

# Re: bilinear pairing between special groups

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2005-06/msg02461.html>

---

- *From:* Zsuzsanna Doncho <nospam@xxxxxxxxxxx>
  - *Date:* Wed, 15 Jun 2005 22:14:44 +0200
- 

Hi,

Definition. The 'Generalized Discrete Logarithm Problem' (GDLP) is the following: given a finite CYCLIC [emphasis added] group  $G$  of order  $n$ , a generator  $a$  of  $G$ , and an element  $b$  of  $G$ , find the integer  $x$ ,  $0 \leq x \leq n-1$  such that  $b = a^x$ .

So, what you describe is neither the DLP nor the GDLP. (Never mind that you never specified a generator; let's assume that's given somewhere). You are working with a group which is NOT cyclic. You can generalize the GDLP further, but then it may not always have solutions.

Yes, it's not the DLP problem nor the GDLP problem, you are right. As you wrote below, you "agree" with my hope that 1. is hard, that means: Given the values  $c_1, c_2, Q_1, Q_2, n$ , is it hard to calculate the values  $x, m_1, m_2$ .

So now I am searching for a way to efficiently calculate the discrete logarithm of  $c = g^x \bmod n^2$ , where  $g$  has order  $n$  in  $Z_{\{n^s\}}$ , so for example I could set it to  $g = n+1$ . Further, we have  $x \in Z_{\{n^2\}}$ , and  $n$  is the product of 2 primes. But this seems to be solved (see below).

For example, let's say  $p=3$  and  $q=5$ . Then  $n=15$ ,  $n^2 = 225$ , and the group of elements prime to 225 is of order  $3*2*5*4 = 120$ . But it is not cyclic. If it were cyclic, then there would be one and only one element of order 2. Yet 224, 199, and 26 all have multiplicative order

## Re: bilinear pairing between special groups

2 modulo 225.

Now, you are in a better position in terms of a subgroup of order 5, since then there is only one choice: if  $x^5 = 1 \pmod{225}$ , then  $x^5 = 1 \pmod{9}$ , hence  $x = 1 \pmod{9}$ , and  $x^5 = 1 \pmod{25}$ , so  $x=1, 6, 11, 16, 21 \pmod{25}$ . Using the Chinese Remainder Theorem gives you the only solutions modulo 225:

1, 181, 136, 91, 46.

So will you be working inside of  $\langle 181 \rangle$  in  $(\mathbb{Z}_{225})^*$ ?

On what grounds do you say that the problem of (i) finding out the cyclic group of order  $q$  in  $(\mathbb{Z}_{n^2})^*$ ; and (ii) solving the GDLP there, is "easy"?

Of course, if  $p < q$ , then since  $q$  is prime to  $p(p-1)$ , the order of the group of units modulo  $p^2$ , this will always happen, so you will have a unique group of order  $q$  sitting inside  $(\mathbb{Z}_{n^2})^*$ . If you have a nontrivial solution to  $x^q = 1 \pmod{q^2}$ , then you can use the Chinese Remainder Theorem to find a generator for this group.

Do you have an efficient way of solving that problem?

You can find the algorithm in:

[http://www.daimi.au.dk/~ivan/GenPaillier\\_finaljour.ps](http://www.daimi.au.dk/~ivan/GenPaillier_finaljour.ps)  
on page 6.

I took again a look to that algorithm, and I found a further requirement:  $\gcd(n, \phi(n)) = 1$ .

On what grounds do you assert that, having found the unique cyclic subgroup of order  $q$  sitting inside  $(\mathbb{Z}_{n^2})^*$ , you have an efficient way of solving the GDLP  $\rightarrow$ there $\leftarrow$ ?

In fact that was my questions. I don't have any grounds, on which I assert solving the GDLP in this special group as you described.

## Re: bilinear pairing between special groups

Solving the GDLP in an arbitrary cyclic group  $G$  of order  $n$  is essentially equivalent to finding an isomorphism between  $G$  and  $Z_n$ . While not an expert on cryptography, I do not see why it would be simpler to solve this problem in the group  $(Z_{n^2})^*$ , which will necessarily involve larger numbers, than in the group  $(Z_q)^*$ .

To tell you the truth (I think you already recognize it), my understanding of math is sadly poor. Although I try to understand things, often I have a lack at the basics. So in fact, although I read the paper, I mentioned above, I wasn't able why the algorithm described in the paper from above, is correct and works efficiently. In fact, I suppose it is correct and does what the authors supposed it does.

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  $x, m_1, m_2$ ?

I would expect so. What makes you think it would be easy?

I agree with you. I only wanted to be sure... maybe I overlook some important details.

2.) Given the values  $c_1, c_2, Q_1, Q_2, n$ , is it "possible" to calculate efficiently the value  $m_1+m_2 \bmod n$ ?

The only thing here which gives me a pain, is the thing with the bilinear pairing. From the paper, I mentioned above, I know that it could be done efficiently, but what happens with the bilinear pairing, are there problems in using it in the groups, you need for the algorithm, i.e.  $(Z_{n^2})^*$ ?

Bye and thanks in advance for any help,  
Zsuzsi

.