INRIA - Projet SECRET, Batiment 25 Domaine de
Voluceau - Rocquencourt, B.P. 105
78153 Le Chesnay Cedex, France
0030-697-7046891
0033-01-39635609
Dimitrios.Simos@inria.fr
https://who.rocq.inria.fr/Dimitrios.Simos/

Dimitris E. Simos

Curriculum Vitae

Research Positions

March 2012 – February 2013 — **ERCIM/Marie Curie Post-Doctoral Fellow**.
Project-Team SECRET, Research Center INRIA Paris-Rocquencourt, France

Duties — Mostly devoted, on the design and analysis of cryptographic algorithms, especially through the study of the involved discrete structures.

Scientific Coordinator — **Directeur de Recherche (DR1)** Nicolas Sendrier

Education

2011 — **Ph.D. in Discrete Mathematics and Combinatorics**.
Department of Mathematics, National Technical University of Athens, Greece

2007 — **M.Sc. in Applied Mathematical Sciences**, *Major in Computational Mathematics*.
School of Applied Mathematics and Physics, National Technical University of Athens, Greece

2006 — **B.Sc. in Mathematics**, *Major in Applied Mathematics*.
Department of Mathematics, University of Athens, Greece

Doctoral Dissertation

Title — *Combinatorial Design Theory, Coding Theory and Cryptography*

Supervisor — **Professor** Christos Koukouvinos

Description — My Ph.D. Thesis focuses on the study and interaction of the later fields. In particular, I have studied combinatorial structures and developed evolutionary algorithms for the construction and optimization of several classes of combinatorial designs which in the continuum are applied in the generation of optimal codes used in Coding Theory. In the discipline of Cryptology, I have studied combinatorial structures as encryption matrices for private-key cryptosystems and the generation of secret-sharing schemes that arose from designs.

Honours & Awards

March 2012 — **Fellow of the ICA (FTICA)**.
Institute of Combinatorics and its Applications (ICA), Canada

December 2011 — **ERCIM "Alain Bensoussan" Fellowship**.
The European Research Consortium for Informatics and Mathematics (ERCIM) co-funded by the European Commission under the FP7 Marie-Curie action named ABCDE

March 2011 **Certificate Award**.
National Military University (NMU) "Vassil Levski" and the Veliko Tarnovo University (VTU) "St. Cyril and St. Methodius", Bulgaria

November 2010 **Associate Fellow of the ICA (AFTICA)**.
Institute of Combinatorics and its Applications (ICA), Canada

Grants & Scholarships

2012 **ECRYPT II Grant: European Network of Excellence in Cryptology II**.
ICT Programme: European Commission under the Action of Framework 7

2008–2011 **Three Year Ph.D. Research Scholarship**.
Secretariat of the Research Committee of National Technical University of Athens, Greece

2011, 2010, 2008 **SCIEnce Grant: Symbolic Computation Infrastructure for Europe**.
SCIEnce Project: European Commission under the Action of Framework 6

2009, 2008, 2007, 2006 **Thomaidio Grant for the Science and Art Progress**.
National Technical University of Athens, Greece

Research Interests

Design Theory **Combinatorial Designs, Sequences with Zero Autocorrelation, Difference sets, Hadamard matrices, Weighing matrices, Orthogonal Designs. Optimal Designs.**

Description Theoretical study and design of combinatorial algorithms for the construction of classes of combinatorial designs.

Coding Theory **Optimal Codes, Self-Dual Codes, Quasi-Cyclic Codes, Optical Orthogonal Codes.**

Description Theoretical aspects of Coding Theory. Isomorphism algorithms for code equivalence. Generation of optimal codes from designs and their interaction within Coding Theory.

Cryptography **Block Ciphers, Private Key Cryptosystems & Cryptanalysis, Code-Based Cryptography, Public-key Signatures, Encryption Schemes from Designs. Secret-Sharing Schemes.**

Description Development of symmetric & code-based cryptosystems and secret-sharing schemes from designs, related cryptanalysis and simulation of cryptographic attacks.

Symbolic Computation **Groebner Bases, Holonomic Functions, Computer Algebra.**

Description Formulation and modeling of tools of Symbolic Computation for the construction of combinatorial designs and applications to Coding Theory and Cryptography.

Optimization **Metaheuristics, Genetic Algorithms, Simulated Annealing, Tabu-Search, Hybrid Heuristics. Competent and Nature-Inspired Metaheuristics.**

Description Devise optimization algorithms for the construction of combinatorial designs and codes.

Research Visits and Stays

INRIA **Project-Team SECRET.** [January 23–26, 2012]
Institut National de Recherche en Informatique et en Automatique (INRIA), France

Project Preliminary Visit for Collaboration within the Framework of an ERCIM Fellowship
Support Research Center INRIA Paris-Rocquencourt
Contact Nicolas Sendrier

SBA **SBA Research.** [November 15–17, 2011]
Secure Business Austria (SBA), Austria
Project Preliminary Visit for Collaboration within the Framework of an ERCIM Fellowship
Support Research Center SBA Research
Contact Peter Kieseberg

RISC **Transnational Access Programme.** [March 27–31, 2011]
Research Institute for Symbolic Computation (RISC), Johannes Kepler University, Austria
Project Symbolic Computation in Orthogonal Designs
Support European Commission FP6 for Integrated Infrastructures Initiatives under the project SCIEnce
Contact Veronika Pillwein, Temur Kutsia and Zafeirakis Zafeirakopoulos

VTU **Department of Mathematics and Informatics.** [March 23–26, 2011]
Veliko Tarnovo University (VTU) "St. Cyril and St. Methodius", Bulgaria
Project Secret-Sharing Schemes from Combinatorial Designs
Support Partial
Contact Zlatko Varbanov

RISC **Transnational Access Programme.** [August 1–14, 2010]
Research Institute for Symbolic Computation (RISC), Johannes Kepler University, Austria
Project Efficient Algorithms for Combinatorial Designs using Computer Algebra Tools and Symbolic Computation
Support European Commission FP6 for Integrated Infrastructures Initiatives under the project SCIEnce
Contact Veronika Pillwein and Zafeirakis Zafeirakopoulos

Professional Activities & Service

Editorships

AMIS **Editorial Board Member (EBM).** [2012–now]
Applied Mathematics & Information Sciences

IJCM **Editorial Board Member (EBM).** [2011–now]
International Journal of Contemporary Advanced Mathematics

ISL **Editorial Board Member (EBM).** [2012–now]
Information Sciences Letters

Conference Organization & Program Committees

MoCrySEn2013 **Workshop Chair**.
The 2nd International Workshop on *"Modern Cryptography and Security Engineering"*
University of Regensurg, Regensburg, September 2–6, 2013, Germany

AReS2013 **Program Committee (PC) Member**.
The 8th International Conference on *"Availability, Reliability and Security"*
University of Regensurg, Regensburg, September 2–6, 2013, Germany

IWSMA2013 **Program Committee (PC) Member**.
The 2nd International Workshop on *"Security of Mobile Applications"*
University of Regensurg, Regensburg, September 2–6, 2013, Germany

NiCaM-WI2012 **International Program Committee (IPC) Member**.
The International Workshop on *"Nature-Inspired Computing and Metaheuristics for Web Intelligence"*
Venetian, Macau, December 4–7, 2012, China

MoCrySEn2012 **Workshop Chair**.
The 1st International Workshop on *"Modern Cryptography and Security Engineering"*
University of Economics, Prague, August 20–24, 2012, Czech Republic

AReS2012 **Program Committee (PC) Member**.
The 7th International Conference on *"Availability, Reliability and Security"*
University of Economics, Prague, August 20–24, 2012, Czech Republic

IWSMA2012 **Program Committee (PC) Member**.
The 1st International Workshop on *"Security of Mobile Applications"*
University of Economics, Prague, August 20–24, 2012, Czech Republic

NiCaM2011 **International Program Committee (IPC) Member**.
International Workshop on *"Nature-Inspired Computing and Metaheuristics"*
Venetian, Macau, October 24–26, 2011, China

MPAE11 **Program Committee (PC) Member**.
Scientific Symposium on *"Modern Problems of Applied Electromagnetism"*
National Military University (NMU), Veliko Tarnovo, March 25, 2011, Bulgaria

Journal Referee

AJC	The Australasian Journal of Combinatorics	[2012–now]
AAECC	Applicable Algebra in Engineering, Communication and Computing	[2013–now]
NCA	Neural Computing & Applications	[2012–now]
JoWUA	Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications	[2012–now]
IJCT	International Journal of Combinatorics	[2010–now]
IJCIS	International Journal on Cryptography and Information Security	[2012–now]
IJBIC	International Journal of Bio-Inspired Computation	[2011–now]
RPE	Recent Patents on Engineering	[2010–now]
JAS	Journal of Applied Statistics	[2010–now]

JAPS	Journal of Applied Probability and Statistics	[2010–now]
HJMS	Hacettepe Journal of Mathematics and Statistics	[2010–now]

Conference & Workshop Referee

WCC2013	8th International Workshop on Coding Theory and Cryptography	[April 2013]
NiCaM-WI2012	International Workshop on Nature-Inspired Computing and Metaheuristics for Web Intelligence	[December 2012]
ARES2012	7th International Conference on Availability, Reliability and Security	[August 2012]
SEA11	10th International Symposium on Experimental Algorithms	[May 2011]

Reviewer

MR	AMS Mathematical Reviews	[2010–now]
ZB-MATH	Zentralblatt MATH Reviews	[2012–now]
Elsevier	Elsevier Insights e-book series	[2012–now]

Invited Talks

April 2012 — **Families of Block Ciphers from Combinatorial Designs.**

Session Talk @ CAIAF12 — Colloquium "Cryptography and its Applications in the Armed Forces"

Hellenic Military Academy (HMA) "Evelpidon", April 6, 2012, Vari, Greece

November 2011 — **A Bird's-Eye View of Optimal Codes and Symmetric Cryptography from Combinatorial Designs.**

Guest Talk @ SBA — Secure Business Austria "sba-research.org"

Research Center Secure Business Austria (SBA), November 16, 2011, Vienna, Austria

April 2011 — **Private-key Cryptosystems from Combinatorial Designs.**

Session Talk @ AMIMS11 — Colloquium "Applications of Mathematics and Informatics in Military Sciences"

Hellenic Military Academy (HMA) "Evelpidon", April 11 – 12, 2011, Vari, Greece

March 2011 — **Encryption Schemes from Orthogonal Matrices and Related Cryptanalysis.**

Plenary Talk @ MPAE11 — Scientific Symposium "Modern Problems of Applied Electromagnetism"

National Military University (NMU) "Vassil Levski", March 25, 2011, Veliko Tarnovo, Bulgaria

March 2011 — **Construction Methods of Optimal Codes from Combinatorial Designs.**

Seminar Lecture @ VTU — Mathematical Foundations of Informatics Seminar

Department of Mathematics and Informatics of Veliko Tarnovo University (VTU) "St. Cyril and St. Methodius", March 24, 2011, Veliko Tarnovo, Bulgaria

Contributed Talks and Presentations

October 2012 — **Self-Presentation.**
Ice Breaking Session @ ABCDE Seminar — ERCIM ABCDE Seminar II 2012
INRIA Sophia-Antipolis, October 24–25, 2012, Alpes-Maritimes, France

October 2012 — **How Easy is Code Equivalence over $GF(q)$?.**
Session Talk @ C2 — Journées Codage et Cryptographie 2012
Manoir de la Vicomté, October 7–12, 2012, Dinard, France

May 2012 — **The Support Splitting Algorithm and its Application to Code-based Cryptography.**
Session Talk @ CBC2012 — Code-based Cryptography Workshop 2012
Technical University of Denmark, May 9–11, 2012, Lyngby, Denmark

July 2011 — **Combinatorial Design Theory, Coding Theory and Cryptography.**
Oral Talk @ NTUA — Ph.D. Thesis Defense
Department of Mathematics, National Technical University of Athens, July 18, 2011, Athens, Greece

May 2011 — **Combinatorial Optimization for Weighing Matrices with the Ordering Messy Genetic Algorithm.**
Contributed Talk @ SEA11 — 10th International Symposium on Experimental Algorithms
Orthodox Academy of Crete, May 5–7, 2011, Kolimpari, Greece

March 2011 — **Efficient Algorithms for Compatible Sequences, Complexity Analysis and Related Problems.**
Seminar Lecture @ RISC — Algorithmic Combinatorics Seminar
Research Institute for Symbolic Computation (RISC), March 30, 2011, Hagenberg, Austria

March 2011 — **Combinatorial Design Theory, Coding Theory and Cryptography.**
Oral Talk @ NTUA — Ph.D. Thesis Report
Department of Mathematics, National Technical University of Athens, March 11, 2011, Athens, Greece

September 2010 — **Numerical and Algorithmic Aspects of Orthogonal Sequences in Combinatorial Design Theory.**

Contributed Talk @ NUMAN10
Third Conference in Numerical Analysis, Recent Approaches to Numerical Analysis: Theory, Methods and Applications
Grand Arsenale, September 15–18, 2010, Chania, Greece

June 2010 **Explorations of Optical Orthogonal and Quasi-Cyclic Codes from a Combinatorial Design Perspective.**

Contributed Talk @ PYTHAG4
Fourth Pythagorean Conference: An Advanced Research Workshop in Geometry, Combinatorial Designs & Cryptology
Corfu & Dasia Chandris Hotels Complex, May 30–June 4, 2010, Corfu, Greece

April 2010 **Quasi-Cyclic Codes from Cyclic-Structured Designs with Good Properties.**

Contributed Talk @ ALCOMA10
Algebraic Combinatorics and Applications: Designs and Codes
Schloss Thurnau, April 11–18, 2010, Thurnau, Germany

September 2009 **High Efficiency Cryptographic Systems and Data Coding for Applications of Secure Information Transmission.**

Tutorial @ ACC09
Second Applied Computing Conference
Asteras Vouliagmenis, September 28–30, 2009, Athens, Greece

May 2009 **Self-Dual Codes over Small Prime Fields from Combinatorial Designs.**

Contributed Talk @ CAI09
Third Conference on Algebraic Informatics
Teloglion Foundation of Art, May 19–22, 2009, Thessaloniki, Greece

September 2008 **Utilization of Meta-Programming in Combinatorial Design Theory.**

Contributed Talk @ NUMAN08
Second Conference in Numerical Analysis, Recent Approaches to Numerical Analysis: Theory, Methods and Applications
Elite Hotel, September 1–5, 2008, Kalamata, Greece

Memberships

Societies

ICA **Fellow,** *Institute of Combinatorics and its Applications (ICA).* [2012–now]
Associate Fellow, *Institute of Combinatorics and its Applications (ICA).* [2010–2012]
ITSOC **Member,** *IEEE Information Theory Society.* [2011–now]
Graduate Student Member, *IEEE Information Theory Society.* [2009–2011]
COMSOC **Member,** *IEEE Communications Society.* [2011–now]
Graduate Student Member, *IEEE Communications Society.* [2010–2011]
COMPSOC **Member,** *IEEE Computer Society.* [2011–now]
MIR Labs **Regular Member,** *Machine Intelligence Research Labs.* [2012–now]

HMS **Member,** *Hellenic Mathematical Society.* [2006–now]

Scientific

CARGO **Member,** *Computer Algebra Research Group.* [2006–now]
Wilfrid Laurier University, Waterloo, Ontario, Canada, `www.cargo.wlu.ca`

MEDICIS **Researcher,** *Centre de calcul formel MEDICIS.* [2006–now]
École Polytechnique, Paris, France, `www.medicis.polytechnique.fr`

SHARCnet **Researcher,** *Shared Hierarchical Academic Research Computing Network.* [2007–2011]
Ontario, Canada, `www.sharcnet.ca`

Training Courses

October 2012 **ERCIM ABCDE Seminar II**.
INRIA Sophia-Antipolis, France

July 2008 **Third RISC/SCIEnce Training School in Symbolic Computation**.
Research Institute for Symbolic Computation (RISC), Johannes Kepler University, Austria

December 2006 **Advanced Subjects in Grid Technology**.
Greek Research & Technology Network, Greece

July 2005 **Summer School on Research for Natural Sciences and Informatics**.
National Center of Scientific Research (NCSR) "Demokritos", Greece

Computer skills

Programming	C/C++, Python	Packages	Matlab, Mathematica, Maple, Magma, GAP
Scripting	bash, awk/sed, perl	OS	Unix, Linux, Windows
Typesetting	LaTeX	Web	(X)Html, PHP, CSS

Experience

Teaching & Tutorship

2006–2011 **Laboratory Instructor**, *Software for Mathematics and Physics*.
School of Applied Mathematics and Physics, National Technical University of Athens
Laboratory tutorials and lectures to undergraduate students in Mathematica & Matlab

2009–2010 **Laboratory Instructor**, *Coding and Information Theory*.
School of Applied Mathematics and Physics, National Technical University of Athens
Laboratory tutorials and lectures to undergraduate students in Gap

2009–2010 **Laboratory Instructor**, *Graphs and 0-1 Matrices*.
School of Applied Mathematics and Physics, National Technical University of Athens
Laboratory tutorials and lectures to postgraduate students in Matlab

2007–2010 **Teaching Assistant**, *Statistical Designs*.
School of Applied Mathematics and Physics, National Technical University of Athens

Lectures to postgraduate students in Statgraphics

2007–2010 **Teaching Assistant**, *Designs and Linear Models*.
School of Applied Mathematics and Physics, National Technical University of Athens

Lectures to undergraduate students in Statgraphics

2004–2005 **Laboratory Instructor**, *Computer Graphics*.
Department of Mathematics, University of Athens

Laboratory tutorials and lectures to undergraduate students in Matlab

2004–2005 **Instructor**, *E-Class: Computer Algebra in Scientific Computing*.
Department of Mathematics, University of Athens

Administration of the e-class and created tutorials for undergraduate students in Maple

2004–2005 **Instructor**, *E-Class: Introduction to Operational Research*.
Department of Mathematics, University of Athens

Administration of the e-class and created tutorials for undergraduate students in Maple

Work & Professional

GRST **Research Associate,** *PENED Project, no. 03ED740.* [September–October, 2008]
General Secretariat of Research and Technology, Greece

Duties Construction of efficient algorithms for the development of high efficiency cryptographic systems and encoding of data with applications in the secure information transmission.

NCSR **Software Engineer,** *Internship.* [July, 2005]
Institute of Material Science, National Center of Scientific Research "Demokritos", Greece

Duties Maintenance of legacy FORTRAN code for quantum mechanics and production of a server-client model application in Java, that allows remote use of multiple servers (Matlab, Maple, etc) under a common GUI.

UOA **Lab Assistant,** *PC Laboratory.* [October 2004–May 2005]
Department of Mathematics, University of Athens, Greece

Duties Supervision of the lab, trouble-shooting, assistance of lab users (i.e. for exercises within the framework of courses taught in the department) and seminar organization.

Publications

Books

[1] C. Koukouvinos and D. E. Simos, *Combinatorial Designs with Applications to Coding Theory and Cryptography*. Berlin: Walter de Gruyter, 2013 (in preparation).

Papers in Refereed Journals

[2] C. Koukouvinos and D. E. Simos, "Encryption schemes based on hadamard matrices with circulant cores." to appear in J. Appl. Math. & Bioinformatics.

[3] I. S. Kotsireas, C. Koukouvinos, P. M. Pardalos, and D. E. Simos, "Competent genetic algorithms for weighing matrices," *J. Comb. Optim.*, vol. 24, pp. 508–525, 2012.

[4] C. Koukouvinos and D. E. Simos, "Encryption schemes from williamson matrices," *J. Inf. Assur. Secur.*, vol. 7, pp. 252–258, 2012.

[5] I. S. Kotsireas, C. Koukouvinos, and D. E. Simos, "A meta-software system for orthogonal designs and hadamard matrices," *J. Appl. Math. & Informatics*, vol. 29, pp. 1571–1581, 2011.

[6] C. Koukouvinos, V. Pillwein, D. E. Simos, and Z. Zafeirakopoulos, "On the average complexity for the verification of compatible sequences," *Inform. Process. Lett.*, vol. 111, pp. 825–830, 2011.

[7] C. Koukouvinos and D. E. Simos, "Encryption schemes using plotkin arrays," *Appl. Math. & Inf. Sci.*, vol. 5, pp. 500–510, 2011.

[8] C. Koukouvinos and D. E. Simos, "Further results on ternary complementary sequences, orthogonal designs and weighing matrices," *Australas. J. Combin.*, vol. 50, pp. 97–112, 2011.

[9] C. Koukouvinos, K. Mylona, and D. E. Simos, "An algorithmic construction of $e(s^2)$–optimal supersaturated designs," *J. Stat. Theory Pract.*, vol. 5, pp. 357–367, 2011.

[10] C. Koukouvinos and D. E. Simos, "On the computation of the non-periodic autocorrelation function of two ternary sequences and its related complexity analysis," *J. Appl. Math. & Informatics*, vol. 29, pp. 547–562, 2011.

[11] C. Koukouvinos and D. E. Simos, "Quasi-cyclic codes from cyclic-structured designs with good properties," *Discrete Math. Algorithms Appl.*, vol. 3, pp. 223–243, 2011.

[12] I. S. Kotsireas, C. Koukouvinos, and D. E. Simos, "Inequivalent hadamard matrices from near normal sequences," *J. Combin. Math. Combin. Comput.*, vol. 75, pp. 105–115, 2010.

[13] C. Koukouvinos and D. E. Simos, "New infinite families of orthogonal designs constructed from complementary sequences," *Int. Math. Forum*, vol. 5, pp. 2655–2665, 2010.

[14] I. S. Kotsireas, C. Koukouvinos, J. Seberry, and D. E. Simos, "New classes of orthogonal designs constructed from complementary sequences with given spread," *Australas. J. Combin.*, vol. 46, pp. 67–78, 2010.

[15] C. Koukouvinos and D. E. Simos, "Improving the lower bounds on inequivalent hadamard matrices through orthogonal designs and meta-programming techniques," *Appl. Numer. Math.*, vol. 60, pp. 370–377, 2010.

[16] C. Koukouvinos and D. E. Simos, "New classes of orthogonal designs and weighing matrices derived from near normal sequences," *Australas. J. Combin.*, vol. 47, pp. 11–20, 2010.

[17] I. S. Kotsireas, C. Koukouvinos, and D. E. Simos, "Mds and near-mds self-dual codes over large prime fields," *Adv. Math. Commun.*, vol. 3, pp. 349–361, 2009.

[18] C. Koukouvinos, E. Lappas, and D. E. Simos, "Encryption schemes using orthogonal arrays," *J. Discrete Math. Sci. Cryptogr.*, vol. 12, pp. 615–628, 2009.

[19] C. Koukouvinos, K. Mylona, D. E. Simos, and A. Skountzou, "An algorithmic construction of four-level response surface designs," *Comm. Statist. Simulation Comput.*, vol. 38, pp. 2152–2160, 2009.

[20] C. Koukouvinos and D. E. Simos, "Construction of new self-dual codes over gf(5) using skew-hadamard matrices," *Adv. Math. Commun.*, vol. 3, pp. 251–263, 2009.

[21] C. Koukouvinos, K. Mylona, and D. E. Simos, "A hybrid saga algorithm for the construction of e(s^2)-optimal cyclic supersaturated designs," *J. Statist. Plann. Inference*, vol. 139, pp. 478–485, 2009.

[22] I. S. Kotsireas, C. Koukouvinos, and D. E. Simos, "Inequivalent hadamard matrices from base sequences," *Util. Math.*, vol. 78, pp. 3–9, 2009.

[23] C. Koukouvinos, K. Mylona, and D. E. Simos, "E(s^2)-optimal and minimax-optimal cyclic supersaturated designs via multi-objective simulated annealing," *J. Statist. Plann. Inference*, vol. 138, pp. 1639–1646, 2008.

[24] C. Koukouvinos, K. Mylona, and D. E. Simos, "k-circulant supersaturated designs and metaheuristics: A comparative study on construction methods of supersaturated designs," *J. Appl. Probab. Stat.*, vol. 2, pp. 37–47, 2007.

[25] C. Koukouvinos, K. Mylona, and D. E. Simos, "Exploring k-circulant supersaturated designs via genetic algorithms," *Comput. Statist. Data Anal.*, vol. 51, pp. 2958–2968, 2007.

[26] I. S. Kotsireas, C. Koukouvinos, and D. E. Simos, "Large orthogonal designs via amicable sets of matrices," *Int. J. Appl. Math.*, vol. 12, pp. 217–232, 2006.

Papers in Refereed Conference Proceedings and Books

[27] N. Sendrier and D. E. Simos, "How easy is code equivalence over $\mathbb{F}_q$?," in *WCC '13: Proceedings of the 8th International Workshop on Coding and Cryptography, to appear*, 2013.

[28] C. Koukouvinos and D. E. Simos, "A bird's eye view of modern symmetric cryptography from combinatorial designs," in *AMIMS '11: Applications of Mathematics and Informatics in Military Science, Springer Optimization and its Applications*, vol. 71, pp. 189–219, 2012.

[29] C. Koukouvinos, D. E. Simos, and Z. Varbanov, "Hadamard matrices, designs and their secret-sharing schemes," in *CAI '11: Proceedings of the 4th International Conference on Algebraic Informatics, Lecture Notes in Computer Science*, vol. 6742, pp. 216–229, 2011.

[30] C. Koukouvinos and D. E. Simos, "Combinatorial optimization for weighing matrices with the ordering messy genetic algorithm," in *SEA '11: Proceedings of the 10th International Symposium on Experimental Algorithms, Lecture Notes in Computer Science*, vol. 6630, pp. 148–156, 2011.

[31] C. Koukouvinos and D. E. Simos, "Self-dual codes over small prime fields from combinatorial designs," in *CAI '09: Proceedings of the 3rd International Conference on Algebraic Informatics, Lecture Notes in Computer Science*, vol. 5725, pp. 278–287, 2009.

[32] I. S. Kotsireas, C. Koukouvinos, and D. E. Simos, "Inequivalent hadamard matrices via orthogonal designs," in *MACIS '06: Proceedings of the 1st International Conference on Mathematical Aspects of Computer and Information Sciences*, pp. 280–286, 2006.

Papers in Other Conference Proceedings

[33] C. Koukouvinos, D. E. Simos, and Z. Zafeirakopoulos, "An algebraic framework for extending orthogonal designs," in *ISSAC '11: Abstracts of Poster Presentations of the 36th International Symposium on Symbolic and Algebraic Computation, ACM Commun. Comput. Algebra*, vol. 45, pp. 123–124, 2011.

[34] C. Koukouvinos and D. E. Simos, "Numerical and algorithmic aspects of orthogonal sequences in combinatorial design theory," in *NumAn '10: Book of Proceedings*, pp. 236–241, 2010.

[35] I. S. Kotsireas, C. Koukouvinos, and D. E. Simos, "Utilization of meta-programming in combinatorial design theory," in *NumAn '08: Book of Proceedings*, pp. 117–121, 2008.

Technical Reports

[36] C. Koukouvinos, V. Pillwein, D. E. Simos, and Z. Zafeirakopoulos, "A note on the average complexity analysis of the computation of periodic and aperiodic ternary complementary pairs," Research Report DK-2010-08, Doctoral Program Computational Mathematics, October 2010.

Citations

Citations Count There are at least **29 citations** to my research papers

Citations

[BFM11] C. Brezinski, P. Fika, and M. Mitrouli, *Moments of a linear operator, with applications to the trace of the inverse of matrices and the solution of equations*, to appear in Numer. Linear Algebra Appl. (2011), Citation to paper [21].

[BKP11] N. Balakrishnan, C. Koukouvinos, and C. Parpoula, *An information theoretical algorithm for analyzing supersaturated designs for a binary response*, Metrika (2011), Citation to paper [23].

[BKP12] _____, *Analysis of a supersaturated design using entropy prior complexity for binary responses via generalized linear models*, Stat. Methodol. **9** (2012), 478–485, Citation to paper [23].

[BR08] D. A. Bulutoglu and K. J. Ryan, *$e(s^2)$-optimal supersaturated designs with good minimax properties when n is odd*, J. Statist. Plann. Inference **138** (2008), 1754–1762, Citation to papers [25], [23].

[But09] N. A. Butler, *Two-level supersaturated designs for 2^k runs and other cases*, J. Statist. Plann. Inference **139** (2009), 23–29, Citation to papers [25], [23].

[Geo12] S. D. Georgiou, *Supersaturated designs: A review of their construction and analysis*, J. Statist. Plann. Inference (2012), Citation to papers [25], [23], [21].

[GG12] K. Guenda and T. A. Gulliver, *Mds and self-dual codes over rings*, Finite Fields Appl. **18** (2012), 1061–1075, Citation to paper [17].

[GHM11] S. Gupta, K. Hisano, and L. B. Morales, *Optimal k-circulant supersaturated designs*, J. Statist. Plann. Inference **141** (2011), 782–786, Citation to paper [25].

[GM12] S. Gupta and L. B. Morales, *Constructing $e(s^2)$-optimal and minimax-optimal k-circulant supersaturated designs via multi-objective tabu search*, J. Statist. Plann. Inference **142** (2012), 1415–1420, Citation to papers [25], [23], [21].

[Gue12] K. Guenda, *New mds self-dual codes over finite fields*, Des. Codes Cryptogr. **62** (2012), 31–42, Citation to paper [17].

[HLW11] F. Huang, H. Lu, and Z. Wu, *Buried pipeline optimization in landslide area*, ICPTT '11: Sustainable Solutions for Water, Sewer, Gas, and Oil Pipelines - Proceedings of the International Conference on Pipelines and Trenchless Technology 2011 (Reston, VA), American Society of Civil Engineers (ASCE), 2011, Citation to paper [15], pp. 2366–2376.

[Jan08] D.-H. Jang, *Mutual information as a criterion for evaluating the degree of the orthogonality of nearly orthogonal arrays*, Journal of the Korean Society for Quality Management **36** (2008), 13–21, Citation to papers [23], [21].

[KK07] I. S. Kotsireas and C. Koukouvinos, *Inequivalent hadamard matrices from orthogonal designs*, PASCO '07: Proceedings of the 2007 international workshop on Parallel symbolic computation (New York, NY, USA), ACM, 2007, Citation to paper [26], pp. 95–96.

[KMM08] C. Koukouvinos, P. Mantas, and K. Mylona, *A general construction of $e(s^2)$-optimal large supersaturated designs*, Metrika **68** (2008), 99–110, Citation to paper [25].

[KMMP11] C. Koukouvinos, E. Massou, K. Mylona, and C. Parpoula, *Analyzing supersaturated designs with entropic measures*, J. Statist. Plann. Inference **141** (2011), 1307–1312, Citation to paper [23].

[KMS11] C. Koukouvinos, K. Mylona, and A. Skountzou, *A variable selection method for analyzing supersaturated designs*, Comm. Statist. Simulation Comput. **40** (2011), 484–496, Citation to papers [23], [21].

[KP12] C. Koukouvinos and C. Parpoula, *Analyzing supersaturated designs by means of an information based criterion*, Comm. Statist. Simulation Comput. **41** (2012), 44–57, Citation to paper [23].

[MGP11] B. N. Mandal, V. K. Gupta, and R. Parsad, *Construction of efficient mixed-level k-circulant supersaturated designs*, J. Stat. Theory Pract. **5** (2011), 627–648, Citation to paper [25].

[MV13] L. B. Morales and G. Vega, *On the enumeration of $e(s^2)$-optimal and minimax-optimal k-circulant supersaturated designs*, J. Comb. Des. (2013), Citation to papers [25], [23].

[SX13] Y. Shi and G. Xiong, *An undetachable threshold digital signature scheme based on conic curves*, Appl. Math. & Inf. Sci **7** (2013), 823–828, Citation to paper [7].

References

Referee **Professor** Christos Koukouvinos
Affiliation Department of Mathematics, National Technical University of Athens, Greece
Relation Ph.D. Advisor
Tel. 0030-210-7721706
e-mail ckoukouv@math.ntua.gr

Referee **Professor** Spyros Magliveras
Affiliation Department of Mathematical Sciences, Florida Atlantic University, USA
Expertise Combinatorial Designs and Cryptography
Tel. (561)-297-0274
e-mail spyros@fau.edu

Referee **Senior Researcher** Xin-She Yang
Affiliation Mathematics and Scientific Computing, National Physical Laboratory, Teddington TW11 0LW, UK
Expertise Optimization
Tel. (44)-208943-6092
e-mail xin-she.yang@npl.co.uk

Permission or notice is not required prior to contacting the referees above; all referees prefer to be contacted by email.