

Re: The importance of IVs

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-08/1680.html>

From: mobius30 (mobius30_at_hushmail.com)

Date: 08/27/05

Date: 27 Aug 2005 14:30:37 -0700

Paul Rubin wrote:

>*No. There is a class of known weak keys for reduced-round variants.*

Yes, I've heard of this, though I don't have any experience with it yet. From what I understand the weak-key attack has no effect on 16-round Blowfish. As you said, only in reduced-round variants. However, it would be interesting to code an app that automatically checks for weak keys after key expansion/generation. I imagine it would involve logically checking each S-box for twins. However this would take up more CPU clock cycles, slowing down the app significantly.