

# Re: bilinear pairing between special groups

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2005-06/msg02483.html>

---

- *From:* Zsuzsanna Doncho <nospam@xxxxxxxxxxx>
  - *Date:* Wed, 15 Jun 2005 23:11:23 +0200
- 

Hi,

pp. 6 of that is the proof that there is a polynomial time algorithm for inverting the map

$$\mathbb{Z}_{n^s} \times (\mathbb{Z}_n)^* \rightarrow (\mathbb{Z}_{n^{s+1}})^*$$

given by  $(x,r) \mapsto (1+n)^x r^{n^s} \pmod{n^{s+1}}$ ,

PROVIDED that you know the lcm of  $p-1$  and  $q-1$  (where  $p$  and  $q$  are primes, and  $n=pq$ ).

So you would need to know  $p$  and  $q$  (as far as we know, though it is possible you may be able to find  $\text{lcm}(p-1,q-1)$  without factoring  $n$ ).

But the algorithm on pp. 6, as far as I understand it, you can use for calculating the discrete logarithm, not?

They wrote:

"Then using the above algorithm find  $i \pmod{n^s}$  and extract  $i$ ." In fact they only know  $n+1$  and the factorization of  $n$  (and the  $\lambda$ ). So they have:  $c = (1+n)^{i \pmod{n^{s+1}}}$  and with that they calculate the value  $i \pmod{n}$ . So it is the "discrete logarithm" of  $c$  with base  $1+n$ .

But is that the question I asked you? I asked you if you had an efficient algorithm for finding the cyclic group of order  $q$  sitting inside of  $(\mathbb{Z}_{n^2})^*$ . How do you obtain it from the fact that the map

$$\mathbb{Z}_{pq} \times (\mathbb{Z}_{pq})^* \rightarrow (\mathbb{Z}_{(pq)^2})^*$$

## Re: bilinear pairing between special groups

given by  $(x,r) \mapsto (1+n)^{x*r^{n^2}}$

can be quickly inverted?

I sadly don't know. Probably not.

But what the authors are saying it does is not what you are saying you will use it for. The first part of the proof says that they are going to give an algorithm for solving the very specific problem of

"Finding  $i$  from  $(1+n)^i \pmod{n^{s+1}}$ "

This is not the discrete logarithm problem, since we do now know the order of  $(1+n)$  in the group in question. Note also that all of the paper assumes that  $n$  is an RSA modulus. so  $n = pq$ , and IN GENERAL, you do not know  $p$  and  $q$  (so, presumably, you do not know  $\text{lcm}(p-1, q-1)$  ->either<-).

You are right, it is not the discrete logarithm problem, but it looks quite similar, not ;).

So there is no solution for my problem (see below)?

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

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.  $(\mathbb{Z}_{n^2})^*$ ?

## Re: bilinear pairing between special groups

The paper EXPLICITLY tells you what the bilinear pairing is. What exactly is your problem?

Where does the paper tells me explicitly what the bilinear pairing is?

So I told you what my problem is:

- 1.) Given the values  $c_1=e(Q_1, Q_2)^x * g^{m_1}$ ,  $c_2=e(Q_1, Q_2)^x * g^{m_2}$ ,  $Q_1, Q_2, g, n$ , (and  $p, q$ , if this doesn't contradict the second problem) is it hard to calculate the values  $x, m_1, m_2$ ?
- 2.) Given the values  $c_1, c_2, Q_1, Q_2, g, n$ , is it "possible" to calculate efficiently the value  $m_1+m_2 \bmod n$ ?

In fact for my purpose it is not important if  $g$  is a generator, or not, it is not important if  $p, q$  are special primes or not, if you know the factorization of  $n$  or not, etc. The only important thing are 1. and 2.

The more you write, the more I think, that such is not possible, but maybe you have an idea of construction.

Thanks in advance,  
Zsuzsi

.