De Componendis Cifris

(Secondo Evento Conoscitivo)

Prof. Daniele Venturi
Dipartimento di Informatica

SAPIENZA
UNIVERSITÀ DI ROMA

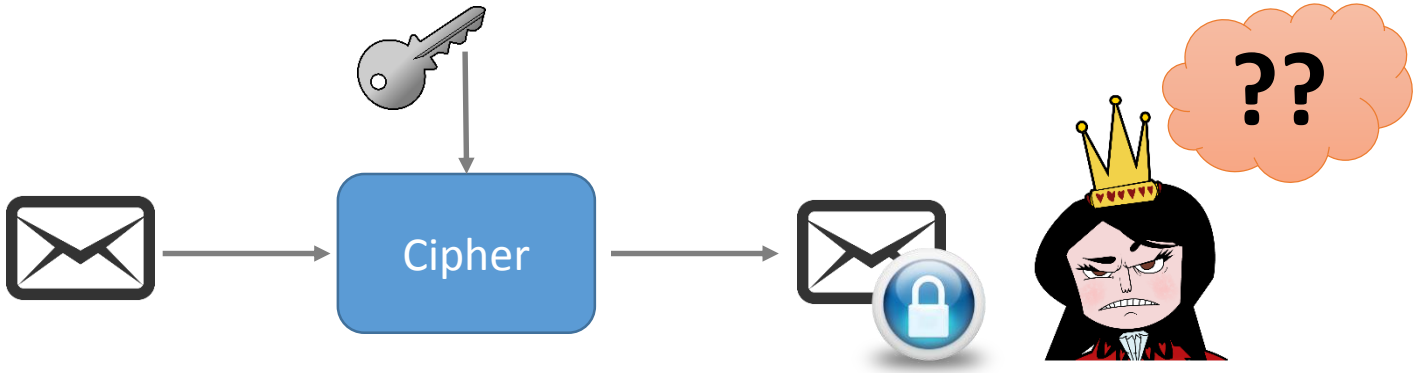
Roma, 22/01/2018

Curriculum Vitae

Year	Position	Institution
November 2008 – April 2012	PhD Student	SAPIENZA UNIVERSITÀ DI ROMA
November 2009 – November 2010	Visiting Researcher	CWI
January 2012 – September 2013	Postdoc	AARHUS UNIVERSITY
September 2013 – March 2016	Postdoc	SAPIENZA UNIVERSITÀ DI ROMA
April 2016 – December 2016	Assistant Professor (Tenure Track)	UNIVERSITÀ DEGLI STUDI DI TRENTO
December 2016 – Now	Assistant Professor (Tenure Track)	SAPIENZA UNIVERSITÀ DI ROMA

Research Focus: Provable Security

- Define security goal
  - E.g., for encryption



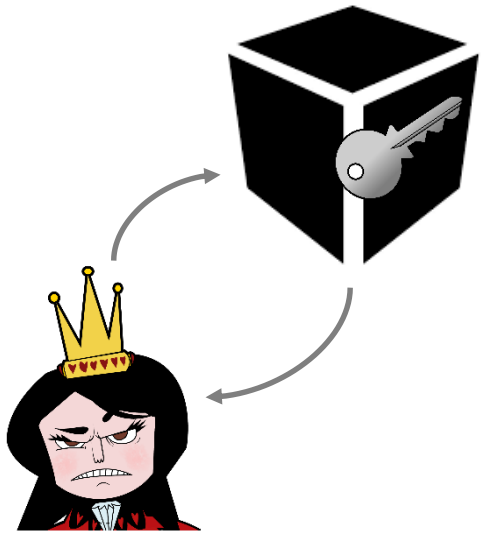
- Design cryptoscheme (e.g., RSA)
- Prove security (by reduction)

If well studied assumption holds (e.g., factoring is hard) → *Crypto scheme is secure*

  - Win-win situation

SAPIENZA UNIVERSITÀ DI ROMA

Research Goal I: Beyond-Black-Box Security



- Observe I/O behavior
  - Internals perfectly hidden
  - RSA believed as hard as factoring

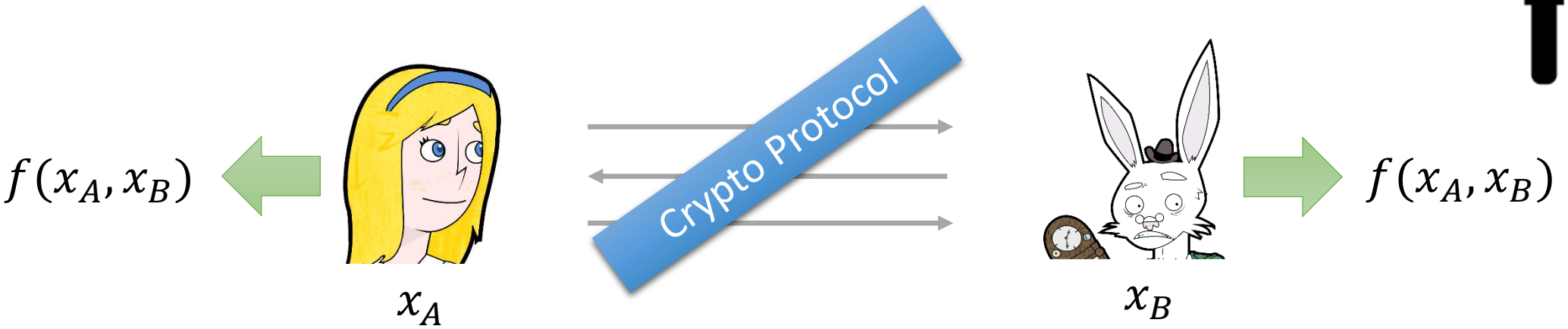
implement

- Devices can leak
- Devices can be faulty
  - Can break implementation within hours

How to Fix it?

- Non-malleable codes
  - Encode a secret in such a way that modifications to the encoded value either yield the original secret or a completely unrelated value
  - Publications at TCC 14-15-16, Eurocrypt 14, Crypto 17, JoC, …
- Leakage- and tamper-resilient cryptography
  - Direct constructions of cryptosystems resisting leakage and tampering attacks with the memory, based on number-theoretic assumptions
  - Publications at Asiacrypt 13, ICALP 15, Asiacrypt 16, JoC, …
- Post-Snowden crypto
  - Design cryptoscheme that remain secure even in the presence of cryptographic backdoors
  - Publication at CCS 15, JoC

Research Goal II: Secure Computation



Can Alice and Bob compute a function on their private inputs, without revealing anything beyond the output?

- Examples: Authentication, Pattern matching, cloud outsourcing, zero knowledge…
  - Publications at Eurocrypt 11, PKC 13, ICALP 13, PKC 16, …

Research Goal III: Distributed Ledgers

- Redactable Blockchain (Euro S&P 2017)
  - Making the blockchain mutable in case of emergency situations
  - Based on chameleon hashing
  - Patent together with Accenture
- Distributed Futures Exchange (S&P 2018 – to appear)
  - Security model for distributed futures market exchange
  - Protocol construction building on zcash
  - Patent application (soon)

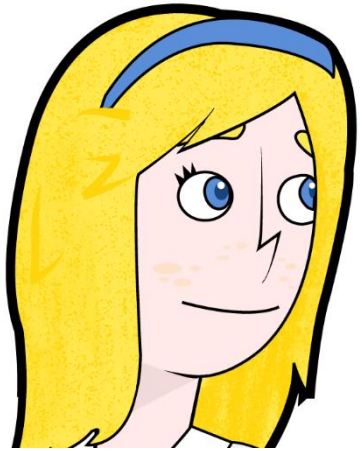
Research Group

- Besides myself
  - 1 full professor (Luigi V. Mancini) – focus on cybersecurity at large
  - 1 RTD-B (Angelo Spognardi) – focus on network security
  - Several PhD/Master students
- Active ongoing collaborations
  - New York University, Stevens Institute of Technology, Bar-Ilan University, TU Darmstadt, Ruhr University of Bochum, IBM Research, Microsoft Research, ETH Zurich, IMDEA Software Institute, UCLA, …

Teaching Activities (Crypto Related)

- Cryptography (6 CFU)
  - Master Degree in Cybersecurity, Computer Science (optional) and Mathematics (optional)
  - Content: One-way functions, pseudorandomness and randomness extraction, secret-key encryption and authentication, public-key encryption, digital signatures, identification schemes
- Secure Computation (6 CFU) – Co-taught with Prof. Riccardo Lazzeretti
  - Master Degree in Cybersecurity (optional)
  - Content: Fully-homorphic encryption, zero knowledge, oblivious transfer, garbled circuits, secret sharing, multi-party computation, cryptocurrencies

Thank You!



Read more at:

http://danieleventuri.altervista.org/