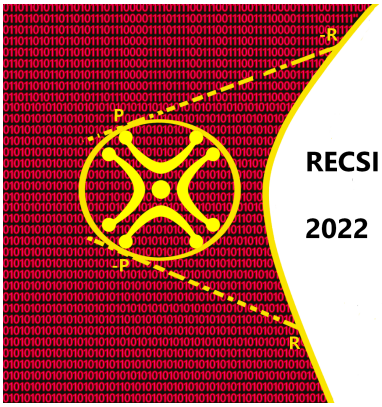
XVII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2022)

Santander, 19-21 October 2022



recsi2022.unican.es

PROGRAMME

The XVII RECSI will be held at the ETS de Ingenieros Industriales y de Telecomunicación of the Universidad de Cantabria, located at Avenida de Los Castros s/n

The academic program will consist of one opening talk, three plenary talks (50 minutes), three semi-plenary talks (30 minutes), 42 contributed talks (20 minutes), and 2 poster talks (10 minutes).

Lunches will be in restaurant Palacio del Mar, a 15 minutes walk from the conference venue. The shuttle service from conference venue to restaurant will leave at 13:15. To return the shuttle will leave from restaurant at 14:45.

The social dinner will be in Gran Casino de Santander, also called *Gran Casino Sardinero* and very close to the famous beach of the same name.

The Welcome Cocktail will be in Palacio la Magdalena on Wednesday 19th. The shuttle service from *Gran Casino de Santander* to *Palacio de la Magdalena* will leave at 19:45. To return will leave at 22:00.

On Friday 21th, at 17:30, the bus will depart from the conference venue for the visit/dinner to *Santillana del Mar/Palacio de Mijares*.

Proceedings

The proceedings of the conference are published by the Publishing House of the University of Cantabria. You can directly download the pdf or access the proceedings page from the publisher.

50UC Universidad de Cantabria
CCN centro criptológico nacional
E.T.S. Ing. Industriales y de Telecomunicación Universidad de Cantabria
SANTANDER CONVENTION BUREAU
SANTANDER CIUDAD

Outline of schedule

XVII

Reunión Española sobre Criptología y Seguridad de la Información

Santander - 2022

Miércoles - 19 Octubre

09:00 INAUGURACIÓN Francisco Javier Azcondo Luis Jiménez

09:30 Gerhard Frey, "Diffie-Hellman type key exchanges, history and future before and with quantum computing

10:30 Pausa Café

11:00 Protocolos criptográficos Detección y ciberdefensa

13:00 Comida - Palacio del Mar

15:00 Detección y ciberdefensa Seguridad en redes y ciberseguridad

16:00 Pausa Café

16:30 Blockchain

20:00

Palacio de la Magdalena

Jueves - 20 Octubre

09:00 Registro

09:30 Pino Caballero-Gil, "Seguridad hacia atrás. Seguridad hacia delante"

10:15 Pausa Café

10:45 Ciberseguridad y Sociedad

13:00 Comida - Palacio del Mar

15:00 IA en seguridad Blockchain

16:30 Pausa Café

17:00 Criptografía cuántica y postcuántica

20:30

Gran Casino de Santander

Viernes - 21 Octubre

08:30 Registro

09:00 Dario Fiore, "Vector Commitments: form Theory to Practice and Back Again"

10:00 Pausa Café

10:30 Privacidad y criptografía aplicada

11:35 Sesión Poster

12:00 Ciberseguridad

13:00 Comida - Palacio del Mar

15:00 Protocolos Criptográficos

17:30

Santillana del Mar
Palacio de Mijares

Wednesday, October 19

8:00-9:00	Registration – Hall Salón de Actos –	
	Salón de Actos	
9:00-9:30	OPENING • **Francisco Javier Azcondo**, Director ETS de Ingenieros Industriales y de Telecomunicación, Universidad de Cantabria. *Saludo de Bienvenida* • **Luis Jiménez**, Subdirector General del Centro Criptológico Nacional. *CNN y mundo académico. Un pilar de la seguridad TIC nacional*	
9:30-10:30	PLENARY TALK *Chair:* Maribel González-Vasco **Gerhard Frey**, University of Duisburg-Essen *Diffie-Hellman type key exchanges, history and future before and with quantum computing*	
10:30-11:00	Coffee break	
	Salon de Actos *Chair:* Josep Climent **Cryptographic protocols**	**Sala de grados** *Chair:* Miguel Soriano **Detection and cyber defense**
11:00-11:20	Oriol Alàs, Francesc Sebé and Sergi Simón *Anonymity and unlinkability in ring signature-based discussion boards*	Manuel Ruiz, Rubén Ríos, Rodrigo Román, Antonio Muñoz, Juan Manuel Martínez and Jorge Wallace *AndroCIES: Automatización de la certificación de seguridad para aplicaciones Android*
11:20-11:40	Sara D. Cardell, Verónica Requena and Amparo Fúster-Sabater *PN-secuencias entrelazadas de polinomios diferentes*	Margarita Robles-Carrillo and Pedro García-Teodoro *An Interdisciplinary Technical and Legal Analysis of Ransomware*
11:50-12:10	Branislav Petrovic, Balint Zoltan Teglasy and Sokratis Katsikas *Authenticated Encryption for Janus-Based Acoustic Underwater Communication*	Ángel Longueira-Romero, Jose Luis Flores, Rosa Iglesias and Iñaki Garitano *Gotta Catch 'em All: Aggregating CVSS Scores*
12:10-12:30	José Andrés Armario, Ronan Egan and Dane Flannery *Generalized partially bent functions and cocyclic Butson matrices*	Javier Correa-Marichal, Pino Caballero-Gil, Carlos Rosa-Remedios and Rames Sarwat-Shaker *Un estudio del DNIe y de su infraestructura*
12:40-13:00	Fabian Ricardo Molina Gomez and Consuelo Martínez López *Two Decoding Algorithms in Group Codes*	Jeimy Cano *Una guía metodológica para la elaboración de libros de jugadas*
13:00-15:00	Lunch break – Palacio del Mar –	

Wednesday, October 19

	Salon de actos *Chair:* Llorenç Huguet **Detection and cyber defense**	**Sala de grados** *Chair:* Daniel Sadornil **Network security. Cybersecurity**
15:00-15:20	José Ignacio Bengoechea-Isasa, Carles Ventura and Helena Rifà-Pous *Transferencia de aprendizaje en redes neuronales para mejora de un IDS*	Ana Isabel Gómez, Domingo Gomez and Andrew Tirkel *Ataques de correlación: Posibilidad de éxito en comunicaciones inalámbricas*
15:20-15:40	Sonia Díaz-Santos and Pino Caballero-Gil *Detección de somnolencia en conductores con un reloj inteligente*	Lilian Bossuet, Anis Fellah-Touta and Carlos Andres Lara-Nino *Auto-Aligned Remote Power Analysis through Ring Oscillator-based Sensors*
15:40-16:00	Aleksander Styrmoe and Slobodan Petrovic *Anomaly Detection Using Improved k-Means Clustering on Apache Flink*	Pablo Pérez, José Antonio Onieva and Gerardo Fernández *CCBHash (Compound Code Block Hash) para Análisis de Malware*
16:00-16:30	Coffee break	
	Salón de Actos *Chair:* David Megías **Blockchain**	
16:30-16:50	Joan Amengual Mesquida, Magdalena Payeras-Capellà and Macià Mut-Puigserver *Aplicación basada en Blockchain para una Lotería en línea con el uso de Tokens ERC-20 y ERC-721*	
16:50-17:10	Carles Anglés-Tafalla, Jordi Castellà-Roca and Alexandre Viejo *Seguridad y Privacidad en un Sistema de Control de Acceso Distribuido para Zonas de Bajas Emisiones*	
17:20-17:40	Adrià Torralba-Agell and Cristina Pérez-Solà *A Comparison of Layer 2 Techniques for Scaling Blockchains*	
17:40-18:00	Magdalena Payeras-Capellà, Macià Mut-Puigserver, Jordi Castellà-Roca, Jaume Ramis Bibiloni, Llorenç Huguet and Miquel-Àngel Cabot-Nadal *e-ticketing mediante NFTs*	
20:00-22:00	Welcome Cocktail – Palacio de la Magdalena –	

Thursday, October 20

9:00-9:30	Registration – Hall Salón de Actos –
	Salón de Actos
9:30-10:15	PLENARY TALK *Chair:* Josep Domingo-Ferrer **Pino Caballero-Gil**, Universidad de la Laguna *Seguridad hacia atrás. Seguridad hacia adelante*
10:15-10:45	Coffee break
	Chair: Luis Hernández Encinas **Cybersecurity technology and society**
10:45-11:15	Sergio Vidal, C4IN R&D Cybersecurity Center. Telefónica TECH. *Captura de amenazas en entornos industriales: en busca de El Dorado... sin saber dónde estamos*
11:20-11:55	Ana Isabel González-Tablas Ferreres, Universidad Carlos III & María Isabel González Vasco, Universidad Rey Juan Carlos I. *CRYPTO GO: una herramienta didáctica para aprender criptografía jugando*
12:00-12:40	José Manuel A. & Eduardo L. Coordinadores de los equipos de Evaluación y Certificación Criptológica, CCN. *CCN-PYTEC. Retos y Desafíos de la Evaluación Criptológica*
12:45-13:00	Group photo – Building main entrance –
13:00-15:00	Lunch break – Palacio del Mar –

Thursday, October 20

	Salon de actos *Chair:* Agustín Martín **AI in Security**	**Sala de grados** *Chair:* Jordi Castellà **Blockchain**
15:00-15:20	Victor Garcia-Font, Tanya Koohpayeharaghi, David Megías, Helena Rifà, Julián Salas and Jordi Serra-Ruiz *Arquitectura para la Detección de Noticias Falsas Basada en Watermarking y Machine Learning*	Amador Jaume, M. Francisca Hinarejos and Josep-Lluís Ferrer-Gomila *Esquema promocional sobre blockchain*
15:20-15:40	Xabier Saez de Camara, Jose Luis Flores, Urko Zurutuza, Cristóbal Arellano and Aitor Urbieta *Aprendizaje Federado con Agrupación de Modelos para la Detección de Anomalías en Dispositivos IoT Heterogéneos*	Sergio Chica, Andrés Marín, David Arroyo and Jesús Díaz *Protegiendo la identidad de las denuncias en un sistema abierto y auditable*
15:50-16:10	Mohammad Hossein Homaei, Andrés Caro Lindo, Jose Carlos Sancho Núñez, Óscar Mogollón Gutiérrez and Javier Alonso Díaz *The role of Artificial Intelligence in Digital Twin*	Cándido Caballero-Gil, Pino Caballero-Gil, Néstor Álvarez-Díaz and Moti Yung *Sistema de Votación Electrónica basado en Blockchain con Encriptación Homomórfica*
16:10-16:30	Alba Cruz Torres, Carlos Rosa-Remedio, Pino Caballero-Gil and Candelaria Hernández-Goya *Reconocimiento Facial e Identificación de Somnolencia en Conductores*	Rosa Pericas-Gornals, Magdalena Payeras-Capellà, Macià Mut-Puigserver and Llorenç Huguet *Sistema de gestión de certificados Digitales COVID-19 basado en blockchain*
16:30-17:00	Coffee break	
	Salón de Actos *Chair:* Amparo Fúster-Sabater **Quantum and post-quantum cryptography**	
17:00-17:20	Miguel Ángel González de la Torre, José Ignacio Sánchez García and Luis Hernández Encinas *Comparative analysis of lattice-based post-quantum cryptosystems*	
17:20-17:40	Marcos Valle-Miñón, Ana Quirce, Angel Valle and Jaime Gutiérrez *Quantum Random Number Generator based on Vertical-cavity Surface-emitting Lasers*	
17:50-18:10	José Daniel Escánez-Expósito, Pino Caballero-Gil and Francisco Martín-Fernández *Evolución de la librería QuantumSolver para el desarrollo cuántico*	
18:10-18:30	Diego José Abengózar Vilar and Carmen Sánchez Ávila *Diseño e implementación de un esquema criptobiométrico post-cuántico de protección de patrones. Aplicación en reconocimiento biométrico mediante mano*	
20:30-22:00	Social dinner – Gran Casino de Santander –	

Friday, October 21

8:30-9:00	Registration – Hall Salón de Actos –
	Salón de Actos
9:00-10:00	PLENARY TALK *Chair:* Domingo Gómez **Dario Fiore**, IMDEA Software *Vector Commitments: from Theory to Practice and Back Again*
10:00-10:30	Coffee break
	Chair: Francesc Sebé **Privacy and applied cryptography**
10:30-10:50	Jesús A. Manjón and Josep Domingo-Ferrer *Computación segura multiparte coútil para cálculo de funciones arbitrarias*
10:50-11:10	Rafael Genés-Durán, Oscar Esparza, Juan Hernández-Serrano, Fernando Román-García, Miquel Soriano and Jose L. Muñoz-Tapia *Comercio de datos con servicio de muestreo gratuito*
11:10-11:30	Patricia Guerra-Balboa, Àlex Miranda-Pascual, Javier Parra-Arnau, Jordi Forné and Thorsten Strufe *La Publicación de Trayectorias: un Estudio sobre la Protección de la Privacidad*
11:35-11:55	POSTER SESSION *Chair:* Ana Isabel Gómez • Noemi de Castro-García, David Escudero (Universidad de Leon) *Asignación multiclase de la severidad de IP mediante aprendizaje no supervisado* • Markel Epelde (Basque Center for Applied Mathematics). *Cardinal Rank Metric Codes and its cryptographic applications*
	Chair: Magdalena Payeras-Capellà **Cybersecurity**
12:00-12:20	Cristòfol Daudén-Esmel, Jordi Castellà-Roca and Alexandre Viejo *Sistema para la gestión automática de las políticas de privacidad y uso de las cookies*
12:20-12:40	Cándido Caballero-Gil and Jezabel Molina Gil *Análisis de ciberseguridad para cerraduras Inteligentes*
12:40-13:00	Adrian Tobar Nicolau, Javier Parra-Arnau and Jordi Forné *Ataques propios de las bases de datos de publicación continua en privacidad sintáctica*
13:00-15:00	Lunch break – Palacio del Mar –
	Chair: Juan Tena **Cryptographic protocols**
15:00-15:20	David Balbás, Daniel Collins and Phillip Gajland *Analysis and Improvements of the Sender Keys Protocol for Group Messaging*
15:20-15:40	José Luis Salazar, Julian Fernandez-Navajas, Jose Ruiz-Mas and Guillermo Azuara *Implementación de cifrado broadcast para mensajes cortos en WiFi*
16:50-16:10	Sebastià Martín Molleví, Marcel Fernández Muñoz and John Livieratos *Algoritmos para códigos separadores*
16:10-16:30	Raúl M. Falcón, N. Mohanapriya and V. Aparna *Minimizing the total number of shadows in secret sharing schemes based on extended neighborhood coronas*
16:30-16:31	CLOSING
17:30-22:00	Visit Santillana del Mar. Dinner Palacio de Mijares – Santillana del Mar –

List of talks

- **Opening talk:** Luis Jimenez, Subdirector General del Centro Criptológico Nacional.
  CNN y mundo académico. Un pilar de la seguridad TIC nacional

- **Plenary talks:**
  - Gerhard Frey, University of Duisburg-Essen.
    Diffie-Hellman type key exchanges, history and future before and with quantum computing
  - Pino Caballero-Gil, Universidad de La Laguna.
    Seguridad hacia atrás. Seguridad hacia delante
  - Dario Fiore, IMDEA Software.
    Vector Commitments: from Theory to Practice and Back Again

- **Semi-plenary talks:**
  - Sergio Vidal, C4IN R&D Cybersecurity Center, Telefónica TECH.
    Captura de amenazas en entornos industriales: en busca de El Dorado... sin saber dónde estamos
  - Ana Isabel González-Tablas Ferreres, Universidad Carlos III & María Isabel González Vasco, Universidad Rey Juan Carlos I.
    CRYPTO GO: una herramienta didáctica para aprender criptografía jugando
  - José Manuel A. & Eduardo L. Coordinadores de los equipos de Evaluación y Certificación Criptológica, Centro Criptológico Nacional.
    CCN-PYTEC. Retos y Desafíos de la Evaluación Criptológica

- **List of short talks:**
  1. Jeimy Cano. Una guía metodológica para la elaboración de libros de jugadas (playbooks) para riesgos cibernéticos
  2. Jesús A. Manjón and Josep Domingo-Ferrer. Computación segura multiparte coútil para cálculo de funciones arbitrarias
  3. Sara D. Cardell, Verónica Requena and Amparo Fúster-Sabater. PN-secuencias entrelazadas de polinomios diferentes
  4. Oriol Alàs, Francesc Sebé and Sergi Simón. Anonymity and unlinkability in ring signature-based discussion boards
  5. Margarita Robles-Carrillo and Pedro García-Teodoro. An Interdisciplinary Technical and Legal Analysis of Ransomware
  6. José Andrés Armario, Ronan Egan and Dane Flannery. Generalized partially bent functions and cocyclic Butson matrices
  7. Rosa Pericas-Gornals, Magdalena Payeras-Capellà, Macià Mut-Puigserver and Llorenç Huguet. Sistema de gestión de certificados Digitales COVID-19 basado en blockchain
  8. Diego José Abengózar Vilar and Carmen Sánchez Ávila. Diseño e implementación de un esquema criptobiométrico post-cuántico de protección de patrones. Aplicación en reconocimiento biométrico mediante mano
  9. Ángel Longueira-Romero, Jose Luis Flores, Rosa Iglesias and Iñaki Garitano. Gotta Catch 'em All: Aggregating CVSS Scores
  10. Sebastià Martín Molleví, Marcel Fernández Muñoz and John Livieratos. Algoritmos para códigos separadores
  11. Marcos Valle-Miñón, Ana Quirce, Angel Valle and Jaime Gutiérrez. Quantum Random Number Generator based on Vertical-cavity Surface-emitting Lasers
  12. Amador Jaume, M. Francisca Hinarejos and Josep-Lluís Ferrer-Gomila. Esquema promocional sobre blockchain
  13. Magdalena Payeras-Capellà, Macià Mut-Puigserver, Jordi Castellà-Roca, Jaume Ramis Bibiloni, Llorenç Huguet and Miquel-Àngel Cabot-Nadal. e-ticketing mediante NFTs
  14. Cándido Caballero-Gil and Jezabel Molina Gil. Análisis de ciberseguridad para cerraduras Inteligentes

15. Fabian Ricardo Molina Gomez and Consuelo Martínez López. Two Decoding Algorithms in Group Codes
16. Carles Anglés-Tafalla, Jordi Castellà-Roca and Alexandre Viejo. Seguridad y Privacidad en un Sistema de Control de Acceso Distribuido para Zonas de Bajas Emisiones
17. Cándido Caballero-Gil, Pino Caballero-Gil, Néstor Álvarez-Díaz and Moti Yung. Sistema de Votación Electrónica basado en Blockchain con Encriptación Homomórfica
18. Sergio Chica, Andrés Marín, David Arroyo and Jesús Díaz. Protegiendo la identidad de las denuncias en un sistema abierto y auditable
19. Miguel Ángel González de la Torre, José Ignacio Sánchez García and Luis Hernández Encinas. Comparative analysis of lattice-based post-quantum cryptosystems
20. Alba Cruz Torres, Carlos Rosa-Remedio, Pino Caballero-Gil and Candelaria Hernández-Goya. Reconocimiento Facial e Identificación de Somnolencia en Conductores
21. Pablo Pérez, José Antonio Onieva and Gerardo Fernández. CCBHash (Compound Code Block Hash) para Análisis de Malware
22. José Daniel Escánez-Expósito, Pino Caballero-Gil and Francisco Martín-Fernández. Evolución de la librería QuantumSolver para el desarrollo cuántico
23. Xabier Saez de Camara, Jose Luis Flores, Urko Zurutuza, Cristóbal Arellano and Aitor Urbieta. Aprendizaje Federado con Agrupación de Modelos para la Detección de Anomalías en Dispositivos IoT Heterogéneos
24. Aleksander Styrmoe and Slobodan Petrovic. Anomaly Detection Using Improved k-Means Clustering on Apache Flink
25. José Ignacio Bengoechea-Isasa, Carles Ventura and Helena Rifà-Pous. Transferencia de aprendizaje en redes neuronales para mejora de un IDS
26. Ana Isabel Gómez, Domingo Gomez and Andrew Tirkel. Ataques de correlación: Posibilidad de éxito en comunicaciones inalámbricas
27. Mohammadhossein Homaei, Andrés Caro Lindo, Jose Carlos Sancho Núñez, Óscar Mogollón Gutiérrez and Javier Alonso Díaz. The role of Artificial Intelligence in Digital Twin's Cybersecurity
28. Patricia Guerra-Balboa, Àlex Miranda-Pascual, Javier Parra-Arnau, Jordi Forné and Thorsten Strufe. La Publicación de Trayectorias: un Estudio sobre la Protección de la Privacidad
29. Joan Amengual Mesquida, Magdalena Payeras-Capellà and Macià Mut-Puigserver. Aplicación basada en Blockchain para una Lotería en línea con el uso de Tokens ERC-20 y ERC-721
30. Adrian Tobar Nicolau, Javier Parra-Arnau and Jordi Forné. Ataques propios de las bases de datos de publicación continua en privacidad sintáctica
31. Manuel Ruiz, Rubén Ríos, Rodrigo Román, Antonio Muñoz, Juan Manuel Martínez and Jorge Wallace. AndroCIES: Automatización de la certificación de seguridad para aplicaciones Android
32. Rafael Genés-Durán, Oscar Esparza, Juan Hernández-Serrano, Fernando Román-García, Miquel Soriano and Jose L. Muñoz-Tapia. Comercio de datos con servicio de muestreo gratuito
33. Cristòfol Daudén-Esmel, Jordi Castellà-Roca and Alexandre Viejo. Sistema para la gestión automática de las políticas de privacidad y uso de las cookies
34. Adrià Torralba-Agell and Cristina Pérez-Solà. A Comparison of Layer 2 Techniques for Scaling Blockchains
35. David Balbás, Daniel Collins and Phillip Gajland. Analysis and Improvements of the Sender Keys Protocol for Group Messaging
36. Branislav Petrovic, Balint Zoltan Teglasy and Sokratis Katsikas. Authenticated Encryption for Janus-Based Acoustic Underwater Communication
37. Javier Correa-Marichal, Pino Caballero-Gil, Carlos Rosa-Remedios and Rames Sarwat-Shaker. Un estudio del DNIe y de su infraestructura
38. Victor Garcia-Font, Tanya Koohpayeharaghi, David Megías, Helena Rifà, Julián Salas and Jordi Serra-Ruiz. Arquitectura para la Detección de Noticias Falsas Basada en Watermarking y Machine Learning

39. Lilian Bossuet, Anis Fellah-Touta and Carlos Andres Lara-Nino. Auto-Aligned Remote Power Analysis through Ring Oscillator-based Sensors
40. Raúl M. Falcón, N. Mohanapriya and V. Aparna. Minimizing the total number of shadows in secret sharing schemes based on extended neighborhood coronas
41. José Luis Salazar, Julian Fernandez-Navajas, Jose Ruiz-Mas and Guillermo Azuara. Implementación de cifrado broadcast para mensajes cortos en WiFi
42. Sonia Díaz-Santos and Pino Caballero-Gil. Detección de somnolencia en conductores con un reloj inteligente

- **List of poster talks:**
  - Noemi de Castro-García, David Escudero (Universidad de Leon).
    Asignación multiclase de la severidad de IP mediante aprendizaje no supervisado
  - Markel Epelde (Basque Center for Applied Mathematics).
    Cardinal Rank Metric Codes and its cryptographic applications