Νικόλαος Κολοκοτρώνης

Βιογραφικό σημείωμα

Παν. Πελοποννήσου
Τμ. Πληροφορικής και Τηλ/νιών
☎ *(+30) 2710 372231*
✉ *nkolok@uop.gr*
www.uop.gr/~nkolok

Ιούνιος 2022

Προσωπικά στοιχεία

Σπουδές

1998–2003 **Ph.D. στην Κρυπτογραφία**
Πανεπιστήμιο Αθηνών, Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Διατριβή: Μη–γραμμική επεξεργασία σήματος και εφαρμογές στην κρυπτογραφία

1996–1998 **M.Sc. στην Επιστήμη Υπολογιστών**
Πανεπιστήμιο Αθηνών, Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Κατεύθυνση: Αλγόριθμοι Υψηλής Απόδοσης
Βαθμολογία: 8,55/10
Διπλωματική: Συμπίεση, προοδευτική μετάδοση, και επιλεκτική αποσυμπίεση εικόνων με τη χρήση wavelets

1990–1995 **B.Sc. στα Μαθηματικά**
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Τμήμα Μαθηματικών
Κατεύθυνση: Εφαρμοσμένα Μαθηματικά
Βαθμολογία: 7,85/10

Διακρίσεις

1994 Υποτροφία από το Ίδρυμα Κρατικών Υποτροφιών (ΙΚΥ) για την αριστεία κατά τη διάρκεια του τρίτου ακαδημαϊκού έτους προπτυχιακών σπουδών

Επαγγελματικές θέσεις

Κύρια θέση

2019–παρόν **Αναπληρωτής καθηγητής**
Πανεπιστήμιο Πελοποννήσου, Τμήμα Πληροφορικής και Τηλεπικοινωνιών

2012–2019 **Επίκουρος καθηγητής**
Πανεπιστήμιο Πελοποννήσου, Τμήμα Πληροφορικής και Τηλεπικοινωνιών

2008–2012 **Λέκτορας**
Πανεπιστήμιο Πελοποννήσου, Τμήμα Πληροφορικής και Τηλεπικοινωνιών

2004–2008 **Επισκέπτης καθηγητής**
Πανεπιστήμιο Πελοποννήσου, Τμήμα Πληροφορικής και Τηλεπικοινωνιών

Λοιπές θέσεις

2005–παρόν **Επισκέπτης καθηγητής**
Πανεπιστήμιο Αθηνών, Τμήμα Πληροφορικής και Τηλεπικοινωνιών

2015–2017 **Συνεργαζόμενο εκπαιδευτικό προσωπικό**
Ανοικτό Πανεπιστήμιο Κύπρου, Σχολή Θετικών και Εφαρμοσμένων Επιστημών

2004–2006 **Επισκέπτης καθηγητής**
Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων

2002–2004 **Σύμβουλος τεχνολογιών πληροφορικής**
Ευρωπαϊκή Δυναμική ΑΕ, Διεύθυνση Ηλεκτρονικού Εμπορίου

2001–2002 **Μηχανικός λογισμικού**
Ένοπλες Δυνάμεις, Σώμα Έρευνας Πληροφορικής

1998–2001 **Επιστημονικός συνεργάτης**
Πανεπιστήμιο Αθηνών, Τμήμα Πληροφορικής και Τηλεπικοινωνιών

Ερευνητικά ενδιαφέροντα

- **Εφαρμοσμένη κρυπτογραφία:** κρυπτοσυστήματα τμήματος/ροής και γεννήτριες, σχεδιασμός s–box, στατιστική κρυπτανάλυση, λογικές συναρτήσεις, blockchain
- **Μοντέρνα κρυπτογραφία:** ασθενείς/ισχυρές ψευδοτυχαίες συναρτήσεις (PRFs), σημασιολογική ασφάλεια, κρυπτογραφικές εφαρμογές στατιστικής μάθησης (LPN, LWE, κ.λπ.), παιγνιο–θεωρητική κρυπτογραφία
- **Μετακβαντική κρυπτογραφία:** κρυπτοσυστήματα κωδίκων, επιθέσεις αποκωδικοποίησης (ISD), κρυπτοσυστήματα πλεγμάτων, κβαντικοί αλγόριθμοι
- **Τεχνολογίες ιδιωτικότητας:** μέθοδοι διασφάλισης ιδιωτικότητας, πρωτόκολλα/συστήματα ανωνυμίας, ομομορφική κρυπτογραφία, ασφάλεια στατιστικών ΒΔ
- **Κυβερνο–ασφάλεια:** ασφάλεια στο IoT, πρωτόκολλα ασφάλειας δικτύων, ασφάλεια ασύρματων δικτύων, ασφάλεια σε M2M επικοινωνίες
- **Ασφάλεια επιπέδου PHY:** πληροφοριο–θεωρητική ασφάλεια, παιγνιο–θεωρητική ασφάλεια, συνεργατικά πρωτόκολλα (DF, AF, CJ), σχήματα επιλογής συνεργατών
- **Διαχείριση εμπιστοσύνης:** μοντέλα εμπιστοσύνης, διαχείριση υπόληψης, θεωρία παιγνίων και εμπιστοσύνη, πληροφοριο–θεωρητικές έννοιες εμπιστοσύνης
- **Θεωρία κωδίκων:** τυχαίοι κώδικες, πιθανοτική αποκωδικοποίηση (λίστας), κώδικες για το κανάλι ωτακουστή, κοινή κωδικοποίηση και κρυπτογράφηση

Διδακτική εμπειρία

Μεταπτυχιακά

2018–παρόν	Ασφάλεια, ιδιωτικότητα, και εμπιστοσύνη μεγάλων δεδομένων (συνδιδασκαλία)	*Παν. Πελ/νήσου*
2018–παρόν	Θέματα κρυπτογραφίας και ασφάλειας	*Παν. Πελ/νήσου*
2005–παρόν	Ασφάλεια συστημάτων (συνδιδασκαλία)	*Παν. Αθηνών*
2015–2017	Ασφάλεια υπολογιστών και δικτύων: προηγμένα θέματα (συνδιδασκαλία)	*Παν. Κύπρου*
2013–2015	Θέματα σχεδιασμού κρυπτογραφικών αλγορίθμων	*Παν. Πελ/νήσου*
2013–2015	Θέματα ασφάλειας επικοινωνιών	*Παν. Πελ/νήσου*
2009–2011	Κρυπτογραφία και εφαρμογές	*Παν. Πελ/νήσου*
2009–2011	Θεωρία πληροφορίας και κωδίκων	*Παν. Πελ/νήσου*
2005	Ασφάλεια δικτυοκεντρικών συστημάτων	*Παν. Πειραιώς*
1998–2000	Θεωρία πληροφορίας και κωδίκων (συνδιδασκαλία)	*Παν. Αθηνών*

Προπτυχιακά

2017–παρόν	Διακριτά μαθηματικά	*Παν. Πελ/νήσου*

2004–παρόν	Κρυπτογραφία	*Παν. Πελ/νήσου*
2004–παρόν	Ασφάλεια συστημάτων	*Παν. Πελ/νήσου*
2013–2016	Πιθανότητες και στατιστική (συνδιδασκαλία)	*Παν. Πελ/νήσου*
2015	Μαθηματικά ΙΙ (συνδιδασκαλία)	*Παν. Πελ/νήσου*
2012–2013	Γραμμική άλγεβρα και θεωρία αριθμών (συνδιδασκαλία)	*Παν. Πελ/νήσου*
2009–2013	Θεωρία πληροφορίας και κωδίκων	*Παν. Πελ/νήσου*
2007–2008	Εισαγωγή στον προγραμματισμό	*Παν. Πελ/νήσου*
2006	Προηγμένη κρυπτογραφία	*Παν. Πελ/νήσου*
2005	Θεωρία αριθμών	*Παν. Πελ/νήσου*
2004–2005	Ασφάλεια πληροφοριών	*Παν. Πειραιώς*
2004	Σήματα και συστήματα	*Παν. Πειραιώς*
1998–2000	Ψηφιακή επεξεργασία σήματος (συνδιδασκαλία)	*Παν. Αθηνών*

Επίβλεψη φοιτητών

Διδακτορικοί

Επιβλέπων

2018	Σ. Μπρότσης, Ασφάλεια πρωτοκόλλων συναίνεσης και τεχνολογιών κατανεμημένων μητρώων	*σε εξέλιξη*
2018	Γ. Γέρμανος, Κυβερνο–ασφάλεια και ιδιωτικότητα στο διαδίκτυο των πραγμάτων	*σε εξέλιξη*
2015	Π. Σμυρλή, Μετακβαντική κρυπτογραφία: συστήματα βασισμένα σε κώδικες	*σε εξέλιξη*

Μέλος συμβουλευτικής επιτροπής

2017	Ε.-Μ. Αθανασάκος, Ασφάλεια στο φυσικό επίπεδο	*σε εξέλιξη*
2016	Κ. Κατσάνος, Σιγμοειδής προγραμματισμός και εφαρμογές στην επεξεργασία σήματος και τις επικοινωνίες	*σε εξέλιξη*

Συνεπιβλέπων

2013	Κ. Ντέμος, Στοχαστικά παίγνια, γνωστικά δίκτυα, και ασφάλεια	*σε εξέλιξη*
2007	Κ. Λιμνιώτης, Κρυπτογραφικά μέτρα πολυπλοκότητας για δυαδικές ακολουθίες	*ολοκληρώθηκε*

Μεταπτυχιακοί

2018	Β. Χάσκος, Συστήματα κυβερνο–ασκήσεων: επισκόπηση και ανοιχτές προκλήσεις	*σε εξέλιξη*
2016	Ι. Λύτσιου, Κρυπτονομίσματα: μοντέλα, ασφάλεια, και εφαρμογές	*ολοκληρώθηκε*
2016	Ι. Γαλανός, Κοινωνικά δίκτυα & προστασία προσωπικών δεδομένων	*ολοκληρώθηκε*
2015	Χ. Καρζής, Φορμαλιστικά μοντέλα ασφάλειας σε συμμετρικά κρυπτοσυστήματα	*ολοκληρώθηκε*
2015	Σ. Μπρότσης, Δύσκολα προβλήματα με εφαρμογές στη σχεδίαση ασύμμετρων κρυπτοσυστημάτων	*ολοκληρώθηκε*
2015	Ι. Χριστάκης, Επιθέσεις ενδιάμεσου στα πρωτόκολλα ασφάλειας διαδικτύου SSL/TLS	*ολοκληρώθηκε*
2014	Μ. Αθανασάκος, Ασφάλεια ασύρματων επικοινωνιών σε φυσικό επίπεδο έναντι παθητικών επιθέσεων	*ολοκληρώθηκε*
2014	Π. Σμυρλή, Κρυπτοσυστήματα βασισμένα σε κώδικες: κατασκευές	*ολοκληρώθηκε*

και επιθέσεις

2014 Ν. Χαρίτος, Ασφάλεια στο διαδίκτυο των πραγμάτων (IoT) *ολοκληρώθηκε*

2013 Η. Φάκλαρης, Ασφάλεια έξυπνου πλέγματος *ολοκληρώθηκε*

2013 Θ. Μουράτης, Ασφαλείς υπηρεσίες ηλεκτρονικού ταχυδρομείου σε περιβάλλον iOS *ολοκληρώθηκε*

2012 Ζ. Δερμάτης, Ασφαλής δρομολόγηση σε ασύρματα κινητά δίκτυα *ολοκληρώθηκε*

2012 Μ. Ντρούλια, Ασφάλεια δικτύων γνωστικών επικοινωνιών *ολοκληρώθηκε*

2011 Α. Σχίζας, Κρυπταναλυτικές επιθέσεις στον αλγόριθμο RSA *ολοκληρώθηκε*

2010 Ε. Μπόζης, Ανάλυση της ασφάλειας και θέματα υλοποίησης σε πρωτοκόλλα αυθεντικοποίησης *ολοκληρώθηκε*

Προπτυχιακοί

2018 Κ.-Π. Γραμματικάκης, Εντοπισμός και ανάλυση κακόβουλου λογισμικού *σε εξέλιξη*

2018 Χ. Δούκας και Κ. Μελανίτης, Θέματα κρυπτογραφίας και ασφάλειας στο web *σε εξέλιξη*

2016 Δ. Μεντεσίδης, Ασύρματες τεχνολογίες επικοινωνιών για τη δημόσια ασφάλεια *ολοκληρώθηκε*

2015 Γ. Παναγόπουλος, Μοντέλα διαχείρισης εμπιστοσύνης σε P2P δίκτυα *ολοκληρώθηκε*

2015 Γ. Γεραμάνης, Επιθέσεις σε υπηρεσίες και πρωτόκολλα ανωνυμίας *ολοκληρώθηκε*

2014 Σ. Μάγκλαρης, Επιθέσεις τύπου poodle στα πρωτόκολλα ασφάλειας SSL/TLS *ολοκληρώθηκε*

2011 Β. Βλαχογιάννη, Θέματα ασφάλειας/πιστοποίησης RFID ετικετών *ολοκληρώθηκε*

2010 Γ. Γκόγκολης, Ανάλυση και υλοποίηση του μοντέλου ασφάλειας RBAC (συνεπίβλεψη) *ολοκληρώθηκε*

2009 Κ. Ψαράκης, Υπηρεσίες και ασφάλεια σε συστήματα η–τραπεζικής *ολοκληρώθηκε*

2008 Μ. Γρημάνη, Ανάλυση των κρυπτογραφικών χαρακτηριστικών σύγχρονων κρυπτοσυστημάτων ροής *ολοκληρώθηκε*

2007 Η. Αγγελής, Ανάλυση της προσφερόμενης ασφάλειας από τη νέα έκδοση του πρωτοκόλλου IPsec *ολοκληρώθηκε*

2006 Μ. Ανθή και Ε. Κασιμάτη, Turbo κώδικες και συμπλέκτες βασισμένοι σε πολυώνυμα μετάθεσης (συνεπίβλεψη) *ολοκληρώθηκε*

2005 Δ.-Ρ. Κουκουτσάκη και Δ.-Ε. Ρέγκλη, Επισκόπηση σύγχρονων κρυπτογραφικών και κρυπταναλυτικών τεχνικών (συνεπίβλεψη) *ολοκληρώθηκε*

Επιτροπές, ομάδες εργασίας

Θέσεις διοίκησης

2018–παρόν Επικεφαλής της ομάδας *κρυπτογραφίας και ασφάλειας* *Τμήμα ΠΤ*

2018–παρόν Μέλος της Ειδικής Διιδρυματικής Επιτροπής του προγράμματος μεταπτυχιακών σπουδών στην *Επιστήμη Δεδομένων* *Τμήμα ΠΤ*

2018–παρόν Μέλος της Συντονιστικής Επιτροπής του προγράμματος μεταπτυχιακών σπουδών στην *Επιστήμη Υπολογιστών* *Τμήμα ΠΤ*

2008–παρόν Μέλος της Συνέλευσης του τμήματος *Τμήμα ΠΤ*

2018 Μέλος της συντονιστικής επιτροπής προετοιμασίας της πρότασης για την πιστοποίηση του προγράμματος προπτυχιακών σπουδών *Τμήμα ΠΤ*

2008–2017 Μέλος της ομάδας *αλγορίθμων, κρυπτογραφίας και υπολογιστικής* *Τμήμα ΠΤ*

λογικής

2011–2017 Μέλος επιτροπών αξιολόγησης για την προμήθεια αγαθών — *Παν. Πελ/νήσου*

2015–2016 Μέλος της επιτροπής προγράμματος προπτυχιακών σπουδών — *Τμήμα ΠΤ*

2010–2016 Τμηματικός υπεύθυνος του έργου "πρακτική άσκηση ανώτατης εκπαίδευσης στο Πανεπιστήμιο Πελοποννήσου" του ΕΣΠΑ — *Παν. Πελ/νήσου*

2009–2016 Μέλος των ομάδων ανάπτυξης και συντήρησης του ιστοχώρου `dit.uop.gr` — *Τμήμα ΠΤ*

2013–2015 Μέλος της ομάδας έργου "ανάπτυξη πληροφοριακού συστήματος της ΜΟΔΙΠ στο Πανεπιστήμιο Πελοποννήσου" του ΕΣΠΑ — *Παν. Πελ/νήσου*

2012–2013 Μέλος της επιτροπής προγράμματος προπτυχιακών σπουδών — *Τμήμα ΠΤ*

Επιτροπές αξιολόγησης

2005–2007 Μέλος έκτακτων επιτροπών αξιολόγησης τεχνικών προσφορών της Γενικής Γραμματείας Εμπορίου (ΓΓΕ) του Υπουργείου Ανάπτυξης

2004–2005 Τακτικός αξιολογητής ερευνητικών έργων και προγραμμάτων–πλαισίων υποβολής προτάσεων της Γενικής Γραμματείας Έρευνας και Τεχνολογίας (ΓΓΕΤ)

Ομάδες εμπειρογνωμόνων

2017 Μέλος ομάδας εργασίας για την επαγγελματική κατάρτιση υπευθύνων ασφάλειας σε ειδικά θέματα του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) EU 2016/679

2000–2002 Μέλος ομάδων εργασίας για την επαγγελματική κατάρτιση στελεχών της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) πάνω σε θέματα ασφάλειας Τηλεπικοινωνιακών δικτύων

Λοιπές συμμετοχές

1998–παρόν Μέλος της IEEE (computer και IT societies)

Ακαδημαϊκές δραστηριότητες

Συντάκτης
- **AE:** EURASIP J. Wireless Commun. Netw. — *2009–2017*

Κριτής
- Adv. Math. Commun.
- Appl. Algebra Engrg. Comm. Comput.
- Benchmarking Int. J.
- Comput. Standards Interfaces
- Cryptogr. Commun.
- Des. Codes Cryptogr.
- Discrete Appl. Math.
- Discrete Math.
- EURASIP J. Wireless Commun. Netw.
- Finite Fields Appl.
- IEEE Commun. Lett.
- IEEE Consum. Electron. Mag.
- IEEE Trans. Commun.
- IEEE Trans. Ind. Informat.
- IEEE Trans. Inf. Forensics & Security
- IEEE Trans. Inf. Theory
- IEEE Trans. Multimedia
- IEEE Trans. Vehicular Tech.
- Inform. Comput. Security
- Inform. Process. Lett.
- Int. J. Commun. Syst.
- Int. J. Comput. Math.
- Int. J. Electron. Governance
- J. Appl. Math. Comput.
- J. Complexity
- J. Comput. Sci. Tech.
- J. Signal Image Video Process.
- Security Commun. Netw.
- Signal Process.

Μέλος TPC	○ E–DEM (Conf. e–Democracy Security Priv. Trust)	*2013, 2015, 2017*
	○ DSP (Int. Conf. Digit. Signal Process.)	*2009, 2011*
	○ EUSIPCO (Eur. Signal Process. Conf.)	*1998, 2008*
	○ ICASSP (Int. Conf. Acoust. Speech Signal Process.)	*2012*
	○ ICCS (Int. Conf. Comput. Sci.)	*2006–2007*
	○ IEEE GLOBECOM (Commun. Inf. Security Symp.)	*2009*
	○ IEEE ICC (Int. Conf. Commun.)	*2011*
	○ IEEE ISCAS (Int. Symp. Circuits Syst.)	*2003*
	○ IEEE ISIT (Int. Symp. Inf. Theory)	*2003, 2011, 2013, 2015*
	○ IEEE MELECON (Mediterranean Electrotech. Conf.)	*2016*
	○ IEEE WDFIA (Wkshp Digit. Forensics Incident Anal.)	*2007–2010*
	○ ISC (Int. Conf. Inf. Security)	*2017*
	○ ISPEC (Inform. Security Pract. Experience Conf.)	*2014*
	○ MCIS (Mediterranean Conf. Inf. Syst.)	*2009*
	○ PARA (Wkshp SoA Sci. Parallel Comput.)	*2006*
	○ PCI (Panhellenic Conf. Inform.)	*2010*
	○ STM (Int. Wkshp Security Trust Manag.)	*2018*
Δημοσιότητα	○ STM (Int. Wkshp Security Trust Manag.)	*2018*

Έργα, χορηγίες

Χορηγίες

2006–2008 Μελέτη της πολυπλοκότητας και ψευδοτυχαιότητας των συμμετρικών αλγορίθμων κρυπτογράφησης

Συντονιστής: Πανεπιστήμιο Αθηνών *Κωδικός:* 70/3/8470
Χρηματοδότηση: Βρετανικό Συμβούλιο *Προϋπολογισμός:* 16,0 K€
Αρμοδιότητες: Κύριος ερευνητής

2005 Μελέτη κρυπταλγορίθμων ροής στη συμμετρική κρυπτογραφία

Συντονιστής: Πανεπιστήμιο Αθηνών *Κωδικός:* 70/4/7818
Χρηματοδότηση: Πανεπιστήμιο Αθηνών *Προϋπολογισμός:* 4,5 K€
Αρμοδιότητες: Κύριος ερευνητής

Ερευνητικά έργα

2019–2022 FORESIGHT: Προηγμένη πλατφόρμα προσομοίωσης κυβερνο–ασφάλειας για την εκπαίδευση ετοιμότητας σε αεροπλοΐα, δικτύα ηλεκτρικής ενέργειας και ναυσιπλοΐα

Συντονιστής: Ευρωπαϊκή Δυναμική ΑΕ *Κωδικός:* 833673 (SU-DS01-2018)
Χρηματοδότηση: Ευρωπαϊκή Επιτροπή, H2020 *Προϋπολογισμός:* 6,0 M€
Αρμοδιότητες: Επικεφαλής ομάδας έργου, υπεύθυνος ενότητας εργασίας, τεχνικός συντονιστής του έργου — μεταξύ των βασικών υπευθύνων προετοιμασίας/σύνταξης της πρότασης

2018–2021 CYBER-TRUST: προηγμένη πλατφόρμα πληροφοριών, ανίχνευσης και αντιμετώπισης κυβερνο–απειλών για ένα αξιόπιστο Διαδίκτυο των πραγμάτων
Συντονιστής: Κέντρο Μελετών Ασφάλειας *Κωδικός:* 786698 (DS-07-2017)
Χρηματοδότηση: Ευρωπαϊκή Επιτροπή, H2020 *Προϋπολογισμός:* 3,0 M€
Αρμοδιότητες: Επικεφαλής ομάδας έργου, υπεύθυνος ενότητας εργασίας, τεχνικός συντονιστής του έργου — επίσης υπεύθυνος για την προετοιμασία/σύνταξη της πρότασης και των βασικών ιδεών καινοτομίας **(κατετάγη 1η μεταξύ 63 προτάσεων με βαθμολογία 15/15)**

2013–2016 HANDICAMS: ετερογενή ad–hoc δίκτυα για κατανεμημένη, συνεργατική και προσαρμοστική πολυμεσική επεξεργασία σήματος
Συντονιστής: Katholieke Univ. Leuven *Κωδικός:* FET–323944
Χρηματοδότηση: Ευρωπαϊκή Επιτροπή, FP7 *Προϋπολογισμός:* 2,0 M€
Αρμοδιότητες: Μέλος ομάδας έργου, υπεύθυνος ενότητας εργασίας

2012–2015 ART–IN–SPACE: προσαρμοστικές, εύρωστες σε απειλές, άνοσες σε μη–γραμμικότητες, αραιές ευκαιριακές γνωστικές επικοινωνίες
Συντονιστής: Πανεπιστήμιο Αθηνών *Κωδικός:* 70/3/11918
Χρηματοδότηση: ΕΣΠΑ Πρόγραμμα Αριστεία *Προϋπολογισμός:* 157,5 K€
Αρμοδιότητες: Μέλος ομάδας έργου, υπεύθυνος ενότητας εργασίας

2012–2015 SWINCOM: ασφαλείς ασύρματες μη–γραμμικές επικοινωνίες στο φυσικό επίπεδο
Συντονιστής: Πανεπιστήμιο Αθηνών *Κωδικός:* 70/3/11668
Χρηματοδότηση: ΕΣΠΑ Πρόγραμμα Θαλής *Προϋπολογισμός:* 512,8 K€
Αρμοδιότητες: Επικεφαλής ομάδας έργου, υπεύθυνος ενότητας εργασίας — επίσης υπεύθυνος για την προετοιμασία και σύνταξη της πρότασης

2004–2007 ECON–TISP: εφαρμογή οικονομικών θεωριών στο σχεδιασμό και ανάπτυξη τηλεπικοινωνιακών και πληροφοριακών συστημάτων και προϊόντων
Συντονιστής: Πανεπιστήμιο Αθηνών *Κωδικός:* 56/90/7425
Χρηματοδότηση: Γ' Κοιν. Πλαίσιο Στήριξης *Προϋπολογισμός:* 90,0 K€
Αρμοδιότητες: Κύριος ερευνητής

2004–2007 SECURE–JUSTICE: ασφαλές πλαίσιο επικοινωνίας και συνεργασίας για το δικαστικό συνεργατικό περιβάλλον
Συντονιστής: Project Automation SpA *Κωδικός:* IST-2002-507188
Χρηματοδότηση: Ευρωπαϊκή Επιτροπή, FP6 *Προϋπολογισμός:* 5,4 M€
Αρμοδιότητες: Συντονιστής ομάδας έργου

2002–2005 DIASTASIS: στατιστικοί δείκτες ψηφιακής εποχής — ορισμός, μέτρηση και εκμετάλλευση νέων κοινωνικο-οικονομικών δεικτών συσχετίζοντας στατιστικά δεδομένα χρήσης web και οικιακή έρευνα
Συντονιστής: Ευρωπαϊκή Δυναμική ΑΕ *Κωδικός:* IST-2000-31083
Χρηματοδότηση: Ευρωπαϊκή Επιτροπή, FP5 *Προϋπολογισμός:* 2,0 M€
Αρμοδιότητες: Συντονιστής του έργου

2002–2005 ICTE–PAN: μεθοδολογίες και εργαλεία για την ανάπτυξη ευφυών συνεργατικών περιβαλλόντων εργασίας σε δίκτυα δημόσιας διοίκησης
Συντονιστής: Ευρωπαϊκή Δυναμική ΑΕ *Κωδικός:* IST-2001-35120
Χρηματοδότηση: Ευρωπαϊκή Επιτροπή, FP5 *Προϋπολογισμός:* 3,2 M€
Αρμοδιότητες: Μέλος ομάδας έργου

2000–2001 CHANNEL SOUNDER: ανάπτυξη ευφυούς μετρητικής διάταξης για τον πολυδιάστατο χαρακτηρισμό ραδιοδιαύλων ευρείας ζώνης
Συντονιστής: Εθ. Μετσόβιο Πολυτεχνείο *Κωδικός:* 61/1189
Χρηματοδότηση: Γενική Γραμματεία Ε& Τ *Προϋπολογισμός:* 176,1 K€
Αρμοδιότητες: Μέλος ομάδας έργου

1999–2001 BILLING MALL: ανάπτυξη ολοκληρωμένου διαδικτυακού περιβάλλοντος η–εμπορίου για την ασφαλή διαχείριση λογαριασμών στις συνδρομητικές υπηρεσίες
Συντονιστής: Πανεπιστήμιο Αθηνών *Κωδικός:* 70/3/4483
Χρηματοδότηση: Γενική Γραμματεία Ε& Τ *Προϋπολογισμός:* 1,1 M€
Αρμοδιότητες: Μέλος ομάδας έργου

1996–1998 EUROMED: τεχνολογίες για την ίδρυση μιας ευρωπαϊκής τηλεϊατρικής κοινωνίας της πληροφορίας
Συντονιστής: Εθ. Μετσόβιο Πολυτεχνείο *Κωδικός:* 70/3/2723
Χρηματοδότηση: Ευρωπαϊκή Επιτροπή, TEDIS *Προϋπολογισμός:* 1,6 M€
Αρμοδιότητες: Μέλος ομάδας έργου

Συμβουλευτικά έργα

2007 Σχέδιο τεχνικών δράσεων και προσδιορισμός πρόσθετων τεχνικών υποδομών για τη λειτουργία του Γενικού Εμπορικού Μητρώου (ΓΕΜΗ)
Συντονιστής: Πανεπιστήμιο Αθηνών *Κωδικός:* 70/3/9291
Χρηματοδότηση: Γενική Γραμμ. Εμπορίου *Προϋπολογισμός:* –
Αρμοδιότητες: Μέλος ομάδας έργου

2000 Συμβουλευτικές υπηρεσίες υποστήριξης εισόδου της ΔΕΗ στην τηλεπικοινωνιακή αγορά
Συντονιστής: Πανεπιστήμιο Αθηνών *Κωδικός:* 70/3/5328
Χρηματοδότηση: Δημ. Επιχ. Ηλεκτρισμού *Προϋπολογισμός:* –
Αρμοδιότητες: Μέλος ομάδας έργου

2000 Δημόσια διαβούλευση και τεύχη προκήρυξης αδειών για την ανάπτυξη δικτύου και παροχή υπηρεσιών κινητής τηλεφωνίας, σταθερής ασύρματης πρόσβασης, και DECT
Συντονιστής: Πανεπιστήμιο Αθηνών *Κωδικός:* 70/3/5255
Χρηματοδότηση: Εθ. Επιτροπή Τηλ/νιών Ταχ. *Προϋπολογισμός:* –
Αρμοδιότητες: Μέλος ομάδας έργου

1999 Διαμόρφωση πολιτικών ασφάλειας στις τηλεπικοινωνίες
Συντονιστής: Πανεπιστήμιο Αθηνών *Κωδικός:* 70/3/4706
Χρηματοδότηση: Υπ. Μεταφ. Επικοινωνιών *Προϋπολογισμός:* –
Αρμοδιότητες: Μέλος ομάδας έργου

Ερευνητικές δραστηριότητες

Προσκεκλημένες ομιλίες

- Cryptographic Boolean functions with maximum algebraic immunity. *2016 International Conference on Cryptography, Cyber–Security, and Information Warfare*, May 2016, Athens, Greece
- On the computation of best second–order approximations of boolean functions. *2014 International Conference on Cryptography, Network Security and Applications in Armed Forces*, Apr. 2014, Athens, Greece
- Code–based public–key cryptosystems: constructions and attacks. *2014 Athens Cryptography Day (ATHECRYPT)*, Jan. 2014, Athens, Greece
- Cryptanalytic attacks and related criteria for stream and block ciphers. *2011 Intensive Program on Information Communication Security (IPICS)*, Aug. 2011, Corfu, Greece
- Towards computing best quadratic approximations. *Information Security Group, Royal Holloway University of London*, Dec. 2006, Surrey, U.K.
- E–commerce security. *National Committee of Telecommunications and Posts*, Nov. 2002, Athens, Greece

- Analysis and design of symmetric cryptographic algorithms. *2001 National Conference on Cyberspace Security and Hacking*, Oct. 2001, Athens, Greece
- Telecommunications security. *National Committee of Telecommunications and Posts*, Apr. 2000, Athens, Greece

Σχολεία, σεμινάρια

- Topics in cryptographic design and cryptanalysis. *ECRYPT Summer School*, May 2007, Samos, Greece

Δημοσιεύσεις

Βιβλία, μονογραφίες, επιμέλεια συλλογικών τόμων

[1] G. Sargsyan, D. Kavallieros, and N. Kolokotronis, *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation*. Now Publishers, March 2022. [online]

[2] S. Shiaeles and N. Kolokotronis, *Internet of Things, Threats, Landscape, and Countermeasures*. CRC Press, April 2021. [online]

[3] N. Kolokotronis and S. Shiaeles, *Cyber-Security Threats, Actors, and Dynamic Mitigation*. CRC Press, April 2021. [online]

[4] P. Kanellis, E. Kiountouzis, N. Kolokotronis, and D. Martakos, *Digital crime and forensic science in cyberspace*. IGI Global Publishing, April 2006. [online]

[5] N. Kolokotronis, "Nonlinear signal processing and applications to cryptography," Ph.D Thesis, Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, December 2003. [online]

Κεφάλαια σε βιβλία και συλλογικούς τόμους

[6] C.-M. Mathas, C. Vassilakis, N. Kolokotronis, and K. P. Grammatikakis, "Trust management system architecture for the Internet of things," in *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation*, G. Sargsyan, D. Kavallieros, and N. Kolokotronis, Eds. Now Publishers, March 2022, pp. 130–160. [online]

[7] S. Brotsis, N. Kolokotronis, and K. Limniotis, "Towards post-quantum blockchain platforms," in *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation*, G. Sargsyan, D. Kavallieros, and N. Kolokotronis, Eds. Now Publishers, March 2022, pp. 105–130. [online]

[8] K. P. Grammatikakis, I. Koufos, and N. Kolokotronis, "Moving-target defense techniques for mitigating sophisticated IoT threats," in *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation*, G. Sargsyan, D. Kavallieros, and N. Kolokotronis, Eds. Now Publishers, March 2022, pp. 51–73. [online]

[9] K. P. Grammatikakis and N. Kolokotronis, "Attack graph generation," in *Cyber-Security Threats, Actors, and Dynamic Mitigation*, N. Kolokotronis and S. Shiaeles, Eds. CRC Press, April 2021, pp. 281–334. [online]

[10] I. Koufos, N. Kolokotronis, and K. Limniotis, "Dynamic risk management," in *Cyber-Security Threats, Actors, and Dynamic Mitigation*, N. Kolokotronis and S. Shiaeles, Eds. CRC Press, April 2021, pp. 247–280. [online]

[11] K. Limniotis and N. Kolokotronis, "Cryptography threats," in *Cyber-Security Threats, Actors, and Dynamic Mitigation*, N. Kolokotronis and S. Shiaeles, Eds. CRC Press, April 2021, pp. 123–158. [online]

[12] K. P. Grammatikakis and N. Kolokotronis, "System threats," in *Cyber-Security Threats, Actors, and Dynamic Mitigation*, N. Kolokotronis and S. Shiaeles, Eds. CRC Press, April 2021, pp. 81–122. [online]

[13] D. Kavallieros, G. Germanos, and N. Kolokotronis, "Profiles of cyber-attackers and attacks," in *Cyber-Security Threats, Actors, and Dynamic Mitigation*, N. Kolokotronis and S. Shiaeles, Eds. CRC Press, April 2021, pp. 1–26. [online]

[14] A. Grigoriadis, E. Darra, D. Kavallieros, E. Chaskos, N. Kolokotronis, and X. Bellekens, "Cyber ranges: The new training era in the cybersecurity and digital forensics world," in *Technology Development for Security Practitioners*, Security Informatics and Law Enforcement, B. Akhgar, D. Kavallieros, and E. Sdongos, Eds. Springer, 2021, pp. 97–117. [online]

[15] V. G. Bilali, D. Kavallieros, G. Kokkinis, P. Kolovos, D. Katsoulis, T. Anatolitis, N. Georgiou, N. Kolokotronis, O. Gkotsopoulou, C. Pavue, S. Cuomo, S. Naldini, S. Shiaeles, and G. Sargsyan, "Cyber-Trust: Meeting the needs of information sharing between ISPs and LEAs," in *Technology Development for Security Practitioners*, Security Informatics and Law Enforcement, B. Akhgar, D. Kavallieros, and E. Sdongos, Eds. Springer, 2021, pp. 73–95. [online]

[16] N. Kolokotronis, K. Limniotis, and P. Rizomiliotis, "Applied cryptography," in *Information and Systems Security in Cyber-Space*, S. K. Katsikas, S. Gritzalis, and C. Lambrinoudakis, Eds. NewTech Publications, 2021, pp. 235–282. [online]

[17] N. Kolokotronis, S. Shiaeles, E. Bellini, L. Charalambous, D. Kavallieros, O. Gkotsopoulou, C. Pavue, A. Bellini, and G. Sargsyan, "Cyber-Trust: The shield for IoT cyber-attacks," in *Resilience and Hybrid Threats*, NATO Science for Peace and Security Series – D: Information and Communication Security, I. Linkov, L. Roslycky, and B. D. Trump, Eds. IOS Press, 2019, vol. 55, pp. 76–93, Research Article. [online]

[18] K. Limniotis, N. Kolokotronis, and D. Kotanidis, "De Bruijn sequences and suffix arrays: analysis and constructions," in *Modern Discrete Mathematics and Analysis: With Applications in Cryptography, Information Systems, and Modelling*, N. J. Daras and T. M. Rassias, Eds. Springer, 2018, pp. 257–276. [online]

[19] N. Kolokotronis and C. D. Koutras, "Zero knowledge proofs and applications," in *Modern Cryptography: Theory and Applications*, M. Burmester, S. Gritzalis, S. K. Katsikas, and V. Chrissikopoulos, Eds. Papasotiriou Pubs, 2011, pp. 635–646. [online]

[20] N. Kolokotronis, "Stream ciphers," in *Modern Cryptography: Theory and Applications*, M. Burmester, S. Gritzalis, S. K. Katsikas, and V. Chrissikopoulos, Eds. Papasotiriou Pubs, 2011, pp. 299–354. [online]

[21] N. Kolokotronis and K. Limniotis, "Algorithmic algebra," in *Modern Cryptography: Theory and Applications*, M. Burmester, S. Gritzalis, S. K. Katsikas, and V. Chrissikopoulos, Eds. Papasotiriou Pubs, 2011, pp. 47–87. [online]

[22] N. Kolokotronis and C. D. Koutras, "Anonymity measures and privacy preservation techniques," in *Protecting Privacy in Information and Communication Technologies:*

Technical and Legal Issues, C. Lambrinoudakis, L. Mitrou, S. Gritzalis, and S. K. Katsikas, Eds. Papasotiriou Pubs, 2010, pp. 123–145. [online]

[23] E. Kofidis, N. Kolokotronis, A. Vassilarakou, S. Theodoridis, and D. Cavouras, "Medical image compression," in *Advanced Infrastructures for Future Healthcare*, Studies in Health Technology and Informatics, A. Marsh, L. Grandinetti, and T. Kauranne, Eds. IOS Press, 2000, vol. 79, pp. 369–406. [online]

Περιοδικά

[24] S. Monogios, K. Magos, K. Limniotis, N. Kolokotronis, and S. Shiaeles, "Privacy issues in Android applications: The cases of GPS navigators and fitness trackers," *International Journal of Electronic Governance*, vol. 14, no. 1/2, pp. 83–111, May 2022. [online]

[25] C.-M. Mathas, C. Vassilakis, N. Kolokotronis, C. C. Zarakovitis, and M.-A. Kourtis, "On the design of iot security: Analysis of software vulnerabilities for smart grids," *Energies*, vol. 14, no. 10, May 2021. [online]

[26] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, "On the suitability of blockchain platforms for iot applications: Architectures, security, privacy, and performance," *Computer Networks*, vol. 191, p. 108005, May 2021. [online]

[27] N. Dalezios, S. Shiaeles, N. Kolokotronis, and B. Ghita, "Digital forensics cloud log unification: Implementing CADF in Apache CloudStack," *Journal of Information Security and Applications*, vol. 54, pp. 1–9, October 2020. [online]

[28] K. Fytrakis, N. Kolokotronis, K. Katsanos, and N. Kalouptsidis, "Optimal cooperative strategies for PHY security maximization subject to SNR constraints," *IEEE Access*, vol. 8, pp. 119312–119323, July 2020. [online]

[29] A. Ramsdale, S. Shiaeles, and N. Kolokotronis, "A comparative analysis of cyber-threat intelligence sources, formats and languages," *Electronics*, vol. 9, no. 5, pp. 1–22, May 2020. [online]

[30] K. Limniotis and N. Kolokotronis, "The error linear complexity spectrum as a cryptographic criterion of Boolean functions," *IEEE Transactions on Information Theory*, vol. 65, no. 12, pp. 8345–8356, December 2019. [online]

[31] N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, "Secured by blockchain: Safeguarding Internet of things devices," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 28–34, May 2019, Special issue: *blockchain technologies for consumer electronics*. [online]

[32] K. Limniotis and N. Kolokotronis, "Boolean functions with maximum algebraic immunity: further extensions of the Carlet–Feng construction," *Designs, Codes and Cryptography*, vol. 86, no. 8, pp. 1685–1706, August 2018. [online]

[33] K. Ntemos, J. Plata-Chaves, N. Kolokotronis, N. Kalouptsidis, and M. Moonen, "Secure information sharing in adversarial adaptive diffusion networks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 111–124, March 2018, Special issue: *distributed signal processing for security and privacy in networked cyber-physical systems*. [online]

[34] N. Kolokotronis, A. Katsiotis, and N. Kalouptsidis, "Secretly pruned convolutional codes: security analysis and performance results," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1500–1514, July 2016. [online]

[35] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "Secondary constructions of Boolean functions with maximum algebraic immunity," *Cryptography and Communications*, vol. 5, no. 3, pp. 179–199, September 2013. [online]

[36] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Best affine and quadratic approximations of particular classes of Boolean functions," *IEEE Transactions on Information Theory*, vol. 55, no. 11, pp. 5211–5222, November 2009. [online]

[37] T. Etzion, N. Kalouptsidis, N. Kolokotronis, K. Limniotis, and K. G. Paterson, "Properties of the error linear complexity spectrum," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4681–4686, October 2009. [online]

[38] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Factorization of determinants over finite fields and application in stream ciphers," *Cryptography and Communications*, vol. 1, no. 2, pp. 135–165, July 2009. [online]

[39] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "On the linear complexity of sequences obtained by state space generators," *IEEE Transactions on Information Theory*, vol. 54, no. 4, pp. 1786–1793, April 2008. [online]

[40] N. Kolokotronis, "Cryptographic properties of nonlinear pseudorandom number generators," *Designs, Codes and Cryptography*, vol. 46, no. 3, pp. 353–363, March 2008. [online]

[41] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "On the nonlinear complexity and Lempel–Ziv complexity of finite length sequences," *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4293–4302, November 2007. [online]

[42] P. Rizomiliotis, N. Kolokotronis, and N. Kalouptsidis, "On the quadratic span of binary sequences," *IEEE Transactions on Information Theory*, vol. 51, no. 5, pp. 1840–1848, May 2005. [online]

[43] N. Kolokotronis, G. Gatt, and N. Kalouptsidis, "On the generation of sequences simulating higher order white noise for system identification," *Signal Processing*, vol. 84, no. 5, pp. 833–852, May 2004. [online]

[44] N. Kolokotronis and N. Kalouptsidis, "On the linear complexity of nonlinearly filtered PN–sequences," *IEEE Transactions on Information Theory*, vol. 49, no. 11, pp. 3047–3059, November 2003. [online]

[45] N. Kolokotronis, P. Rizomiliotis, and N. Kalouptsidis, "Minimum linear span approximation of binary sequences," *IEEE Transactions on Information Theory*, vol. 48, no. 10, pp. 2758–2764, October 2002. [online]

[46] C. Margaritis, N. Kolokotronis, P. Papadopoulou, D. Martakos, and P. Kanellis, "Securing web–based information systems: a model and implementation guidelines," *Informatica (Slovenia)*, vol. 26, no. 2, pp. 159–168, July 2002, Special issue: *security and protection*. [online]

[47] N. Kolokotronis, C. Margaritis, P. Papadopoulou, P. Kanellis, and D. Martakos, "An integrated approach for securing electronic transactions over the web," *Benchmarking: An International Journal*, vol. 9, no. 2, pp. 166–181, March 2002, Special issue: *electronic commerce — a best practice perspective*. [online]

[48] E. Kofidis, N. Kolokotronis, A. Vassilarakou, S. Theodoridis, and D. Cavouras, "Wavelet–based medical image compression," *Future Generation Computer Systems*, vol. 15, no. 2, pp. 223–243, March 1999. [online]

Συνέδρια (με κρίση)

[49] K. P. Grammatikakis, I. Koufos, and N. Kolokotronis, "A collaborative intelligent intrusion response framework for smart electrical power and energy systems," in *17th International Conference on Availability, Reliability and Security — ARES*. ACM, August 2022, **accepted**.

[50] E. Chaskos, J. Diakoumakos, N. Kolokotronis, and G. Lepouras, "Handling critical infrastructures in federation of cyber ranges: A classification model," in *17th International Conference on Availability, Reliability and Security — ARES*. ACM, August 2022, **accepted**.

[51] S. Brotsis and N. Kolokotronis, "Blockchain-enabled digital forensics for the IoT: Challenges, features, and current frameworks," in *IEEE International Conference on Cyber Security and Resilience — CSR*. IEEE, July 2022, **accepted**.

[52] N. Koutsouris, C. Vassilakis, and N. Kolokotronis, "Cyber-security training evaluation metrics," in *IEEE International Conference on Cyber Security and Resilience — CSR*. IEEE, July 2021, pp. 192–197. [online]

[53] J. Diakoumakos, E. Chaskos, N. Kolokotronis, and G. Lepouras, "Cyber-range federation and cyber-security games: A gamification scoring model," in *IEEE International Conference on Cyber Security and Resilience — CSR*. IEEE, July 2021, pp. 186–191. [online]

[54] E. Pantelidis, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "Insider threat detection using deep autoencoder and variational autoencoder neural networks," in *IEEE International Conference on Cyber Security and Resilience — CSR*. IEEE, July 2021, pp. 129–134. [online]

[55] K. Grammatikakis, I. Koufos, N. Kolokotronis, C. Vassilakis, and S. Shiaeles, "Understanding and mitigating banking trojans: From Zeus to Emotet," in *IEEE International Conference on Cyber Security and Resilience — CSR*. IEEE, July 2021, pp. 121–128. [online]

[56] J. R. Rose, M. Swann, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "Intrusion detection using network traffic profiling and machine learning for IoT," in *7th IEEE International Conference on Network Softwarization — NetSoft, SecSoft workshop*, K. Shiomoto, Y. Kim, C. E. Rothenberg, B. Martini, E. Oki, B. Choi, N. Kamiyama, and S. Secci, Eds. IEEE, June 2021, pp. 409–415. [online]

[57] D. Buckley, G. Bendiab, S. Shiaeles, N. Savage, and N. Kolokotronis, "CHAINGE: A blockchain solution to automate payment detail updates to subscription services," in *IEEE International Conference on Communications Workshops — ICC*. IEEE, June 2021, pp. 1–6. [online]

[58] G. Kermezis, K. Limniotis, and N. Kolokotronis, "User-generated pseudonyms through Merkle trees," in *9th Annual Privacy Forum — APF*, Lecture Notes in Computer Science, N. Gruschka, L. F. C. Antunes, K. Rannenberg, and P. Drogkaris, Eds., vol. 12703. Springer, June 2021, pp. 89–105. [online]

[59] G. Germanos, D. Kavallieros, N. Kolokotronis, and N. Georgiou, "Privacy issues in voice assistant ecosystems," in *2020 IEEE World Congress on Services — SERVICES*. IEEE, October 2020, pp. 205–212. [online]

[60] S. Brotsis, N. Kolokotronis, K. Limniotis, G. Bendiab, and S. Shiaeles, "On the security and privacy of Hyperledger Fabric: Challenges and open issues," in *2020 IEEE World Congress on Services — SERVICES*. IEEE, October 2020, pp. 197–204. [online]

[61] C. Mathas, C. Vassilakis, and N. Kolokotronis, "A trust management system for the IoT domain," in *2020 IEEE World Congress on Services — SERVICES*. IEEE, October 2020, pp. 183–188. [online]

[62] G. Bendiab, K. Grammatikakis, I. Koufos, N. Kolokotronis, and S. Shiaeles, "Advanced metering infrastructures: Security risks and mitigation," in *15th International Conference on Availability, Reliability and Security — ARES*, M. Volkamer and C. Wressnegger, Eds. ACM, August 2020, pp. 1–8. [online]

[63] C. Mathas, K. Grammatikakis, C. Vassilakis, N. Kolokotronis, V. Bilali, and D. Kavallieros, "Threat landscape for smart grid systems," in *15th International Conference on Availability, Reliability and Security — ARES*, M. Volkamer and C. Wressnegger, Eds. ACM, August 2020, pp. 1–7. [online]

[64] S. Brotsis, N. Kolokotronis, K. Limniotis, and S. Shiaeles, "On the security of permissioned blockchain solutions for IoT applications," in *6th IEEE Conference on Network Softwarization — NetSoft, SecSoft Workshop*, F. D. Turck, P. Chemouil, T. Wauters, M. F. Zhani, W. Cerroni, R. Pasquini, and Z. Zhu, Eds. IEEE, June 2020, pp. 465–472. [online]

[65] G. Bendiab, S. Shiaeles, A. Alruban, and N. Kolokotronis, "IoT malware network traffic classification using visual representation and deep learning," in *6th IEEE Conference on Network Softwarization — NetSoft, SecSoft Workshop*, F. D. Turck, P. Chemouil, T. Wauters, M. F. Zhani, W. Cerroni, R. Pasquini, and Z. Zhu, Eds. IEEE, June 2020, pp. 444–449. [online]

[66] F. Alsakran, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "Intrusion detection systems for smart home IoT devices: Experimental comparison study," in *7th International Symposium on Security in Computing and Communications — SSCC*, Communications in Computer and Information Science, S. M. Thampi, G. M. Pérez, R. K. L. Ko, and D. B. Rawat, Eds., vol. 1208. Springer, December 2019, pp. 87–98. [online]

[67] S. Monogios, K. Limniotis, N. Kolokotronis, and S. Shiaeles, "A case study of intra-library privacy issues on android GPS navigation apps," in *8th International Conference on E-Democracy — e-Democracy*, Communications in Computer and Information Science, S. K. Katsikas and V. Zorkadis, Eds., vol. 1111. Springer, December 2019, pp. 34–48. [online]

[68] R. Shire, S. Shiaeles, K. Bendiab, B. V. Ghita, and N. Kolokotronis, "Malware squid: A novel iot malware traffic analysis framework using convolutional neural network and binary visualisation," in *19th International Conference on Internet of Things, Smart Spaces, and Next Generation Networks and Systems — NEW2AN*, Lecture Notes in Computer Science, O. Galinina, S. Andreev, S. I. Balandin, and Y. Koucheryavy, Eds., vol. 11660. Springer, August 2019, pp. 65–76. [online]

[69] T. Chantzios, P. Koloveas, S. Skiadopoulos, N. Kolokotronis, C. Tryfonopoulos, V. Bilali, and D. Kavallieros, "The quest for the appropriate cyber-threat intelligence sharing

platform," in *8th International Conference on Data Science, Technology and Applications — DATA*, S. Hammoudi, C. Quix, and J. Bernardino, Eds. SciTePress, July 2019, pp. 369–376. [online]

[70] S. Shiaeles, N. Kolokotronis, and E. Bellini, "IoT vulnerability data crawling and analysis," in *2019 IEEE World Congress on Services — SERVICES*, C. K. Chang, P. Chen, M. Goul, K. Oyama, S. Reiff-Marganiec, Y. Sun, S. Wang, and Z. Wang, Eds. IEEE, July 2019, pp. 78–83. [online]

[71] N. Kolokotronis, S. Brotsis, G. Germanos, C. Vassilakis, and S. Shiaeles, "On blockchain architectures for trust-based collaborative intrusion detection," in *2019 IEEE World Congress on Services — SERVICES*, C. K. Chang, P. Chen, M. Goul, K. Oyama, S. Reiff-Marganiec, Y. Sun, S. Wang, and Z. Wang, Eds. IEEE, July 2019, pp. 21–28. [online]

[72] C. Constantinides, S. Shiaeles, B. V. Ghita, and N. Kolokotronis, "A novel online incremental learning intrusion prevention system," in *10th IFIP International Conference on New Technologies, Mobility and Security — NTMS*. IEEE, June 2019, pp. 1–6. [online]

[73] S. Brotsis, N. Kolokotronis, K. Limniotis, S. Shiaeles, D. Kavallieros, E. Bellini, and C. Pavué, "Blockchain solutions for forensic evidence preservation in IoT environments," in *5th IEEE International Conference on Network Softwarization — NetSoft, SecSoft Workshop*, C. Jacquenet, F. D. Turck, P. Chemouil, F. Esposito, O. Festor, W. Cerroni, and S. Secci, Eds. IEEE, June 2019, pp. 110–114. [online]

[74] O. Gkotsopoulou, E. Charalambous, K. Limniotis, P. Quinn, D. Kavallieros, G. Sargsyan, S. Shiaeles, and N. Kolokotronis, "Data protection by design for cybersecurity systems in a smart home environment," in *5th IEEE International Conference on Network Softwarization — NetSoft, SecSoft Workshop*, C. Jacquenet, F. D. Turck, P. Chemouil, F. Esposito, O. Festor, W. Cerroni, and S. Secci, Eds. IEEE, June 2019, pp. 101–109. [online]

[75] I. Baptista, S. Shiaeles, and N. Kolokotronis, "A novel malware detection system based on machine learning and binary visualization," in *53rd IEEE International Conference on Communications — ICC, DDINS Workshop*. IEEE, May 2019, pp. 1–6. [online]

[76] K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "A novel blockchain–based trust model for cloud identity management," in *16th IEEE International Conference on Dependable, Autonomic and Secure Computing — DASC*. IEEE Computer Society, August 2018, pp. 724–729. [online]

[77] K.-P. Grammatikakis, A. Ioannou, S. Shiaeles, and N. Kolokotronis, "Are cracked applications really free? An empirical analysis on Android devices," in *16th IEEE International Conference on Dependable, Autonomic and Secure Computing — DASC*. IEEE Computer Society, August 2018, pp. 730–735. [online]

[78] K. Ntemos, N. Kalouptsidis, and N. Kolokotronis, "Trust–based strategies for wireless networks under partial monitoring," in *25th European Signal Processing Conference — EUSIPCO*. EURASIP, August 2017, pp. 2591–2595. [online]

[79] K. Ntemos, N. Kolokotronis, and N. Kalouptsidis, "Using trust to mitigate malicious and selfish behavior of autonomous agents in CRNs," in *27th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications — PIMRC*, September 2016, pp. 1–7. [online]

[80] N. Kolokotronis and M. Athanasakos, "Improving physical layer security in DF relay networks via two–stage cooperative jamming," in *24rd European Signal Processing Conference — EUSIPCO*. EURASIP, August 2016, pp. 1173–1177. [online]

[81] K. Limniotis and N. Kolokotronis, "Boolean functions with maximum algebraic immunity based on properties of punctured Reed–Muller codes," in *2nd International Conference on Cryptography and Information Security in the Balkans — BALKANCRYPTSEC*, Lecture Notes in Computer Science, E. Pasalic and L. R. Knudsen, Eds., vol. 9540. Berlin, Germany: Springer, September 2015, pp. 3–16. [online]

[82] K. Ntemos, N. Kalouptsidis, and N. Kolokotronis, "Managing trust in diffusion adaptive networks with malicious agents," in *23rd European Signal Processing Conference — EUSIPCO*. EURASIP, August 2015, pp. 91–95. [online]

[83] A. Katsiotis, N. Kolokotronis, and N. Kalouptsidis, "Secure encoder designs based on turbo codes," in *2015 IEEE International Conference on Communications — ICC*, June 2015, pp. 4315–4320. [online]

[84] N. Kolokotronis, K. Fytrakis, A. Katsiotis, and N. Kalouptsidis, "A cooperative jamming protocol for physical layer security in wireless networks," in *2015 IEEE International Conference on Acoustics, Speech and Signal Processing — ICASSP*, April 2015, pp. 5803–5807. [online]

[85] N. Kolokotronis, K. Fytrakis, A. Katsiotis, and N. Kalouptsidis, "Cooperation for secure wireless communications with resource–bounded eavesdroppers," in *2014 IEEE Global Communications Conference — GLOBECOM, TPLS Workshop*, December 2014, pp. 1483–1488. [online]

[86] N. Kolokotronis, A. Katsiotis, and N. Kalouptsidis, "Attacking and defending lightweight PHY security schemes for wireless communications," in *7th ACM Conference on Security and Privacy in Wireless and Mobile Networks — WISEC*, July 2014, pp. 177–182. [online]

[87] A. Katsiotis, N. Kolokotronis, and N. Kalouptsidis, "Physical layer security via secret trellis pruning," in *24th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications — PIMRC*, September 2013, pp. 507–512. [online]

[88] N. Kolokotronis and K. Limniotis, "A greedy algorithm for checking normality of cryptographic Boolean functions," in *International Symposium on Information Theory and its Applications — ISITA*. IEEE, October 2012, pp. 601–605. [online]

[89] N. Kolokotronis and K. Limniotis, "On the second–order nonlinearity of cubic Maiorana–McFarland Boolean functions," in *International Symposium on Information Theory and its Applications — ISITA*. IEEE, October 2012, pp. 596–600. [online]

[90] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "Constructing Boolean functions in odd number of variables with maximum algebraic immunity," in *2011 IEEE International Symposium on Information Theory — ISIT*, July 2011, pp. 2686–2690. [online]

[91] N. Kalouptsidis and N. Kolokotronis, "Fast decoding of regular LDPC codes using greedy approximation algorithms," in *2011 IEEE International Symposium on Information Theory Proceedings — ISIT*, July 2011, pp. 2005–2009. [online]

[92] T. Etzion, N. Kalouptsidis, N. Kolokotronis, K. Limniotis, and K. G. Paterson, "On the error linear complexity profiles of binary sequences of period 2^n," in *2008 IEEE International Symposium on Information Theory — ISIT*, July 2008, pp. 2400–2404. [online]

[93] N. Kolokotronis, "On symplectic matrices of cubic Boolean forms and connections with second order nonlinearity," in *2008 IEEE International Symposium on Information Theory — ISIT*, July 2008, pp. 1636–1640. [online]

[94] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Efficient computation of the best quadratic approximations of cubic Boolean functions," in *11th IMA Conference on Cryptography and Coding — IMACC*, Lecture Notes in Computer Science, S. D. Galbraith, Ed., vol. 4887. Berlin, Germany: Springer, December 2007, pp. 73–91. [online]

[95] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Improved bounds on the linear complexity of keystreams obtained by filter generators," in *2007 Information Security and Cryptology — INSCRYPT*, Lecture Notes in Computer Science, D. Pei, M. Yung, D. Lin, and C. Wu, Eds., vol. 4990. Berlin, Germany: Springer, September 2007, pp. 246–255. [online]

[96] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Best affine approximations of Boolean functions and applications to low order approximations," in *2007 IEEE International Symposium on Information Theory — ISIT*, June 2007, pp. 1836–1840. [online]

[97] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Lower bounds on sequence complexity via generalised Vandermonde determinants," in *2006 Sequences and Their Applications — SETA*, Lecture Notes in Computer Science, G. Gong, T. Helleseth, H.-Y. Song, and K. Yang, Eds., vol. 4086. Berlin, Germany: Springer, September 2006, pp. 271–284. [online]

[98] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "Nonlinear complexity of binary sequences and connections with Lempel–Ziv compression," in *2006 Sequences and Their Applications — SETA*, Lecture Notes in Computer Science, G. Gong, T. Helleseth, H.-Y. Song, and K. Yang, Eds., vol. 4086. Berlin, Germany: Springer, September 2006, pp. 168–179. [online]

[99] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "New results on the linear complexity of binary sequences," in *2006 IEEE International Symposium on Information Theory — ISIT*, July 2006, pp. 2003–2007. [online]

[100] N. Kolokotronis, "Cryptographic properties of stream ciphers based on t–functions," in *2006 IEEE International Symposium on Information Theory — ISIT*, July 2006, pp. 1604–1608. [online]

[101] P. Rizomiliotis, N. Kolokotronis, and N. Kalouptsidis, "On the quadratic span of binary sequences," in *2003 IEEE International Symposium on Information Theory — ISIT*, July 2003, p. 377. [online]

[102] N. Kolokotronis, G. Gatt, and N. Kalouptsidis, "On the generation of sequences simulating higher order white noise for system identification," in *11th European Signal Processing Conference — EUSIPCO*, vol. I. EURASIP, September 2002, pp. 217–220. [online]

[103] P. Rizomiliotis, N. Kolokotronis, and N. Kalouptsidis, "Construction of sequences with four–valued autocorrelation from GMW sequences," in *2002 IEEE International Symposium on Information Theory — ISIT*, July 2002, p. 183. [online]

[104] C. Margaritis, N. Kolokotronis, P. Papadopoulou, P. Kanellis, and D. Martakos, "A model and implementation guidelines for information security strategies in web environments,"

in *Advances in Information Security Management and Small Systems Security*, IFIP Advances in Information and Communication Technology, J. H. P. Eloff, L. Labuschagne, R. von Solms, and G. Dhillon, Eds., vol. 72. Kluwer Academic Publishers, September 2001, pp. 13–34. [online]

[105] N. Kolokotronis, P. Rizomiliotis, and N. Kalouptsidis, "First–order optimal approximation of binary sequences," in *2001 Sequences and Their Applications — SETA*, Discrete Mathematics and Theoretical Computer Science, T. Helleseth, P. V. Kumar, and K. Yang, Eds. Berlin, Germany: Springer, May 2001, pp. 242–256. [online]

[106] P. Papadopoulou, N. Kolokotronis, P. Kanellis, and D. Martakos, "Conceptualizing and implementing an information security strategy for internet billing systems," in *Advances in Infrastructure for e-Business, e-Science, and e-Education on the Internet*. Scuola Superiore Guglielmo Reiss Romoli — SSGRR, July 2000, pp. 1–9. [online]

Τεχνικές αναφορές

[107] N. Kolokotronis and S. Shiaeles, "Effective response and mitigation of advanced cyber-attacks via an intelligent cyber-defence framework," Open Access Government, September 2019. [online]

[108] S. Shiaeles and N. Kolokotronis, "Cyber-Trust: Safeguarding IoT and building trust through blockchain," Open Access Government, September 2019. [online]

[109] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "Modifying Boolean functions to ensure maximum algebraic immunity," IACR Cryptology ePrint Archive, Report 2012/046, January 2012. [online]

[110] N. Kolokotronis and K. Limniotis, "Maiorana–McFarland functions with high second–order nonlinearity," IACR Cryptology ePrint Archive, Report 2011/212, May 2011. [online]

[111] N. Kolokotronis, K. Limniotis, and N. Kalouptsidis, "Best quadratic approximations of cubic Boolean functions," IACR Cryptology ePrint Archive, Report 2007/037, February 2007. [online]

[112] E. Kopanaki, N. Kolokotronis, and D. Martakos, "What is the Hellenic billing mall and how it works," *Bancassurance and Banking*, no. 3, pp. 28–36, July 2000, invited Article.

Σε εξέλιξη

[113] E. Chaskos, J. Diakoumakos, N. Kolokotronis, and G. Lepouras, "Gamification mechanisms in cyber range and cyber security training environments," pp. 1–17, **under review** (book chapter).

[114] G. Bendiab, A. Hameurlaine, G. Germanos, N. Kolokotronis, and S. Shiaeles, "Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence," pp. 1–24, **under review** (journal).

[115] J. R. Rose, M. Swann, K. P. Grammatikakis, I. Koufos, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "IDERES: Intrusion detection and response system using machine learning and attack graphs," pp. 1–12, **under review** (journal).

[116] A. Varelias, K. Limniotis, and N. Kolokotronis, "Cryptographic properties of boolean functions generating similar De Bruijn sequences," pp. 1–23, **under review** (book chapter).

[117] I. Tzinos, K. Limniotis, and N. Kolokotronis, "Evaluating the performance of post-quantum secure algorithms in the TLS protocol," pp. 1–21, **under review** (journal).

[118] J. Diakoumakos, E. Chaskos, N. Kolokotronis, and G. Lepouras, "Cyber-security gamification in federation of cyber-ranges: Design, implementation, and evaluation," pp. 1–14, **under review** (journal).

[119] E. Chaskos and N. Kolokotronis, "A survey on cyber-range systems for cyber-security training," under preparation (journal).

[120] N. Kolokotronis and P. Smyrli, "Multilayer constructions of ISD algorithms for solving the CSD problem," under preparation (journal).

[121] N. Kolokotronis and K. Limniotis, "Low–order approximation attacks on block ciphers: applications in AES–128 and 3DES," under preparation (journal).

[122] N. Kolokotronis, "Cryptography: algorithm design and advanced cryptanalysis," under preparation (book).

Αναφορές στο επιστημονικό έργο

Το Google Scholar καταγράφει συνολικό αριθμό **902** αναφορών, με βιβλιομετρικούς δείκτες h–index και i10–index ίσους με 17 και 25 αντίστοιχα.

Digitally signed by NIKOLAOS KOLOKOTRONIS
Date: 2022.06.11 00:48:53 +03'00'