Computer Science > Information Theory

On fuzzy syndrome hashing with LDPC coding

Marco Baldi, Marco Bianchi, Franco Chiaraluce, Joachim Rosenthal, Davide Schipani

(Submitted on 8 Jul 2011 (v1), last revised 31 Oct 2011 (this version, v2))

The last decades have seen a growing interest in hash functions that allow some sort of tolerance, e.g. for the purpose of biometric authentication. Among these, the syndrome fuzzy hashing construction allows to securely store biometric data and to perform user authentication without the need of sharing any secret key. This paper analyzes this model, showing that it offers a suitable protection against information leakage and several advantages with respect to similar solutions, such as the fuzzy commitment scheme. Furthermore, the design and characterization of LDPC codes to be used for this purpose is addressed.

Comments: in Proceedings 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), ACM 2011. This is the author's version of the work. It is posted here by permission of ACM for your personal use. Not for redistribution

Subjects: **Information Theory (cs.IT)**; Cryptography and Security (cs.CR)

Cite as: **arXiv:1107.1600 [cs.IT]**

(or **arXiv:1107.1600v2 [cs.IT]** for this version)

Submission history

From: Davide Schipani [view email]

[v1] Fri, 8 Jul 2011 10:32:26 GMT (103kb)

[v2] Mon, 31 Oct 2011 15:20:14 GMT (103kb)

Which authors of this paper are endorsers?