CRISP

Center for Research
in Security and Privacy

Transputation: Transport framework for secure computation

Markus Brandt, Claudio Orlandi, **Kris Shrishak,** Haya Shulman

CRISP is a joint project of

TECHNISCHE UNIVERSITÄT DARMSTADT

CYSEC

Fraunhofer SIT

Fraunhofer IGD

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES

Secure Computation

Alice and Bob

.. have private inputs

.. want to jointly compute a function

.. reveal the output and nothing more

Secure 2PC setting in this talk

- Yao's garbled circuits: Constant round
- Passive security
- Concrete efficiency

1 Bandwidth – bottleneck?

- Computation time has significantly reduced due to
  - Circuit optimizations
  - Hardware support for cryptography
- 2PC based on garbled circuits have reached the theoretical lower bound [ZRE15]
- Bandwidth is believed to be the main bottleneck
- Bandwidth is underutilized.
- TCP sockets are used in all
  - secure computation implementations
  - network settings

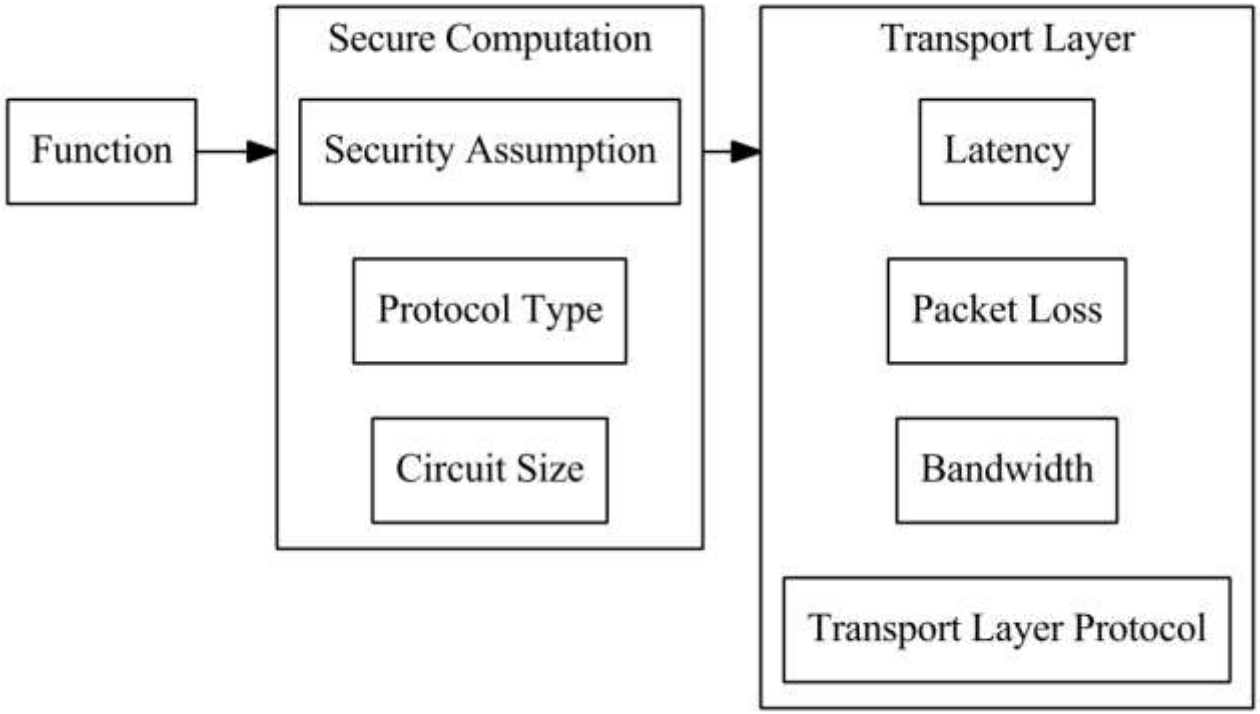
2 Why not use other transport protocols?

- Hard to integrate transport protocols to the application
- One-size does not fit all
- Depends on
  - Circuit size
  - Size of inputs
  - Network conditions

3 The problem with evaluations

- Do not reflect real world complexities
- Performance measured in ideal settings
- Extra work to setup realistic evaluation testbed

Transputation Framework



Transputation Framework

- Automates the usage and integration of transport layer protocols into secure computation implementations.
- Modular design
  - Separates program logic from network code
  - Allows extension with other secure computation protocols
  - Easy to extend with new transport protocols

2PC Layer

- PRF assumption [GLNP15]
  - 4-2 Garbled-row-reduction + XOR-1
- Circular related key assumption [ZRE15]
  - Free-XOR + Half-gates
- Ideal cipher assumption [BHKR13]
  - Fixed-Key AES + Free-XOR + Half-gates

Assumption	AES	SHA256	MinCut
PRF	0.59	3.41	69.04
Circularity	0.21	2.77	30.52
Ideal cipher	0.21	2.77	30.52

Garbled circuit size in MB

Transport Layer: Basics

- End-to-end communication between the applications on different hosts
- Sender: Segments data received from the application
- Receiver: Reassembles segments into messages

Transport Layer

Principles

- ❑Reliability
- ❑Flow control
- ❑Congestion control
- ❑Fairness

Protocol selection

- ❑Latency
- ❑Bandwidth
- ❑Packet Loss

Transport Layer Protocols

- TCP
  - Reliable but poor bandwidth utilization
  - Reacts on packet-level events (ACK)
  - Transmission rate controlled with additive increase multiplicative decrease (AIMD) algorithm
- UDP
  - Unreliable

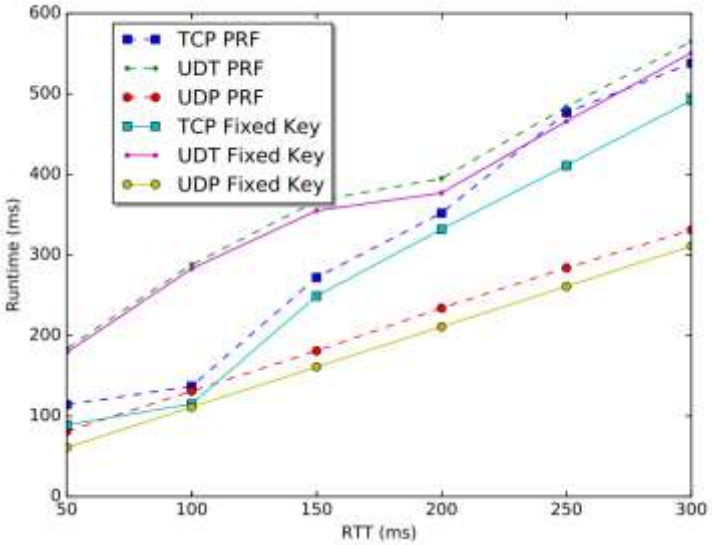
Transport Layer Protocols

- UDT
  - UDP-based data transfer protocol
  - Reliability added at the application layer
  - Timer-based congestion control
  - Loss indicated with Negative ACK (NACK)
  - Uses Decreasing AIMD algorithm.

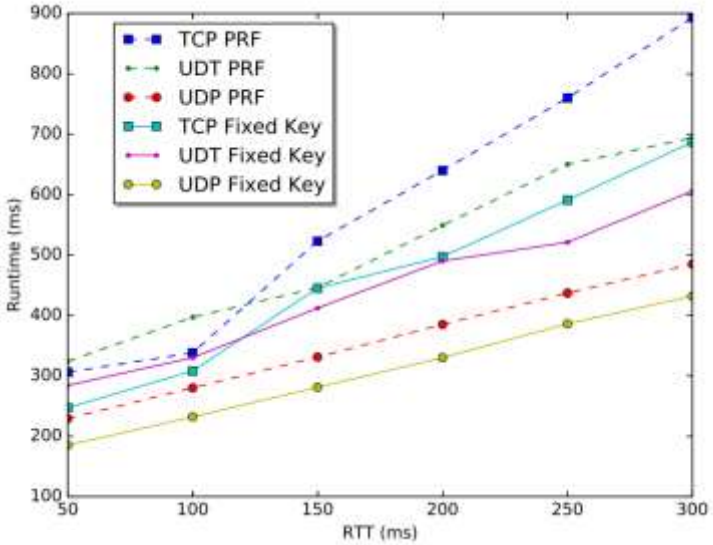
Evaluation Testbed

- Distributed evaluation setup tailored for 2PC
- Supports various transport protocols
- Allows 2PC developers to perform real life evaluations

Evaluations: Latency

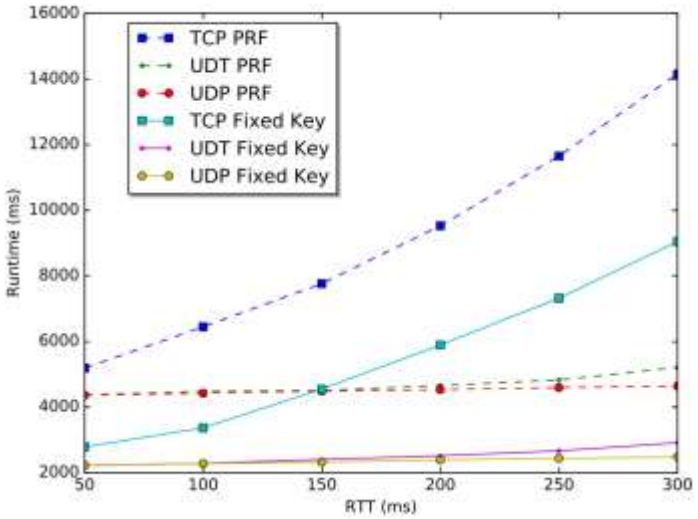


AES

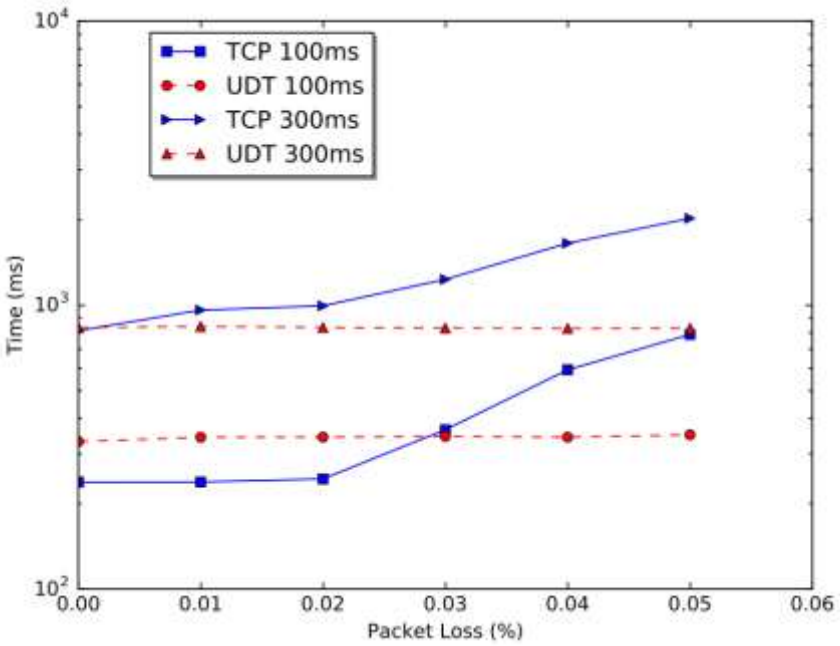


SHA256

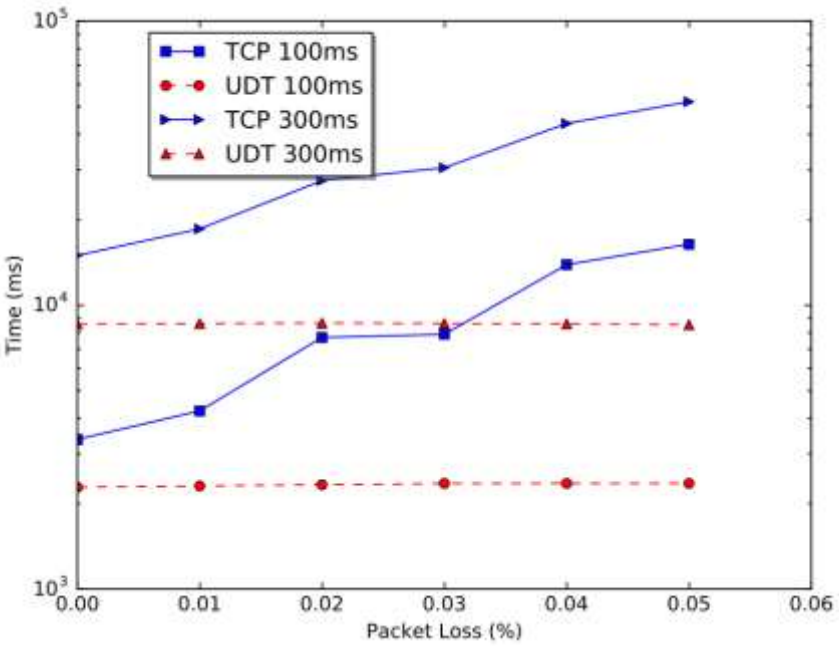
MinCut



Evaluations: Packet loss

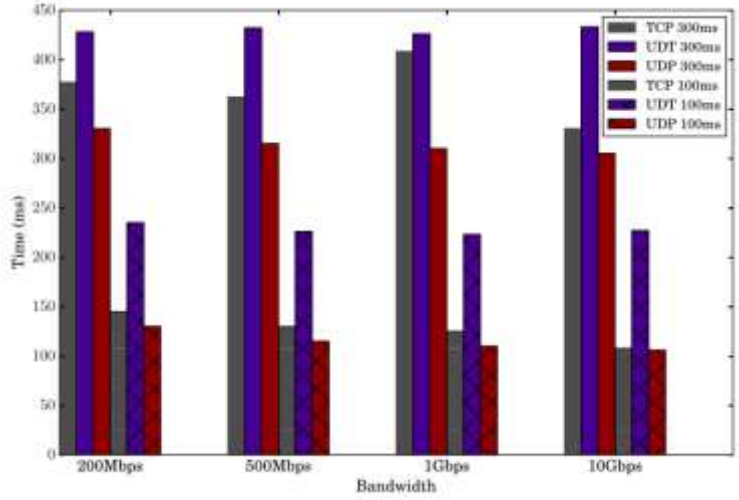


SHA256

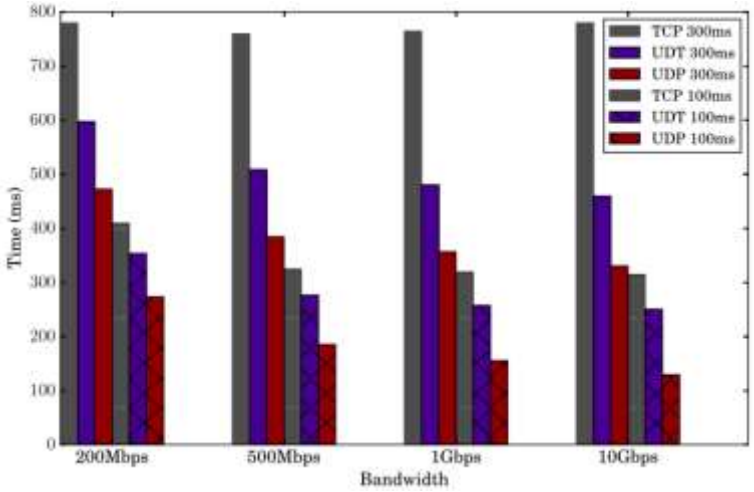


MinCut

Evaluations: Bandwidth

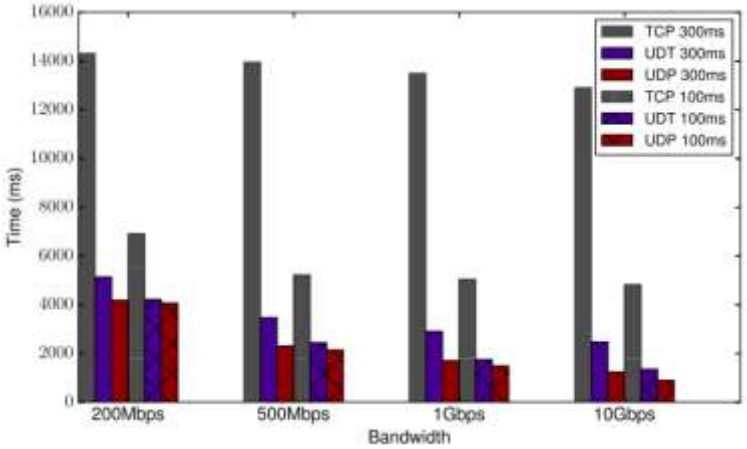


AES



SHA256

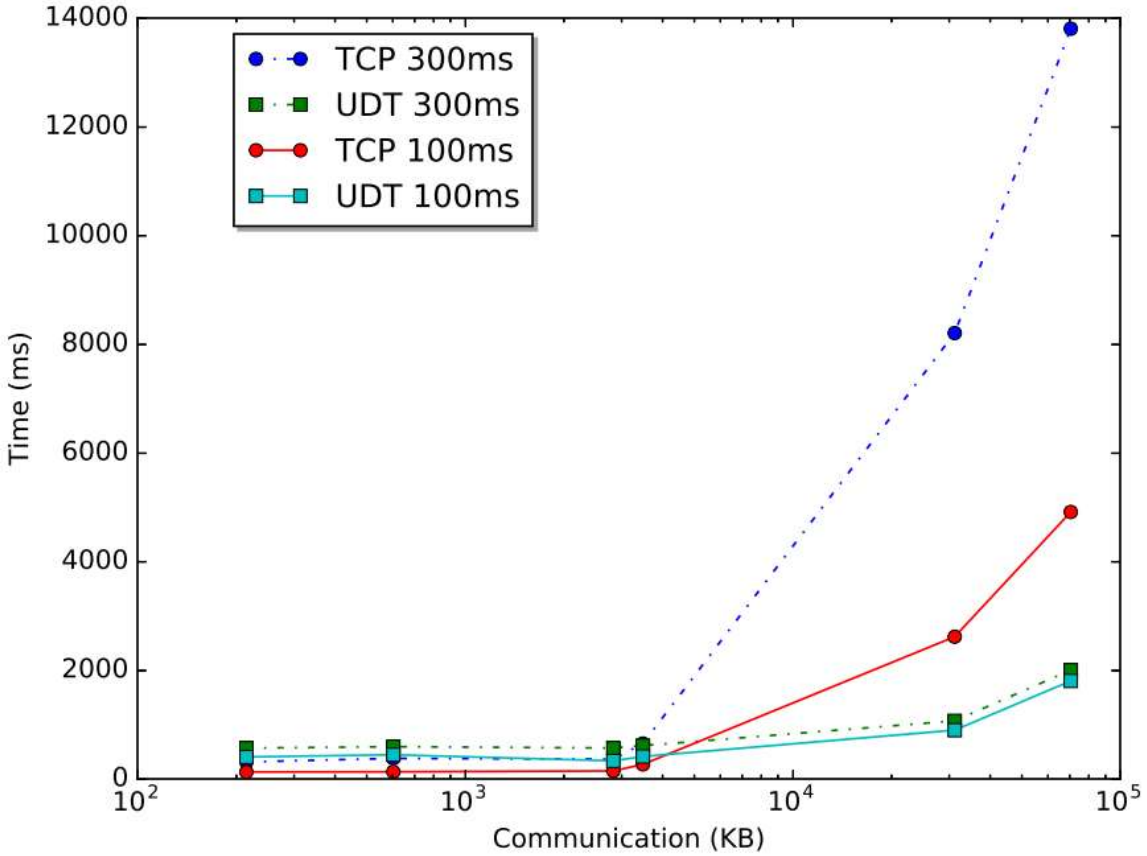
MinCut



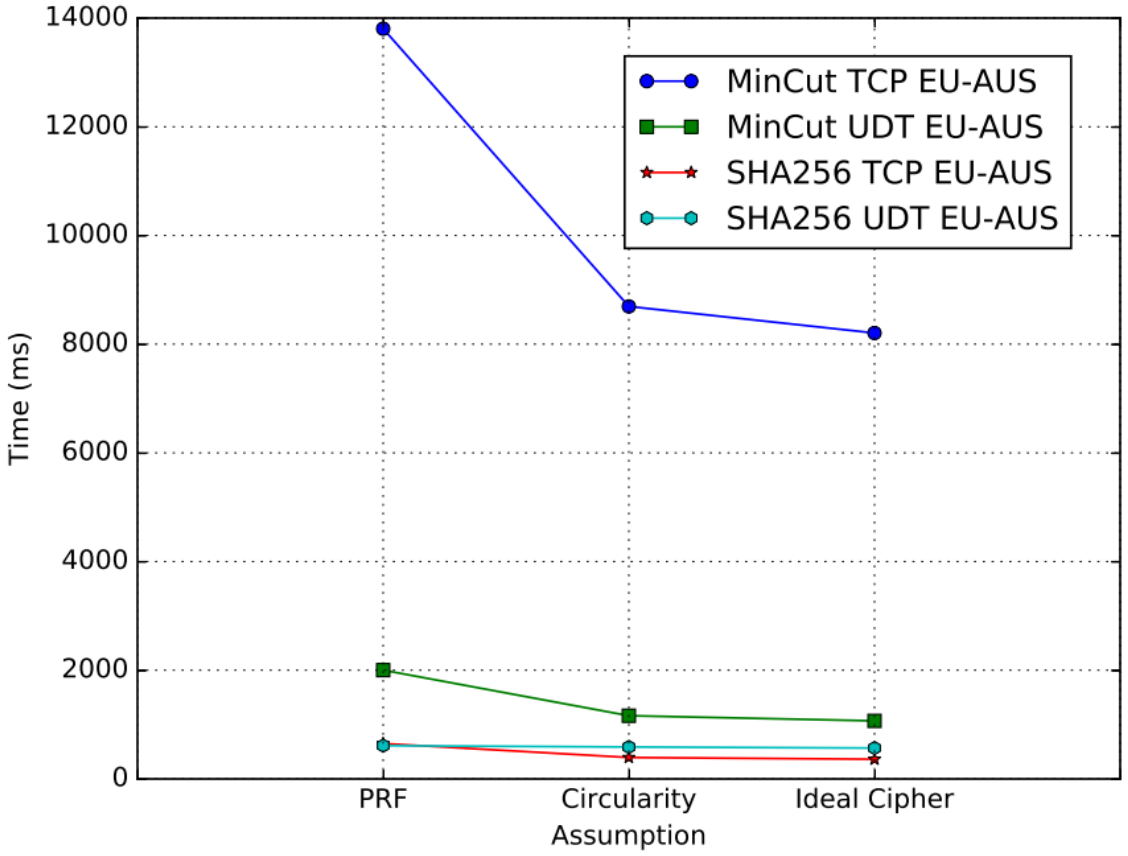
Evaluation results

Circuit	Setting	Ideal cipher		Circularity		PRF	
		TCP	UDT	TCP	UDT	TCP	UDT
AES	LAN	**2.4**	187.1	**2.9**	191.3	**7**	202.7
	EU-US	**127.4**	403.9	**126.3**	408.3	**130.4**	444.2
	EU-AUS	**312.44**	566.84	**310.88**	580.2	**377.92**	592.5
SHA256	LAN	**13.5**	191.9	**19.9**	226.7	**30.5**	233.45
	EU-US	**146.23**	332.24	**151.99**	318.26	**266.46**	411.96
	EU-AUS	**362.53**	568.22	**394.13**	587.03	650.44	**612.43**
MinCut	LAN	**255.19**	598.2	**267.2**	740.2	**700.8**	1255.9
	EU-US	2616.59	**896.74**	2783.6	**957.6**	4911.89	**1802.25**
	EU-AUS	8204.61	**1068.07**	8693.57	**1163.14**	13805.2	**2001.27**

Garbled circuit size



Comparison for different assumptions



Future Work

- Active security
- MPC
- Custom transport protocol for specific applications

CRISP

Center for Research
in Security and Privacy

Thank you

References

[BHKR13] Mihir Bellare, Viet Tung Hoang, Sriram Keelveedhi, and Phillip Rogaway.

Efficient Garbling from a Fixed-Key Blockcipher, S&P 2013

[GLNP15] Shay Gueron, Yehuda Lindell, Ariel Nof, and Benny Pinkas.

Fast garbling of circuits under standard assumptions, CCS 2015

[ZRE15] Samee Zahur, Mike Rosulek, and David Evans.

Two halves make a whole - reducing data transfer in garbled circuits using half gates, EUROCRYPT 2015