Bounded-Communication Leakage Resilience via Parity-Resilient Circuits

Vipul Goyal [1] Yuval Ishai [2,3] Hemanta K. Maji [4]
Amit Sahai [3] Alexander A. Sherstov [3]

[1]Microsoft Research, India

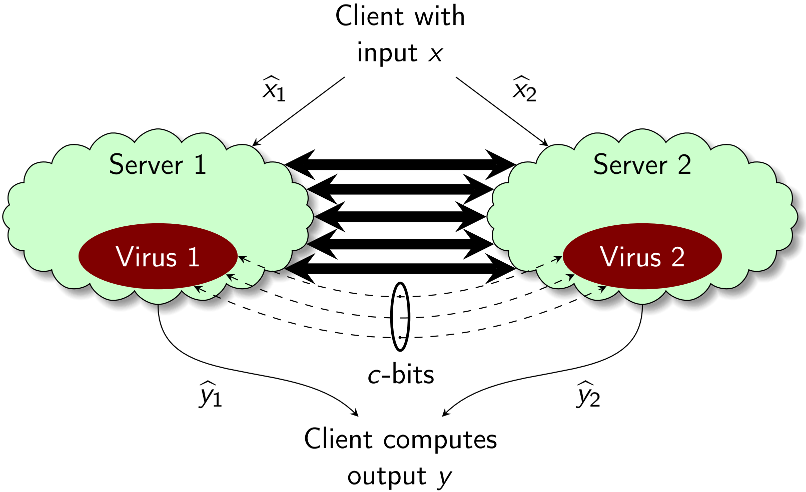
[2]Technion

[3]University of California, Los Angeles

[4]Purdue University

October 14, 2016 (FOCS–2016)

Motivation: Delegating Computation to Two Servers



Assumptions on Viruses

Assumptions

1. Passive: Do not tamper with the server messages
2. Bounded Communication: Only c-bits of virus communication

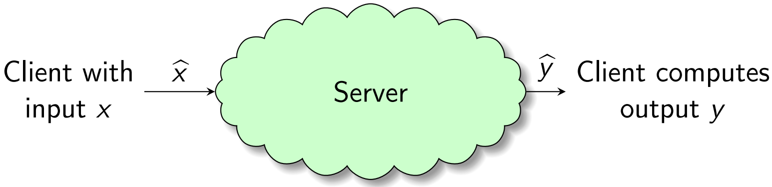
Justification

Virus Detection Mechanisms make tampering server messages and large communication between viruses difficult

Note

Viruses can store the entire server view before communicating

Related Problem 1: Delegation to Single Server



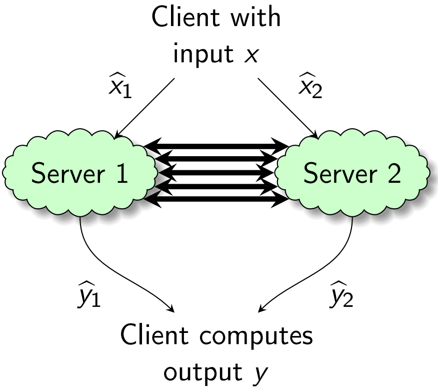
Solution

Fully Homomorphic Encryption [Gentry–09]

Concerns

- Quite far from practical
- Relies on a relatively narrow class of cryptographic hardness assumptions
- No information-theoretic analogue

Related Problem 2: Non-communicating Viruses



Solution

Secure Two-party Computation [Yao–82, Goldreich–Micali–Wigderson–87]

Features

- Information-theoretic Security using OT or correlated private randomness
- Computational Security based on general cryptographic assumptions

Primary Concern

Yao and GMW are insecure even for 1-bit virus communication

Main Result: Informal

Definition (Bounded Communication Leakage Resilience)

A *c-BCL-resilient* protocol delegates a computation to two servers, such that any c-bounded communication leakage reveals essentially nothing about the input

Theorem (Our Main Result: Informal)

Given an n-bit input/output circuit C_f of

- size s, and depth h

We construct a c-BCL-resilient protocol such that:

- Client is implemented by a circuit of size $\widetilde{O}(n+c)$
- Servers are implemented by a circuit of size $\widetilde{O}(s+ch+c^2)$
- Information-theoretic security given OT
- Computational security based on standard cryptographic assumptions

Comparison to Previous Work (1)

[Dziembowski–Faust–12]

Information-theoretic 2-server Solution using “Leak-free Hardware”

Drawback

The size of the “Leak-free Components” depends on the leakage bound and the statistical security parameter

Feature of our solution

The size of “Leak-free Components” (Oblivious Transfer functionality, which is minimal) is constant

- Crucial to instantiating our construction with standard cryptographic assumptions

Comparison to Previous Work (2)

[Goldwasser–Rothblum–12] & [Bitansky–Dachman-Soled–Lin–14]

Information-theoretic solution using large-number of servers

Drawback

The number of servers is large

Feature of our solution

A 2-server solution (which is minimal)

Comparison to Previous Work (3)

[Dachman-Soled–Liu–Zhou–15]

Instantiated the hardware components of [Dziembowski–Faust–12] using Deniable Encryption in the computational setting

Drawback

Only known instantiations of Deniable Encryption rely on iO [Garg–Gentry–Halevi,Raykova–Sahai–Waters–13,Sahai–Waters–14]

Feature of our solution

Milder cryptographic hardness assumptions like the intractability of factoring Blum Integers and the Decisional Diffie Hellman

Efficiency Comparison to Previous Works

Legend:

- Circuit size of an implementation of f: s
- Circuit size of BCL-resilient Protocol: S
- Bound on the communication complexity of viruses: c

Previous Works: Computational Overhead

Computational Overhead $S/s \geqslant c$

Our Solution: Computational Overhead

Computational Overhead $S/s = \mathrm{polylog}\, c$, where $c \approx s^{1/2}$

Key Technical Idea: The Beginning

Two Distributions

- Let μ be a ε-biased distribution
- Let R be a distribution with $(n - c)$ min-entropy

Theorem (Small-Bias Masking [Dodis–Smith–05])

$$\mathrm{SD}\left(\mu + R, U_n\right) \leqslant 2^{c/2}\varepsilon$$

Reformulation in Two-Server Model

Two Distributions

- Let μ be a ε-biased distribution
- Let R be a uniform distribution over n-bit strings

Two-server setting

- View of Server 1 is R, and View of Server 2 is $\mu + R$
- Virus 1 sends one c-bit message $L = \mathcal{L}(R)$ to Virus 2

Note

R conditioned on the leakage L has high average min-entropy:

$$\widetilde{H}_\infty(R|L) \geqslant (n - c)$$

Theorem (Small-Bias Masking [Dodis–Smith–05])

$$\mathrm{SD}\left((\mu + R, L) \, , \, (U_n, L) \right) \leqslant 2^{c/2}\varepsilon$$

Virus 2's view looks essentially random

Generalization Goal

Two Directions

- Generalize "ε-bias" to "ε-indistinguishability"
  - Let μ_0 and μ_1 be two distributions that are indistinguishable by linear tests
  - We want: $(\mu_0 + R, L)$ and $(\mu_1 + R, L)$ to look similar
- Generalize "one-round c-bit message" by "arbitrary c-bit communication"

General Small-bias Masking

Theorem (Generalized Small-bias Masking)

Let μ_0 and μ_1 be be probability distribution that are ε-indistinguishable by linear tests. Then a c-bit communication protocol π that outputs a bit obeys:

$$\left| \mathop{\mathbb{E}}_{w \sim \mu_0} \mathop{\mathbb{E}}_{r \xleftarrow{\$} \{0,1\}^n} [\pi(r, w + r)] - \mathop{\mathbb{E}}_{w \sim \mu_1} \mathop{\mathbb{E}}_{r \xleftarrow{\$} \{0,1\}^n} [\pi(r, w + r)] \right| \leqslant 2^{c/2} \varepsilon$$

What we achieved: Reduction to Parity-Resilient Circuit

x_0 $\quad$ x_1

$\mu_0 \equiv C[x_0]$ $\quad$ If Indistinguishable By Linear Tests $\quad$ $\mu_1 \equiv C[x_1]$

Server 1 View R $\quad$ Server 2 View $\mu_0 + R$ $\quad$ Server 1 View R $\quad$ Server 2 View $\mu_1 + R$

$\pi(R, \mu_0 + R)$ $\quad$ $\pi(R, \mu_1 + R)$

Then Indistinguishable

Starting Point: Private Circuits [Ishai–Sahai–Wagner–03]

Algorithms (I', C', O') such that

$$x \xrightarrow[\text{using } I']{\text{Client Encodes}} \widehat{x} \xrightarrow[\text{Private Circuit } C']{\text{Evaluation of}} \widehat{y} \xrightarrow[\text{using } O']{\text{Client Decodes}} y$$

Definition (Private Circuits)

Probing k-wires of C' reveals nothing about the client input x

Parity-resilient Circuit

Algorithms (I, C, O) such that

$$x \xrightarrow[\text{using } I]{\text{Client Encodes}} \widehat{x} \xrightarrow[\text{Parity-Resilient Circuit } C]{\text{Evaluation of}} \widehat{y} \xrightarrow[\text{using } O]{\text{Client Decodes}} y$$

Definition (Parity-Resilient Circuits)

Parity of wire-values of any subset of wires of C reveals nothing about the client input x

Construction of C from C'

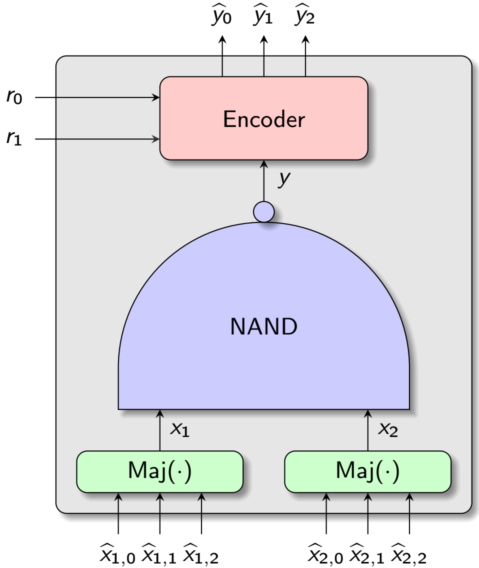
Every wire w in C' is encoded as 3 wires in C whose <u>majority</u> is w

Caution

The actual encoding used in the paper is slightly more complicated than what is presented here. This complication is necessitated due to the fact that the randomness used to encode the wire w is also present in the circuit C

Parity-resilient Circuit: The NAND-Gadget

NAND-Gadget: An 8-bit input and 3-bit output Function

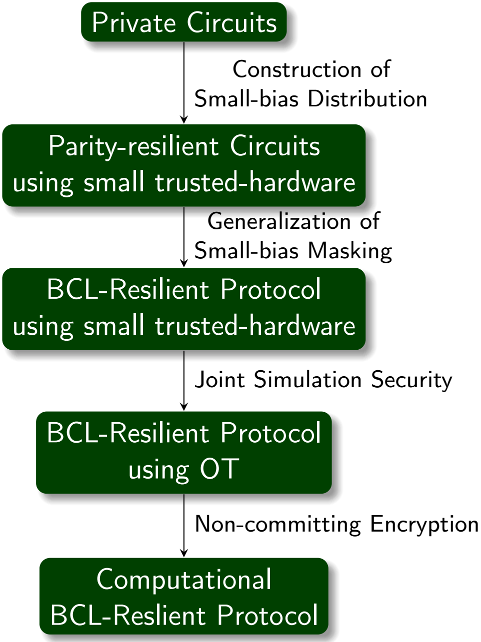


Parity-resilient Circuit: Proof

Why does it work?

- *Small* parity tests are fooled by the privacy guarantee
- *Big* parity tests are fooled because the XOR of a large number of independent & small-biased bits is close to uniform

Overall Construction



Thank You!

Open Problems

- Continual Leakage Setting
- Information-theoretic construction for 3-Servers in the plain model

Summary of Our Construction

Private Circuits

↓ Construction of Small-bias Distribution

Parity-resilient Circuits using small trusted-hardware

↓ Generalization of Small-bias Masking

BCL-Resilient Protocol using small trusted-hardware

↓ Joint Simulation Security

BCL-Resilient Protocol using OT

↓ Non-committing Encryption

Computational BCL-Reslient Protocol