De Cifris incontra Milano

Milano-Bicocca – 11 settembre 2018

Blockchains, and the search for Cryptographic Boolean Functions

Alberto Leporati

Università degli Studi di Milano – Bicocca
Dip. di Informatica, Sistemistica e Comunicazione (DISCo)
Viale Sarca 336/14 – Milano - Italy

About me

- Associate Professor at the Department of Informatics, Systems and Communication (DISCo) of the University of Milan – Bicocca
- Founder and current director of Bicocca Security Lab
  - interests also in Cybersecurity
  - inside the lab, Luca Mariot and me have competencies on Cryptography
- Teacher of a course on Information Theory and Cryptography for the Master Degree on Computer Science, since 2008
- Supervisor of many bachelor (90+) and master (30+) theses
- Supervisor of two Ph.D. theses on Cryptography
- Supervisor of a post-doc research project on Cryptography
- Member of CINI Cybersecurity Lab (Milan – Bicocca node)

Bicocca Security Lab

- BiS Lab = Bicocca Security Lab
- Interdepartmental lab: Computer Science + Law
- The founders (from left to right):

  > Prof. Alberto Leporati (Computer Science)

  > Prof. Andrea Rossetti (Law)

  > Prof. Claudio Ferretti (Computer Science)

Bicocca Security Lab

BiS Lab activities

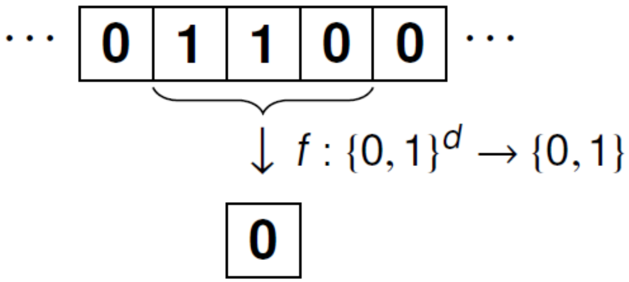
- Law assistance + security audits for private companies
  - Compliance with the new regulation and laws about data privacy (GDPR)
- Courses and dissemination of cybersecurity ideas and principles
  - Training courses for students
  - Participation to public events:
    - “MEETmeTONIGHT: Face to face with research”
    - Digital Week
    - Bookcity
- Participation to EU and Regional research calls

Research in Cryptography

- Theoretical foundations of cryptographic primitives
- Search for Boolean functions with good cryptographic properties: *k*-resiliency, nonlinearity, balancedness
- Relations with Secret Sharing Schemes, Orthogonal Arrays, combinatorial designs, linear codes
- Relations with parallel models of computation, mainly Boolean circuits and Cellular Automata

Research in Cryptography

- CA-based block cipher design:



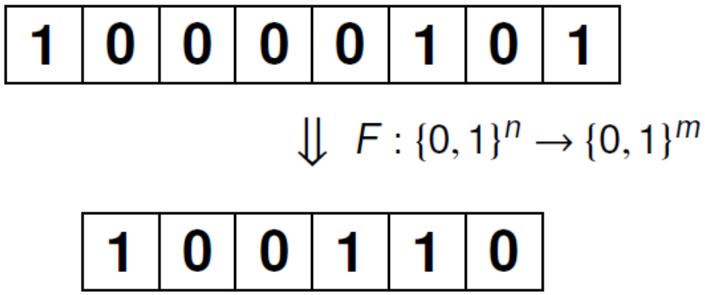
$$\cdots\ \boxed{0}\underbrace{\boxed{1}\boxed{1}\boxed{0}}\boxed{0}\ \cdots$$

$$\downarrow\ f:\{0,1\}^d \to \{0,1\}$$

$$\boxed{0}$$

- local rules are Boolean functions
- strong functions can be used for stream ciphers and for PRNGs

- global rules can be seen as S-boxes
- goal: find S-boxes with high nonlinearity and with low differential uniformity



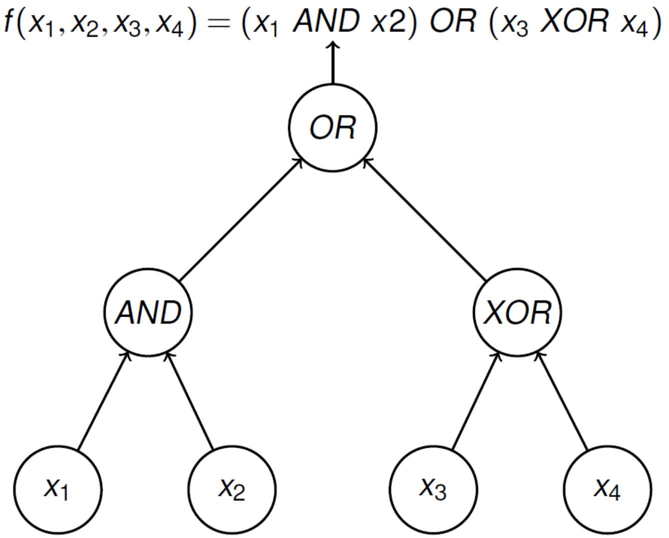
$$\boxed{1}\boxed{0}\boxed{0}\boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{1}$$

$$\Downarrow\ F:\{0,1\}^n \to \{0,1\}^m$$

$$\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{0}$$

Research in Cryptography

- The number of Boolean functions grows in a double exponential way wrt to the number n of inputs: 2^{2^n}. Exhaustive search becomes impossible
- Evolutionary techniques used: PSO, Genetic Algorithms, Genetic Programming
- Search spaces:
  - truth tables of Boolean functions
  - Walsh spectra of pseudo-Boolean real functions
  - trees of Boolean operators
- Example of encoding in GP:



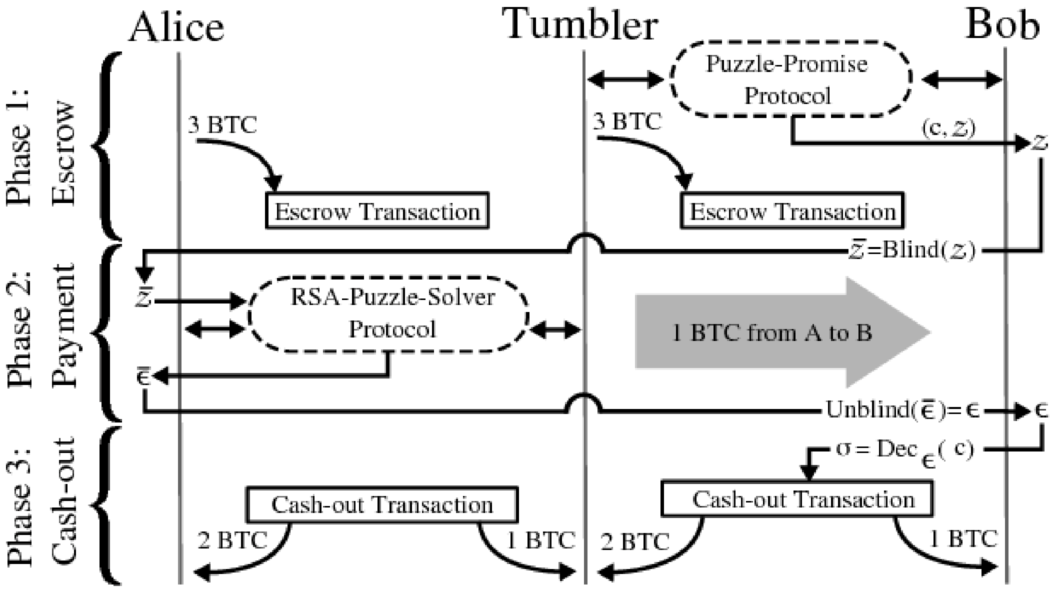
$f(x_1, x_2, x_3, x_4) = (x_1 \ AND \ x2) \ OR \ (x_3 \ XOR \ x_4)$

Research in Cryptography

- Results obtained:
  - for $n = 4$ and $n = 5$, we obtained CA rules inducing S-boxes with optimal crypto properties, and with implementation cost similar to or slightly better than the state of the art in the literature
  - for $n > 5$, GP finds S-boxes with optimal cryptographic properties up to $n = 7$, but with too high implementation costs
- In general, Genetic Programming seems to work better than Genetic Algorithms (Why?)

Blockchains: research

- Modification of the TumbleBit payment protocol:



  - in the context of permissioned blockchains
  - in order to obtain transferability of tokens between receivers
  - without making the two receivers linkable

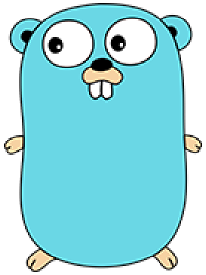
Blockchains: applications

- Design of blockchain-based applications
  - supply chain management
  - definition of utility (crypto) tokens backed by tangible assets
  - development of smart contracts with Ethereum (Solidity) and Hyperledger (Go Lang)

ethereum
BLOCKCHAIN APP PLATFORM

Solidity

HYPERLEDGER



Blockchains: applications

Two use cases:

- Anti-counterfeiting of luxury clothes and accessories, using a blockchain + RFIDs
  - each cloth / accessory has a unique RFID
  - every production / assembly / transportation / sell operation is written on the blockchain
  - it becomes incredibly difficult to sell counterfeit items!
- Storage of sensor data from (non-autonomous) vehicles
  - hashes of contents of the car's black box are regularly saved on the blockchain
  - when needed, the driver can prove that his/her data have not been altered

Thanks for your attention!

BiS Lab

bislab@unimib.it

Alberto Leporati

alberto.leporati@unimib.it