1.	Record Nr.	UNINA9911046556503321
	Autore	Chen Xiaofeng
	Titolo	Data Security and Privacy Protection : Third International Conference, DSPP 2025, Xi'an, China, October 16–18, 2025, Proceedings, Part II / / edited by Xiaofeng Chen, Haibo Hu, Ding Wang
	Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2026
	ISBN	981-9531-85-3
	Edizione	[1st ed. 2026.]
	Descrizione fisica	1 online resource (376 pages)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 16177
	Altri autori (Persone)	HuHaibo WangDing
	Disciplina	005.8
	Soggetti	Data protection Data protection - Law and legislation Cryptography Data encryption (Computer science) Computer security Computer networks - Security measures Data and Information Security Privacy Cryptology Security Services Principles and Models of Security Mobile and Network Security
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	-- AI-based Security Applications and Technologies. -- Dual-FER: A Dual-Network Approach to Facial Expression Recognition with Enhanced Generalization. -- Digital Forensics in Ransomware Analysis for Windows-Based Computer Systems. -- Evaluating Deep Learning in Gait Recognition. -- Composite Weather Image Restoration Based on Two-Stage Feature Learning. -- An Efficient Explainability Framework for Graph Neural Networks. -- Cryptographic Protocols Design and Analysis. -- Post-Quantum Privacy-Preserving Smart Meter Data Collection Scheme from Coding. -- High-Throughput Threshold SM2

Signatures with Robustness. -- Attacks on Implementations of Lindell 17 and its Variants. -- RRSC: Revocable Ring Signature Scheme over CRYSTALS-Dilithium for VANETs. -- A Key Derivation Tree-Based Encryption and Verification Scheme for EV Data Auditing. -- Security Weaknesses in ISO 15118-Based CCS2 Charging. -- Model Security and Copyright Protection. -- SemBits: Multi-Bit Semantic Watermarking with Sentence-Level Hashing for LLMs. -- Robust Ownership Verification in Large Language Models via Equivalent Neuron Pair Encoding. -- FreMark: Frequency-Domain Watermark Embedding in Quantized LLMs. -- Bypassing Cross-Domain Restrictions with Unsupervised Visual Translation.

Sommario/riassunto

This book constitutes the proceedings of the 3rd International Conference on Data Security and Privacy Protection, DSPP 2025, held in Xi'an, China, during October 16–18, 2025. The 36 full papers and 11 short papers presented in these two volumes were carefully reviewed and selected from 105 submissions. The papers are organized in the following topical sections: Part I:AI and System Security; Blockchain and Related Technologies; Privacy Preserving/Enhancing Technologies; Cryptographic Primitives; Privacy-Aware Federated Learning; AI-based Security Applications and Technologies. Part II: AI-based Security Applications and Technologies; Cryptographic Protocols Design and Analysis; Model Security and Copyright Protection.