Privacy-Preserving Remote Diagnostics

Philip Schmieg and Manjiri Birajdar

TU Darmstadt

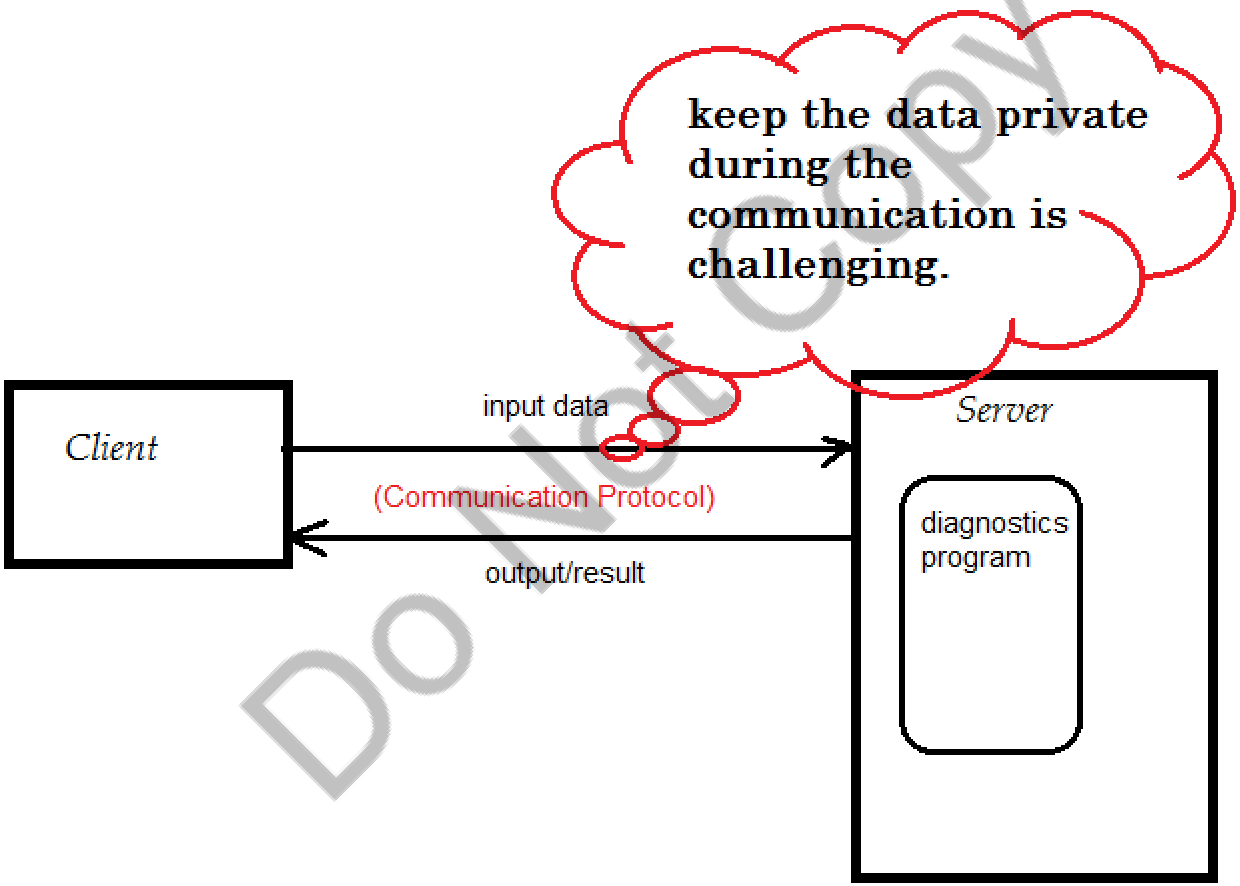
Agenda

- ❑ Introduction
- ❑ Remote Diagnostics
- ❑ Basic knowledge and terminologies
  - Branching Program (BP)
  - Oblivious Transfer (OT)
  - Garbled Circuits (GC)
  - Homomorphic Encryption (HE)

Agenda

- ❑ Protocol Digest
  - Secure branching program protocol
  - A protocol for secure evaluation of private LBPs - SecureEvalPrivateLBP
- ❑ Performance Comparison

Introduction

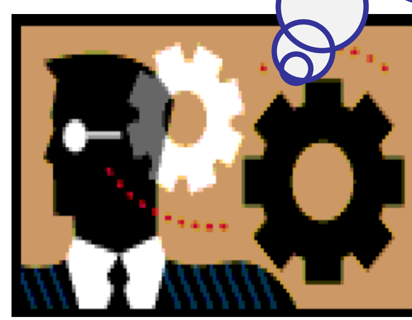


Remote diagnostics - risk for both the parties

I want my personal information and secrets protected

I want to protect the diagnostics program and the intellectual property

client



Server

Remote diagnostics

TECHNISCHE UNIVERSITÄT DARMSTADT

❑ Applications:

- Healthcare (medical treatment sector)
- Remote software fault analysis (fault diagnostics)
- ElectroCardioGram signals

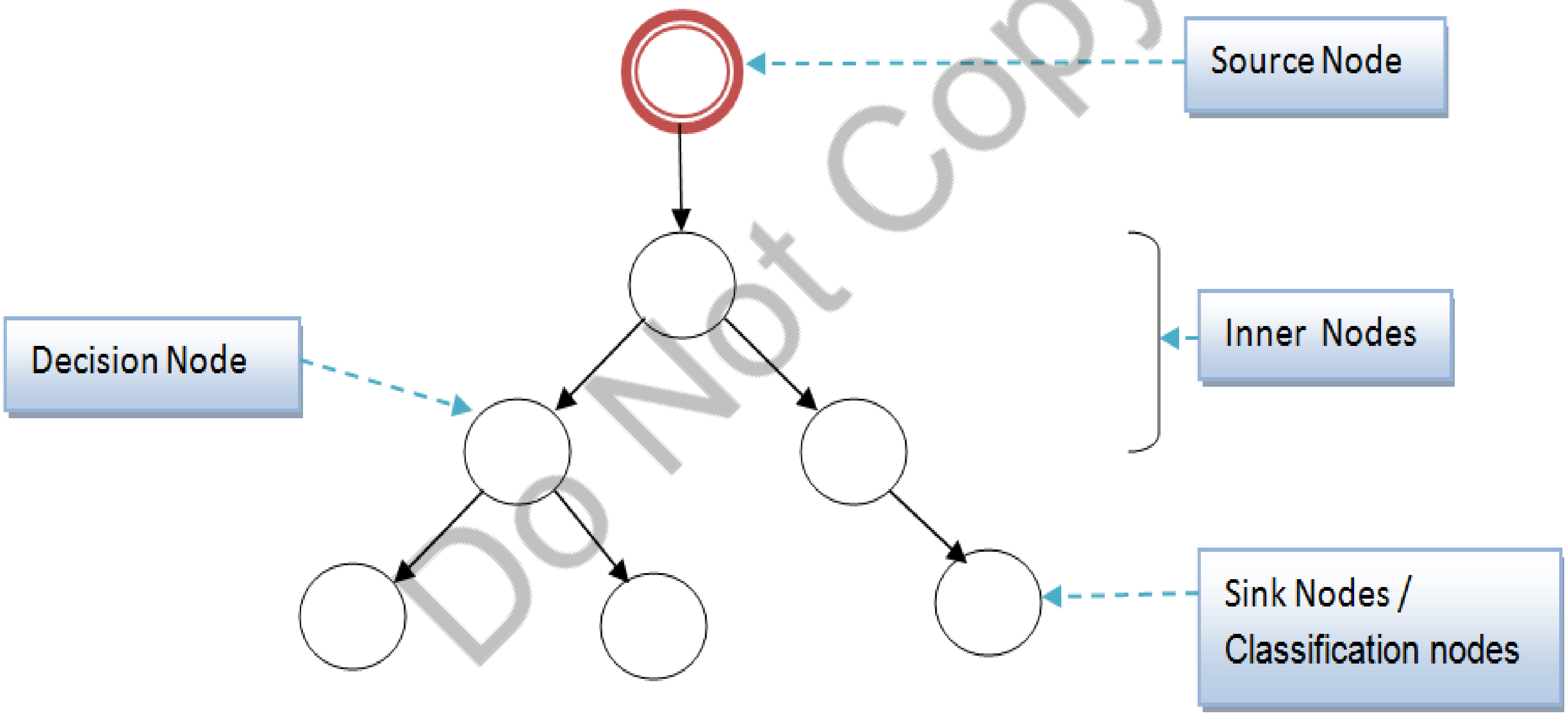
Example: In medical applications:

- **Patient** wants his personal data to be protected from medical applications while receiving an analysis
- The **service provider** wants his algorithms to be protected as it is an intellectual property

Branching Programs (BP)

- Set of decision and classification nodes
- Decision nodes are inner nodes on which the program branches until a classification node is reached
- Can represent boolean functions which are compatible with Garbled Circuits

Branching Programs (BP)



Linear Branching Programs

- Linear Branching Programs are a generalization BPs
- While BP use only one attribute for comparison in decision nodes, **LBP use a linear combination of the users attribute vector**

Oblivious Transfer

TECHNISCHE UNIVERSITÄT DARMSTADT

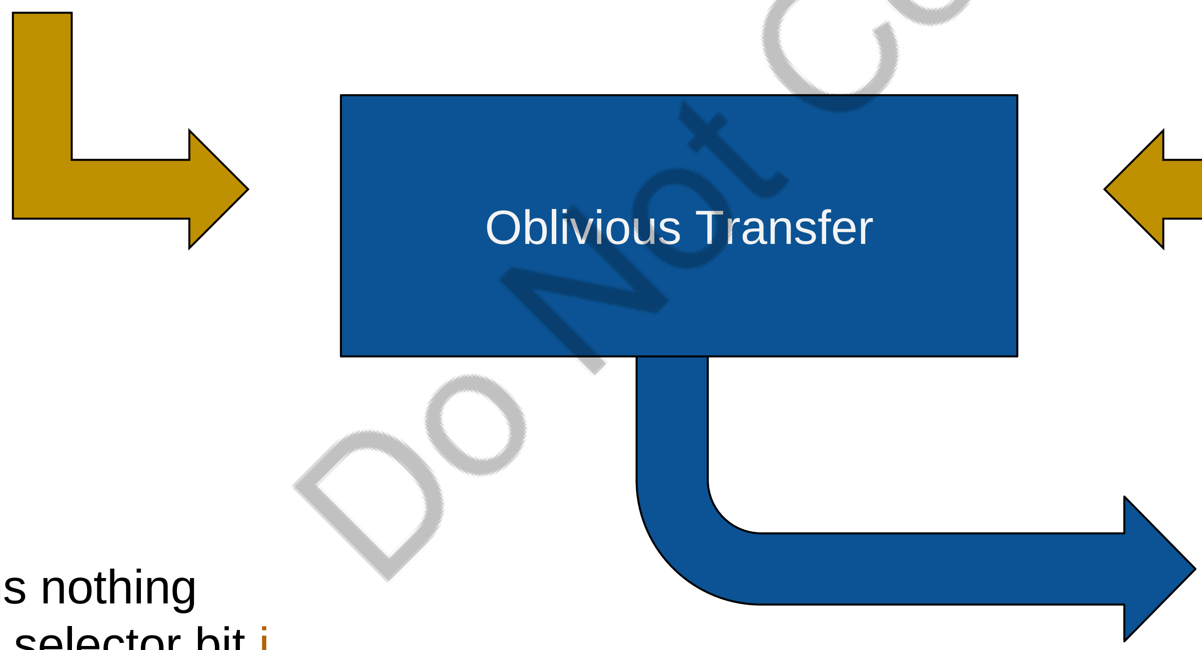
- Method for information transfer between a sender and receiver
- The sender does not know which information was requested
- While the receiver only learns one of the two inputs
- Used by Bob to learn his input values for the GC from Alice

Oblivious Transfer

TECHNISCHE UNIVERSITÄT DARMSTADT

Alice
x_1, x_2

Bob
choose bit i={0,1}



Learns nothing
about selector bit i

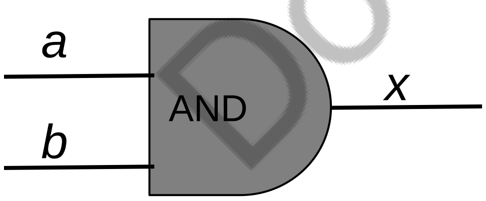
Learns **x_i** and
nothing about
x_i-1

Oblivious Transfer

- The receiver chooses a bit b = {0,1} which correlates to the input he wants to select
- The Sender inputs two values between the receiver will chose
- The receiver receives the chosen value while not learning anything about the other value

Garbled Circuit

- Encrypted circuit with a pair of wire keys for every input wire.
- The wire keys enable the computation of the output based on the encrypted input
- Nothing is learned from the gate computation



a	b	x
a_1	b_1	$Enc_{a_1 \| b_1}(x_1)$
a_1	b_0	$Enc_{a_1 \| b_0}(x_0)$
a_0	b_1	$Enc_{a_0 \| b_1}(x_0)$
a_0	b_0	$Enc_{a_0 \| b_0}(x_0)$

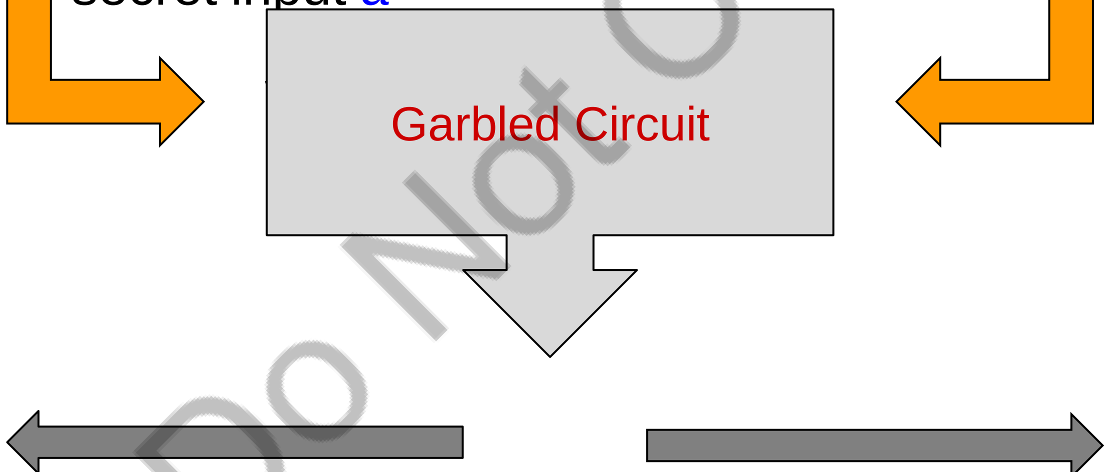
Garbled Circuits (GC) - Yao's garbled circuits protocol

Alice(Server)

agree on function *f*

Bob(Client)

secret input *a*



learns nothing about *b*

m = $f(a,b)$

learns nothing about *a*

$f(a,b)$

m = $f(a,b)$

Yao’s garbled circuits protocol

TECHNISCHE UNIVERSITÄT DARMSTADT

- Protocol for secure two-party computation
  - Constant number of rounds
  - Secure against semi honest adversary
- Can compute any function based on a boolean circuit securely
- Builds on garbled circuits and oblivious transfer

Yao's Protocol Steps

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Step 1:** Alice generates the garbled circuit C and two encrypted labels for each input wire
- **Step 2:** Alice sends her encrypted input (wire labels) to Bob
- **Step 3:** Bob receives his wire labels from Alice using 1-out-of-2 oblivious transfer without revealing his inputs to Alice
- **Step 4:** Bob uses Alice's wire labels and his own wire labels to compute the output and send it back to Alice

Homomorphic Encryption

- Manipulation of plaintext without knowing the corresponding ciphertext
- Additiv homomorphic encryption is :

$$\mathrm{Enc}_k(x_1 + x_2) = Enc_k(x_1) + Enc_k(x_2$$

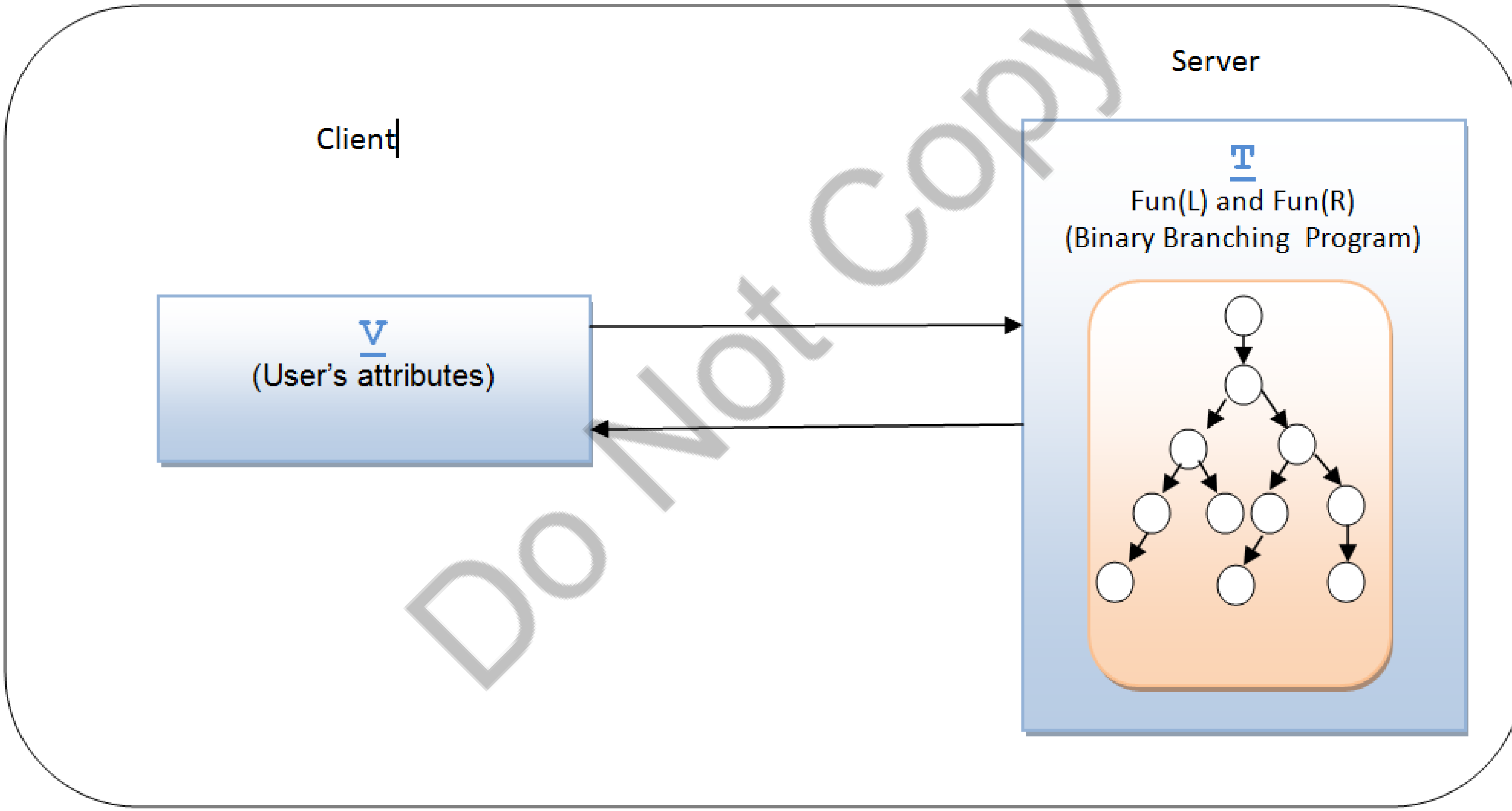
- Addition can be done on ciphertext and decrypted plaintext result is correct

Protocol Digest

- **Secure branching program protocol**
  - used for secure evaluation of binary branching programs.

- **A protocol for secure evaluation of private LBPs - SecureEvalPrivateLBP**
  - secure evaluation of private linear branching programs.

Secure branching program protocol



The main goal of the protocol is to securely analyze the T on V

Secure branching program protocol

TECHNISCHE UNIVERSITÄT DARMSTADT

Phase I (Offline): Creation of the secure branching program

- Transforms the nodes in branching program T into secure nodes in branching program T’
- **Classification node** is replaced by encryption of its **classification label**.
- **Decision node** is replaced with a **small garbled circuit** performing offset integer comparison
- User can figure out one of the decryption keys
- the revealed key can help to decrypt the next node on the evaluation path

Secure branching program protocol

Phase II: Oblivious attribute selection

Phase III: Evaluation of the secure branching program

A protocol for secure evaluation of private LBPs - SecureEvalPrivateLBP

TECHNISCHE UNIVERSITÄT DARMSTADT

- Secure evaluation of private linear branching programs
- **Linear Branching Programs (LBP)** generalize binary classification or decision trees and Ordered Binary Decision Diagrams (OBDDs)
- The protocol **SecureEvalPrivateLBP** is divided into **three phases:**
  - Phase I: CreateGarbledLBP
  - Phase II: ObliviousLinearSelect
  - Phase III: EvalGarbledLBP

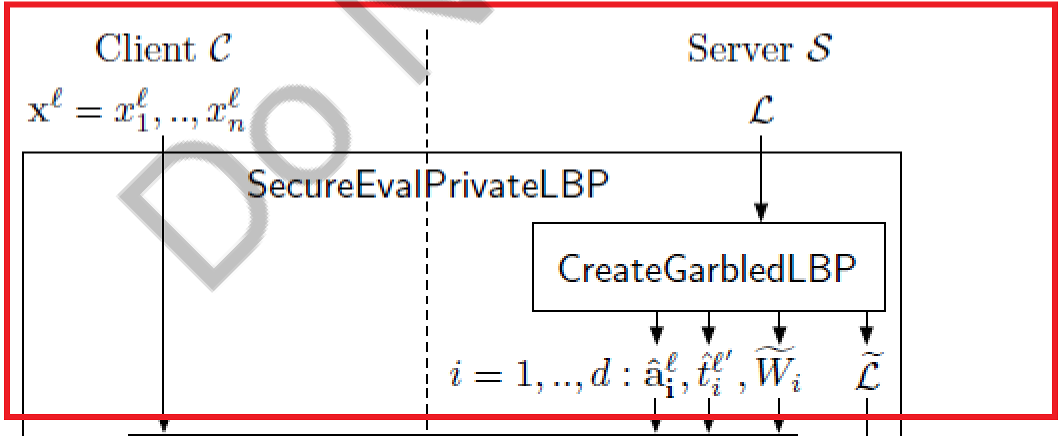
A protocol for secure evaluation of private LBPs - SecureEvalPrivateLBP

C : attribute vector x^l

S : server

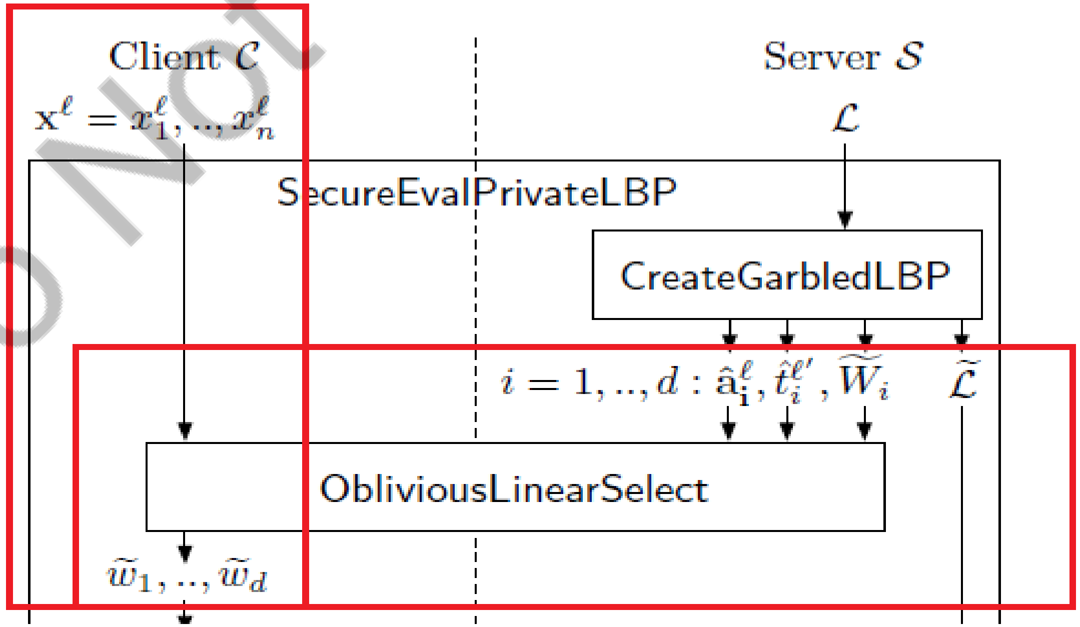
$\mathscr{L}$: linear branching program

- Phase I: CreateGarbledLBP
  - the server S generates the garbled version of the LBP $\mathscr{L}$
  - randomize LBP permutation



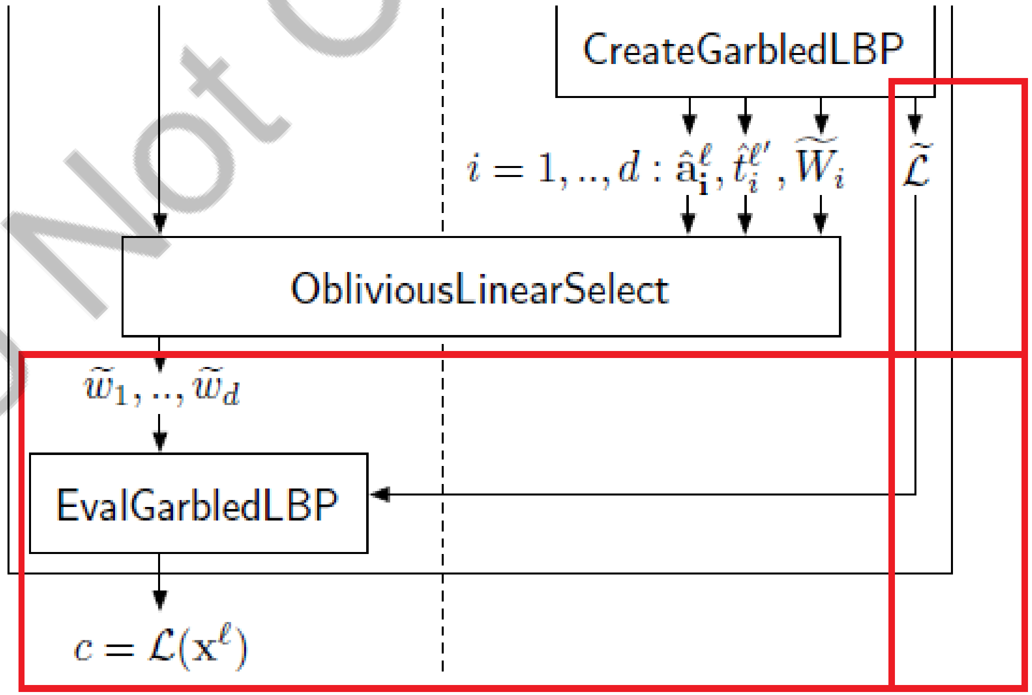
A protocol for secure evaluation of private LBPs - SecureEvalPrivateLBP

- Phase II: ObliviousLinearSelect
  - S blinds the encrypted value in order to hide the encrypted plaintext from C
  - protocol makes sure that S and C should not learn anything about the plaintexts.



A protocol for secure evaluation of private LBPs - SecureEvalPrivateLBP

- Phase III: EvalGarbledLBP
  - This stage takes the garbled values as input and produces the classification label as output



Performance

- ❑ Performance is a critical criteria for privacy preserving protocols
- ❑ Efficiency depends on the offline and online computations
- ❑ The garbled circuits can be pre computed on the server
- ❑ The exchange of garbled values happens in an online phase which uses oblivious transfer
- ❑ The evaluation of the Garbled Circuit happens on the client

Performance Improvements of Barni et al.

- ❑ Point and permute
  - Circuit evaluator only needs to decrypt a single ciphertext per garbled gate
- ❑ Incorporate classification nodes into decision nodes
  - Reduces size of LBP and number of Oblivious Transfers by the number of classification nodes
- ❑ Packing
  - Packing multiple ciphertexts into one and thus reducing number of decryptions and communication complexity

Performance Improvements of Barni et al.

- TinyLBPs
  - Constructing the LBP as single Yao gate with *d* inputs
  - only feasible for small *d* because the size of the LBP grow exponentially in *d*
- Key-offsets

Performance Comparison

TECHNISCHE UNIVERSITÄT DARMSTADT

- The improved hybrid version of Barni et al. reduces the number of Garbled Circuit and Oblivious Transfer and Homomorphic Encryption computations
- The reduction results are shown in the following table:

Oblivious Selection Protocol	Private Function	Moves	Asymptotic Communication Complexity GC	OT	HE
[BPSW07]	BP	OT+2	$12zl(t+\kappa)$	OT_t^{zl}	$(n+z)2T$
[BFK+09] Hybrid	LBP	OT+2	$12dl't$	$OT_t^{dl'}$	$(n+\frac{l'}{T-\kappa}d)2T$

Acknowledgments

We thank

Engineering Cryptographic Protocols Group

(ENCRYPTO),

Dr. Thomas Schneider and Agnes Kiss

for their help and support.

References

- [BFK+09] Mauro Barni, Pierluigi Failla, Vladimir Kolesnikov, Riccardo Lazzeretti, Ahmad-Reza Sadeghi, and Thomas Schneider. Secure evaluation of private linear branching programs with medical applications.
- [BPSW07] Justin Brickell, Donald E. Porter, Vitaly Shmatikov, and Emmett Witchel. Privacypreserving remote diagnostics.
- [GQ17] D. Giry and J.-J. Quisquater. Cryptographic key length recommendation. Website, 2017. Online https://www.keylength.com
- [Yao86] Andrew Chi-Chih Yao. How to generate and exchange secrets.

Any

Questions?