Andre Scedrov

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/4567256/publications.pdf

Version: 2024-02-01

106

papers

2,504

citations

304368

22

h-index

233125

45

g-index

118

all docs

118

docs citations

118

times ranked

627

citing authors

#	Article	IF	Citations
1	Uniform proofs as a foundation for logic programming. Annals of Pure and Applied Logic, 1991, 51, 125-157.	0.3	391
2	Decision problems for propositional linear logic. Annals of Pure and Applied Logic, 1992, 56, 239-311.	0.3	164
3	Bounded linear logic: a modular approach to polynomial-time computability. Theoretical Computer Science, 1992, 97, 1-66.	0.5	161
4	Inheritance as implicit coercion. Information and Computation, 1991, 93, 172-221.	0.5	141
5	Functorial polymorphism. Theoretical Computer Science, 1990, 70, 35-64.	0.5	126
6	An Extension of System F with Subtyping. Information and Computation, 1994, 109, 4-56.	0.5	111
7	Multiset rewriting and the complexity of bounded security protocols. Journal of Computer Security, 2004, 12, 247-311.	0.5	106
8	A probabilistic polynomial-time process calculus for the analysis of cryptographic protocols. Theoretical Computer Science, 2006, 353, 118-164.	0.5	66
9	Breaking and fixing public-key Kerberos. Information and Computation, 2008, 206, 402-424.	0.5	53
10	Soundness of Formal Encryption in the Presence of Key-Cycles. Lecture Notes in Computer Science, 2005, , 374-396.	1.0	52
11	Formal analysis of Kerberos 5. Theoretical Computer Science, 2006, 367, 57-87.	0.5	46
12	The lack of definable witnesses and provably recursive functions in intuitionistic set theories. Advances in Mathematics, 1985, 57, 1-13.	0.5	45
13	Probabilistic Polynomial-Time Equivalence and Security Analysis. Lecture Notes in Computer Science, 1999, , 776-793.	1.0	42
14	Relating state-based and process-based concurrency through linear logic (full-version). Information and Computation, 2009, 207, 1044-1077.	0.5	38
15	A categorical approach to realizability and polymorphic types. Lecture Notes in Computer Science, 1988, , 23-42.	1.0	36
16	A Brief Guide to Linear Logic. , 1993, , 377-394.		34
17	A Probabilistic Polynomial-time Calculus For Analysis of Cryptographic Protocols. Electronic Notes in Theoretical Computer Science, 2001, 45, 280-310.	0.9	33
18	An extension of system F with subtyping. Lecture Notes in Computer Science, 1991, , 750-770.	1.0	30

#	Article	IF	Citations
19	Formal Analysis of Multiparty Contract Signing. Journal of Automated Reasoning, 2006, 36, 39-83.	1.1	29
20	FSR: Formal Analysis and Implementation Toolkit for Safe Interdomain Routing. IEEE/ACM Transactions on Networking, 2012, 20, 1814-1827.	2.6	27
21	Probabilistic Bisimulation and Equivalence for Security Analysis of Network Protocols. Lecture Notes in Computer Science, 2004, , 468-483.	1.0	26
22	Automated Analysis of Cryptographic Assumptions in Generic Group Models. Lecture Notes in Computer Science, 2014, , 95-112.	1.0	26
23	Strongly-Optimal Structure Preserving Signatures from TypeÂII Pairings: Synthesis and Lower Bounds. Lecture Notes in Computer Science, 2015, , 355-376.	1.0	25
24	Subexponentials in non-commutative linear logic. Mathematical Structures in Computer Science, 2019, 29, 1217-1249.	0.5	24
25	A formal analysis of ome properties of kerberos 5 using MSR. , 0, , .		23
26	Maintaining distributed logic programs incrementally. , 2011, , .		22
27	First-order linear logic without modalities is NEXPTIME-hard. Theoretical Computer Science, 1994, 135, 139-153.	0.5	21
28	Computationally sound mechanized proofs for basic and public-key Kerberos. , 2008, , .		21
29	Games and the Impossibility of Realizable Ideal Functionality. Lecture Notes in Computer Science, 2006, , 360-379.	1.0	21
30	The Undecidability of Second Order Multiplicative Linear Logic. Information and Computation, 1996, 125, 46-51.	0.5	20
31	Key-dependent message security under active attacks â€“ BRSIM/UC-soundness of Dolevâ€“Yao-style encryption with key cycles. Journal of Computer Security, 2008, 16, 497-530.	0.5	19
32	Bounded memory Dolevâ€“Yao adversaries in collaborative systems. Information and Computation, 2014, 238, 233-261.	0.5	19
33	Contract Signing, Optimism, and Advantage. Lecture Notes in Computer Science, 2003, , 366-382.	1.0	19
34	Classifying topoi and finite forcing. Journal of Pure and Applied Algebra, 1983, 28, 111-140.	0.3	18
35	Collaborative Planning with Confidentiality. Journal of Automated Reasoning, 2011, 46, 389-421.	1.1	17
36	Key-dependent Message Security under Active Attacks--BRSIM/UC-Soundness of Symbolic Encryption with Key Cycles. Computer Security Foundations Workshop (CSFW), Proceedings of the IEEE, 2007, , .	0.0	16

#	Article	IF	Citations
37	Soundness and completeness of formal encryption: The cases of key cycles and partial information leakage. Journal of Computer Security, 2009, 17, 737-797.	0.5	16
38	Phase semantics for light linear logic. Theoretical Computer Science, 2003, 294, 525-549.	0.5	15
39	A rewriting framework and logic for activities subject to regulations. Mathematical Structures in Computer Science, 2017, 27, 332-375.	0.5	14
40	Time, computational complexity, andÂprobability in the analysis ofÂdistance-bounding protocols. Journal of Computer Security, 2017, 25, 585-630.	0.5	14
41	Set existence property for intuitionistic theories with dependent choice. Annals of Pure and Applied Logic, 1983, 25, 129-140.	0.3	13
42	Specifying Kerberos 5 cross-realm authentication. , 2005, , .		13
43	Discrete vs. Dense Times in the Analysis of Cyber-Physical Security Protocols. Lecture Notes in Computer Science, 2015, , 259-279.	1.0	12
44	A comparison between strand spaces and multiset rewriting for security protocol analysis. Journal of Computer Security, 2005, 13, 265-316.	0.5	11
45	Undecidability of the Lambek Calculus with a Relevant Modality. Lecture Notes in Computer Science, 2016, , 240-256.	1.0	11
46	Large sets in intuitionistic set theory. Annals of Pure and Applied Logic, 1984, 27, 1-24.	0.3	10
47	Contract signing, optimism, and advantage. The Journal of Logic and Algebraic Programming, 2005, 64, 189-218.	1.4	10
48	Cryptographically sound security proofs for basic and public-key Kerberos. International Journal of Information Security, 2011, 10, 107-134.	2.3	10
49	Declarative privacy policy. , 2012, , .		10
50	Diagonalization of continuous matrices as a representation of intuitionistic reals. Annals of Pure and Applied Logic, 1986, 30, 201-206.	0.3	9
51	Specifying Real-Time Finite-State Systems in Linear Logic (Extended Abstract). Electronic Notes in Theoretical Computer Science, 1998, 16, 42-59.	0.9	9
52	Policy Compliance in Collaborative Systems. , 2009, , .		9
53	Analysis of EAP-GPSK Authentication Protocol. Lecture Notes in Computer Science, 2008, , 309-327.	1.0	9
54	Reduction-Based Formal Analysis of BGP Instances. Lecture Notes in Computer Science, 2012, , 283-298.	1.0	9

#	Article	IF	Citations
55	Linearizing intuitionistic implication. Annals of Pure and Applied Logic, 1993, 60, 151-177.	0.3	8
56	A reduction-based approach towards scaling up formal analysis of internet configurations. , 2014, , .		8
57	Undecidability of the Lambek Calculus with Subexponential and Bracket Modalities. Lecture Notes in Computer Science, 2017, , 326-340.	1.0	8
58	The Complexity of Multiplicative-Additive Lambek Calculus: 25ÂYearsÂLater. Lecture Notes in Computer Science, 2019, , 356-372.	1.0	8
59	Differential equations in constructive analysis and in the recursive realizability topos. Journal of Pure and Applied Algebra, 1984, 33, 69-80.	0.3	7
60	Extending GÃ¶del's Modal Interpretation to Type Theory and Set Theory. Studies in Logic and the Foundations of Mathematics, 1985, 113, 81-119.	0.2	7
61	Phase Semantics for Light Linear Logic (Extended Abstract). Electronic Notes in Theoretical Computer Science, 1997, 6, 221-234.	0.9	7
62	Timed Multiset Rewriting and the Verification of Time-Sensitive Distributed Systems. Lecture Notes in Computer Science, 2016, , 228-244.	1.0	7
63	Arithmetic transfinite induction and recursive well-orderings. Advances in Mathematics, 1985, 56, 283-294.	0.5	6
64	A guide to polymorphic types. Lecture Notes in Mathematics, 1990, , 111-150.	0.1	6
65	Maintaining distributed logic programs incrementally. Computer Languages, Systems and Structures, 2012, 38, 158-180.	1.4	6
66	Automated synthesis of reactive controllers for software-defined networks. , 2013, , .		6
67	Resource and timing aspects of security protocols. Journal of Computer Security, 2021, 29, 299-340.	0.5	6
68	Breaking and Fixing Public-Key Kerberos. Lecture Notes in Computer Science, 2007, , 167-181.	1.0	6
69	Linear Logic and Computation: A Survey. , 1995, , 379-395.		6
70	When Not All Bits Are Equal: Worth-Based Information Flow. Lecture Notes in Computer Science, 2014, , 120-139.	1.0	6
71	Boolean classifying topoi. Journal of Pure and Applied Algebra, 1983, 28, 15-30.	0.3	5
72	On some non-classical extensions of second-order intuitionistic propositional calculus. Annals of Pure and Applied Logic, 1984, 27, 155-164.	0.3	5

#	Article	IF	Citations
73	Complete topoi representing models of set theory. Annals of Pure and Applied Logic, 1992, 57, 1-26.	0.3	5
74	Relating State-Based and Process-Based Concurrency through Linear Logic. Electronic Notes in Theoretical Computer Science, 2006, 165, 145-176.	0.9	5
75	Collaborative Planning With Privacy. Computer Security Foundations Workshop (CSFW), Proceedings of the IEEE, 2007, , .	0.0	5
76	A Multiset Rewriting Model for Specifying and Verifying Timing Aspects of Security Protocols. Lecture Notes in Computer Science, 2019, , 192-213.	1.0	5
77	Reconciling Lambekâ€™s restriction, cut-elimination and substitution in the presence of exponential modalities. Journal of Logic and Computation, 2020, 30, 239-256.	0.5	5
78	The Multiplicative-Additive Lambek Calculus with Subexponential and Bracket Modalities. Journal of Logic, Language and Information, 2021, 30, 31-88.	0.4	5
79	Verifying Confidentiality and Authentication in KerberosÂ5. Lecture Notes in Computer Science, 2004, , 1-24.	1.0	5
80	Intuitionistically provable recursive well-orderings. Annals of Pure and Applied Logic, 1986, 30, 165-171.	0.3	4
81	Bounded memory protocols. Computer Languages, Systems and Structures, 2014, 40, 137-154.	1.4	4
82	Resource-Bounded Intruders in Denial of Service Attacks. , 2019, , .		4
83	Soft Subexponentials and Multiplexing. Lecture Notes in Computer Science, 2020, , 500-517.	1.0	4
84	L-Models and R-Models for Lambek Calculus Enriched with Additives and the Multiplicative Unit. Lecture Notes in Computer Science, 2019, , 373-391.	1.0	4
85	Bounded Memory Dolev-Yao Adversaries in Collaborative Systems. Lecture Notes in Computer Science, 2011, , 18-33.	1.0	4
86	Some properties of epistemic set theory with collection. Journal of Symbolic Logic, 1986, 51, 748-754.	0.4	3
87	Linear Logic Proof Games and Optimization. Bulletin of Symbolic Logic, 1996, 2, 322-338.	0.2	3
88	Optimization complexity of linear logic proof games. Theoretical Computer Science, 1999, 227, 299-331.	0.5	3
89	Automated Analysis of Cryptographic Assumptions in Generic Group Models. Journal of Cryptology, 2019, 32, 324-360.	2.1	3
90	Embedding sheaf models for set theory into boolean-valued permutation models with an interior operator. Annals of Pure and Applied Logic, 1986, 32, 103-109.	0.3	2

#	Article	IF	Citations
91	Small decidable sheaves. Journal of Symbolic Logic, 1986, 51, 726-731.	0.4	2
92	Lindenbaum algebras of intuitionistic theories and free categories. Annals of Pure and Applied Logic, 1987, 35, 167-172.	0.3	2
93	Kleene computable functionals and the higher order existence property. Journal of Pure and Applied Algebra, 1988, 52, 313-320.	0.3	2
94	Towards an automated assistant for clinical investigations. , 2012, , .		2
95	On the impossibility of explicit upper bounds on lengths of some provably finite algorithms in computable analysis. Annals of Pure and Applied Logic, 1986, 32, 291-297.	0.3	1
96	Moez Alimohamed, 1967â€“1994. Theoretical Computer Science, 1995, 146, 1-3.	0.5	1
97	Stronglyâ€•optimal structure preserving signatures from Type II pairings: synthesis and lower bounds. IET Information Security, 2016, 10, 358-371.	1.1	1
98	Language models for some extensions of the Lambek calculus. Information and Computation, 2021, , 104760.	0.5	1
99	Undecidability of a Newly Proposed Calculus for CatLog3. Lecture Notes in Computer Science, 2019, , 67-83.	1.0	1
100	Some Aspects of Categorical Semantics: Sheaves and Glueing. Studies in Logic and the Foundations of Mathematics, 1987, 122, 281-301.	0.2	0
101	Decompositions of finitely generated modules over C(X): sheaf semantics and a decision procedure. Mathematical Proceedings of the Cambridge Philosophical Society, 1988, 103, 257-268.	0.3	0
102	The Complexity of Local Proof Search in Linear Logic. Electronic Notes in Theoretical Computer Science, 1996, 3, 120-129.	0.9	0
103	The work of Dean Rosenzweig. , 2007, , .		0
104	Reduction-based analysis of BGP systems with BGPVerif. , 2012, , .		0
105	Reduction-based analysis of BGP systems with BGPVerif. Computer Communication Review, 2012, 42, 89-90.	1.5	0
106	On the Security and Complexity of Periodic Systems. SN Computer Science, 2022, 3, .	2.3	0