Cryptology ePrint Archive: Report 2011/038

Cold Boot Key Recovery by Solving Polynomial Systems with Noise

Martin Albrecht and Carlos Cid

Abstract: A method for extracting cryptographic key material from DRAM used in modern computers has been recently proposed in [9]; the technique was called Cold Boot attacks. When considering block ciphers, such as the AES and DES, simple algorithms were also proposed in [9] to recover the cryptographic key from the observed set of round subkeys in memory (computed via the cipher's key schedule operation), which were however subject to errors due to memory bits decay. In this work we extend this analysis to consider key recovery for other ciphers used in Full Disk Encryption (FDE) products. Our algorithms are also based on closest code word decoding methods, however apply a novel method for solving a set of non-linear algebraic equations with noise based on Integer Programming. This method should have further applications in cryptology, and is likely to be of independent interest. We demonstrate the viability of the Integer Programming method by applying it against the Serpent block cipher, which has a much more complex key schedule than AES. Furthermore, we also consider the Twoﬁsh key schedule, to which we apply a dedicated method of recovery.

Category / Keywords: secret-key cryptography / polynomial system solving, side-channel attacks, blockcipher, noise-tolerant learning

Date: received 20 Jan 2011

Contact author: malb at lip6 fr