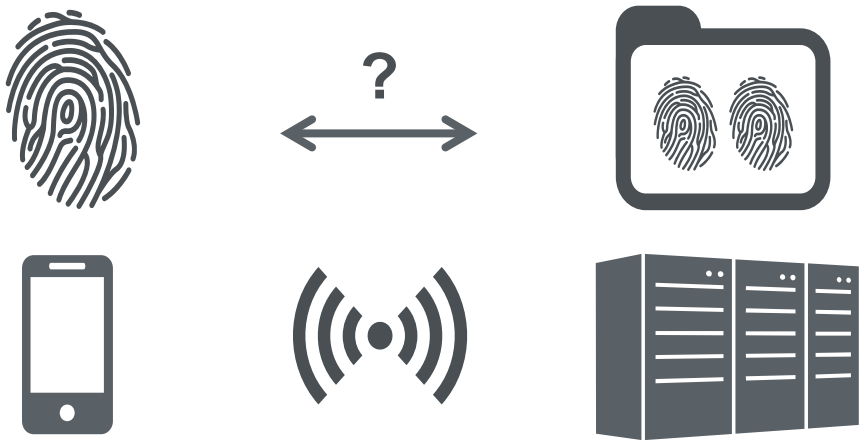
Towards Practical Two-Party Computations

Stefan Katzenbeisser

TECHNISCHE UNIVERSITÄT DARMSTADT



CROSSING

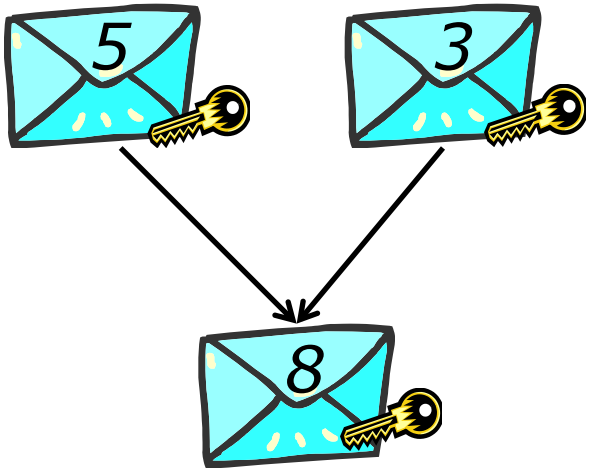
DFG Deutsche Forschungsgemeinschaft

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy-Enhancing Technologies (PETs)

CROSSING

- Strike a balance between data availability and privacy
- **Paradigm:** keep data encrypted, PETs **compute with encrypted data**
- **Privacy By Design**:
  Cryptographic protocols precisely limit amount of information available
- Cryptographic tools are available!
- **S**ecure-**T**wo-party **C**omputation
  - Homomorphic encryption
  - Yao's Garbled circuits
  - Customized protocols
    (private set intersection, ...)



Applications

CROSSING

Auctions

Private Set Intersection

Machine Learning

Biometric Identification

...

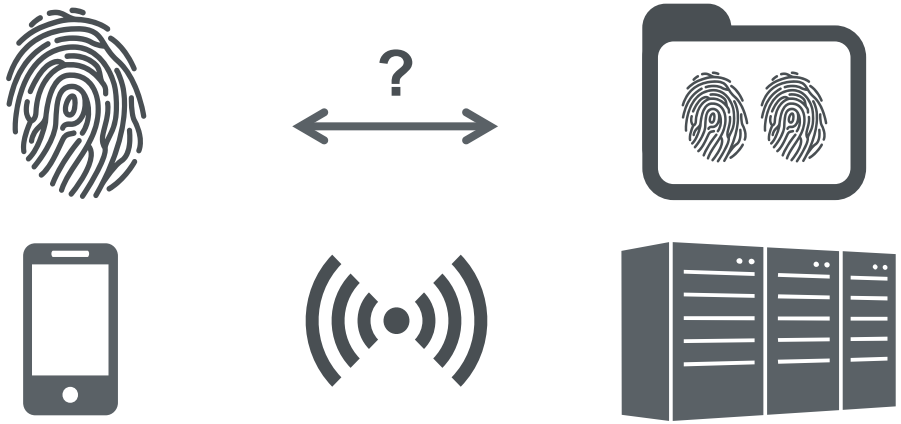
Secure Two-party Computation Challanges in Practice

CROSSING

Secure computation for processing sensitive data

Complex | Resource intensive | Hard to implement

Privacy-preserving fingerprint matching between mobile and server



Selected Work @Darmstadt
Towards Practical STC

CROSSING

Efficient STC Protocols & Frameworks

- More efficient **Oblivious Transfers**
- **ABY** – Framework for efficient mixed protocol STC

CROSSING

Practical Compilers for STC

- **CBMC-GC** – An ANSI C Compiler for Garbled Circuits
- **ParCC** – Compiler and framework for parallel STC
- **Compiler for mixed-mode ST**

CROSSING

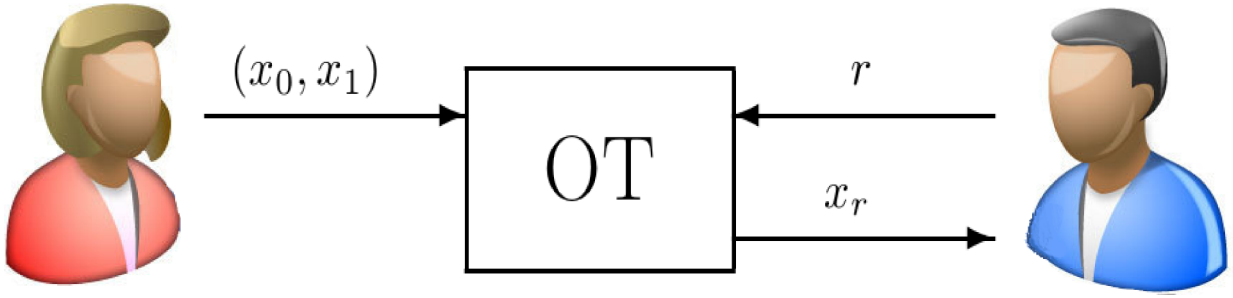
EC SPRIDE

Efficient Oblivious Transfer

CROSSING

Optimizations for OTExtension in the semi-honest and malicious model

- Specific OT functionalities for more efficient STC
- Open source implementation



Asharov, Lindell, *Schneider, Zohner* (CCS'13, Eurocrypt'15)

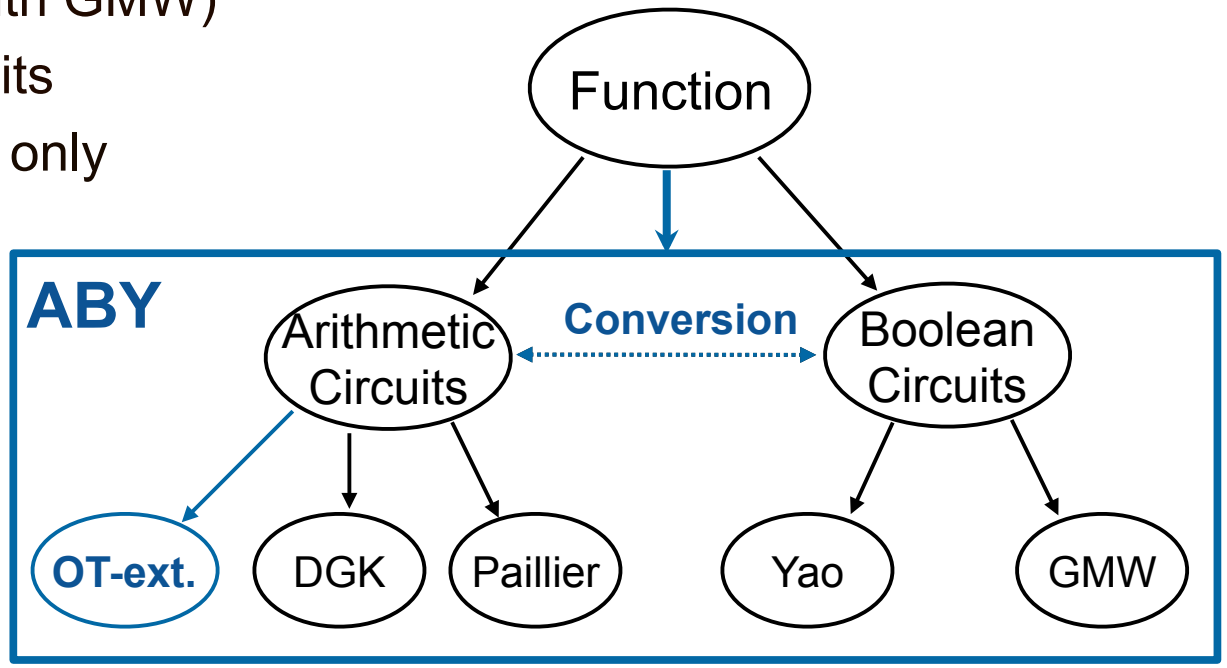
ABY – A Framework for Efficient Mixed-Protocol Secure Two-Party Computation

CROSSING

ABY: Framework for efficient mixed-protocols

- **A**rithmetic Sharing
- **B**oolean Sharing (with GMW)
- **Y**ao's Garbled Circuits

- Conversions using OT only
- Open source



Demmler, Schneider, Zohner (NDSS'15)

ABY – A Framework for Efficient Mixed-Protocol Secure Two-Party Computation

CROSSING

ABY: Framework for efficient mixed-protocols

- **A**rithmetic Sharing
- **B**oolean Sharing (with GMW)
- **Y**ao's Garbled Circuits

- Conversions using OT only
- Open source

	LAN	Cloud
Yao only	2.55s	26.6s
GMW only	2.43s	39.41s
ABY	**0.19s**	**3.42s**

Example: Biometric matching with 512 samples

Demmler, Schneider, Zohner (NDSS'15)

CBMC-GC:
An ANSI-C Compiler for STC

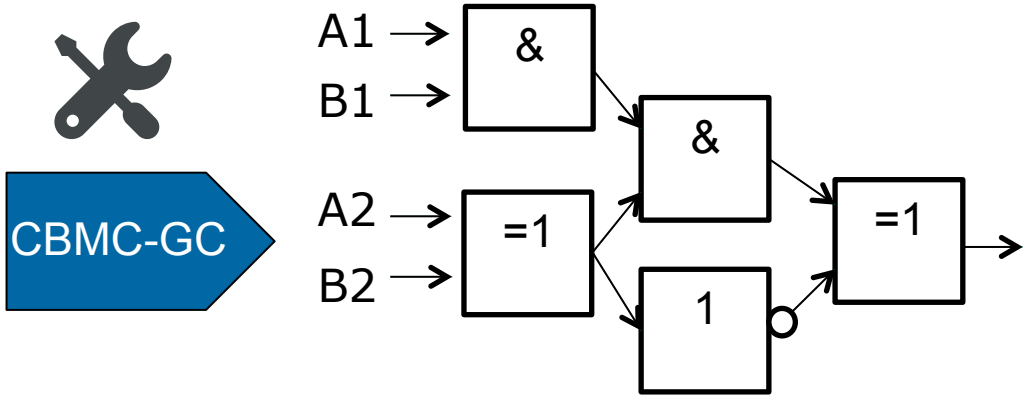
CROSSING

First compiler for ANSI-C to Garbled Circuits

- Supports a large subset of C, simple naming conventions
- Open source: `http://forsyte.at/software/cbmc-gc/`

```
void millionaires() {
  int INPUT_A_mila;
  int INPUT_B_milb;

  int OUTPUT_res;
  if (INPUT_A_mila > INPUT_B_milb)
    OUTPUT_res = 1;
  else
    OUTPUT_res = 0;
}
```



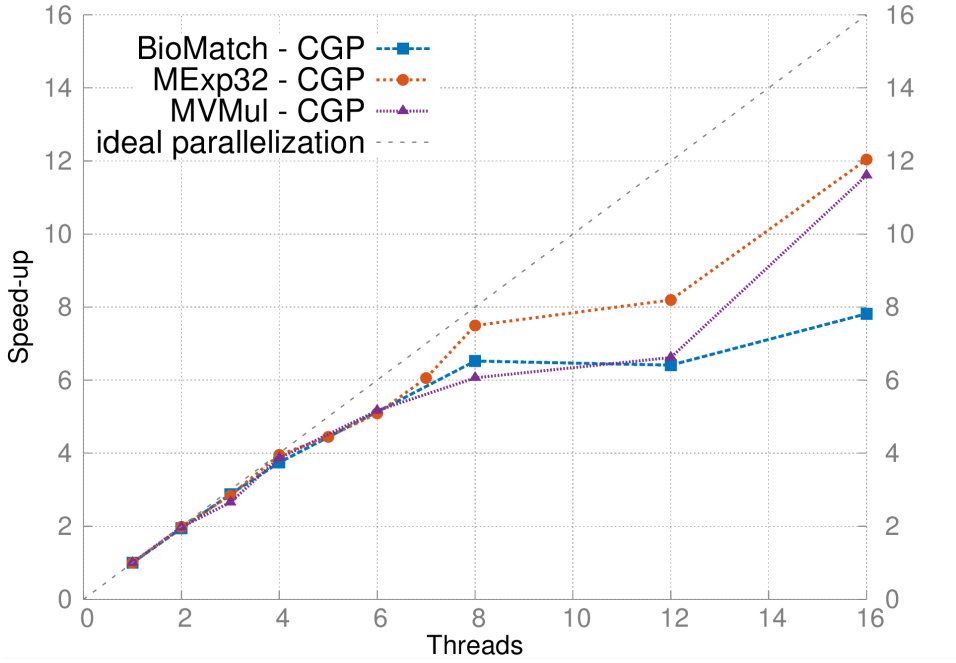
Holzer, *Franz, Katzenbeisser,* Veith (CCS'12, CC'14)

Extension of CMBC-GC: Automatic Parallelization

CROSSING

ParCC: Parallel Circuit Compiler

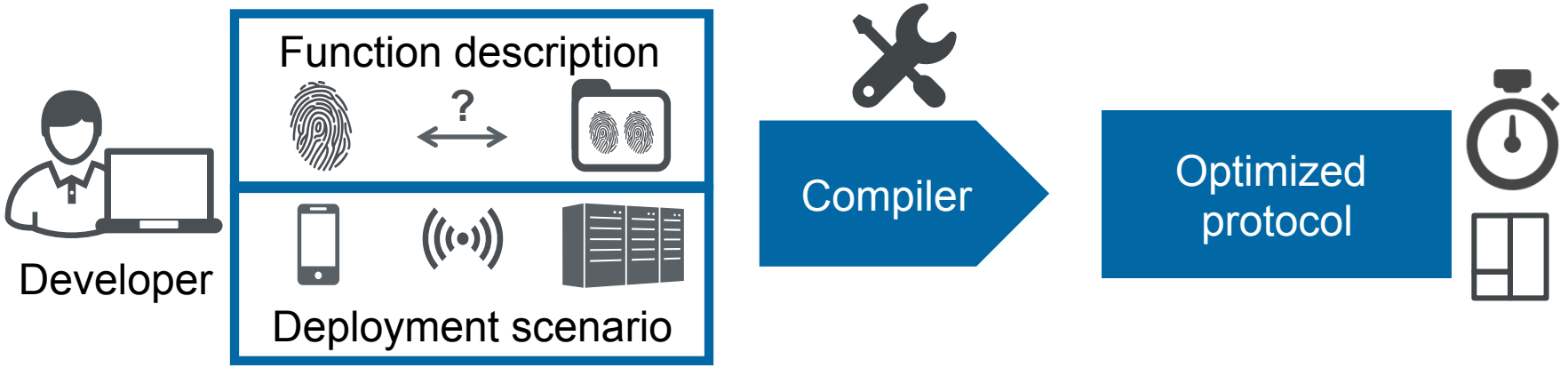
- Extends CBMC-GC to detect parallelism in source code
- Parallel Circuits achieve speed-ups with high efficiency even in the semi-honest model



Future Work:
Automatic, Scenario-Dependent Compiliation

CROSSING

Goal Automatically generate optimized secure computation protocols.



Challenges

Metrics for efficiency comparisons

Mix multiple protocols for better efficiency

Automated generation and optimization

CROSSING