Cryptology ePrint Archive: Report 2011/254

Using the Cloud to Determine Key Strengths

T. Kleinjung and A.K. Lenstra and D. Page and N.P. Smart

Abstract: We develop a new methodology to assess cryptographic key strength using cloud computing, by calculating the true economic cost of (symmetric- or private-) key retrieval for the most common cryptographic primitives. Although the present paper gives the current costs, more importantly it provides the tools and infrastructure to derive new data points at any time in the future, while allowing for improvements such as of new algorithmic approaches. Over time the resulting data points will provide valuable insight in the selection of cryptographic key sizes.

Category / Keywords: implementation /

Date: received 23 May 2011

Contact author: nigel at cs bris ac uk