

sci.crypt: Re: My solution to chess grandmaster problem in zero knowledge proofs of identity.

## Re: My solution to chess grandmaster problem in zero knowledge proofs of identity.

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-02/4896.html>

---

*From:* Vladimir Shabanov ([virl\\_at\\_mail.ru](mailto:virl_at_mail.ru))

*Date:* 02/27/05

Date: 27 Feb 2005 11:26:57 -0800

Maybe I don't understand grandmaster problem.  
My protocol is intended to be against "mafia fraud" attacks.

> *Step 2 is useless from the standpoint of authentication*

No, I think it doesn't.

> *Bob does not "restore" the unsigned message--he verifies  
> that the signature could only have been  
> computed by someone holding Alice's private key(s).*

Yes, of course.

> *When he decrypts  $Q$  using his private key, of course  
> it's going to be what he sent since it was encrypted  
> with his own public key.  
> In other words, anyone could have encrypted it.*

But Bob, thanks to this protocol, in result gets knowledge of two things:

- 1) That other side knows private key that corresponds to public key this side sent to Bob.
- 2) That other side is not mafiosi (who just redirects Alice's answers).