

1. Record Nr.	UNINA9911015637303321
Autore	Susilo Willy
Titolo	Information Security and Privacy : 30th Australasian Conference, ACISP 2025, Wollongong, NSW, Australia, July 14–16, 2025, Proceedings, Part III / / edited by Willy Susilo, Josef Pieprzyk
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2025
ISBN	981-9691-01-X
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (764 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15660
Altri autori (Persone)	PieprzykJosef
Disciplina	005.8
Soggetti	Data protection Computer security Cryptography Data encryption (Computer science) Data protection - Law and legislation Computer networks - Security measures Blockchains (Databases) Data and Information Security Principles and Models of Security Cryptology Privacy Mobile and Network Security Blockchain
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- Privacy Enhancing Technologies. -- Comparing and Improving Frequency Estimation Perturbation Mechanisms under Local Differential Privacy. -- Strong Federated Authentication With Password-based Credential Against Identity Server Corruption. -- Anonymous Credentials with Credential Redaction and Its Application to SSI-based Plug Charge for Shared Vehicles. -- Direction-Oriented Smooth Sensitivity and Its Application to Genomic Statistical Analysis. -- Sentence Embedding Generation Method for Differential Privacy Protection. .-KD-IBMRKE-PPFL: A Privacy-Preserving Federated Learning

Framework Integrating Knowledge Distillation and Identity-Based
 Multi-Receiver Key Encapsulation. -- AI Security and Privacy. --
 Identifying the Truth of Global Model: A Generic Solution to Defend
 Against Byzantine and Backdoor Attacks in Federated Learning. --
 RAGLeak: Membership Inference Attacks on RAG-Based Large Language
 Models. -- DeGain: Detecting GAN-based Data Inversion in
 Collaborative Deep Learning. -- FRFL: Fair and Robust Federated
 Learning Incentive Model Based on Game Theory. -- DPFedSub: A
 Differentially Private Federated Learning with Randomized Subspace
 Descend. -- MG-Det: Deepfake Detection with Multi-Granularity. --
 LPIA: Label Preference Inference Attack against Federated Graph
 Learning. -- DARA: Enhancing Vulnerability Alignment via Adaptive
 Reconstruction and Dual-Level Attention. -- Zeroth-Order Federated
 Private Tuning for Pretrained Large Language Models. --
 Understanding the Robustness of Machine-Unlearning Models. --
 System Security. -- Mitigating the Unprivileged User Namespaces
 based Privilege Escalation Attacks with Linux Capabilities. -- SoK:
 From Systematization to Best Practices in Fuzz Driver Generation. --
 Facial Authentication Security Evaluation against Deepfake Attacks in
 Mobile Apps. -- Short Papers. -- EAPIR: Efficient and Authenticated
 Private Information Retrieval with Fast Server Processing. --
 Ransomware Encryption Detection: Adaptive File System Analysis
 Against Evasive Encryption Tactics. -- Receiver-initiated Updatable
 Public Key Encryption: Construction, Security and Application. --
 Robust and Privacy-Preserving Dynamic Average Consensus with
 Individual Weight. -- Improving RSA Cryptanalysis: Combining
 Continued Fractions and Coppersmith's Techniques. -- Shortest
 Printable Shellcode Encoding Algorithm Based on Dynamic Bitwidth
 Selection. -- Position Paper. -- Bridging Clone Detection and
 Industrial Compliance: A Practical Pipeline for Enterprise Codebases.

Sommario/riassunto

This three-volume set in LNCS constitutes the refereed proceedings of
 the 30th Australasian Conference on Information Security and Privacy,
 ACISP 2025, held in Wollongong, NSW, Australia, during July 14–16,
 2025. The 54 full papers, 6 short papers and 1 invited paper included
 in this book were carefully reviewed and selected from 181
 submissions. They were organized in topical sections as follows:
 symmetric-key cryptography and cryptanalysis; public-key encryption;
 digital signatures and zero knowledge; cryptographic protocols and
 blockchain; post-quantum cryptography; homomorphic encryption and
 applications; cryptographic foundations and number theory; privacy
 enhancing technologies; AI security and privacy; system security.