

Re: privacy amplification

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-11/1335.html>

From: Anton Stiglic (*astiglic_at_okiok.com*)

Date: 11/26/04

Date: 26 Nov 2004 10:39:15 -0800

simon.johnson@gmail.com (Simon Johnson) wrote in message
news:<f03d8ae0.0411260706.c5d302@posting.google.com>...
> *chrismuktar@gmail.com (Chris Muktar) wrote in message*
news:<f3bd390a.0411260304.2ab2bdbc@posting.google.com>...
> > Hi,
> >
> > I'm just trying to understand "Privacy Amplification" and am working
> > from paper [1].
> >
> > I understand that Bob and Alice randomly select a compression function
> > g from a set of compression functions G , and encode the secret $K =$
> > $g(W)$ where W is the input string.
> >
> > It is understood that Eve has full knowledge of the set G , and
> > therefore also g , but it is also understood that if Eve does not know
> > which g to select, she will be unable to deduce the secret K from the
> > input string W .
> >
> > The problem I encounter is, how do Bob and Alice agree which g they
> > are going to use, such that their compression functions coincide?
> >
> > Note: I am working in the context of quantum cryptography, so that
> > $P[VW]$ is specific to that application.
> >
> > Cheers!
> > Chris
> >
> > [1] "Generalized Privacy Amplification", Bennet, Brassard, Crepeau,
> > Maurer, *IEEE Transactions on Information Theory* Vol 41, No 6, November
> > 1995
> >
> > Unless i'm completely missing the point this is actually a well solved
> > problem. You could use a signed diffie-helman exchange to agree the
> > choice of g over an insecure channel without Eve knowing which g you
> > picked.

The idea of privacy amplification is for Alice and Bob to take some secret, for which an adversary might have some knowledge about, and to

sci.crypt: Re: privacy amplification

generate from it a secret for which the adversary has hardly any information about, using a public communication channel. Furthermore, we want some mechanism that provides us with unconditional security. If you introduce DH, you break the unconditional security property, you security becomes conditional to the DH problem (type of problems that become easy to solve with a quantum computer as you noted).

I think the general idea, in a quantum setting, is to do a quantum key exchange (unconditionally secure) in order to come up with a shared secret string, for which an adversary might have some information, and then apply privacy amplification to generate a secret shared string for which the adversary has almost no information about.

Of course, the problem with quantum key exchange is the need to authenticate the other party in the key exchange, and to implement this you need to either share a small secret a priori or execute some protocol whos security is based on some assumption. This has already been discussed at length on this newsgroup.

--Anton