Cambridge International University

Universidad Internacional Abierta Generalísimo Sebastián Francisco de Miranda

Quantum Cryptography

Postgraduate

Diplomado

INSTITUCIONES

UNIAGSFMI - **Universidad Internacional Abierta Generalísimo Sebastián Francisco de Miranda** - (Virtual University - Distance Learning), es una Institución privada de formación permanente para personas adultas, utilizando métodos propios, desarrollados para cubrir y resolver las necesidades culturales profesionales y educativas de graduación, ofreciendo grados y post-grados presenciales, semi-presenciales y a distancia, así como otros programas consolidados en plataformas internacionales.

Protocolizada en la Secretaria de Educación del estado de Sao Paolo, República Federativa de Brasil y registrada en la República de Venezuela, ante el Ministerio del Poder Popular de Interiores y Justicia, Rif.: J-31491944-0, es Miembro del consejo para la educación en el Consorcio EuroAmericano de Universidades (CUE) con el número 0116. Acreditada por la International Commission of Diplomatic Relation Human Rights and peace, el 2 de agosto del año 2016 hasta el 7 de octubre del año 2050, autorizado por el Consejo global de evaluación y acreditación, como institución autónoma de educación superior en línea, Numero de acreditación:

AHEOL20082016SG, después de supervisados y satisfaciendo los criterios de esta Organización en la misión de prácticas educativas, administración, estabilidad financiera, políticas, y servicios al estudiante.

CIU - **Cambridge International University** - es una institución privada e independiente de educación superior a distancia especializada en la enseñanza de postgrado para adultos. Está legalmente registrada e incorporada bajo las leyes del Estado de Florida, EE.UU. Codex: P12000025755 y CIF 39-2080764. Registrada en el Reino de España (UE), con el número de identificación CIF: N4007153D. CIU Cambridge International University está acreditada y es miembro de pleno derecho por la Comisión de Educación Superior de UEC University EuroAmerican Consortium (EU) y Middle States Commission on Higher Educatión (USA).

DESCRIPCIÓN

El propósito de la titulación de Posgraduate Degree es proporcionar a los estudiantes un conocimiento extenso sobre todas las materias directa e indirectamente relacionadas con su campo de estudios.

El nivel, Posgraduate Degree significa introducirse y adquirir los conocimientos generales, en un particular campo de estudio y obtener una formación especializada, que permite el acceso a niveles de maestría.

Todo el programa de estudios se desarrolla en idioma español.

Este **Diplomado de Ciencias en Criptografía Cuántica o Posgraduate of Science in Quantum Cryptography**, proporciona los fundamentos esenciales de la física cuántica aplicándolos al mundo de la computación y la criptografía y destaca sus aspectos más importantes.

La computación cuántica permite, en principio, aumentos dramáticos en la potencia de cálculo gracias a la posibilidad de superposición de bits cuánticos.

A día de hoy, es una alternativa realista a las técnicas criptográficas actuales, que sería de aplicación, sustituyendo, en un futuro cercano, los métodos clásicos de criptografía actuales.

A QUIEN VA DIRIGIDO

El Posgraduate of Science in Quantum Cryptography, está orientado a profesionales universitarios Títulos de :

1. Ingeniería, Física, Matemáticas, informática, Computación, Sistemas.

2. Personas con la capacidad para aprender, resolver problemas, y buscar información, abstracción y uso del lenguaje matemático.

El programa de Posgraduate Degree, en la modalidad “Distance Learning” está diseñado para adultos que trabajan y que disponen de poco tiempo.

Profesionales de otras áreas académicas y adultos que aseguren, como mínimo, en su solicitud, estudios base en informática, computación, física, matemáticos, y perfiles profesionales afines a estas ciencias.

Puede ser finalizado, en aproximadamente, 6 meses o antes dependiendo de la disponibilidad de tiempo y motivación del estudiante.

Este programa está diseñado para adultos que aporten como mínimo estudios universitarios. En la Solicitud de Acceso a este programa, también se evalúa las cualificaciones del postulante.

OBJETIVOS

Proporcionar una formación amplia en el campo de Criptografía Cuántica, que le permita ser capaz de describir el comportamiento de las partículas del microcosmos, enumerar los postulados de la Física Cuántica y aplicarlos en casos concretos. Aprenderá los protocolos basados en conjuntos de estados no ortogonales, y los estados entrelazados. También los diferentes protocolos, incluido el sistema ID-3000 de id-Quantique.

Conocer las entidades certificadoras, autenticación y certificación.

Describir la lógica de algoritmos cuánticos.

Conocer e implementar redes de distribución cuántica de claves.

Aprenderá los detalles de desarrollo de un diseño de proyecto, requisitos e implementación, así como las vulnerabilidades, y los ataques conocidos como Dropping, Man-in-the-middle y Photon Number Splitting.

Preparar a los egresados de este Posgraduate, para trabajar de forma competente y segura como profesionales en este novedoso método

criptográfico y para satisfacer las demandas de este sector profesional.

Finalmente, todos nuestros egresados, podrán inscribirse, de forma opcional, como miembros numerarios en el General Registry of the European Union Professionals, que le permite estar informado de su sector profesional estudios de mercado, oportunidades laborales internacionales, y un registro profesional de gran reconocimiento a nivel empresarial, siendo una insignia diferenciadora, en cualquier sector laboral. +Información: http://www.registrogeneralprofesionales.eu

PARA QUE TE PREPARA

1.- Como investigadores en Criptografía Cuántica.

2.- Trabajar en Empresas de Seguridad Informática.

3.- Trabajar en Centros de Enseñanza.

SALIDAS LABORALES

Podrá desarrollar sus funciones como consultores, o auditores de seguridad informática empresarial, bien en entidades públicas y privadas o en el ejercicio libre de la profesión (freelance) y en la comunidad a través de empresas especializadas.

PROGRAMACION:

¡Inscríbete Ya!

I. Introducción: Criptografía Cuántica Aplicada

1.1. Un poco de historia.

1.1.1. Cronología.

1.2. Conceptos previos.

1.2.1. Principios de incertidumbre y teorema de no-clonación.

1.2.2. Superposición y entrelazamiento.

II. Sistema. Protocolos.

2.1. Consideraciones previas.

2.2. Protocolos basados en conjuntos de estados no ortogonales.

2.2.1. BB84.

2.2.2. B92.

2.2.3. Estados trampa. (Decoy states).

2.2.4. SARG04 (versión prepara-y-mide).

2.3. Protocolos basados en estados entrelazados.
2.3.1. E91.

III. Implementación a nivel físico.

3.1. Componentes del medio físico.
3.1.1. El fotón.
3.1.2. Emisor de fotones.
3.1.3. Detector de fotones,
3.1.4. Canal de comunicación.

3.2. Codificación.
3.2.1. Fase vs. polarización.
3.2.2. Codificación con polarización.
3.2.3. Codificación en fase.

3.3. Estrategias de conexión.
3.3.1. La idea original.
3.3.2. Sistemas de dirección única (one-way).
3.3.3. Sistemas de doble dirección o Plug and Play (two-ways).
3.3.4. Fuente común.

3.4. El sistema ID-3000 de id-Quantique.
3.4.1. Arquitectura del sistema.
3.4.2. Secuencia de funcionamiento.

IV. Arquitectura.

4.1. Intercambio de una clave.
4.1.1. Intercambio de una clave en bruto.
4.1.2. Reconciliación de bases.

4.2. Entropía y error.
4.2.1. Entropía de la clave reconciliada.
4.2.2. Error cuántico o ruido.
4.2.3. Límite de seguridad.

4.3. Destilación de la clave.
4.3.1. Corrección de errores.
4.3.2. Amplificación de la privacidad.

4.4. Estimación de la información de un espía.
4.4.1. Entropía de Bennett et al.
4.4.2. Entropía de Slutsky et al.
4.4.3. Otras estimaciones.

4.5. Autenticación.

4.6. Conclusiones.
4.6.1. Evolución de la clave.

V. Implementación del software.

5.1. Entorno de desarrollo.
5.1.1. Control de versiones.

5.2. Diseño del proyecto.
5.2.1. Estructura.
5.2.2. Sincronización.

5.3. Requisitos estructurales.
5.3.1. Sistema de ficheros.
5.3.2. Puertos USB.

5.4. Ejecución.
5.4.1. Medición de la línea.
5.4.2. Resultados.
5.4.3. Registros de información.

VI. Integración. Redes.

6.1. Cifrado y distribución actual de claves.
6.1.1. Cifrado asimétrico o de clave pública.
6.1.2. Cifrado de Vernam.
6.2. Integración con los sistemas de cifrado actuales.
6.2.1. IPsec. Seguridad a nivel de red, IP.
6.2.2. SSL. Seguridad a nivel de transporte, TCP.
6.2.3. SSH. Seguridad a nivel de aplicación.

VII. Redes de distribución cuántica de claves.

7.1. Punto a punto. Red privada virtual.
7.2. Anillo de distribución.
7.3. Configuración en estrella.

7.4. Canal compartido.
7.4.1. Conmutadores ópticos.
7.4.2. Multiplexación en frecuencia.

7.5. Topologías en QKDN.

7.5.1. Topología en anillo.
7.5.2. Topología en estrella.
7.5.3. Topologías híbridas.

7.6. Intercambio a 3 bandas.
7.7. Niveles de una red QKD.

7.8. Componentes en una red QKD funcional.
7.8.1. Red principal. Backbone.
7.8.2. Redes de acceso.

VIII. Autenticación y certificación.

8.1. Entidad certificadora.
8.1.1. Almacén cuántico de claves.

8.2. Certificación.
8.3. Un escenario futuro/real.

IX. Ataques y vulnerabilidades.

9. Ataques.
9.1. Condiciones.

9.2. Estrategias para el ataque.
9.2.1. Intercepta y reenvía. (Dropping, Man-in-the-middle).
9.2.2. División del número de fotones. (Photon Number Splitting).

9.3. Ataques experimentales.
9.4. Otras estrategias para la realización de ataques.

X. Vulnerabilidades.

10.1. Aleatoriedad.
10.1.1. El generador de números aleatorios.
10.1.2. Distribución de las detecciones.

10.2. Pulsos fantasmas.
10.2.1. Una situación real.

XI. Apéndice.

11. Perspectivas de futuro.
11.1. Focos de investigación.

A. Definiciones y demostraciones.
A.1. Resumen de algunas definiciones importantes.
A.2. Demostraciones193

B. Referencias.
B.1. Referencias externas.
B.1.1. IPsec.

B.2. Aclaraciones sobre la distribución cuántica de claves.
B.3. ITU-T Recommendation G.694.
12. Evaluación, Conclusión y Clausura del Programa.

Acceso a TDR (Contenido Digital en Formato PDF) en el Campus Virtual utilizando las credenciales de CIU Cambridge International University.

¡Inscríbete Ya!

DURACIÓN DEL POSTGRADO

Puede estudiar a su ritmo al tratarse de un programa a distancia.

Está valorado en 45 Créditos equivalente a 450 horas lectivas.

MATERIAL DE ESTUDIO Y RECURSOS DEL POSTGRADO

Unidades didácticas clasificadas por áreas de estudio:

Guía didáctica: “Manual de Instrucciones” del Posgraduate Degree.

Todo el material necesario para el estudio del Posgraduate of Science in Quantum Cryptography, estará disponible en formato impreso o a través del campus virtual de la CIU Cambridge International University.

Cualquier material complementario será accesible a través del Campus Virtual.

Para preparar los contenidos que le serán exigidos usted dispondrá de materiales específicamente preparados para este Posgraduate Degree (guía de la metodología de uso del campus virtual, guía didáctica, temario y ejercicios de evaluación).

Bibliografía suministrada: El material de estudio específicamente para este programa consta de:

- Applied Quantum Cryptography (Criptografía Cuántica Aplicada). Formato: PDF o Impreso, Autor: Vicente Martín Ayuso, Jesús Martínez de Mateo, Editorial: (GIICC – Grupo de Investigación en Información y Computación Cuántica). Pág.: 214 Pág.
- Computación y Criptografía Cuántica; Introducción. Formato: Video en Línea o Mp4, Autor: Jesús García.

Campus Virtual: Se facilitan las credenciales del Campus Virtual, para el acceso a los recursos de apoyo al estudio: Acceso a Zona de Evaluación Calificación, Acceso a Bases Documentales, Especializadas como fuente de consulta, Videoteca, Anexos, Posibilidad de abrir foros y asociarlos al programa, Zona de Tesis, que permite la gestión íntegra de esta hasta su presentación ante el Comité de Evaluación designado, etc.

Se incluye una programación audiovisual, para la correcta utilización y aprovechamiento de los recursos disponibles en el Campus Virtual.

MODALIDAD DE ENSEÑANZA

Este programa está disponible en la modalidad o modalidades, indicadas a continuación:

A distancia. El alumnado recibirá el material de estudio impreso, y debidamente encuadernado, junto a la Guía de Metodología de Estudio, y asignación del Tutor. También se facilitan las credenciales de acceso al Campus Virtual, para el acceso a los recursos programados para el proceso de evaluación.

Online. Las acciones formativas están diseñadas para propiciar el fomento de las habilidades, conocimientos y experiencias relevantes para el desarrollo profesional dentro del ámbito de la temática del Posgraduate of Science in Quantum Cryptography.

TUTORIAS

Al comenzar el programa del Postgrado se asignará al alumno el tutor del área correspondiente, con el que seguirá el programa del curso hasta su finalización. Para ello se pone a su disposición el correo electrónico, que el tutor atenderá de manera personalizada..

TITULACION

CIU Cambridge International University promociona sus propios Certificados y Diplomas en idioma inglés, por lo que una vez superado el proceso de evaluación, y calificado por la Comisión Académica se extenderá el respectivo certificado de estudios y Título de Posgraduate Degree, al alumno que acredita su realización y superación del mismo.

Por lo tanto, al finalizar la Postgrado el alumno recibirá la Certificación que avala los conocimientos adquiridos a través de los estudios realizados: **Posgraduate of Science in Quantum Cryptography / Diplomado de Ciencias en Criptografía Cuántica**

Todas las titulaciones pueden ser entregadas debidamente legalizadas y apostilladas, con su Diploma, Certificado de Estudios y Certificado Académico.

Titulación Acreditada por la Comisión Internacional de Formación de CUE University Euroamerican Consortium.

En la Universidad Internacional Abierta Generalísimo Sebastián Francisco de Miranda y Cambridge International University, el nivel de DIPLOMADO es concedido después de la terminación satisfactoria de un programa de entre 30 / 45 créditos, equivalente a 300 y 450 horas, respectivamente. Este nivel es designado a nivel internacional de diferentes formas. Está catalogado en los niveles académicos privados, y en el área de postgrado.

Todas las titulaciones están acreditadas por la Comisión Internacional de Formación de CUE University Euroamerican Consortium. Una vez en posesión del Expert Postgraduate el egresado puede optar al nivel de Master a través de la oferta disponible en el sitio web de UNIAGSFMI Universidad Internacional Abierta Generalísimo Sebastián Francisco de Miranda o CIU Cambridge International University.

TASAS ACADÉMICAS Y ADMINISTRATIVAS

Postgraduate completo al contado:		**UE€ 450**
Postgraduate fraccionado:		3 cuotas a **UE€ 200** = **UE€ 600**
Gastos de envío*	España UE€ **35**	Internacional UE€ **85**
**Tasa académica especial fraccionada Delegación UNIAGSFMI		
		2 cuotas de UE€ 200 + 1 cuota de 50 = **UE€ 450**

* Solo modalidad A distancia (textos impresos remitidos por correo postal certificado). Los gastos de Registro y apostille no están incluidos en estos pagos.

** Solo optan por esta tasa especial los que cancelen y se inscriban en la Delegación UNIAGSFMI

FORMA DE PAGO

¡Inscríbete Ya!

Puede utilizar los siguientes recursos:

1. Transferencia Bancaria

2. Criptomoneda (Tenemos Punto de Venta)

3. Zelle

SOLICITUD DE ADMISIÓN

¡Inscríbete Ya!

La solicitud de admisión tiene cuatro pasos:

1. Debe Registrarse en Uniagsfmi.com
2. Llenar y enviar el formato digital **--Datos de inscripción--**
3. Utilice el correo electrónico Uniagsfmi.cloud@gmail.com para realizar el envío de los siguientes documentos:
   - Digitalización de la Cedula o Documento de Identidad.
   - Digitalización de una fotografía tamaño carnét.
   - Curriculum Vitae indicando el o los títulos de pre y postgrado que posee, así como su experiencia profesional. *

** En la valoración de su solicitud de admisión la experiencia académica y profesional que aparece en su Curriculum es muy importante así que recomendamos hacerla de manera detallada, existe la posibilidad de solicitarle documentación adicional.*

4. Culminado este proceso anterior recibirá la aceptación de su admisión a la formación requerida mediante un correo electrónico. A partir de esta confirmación, puede proceder a

formalizar su matriculación cancelando las Tasas Académicas y Administrativas respectiva.

CONTACTO

Puede comunicarse con los diferentes departamentos, mediante los datos siguientes:

Universidad Internacional Abierta Generalísimo Sebastián Francisco de Miranda - Sede Principal para los Países de Habla Hispana
Instagram@uniagsfmi.es
Teléfono – Wasapp : (+58) 412 796 33 84
EMail: info@ uniagsfmi.com
URL: http://www. uniagsfmi.com

NOTA IMPORTANTE:

La Doble titulación es para quienes se inscriben y cancelan sus cuotas a través de UNIAGSFMI como Universidad Delegada, quien se inscribe y cancelan sus cuotas directamente en la plataforma de CIU quedará sujeto a la normativa de esa universidad española sin derecho a reclamo alguno y rechazará la doble titulación.

Cambridge International University - Sede Principal para los Países de Habla Hispana

Línea Telefónica 1: (+34) 952 307 915

Línea Telefónica 2: (+34) 670 612 202

Fax: (+34) 952 277 020

E-Mail: ciu@ciu-edu.org

URL: https://www.ciu-edu.org

Cambridge International University

Universidad Internacional Abierta Generalísimo Sebastián Francisco de Miranda