

Re: Is this simple scheme secure?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-01/2081.html>

From: Gregory G Rose (ggr_at_qualcomm.com)

Date: 01/30/04

Date: 30 Jan 2004 14:13:51 -0800

In article <q%zSb.80748\$dP1.206618@newsc.telia.net>,

Foo Bar <foobar965@hotmail.com> wrote:

>It can be used for things like "I know a n -coloring of this graph" or "I
>know an isomorphism between these two graphs". I don't know the area
>well enough to comment on the case of more general secrets.

Zero Knowledge Proofs are truly magical stuff. The problem is it's almost impossible to understand without reading the literature. The hash example presented earlier in this thread isn't zero-knowledge, because A can go offline and verify guesses about M... information about M came back from B.

Anything that can be proven can be proven in the zero-knowledge framework; that is one of the relatively surprising (to me, anyway) results. But not necessarily efficiently...

Greg.

--

Greg Rose

232B EC8F 44C6 C853 D68F E107 E6BF CD2F 1081 A37C

Qualcomm Australia: <http://www.qualcomm.com.au>