# Security questions of digital money systems

(Abstract)

The purpose of this study is to systematically investigate the attributes of digital cash systems on a large scale, with special emphasis on anonimity as a tool for protecting personal data, and to summarise the expected requirements for an ideal system. After defining the basic attributes of the digital cash scheme, the authorgives an overview of the evolutionary development of digital financial systems, its main phases and characteristics. He presents a wide range of various schemes and technologies, including new and creative cryptographic solutions, which can be used as basic elements of the schemes or can ensure the required attributes in a modular way. He refers to scientific publications on the schemes and presents an analysis of the attributes discussed by comparative works. He discusses certain attributes, analyses certain digital money schematics. The author then specifies the attributes of an imaginary, ideal digital cash system. Finally he discusses the main problems still unsolved in the whole research area, and gives a subjective look on the expected developments.