1.	Record Nr.	UNISA996396413603316
	Autore	Shute Giles <b. 1650 or 51.>
	Titolo	A new test in lieu of the old one, by way of supposition, or, A satisfactory answer to that great and common question [[electronic resource]] : viz. if the penal laws and tests should be abolished, how shall the Protestant religion and interest be secured? / / by G.S
	Pubbl/distr/stampa	London, : Printed by George Larkin ..., 1688
	Descrizione fisica	[2], 34 [i.e. 38] p
	Soggetti	Church and state - England Great Britain History Restoration, 1660-1688
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Attributed to Giles Shute. Cf. Halkett & Laing (2nd ed.) Copy at reel 1070:15 is incorrectly identified as Wing S3711 in reel guide. Imperfect: pages stained. Reproduction of originals in the Huntington Library and the Union Theological Seminary Library, New York.
	Sommario/riassunto	eebo-0113

2. Record Nr.	UNINA9910556895903321
Titolo	Security of Biochip Cyberphysical Systems / / by Shayan Mohammed, Sukanta Bhattacharjee, Yong-Ak Song, Krishnendu Chakrabarty, Ramesh Karri
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	3-030-93274-5
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (135 pages) : illustrations
Disciplina	610.28
Soggetti	Embedded computer systems Electronic circuit design Cooperating objects (Computer systems) Embedded Systems Electronics Design and Verification Cyber-Physical Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Introduction -- Threat landscape -- Architecture for Security -- Tools for Security -- Watermarking of Bio-IP -- Obfuscation of Bio-IP -- Conclusion.
Sommario/riassunto	This book provides readers with a valuable guide to understanding security and the interplay of computer science, microfluidics, and biochemistry in a biochip cyberphysical system (CPS). The authors uncover new, potential threat and trust-issues to address, as this emerging technology is poised to be adapted at a large scale. Readers will learn how to secure biochip CPS by leveraging the available resources in different application contexts, as well as how to ensure intellectual property (IP) is protected against theft and counterfeits. This book enables secure biochip CPS design by helping bridge the knowledge gap at the intersection of the multi-disciplinary technology that drives biochip CPS. Provides tools for security analysis and verification: a machine learning (ML) framework; Paints the threat landscape of the biochip CPS, describing the threat models - the who,

the how, and the why; Uses real case studies to describe models of tampering attack, microfluidic trojan attack.