

Re: Curve25519-based EC-KCDSA

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-08/msg01654.html>

- *From:* Kristian Gjøsteen <kristiag+news@xxxxxxxxxxxxx>
 - *Date:* Wed, 30 Aug 2006 12:36:47 +0000 (UTC)
-

David Wagner <daw-usenet@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

In other words, perhaps I should have phrased my concern in terms of the level of assurance, rather than a binary "has a security proof" vs "doesn't" distinction.

Ok, that muddies everything up. Then simple analysis won't help any more, I guess.

Still, I feel that some attacks on DSA without hash function would be interesting, because they could put a lot more stress on the hash function. The only attack I know of generates a signature on a random message, but since the hash function is already designed to be one-way, that attack isn't interesting.

Unless I'm still not thinking clearly or have missed interesting attacks (which is likely), it seems possible there aren't any interesting attacks on DSA without hash function.

I don't think the "mostly invertible" bit is necessary.

The "mostly invertible" bit is a heuristic suggestion that any scheme that relies only on a collision resistant hash function (not random oracle) to process the message must probably be secure without that hash function.

--
Kristian Gjøsteen