1. Record Nr. UNINA9910254981303321

Autore	Traverso Giulia
Titolo	Homomorphic Signature Schemes : A Survey / / by Giulia Traverso, Denise Demirel, Johannes Buchmann
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2016
ISBN	3-319-32115-3
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (73 p.)
Collana	SpringerBriefs in Computer Science, , 2191-5768
Disciplina	004
Soggetti	Data structures (Computer science) Discrete mathematics Data Structures and Information Theory Discrete Mathematics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Chapter 1 From Digital to Homomorphic Signature Schemes -- Chapter 2 Homomorphic Signature Schemes -- Chapter 3 Evaluation of Homomorphic Signature Schemes -- Chapter 4 State of the Art of Homomorphic Signature Schemes -- Chapter 5 Suitable Homomorphic Signature Schemes for eVoting, Smart Grids, and eHealth -- Chapter 6 Conclusion -- References. .
Sommario/riassunto	Homomorphic signature schemes are an important primitive for many applications and since their introduction numerous solutions have been presented. Thus, in this work we provide the first exhaustive, complete, and up-to-date survey about the state of the art of homomorphic signature schemes. First, the general framework where homomorphic signatures are defined is described and it is shown how the currently available types of homomorphic signatures can then be derived from such a framework. In addition, this work also presents a description of each of the schemes presented so far together with the properties it provides. Furthermore, three use cases, electronic voting, smart grids, and electronic health records, where homomorphic signature schemes can be employed are described. For each of these applications the requirements that a homomorphic signature scheme should fulfill are defined and the suitable schemes already available are listed. This also

highlights the shortcomings of current solutions. Thus, this work concludes with several ideas for future research in the direction of homomorphic signature schemes.