ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΓΡΑΜΜΑΤΕΙΑ ΣΥΓΚΛΗΤΟΥ
Διεύθυνση: Ερυθρού Σταυρού 28 & Καρυωτάκη, 22131Τρίπολη
Τηλ.:2710-230000, fax: 2710-230005

ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΠΟΦΑΣΗ ΣΥΓΚΛΗΤΟΥ
ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΛΟΠΟΝΝΗΣΟΥ
Απόφαση 7α/17.01.2017 Συνεδρίαση 99η

Θέμα: Συγκρότηση του μητρώου εσωτερικών και εξωτερικών μελών για κρίση εκλογής, εξέλιξης ή μονιμοποίησης σε θέση Επίκουρου Καθηγητή και για κρίση εκλογής ή εξέλιξης σε θέση Αναπληρωτή Καθηγητή του Τμήματος Πληροφορικής και Τηλεπικοινωνιών στο γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές»

Η ΣΥΓΚΛΗΤΟΣ ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΛΟΠΟΝΝΗΣΟΥ

Έχοντας υπόψη:

1. Τις διατάξεις του άρθρου 19 του Ν. 4009/2011 (ΦΕΚ 195 Α') όπως αντικαταστάθηκε με το άρθρο 70 του Ν. 4386/ 2016 (ΦΕΚ 83 Α΄) και τροποποιήθηκε με το άρθρο 4 του Ν. 4405/2016 (ΦΕΚ 129 Α')
2. Την υπ' αριθμ. Φ.122.1/88/119483/Ζ2 εγκύκλιο του Υπουργείου Παιδείας, Έρευνας και Θρησκευμάτων με θέμα: "Οδηγίες εφαρμογής του Ν.4369/2016 (Α' 27), του Ν. 4386/2016 (Α' 83) και του Ν. 4405/2016 (Α΄129)"
3. Το απόσπασμα πρακτικών της Συνεδρίασης της 5ης Συνέλευσης της Κοσμητείας της Σχολής Οικονομίας, Διοίκησης και Πληροφορικής (12-12-2016)

Αποφασίζει

Να εγκρίνει τη συγκρότηση του μητρώου εσωτερικών και εξωτερικών μελών για κρίσεις εκλογής, εξέλιξης ή μονιμοποίησης σε θέσεις Επίκουρων Καθηγητών και για κρίσεις εκλογής ή εξέλιξης σε θέσεις Αναπληρωτών Καθηγητών του Τμήματος Πληροφορικής και Τηλεπικοινωνιών στο γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές», ως ακολούθως:

Τα μέλη του παρόντος μητρώου επιλέχθηκαν από το γενικό μητρώο του πληροφοριακού συστήματος ΑΠΕΛΛΑ[1], σύμφωνα με την κοινή υπουργική απόφαση Φ.122.1/1137/145793/Β2/

[1] http://apella.minedu.gov.gr

9.10.2013 (Β΄2619), η οποία εφαρμόζεται κατά το μέρος που δεν αντίκειται στις διατάξεις του άρθρου 19 του Ν. 4009/2011 (Α΄195) όπως τροποποιήθηκε από τους Ν. 4386/2016 (Α΄83), Ν. 4405/2016 (Α΄129) και ισχύει.

Σύμφωνα με τα ανωτέρω, για την κατάρτιση του μητρώου επιλέχθηκαν μέλη ΔΕΠ βαθμίδας Καθηγητή, Αναπληρωτή Καθηγητή, και μόνιμου Επίκουρου Καθηγητή, ή Ερευνητές αντίστοιχων βαθμίδων, με ΦΕΚ διορισμού ή επιστημονικό έργο *στο ίδιο* γνωστικό αντικείμενο. Για τη συμπλήρωση ικανοποιητικού αριθμού μελών του μητρώου επιλέχθηκαν και μέλη ΔΕΠ βαθμίδας Καθηγητή, Αναπληρωτή Καθηγητή, και μόνιμου Επίκουρου Καθηγητή, ή Ερευνητές αντίστοιχων βαθμίδων, με ΦΕΚ διορισμού ή επιστημονικό έργο σε *συναφή* γνωστικά αντικείμενα, όπως ασφάλεια πληροφοριών/λογισμικού/εφαρμογών/συστημάτων, ασφάλεια και ιδιωτικότητα σε βάσεις δεδομένων/επικοινωνίες/δίκτυα, θέματα υλοποίησης και αποτίμησης κρυπτογραφικών αλγορίθμων ή μηχανισμών ασφάλειας, αντικείμενα που αποτελούν θεμέλια της κρυπτογραφίας, όπως θεωρία πληροφορίας, θεωρία κωδίκων, αλγόριθμοι και πολυπλοκότητα, κ.ο.κ.

Η διαμόρφωση του ανωτέρω καταλόγου των επιστημονικών περιοχών βασίστηκε πρωτίστως στη θεματική κατάταξη της ACM[2] (Association for Computing Machinery), την αντίστοιχη κατάταξη της AMS[3] (American Mathematical Society), και στην κοινή περί του αντικειμένου αντίληψη στον χώρο. Το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές» περιλαμβάνεται στις εξής κατηγορίες στον κατάλογο της ACM (όπου περιλαμβάνονται και συναφείς περιοχές):

Information systems
- » Data management systems
  - » Data structures
    - » Data layout
      - » Data compression
      - » Data **encryption**

Security and privacy
- » **Cryptography**
- » Formal methods and theory of security
- » Security services
- » Intrusion/anomaly detection and malware mitigation
- » Security in hardware
- » Systems security
- » Network security
- » Database and storage security
- » Software and application security
- » Human and societal aspects of security and privacy

Theory of computation
- » Computational complexity and **cryptography**
  - » Complexity classes
  - » Problems, reductions and completeness
  - » Communication complexity
  - » Circuit complexity
  - » Oracles and decision trees
  - » Algebraic complexity theory
  - » Quantum complexity theory
  - » Proof complexity
  - » Interactive proof systems

[2] http://www.acm.org/about/class/class/2012
[3] http://www.ams.org/mathscinet/msc

» Complexity theory and logic
» **Cryptographic** primitives
» **Cryptographic** protocols

Ομοίως στον κατάλογο της AMS (όπου περιλαμβάνονται και ενδεικτικές συναφείς περιοχές):

11–XX Number theory
» 11Txx Finite fields and commutative rings (number theoretic aspects)
» 11T71 Algebraic coding theory; **cryptography**
14–XX Algebraic geometry
» 14Gxx Arithmetic problems; diophantine geometry
» 14G50 Applications to coding theory and **cryptography**
68–XX Computer science
» 68Pxx Theory of data
» 68P15 Database theory
» 68P25 Data **encryption**
» 68P30 Coding and information theory (compaction, compression, models of communication, encoding schemes, etc.)
94–XX Information and communication, circuits
» 94Axx Communication, information
» 94A05 Communication theory
» 94A12 Signal theory (characterization, reconstruction, filtering, etc.)
» 94A15 Information theory, general
» 94A17 Measures of information, entropy
» 94A24 Coding theorems (Shannon theory)
» 94A29 Source coding
» 94A55 Shift register sequences and sequences over finite alphabets
» 94A60 **Cryptography**
» 94A62 Authentication and secret sharing

Για κάθε Καθηγητή, Αναπληρωτή Καθηγητή, και μόνιμο Επίκουρο Καθηγητή, ή Ερευνητή αντίστοιχης βαθμίδας που επιλέχθηκε για το μητρώο δίνεται αιτιολόγηση συνάφειας. Εφόσον ο καθηγητής έχει ΦΕΚ διορισμού ή δραστηριοποιείται στο γνωστικό αντικείμενο της κρυπτογραφίας και των εφαρμογών της θεωρείται ότι έχει *άμεση* συνάφεια με το συγκεκριμένο γνωστικό αντικείμενο· διαφορετικά, εφόσον έχει ΦΕΚ διορισμού ή δραστηριοποιείται σε συναφείς περιοχές θεωρείται ότι έχει *έμμεση* συνάφεια με το γνωστικό αντικείμενο. Σε κάθε περίπτωση, δίνεται και ενδεικτική λίστα συναφών με το γνωστικό αντικείμενο επιστημονικών εργασιών.

Μητρώο εσωτερικών μελών/κριτών

Βασιλάκης Κωνσταντίνος, Αναπληρωτής Καθηγητής, *Πανεπιστήμιο Πελοποννήσου, Τμήμα πληροφορικής και τηλεπικοινωνιών*, με γνωστικό αντικείμενο «Πληροφοριακά συστήματα»

Ο κ. Βασιλάκης έχει γνωστικό αντικείμενο το οποίο άπτεται του αντικειμένου του παρόντος μητρώου. Συγκεκριμένα, τα πληροφοριακά συστήματα, και ειδικότερα το πλαίσιο ασφάλειας αυτών, αποτελεί πεδίο εφαρμογής κρυπτογραφικών μηχανισμών, πρωτοκόλλων και υπηρεσιών (βλ. κατηγοριοποίηση ACM). Διαθέτει ερευνητικό έργο στην ευρύτερη περιοχή της ασφάλειας συστημάτων, κι ως εκ τούτου, κρίνεται ότι έχει <u>άμεση συνάφεια</u> με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Βασιλάκη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- P. Giannikopoulos and C. Vassilakis, "A distributed recommender system architecture," *International Journal of Web Engineering and Technology*, Vol. 7, No. 3, pp. 203–227, 2012.
- C. Vassilakis and C. Kareliotis, "A framework for adaptation in secure web services," in Proc. *MCIS 2009*, p. 104, 2009.
- C. Vassilakis, G. Lepouras, J. Fraser, S. Haston and P. Georgiadis, "Barriers to electronic service development," *e-Service Journal*, Vol. 4, No. 1, pp. 41–63, 2005.
- C. Boukouvalas, P. Georgiadis and C. Vassilakis, "An enhanced system for file access in a distributed UNIX environment," in Proc. *Hellenic Informatics Conference*, pp. 525–534, 1993.

Κούτρας Κωνσταντίνος, Αναπληρωτής Καθηγητής, *Πανεπιστήμιο Πελοποννήσου, Τμήμα πληροφορικής και τηλεπικοινωνιών*, με γνωστικό αντικείμενο «Υπολογισιμότητα και υπολογιστική λογική (computability and computational logic)»

Ο κ. Κούτρας έχει γνωστικό αντικείμενο κι ερευνητικό έργο στην περιοχή της υπολογιστικής πολυπλοκότητας και κρυπτογραφίας, η οποία μεταξύ άλλων περιλαμβάνει κρυπτογραφικές κατασκευές/πρωτόκολλα και λογική (βλ. κατηγοριοποίηση ACM). Συνεπώς, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Κούτρα που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- C. Koutras, C. Moyzes and Y. Zikos, "A modal logic of knowledge, belief, and estimation," in Proc. *14th JELIA 2014 (European Conf. Logics in Artificial Intelligence)*, Springer LNCS 8761, pp. 637–646, 2014.
- N. Kolokotronis and C. Koutras, "Zero knowledge proofs and applications," in *Modern Cryptography: Theory and Applications*, M. Burmester *et al.* (Eds.) Papasotiriou Pubs, pp. 635–646, 2011.
- N. Kolokotronis and C. Koutras, "Anonymity measures and privacy preservation techniques," in *Protecting Privacy in Information and Communication Technologies: Technical and Legal Issues*, C. Lambrinoudakis *et al.* (Eds.) Papasotiriou Pubs, pp. 123–145, 2010.
- C. Koutras and C. Nomikos, "The computational complexity of satisfiability in many-valued modal logic," in Proc. *3rd PLS 2001 (Panhellenic Logic Symposium)*, 2001.

Μαλαμάτος Θεοχάρης, μόνιμος Επίκουρος Καθηγητής, *Πανεπιστήμιο Πελοποννήσου, Τμήμα πληροφορικής και τηλεπικοινωνιών*, με γνωστικό αντικείμενο «Αλγόριθμοι και πολυπλοκότητα»

Ο κ. Μαλαμάτος έχει γνωστικό αντικείμενο κι ερευνητικό έργο που άπτεται του αντικειμένου του παρόντος μητρώου. Συγκεκριμένα, η περιοχή των αλγορίθμων και πολυπλοκότητας (βλ. την κατηγοριοποίηση της ACM) είναι συναφής με την κρυπτογραφία και αποτελεί αναπόσπαστο κομμάτι σημαντικών πλαισίων ανάλυσης και σχεδιασμού κρυπτοσυστημάτων. Επιπρόσθετα, το ερευνητικό του έργο που αφορά αλγορίθμους αλγεβρικής γεωμερίας (βλ. κατηγορία 14G50, υπό την 14–XX, στον κατάλογο της AMS) σχετίζεται άμεσα με την κρυπτογραφία, η οποία και αποτελεί σημαντικό πεδίο εφαρμογής αποτελεσμάτων αλγεβρικής γεωμερίας. Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Μαλαμάτου που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- S. Arya, T. Malamatos and D. Mount, "Space-time tradeoffs for approximate nearest neighbor searching," *Journal of the ACM*, 57 (1): 1–54, 2009.
- S. Arya, T. Malamatos and D. Mount, "A simple entropy-based algorithm for planar point location," *ACM Transactions on Algorithms*, 3(2) Article No. 17, 2007.

- S. Arya, T. Malamatos and D. Mount, "Space-time tradeoffs for approximate spherical range counting," in Proc. *SODA 2005*, pp. 535–544, 2005.
- S. Arya, T. Malamatos and D. Mount, "Space-efficient approximate Voronoi diagrams," in Proc. *STOC 2002*, pp. 721–730, 2002.

Μαράς Ανδρέας, Καθηγητής, *Πανεπιστήμιο Πελοποννήσου, Τμήμα πληροφορικής και τηλεπικοινωνιών*, με γνωστικό αντικείμενο «Τηλεπικοινωνίες»

Ο κ. Μαράς έχει γνωστικό αντικείμενο που άπτεται του αντικειμένου του παρόντος μητρώου, καθώς οι επικοινωνίες αποτελούν σημαντικό πεδίο εφαρμογής κρυπτογραφικών μηχανισμών και λοιπών μεθοδολογιών διασφάλισης του απορρήτου. Μέρος του ερευνητικού του έργου έργου εμπίπτει στις περιοχές της θεωρίας πληροφορίας και της θεωρίας κωδίκων (βλ. σχέσεις μεταξύ των κατηγοριών 14G50, 68P30, 94A15, 94A17, 94A24, και 94A60 στον κατάλογο της AMS). Συνεπώς, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Μαρά που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- K. Peppas, N. Sagias and A. Maras, "Physical layer security for multiple-antenna systems: a unified approach," *IEEE Trans. Communications*, 64(1) pp. 314-328, 2016.
- K. Peppas and A. Maras, "Performance evaluation of space-time block codes over keyhole Weibull fading channels," *Wireless Personal Communications*, 46(4) pp. 385-395, 2008.
- L. Nikolopooulos and A. Maras, "Information leakage in a quantum computing prototype system: stochastic noise in a microcavity", Lecture Series on Computer and Computational Sciences, Vol. 1, pp. 226-229, VSP International Science Pubs, 2004.
- A. Maras, A. Katsaros and C. Goutis, "Optimum threshold soft-decision decoding of linear block codes in impulsive noise," *IEE Electronics Letters*, 25, pp. 1160-1162, 1989.

Σκιαδόπουλος Σπυρίδωνας, Αναπληρωτής Καθηγητής, *Πανεπιστήμιο Πελοποννήσου, Τμήμα πληροφορικής και τηλεπικοινωνιών*, με γνωστικό αντικείμενο «Διαχείριση πληροφοριών»

Ο κ. Σκιαδόπουλος έχει γνωστικό αντικείμενο σε συναφή περιοχή με αυτή του παρόντος μητρώου. Περιλαμβάνει γενικότερα θέματα διαχείρισης, αποθήκευσης, και ανάκτησης πληροφοριών, με ζητήματα κρυπτογράφησης δεδομένων, καθώς και προστασίας/ασφάλειας/ιδιωτικότητας συστημάτων διαχείρισης βάσεων δεδομένων να αποτελούν σημαντική υποκατηγορία (βλ. τους καταλόγους ACM, και 68Pxx στην AMS). Μέρος του ερευνητικού του έργου εστιάζει σε θέματα σχετιζόμενα με ασφάλεια δεδομένων, και συνεπώς κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Σκιαδόπουλου που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- G. Poulis, A. Gkoulalas-Divanis, G. Loukides, S. Skiadopoulos and C. Tryfonopoulos, "SECRETA: a tool for anonymizing relational, transaction and RT-datasets," in *Medical Data Privacy Handbook*, pp. 83-109, 2015.
- G. Poulis, S. Skiadopoulos, G. Loukides and A. Gkoulalas-Divanis, "A priori-based algorithms for k^m-anonymizing trajectory data," *Trans. Data Privacy*, 7(2) pp. 165-194, 2014.
- G. Poulis, S. Skiadopoulos, G. Loukides and A. Gkoulalas-Divanis, "Distance-based k^m-anonymization of trajectory data," in Proc. *MDM*, (2) pp. 57-62, 2013.
- M. Terrovitis, J. Liagouris, N. Mamoulis and S. Skiadopoulos, "Privacy preservation by disassociation," in Proc. *PVLDB*, 5(10), pp. 944-955, 2012.

Μητρώο εξωτερικών μελών/κριτών – Πανεπιστήμια της ημεδαπής

Αφράτη Φώτω, Καθηγήτρια, *Εθνικό Μετσόβιο Πολυτεχνείο, Τμήμα ηλεκτρολόγων μηχανικών και μηχανικών υπολογιστών*, με γνωστικό αντικείμενο «Θεωρία πληροφορίας, κωδικοποίηση, αλγόριθμοι και υπολογιστική πολυπλοκότητα»

Η κα. Αφράτη έχει γνωστικό αντικείμενο κι ερευνητικό έργο το οποίο άπτεται του

αντικειμένου του παρόντος μητρώου. Συγκεκριμένα, οι περιοχές της θεωρίας πληροφορίας (βλ. κατηγορίες 94A15, 94A17, 94A24, 94A60, υπό την 94Axx, στον κατάλογο της AMS) και αλγορίθμων και πολυπλοκότητας (βλ. την κατηγοριοποίηση της ACM) είναι συναφείς με την κρυπτογραφία. Οι προαναφερθείσες περιοχές αποτελούν αναπόσπαστο κομμάτι σημαντικών πλαισίων ανάλυσης και σχεδιασμού κρυπτοσυστημάτων. Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις της κα. Αφράτη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- F.N. Afrati, S. Cohen and G.M. Kuper, "On the complexity of tree pattern containment with arithmetic comparisons," *Inf. Process. Lett.*, 111(15) pp. 754-760, 2011.
- F.N. Afrati and P.G. Kolaitis, "Answering aggregate queries in data exchange," in Proc. *PODS 2008*, pp. 129-138, 2008.
- F.N. Afrati and C.H. Papadimitriou, "The parallel complexity of simple logic programs," *J. ACM*, 40(4) pp. 891-916, 1993.
- F.N. Afrati, S.S. Cosmadakis, C.H. Papadimitriou, G. Papageorgiou and N. Papakostantinou, "The complexity of the travelling repairman problem," in Proc. *ITA*, 20(1) pp. 79-87, 1986.

Γαρεφαλάκης Θεόδουλος, Αναπληρωτής Καθηγητής, *Πανεπιστήμιο Κρήτης, Τμήμα μαθηματικών και εφαρμοσμένων μαθηματικών*, με γνωστικό αντικείμενο «Μαθηματική κρυπτογραφία–κωδικοποίηση»

Ο κ. Γαρεφαλάκης έχει γνωστικό αντικείμενο που επί της ουσίας ταυτίζεται με αυτό του παρόντος μητρώου, συνεπώς κρίνεται ότι έχει άμεση συνάφεια λόγω γνωστικού αντικειμένου ΦΕΚ με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Γαρεφαλάκη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- M. Christopoulou, T. Garefalakis, D. Panario and D. Thomson, "Gauss periods as constructions of low complexity normal bases," *Designs Codes and Cryptography*, 62(1) pp. 43-62, 2012.
- I.F. Blake and T. Garefalakis, "Polynomial approximation of Bilinear Diffie-Hellman maps," *Finite Fields and Applications*, 14(2) pp. 379-389, 2008.
- I.F. Blake, T. Garefalakis and I.E. Shparlinski, "On the bit security of the Diffie-Hellman key," *Appl. Algebra in Engin., Commun. and Computing*, 16(6) pp. 397-404, 2006.
- T. Garefalakis, "The generalized Weil pairing and the discrete logarithm problem on elliptic curves," *Theoretical Comp. Sci.*, 321, pp. 59-72, 2004.

Γκρίτζαλης Δημήτριος, Καθηγητής, *Οικονομικό Πανεπιστήμιο Αθηνών, Τμήμα πληροφορικής*, με γνωστικό αντικείμενο «Ασφάλεια στην πληροφορική και τις επικοινωνίες»

Ο κ. Γκρίτζαλης έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Γκρίτζαλη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- G. Stergiopoulos and D. Gritzalis, "Hacking and penetration testing with low power devices," *Computers & Security*, vol. 49, pp. 274-275, 2015.
- N. Tsalis, A. Mylonas and D. Gritzalis, "An intensive analysis of security and privacy browser add-ons," in Proc. *CRiSIS 2015*, pp. 258-273, 2015.
- G. Stergiopoulos, M. Kandias and D. Gritzalis, "Approaching encryption through complex number logarithms," in Proc. *SECRYPT 2013*, pp. 574-579, 2013.

- N. Virvilis, D. Gritzalis and T.K. Apostolopoulos, "Trusted computing vs. advanced persistent threats: can a defender win this game?," in Proc. *UIC/ATC 2013*, pp. 396-403, 2013.

Γκρίτζαλης Στέφανος, Καθηγητής, Πανεπιστήμιο Αιγαίου, *Τμήμα μηχανικών πληροφοριακών και επικοινωνιακών συστημάτων*, με γνωστικό αντικείμενο «Ασφάλεια πληροφοριακών και επικοινωνιακών συστημάτων»

Ο κ. Γκρίτζαλης έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Γκρίτζαλη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- J. Park, S. Gritzalis, B. Cheng and N. Zhang, "Challenges and opportunities in next-generation cyberspace security," *Security and Communication Networks*, 9(6) pp. 455-456, 2016.
- J. Clarke, S. Gritzalis, J. Zhou and R. Roman, "Protecting the internet of things," *Security and Communication Networks*, 7(12) pp. 2637-2638, 2014.
- P. Rizomiliotis and S. Gritzalis, "GHB#: a provably secure HB-like lightweight authentication protocol," in Proc. *ACNS 2012*, pp. 489-506, 2012.
- T. Balopoulos, S. Gritzalis and S.K. Katsikas, "Specifying and implementing privacy-preserving cryptographic protocols," *Int. J. Inf. Sec.*, 7(6) pp. 395-420, 2008.

Καλουπτσίδης Νικόλαος, Καθηγητής, *Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, Τμήμα πληροφορικής και τηλεπικοινωνιών*, με γνωστικό αντικείμενο «Επεξεργασία σημάτων και θεωρία συστημάτων»

Ο κ. Καλουπτσίδης έχει γνωστικό αντικείμενο το οποίο άπτεται του αντικειμένου του παρόντος μητρώου. Συγκεκριμένα, οι περιοχές της επεξεργασίας σήματος και θεωρίας συστημάτων είναι συναφείς με την κρυπτογραφία (βλ. κατηγορίες 94A12 & 94A60, υπό την 94Axx, στον κατάλογο της AMS) κι αφορούν την επεξεργασία πληροφορίας. Διαθέτει σημαντικό ερευνητικό έργο στην ευρύτερη περιοχή της κρυπτογραφίας, της θεωρίας πληροφορίας και της θεωρίας κωδίκων (βλ. σχέσεις μεταξύ των κατηγοριών 14G50, 68P30, 94A15, 94A17, 94A24, και 94A60 στον κατάλογο της AMS). Συνεπώς, το έργο του κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Καλουπτσίδη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- K. Limniotis, N. Kolokotronis and N. Kalouptsidis, "Secondary constructions of Boolean functions with maximum algebraic immunity," *Cryptography and Communications*, 5(3) pp. 179-199, 2013.
- T. Etzion, N. Kalouptsidis, N. Kolokotronis, K. Limniotis and K.G. Paterson, "Properties of the error linear complexity spectrum," *IEEE Trans. Inform. Theory*, 55(10) pp. 4681-4686, 2009.
- P. Rizomiliotis and N. Kalouptsidis, "Results on the nonlinear span of binary sequences," *IEEE Trans. Information Theory*, 51(4) pp. 1555-1563, 2005.
- N. Kalouptsidis and K. Limniotis, "Nonlinear span, minimal realizations of sequences over finite fields and De Bruijn generators," in Proc. *Int. Symposium on Information Theory and its Applications (ISITA)*, pp. 794-799, 2004.

Καμπουράκης Γεώργιος, Αναπληρωτής Καθηγητής, *Πανεπιστήμιο Αιγαίου, Τμήμα μηχανικών πληροφοριακών και επικοινωνιακών συστημάτων*, με γνωστικό αντικείμενο «Ασφάλεια κινητών και ασύρματων δικτύων επικοινωνιών»

Ο κ. Καμπουράκης έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή

από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Καμπουράκη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- M. Anagnostopoulos, G. Kambourakis and S. Gritzalis, "New facets of mobile botnet: architecture and evaluation," *Int. J. Inf. Sec.*, 15(5) pp. 455-473, 2016.
- Y.-D. Lin, C.-Y. Huang, M.K. Wright and G. Kambourakis, "Mobile application security," *IEEE Computer*, 47(6) pp. 21-23, 2014.
- G. Kambourakis, "Anonymity and closely related terms in the cyberspace: an analysis by example," *J. Inf. Sec. Appl.*, 19(1) pp. 2-17, 2014.
- D. Kasiaras, T. Zafeiropoulos, N.L. Clarke and G. Kambourakis, "Android forensics: correlation analysis," in Proc. *ICITST 2014*, pp. 157-162, 2014.

Καρύδα Μαρία, μόνιμη Επίκουρος Καθηγητής, *Πανεπιστήμιο Αιγαίου, Τμήμα μηχανικών πληροφοριακών και επικοινωνιακών συστημάτων*, με γνωστικό αντικείμενο «Διοίκηση ασφάλειας πληροφοριακών συστημάτων»

Η κα. Καρύδα έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις της κα. Καρύδα που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- M. Karyda and L. Mitrou, "Data breach notification: issues and challenges for security management," in Proc. *MCIS 2016*, p. 60, 2016.
- K. Vemou and M. Karyda, "Evaluating privacy practices in Web 2.0 services," in Proc. *MCIS 2015*, p. 7, 2015.
- A. Tsohou, M. Karyda, S. Kokolakis and E.A. Kiountouzis, "Analyzing information security awareness through networks of association," in Proc. *TrustBus 2010*, pp. 227-237, 2010.
- M. Karyda, E.A. Kiountouzis and S. Kokolakis, "Information systems security policies: a contextual perspective," *Computers & Security*, 24(3) pp. 246-260, 2005.

Κατσαρός Παναγιώτης, μόνιμος Επίκουρος Καθηγητής, *Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Τμήμα πληροφορικής*, με γνωστικό αντικείμενο «Αξιοπιστία και ασφάλεια λογισμικού»

Ο κ. Κατσαρός έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Κατσαρού που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- G. Stergiopoulos, P. Petsanas, P. Katsaros and D. Gritzalis, "Automated exploit detection using path profiling: the disposition should matter, not the position," in Proc. *12th Int. Conference on Security and Cryptography (SECRYPT)*, pp. 100-111, 2015.
- S. Basagiannis, S. Petridou, N. Alexiou, G. Papadimitriou and P. Katsaros, "Quantitative analysis of a certified e-mail protocol in mobile environments: a probabilistic model checking approach," *Computers & Security*, Vol. 30 (4) pp. 257-272, 2011.
- S. Basagiannis, P. Katsaros and A. Pombortsis, "Synthesis of attack actions using model checking for the verification of security protocols," *Security and Communication Networks*, Vol. 4 (2) pp. 147-161, 2011.
- S. Basagiannis, P. Katsaros, A. Pombortsis and N. Alexiou, "Probabilistic model checking for the quantification of DoS security threats," *Computers & Security*, Vol. 28 (6) pp. 450-465,

2009.

Κάτσικας Σωκράτης, Καθηγητής, *Πανεπιστημίο Πειραιώς, Τμήμα ψηφιακών συστημάτων*, με γνωστικό αντικείμενο «Πληροφορική»

Ο κ. Κάτσικας έχει γνωστικό αντικείμενο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα των πληροφοριακών συστημάτων, με τα ζητήματα κρυπτογράφησης δεδομένων, προστασίας & ασφάλειας υπηρεσιών, πόρων, κ.α., να αποτελούν σημαντική υποκατηγορία (βλ. κατηγοριοποιήσεις ACM και AMS). Ωστόσο, το ερευνητικό του έργο εστιάζει αποκλειστικά σε θέματα ασφάλειας πληροφοριών και συνεπώς κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Κάτσικα που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- E. Darra, C. Skouloudi and S.K. Katsikas, "A simulation platform for evaluating DoS attacks in wireless sensor networks," in Proc. *Panhellenic Conference on Informatics 2015*, pp. 144-149, 2015.
- V.G. Tasiopoulos and S.K. Katsikas, "Bypassing antivirus detection with encryption," in Proc. *Panhellenic Conference on Informatics 2014*, pp. 16:1-16:2, 2014.
- T. Balopoulos, S. Gritzalis and S.K. Katsikas, "Specifying and implementing privacy-preserving cryptographic protocols," *Int. J. Inf. Sec.*, 7(6) pp. 395-420, 2008.
- I. Kantzavelou and S.K. Katsikas, "A generic intrusion detection game model in IT security," in Proc. *TrustBus 2008*, pp. 151-162, 2008.

Κιαγιάς Άγγελλος, Αναπληρωτής Καθηγητής, *Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, Τμήμα πληροφορικής και τηλεπικοινωνιών*, με γνωστικό αντικείμενο «Κρυπτογραφία και ασφάλεια»

Ο κ. Κιαγιάς έχει γνωστικό αντικείμενο που εμπεριέχει αυτό του παρόντος μητρώου, και ως εκ τούτου κρίνεται ότι έχει άμεση συνάφεια λόγω γνωστικού αντικειμένου ΦΕΚ με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Κιαγιά που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- A. Kiayias, F.-H. Liu and Y. Tselekounis, "Practical non-malleable codes from l-more extractable hash functions," in Proc. *ACM Conference on Computer and Communications Security 2016*, pp. 1317-1328, 2016.
- G. Argyros, I. Stais, S. Jana, A.D. Keromytis and A. Kiayias, "SFADiff: automated evasion attacks and fingerprinting using black-box differential automata learning, in Proc. *ACM Conference on Computer and Communications Security 2016*, pp. 1690-1701, 2016.
- A. Kiayias, H.-S. Zhou and V. Zikas, "Fair and robust multi-party computation using a global transaction ledger," in Proc. *EUROCRYPT 2016*, pp. 705-734, 2016.
- J.A. Garay, R. Gelles, D.S. Johnson, A. Kiayias and M. Yung, "A little honesty goes a long way - the two-tier model for secure multiparty computation," in Proc. *TCC 2015*, pp. 134-158, 2015.

Κωνσταντίνου Ελισάβετ, μόνιμη Επίκουρος Καθηγητής, *Πανεπιστήμιο Αιγαίου, Τμήμα μηχανικών πληροφοριακών και επικοινωνιακών συστημάτων*, με γνωστικό αντικείμενο «Κρυπτογραφία»

Η κα. Κωνσταντίνου έχει γνωστικό αντικείμενο που επί της ουσίας ταυτίζεται με αυτό του παρόντος μητρώου, συνεπώς κρίνεται ότι έχει άμεση συνάφεια λόγω γνωστικού αντικειμένου ΦΕΚ με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις της κα. Κωνσταντίνου που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- G. Fotiadis and E. Konstantinou, "More sparse families of pairing-friendly elliptic curves, in

Proc. *13th Int. Conf. Cryptology and Network Security (CANS)*, D. Gritzalis *et al.* (eds), pp. 384-389, 2014.

- H.H. Chan, E. Konstantinou, A. Kontogeorgis and C.H. Tan, "What is your birthday elliptic curves?," *Finite Fields and Applications*, vol. 18, no. 6, pp. 1232-1241, 2012.
- E. Konstantinou, "Efficient cluster-based group key agreement protocols for wireless ad hoc networks," *J. Networks and Computer Applications*, vol. 34, no. 1, pp. 384-393, 2011.
- E. Konstantinou and A. Kontogeorgis, "Ramanujan's class invariants and their use in elliptic curve cryptography," *Computers and Mathematics with Applications*, vol. 59, no. 8, pp. 2901-2917, 2010.

Λαμπρινουδάκης Κωνσταντίνος, Αναπληρωτής Καθηγητής, *Πανεπιστήμιο Πειραιώς, Τμήμα ψηφιακών συστημάτων*, με γνωστικό αντικείμενο «Τεχνολογίες διασφάλισης ιδιωτικότητας»

Ο κ. Λαμπρινουδάκης έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Λαμπρινουδάκη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- P. Drogkaris, S. Gritzalis, C. Kalloniatis and C. Lambrinoudakis, "A hierarchical multitier approach for privacy policies in e-government environments," *Future Internet*, 7(4) pp. 500-515, 2015.
- D. Georgiou and C. Lambrinoudakis, "Cloud computing security requirements and a methodology for their auditing," in Proc. *e-Democracy 2015*, pp. 51-61, 2015.
- E.-L. Makri and C. Lambrinoudakis, "Privacy principles: towards a common privacy audit methodology," in Proc. *TrustBus 2015*, pp. 219-234, 2015.
- N. Pitropakis, N. Yfantopulos, D. Geneiatakis and C. Lambrinoudakis, "Towards an augmented authenticator in the cloud," in Proc. *ISSPIT 2014*, pp. 296-300, 2014.

Μάγκος Εμμανουήλ, μόνιμος Επίκουρος Καθηγητής, *Ιόνιο Πανεπιστήμιο, Τμήμα πληροφορικής*, με γνωστικό αντικείμενο «Κρυπτογραφία και ασφάλεια υπολογιστικών συστημάτων»

Ο κ. Μάγκος έχει γνωστικό αντικείμενο που εμπεριέχει αυτό του παρόντος μητρώου, και ως εκ τούτου κρίνεται ότι έχει άμεση συνάφεια λόγω γνωστικού αντικειμένου ΦΕΚ με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Μάγκου που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- E. Magkos and P. Kotzanikolaou, "SCN-SI-021 achieving privacy and access control in pervasive computing environments," *Security and Communication Networks*, 9(2) pp. 94-105, 2016.
- E. Magkos, P. Kotzanikolaou, M. Magioladitis, S. Sioutas and V.S. Verykios, "Towards secure and practical location privacy through private equality testing," in Proc. *Privacy in Statistical Databases 2014*, pp. 312-325, 2014.
- M. Burmester, E. Magkos and V. Chrissikopoulos, "Secure and privacy-preserving, timed vehicular communications," *IJAHUC*, 10(4) pp. 219-229, 2012.
- M. Burmester, E. Magkos and V. Chrissikopoulos, "Modeling security in cyber-physical systems," *IJCIP*, 5(3-4) pp. 118-126, 2012.

Μαυρίδης Ιωάννης, Αναπληρωτής Καθηγητής, *Πανεπιστήμιο Μακεδονίας, Τμήμα εφαρμοσμένης πληροφορικής*, με γνωστικό αντικείμενο «Ασφάλεια πληροφοριακών συστημάτων»

Ο κ. Μαυρίδης έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και

ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Μαυρίδη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- A. Gouglidis and I. Mavridis, "domRBAC: an access control model for modern collaborative systems," *Computers & Security*, Vol. 31, Issue 4, pp. 540-556, 2012.
- I. Mavridis, "Deploying privacy improved RBAC in web information systems," *Int. Journal of Information Technologies and the Systems Approach (IJITSA)*, Special Issue on Privacy and Security Issues in IT, 4(2) pp.70-87, 2011.
- A. Chatzipoulidis and I. Mavridis, "An ICT security management framework," in Proc. *Int. Conference on Security and Cryptography (SECRYPT)*, 2010.
- D. Michalopoulos and I. Mavridis, "Towards risk based prevention of grooming attacks," in Proc. *Int. Conference on Security and Cryptography (SECRYPT)*, 2010.

Μήτρου Ευαγγελία, Αναπληρωτής Καθηγητής, *Πανεπιστήμιο Αιγαίου, Τμήμα μηχανικών πληροφοριακών και επικοινωνιακών συστημάτων*, με γνωστικό αντικείμενο «Νομικό περιβάλλον στην κοινωνία της πληροφορίας με έμφαση στην προστασία προσωπικών δεδομένων»

Η κα. Μήτρου έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας, καθώς και κοινωνικά, θεσμικά, κ.α. (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις της κα. Μήτρου που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- M. Karyda and L. Mitrou, "Data breach notification: issues and challenges for security management," in Proc. *MCIS 2016*, p. 60, 2016.
- M. Tsavli, P.S. Efraimidis, V. Katos and L. Mitrou, "Reengineering the user: privacy concerns about personal data on smartphones," *Information and Computer Security*, vol. 23, no. 4, pp. 394-405, 2015.
- E. Lalas, L. Mitrou and C. Lambrinoudakis, "ProCAVE: privacy-preserving collection and authenticity validation of online evidence," in Proc. *10th Int. Conf. Trust, Privacy & Security in Digital Business (TRUSTBUS)*, LNCS 8058, pp. 137-148, 2013.
- M.E. Skarkala, H. Toivonen, P. Moen, M. Maragoudakis, S. Gritzalis and L. Mitrou, "Privacy preservation by *k*-anonymization of weighted social networks," in Proc. *2012 IEEE/ACM Int. Conf. Advances in Social Networks Analysis and Mining*, pp. 423-428, 2012.

Ξενάκης Χρήστος, Αναπληρωτής Καθηγητής, *Πανεπιστήμιο Πειραιώς, Τμήμα ψηφιακών συστημάτων*, με γνωστικό αντικείμενο «Ασφάλεια δικτυακών συστημάτων»

Ο κ. Ξενάκης έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Ξενάκη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- C. Ntantogian, S. Malliaros and C. Xenakis, "Gaithashing: a two-factor authentication scheme based on gait features," *Computers & Security*, Vol. 52, Issue 1, pp. 17-32, 2015.
- C. Xenakis and C. Ntantogian, "Attacking the baseband modem of mobile phones to breach the users' privacy and network security," in Proc. *7th International Conference on Cyber Conflict (CyCon)*, 2015.
- F. Demertzis and C. Xenakis, "SOMA-E: self-organised mesh authentication extended," *Mathematical and Computer Modeling*, Vol. 57, Issue 7-8, pp. 1606-1616, 2013.

- D. Apostolopoulos, G. Marinakis, C. Ntantogian and C. Xenakis, "Discovering authentication credentials in volatile memory of Android mobile devices," in Proc. *12th IFIP Conference on e-Business, e-Services, e-Society (I3E)*, 2013.

Πολέμη Δέσποινα, Αναπληρωτής Καθηγητής, *Πανεπιστήμιο Πειραιώς, Τμήμα πληροφορικής*, με γνωστικό αντικείμενο «Ηλεκτρονικό επιχειρείν και συστήματα ασφάλειας πληροφοριών»

Η κα. Πολέμη έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις της κα. Πολέμη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- K. Dellios, D. Papanikas and D. Polemi, "Information security compliance over intelligent transport systems: is it possible?," *IEEE Security & Privacy*, 13(3) pp. 9-15, 2015.
- A. Karantjias and D. Polemi, "Assessment of advanced cryptographic antiviral techniques," *IJESDF* 3(1) pp. 60-72, 2010.
- S. Papastergiou, A. Karantjias, D. Polemi and M. Markovic, "A secure mobile framework for m-services," in Proc. *ICIW 2008*, pp. 309-313, 2008.
- D. Polemi, "An algebraic-geometric public key cryptosystem," *Developments in Language Theory*, pp. 521-528, 1997.

Πουλάκης Δημήτριος, Καθηγητής, *Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Τμήμα μαθηματικών*, με γνωστικό αντικείμενο «Θεωρία αριθμών ή αλγεβρική γεωμετρία»

Ο κ. Πουλάκης έχει γνωστικό αντικείμενο σε συναφή περιοχή με αυτή του παρόντος μητρώου η οποία περιλαμβάνει θεωρίες, εργαλεία, κι αποτελέσματα που χρησιμοποιούνται για τη μελέτη (σχεδιασμό και ανάλυση) κρυπτοσυστημάτων (βλ. κατηγοριοποίηση της AMS, και την 11–XX). Σημαντικό μέρος του πρόσφατου ερευνητικού του έργου εστιάζει στην κρυπτογραφία, και συγκεκριμένα σε θέματα που αφορούν ψηφιακές υπογραφές. Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Πουλάκη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- D. Poulakis, "New lattice attacks on DSA schemes," *J. Mathematical Cryptology*, 10(2) pp. 135-144, 2016.
- K. Draziotis and D. Poulakis, "Lattice attacks on DSA schemes based on Lagrange's algorithm," in Proc. *CAI 2013*, pp. 119-131, 2013.
- D. Poulakis, "Some lattice attacks on DSA and ECDSA," *Appl. Algebra Eng. Commun. Comput.*, 22(5-6) pp. 347-358, 2011.
- D. Poulakis, "A variant of Digital Signature Algorithm," *Des. Codes Cryptography*, 51(1) pp. 99-104, 2009.

Ράπτης Ευάγγελος, Καθηγητής, *Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, Τμήμα μαθηματικών*, με γνωστικό αντικείμενο «Θεωρία ομάδων»

Ο κ. Ράπτης έχει γνωστικό αντικείμενο σε συναφή περιοχή με αυτή του παρόντος μητρώου η οποία περιλαμβάνει θεωρίες, εργαλεία, κι αποτελέσματα που χρησιμοποιούνται για τη μελέτη (σχεδιασμό κι ανάλυση) κρυπτοσυστημάτων (βλ. κατηγοριοποίηση AMS, και την 11–XX). Το ερευνητικό έργο αντιμετωπίζει θέματα με άμεση εφαρμογή σε αλγεβρικές και αριθμοθεωρητικές κατασκευές κρυπτογραφικών αλγορίθμων και πρωτοκόλλων, κι άρα κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Ράπτη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- V. Metaftsis, E. Raptis and D. Varsos, "On the linearity of HNN-extensions with abelian base," *J. Pure and Applied Algebra*, Vol. 216, No. 5, pp. 997-1003, 2012.
- E. Raptis, O. Talelli and D. Varsos, "On residual finiteness of graphs of nilpotent groups," *Int. J. Algebra and Computation*, 14(4) pp. 403-408, 2004.
- E. Raptis, O. Talelli and D. Varsos, "On the conjugacy separability of certain graphs of groups," *J. Algebra*, Vol. 199, No. 1, pp. 327-336, 1998.
- E. Raptis, O. Talelli and D. Varsos, "On finiteness conditions of certain graphs of groups," *Int. J. Algebra and Computation*, 5(6) pp. 719-724, 1995.

Ριζομυλιώτης Παναγιώτης, μόνιμος Επίκουρος Καθηγητής, *Πανεπιστήμιο Αιγαίου, Τμήμα μηχανικών πληροφοριακών και επικοινωνιακών συστημάτων*, με γνωστικό αντικείμενο «Θεωρία πληροφορίας με εφαρμογές στην κρυπτογραφία»

Ο κ. Ριζομυλιώτης έχει γνωστικό αντικείμενο το οποίο είναι εξαιρετικά συναφές με αυτό του παρόντος μητρώου, συνεπώς κρίνεται ότι έχει άμεση συνάφεια λόγω γνωστικού αντικειμένου ΦΕΚ με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Ριζομυλιώτη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- E. Rekleitis, P. Rizomiliotis and S. Gritzalis, "How to protect security and privacy in the internet of things: a policy-based RFID tag management protocol," *Security and Communication Networks*, Vol. 7, No. 12, pp. 2669-2683, 2014.
- P. Rizomiliotis and S. Gritzalis, "On the security of AUTH, an authentication protocol based on the subspace LPN problem," *Int. J. Information Security*, Vol. 12, No. 2, pp. 151-154, 2013.
- P. Rizomiliotis, "Improving the high order nonlinearity lower bound for Boolean functions with given algebraic immunity," *Discrete Applied Mathematics*, Vol. 158, No. 18, pp. 2049-2055, 2010.
- P. Rizomiliotis, "Constructing periodic binary sequences of maximum nonlinear span," *IEEE Transactions on Information Theory*, Vol. 52, No. 9, pp. 4257-4261, 2006.

Σκλάβος Νικόλαος, Αναπληρωτής Καθηγητής, *Πανεπιστήμιο Πατρών, Τμήμα μηχανικών ηλεκτρονικών υπολογιστών και πληροφορικής*, με γνωστικό αντικείμενο «Ηλεκτρονική με έμφαση στον ψηφιακό σχεδιασμό»

Ο κ. Σκλάβος έχει γνωστικό αντικείμενο το οποίο άπτεται του αντικειμένου του παρόντος μητρώου. Συγκεκριμένα, τα θέματα αποδοτικής υλοποίησης κρυπτογραφικών αλγορίθμων σε υλικό αποτελούν βασικά κριτήρια σχεδιασμού και αποτίμησης της απόδοσής τους. Ωστόσο, το ερευνητικό του έργο εστιάζει σχεδόν αποκλειστικά σε θέματα σχεδιασμού, υλοποίησης, καθώς και βελτιστοποίησης κρυπτογραφικών μηχανισμών, κι άρα κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Σκλάβου που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- A. Fournaris, L. Papachristodoulou, L. Batina and N. Sklavos, "Residue number system as a side channel and fault injection attack countermeasure in elliptic curve cryptography," in Proc. *DTIS 2016*, pp. 1-4, 2016.
- A. Fournaris, I. Zafeirakis, C. Koulamas, N. Sklavos and O. Koufopavlou, "Designing efficient elliptic curve Diffie-Hellman accelerators for embedded systems," in Proc. *ISCAS 2015*, pp. 2025-2028, 2015.
- A. Fournaris and N. Sklavos, "Secure embedded system hardware design - a flexible security and trust enhanced approach," *Computers & Electrical Engineering*, 40(1) pp. 121-133, 2014.
- N. Sklavos, "Securing communication devices via physical unclonable functions (PUFs)," in Proc. *ISSE 2013*, pp. 253-261, 2013.

Σταματίου Ιωάννης, Αναπληρωτής Καθηγητής, *Πανεπιστήμιο Πατρών, Τμήμα διοίκησης επιχειρήσεων*, με γνωστικό αντικείμενο «Ασφάλεια συναλλαγών στο ηλεκτρονικό επιχειρείν»

Ο κ. Σταματίου έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Σταματίου που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- K. Ispoglou, C. Makris, Y.C. Stamatiou, E.C. Stavropoulos, A.K. Tsakalidis and V. Iosifidis, Partial Order Preserving Encryption Search Trees. DEXA (2) 2015: 49-56
- P.E. Nastou and Y.C. Stamatiou, "A distributed, parametric platform for constructing secure s-boxes in block cipher designs," in Proc. *FGIT-SecTech 2011*, pp. 155-166, 2011.
- E. Konstantinou, A. Kontogeorgis, Y.C. Stamatiou and C.D. Zaroliagis, "On the efficient generation of prime-order elliptic curves," *J. Cryptology*, 23(3) pp. 477-503, 2010.
- E. Konstantinou, Y.C. Stamatiou and C.D. Zaroliagis, On the use of Weber polynomials in elliptic curve cryptography," in Proc. *EuroPKI 2004*, pp. 335-349, 2004.

Στεφανίδης Γεώργιος, Καθηγητής, *Πανεπιστήμιο Μακεδονίας, Τμήμα εφαρμοσμένης πληροφορικής*, με γνωστικό αντικείμενο «Εφαρμοσμένα μαθηματικά»

Ο κ. Στεφανίδης έχει γνωστικό αντικείμενο σε συναφή ευρεία περιοχή με αυτή του παρόντος μητρώου, η οποία περιλαμβάνει θεωρίες, εργαλεία, και αποτελέσματα που χρησιμοποιούνται για τη μελέτη (σχεδιασμό κι ανάλυση) κρυπτοσυστημάτων. Σημαντικό μέρος του ερευνητικού έργου εστιάζει στην κρυπτογραφία, κι ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Στεφανίδη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- D.G. Papachristoudis, S.T. Halkidis and G. Stephanides, "An experimental comparison of some LLL-type lattice basis reduction algorithms," *Int. J. Applied and Computational Mathematics*, Vol. 1, No. 3, pp. 327–342, 2015.
- A. Polychroniadou, K. Chalkias and G. Stephanides, "The concept of compatibility between identity-based and certificateless encryption schemes," in Proc. *SECRYPT 2012*, pp. 403-407, 2012.
- G. Stephanides, "Short-key certificateless encryption," in Proc. *Wrkshp Lightweight Security & Privacy: Devices, Protocols, and Applications (LightSec 2011)*, pp. 69-75, IEEE Press, 2011.
- K. Chalkias, G. Filiadis, G. Stephanides, "Implementing authentication protocol for exchanging encrypted messages via an authentication server based on elliptic curve cryptography with the ElGamal's algorithm," *Int. J. Computer, Control, Quantum and Information Engineering*, Vol. 1, No. 7, 2007.

Χρυσικόπουλος Βασίλειος, Καθηγητής, *Ιόνιο Πανεπιστήμιο, Τμήμα πληροφορικής*, με γνωστικό αντικείμενο «Πληροφορική – δίκτυα – ασφάλεια πληροφοριών»

Ο κ. Χρυσικόπουλος έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Χρυσικόπουλου που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- M. Burmester, E. Magkos and V. Chrissikopoulos, "Secure and privacy-preserving, timed vehicular communications," *IJAHUC*, 10(4) pp. 219-229, 2012.
- M. Burmester, E. Magkos and V. Chrissikopoulos, "Modeling security in cyber-physical

systems," *IJCIP*, 5(3-4) pp. 118-126, 2012.

- M. Burmester, V. Chrissikopoulos, P. Kotzanikolaou and E. Magkos, "Strong forward security," in Proc. *SEC 2001*, pp. 109-122, 2001.
- N. Alexandris, M. Burmester, V. Chrissikopoulos and D. Peppes, "Efficient and provably secure key agreement," in Proc. *SEC 1996*, pp. 227-236, 1996.

Μητρώο εξωτερικών μελών/κριτών – Πανεπιστήμια της αλλοδαπής

Burmester Mike, Professor, *Florida State University, Department of computer science*, με γνωστικό αντικείμενο «Computer science»

Ο κ. Burmester έχει γνωστικό αντικείμενο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου, η οποία περιλαμβάνει γενικότερα θέματα πληροφοριακών συστημάτων, με τα ζητήματα κρυπτογράφησης δεδομένων, προστασίας & ασφάλειας υπηρεσιών, πόρων, κ.α., να αποτελούν σημαντική υποκατηγορία (βλ. κατηγοριοποιήσεις ACM και AMS). Ωστόσο, το ερευνητικό του έργο εστιάζει αποκλειστικά σε θέματα ασφάλειας πληροφοριών και συνεπώς κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Burmester που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- M. Burmester, E. Magkos and V. Chrissikopoulos, "Secure and privacy-preserving, timed vehicular communications," *IJAHUC*, 10(4) pp. 219-229, 2012.
- M. Burmester, E. Magkos and V. Chrissikopoulos, "Modeling security in cyber-physical systems," *IJCIP*, 5(3-4) pp. 118-126, 2012.
- M. Burmester, V. Chrissikopoulos, P. Kotzanikolaou and E. Magkos, "Strong forward security," in Proc. *SEC 2001*, pp. 109-122, 2001.
- N. Alexandris, M. Burmester, V. Chrissikopoulos and D. Peppes, "Efficient and provably secure key agreement," in Proc. *SEC 1996*, pp. 227-236, 1996.

Δημητρίου Αναστάσιος, Associate Professor, *Kuwait University, Department of computer engineering*, με γνωστικό αντικείμενο «Computer and network security, sensor, ad–hoc and RFID networks, smart electricity grids, ubiquitous computing, analysis of algorithms»

Ο κ. Δημητρίου έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Δημητρίου που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- T. Dimitriou, "Key evolving RFID systems: forward/backward privacy and ownership transfer of RFID tags," *Ad Hoc Networks*, vol. 37, pp. 195-208, 2016.
- T. Dimitriou and A. Michalas, "Multi-party trust computation in decentralized environments in the presence of malicious adversaries," *Ad Hoc Networks*, vol. 15, pp. 53-66, 2014.
- A. Michalas, T. Dimitriou, T. Giannetsos, N. Komninos and N.R. Prasad, "Vulnerabilities of decentralized additive reputation systems regarding the privacy of individual votes," *Wireless Personal Communications*, 66(3) pp. 559-575, 2012.
- T. Tiropanis and T. Dimitriou, "Use of ID-based cryptography for the efficient verification of the integrity and authenticity of web resources," in Proc. *SecureComm 2009*, pp. 340-349, 2009.

Κάτος Βασίλειος, Professor, *Bournemouth University, Department of computing and informatics*, με γνωστικό αντικείμενο «Computing – information security, cyber security, digital forensics»

Ο κ. Κάτος έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση

συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».
Ενδεικτικές δημοσιεύσεις του κ. Κάτου που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- S.A. Menesidou, D. Vardalis and V. Katos, "Automated key exchange protocol evaluation in delay tolerant networks," *Computers and Security*, vol. 59, pp. 1-8, 2016.
- S.-A. Menesidou and V. Katos, "Authenticated key exchange (AKE) in delay tolerant networks," in Proc. *SEC 2012*, pp. 49-60, 2012.
- V. Katos and B.S. Doherty, "Exploring confusion in product ciphers through regression analysis," *Inf. Sci.*, 177(8) pp. 1789-1795, 2007.
- V. Katos, "Diffusion behaviour of cryptographic primitives in Feistel networks," in Proc. *WOSIS 2004*, pp. 79-87, 2004.

Μαρκαντωνάκης Κωνσταντίνος, Associate Professor, *Royal Holloway, University of London, Information security group*, με γνωστικό αντικείμενο «Information security»
Ο κ. Μαρκαντωνάκης έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».
Ενδεικτικές δημοσιεύσεις του κ. Μαρκαντωνάκη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- P.-F. Bonnefoi, P. Dusart, D. Sauveron, R.N. Akram and K. Markantonakis, "A set of efficient privacy protection enforcing lightweight authentication protocols for low-cost RFID tags," in Proc. *TrustCom 2015*, pp. 612-620, 2015.
- K. Markantonakis, R.N. Akram and M.G. Msgna, "Secure and trusted application execution on embedded devices," in Proc. *SECITC 2015*, pp. 3-24, 2015.
- R.N. Akram, K. Markantonakis and K. Mayes, "A privacy preserving application acquisition protocol," in Proc. *TrustCom 2012*, pp. 383-392, 2012.
- L. Francis, G.P. Hancke, K. Mayes and K. Markantonakis, "Practical NFC peer-to-peer relay attack using mobile phones," in Proc. *RFIDSec 2010*, pp. 35-49, 2010.

Μουρατίδης Χαράλαμπος, Professor, *University of Brighton, Department of computing, engineering and mathematics*, με γνωστικό αντικείμενο «Software engineering, security engineering, information systems, requirements engineering, secure software systems engineering, multi–agent systems»
Ο κ. Μουρατίδης έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».
Ενδεικτικές δημοσιεύσεις του κ. Μουρατίδη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- S. Simou, C. Kalloniatis, H. Mouratidis and S. Gritzalis, "Towards a model-based framework for forensic-enabled cloud information systems," in Proc. *TrustBus 2016*, pp. 35-47, 2016.
- M. Pavlidis, S. Islam, H. Mouratidis and P. Kearney, "Modeling trust relationships for developing trustworthy information systems," *Int. J. Information System Modeling & Design*, 5(1) pp. 25-48, 2014.
- H. Mouratidis and M. Kang, "Secure by design: developing secure software systems from the ground up," *Int. J. Secure Software Engineering*, 2(3), pp. 23-41, 2011.
- H. Mouratidis and P. Giorgini, "Security attack testing (SAT) - testing the security of information systems at design time," *Inf. Syst.*, 32(8), pp. 1166-1183, 2007.

Σπανουδάκης Γεώργιος, Professor, *City University London, Department of computer science*, με γνωστικό αντικείμενο «Software engineering, software systems security, cloud & service

oriented computing»

Ο κ. Σπανουδάκης έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Σπανουδάκη που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- N.E. Petroulakis, G. Spanoudakis and I.G. Askoxylakis, "Patterns for the design of secure and dependable software defined networks," *Computer Networks*, vol. 109, pp. 39-49, 2016.
- M. Krotsiani, G. Spanoudakis and C. Kloukinas, "Monitoring-based certification of cloud service security," in Proc. *OTM Conferences 2015*, pp. 644-659, 2015.
- L. Pino and G. Spanoudakis, "Constructing secure service compositions with patterns," in Proc. *SERVICES 2012*, pp. 184-191, 2012.
- C. Kloukinas and G. Spanoudakis, "A pattern-driven framework for monitoring security and dependability," in Proc. *TrustBus 2007*, pp. 210-218, 2007.

Τσαπτσίνος Δημήτριος, Associate Professor, *Kingston University, Department of computer science and mathematics*, με γνωστικό αντικείμενο «Computer science with interest in cyber security, digital forensics and learning & teaching»

Ο κ. Τσαπτσίνος έχει γνωστικό αντικείμενο κι ερευνητικό έργο σε ευρύτερη περιοχή από αυτή του παρόντος μητρώου η οποία περιλαμβάνει γενικότερα θέματα ασφάλειας και ιδιωτικότητας (βλ. κατηγοριοποίηση ACM). Ως εκ τούτου, κρίνεται ότι έχει άμεση συνάφεια με το γνωστικό αντικείμενο «Κρυπτογραφία, Κρυπτανάλυση και Εφαρμογές».

Ενδεικτικές δημοσιεύσεις του κ. Τσαπτσίνου που σχετίζονται με το γνωστικό αντικείμενο του παρόντος μητρώου είναι οι ακόλουθες:

- T. Bjerkestrand, D. Tsaptsinos and E. Pfluegel, "An evaluation of feature selection and reduction algorithms for network IDS data," in Proc. *CyberSA 2015*, pp. 1-2, 2015.
- C.A. Clarke, E. Pfluegel and D. Tsaptsinos, "Multi-channel overlay protocols: implementing ad-hoc message authentication in social media platforms," in Proc. *CyberSA 2015*, pp. 1-6, 2015.
- C.A. Clarke, E. Pfluegel and D. Tsaptsinos, "Hide-as-you-type: an approach to natural language steganography through sentence modification," in Proc. *HPCC/CSS/ICESS 2014*, pp. 945-952, 2014.
- C.A. Clarke, E. Pfluegel and D. Tsaptsinos, "Enhanced virtual private social networks: implementing user content confidentiality," in Proc. *ICITST 2013*, pp. 306-312, 2013.

Ίδρυμα: Πανεπιστήμιο Πελοποννήσου
Τμήμα: Πληροφορικής και Τηλεπικοινωνιών
Γνωστικό αντικείμενο: Κρυπτογραφία, κρυπτανάλυση και εφαρμογές
Βαθμίδα: Επίκουρος Καθηγητής (μονιμοποίηση)

Μητρώο Εσωτερικών Μελών/Κριτών

Α/Α	Επώνυμο	Όνομα	Ίδρυμα	Τμήμα	Βαθμίδα	Γνωστικό αντικείμενο	ΦΕΚ διορισμού	Συνάφεια
1	Βασιλάκης	Κωνσταντίνος	Πανεπιστήμιο Πελοποννήσου	Πληροφορικής και τηλεπικοινωνιών	Αναπληρωτής Καθηγητής	Πληροφοριακά συστήματα	460/14.07.11 τ.Γ	Βάσει έργου (άμεση)
2	Κούτρας	Κωνσταντίνος	Πανεπιστήμιο Πελοποννήσου	Πληροφορικής και τηλεπικοινωνιών	Αναπληρωτής Καθηγητής	Υπολογισιμότητα και υπολογιστική λογική (computability and computational logic)	789/06.08.12 τ.Γ	Βάσει ΦΕΚ (άμεση)
3	Μαλαμάτος	Θεοχάρης	Πανεπιστήμιο Πελοποννήσου	Πληροφορικής και τηλεπικοινωνιών	Επίκουρος Καθηγητής	Αλγόριθμοι και πολυπλοκότητα	316/11.04.08 τ.Γ, ΦΕΚ μονιμοποίησης 1070/03.10.12 τ.Γ	Βάσει ΦΕΚ (άμεση)
4	Μαράς	Ανδρέας	Πανεπιστήμιο Πελοποννήσου	Πληροφορικής και τηλεπικοινωνιών	Καθηγητής Α' Βαθμίδας	Τηλεπικοινωνίες	207/09.12.99 τ.ΝΠΔΔ	Βάσει έργου (άμεση)
5	Σκιαδόπουλος	Σπυρίδωνας	Πανεπιστήμιο Πελοποννήσου	Πληροφορικής και τηλεπικοινωνιών	Αναπληρωτής Καθηγητής	Διαχείριση πληροφοριών	460/14.07.11 τ.Γ	Βάσει έργου (άμεση)

Σημειώσεις:

1. Στην τελευταία στήλη (Συνάφεια) πρέπει να σημειώνεται εάν πρόκειται για συνάφεια βάσει ΦΕΚ (δηλαδή βάσει του γνωστικού αντικειμένου που αναγράφεται στο οικείο ΦΕΚ τελευταίου διορισμού) ή για συνάφεια βάσει έργου.

2. Στην τελευταία στήλη (Συνάφεια) μπορεί επιπλέον να σημειώνεται και μία ένδειξη ως προς το βαθμό συνάφειας (π.χ. άμεση ή έμμεση συνάφεια). Μπορεί όμως, κατά την κρίση του οικείου Τμήματος, να σημειώνονται και ενδείξεις για πιο αναλυτικές διαφοροποιήσεις ως προς τον βαθμό συνάφειας.

3. Για τη διευκόλυνση της αρχειοθέτησης, ο αριθμός του ΦΕΚ διορισμού πρέπει να αναγράφεται με μία από τις μορφές που σημειώνονται στις παραπάνω περιπτώσεις.

Ίδρυμα: Πανεπιστήμιο Πελοποννήσου
Τμήμα: Πληροφορικής και Τηλεπικοινωνιών
Γνωστικό αντικείμενο: Κρυπτογραφία, κρυπτανάλυση και εφαρμογές
Βαθμίδα: Επίκουρος Καθηγητής (μονιμοποίηση)

Μητρώο Εξωτερικών Μελών/Κριτών - Ελληνικά Πανεπιστήμια

Α/Α	Επώνυμο	Όνομα	Ίδρυμα	Τμήμα	Βαθμίδα	Γνωστικό αντικείμενο	ΦΕΚ διορισμού	Συνάφεια
1	Αφράτη	Φώτω	Εθνικό Μετσόβειο Πολυτεχνείο	Ηλεκτρολόγων μηχανικών και μηχανικών υπολογιστών	Καθηγητής Α' Βαθμίδας	Θεωρία πληροφορίας, κωδικοποίηση, αλγόριθμοι και υπολογιστική πολυπλοκότητα	119/23.09.93 τ.ΝΠΔΔ	Βάσει ΦΕΚ (άμεση)
2	Γαρεφαλάκης	Θεόδουλος	Πανεπιστήμιο Κρήτης	Μαθηματικών και εφαρμοσμένων μαθηματικών	Αναπληρωτής Καθηγητής	Μαθηματική κρυπτογραφία-κωδικοποίηση	813/01.08.13 τ.Γ	Βάσει ΦΕΚ (άμεση)
3	Γκρίτζαλης	Δημήτριος	Οικονομικό Πανεπιστήμιο Αθηνών	Πληροφορικής	Καθηγητής Α' Βαθμίδας	Ασφάλεια στην πληροφορική και τις επικοινωνίες	663/21.08.09 τ.ΝΠΔΔ	Βάσει ΦΕΚ (άμεση)
4	Γκρίτζαλης	Στέφανος	Πανεπιστήμιο Αιγαίου	Μηχανικών πληροφοριακών και επικοινωνιακών συστημάτων	Καθηγητής Α' Βαθμίδας	Ασφάλεια πληροφοριακών και επικοινωνιακών συστημάτων	731/06.08.08 τ.Γ	Βάσει ΦΕΚ (άμεση)
5	Καλουπτσίδης	Νικόλαος	Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών	Πληροφορικής και τηλεπικοινωνιών	Καθηγητής Α' Βαθμίδας	Επεξεργασία σημάτων και θεωρία συστημάτων	186/19.09.88 τ.ΝΠΔΔ	Βάσει έργου (άμεση)
6	Καμπουράκης	Γεώργιος	Πανεπιστήμιο Αιγαίου	Μηχανικών πληροφοριακών και επικοινωνιακών	Αναπληρωτής Καθηγητής	Ασφάλεια κινητών και ασύρματων δικτύων επικοινωνιών	28/20.01.16 τ.Γ	Βάσει ΦΕΚ (άμεση)

				συστημάτων				
7	Καρύδα	Μαρία	Πανεπιστήμιο Αιγαίου	Μηχανικών πληροφοριακών και επικοινωνιακών συστημάτων	Επίκουρος Καθηγητής	Διοίκηση ασφάλειας πληροφοριακών συστημάτων	542/12.06.15 τ.Γ ΦΕΚ αλλαγής γν. αντ. 916/05.04.16 τ.Β	Βάσει ΦΕΚ (άμεση)
8	Κατσαρός	Παναγιώτης	Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης	Πληροφορικής	Επίκουρος Καθηγητής	Αξιοπιστία και ασφάλεια λογισμικού	554/25.06.10 τ.Γ ΦΕΚ μονιμοποίησης 324/15.04.15 τ.Γ	Βάσει ΦΕΚ (άμεση)
9	Κάτσικας	Σωκράτης	Πανεπιστημίο Πειραιώς	Ψηφιακών συστημάτων	Καθηγητής Α' Βαθμίδας	Πληροφορική	294/02.05.07 τ.Γ	Βάσει έργου (άμεση)
10	Κιαγιάς	Άγγελλος	Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών	Πληροφορικής και τηλεπικοινωνιών	Αναπληρωτής Καθηγητής	Κρυπτογραφία και ασφάλεια	524/08.06.15 τ.Γ	Βάσει ΦΕΚ (άμεση)
11	Κωνσταντίνου	Ελισάβετ	Πανεπιστήμιο Αιγαίου	Μηχανικών πληροφοριακών και επικοινωνιακών συστημάτων	Επίκουρος Καθηγητής	Κρυπτογραφία	542/12.06.15 τ.Γ	Βάσει ΦΕΚ (άμεση)
12	Λαμπρινουδάκης	Κωνσταντίνος	Πανεπιστημίο Πειραιώς	Ψηφιακών συστημάτων	Αναπληρωτής Καθηγητής	Τεχνολογίες διασφάλισης ιδιωτικότητας	464/29.04.13 τ.Γ	Βάσει ΦΕΚ (άμεση)
13	Μάγκος	Εμμανουήλ	Ιόνιο Πανεπιστήμιο	Πληροφορικής	Επίκουρος Καθηγητής	Κρυπτογραφία και ασφάλεια υπολογιστικών συστημάτων	1340/31.12.15 τ.Γ	Βάσει ΦΕΚ (άμεση)
14	Μαυρίδης	Ιωάννης	Πανεπιστήμιο Μακεδονίας	Εφαρμοσμένης πληροφορικής	Αναπληρωτής Καθηγητής	Ασφάλεια πληροφοριακών συστημάτων	635/03.07.12 τ.Γ	Βάσει ΦΕΚ (άμεση)

15	Μήτρου	Ευαγγελία	Πανεπιστήμιο Αιγαίου	Μηχανικών πληροφοριακών και επικοινωνιακών συστημάτων	Αναπληρωτής Καθηγητής	Νομικό περιβάλλον στην κοινωνία της πληροφορίας με έμφαση στην προστασία προσωπικών δεδομένων	426/11.04.12 τ.Γ ΦΕΚ διόρθωσης 475/27.04.12 τ.Γ	Βάσει έργου (άμεση)
16	Ξενάκης	Χρήστος	Πανεπιστημίο Πειραιώς	Ψηφιακών συστημάτων	Αναπληρωτής Καθηγητής	Ασφάλεια δικτυακών συστημάτων	247/24.03.15 τ.Γ	Βάσει ΦΕΚ (άμεση)
17	Πολέμη	Δέσποινα	Πανεπιστημίο Πειραιώς	Πληροφορικής	Αναπληρωτής Καθηγητής	Ηλεκτρονικό επιχειρείν και συστήματα ασφάλειας πληροφοριών	1567/31.12.13 τ.Γ	Βάσει ΦΕΚ (άμεση)
18	Πουλάκης	Δημήτριος	Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης	Μαθηματικών	Καθηγητής Α' Βαθμίδας	Θεωρία αριθμών ή αλγεβρική γεωμετρία	221/11.09.00 τ.ΝΠΔΔ	Βάσει ΦΕΚ (άμεση)
19	Ράπτης	Ευάγγελος	Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών	Μαθηματικών	Καθηγητής Α' Βαθμίδας	Θεωρία ομάδων	958/06.10.10 τ.Γ	Βάσει ΦΕΚ (άμεση)
20	Ριζομυλιώτης	Παναγιώτης	Πανεπιστήμιο Αιγαίου	Μηχανικών πληροφοριακών και επικοινωνιακών συστημάτων	Επίκουρος Καθηγητής	Θεωρία πληροφορίας με εφαρμογές στην κρυπτογραφία	542/12.06.15 τ.Γ	Βάσει ΦΕΚ (άμεση)
21	Σκλάβος	Νικόλαος	Πανεπιστήμιο Πατρών	Μηχανικών ηλεκτρονικών υπολογιστών και πληροφορικής	Αναπληρωτής Καθηγητής	Ηλεκτρονική με έμφαση στον ψηφιακό σχεδιασμό	453/19.05.15 τ.Γ	Βάσει έργου (άμεση)
22	Σταματίου	Ιωάννης	Πανεπιστήμιο Πατρών	Διοίκησης επιχειρήσεων	Αναπληρωτής Καθηγητής	Ασφάλεια συναλλαγών στο ηλεκτρονικό επιχειρείν	1067/12.12.11 τ.Γ	Βάσει ΦΕΚ (άμεση)
23	Στεφανίδης	Γεώργιος	Πανεπιστήμιο Μακεδονίας	Εφαρμοσμένης πληροφορικής	Καθηγητής Α' Βαθμίδας	Εφαρμοσμένα μαθηματικά	416/22.06.11 τ.Γ	Βάσει έργου (άμεση)
24	Χρυσικόπουλος	Βασίλειος	Ιόνιο Πανεπιστήμιο	Πληροφορικής	Καθηγητής Α' Βαθμίδας	Πληροφορική - δίκτυα - ασφάλεια πληροφοριών	204/28.03.07 τ.Γ	Βάσει ΦΕΚ

								(άμεση)

Σημειώσεις:

1. Στην τελευταία στήλη (Συνάφεια) πρέπει να σημειώνεται εάν πρόκειται για συνάφεια βάσει ΦΕΚ (δηλαδή βάσει του γνωστικού αντικειμένου που αναγράφεται στο οικείο ΦΕΚ τελευταίου διορισμού) ή για συνάφεια βάσει έργου.

2. Στην τελευταία στήλη (Συνάφεια) μπορεί επιπλέον να σημειώνεται και μία ένδειξη ως προς το βαθμό συνάφειας (π.χ. άμεση ή έμμεση συνάφεια). Μπορεί όμως, κατά την κρίση του οικείου Τμήματος, να σημειώνονται και ενδείξεις για πιο αναλυτικές διαφοροποιήσεις ως προς τον βαθμό συνάφειας.

3. Για τη διευκόλυνση της αρχειοθέτησης, ο αριθμός του ΦΕΚ διορισμού πρέπει να αναγράφεται με μία από τις μορφές που σημειώνονται στις παραπάνω περιπτώσεις.

Ίδρυμα: Πανεπιστήμιο Πελοποννήσου
Τμήμα: Πληροφορικής και Τηλεπικοινωνιών
Γνωστικό αντικείμενο: Κρυπτογραφία, κρυπτανάλυση και εφαρμογές
Βαθμίδα: Επίκουρος Καθηγητής (μονιμοποίηση)

Μητρώο Εξωτερικών Μελών/Κριτών - Πανεπιστήμια Εξωτερικού

Α/Α	Επώνυμο	Όνομα	Ίδρυμα	Τμήμα	Βαθμίδα	Γνωστικό αντικείμενο	Χώρα	Συνάφεια
1	Burmester	Mike	Florida State University	Computer science	Professor	Computer science	Ηνωμένες Πολιτείες Αμερικής	Βάσει έργου (άμεση)
2	Δημητρίου	Αναστάσιος	Kuwait University	Computer engineering	Associate Professor	Computer and network security, sensor, ad-hoc and RFID networks, smart electricity grids, ubiquitous computing, analysis of algorithms	Κουβέιτ	Βάσει θέσης (άμεση)
3	Κάτος	Βασίλειος	Bournemouth University	Computing and informatics	Professor	Computing - information security, cyber security, digital forensics	Ηνωμένο Βασίλειο	Βάσει θέσης (άμεση)
4	Μαρκαντωνάκης	Κωνσταντίνος	Royal Holloway, University of London	Information security group	Associate Professor	Information security	Ηνωμένο Βασίλειο	Βάσει θέσης (άμεση)

5	Μουρατίδης	Χαράλαμπος	University of Brighton	Computing, engineering and mathematics	Professor	Software engineering, security engineering, information systems, requirements engineering, secure software systems engineering, multi-agent systems	Ηνωμένο Βασίλειο	Βάσει θέσης (άμεση)
6	Σπανουδάκης	Γεώργιος	City University London	Computer science	Professor	Software engineering, software systems security, cloud & service oriented computing	Ηνωμένο Βασίλειο	Βάσει θέσης (άμεση)
7	Τσαπτσίνος	Δημήτριος	Kingston University	Computer science and mathematics	Associate Professor	Computer science with interest in cyber security, digital forensics and learning & teaching	Ηνωμένο Βασίλειο	Βάσει θέσης (άμεση)

Σημειώσεις:

1. Στην τελευταία στήλη (Συνάφεια) πρέπει να σημειώνεται εάν πρόκειται για συνάφεια βάσει έργου ή βάσει θέσης στο Πανεπιστήμιο του εξωτερικού, αφού εδώ δεν υφίσταται η έννοια του ΦΕΚ διορισμού.

2. Στην τελευταία στήλη (Συνάφεια) μπορεί επιπλέον να σημειώνεται και μία ένδειξη ως προς το βαθμό συνάφειας (π.χ. άμεση ή έμμεση συνάφεια). Μπορεί όμως, κατά την κρίση του οικείου Τμήματος, να σημειώνονται και ενδείξεις για πιο αναλυτικές διαφοροποιήσεις ως προς τον βαθμό συνάφειας.

3. Στην έκτη στήλη (Βαθμίδα) θα πρέπει να αναγράφεται ο τίτλος της κατεχόμενης θέσης στην οικεία γλώσσα και στη συνέχεια να σημειώνεται σε παρένθεση στην ελληνική γλώσσα η ισοδυναμία της κατεχόμενης θέσης με θέση καθηγητή πρώτης βαθμίδας ή με θέση αναπληρωτή καθηγητή βάσει της ελληνικής νομοθεσίας.

Ο Πρύτανης

Καθηγητής Κωνσταντίνος Μασσέλος