For the past years, I have been quite attracted by the many interesting challenges posed by Radio Frequency Identification (RFID) systems. I've focused my attention mostly in the needs of low-cost RFID tags, and their many security and privacy implications and shortcomings.

These devices, currently quite successfully present in multiple scenarios, are thought by many to become soon one of the most widely deployed and pervasive technologies. But providing them with a reasonable degree of security, to avoid some attacks and guarantee a good degree of privacy to its owners, is proving a very challenging task.

Over the last years, this field has become very active, with literally hundreds of proposals than in most cases are quite short-lived.

Furthermore, the field is particularly interesting because it has explored some completely new avenues that are unique to the area and could have many interesting applications in other scenarios, like distance bounding protocols and yooking proofs.

In this presentation I will take the opportunity to offer a general introduction to the field, and then show a very detailed account of how we cryptanalyzed one of the most promising recent protocols in the area. I will end with a note on other interesting security issues affecting the technology, that have implications from Implantable Medical Devices (IMDs) to e-Passports.