

Re: bilinear pairing between special groups

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-06/msg02459.html>

- *From:* magidin@xxxxxxxxxxxxxxxxxxxx (Arturo Magidin)
 - *Date:* Wed, 15 Jun 2005 20:30:57 +0000 (UTC)
-

In article <d8q271\$a12\$04\$1@xxxxxxxxxxxxxxxxxxxx>, Zsuzsanna Doncho <nospam@xxxxxxxxxx> wrote:

>> 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
 >on page 6.

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

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

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 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

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

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

can be quickly inverted?

>> Solving the GDLP in an arbitrary cyclic group G of order n is

Re: bilinear pairing between special groups

>> 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.

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<-).

>>>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. $(Z_{n^2})^*$?

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

--
=====
"It's not denial. I'm just very selective about
what I accept as reality."
--- Calvin ("Calvin and Hobbes")
=====

Arturo Magidin
magidin@xxxxxxxxxxxxxxxxxxxx

.



Re: bilinear pairing between special groups

- **Follow-Ups:**
 - ◆ **Re: bilinear pairing between special groups**
 - ◇ From: Zsuzsanna Doncho

- **References:**
 - ◆ **bilinear pairing between special groups**
 - ◇ From: Zsuzsanna Doncho
 - ◆ **Re: bilinear pairing between special groups**
 - ◇ From: Zsuzsanna Doncho
 - ◆ **Re: bilinear pairing between special groups**
 - ◇ From: Arturo Magidin
 - ◆ **Re: bilinear pairing between special groups**
 - ◇ From: Zsuzsanna Doncho

- Prev by Date: **Re: any math forum that supports math equations?**
- Next by Date: **Re: Orlow cardinality question**
- Previous by thread: **Re: bilinear pairing between special groups**
- Next by thread: **Re: bilinear pairing between special groups**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**