UNIVERSITAT JAUME I
Escola Superior de Tecnologia i Ciències Experimentals · ESTCE

LA CORRIOLA

Escola Superior de Tecnologia i Ciències Experimentals

Revista de divulgació de l'Escola Superior de Tecnologia i Ciències Experimentals
Número 23 • gener de 2018 // Revista de publicació quadrimestral

L'UJI recull el certificat del segell de qualitat EUR-ACE® de quatre titulacions de l'àmbit de l'enginyeria

Quatre titulacions de la Universitat Jaume I que tenen el segell europeu de qualitat EUR-ACE®, han rebut el certificat en el marc de la jornada que s'ha celebrat a la seu de l'Institut de l'Enginyeria d'Espanya a Madrid, el títol de la qual era «El segell EUR-ACE: reflexions i nous reptes».

Ideen un videojoc infantil basat en el joc 'Pedra, paper, tisora'

Les estudiantes Marina Granell, Araceli Cazorla i Lucía Menéndez, graduades en Disseny i Desenvolupament de Videojocs, han desenvolupat un videojoc molt ben resolt tècnicament, inspirat en el tradicional Pedra, paper, tisora, al qual han anomenat Meowgic. Van fer una presentació en el Hackathon i van ser un dels grups que va presentar un projecte millor acabat, amb una aplicació pràcticament a punt per a pujar-la a les botigues digitals, descarregar-la i jugar.

Noves iniciatives en el grau en Arquitectura Tècnica

Un grup d'alumnes d'Arquitectura Tècnica de l'UJI treballen en un estudi sobre rehabilitació d'habitatges socials municipals de Castelló, mentre que un altre grup inicia l'estudi de l'arquitectura tradicional al poble de Llucena.

El monoplaça d'UJI Motorsport s'exhibeix per primera vegada al campus universitari

L'UJI Motorsport ha aconseguit crear un monoplaça competitiu al mateix nivell d'altres universitats amb pressupostos que superen el milió d'euros, com és el cas d'alguns equips alemanys o nord-americans. Pel que fa a equips espanyols, el de l'UJI és l'equip amb el cotxe més econòmic.

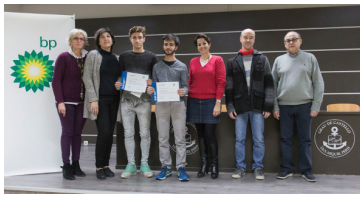
Dos alumnes de l'UJI guanyen el primer concurs de videojocs de la Comunitat Valenciana

Aurelio Puerta Martín i Kiko Alfaro Moscardó, dos estudiants d'últim curs del grau en Disseny i Desenvolupament de Videojocs, han guanyat el primer concurs d'estudiants de videojocs de la Comunitat Valenciana (Student Game Contest) amb el seu prototip Towerglass.

L'UJI col·labora amb professorat de secundària per a participar en la primera celebració del Dia Internacional de la Llum

Amb motiu de la recent declaració per part del Comitè Executiu de l'UNESCO del 16 de maig com el Dia Internacional de la Llum, que se celebrarà per primera vegada durant l'any 2018, es proposa la realització de material vinculat amb l'òptica i les seues aplicacions, com ara vídeos, pòsters i experiències, que s'exposaran en l'edifici Menador el dia 16 de maig de 2018.

Lliurament del Premi BP de ciències a dos alumnes de l'IES Miquel Peris del Grau de Castelló



La Universitat Jaume I i la Refineria de Castelló de BP Oil España han fet el lliurament del «Premi BP al millor treball de ciències dels instituts d'Almassora i del Grau de Castelló», als alumnes Marc Espinosa Edo i Víctor Gómez Pol, de segon curs de batxillerat de l'IES Miquel Peris i Segarra del Grau de Castelló.

Iniciativa de col·laboració en el grau d'Enginyeria Agroalimentària

Els alumnes de l'assignatura Regs i Drenatges d'Enginyeria Agroalimentària i del Medi Rural han desenvolupat un projecte de col·laboració amb estudiants del Taller de Formació Professional en l'especialitat de Jardineria,Viverisme i Horticultura Ecològica de Càritas Diocesana de Sogorb-Castelló (Taller CFO), per a millorar l'àmbit del reg.

Criptografia Quàntica

PABLO SERNA GALLÉN

Guanyador del Premi Literari en Valencià de Divulgació Cientificotecnològica ESTCE 2017

Una mirada als nostres voltants hauria de ser suficient per a adonar-nos que, indubtablement, la nostra societat està regida pels avanços científics. Durant les darreres dècades hem aconseguit controlar des de casa, del treball, o potser, fins i tot, quan viatgem, certes coses que uns anys enrere eren impensables. En l'actualitat, només prement unes quantes tecles i fent alguns clics, podem fer compres a la xarxa, transaccions bancàries o emplenar sol•licituds administratives. Solem estar convençuts que el procediment emprat és segur si a la barra d'adreces distingim l'encapçalament https (amb la darrera s certificant la nostra seguretat en línia). Ara bé, hauríem de plantejar-nos si realment les nostres dades estan segures; què hi ha al darrere de tot això? I més encara quan tot el nostre patrimoni podria dependre en uns anys dels incipients bitcoins... A ningú ens agradaria que els nostres coins s'esfumaren cap a la butxaca d'un hacker. Aleshores, és quan hem de començar a parlar de la criptografia.

Ja les antigues civilitzacions —com Egipte o Mesopotàmia— s'adonaren de la importància d'establir una comunicació segura per a evitar que els secrets més rellevants de l'imperi caigueren en mans enemigues. Amb el pas dels anys, les tècniques criptogràfiques (que permetien generar codis i claus segures) van desenvolupar-se. Al segle V aC els espartans empraven l'escítala, un conjunt de dues vares idèntiques al voltant de les quals s'enrotllava una cinta de cuir en espiral, s'hi escrivia el missatge longitudinalment i s'enviava al receptor, qui disposava de la vara bessona, sense la qual el missatge tan sols era un recull de lletres inintel•ligibles per qualsevol altre.

Fig. 1. Imatge d'una escítala.

L'interès popular per la criptografia tot just havia començat. Amb els segles, sorgiren fonamentalment dos tipus de sistemes criptogràfics (o criptosistemes). D'una banda, tenim el criptosistema simètric, en el qual la clau és privada (només coneguda per l'emissor i el receptor), però ens enfrontem amb el problema de la seguretat a l'hora de la distribució d'aquesta clau. D'altra banda, trobem el criptosistema asimètric, com el RSA, desenvolupat en 1978 per Rivest, Shamir i Adleman. En aquest sistema, els usuaris empren dues claus: una permet xifrar el missatge —l'anomenada clau pública, a l'abast de tothom—, i l'altra —només en coneixement del destinatari—, desxifrar-lo. Actualment, aquest darrer sistema encara domina els nostres mercats internacionals i vetla per la seua protecció. La majoria es basen en algoritmes matemàtics molt fàcils de realitzar en un sentit (per exemple, la multiplicació) però intractables en el sentit invers, com és el cas de la factorització en nombres primers de nombres amb molts dígits, un procés molt lent. D'aquesta manera, se sol dir que per al moment en què l'algoritme matemàtic estiguera resolt, la informació protegida hauria perdut gairebé el seu valor. Tot i això, hem de ser escèptics amb aquests criptosistemes, ja que nous desenvolupaments d'encriptació podrien vèncer aquestes barreres amb un temps bastant inferior. Per tant, la criptografia moderna està subjecta i és vulnerable als avanços tecnològics computacionals i a l'evolució en el tractament matemàtic dels algoritmes.

Davant d'aquesta situació, la qual podria representar un greu problema per a determinades àrees —com les de seguretat nacional, intel•ligència militar o empreses privades—, sorgeix la necessitat d'anar més enllà del que els nostres sentits poden concebre. És el moment d'allunyar-nos de la concepció clàssica que tenim del nostre voltant i endinsar-nos en el món del règim quàntic. És el moment de donar pas a la criptografia quàntica, una nova manera de solucionar els problemes esmentats.

En lloc de dependre de la complexitat de la factorització de llargs nombres, la criptografia quàntica es basa en els principis fonamentals de la mecànica quàntica. El primer que hem de tenir en compte és l'anomenat problema del mesurament, segons el qual és impossible mesurar l'estat quàntic d'un sistema sense pertorbar-lo. Aquest és un gran punt a favor de la criptografia si tenim en compte la presència de possibles espies que volen esbrinar el missatge. D'altra banda, també és important destacar el principi de

polarització dels fotons (les partícules que formen la llum), que descriu la manera en què aquests poden ser orientats o polaritzats en diferents direccions, una propietat que és fonamental.

Amb aquestes consideracions, l'any 1984 Charles H. Bennet i Grills Brassard desenvoluparen el primer protocol de criptografia quàntica, que va rebre el nom de BB84. Els investigadors van pensar que podien crear una clau d'encriptació en funció de la quantitat de fotons que impactaren en un detector i la manera en què ho feien. Quan encenem un llum es generen fotons en totes les direccions possibles, no obstant això, mitjançant filtres de polarització podem seleccionar les direccions d'interès (trobem un exemple d'aquesta aplicació en les ulleres de sol que sovint portem). D'aquesta manera, es podria crear un missatge on cada fotó —orientat d'una manera corresponent— representaria un dígit (els anomenats bits, els quals prenen el valor de 0 i 1).

Per a explicar el funcionament del protocol BB84, a grans trets, sovint s'ha recorregut a la creació de tres personatges: Alice (l'emissora de la clau per a desxifrar el missatge), Bob (el receptor) i Eve (una possible espia). La comunicació comença quan Alice envia a Bob fotons polaritzats a diferents angles (0, 45, 90 o 135 graus). Per a cada fotó, Bob selecciona aleatòriament un filtre que detectarà els fotons rectilinis o, per contra, els diagonals. Aleshores, per probabilitat, Bob mesurarà correctament el 50% dels fotons. A continuació, Bob informa Alice dels filtres que ha emprat, de manera que descarten els fotons mesurats incorrectament i els correctes són transformats en bits. En cas que Eve intentara obtenir informació, alteraria les probabilitats i, per tant, Alice i Bob s'adonarien de l'existència d'un espia i immediatament aturarien la comunicació.

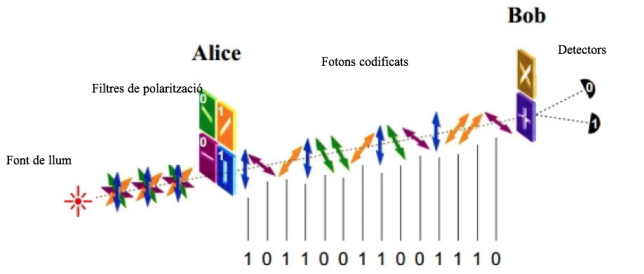


Fig. 2. Esquema de funcionament del protocol BB84

Durant els darrers anys, la criptografia quàntica ha adquirit renom. Membres de la Unió Europea han invertit importants quantitats de diners en la recerca de sistemes de comunicació basats en aquesta tecnologia. A més a més, algunes companyies com MagiQ Technologies —amb seu a Nova York— ja està implementant la criptografia quàntica per buscar solucions als actuals sistemes de seguretat. La proposta que ofereix MagiQ és un model híbrid que implementa al mateix temps els algoritmes matemàtics i els nous conceptes quàntics basats en el model BB84.

Malgrat els avanços fets en l'àmbit de la criptografia quàntica, encara queden molts aspectes per a perfilar i problemes per a solucionar fins que aquesta es convertisca en el sistema implementat en termes de seguretat. Tot i això, recentment a la Xina han aconseguit l'intercanvi de claus quàntiques via satèl•lit amb una distància propera als 1.200 km. Indubtablement, la criptografia quàntica trobarà grans aplicacions comercials en els anys vinents. Ara bé... la fortalesa de sistemes de criptografia quàntica tan potents podria convertir-se en el seu propi taló d'Aquil•les, ja que ni les agències de seguretat serien capaces de descodificar els criptogrames quàntics. Potser ens resulte difícil a hores d'ara intentar concebre que la solució es troba en un món quàntic, del qual no podem ser partícips. Però... ben pensat, no ens ha d'estranyar; segons el problema del mesurament... és impossible que mesurem l'estat quàntic de les nostres percepcions humanes sense que abans pertorbem els nostres sentits. Només ens resta, per tant, fascinar-nos.

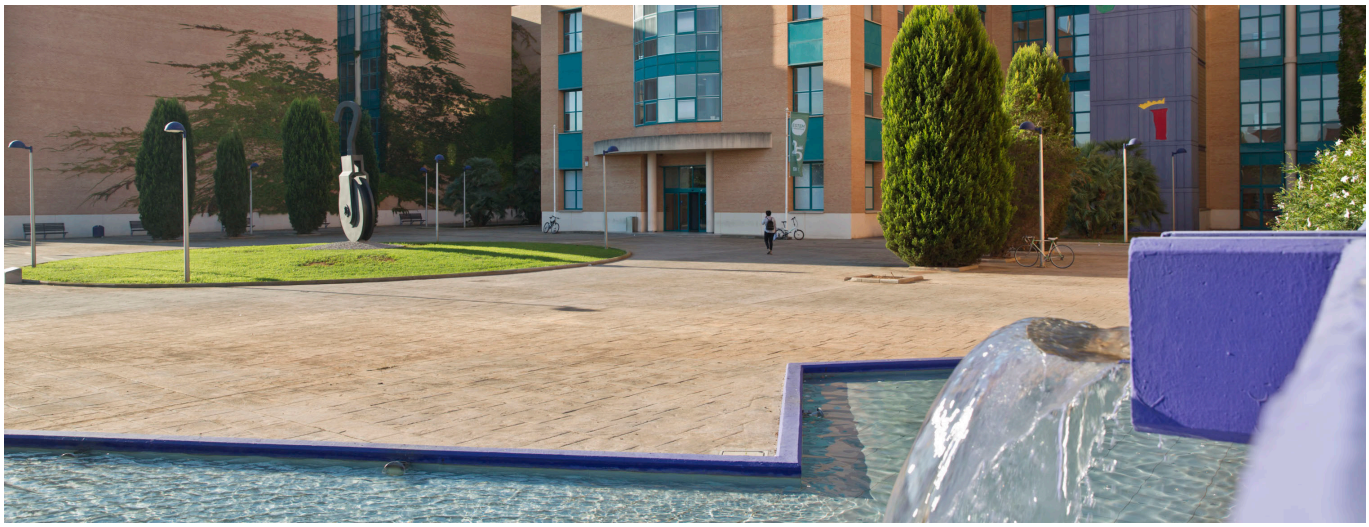
FONTS:

Ashley G. Smart (2017). Quantum entanglement reaches new heights. (American Institute of Physics)

Petra Pajic (2013). Quantum Cryptography. (Bachelor Thesis, University of Vienna).

J. Aditya, P. Shankar Rao. Quantum Cryptography (Dept. of CSE, Andhra University).

Villafranca Ramosa, A. (2006). Computación y criptografía cuánticas: Retos para la seguridad en la sociedad de la información. Jornada Tecnimap Sevilla.



Campus Universitat Jaume I

Oferta de graus de l'ESTCE: El teu futur

L'ESTCE de la Universitat Jaume I de Castelló, centre docent i investigador de prestigi, ofereix els següents graus oficials

Tecnologies de la Informació i les Comunicacions:

1. Grau en Enginyeria Informàtica 2. Grau en Matemàtica Computacional 3. Grau en Disseny i Desenvolupament deVideojocs	Els dos primers graus comparteixen un gran nombre d'assignatures la qual cosa facilita la transició entre graus i l'obtenció del doble grau. Matemàtica Computacional i Disseny i Desenvolupament deVideojocs son graus de caràcter innovador i pioners a l'estat. Matemàtica Computacional només oferta 30 places d'entrada.

Enginyeries Industrials:

4. Grau en Enginyeria Elèctrica 5. Grau en Enginyeria Mecànica 6. Grau en Enginyeria Química 7. Grau en Enginyeria en Tecnologies Industrials	Comparteixen un gran nombre d'assignatures la qual cosa facilita la transició entre graus i l'obtenció de dobles graus. Possibilitat de doble diploma amb 'Grandes Écoles' de França (EURUJI).
8. Enginyeria Agroalimentària i del Medi Rural	Grau amb molts perfils professionals relacionats amb el nostre entorn.
9. Grau en Arquitectura Tècnica	Presenta una metodologia docent per projectes molt innovadora. Possibilitat de doble títol amb VIA University College, Dinamarca.
10. Grau en Enginyeria de Disseny Industrial i Desenvolupament de Productes	Ofereix una formació innovadora, orientada a l'exercici professional, pionera en els seus inicis i fortament consolidada en l'actualitat.
11. Grau en Química	Únic grau de la branca de Ciències. Avalat amb el segell d'una ampla tradició històrica i de qualitat.

LA CORRIOLA Número 23 • gener de 2018

Escola Superior de Tecnologia i Ciències Experimentals
UNIVERSITAT JAUME • I

Equip de redacció

Ximo Gual, Merche Fernández, Antonio Gallardo - Novetats de l'ESTCE
Carmen Pesudo - Secció preuniversitaria
Francisco José Colomer - Científics i enginyers il·lustres

Més informació a: www.estce.uji.es

Per a col·laborar en la revista envia un mail a: estce@uji.es

Edita:

ESTCE • Dipòsit legal: CS 364-2010 • Imprimeix: Innovació Digital Castelló, s.l.u.