

1. Record Nr.	UNINA9910961692103321
Titolo	Variation and change in morphology : selected papers from the 13th International Morphology Meeting, Vienna, February 2008 // edited by Franz Rainer ... [et al.]
Pubbl/distr/stampa	Amsterdam ; ; Philadelphia, : John Benjamins Pub. Company, c2010
ISBN	9786612558719 9781282558717 1282558714 9789027288523 9027288526
Edizione	[1st ed.]
Descrizione fisica	1 online resource (264 p.)
Collana	Current issues in linguistic theory, , 0304-0763 ; ; v. 310
Altri autori (Persone)	RainerFranz
Disciplina	415
Soggetti	Grammar, Comparative and general - Morphology Linguistics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Foreword & acknowledgements -- Editors' introduction -- Affixation vs. conversion: the resolution of conflicting patterns / Laurie Bauer, Salvador Valera & Ana Diaz Negrillo -- The -alis/-aris allomorphy revisited / Andras Cser -- French property nouns based on toponyms or ethnic adjectives: A case of base variation / Georgette Dal & Fiammetta Namer -- Morphological variation in the construction of French names for inhabitants / Elmar Eggert -- The invisible hand of grammaticalization: West-Germanic substitutive infinitive and the prefix ge- / Livio Gaeta -- Paradigmatic realignment and morphological change: Diachronic deponency in Network Morphology / Andrew Hippisley -- Variation within voice patterns: Morphological change due to syntactic reanalysis / Dalina Kallulli -- Areal-typological aspects of word-formation: The case of aktionsart-formation in German, Hungarian, Slavic, Baltic, Romani and Yiddish / Ferenc Kiefer -- Variation and change in morphology and syntax: Romance object agreement / Michele Loporcaro -- Optional multiple plural marking in Maay /Mary Paster -- Lettered words: Using Roman letters to create

words in Chinese / Helena Riha & Kirk Baker -- Word creation: Definition, Function, Typology / Elke Ronneberger-Sibold -- Pleonastic morphology dies hard: Change and variation of definiteness inflection in Lithuanian / Thomas Stolz -- Index of subjects & terms.

Sommario/riassunto

The papers in this volume derive from the 13th International Morphology Meeting (Vienna 2008). They all address the main topic of the meeting, viz. variation and change in morphology. Inflectional and derivational morphology are represented on equal terms. The focus is on cases of language-internal variation, such as pattern competition, base variation, form-function mismatches, or morphological pleonasm. Other recurring themes are language contact as a cause of variation, the output-orientedness of morphological patterns, and linguistic economy. The contributions cover a wide variety of languages, both Indo-European (Romance, Germanic and Slavic; Latin, Lithuanian and Romani) and non-Indo-European (Hungarian, Maay, Chinese).

2. Record Nr.

UNINA9910143639503321

Titolo

Selected Areas in Cryptography : 6th Annual International Workshop, SAC'99 Kingston, Ontario, Canada, August 9-10, 1999 Proceedings / / edited by Howard Heys, Carlisle Adams

Pubbl/distr/stampa

Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2000

ISBN

3-540-46513-8

Edizione

[1st ed. 2000.]

Descrizione fisica

1 online resource (VIII, 241 p.)

Collana

Lecture Notes in Computer Science, , 0302-9743 ; ; 1758

Disciplina

005.82

Soggetti

Data encryption (Computer science)
Coding theory
Information theory
Computer science
Computer networks
Algorithms
Management information systems
Cryptology
Coding and Information Theory
Computer Science, general
Computer Communication Networks
Algorithm Analysis and Problem Complexity
Management of Computing and Information Systems

Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	<p>Cryptosystems and Pseudorandom Number Generators -- A Universal Encryption Standard -- Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator -- Elliptic Curve Pseudorandom Sequence Generators -- Security Aspects of Block Ciphers -- Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness -- Guesswork and Variation Distance as Measures of Cipher Security -- Modeling Linear Characteristics of Substitution-Permutation Networks -- Strong Linear Dependence and Unbiased Distribution of Non-propagative Vectors -- Cryptanalysis of Block Ciphers -- Security of E2 against Truncated Differential Cryptanalysis -- Key-Schedule Cryptanalysis of DEAL -- Efficient Evaluation of Security against Generalized Interpolation Attack -- Efficient Implementations of Cryptosystems -- Efficient Implementation of Cryptosystems Based on Non-maximal Imaginary Quadratic Orders -- Improving and Extending the Lim/Lee Exponentiation Algorithm -- Software Optimization of Decorrelation Module -- Cryptography for Network Applications -- Pseudonym Systems -- Unconditionally Secure Proactive Secret Sharing Scheme with Combinatorial Structures -- Protecting a Mobile Agent's Route against Collusions -- Photuris: Design Criteria.</p>
Sommario/riassunto	<p>SAC'99 was the sixth in a series of annual workshops on Selected Areas in Cryptography. Previous workshops were held at Carleton University in Ottawa (1995 and 1997) and at Queen's University in Kingston (1994, 1996, and 1998). The intent of the annual workshop is to provide a relaxed atmosphere in which researchers in cryptography can present and discuss new work on selected areas of current interest. The themes for the SAC'99 workshop were: { Design and Analysis of Symmetric Key Cryptosystems { E cient Implementations of Cryptographic Systems { Cryptographic Solutions for Web/Internet Security The timing of the workshop was particularly fortuitous as the announcement by NIST of the v e nalists for AES coincided with the rst morning of the workshop, precipitating lively discussion on the merits of the selection! A total of 29 papers were submitted to SAC'99 and, after a review process that had all papers reviewed by at least 3 referees, 17 were accepted and p- sented. As well, two invited presentations were given: one by Miles Smid from NIST entitled \From DES to AES: Twenty Years of Government Initiatives in Cryptography" and the other by Mike Reiter from Bell Labs entitled \Password Hardening with Applications to VPN Security". The program committee for SAC'99 consisted of the following members: Carlisle Adams, Tom Cusick, Howard Heys, Lars Knudsen, Henk Meijer, Luke O'Connor, Doug Stinson, Stao rd Tavares, and Serge Vaudenay.</p>