain Heraud <sylvain.heraud@gmail.com> a écrit :

[Quoted text hidden]

Sylvain Heraud <sylvain.heraud@gmail.com> **Fri, Nov 26, 2010 at 13:09**
To: Santiago Zanella <szanella@gmail.com>

[Quoted text hidden]
