La *De Cifris* incontra Torino

Crittografia @UniMI: Applicazioni e Teoria

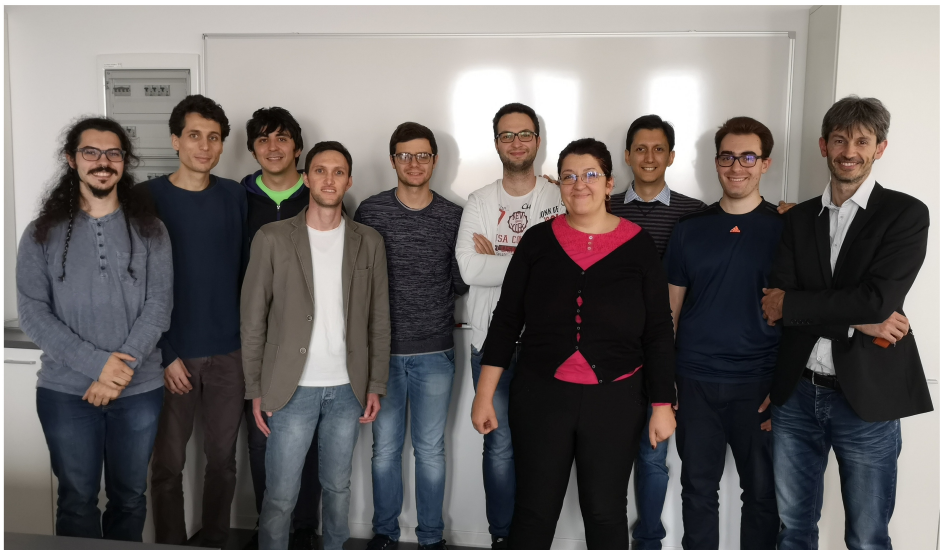
Andrea VISCONTI

Dipartimento di Informatica
Università degli Studi di Milano

Crittografia @UniMI: CLUB

CLUB (Cryptography and Coding) is ...

a research group @UniMI under the ombrella of System Security and Cryptography Lab: www.club.unimi.it



Activities: CLUB, October 2019

- 1 post-doc, 2 phd students, several students (MSc and BSc)
- Cryptowars 2018 and 2019, De Cifris Hackhaton 2019, ...

Overview

1. High-speed Cryptography
2. New crypto primitives
3. Blockchain and applications

High-speed Cryptography

High-speed Cryptography

Why is SW/HW **performance** so **important** for cryptography?

Efficient operations have high relevance both in HW and SW.

Usually **small speedups**: 3%, 5%, 10%.

Does the impact **justify the effort**?

High-speed Cryptography

A large **server farm**: –5/10% HW cost, –5/10% power cost, etc.

Constrained devices in the Internet of Things.

SW efficiency: data transfer cannot be bottlenecked by cryptography.

Could **careful implementation** of a cryptographic function improve performance?

It is possible to increase performance **by a factor of 10**!!

High-speed Cryptography

High-speed cryptography <==> High-speed **cryptanalysis**

To evaluate the **cipher strength** — e.g. computational resources required (time, memory, data)

To **try to gain access** to the contents of encrypted messages

Cryptanalytical implementations **do not take care about security**:

- clever **computer science tricks**;
- the choice of **specific mathematical structures**;

New crypto primitives

New crypto primitives

Cryptographic primitives are designed to protect data and keys in the **black-box attack model**, in which encryption/decryption operations cannot be tampered with.

These assumptions might not be applicable in some cases, for example DRM applications, Pay Tv, etc.

For this reason we refer to the **white-box model** as an attack model in which the adversary has total visibility of the software implementation of the cryptosystem, and full control over its execution platform.

New crypto primitives

White-Box Cryptography was originally defined as an obfuscation technique intended to implement cryptographic primitives in such a way that an adversary having full access to the implementation and execution platform is **unable to extract the key**.

Why should an adversary be interested in recovering the key?

... DRM applications: a **key recovery attack** would allow an adversary to illegally **redistribute contents** to non-subscribers.

New crypto primitives

2003–2011: White-Box implementations of **well-known cipher**.

These implementations are subjected to algebraic **attacks**, Differential Fault Analysis, Differential Computational Analysis, ...

Researchers have developed **dedicated** design approaches for white-box block ciphers.

PROS: interesting security properties.
CONS: efficiency could be a bottleneck.

Open problems: how to design a block cipher with a faster and secure key mixing.

Authclick srl: an example of a notary service

Blockchain and applications

Blockchain and Cryptography...

- Hash Functions
  - Collision-free (collisions exist but we are not able to find them)
  - Preimage resistant (non-reversible)
  - Second preimage resistant
- Digital signature
- Merkle tree (binary tree)
- Zero-knowledge
- ...

Blockchain and applications

Main idea

Art is a universal language. Why don't we share it?

We will **focus on young photographers** and their images.

We need to protect their artworks because

- photographers,
- auction houses,
- galleries,
- world's art collectors
- ...

may **have conflicting interests**!!

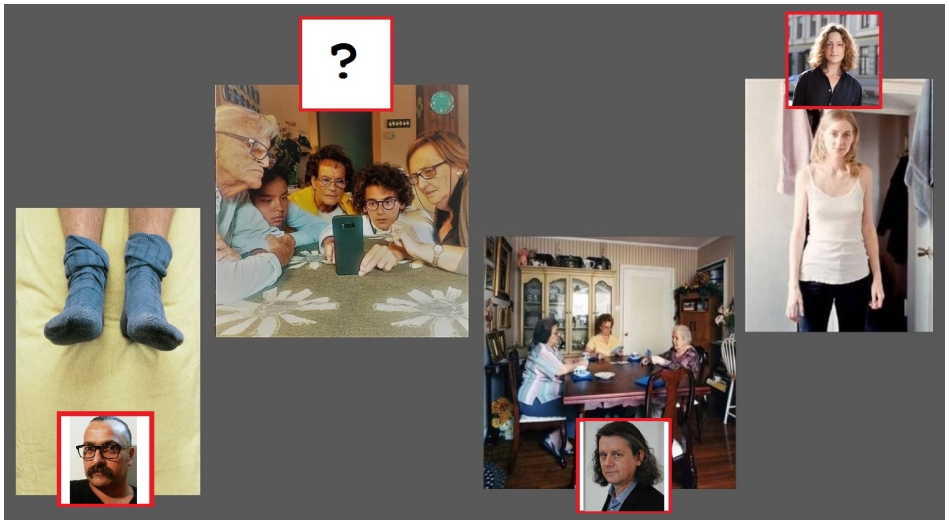
A simple challenge:

Which would you bet on? . . . without expertise!

Blockchain and applications

These images are not randomly chosen. Indeed...

Blockchain and applications



Alberto Balletti is an Italian artist.

? is a professor @UniMi.

Jeffrey Wall is a Canadian artist.

Vibeke Tandberg is a Norwegian artists.

Blockchain and applications

This simple challenge show us why **expertise is so important**.

A blockchain can be used **not only to store** the fingerprint of images!

We also need to store their **history**, what the viewer **observers**, **thinks**, and **feels** about these images.

. . . and to do so, we need to design and implement a smart contract application.

Thanks for your attention!

andrea.visconti@unimi.it
www.di.unimi.it/visconti