Data protection using optical encryption

John Fredy Barrera Ramírez

Professor

Optics and Photonic's Group

Physics Institute - Universidad de Antioquia

Medellín - Colombia

Universidad de Antioquia
Medellín - Colombia

Optics and Photonic's Group

Encryption

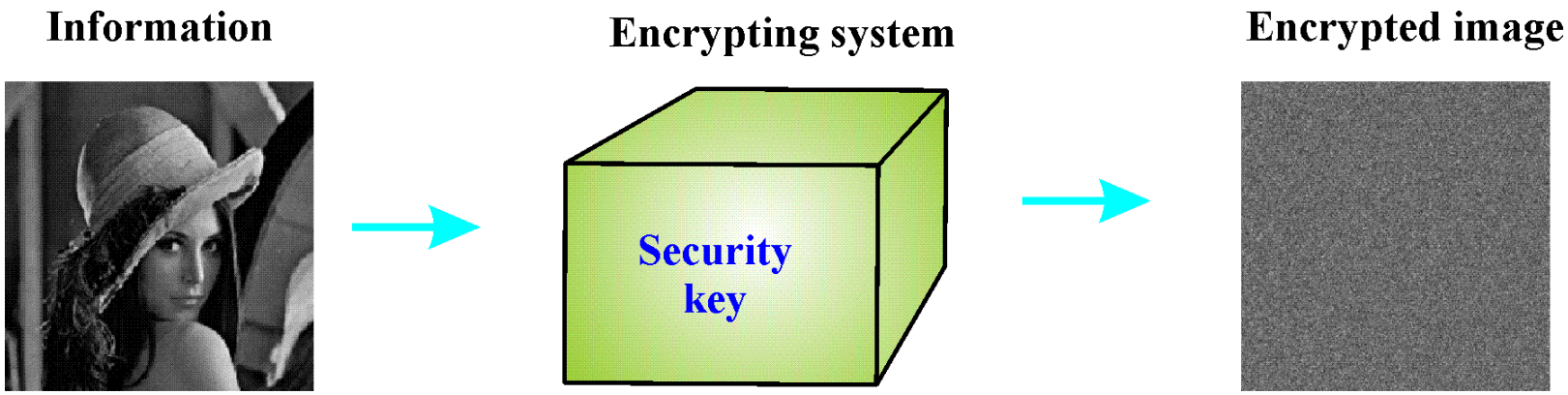
"Over the years many encrypting systems that were originally thought to be secure have finally been broken".

The optical processing is an alternative:

- Optical systems provide several degrees of freedom, thus increasing the security of the processes.
- A random physical key is an important element to protect information.

Encryption process

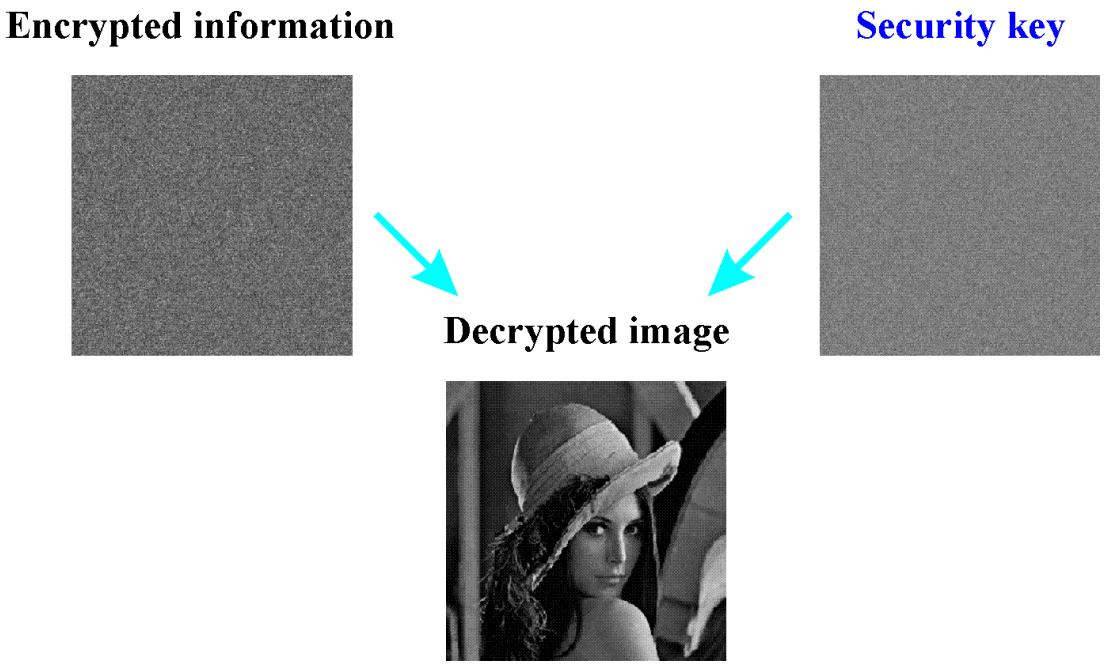
Encryption is the process of converting information in an unreadable data.



The encryption system contains an important element called security key. This element allows not only encrypting the information, but also recovers it when the encrypted information becomes available.

Decryption

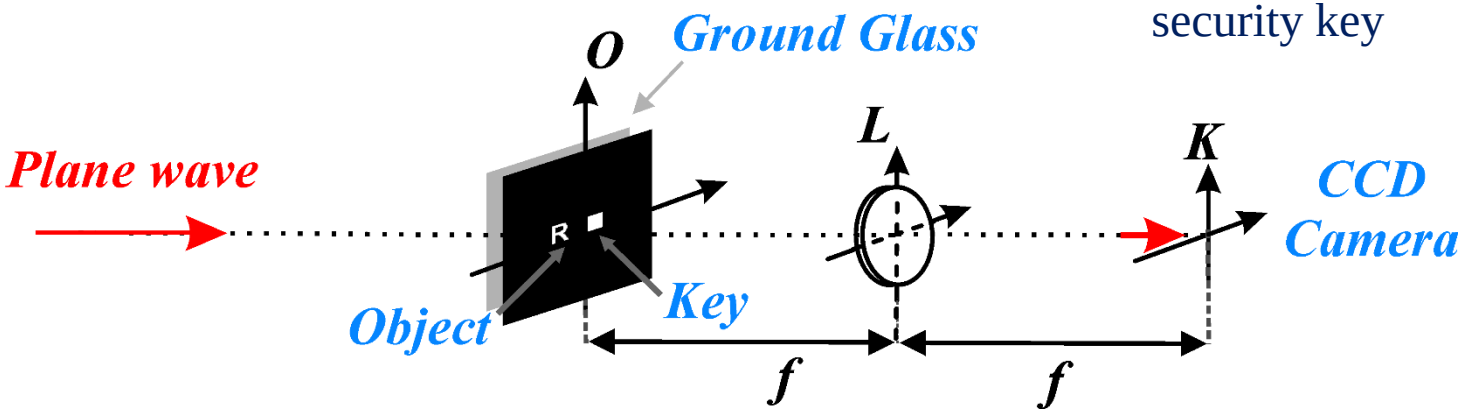
Decryption is the process of converting encrypted data back into its original form.

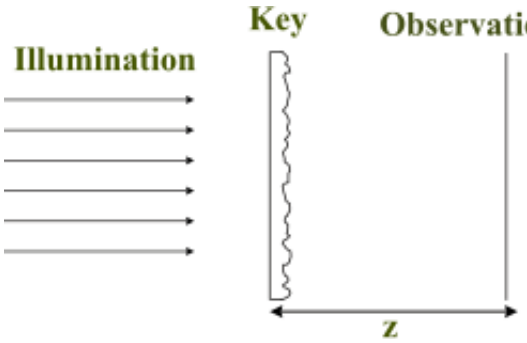


The information is recovered using together the encrypted information and the security key.

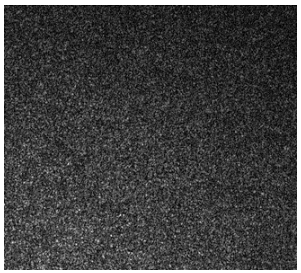
Encrypting system

Information of the security key





Pattern generated by the security key



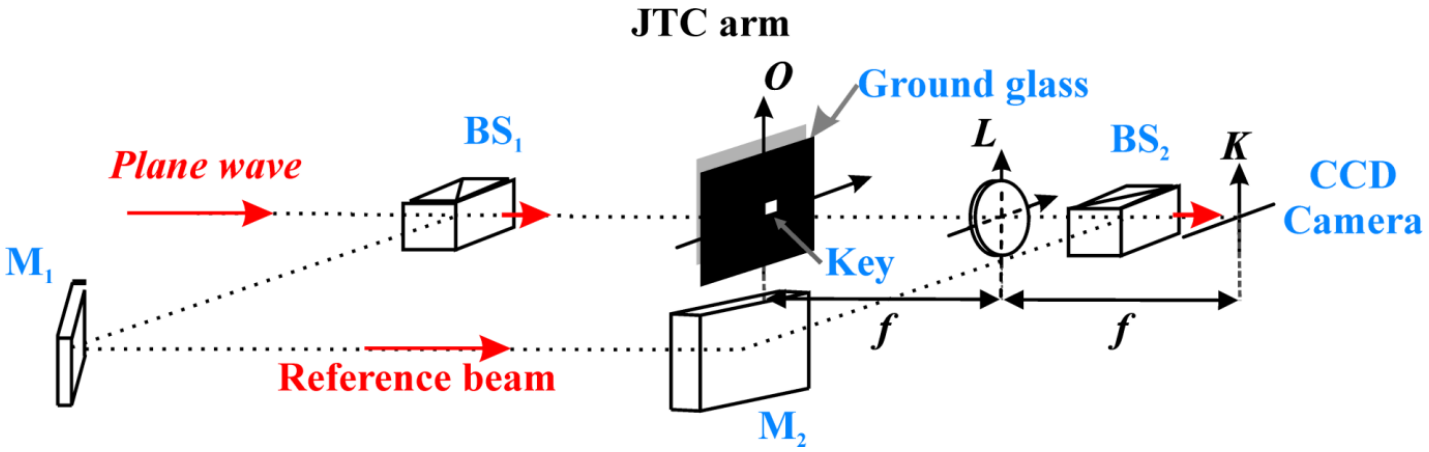
The joint power spectrum is processed to obtain the encrypted information

(a) **(b)**

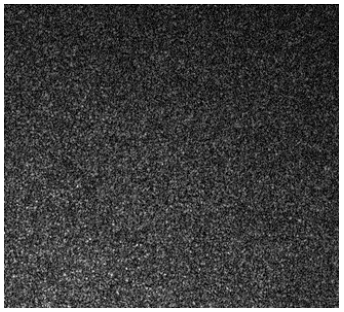
(a) Original object and (b) its corresponding encrypted version.

"Experimental analysis of a Joint Free Space Cryptosystem", J.F. Barrera R., A. Jaramillo, A. Mira, R. Torroba, Opt. Laser Eng. 83, 126-130 (2016).

Storing the information of the security key

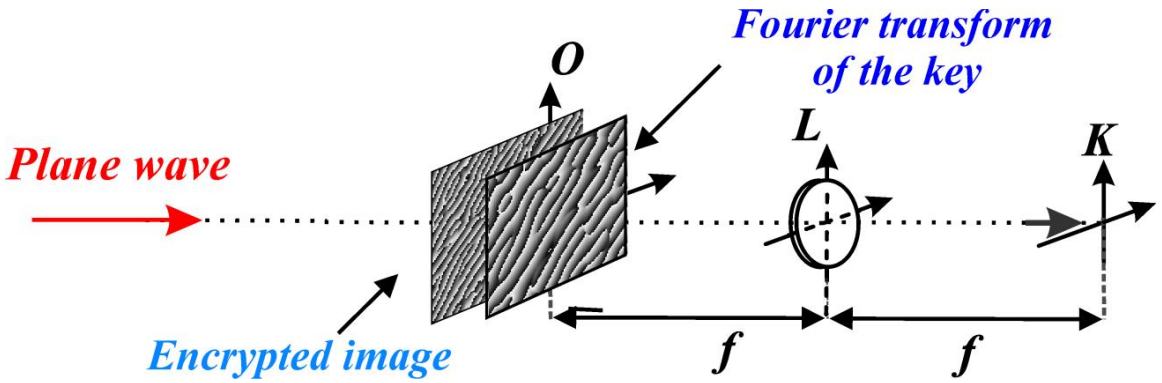


Information of the security key

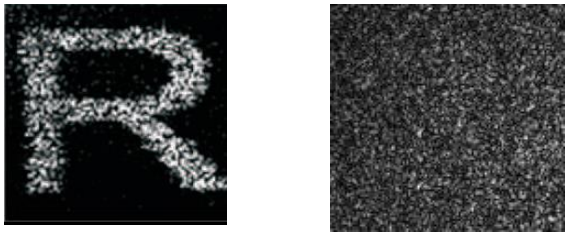


"Three-dimensional joint transform correlator cryptosystem", A. Vélez, J.F. Barrera R., R. Torroba, Opt. Lett. 41, 599-602 (2016).

Recovering system



Experimental results



(a) **(b)**

Recovering object with (a) the security key and (b) with another random phase mask.

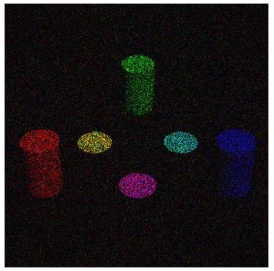
"Innovative speckle noise reduction procedure in optical encryption", A. Velez, J.F. Barrera R., R. Torroba, J. Opt. 19, 055704 (2017).

Experimental results: Decrypted information

Users: security and high fidelity recovering

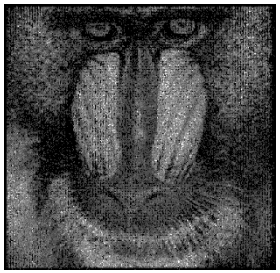
Character

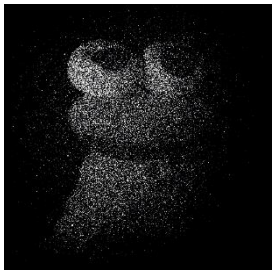
Binary movies and movies in color



Multiple data

Grayscale and 3D objects





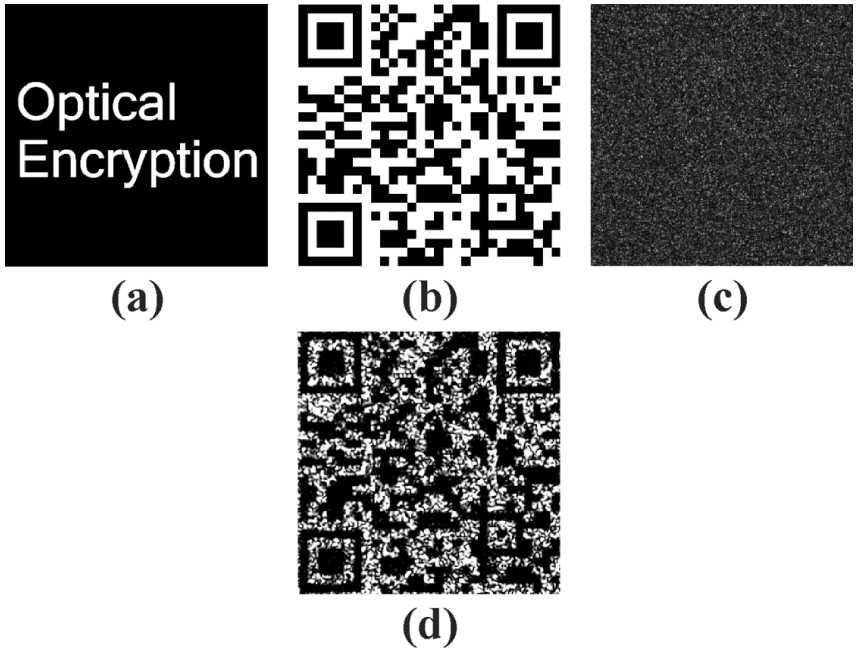
"Experimental optical encryption of grayscale information", A. Vélez, J.F. Barrera R., R. Torroba, Appl. Opt. 56, 5883-5889 (2017).

"Cryptographic salting for security enhancement of double random phase encryption schemes", A. Velez, J.F. Barrera R., R. Torroba, J. Opt. In Press (2017).

Eliminating noise

In summary, the optical encryption offers security and a wide range of possibilities, but for practical applications the noise produced in the optical processing has to be suppressed.

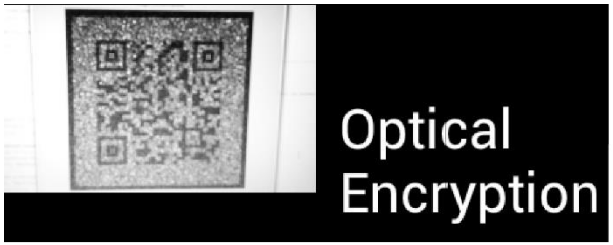
Merging optical encryption and QR coding



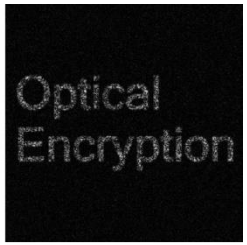
(a) Object y (b) its respective QR code, (c) encrypted QR code and (d) decrypted QR code.

"Optical encryption and QR codes: Secure and noise-free information retrieval", J.F. Barrera R., A. Mira, R. Torroba, Opt. Express 21 5373-5378 (2013).

Noise-free recovered information

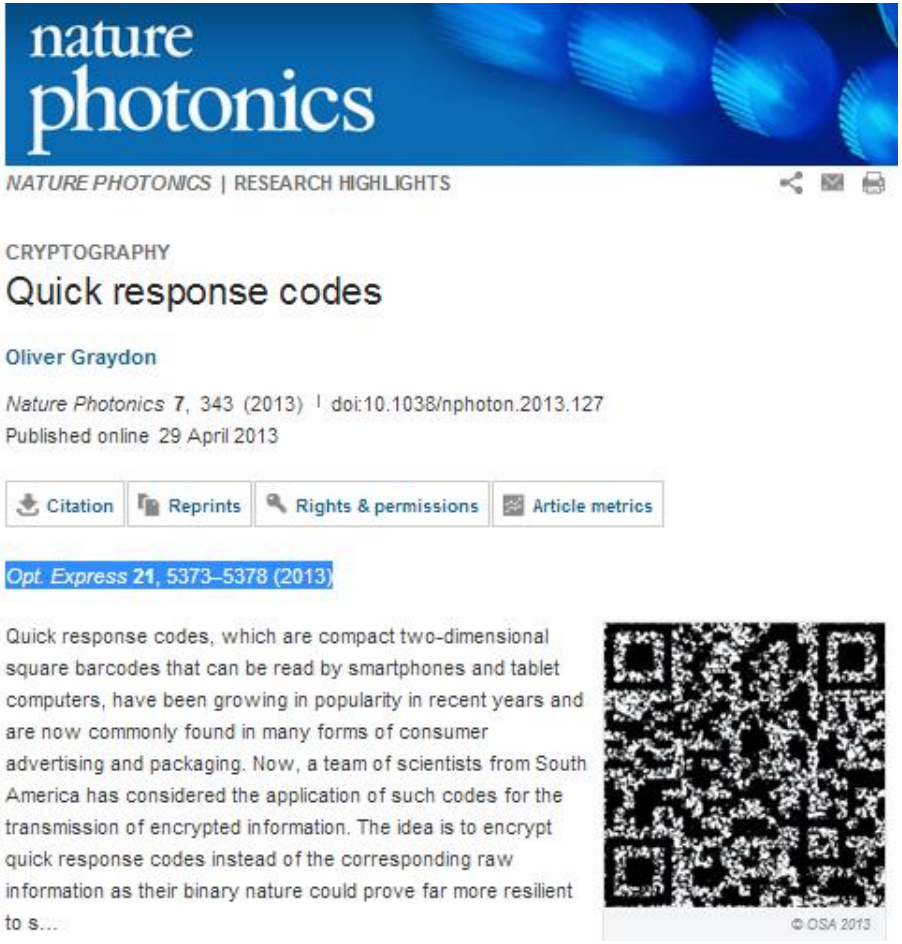


(a)



(b)

(a) Reading of the decrypted QR (reading with a smartphone) and (b) recovering whitouth including QR codes (conventinal method).



nature photonics

NATURE PHOTONICS | RESEARCH HIGHLIGHTS

CRYPTOGRAPHY

Quick response codes

Oliver Graydon

Nature Photonics **7**, 343 (2013) | doi:10.1038/nphoton.2013.127
Published online 29 April 2013

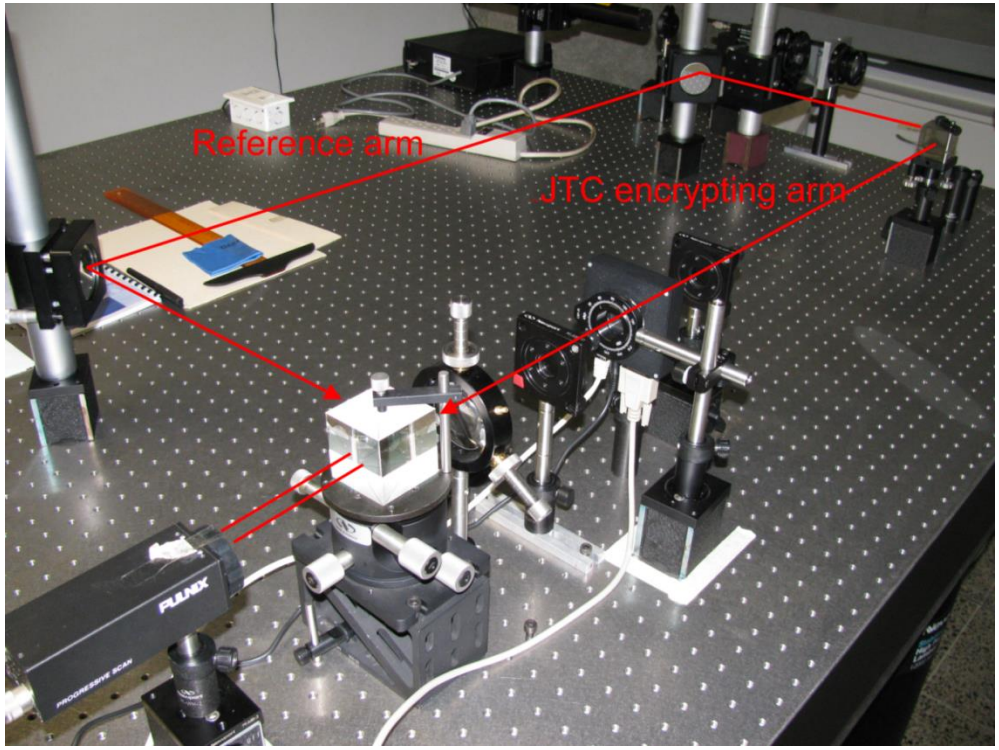
Citation | Reprints | Rights & permissions | Article metrics

Opt. Express **21**, 5373–5378 (2013)

Quick response codes, which are compact two-dimensional square barcodes that can be read by smartphones and tablet computers, have been growing in popularity in recent years and are now commonly found in many forms of consumer advertising and packaging. Now, a team of scientists from South America has considered the application of such codes for the transmission of encrypted information. The idea is to encrypt quick response codes instead of the corresponding raw information as their binary nature could prove far more resilient to s...

"The creative power of collaboration", S. Treacy, TWAS Annual Report 2002, The World Academy of Sciences (2013).

Experimental setup



Low-cost setup

Laser
Collimation system
Two beam sppliters
Two mirrors
Lens
CCD camera
SLM
Two polarizers
Diffuser

Patent: "Opto-physical apparatus and procedures for encrypting information and its recovering free of noise", J.F. Barrera R., A. Mira, R. Torroba (2015).

Collaborators

Universidad de Antioquia

Dr. Rodrigo Henao
Dr. Edgar Rueda
Dr. Alejandro Mira
PhD student, Msc Sorayda Trejos
Msc student, Alexis Jaramillo

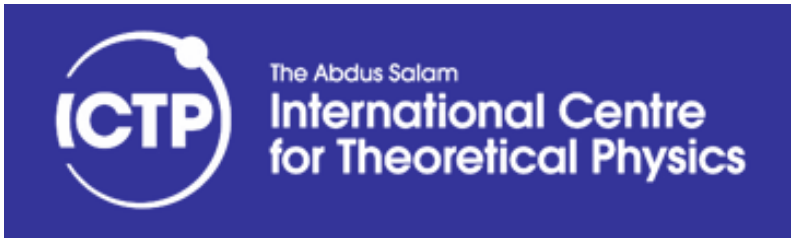
Centro de Investigaciones Ópticas (CIOp) – Argentina
Universidad Nacional de la Plata

Dr. Roberto Torroba
Dra. Myrian Tebaldi
Dr. Néstor Bolognini
PhD student, Alejandro Velez

University of New South Wales TFS - Australia
PhD student, Msc Carlos Vargas

Universidad de Oxford
Postdoc, PhD Carlos Ríos

Institutions




Thank you!!!