



ΠΑΝΕΠΙΣΤΗΜΙΟ  
ΠΑΤΡΩΝ  
UNIVERSITY OF PATRAS

ΑΝΟΙΚΤΑ ακαδημαϊκά  
μαθήματα ΠΠ

# Κβαντική Επεξεργασία Πληροφορίας

Ενότητα 20: Κβαντική Κρυπτογραφία

Σγάρμπας Κυριάκος

Πολυτεχνική Σχολή

Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας  
Υπολογιστών

# Σκοποί ενότητας

Κβαντική Κρυπτογραφία



# Περιεχόμενα ενότητας

## Κβαντική Κρυπτογραφία

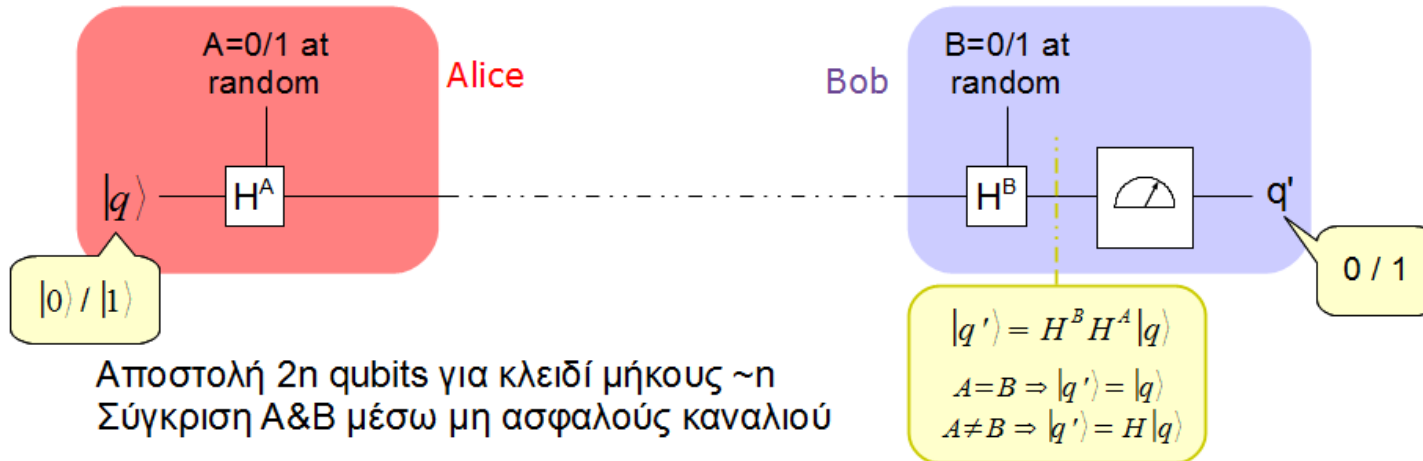


# Κβαντική Κρυπτογραφία

# Κβαντική Κρυπτογραφία

Quantum Key Distribution – The BB84 Protocol

Bennett and Brassard, 1984



Αποστολή  $2n$  qubits για κλειδί μήκους  $\sim n$   
 Σύγκριση A&B μέσω μη ασφαλούς καναλιού

Alice	0	1	1	0	1	1	0	0	0	1	0	1
	I	H	I	H	H	I	I	H	H	H	I	I
Bob	I	H	H	I	H	I	H	I	H	I	I	H
	0	1	0/1	0/1	1	1	0/1	0/1	0	0/1	0	0/1

σύγκριση

**KEY = 0 1 1 1 0 0**

C.H.Bennett, G.Brassard, "Quantum cryptography: Public key distribution and coin tossing", Proc. IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp.175-179, December 1984.



Τέλος Ενότητας

# Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στο πλαίσιο του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αθηνών**» έχει χρηματοδοτήσει μόνο την αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.



Σημειώματα



# Σημείωμα Ιστορικού Εκδόσεων Έργου

Το παρόν έργο αποτελεί την έκδοση **1.0**.

Έχουν προηγηθεί οι κάτωθι εκδόσεις:

- Έκδοση **1.0** διαθέσιμη [εδώ](#).



# Σημείωμα Αναφοράς

Copyright Πανεπιστήμιο Πατρών, **Σγάρμπας Κυριάκος**. «**Κβαντική Επεξεργασία Πληροφορίας, Κβαντική Κρυπτογραφία**». Έκδοση: **1.0**. Πάτρα **2014**. Διαθέσιμο από τη δικτυακή διεύθυνση:

[https://eclass.upatras.gr/modules/course\\_metadata/opencourses.php?fc=15](https://eclass.upatras.gr/modules/course_metadata/opencourses.php?fc=15)



# Σημείωμα Αδειοδότησης

Το παρόν υλικό διατίθεται με τους όρους της άδειας χρήσης Creative Commons Αναφορά, Μη Εμπορική Χρήση Παρόμοια Διανομή 4.0 [1] ή μεταγενέστερη, Διεθνής Έκδοση. Εξαιρούνται τα αυτοτελή έργα τρίτων π.χ. φωτογραφίες, διαγράμματα κ.λ.π., τα οποία εμπεριέχονται σε αυτό και τα οποία αναφέρονται μαζί με τους όρους χρήσης τους στο «Σημείωμα Χρήσης Έργων Τρίτων».



[1] <http://creativecommons.org/licenses/by-nc-sa/4.0/>

Ως **Μη Εμπορική** ορίζεται η χρήση:

- που δεν περιλαμβάνει άμεσο ή έμμεσο οικονομικό όφελος από την χρήση του έργου, για το διανομέα του έργου και αδειοδόχο
- που δεν περιλαμβάνει οικονομική συναλλαγή ως προϋπόθεση για τη χρήση ή πρόσβαση στο έργο
- που δεν προσπορίζει στο διανομέα του έργου και αδειοδόχο έμμεσο οικονομικό όφελος (π.χ. διαφημίσεις) από την προβολή του έργου σε διαδικτυακό τόπο

Ο δικαιούχος μπορεί να παρέχει στον αδειοδόχο ξεχωριστή άδεια να χρησιμοποιεί το έργο για εμπορική χρήση, εφόσον αυτό του ζητηθεί.

# Διατήρηση Σημειωμάτων

Οποιαδήποτε αναπαραγωγή ή διασκευή του υλικού θα πρέπει να συμπεριλαμβάνει:

- το Σημείωμα Αναφοράς
- το Σημείωμα Αδειοδότησης
- τη δήλωση Διατήρησης Σημειωμάτων
- το Σημείωμα Χρήσης Έργων Τρίτων (εφόσον υπάρχει)

μαζί με τους συνοδευόμενους υπερσυνδέσμους.



# Σημείωμα Χρήσης Έργων Τρίτων

Το Έργο αυτό κάνει χρήση των ακόλουθων έργων:

**Εικόνες/Σχήματα/Διαγράμματα/Φωτογραφίες**

