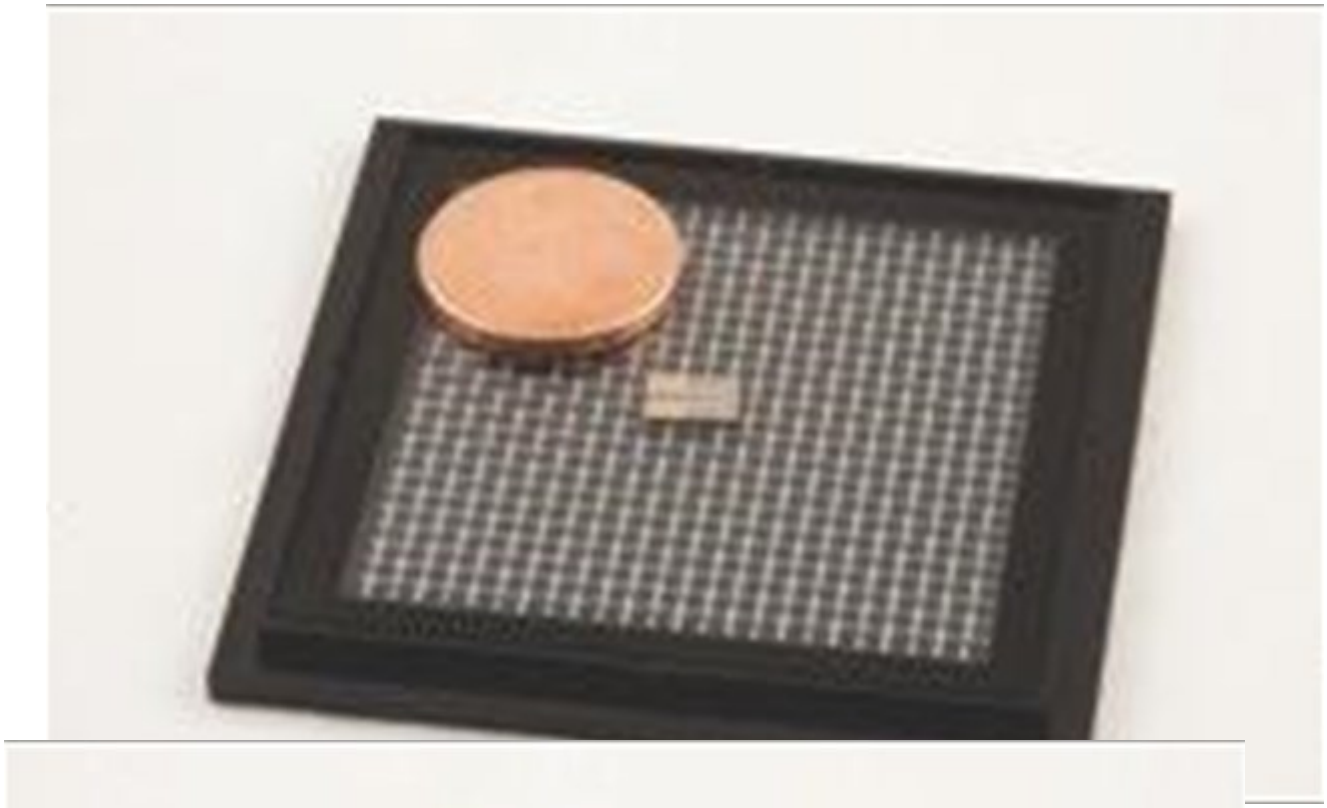
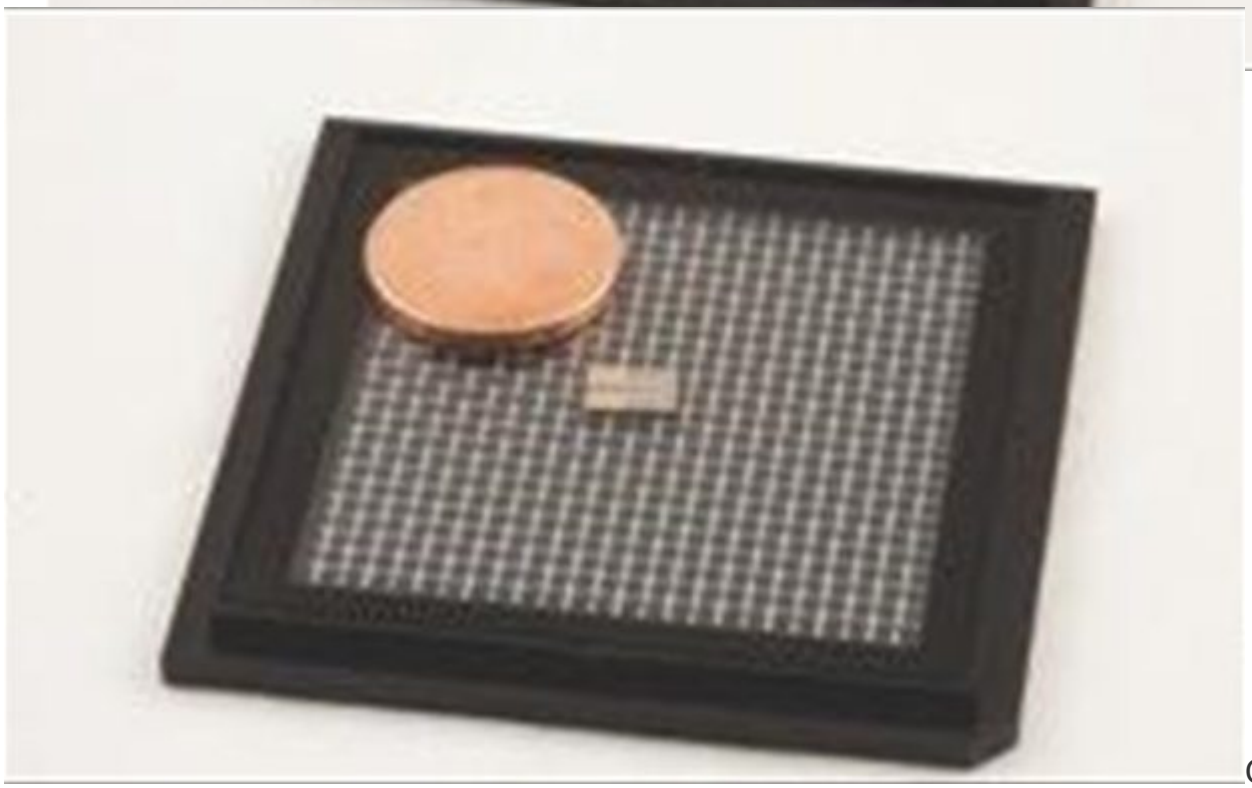
11 Σεπτεμβρίου 2016

Τσιπ για άνευ προηγουμένου επίπεδο κρυπτογράφησης σε φορητές συσκευές

/ Επιστήμες, Τέχνες & Πολιτισμός





Οι

γεννήτριες τυχαίων αριθμών παίζουν πολύ σημαντικό ρόλο σε ό,τι αφορά στην κρυπτογράφηση ηλεκτρονικών συσκευών, από τις φορητές συσκευές και τις online αγορές μέχρι τη χρήση ATM.

Σύμφωνα με δημοσίευμα του Phys.Org, για πρώτη φορά ερευνητές δημιούργησαν μία ταχεία γεννήτρια που βασίζεται σε διαδικασία κβαντικής μηχανικής, η οποία μπορεί να παρέχει τα πιο ασφαλή «κλειδιά» κρυπτογράφησης στον κόσμο, σε «συσκευασία» αρκετά μικρή για χρήση σε φορητές συσκευές.

Η δουλειά των ερευνητών παρουσιάζεται στο Optica (Optical Society) και αποτελεί σημαντική πρόοδο στον τομέα της ενσωμάτωσης της τεχνολογίας κβαντικών γεννητριών αριθμών σε υπολογιστές, tablets και κινητά τηλέφωνα. «Καταφέραμε να βάλουμε κβαντική τεχνολογία που χρησιμοποιείται σε μεγαλεπήβολα επιστημονικά πειράματα σε ένα ‘πακέτο’ το οποίο μπορεί να χρησιμοποιήσει την εμπορική αξιοποίησή της» αναφέρει ο πρώτος συντάκτης του σχετικού paper, Κάρλος Αμπελάν, διδακτορικός φοιτητής του ICFO (Ινστιτούτο Φωτονικών Επιστημών) του Ινστιτούτου Επιστημών και Τεχνολογίας της Βαρκελώνης.

Η νέα συσκευή λειτουργεί σε ταχύτητες gigabits ανά δευτερόλεπτο και είναι αρκετά γρήγορη για κρυπτογράφηση σε πραγματικό χρόνο δεδομένων επικοινωνιών, όπως σε τηλέφωνα ή βιντεοκλήσεις, ή για την κρυπτογράφηση μεγάλων όγκων δεδομένων που κινούνται από ή προς servers όπως αυτοί που χρησιμοποιούνται σε μέσα κοινωνικής δικτύωσης. Επίσης, θα μπορούσε να δει χρήση σε συστήματα προγνώσεων χρηματιστηρίων και πολύπλοκες επιστημονικές εξομοιώσεις σχετικά με βιολογικές αλληλεπιδράσεις ή πυρηνικές αντιδράσεις.

Οι σημερινές γεννήτριες τυχαίων αριθμών βασίζονται σε αλγορίθμους υπολογιστών ή στην τυχαιότητα των φυσικών διαδικασιών. Στην ουσία πρόκειται για πολύπλοκες εκδοχές του ριξίματος ζαριών ξανά και ξανά για την παραγωγή τυχαίων αριθμών. Αν και οι αριθμοί που παράγονται φαίνονται τυχαίοι, η κατοχή συγκεκριμένων πληροφοριών, όπως το πόσα «ζάρια» ρίχνονται, μπορεί να επιτρέψει σε χάκερ κάποιες φορές να βρουν τους αριθμούς, με αποτέλεσμα να αποκτούν πρόσβαση σε προστατευμένα δεδομένα που θεωρούνταν ασφαλή.

Η νέα αυτή συσκευή, ωστόσο, παράγει τυχαίους αριθμούς βάσει των κβαντικών ιδιοτήτων του φωτός- μια διαδικασία που είναι εκ των πραγμάτων τυχαία και άρα αδύνατον να προβλεφθεί, όσο πολλές πληροφορίες και αν έχει κάποιος. Αν και άλλοι ερευνητές στο παρελθόν είχαν καταφέρει να αναπτύξουν κβαντικές γεννήτριες τυχαίων αριθμών, ήταν είτε μεγαλύτερες είτε πιο αργές σε σχέση με τη συσκευή που περιγράφεται στο Optica.

Πηγή: naftemporiki.gr