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 7β/17.01.2017 Συνεδρίαση 99η

Θέμα: Συγκρότηση μητρώου εσωτερικών και εξωτερικών μελών για κρίση εκλογής ή/ και εξέλιξης σε θέση Καθηγητή πρώτης βαθμίδας 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 μητρώου εσωτερικών και εξωτερικών μελών για κρίση εκλογής ή/ και εξέλιξης στη βαθμίδα του Καθηγητή πρώτης βαθμίδας 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/ 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.

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

4405/2016 (Α΄129) και ισχύει.

Σύμφωνα με τα ανωτέρω, για την κατάρτιση του μητρώου επιλέχθηκαν μέλη ΔΕΠ βαθμίδας Καθηγητή πρώτης βαθμίδας ή Ερευνητές αντίστοιχης βαθμίδας, με ΦΕΚ διορισμού ή επιστημονικό έργο *στο ίδιο* γνωστικό αντικείμενο. Για τη συμπλήρωση ικανοποιητικού αριθμού μελών του μητρώου επιλέχθηκαν και μέλη ΔΕΠ βαθμίδας Καθηγητή, πρώτης βαθμίδας η Ερευνητές αντίστοιχης βαθμίδας, 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
  - » Complexity theory and logic
  - » **Cryptographic** primitives

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

» **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 πρώτης βαθμίδας 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

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 <u>άμεση συνάφεια</u> 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 <u>A. Maras</u>, "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.

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.

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.

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.

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.

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.

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.

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.

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

Μητρώο Εσωτερικών Μελών/Κριτών

Α/Α	Επώνυμο	Όνομα	Ίδρυμα	Τμήμα	Βαθμίδα	Γνωστικό αντικείμενο	ΦΕΚ διορισμού	Συνάφεια
1	Μαράς	Ανδρέας	Πανεπιστήμιο Πελοποννήσου	Πληροφορικής και τηλεπικοινωνιών	Καθηγητής Α' Βαθμίδας	Τηλεπικοινωνίες	207/09.12.99 τ.ΝΠΔΔ	Βάσει έργου (άμεση)

Σημειώσεις:

1. Στην τελευταία στήλη (Συνάφεια) πρέπει να σημειώνεται εάν πρόκειται για συνάφεια βάσει ΦΕΚ (δηλαδή βάσει του γνωστικού αντικειμένου που αναγράφετα 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 όμω 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 περιπτ

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

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	Γκρίτζαλης	Δημήτριος	Οικονομικό Πανεπιστήμιο Αθηνών	Πληροφορικής	Καθηγητής Α' Βαθμίδας	Ασφάλεια στην πληροφορική και τις επικοινωνίες	663/21.08.09 τ.ΝΠΔΔ	Βάσει ΦΕΚ (άμεση)
3	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)
4	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)
5	Κάτσικας	Σωκράτης	Πανεπιστημίο Πειραιώς	Ψηφιακών συστημάτων	Καθηγητής Α' Βαθμίδας	Πληροφορική	294/02.05.07 τ.Γ	Βάσει έργου (άμεση)
6	Πουλάκης	Δημήτριος	Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης	Μαθηματικών	Καθηγητής Α' Βαθμίδας	Θεωρία αριθμών ή αλγεβρική γεωμετρία	221/11.09.00 τ.ΝΠΔΔ	Βάσει ΦΕΚ (άμεση)
7	Ράπτης	Ευάγγελος	Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών	Μαθηματικών	Καθηγητής Α' Βαθμίδας	Θεωρία ομάδων	958/06.10.10 τ.Γ	Βάσει ΦΕΚ (άμεση)

8	Στεφανίδης	Γεώργιος	Πανεπιστήμιο Μακεδονίας	Εφαρμοσμένης πληροφορικής	Καθηγητής Α' Βαθμίδας	Εφαρμοσμένα μαθηματικά	416/22.06.11 τ.Γ	Βάσει έργου (άμεση)
9	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 οικ 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 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: Καθηγητής

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	Κάτος	Βασίλειος	Bournemouth University	Computing and informatics	Professor	Computing - information security, cyber security, digital forensics	Ηνωμένο Βασίλειο	Βάσει θέσης (άμεση)
3	Μουρατίδης	Χαράλαμπος	University of Brighton	Computing, engineering and mathematics	Professor	Software engineering, security engineering, information systems, requirements engineering, secure	Ηνωμένο Βασίλειο	Βάσει θέσης (άμεση)

						software systems engineering, multi-agent systems		
4	Σπανουδάκης	Γεώργιος	City University London	Computer science	Professor	Software engineering, software systems security, cloud & service oriented computing	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.

Ο Πρύτανης

Καθηγητής Κωνσταντίνος Μασσέλος