

Zero Knowledge Protocols

Guevara Noubir
<http://www.ccs.neu.edu/home/noubir/Courses/CSG252/F04>

Textbook: "A Course in Number Theory and Cryptography",
 Neal Koblitz

Reading: Chapter IV, page 117-123.

Outline

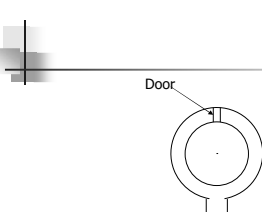
- Motivation for Zero Knowledge Protocols
- Zero Knowledge Protocols
 - Map Coloring, Discrete Logarithm
- Oblivious Transfer

Fall'04: CSG252 Classical Cryptography 2

Motivation for Zero Knowledge Protocols

- Tartaglia and Cardan story
 - <http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Tartaglia.html>
 - Tartaglia (XVI century) was able to find a technique to solve cubic equations, Cardan convinced him to show him the technique. Cardan later extended and published the technique! [There are many variations to the story]
- Concept behind ZK:
 - Prover tries to convince another (Verifier) probabilistically of the truth of a statement without revealing any of the proof
 - A Zero Knowledge protocol leaks no knowledge
- Example:
 - Ali-Baba (Prover) claims that he is a wizard who can open the secret door under the ground between cave A and cave B
 - This means that he can come back from a different cave, though an ordinary person can not come back from cave A if he/she enters cave B, and vice-versa
 - We assume that you are on the ground, and you do not know which cave Ali-Baba enters.
 - Also, you can not see Ali-Baba opening the secret door because you are on the ground.
 - How can you (Verifier) verify that he is really a wizard?

Fall'04: CSG252 Classical Cryptography 3

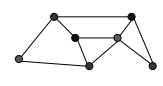


Door

- **Step 1:** Ali-Baba enters one of two caves, cave A or cave B secretly.
- **Step 2:** You choose one of two caves randomly and tell him to come back from the cave you choose
- **Step 3:** You check whether or not he came back from the cave you chose.
- **Step 4:** Repeat Step1 – Step 3
- If he succeeds to come back from the cave you choose every time (e.g. 1000 times in a row), you can leave no room to doubt that he is a real wizard because the probability (He is a liar and survives 1000 trials) is $(1/2)^{1000}$.

Fall'04: CSG252 Classical Cryptography 4

ZK for 3-Colorability



- Given a graph $G = (V, E)$, is G 3-colorable?
 - I.e., No edge has two vertices with the same color
 - 3-colorability is NP-Complete [we don't have any polynomial-time algorithm]
- ZK Protocol:
 - P (prover) takes his 3 coloring and randomly permutes the colors
 - P then writes the new color code on the vertices and covers them up
 - V picks an edge randomly, and P uncovers the colors of the endpoints
 - -if the colors are different V accepts, else reject
 - If true, then P can convince V with a probability of 1
 - If P is lying he can succeed on one trial with a probability of $1-1/E$
 - On repeated attempts: $((1-1/E)^{100})^E = e^{-100} \approx 1/E \rightarrow 0$
- Why doesn't it leak any information?

Fall'04: CSG252 Classical Cryptography 5

Types of Zero Knowledge Proofs

- ZK proof of a statement
 - Goal: to convince V that a statement is true without leaking any information
 - E.g., graph is 3-colorable
- ZK proof of knowledge of a secret
 - Goal: to convince V that P knows a secret
 - E.g., discrete logarithm of a number
- Interactive vs. Non-interactive ZK Proofs

Fall'04: CSG252 Classical Cryptography 6

Properties of ZK Protocols

- **Completeness:**
 - Given a honest 'prover' and a honest 'verifier', the protocol succeeds with overwhelming probability
- **Soundness:**
 - No one who doesn't know the secret can convince the verifier with non-negligible probability
- **Zero knowledge:**
 - The proof does not leak any additional information

Fall'04: CS6252 Classical Cryptography 7

ZK for Discrete Logarithm

- **Input:**
 - G is a finite group containing N elements (order N)
 - b is a fixed element of G and y is an element of G for which P has found a discrete logarithm to the base b (i.e., $y = b^x$)
- **Goal:**
 - Convince V , that P knows x , without revealing anything about x
- **Protocol:**
 1. P generates a random positive integer $e < N$ and send $b^e = b^e$
 2. V uses a random bit:
 1. If 0 then P must reveal $e \Rightarrow V$ verifies that $b^e = b^e$
 2. If 1 then P must send $e+x \pmod N \Rightarrow V$ verifies that $y b^e = b^{e+x}$
 3. Repeat steps 1-2 until V is convinced

Fall'04: CS6252 Classical Cryptography 8

Oblivious Transfer

- **Definition:**

An "Oblivious Transfer Channel" from P to V is a system for P to send V two encrypted packets of information subject to the following conditions:

 1. V can decipher one and only one of the two packets
 2. P does not know which of the two packets he can read
 3. Both P and V are certain that conditions 1 and 2 hold
- **Applications:**
 - Build non-interactive ZK proofs

Fall'04: CS6252 Classical Cryptography 9

Oblivious Transfer Protocol

- Input:
 - F_q : Large Finite Field
 - b : fixed s.t. Diffie-Hellman is difficult in F_q^*
 - $\psi(u): F_q \rightarrow F_2^n$ s.t. $\psi^{-1}(F_2^{n/2}) \subseteq F_q$
 - C is a number with secret discrete log (provided by a trusted third party)
- Protocol to send $m_1, m_2 \in F_2^n$:
 - V:
 - Choose random $x \in \{1, \dots, q-2\}$ and $x \in \{1, 2\}$
 - Compute: $\beta_1 = b^x, \beta_2 = C/b^x$ and make public (β_1, β_2)
 - P: verifies that $\beta_1 \beta_2 = C$
 - Choose y_1, y_2 random from $\{1, \dots, q-2\}$
 - Send $b^{y_1}, b^{y_2}; a_1 = m_1 + \psi(\beta_1^{y_1}), a_2 = m_2 + \psi(\beta_2^{y_2})$
 - V: obtain m_1 or m_2 depending on if $\beta_1 = b^x$ or $\beta_2 = b^x$
 - What if the same information has to be sent twice?
