# Cryptology ePrint Archive: Report 2012/724

**A Coding-Theoretic Approach to Recovering Noisy RSA Keys**

*Kenneth G. Paterson and Antigoni Polychroniadou and Dale L. Sibborn*

**Abstract:** Inspired by cold boot attacks, Heninger and Shacham (Crypto 2009) initiated the study of the problem of how to recover an RSA private key from a noisy version of that key. They gave an algorithm for the case where some bits of the private key are known with certainty. Their ideas were extended by Henecka, May and Meurer (Crypto 2010) to produce an algorithm that works when all the key bits are subject to error. In this paper, we bring a coding-theoretic viewpoint to bear on the problem of noisy RSA key recovery. This viewpoint allows us to cast the previous work as part of a more general framework. In turn, this enables us to explain why the previous algorithms do not solve the motivating cold boot problem, and to design a new algorithm that does (and more). In addition, we are able to use concepts and tools from coding theory -- channel capacity, list decoding algorithms, and random coding techniques -- to derive bounds on the performance of the previous algorithms and our new algorithm.

**Category / Keywords:**

**Publication Info:** Full version of paper published at Asiacrypt 2012

**Date:** received 27 Dec 2012, last revised 6 Jan 2013

**Contact author:** kenny paterson at rhul ac uk