

Overview over homomorphic encryption schemes

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-08/1827.html>

From: Anika Schwanstein (*schwanstein_at_msn.it*)

Date: 08/27/04

Date: Fri, 27 Aug 2004 14:53:38 +0200

Hi,

can someone give me a short overview over the different cryptosystems which are homomorphic. I know about 3 systems:

ElGamal-scheme

Paillier-scheme

Damgaard/Jurik-scheme

Are there more?

A very interesting property of the Damgaard/Jurik-scheme is the length-flexibility. Are there more schemes which support this length flexibility?

Thanks in advance,
Anika