

Re: Order question

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-04/2761.html>

From: Peter Fairbrother (zenadsl6186_at_zen.co.uk)

Date: 04/30/04

Date: Fri, 30 Apr 2004 04:20:04 +0100

An Metet wrote:

> *NOTE: This message was sent thru a mail2news gateway.*

> *No effort was made to verify the identity of the sender.*

> -----

>

> *Peter Fairbrother wrote:*

>>> *Next question. Can you simply show that the subgroup of order q is the same*

>>> *group as the group of QR's? I've done this before, but I lost it.*

>

> *We will show that every element in the subgroup of order q is a QR,*

> *by constructing a square root for each element. Each such element can*

> *be expressed as g^k for a g which generates the group. If k is even*

> *the square root is $g^{(k/2)}$. If k is odd, $k+q$ is even since q is odd,*

> *so $g^{((k+q)/2)}$ is the square root. QED.*

Neat. I like it.

>> *A typical DH with optimisation will have $p = mq+1$, and use a generator of*

>> *the subgroup of order q . Are there any security implications to using a q of*

>> *the usual say 160 bits size, but with small Hamming weight?*

>

> *Of course DH is not known to be as secure as the DL problem. So there*

> *are two questions here: one is whether such a q would provide an attack*

> *on DH without solving discrete logs; and the other is whether such a*

> *q would speed up solutions of the DL problem. Unfortunately I am not*

> *qualified to answer either of these.*

Actually, it's DDH in this particular case, now that I think about it.

> *I can only state the obvious, that the commonly discussed DL algorithms,*

> *including Shanks, Pollard rho and kangaroo, do not get sped up by a*

> *special q , nor would methods aiming at p like the number field sieve be*

> *affected by q at all. The one minor consideration is that a low hamming*

> *weight q is likely to be half the size of an average q of the same bit*

> *length, hence would be solved $\sqrt{2}$ times faster than an average q by*

> *the q -based algorithms.*

sci.crypt: Re: Order question

Half the size? Shurely shome mishtake. I make it $2/3$ on average.

Careful selection would overcome that not-very-important problem anyway.

- > *A low hamming weight q would be advantageous for allowing quick tests*
- > *of group membership. Many DL protocols have hidden flaws if they skip*
- > *these tests, as shown for example by the work of Lim and Lee. If such*
- > *q values are in fact safe then they would be useful for DL protocols.*

That's what I want to use them for. The intermediate modular squarings are available for free (we are going to do the exponentiation anyway, unless the test fails), and a low Hamming weight q means that only a few modmults will test group membership. Almost a free test, and it's essential for semantic security.

--

Peter Fairbrother