1.	Record Nr.	UNISA996465440603316
	Titolo	Advances in Information and Computer Security [[electronic resource]] : 8th International Workshop on Security, IWSEC 2013, Okinawa, Japan, November 18-20, 2013, Proceedings / / edited by Kazuo Sakiyama, Masayuki Terada
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
	ISBN	3-642-41383-8
	Edizione	[1st ed. 2013.]
	Descrizione fisica	1 online resource (XII, 319 p. 53 illus.)
	Collana	Security and Cryptology ; ; 8231
	Disciplina	005.8
	Soggetti	Computer security Data encryption (Computer science) Computer science—Mathematics Algorithms Computer communication systems Systems and Data Security Cryptology Discrete Mathematics in Computer Science Algorithm Analysis and Problem Complexity Computer Communication Networks
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di contenuto	Software and System Security -- Secure Log Transfer by Replacing a Library in a Virtual Machine -- Static Integer Overflow Vulnerability Detection in Windows Binary -- Solving Google's Continuous Audio CAPTCHA with HMM-Based Automatic Speech Recognition -- Constructions of Almost Secure Frameproof Codes Based on Small-Bias Probability Spaces -- Cryptanalysis -- Differential Power Analysis of MAC-Keccak at Any Key-Length -- Generic State-Recovery and Forgery Attacks on ChopMD-MAC and on NMAC/HMAC -- New Property of Diffusion Switching Mechanism on CLEFIA and Its Application to DFA -- Improvement of Faug`ere et al.'s Method to Solve ECDLP -- Privacy and Cloud Computing -- Statistics on Encrypted Cloud Data -- Toward

Practical Searchable Symmetric Encryption -- Unconditionally Secure Oblivious Transfer from Real Network Behavior -- Cryptographically-Secure and Efficient Remote Cancelable Biometrics Based on Public-Key Homomorphic Encryption -- Public Key Cryptosystems -- Efficient Algorithm for Tate Pairing of Composite Order -- How to Factor N1 and N2 When p1 = p2 mod 2t -- Achieving Chosen Ciphertext Security from Detectable Public Key Encryption Efficiently via Hybrid Encryption -- Cryptanalysis of the Quaternion Rainbow -- Security Protocols -- On Cheater Identifiable Secret Sharing Schemes Secure against Rushing Adversary -- One-Round Authenticated Key Exchange without Implementation Trick -- Attacks to the Proxy Re-Encryption Schemes from IWSEC2011 -- Game-Theoretic Security for Bit Commitment.

Sommario/riassunto

This book constitutes the refereed proceedings of the 8th International Workshop on Security, IWSEC 2013, held in Okinawa, Japan, in November 2013. The 20 revised selected papers presented in this volume were carefully reviewed and selected from 63 submissions. They are organized in topical sections named: software and system security, cryptanalysis, privacy and cloud computing, public key cryptosystems, and security protocols.