Private Circuits

Yury Lifshits
Steklov Institute of Mathematics, St. Petersburg, Russia
yury@logic.pdmi.ras.ru
Tartu University
16/03/2006

Outline

1. Private circuits: Definition and Motivation
2. Secret Sharing Construction
3. Fake Channels Construction

Boolean circuits

Who are boolean circuits?
• Input wires
• AND and NOT gates
• Random bit gates
• Sometimes, memory

Security Against Probing Attacks

Adversary is able to listen up to \( t \) wires

Perfect security: distribution of any \( t \) wires is independent on input

Statistical security: for any fixed \( t \)-attack it is a negligible chance over a random execution that observable distribution differs with secure (independent from input) distribution

Motivation

Main application:
Protection hardware realizations of block cyphers (AES,...) with embedded key from probing attacks
Basic Idea

Any ideas?

Trivial (still working) approach: use \( t + 1 \) wires in \( C' \) for each wire in \( C \). For simplicity of further proof we use \( m = 2t + 1 \) wires.

Are we done? What do we need?

How to compute gates? What Encoding/Decoding to use?

NOT Gate

Encoding:
Encode input bit \( b_i \) to \( r_1, \ldots, r_{2t}, b_i \oplus \sum_{j=1}^{2t} r_j \)

Decoding:
Decode output bit \( c_i = \sum_{j=1}^{2t+1} w_j \)

NOT gate:
Apply not to first wire in a bundle

AND Gate

We need to compute encoding for \( c = \sum_{i,j} a_i b_j \)

We take the following encoding:
\[
  c_i = a_i b_i \oplus z_{i,j},
\]

where for \( i < j \) we take \( z_{i,j} \) at random, while for \( i > j \) we take
\[
  z_{i,j} = (z_{j,i} \oplus a_i b_j) \oplus a_i b_i
\]

Outline

1. Private circuits: Definition and Motivation
2. Secret Sharing Construction
3. Fake Channels Construction

Statistical Security

Two parameters: security parameter \( k \) and adversary power \( t \)

Statistical security:
For any fixed \( t \)-attack
chance over a random execution that
observable distribution differs with independently from input distribution
is negligible (in terms of \( k \))

Our goal: \( t \cdot \text{poly}(k) \) cost

Step 1: Security Against Random Attack

Random attack: adversary is able to observe each wire with probability \( 1/10k \)

Take secret sharing construction for \( k \) adversary power

To broke a circuit adversary need \( k/2 >> \frac{1}{10k} k^2 \) wires in some gate

Probability calculations shows that this has a negligible chance

Refreshing Effect

Observation over secret sharing construction: \( t/2 \) observations even for every gate provide no information on original data

Proof: refreshing effect
Step 2: Security Against Worst Case Attack

**Final step:** to force any attack no more effective than random attack
- Split every wire to \( s \) wires
- Only one contain 0/1 information
- All others contain special symbol ★
- A meaningful channel is elected in run time

Summary

**Main points:**
- New model of hardware attack: up to \( t \) wires are observed by adversary
- Two types of data security: perfect and statistical
- Cost of protecting transformation is \( t^2|C| \) and \( t\text{poly}(k)|C| \) correspondingly

Home Problem 5

**HP5:** Invent a \( n^2 \) sorting circuit (one gate sorts two elements)

Comment on Home Problem 4: prove that probability is smaller than \( 1/m \) from some \( m_0 \)

Deadline 1: tomorrow lecture, 17/03/2006 — 16-15
Deadline 2: 31/03/2006 — 16-15

Reading List

- Y. Ishai, A. Sahai, D. Wagner
  http://www.cs.ucla.edu/~sahai/work/privcirc-crypto03.ps

Thanks for attention. Questions?