Privacy-Enhancing Cryptography: From Theory into Practice

Jan Camenisch

IBM Research – Zurich, Rüschlikon, Switzerland
jca@zurich.ibm.com

Abstract. We conduct an increasing part of our daily transactions electronically and thereby we leave an eternal electronic trail of personal data. We are almost never able to see what data about us we imprint, where it is processed or where it is stored. Indeed, controlling the dispersal of our data and protecting our privacy has become virtually impossible.

In this talk we will investigate the extent to which tools from cryptography and other technical means can help us to regain control of our data and to save our privacy. To this end, we will review the most important of the practical cryptographic mechanisms and discuss how they could be applied. In a second part, we will report on the readiness of the industry to indeed employ such technologies and on how governments address the current erosion of privacy.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-3-642-11799-2_36

D. Micciancio (Ed.): TCC 2010, LNCS 5978, p. 498, 2010.