The Arithmetic Codex: Theory and Applications

Ronald Cramer

CWI, Amsterdam & Mathematical Institute, Leiden University, The Netherlands
http://www.cwi.nl/~cramer

Abstract. We define the notion of an *arithmetic codex* (or *codex*, for short), and as a special case, *arithmetic secret sharing*. This notion encompasses as well as generalizes, in a single mathematical framework, all known types of specialized secret sharing schemes from the area of secure multi-party computation, i.e., the so-called *(strongly) multiplicative linear secret sharing schemes*.

These schemes were first studied as an abstract primitive by Cramer, Damgård, and Maurer in the late 1990s. They showed that the "*Fundamental Theorem of Information-Theoretically Secure Multi-Party Computation*," the landmark 1988 result by Ben-Or, Goldwasser, and Wigderson and, independently at the same time by Chaum, Crépeau, Damgård, admits a proof that uses this primitive as a blackbox: it is possible to bootstrap, in a blackbox fashion, from this primitive a set of atomic sub-protocols upon which general secure computation can be based. They also showed when and how multiplicative schemes (but not strongly multiplicative ones) reduce to ordinary ones and gave applications to security against non-threshold adversaries.

In 2006, Chen and Cramer showed an "asymptotically good" version of the Fundamental Theorem, where the size of the network is unbounded and where an adversary corrupts a constant fraction of the network, yet the information rate of the secret sharing primitive is constant. Their result relies on a careful choice of algebraic geometric codes, in combination with the earlier work of Cramer, Damgård, and Maurer.

In 2007 this asymptotic result turned out to have a surprising application in *two-party cryptography*, through the work of Ishai, Kushilevitz, Ostrovsky and Sahai ("*Multi-Party Computation in the Head*"). This first application was to zero knowledge for circuit satisfiability, but soon after other applications to secure two-party computation and information theory (correlation extractors) followed.

Our notion of arithmetic secret sharing is not merely a unification for its own sake. First, it casts these schemes in terms of a dedicated "representation" of K-algebras, thereby bringing the relevant mathematical structure to the surface. Second, it identifies novel types of special secret sharing schemes. And, third, there are novel cryptographic applications.

Besides presenting some elementary examples and giving an overview of the basic theory and the main applications, we discuss a construction of arithmetic secret sharing schemes based on a novel algebraic-geometric paradigm that we also introduce. This talk is mainly based on several recent joint works with Nacho Cascudo (CWI) and Chaoping Xing (NTU). But in part it is also based on recent joint work with Ivan Damgård (Aarhus University) and Valerio Pastro (Aarhus University).

K.G. Paterson (Ed.): Eurocrypt 2011, LNCS 6632, p. 1, 2011.