

# Re: bilinear pairing between special groups

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2005-06/msg02409.html>

---

- *From:* Zsuzsanna Doncho <nospam@xxxxxxxxxxx>
  - *Date:* Wed, 15 Jun 2005 20:08:52 +0200
- 

Hi,

I will try to explain things a bit clearer, tell me if things after that posting are still not clear.

Don't you think that would have been something important to mention?

Yes...sorry.

You're wrong. It's not that "it is not possible to calculate the discrete logarithm". It's that the discrete logarithm problem ->seems<- to be hard (all known deterministic algorithms run in exponential time).

Ok, you are right... it seems to be hard.

So in fact, for 2 given points  $Q_1, Q_2 \in G_1$  ( $G_1$  is of prime order  $q$ ) and a given value  $a = e(Q_1, Q_2)^x \in G_2$ , where  $G_2$  is of prime order  $q$ , I can't calculate the value  $x$  ( $x \in \mathbb{Z}_q$ ).

We do not know of any way to ->efficiently<- find it.

Yes, that was what I want to say.

As far as I know, it is possible to calculate the

## Re: bilinear pairing between special groups

discrete logarithm of  $a=g^x \bmod n^2$ , where  $g$  has order  $n$ . Then it is possible to calculate the value  $x \bmod n$ .

I don't understand this sentence.

Do you mean, there are  $\rightarrow$ efficient $\leftarrow$  algorithms to find the discrete logarithm base  $g$  modulo  $n^2$  when  $g$  has order  $n$  in  $(\mathbb{Z}_{\{n^2\}})^*$ ?

And what does the last sentence mean? An assertion that you can find  $x$ , or a hope?

What I wanted to say, with the sentence above was:  
Given the value  $g, n$  and  $a=g^x \bmod n^2$ , where  $g$  has order  $n$  and  $x \in \mathbb{Z}_n$ , one can efficiently calculate the value  $x \bmod n$ . So that's the discrete log of  $a \bmod n^2$ , or am I misunderstanding something?

What I now wanna do is the following:  
Given the values:  
 $c_1 = e(Q_1, Q_2)^x * g^{\{m_1\}} \bmod n^2$   
 $c_2 = e(Q_1, Q_2)^{-x} * g^{\{m_2\}} \bmod n^2$   
it is impossible to calculate  $m_1$  and  $m_2$  and  $x$ ,

You keep using that word ("impossible"). I do not think it means what you think it means.

Yes... with impossible, I wanted to say, that you can't calculate it efficiently, and possible means: it can be calculated efficiently.

but it is possible to calculate the following:  
 $c_1 * c_2 = e(Q_1, Q_2)^x * g^{\{m_1\}} * e(Q_1, Q_2)^{-x} * g^{\{m_2\}} \bmod n^2$   
 $= g^{\{m_1+m_2\}} \bmod n^2$ , where  $g$  has order  $n$ , then it is possible to calculate  $m_1+m_2 \bmod n$ .

Can I do such things?

So I wanna know 2 things:

- 1.) Given the values  $c_1, c_2, Q_1, Q_2, n$ , is it hard to calculate the values  $x, m_1, m_2$ ?
- 2.) Given the values  $c_1, c_2, Q_1, Q_2, n$ , is it "possible" to calculate

Re: bilinear pairing between special groups

efficiently the value  $m_1+m_2 \bmod n$ ?

Bye and thanks for your patience,  
Zsuzsi

.