Cryptology ePrint Archive: Report 2011/309

On Constructing Homomorphic Encryption Schemes from Coding Theory

Frederik Armknecht and Daniel Augot and Ludovic Perret and Ahmad-Reza Sadeghi

Abstract: Homomorphic encryption schemes are powerful cryptographic primitives that allow for a variety of applications. Consequently, a variety of proposals have been made in the recent decades but none of them was based on coding theory. The existence of such schemes would be interesting for several reasons. First, it is well known that having multiple schemes based on different hardness assumptions is advantageous. In case that one hardness assumption turns out be wrong, one can switch over to one of the alternatives. Second, fo some codes decoding (which would represent decryption in this case) is a linear mapping only (if the error is known), i.e., a comparatively simple operation. This would make such schemes interesting candidates for constructing of fully-homomorphic schemes based on bootstrapping (see Gentry, STOC'09).

We show that such schemes are indeed possible by presenting a natural construction principle. Moreover, these possess several non-standard positive features. First, they are not restricted to linear homomorphism but allow for evaluating multivariate polynomials up to a fixed (but arbitrary) degree $\mult$ on encrypted field elements. Second, they can be instantiated with various error correcting codes, even for codes with poor correcting capabilities. Third, depending on the deployed code, one can achieve very efficient schemes. As a concrete example, we present an instantiation based on Reed-Muller codes where for $\mult=2$ and $\mult=3$ and security levels between 80 and 128 bits, all operations take less than a second (after some pre-computation). However, our analysis reveals also limitations on this approach. For structural reasons, such schemes cannot be public-key, allow for a limited number of fresh encryptions only, and cannot be combined with the bootstrapping technique. We argue why such schemes are nonetheless useful in certain application scenarios and discuss possible directions on how to overcome these issues.

Category / Keywords: foundations / Homomorphic Encryption, Coding Theory, Efficiency, Provable Security

Date: received 9 Jun 2011

Contact author: armknecht at uni-mannheim de