

Re: Signature length of DSA

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-11/2018.html>

From: Henrick Hellström (henrick.hellstrm_at_telia.com)

Date: 11/29/03

Date: Sat, 29 Nov 2003 01:24:22 GMT

Paul Rubin wrote:

- > *I seem to remember reading that there's some trick that lets you*
- > *shrink ECDSA signatures to 200 bits(?) or so, with the same security*
- > *as normal 320 bit signatures. I don't remember any more though. Anyone?*

Confer the paper "Signcryption and Its Applications in Efficient Public Key Solutions" by Yuliang Zheng. The trick is to use a keyed hash function (e.g. hmac) to calculate r and only use half of the bits of the output.