

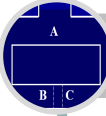

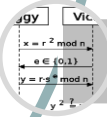





# Zero Knowledge Proofs

Sebastian Angermann - 2017

- 
Introduction
- 
Properties of Zero Knowledge-Protocols
- 
Example I  
Guillou-Quisquater's Analogy
- 
Example II  
The graph three coloring problem
- 
Example III Fiat-Shamir Identification
- 
Pros & Cons and Applications

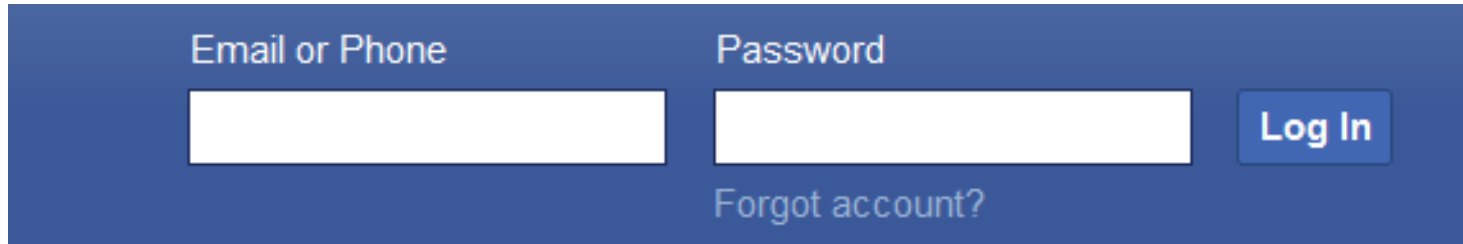


[Unsere Aufgaben](#) [Ihre Sicherheit](#) [Aktuelle Informationen](#) [Kontakt aufnehmen](#) [Karriere und Beruf](#) [Das BKA](#) 

[Startseite](#) → [Aktuelle Informationen](#) → [Aktuelle Meldungen](#) → [Meldungen](#) →  
Hacker-Sammlung gefunden: 500 Mio. E-Mail-Adressen und Passwörter betroffen

## Hacker-Sammlung gefunden: 500 Mio. E-Mail-Adressen und Passwörter betroffen

Datum: 06. Juli 2017



Email or Phone

Password

Log In

[Forgot account?](#)

1. Client (Prover) creates account at web server, chosen password is stored encrypted in data table as a hash.
  2. Client transmits password to log in.
  3. Server (Verifier) computes hash and compares with stored value.
  4. Server thus knows clearword password.
- Information leakage if Server is compromised.

1. Prior to Zero Knowledge cryptography research focused on the client side (dishonest prover).
2. What happens if you don't trust the verifier?

Tartaglia 1535 cubic equations:  $x^3+px=q$

*“I don't tell you my secret, but I will prove to you that I know the secret.”*

1985: Goldwasser, Micali, Rackoff:

„The Knowledge complexity of interactive proof systems“

- IBS: Abstract protocol that models computation as the exchange of two parties,  
A Prover who want to proof to a Verifier that a statement is true ( $x \in L$ ).
- Knowledge complexity measures the amount of additional information conveyed above „said statement is true“.

## **Completeness:**

The Verifier will always accept a proof from the Prover, given that they both follow the correct protocol.

## **2. Soundness:**

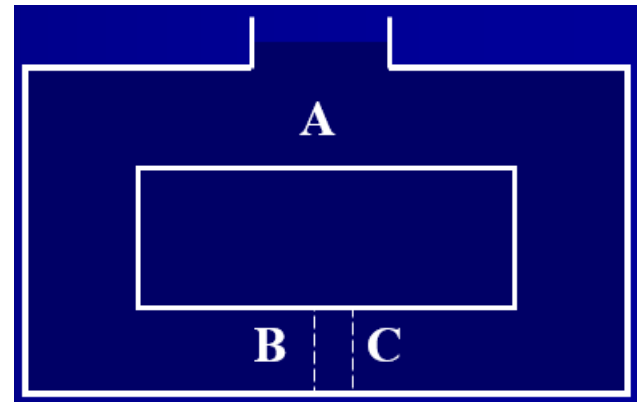
The Verifier will not accept any “incorrect” proof from the Prover, given that the Verifier follows the correct protocol.

## **3. Zero-Knowledge:**

During the whole “proving” process, the Verifier will learn nothing about the Prover’s secret, nor will he be able to prove that secret to any other party.

- Ali Baba (P) knows how to open a secret doorway that connects the dead ends B and C.
- He wants to impress a reporter (V) with this knowledge without telling the secret words
- They conduct a series of N verification experiments:
- P commits to go behind B or C unseen.
- V at A randomly calls out a side for P to come forth.
- The whole thing is recorded

### The Analogy of Ali Baba's Cave



If P cheats he will be exposed with  $(1-0,5)^N$  probability.



### Proof of ZK Property by Simulation:

- Another Reporter reenacts the proof with a look-a-like actor and records.
- Verification Experiment fails 50% of the time, those are cut out.
- Look-A Like does not know the secret and hence can't convey information.
- If both videos are indistinguishable the first can't either.

→ It is impossible for  $V$  to tell on  $P$  even though he is convinced  $P$  knows the secret!

- By performing a series of verification experiment, it is possible to prove that you know a certain secret without sharing it with anyone.
- Zero-Knowledge Protocols help prevent leaks of any secret information by not directly requesting the secret itself during verification.
- Zero-Knowledge Protocols won't care if you actually know the password or not, as long as you can prove that you know it.
- Faking the proof of knowing the secret is possible, but it has a low probability of success.

An IBS is a protocol  $(P, V)$  between a Prover and a Verifier that decides  $L \in \Sigma^*$  if  $\forall x \in \Sigma^*, \|x\| = n$

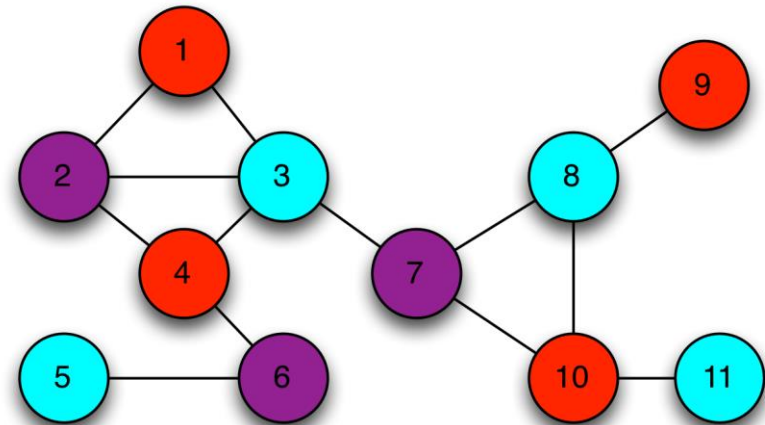
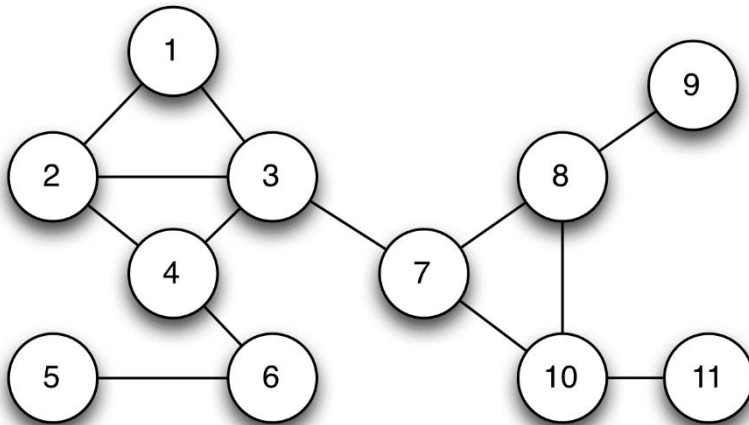
1. If  $x \in L$  then P accepts with  $P(x \in L) \leq (1 - 2^{-n})$
2. If  $x \notin L$ , there is no IBS such as P accepts with  $P(x \in L) > 2^{-n}$

Such an IBS is zero knowledge for L, if for any probabilistic polynomial time (PPT) verifier  $\hat{V}$  there exists a PPT simulator  $S$  such that

$$\forall x \in L, z \in \{0,1\}^*, \text{View}_{\hat{V}} [P(x) \leftrightarrow \hat{V}(x,z)] = S(x,z)$$

# Example II

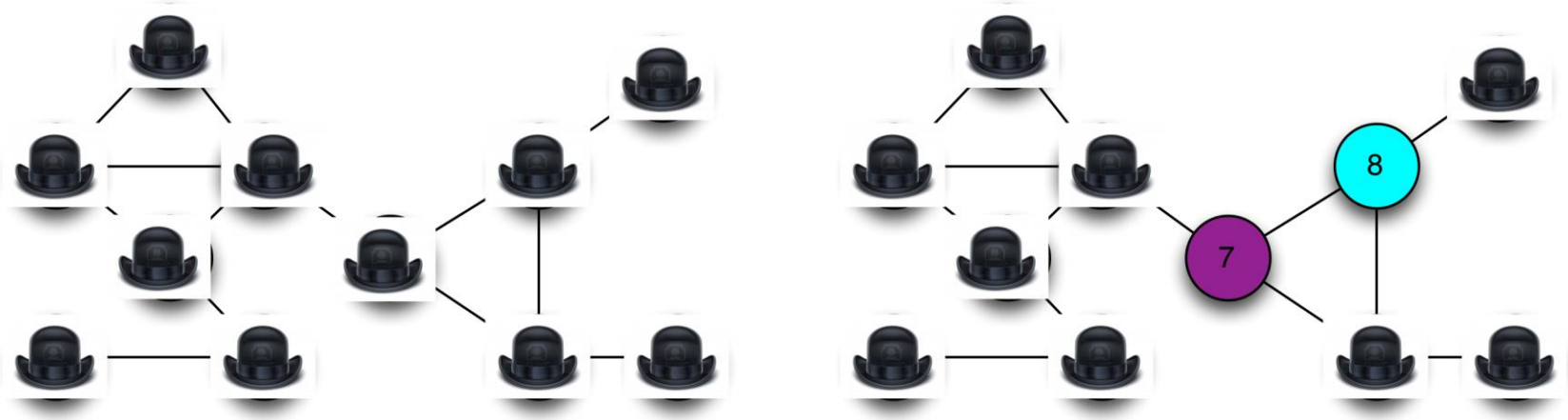
## The graph three coloring problem



complexity class: NP-Complete

# Example II

## The graph three coloring problem



Propability of succesful cheat:  $<(1-1/E)$

[Skript](#)

### 1. Completeness:

If Google is telling the truth, then they will eventually convince me.

### 2. Soundness:

Google can *only* convince me *if* they're actually telling the truth.

### 3. Zero-knowledge:

I don't learn anything else about Google's solution.

**Protocol:**  $P$  colors the graph  $G = (N, E)$  with colors (red, blue, green) and performs with  $V$   $|E|^2$ - times the following interactions, where  $n_1, \dots, n_n$  are nodes of  $N$ .

1.  $P$  choose a random permutation of colors, recolors  $G$ , and encrypts, for  $i = 1, 2, \dots, n$ , the color  $c_i$  of node  $n_i$  by an encryption procedure  $e_i$  - for each  $i$  different.

$P$  then removes colors from nodes, labels the  $i$ -th node of  $G$  with cryptotext  $y_i = e_i(c_i)$ , and design a decryption table

$P$  finally shows  $V$  the graph with nodes labeled by cryptotexts.

2.  $V$  chooses an edge and asks  $P$  to show him coloring of the corresponding nodes.

3.  $P$  shows  $V$  entries of the table corresponding to the nodes of the chosen edge.

4.  $V$  performs encryptions to verify that nodes really have colors as shown.

Since graph coloring is NP complete it can be used to prove any statement in the class NP.

If there exists *any* decision problem (that is, a problem with a yes/no answer) whose witness (solution) can be verified in polynomial time, then:

It can be proven that said solution exists by

- translating the problem into an instance of the graph three-coloring problem, and
- running the GMW protocol.

→ A ZKP exists for any statement in NP.



## Example III

### Fiat-Shamir Identification

- Chosen is an arithmetic modulo  $n = pq$ , where  $p$  and  $q$  are primes.
- Peggy (Prover) will choose a number  $s$  in  $\mathbf{Z}_n$ . She will keep  $s$  (private key) a secret but publish  $v = s^2 \bmod n$  (public key).
- During authentication, Peggy will randomly choose a number  $r$  in  $\mathbf{Z}_n$  and sends  $x = r^2 \bmod n$  to Victor (Verifier).
- After receiving  $x$ , Victor will randomly choose a number  $e$  in  $\{0,1\}$ , and send it to Peggy.
- After receiving  $e$ , Peggy will send  $y = r s^e$  to Victor.
- Victor will now need to check whether  $y^2 \bmod n = x v^e \bmod n$ . If yes, Peggy has passed the test. Victor might request Peggy to perform the experiment as many times as he desires until he's certain of Peggy's authority. Throughout the entire process, Victor will only need to work with the publicly known number  $x$ ,  $e$ , &  $v$  and will learn nothing about the secret  $s$ . Confidence is 50% for each run.

## •Advantages:

- Secured – Not requiring the revelation of one's secret.
- Simple – Does not involve complex encryption methods.

## Disadvantages:

- Limited – Secret must be numerical, otherwise a translation is needed.
- Lengthy – There are  $2^k$  computations, each computation requires a certain amount of running time.
- Imperfect – A Malice can still intercept the transmission.
- Unhandy – in a multi-protocol environment (Internet).

- Network Authentications
- Smart Cards
- Key Exchanges
- Digital Signatures

## Zero Knowledge Proofs

- ✓ Convey no extra information about a proof
- ✓ Completeness & Soundness
- ✓ ZKP is valid for all NP, proof by simulation
- ✓ practical protocols: GMP & Fiat-Shamir



# Appendix

- *Commitment Schemes and Zero-Knowledge Protocols (2008)*, Ivan Damgård and Jesper Buus Nielsen, Aarhus University, BRICS
- "How to Explain Zero-Knowledge Protocols to Your Children", (Quisquater, Jean-Jacques; Guillou, Louis C.; Berson, Thomas A. (1990). *Advances in Cryptology – CRYPTO '89: Proceedings*. **435**: 628–631.
- *Nicht-interaktive Zero-Knowledge Beweise von Wissen mittels Fiat-Shamir Transformation*. Masterarbeit. Julian Liedtke
- "The knowledge complexity of interactive proof systems", Goldwasser, S.; Micali, S.; Rackoff, C. (1989), *SIAM Journal on Computing*, Philadelphia: Society for Industrial and Applied Mathematics, **18**

[https://en.wikipedia.org/wiki/Zero-knowledge\\_proof](https://en.wikipedia.org/wiki/Zero-knowledge_proof)

<https://blog.cryptographyengineering.com/2017/01/21/zero-knowledge-proofs-an-illustrated-primer-part-2/>

Zero Knowledge Proofs and Protocols, .pptx, Nikolay Vyahhi, St. Petersburg State University.

, "Zero Knowledge Protocols and Small Systems", H. A. Aronsson, "http://www.tml.hut.fi/Opinnot/Tik-110.501/1995/zeroknowledge.html", 1995

"Authentication Protocols Lecture Notes", "http://www.cs.cmu.edu/afs/cs/academic/class/15827-f98/www/Slides/lecture3", 1998, H. L. Marko,