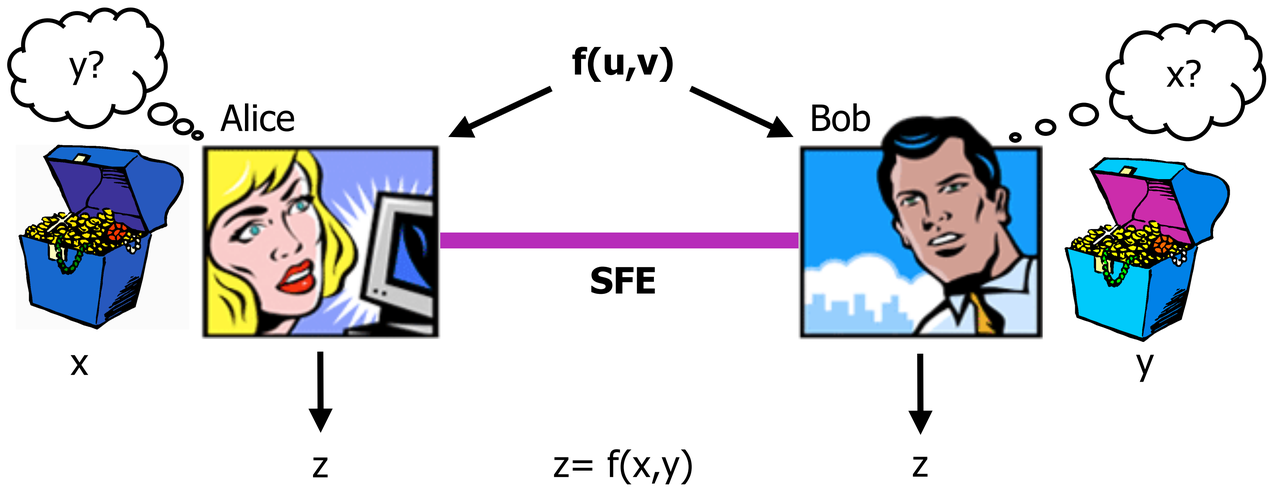
TECHNISCHE FAKULTÄT

Elektrotechnik, Elektronik und Informationstechnik
Chemie- und Bioingenieurwesen
Werkstoffwissenschaften
Maschinenbau
Informatik

Practical Secure Function Evaluation

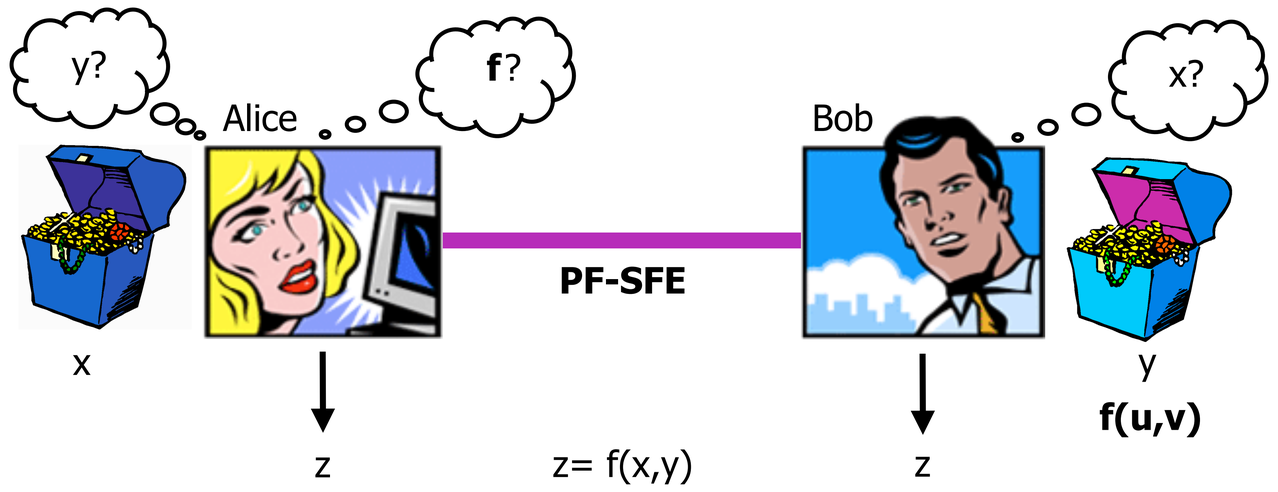
Diplomarbeit of Thomas Schneider, Supervision: Prof. V. Strehl and V. Kolesnikov, PhD
{thomas.schneider@informatik.stud, strehl@informatik}.uni-erlangen.de, kolesnikov@research.bell-labs.com

Secure Function Evaluation (SFE) allows two parties Alice and Bob to securely evaluate a function f(u,v) on their private inputs x and y:
- each party learns the result z = f(x,y)
- each party learns nothing about the other party's secret y resp. x



Practical Examples:
- Millionaires Problem (Maximum)
- Auctions
- Voting
- Keyed Database Search
- ...

Secure Function Evaluation of Private Functions (PF-SFE) - same as SFE with additionally f being private:
- f is known by Bob only
- Alice learns nothing about f (besides size, #inputs and #outputs)



Practical Examples:
- No-Fly-List Checking
- Privacy-Preserving Credit Report (or Medical History) Checking
- Mobile Code (executed in untrustworthy environment)
- Privacy-Preserving Database Querying (e.g. patent database)
- ...

Contents and Contributions of this Thesis:

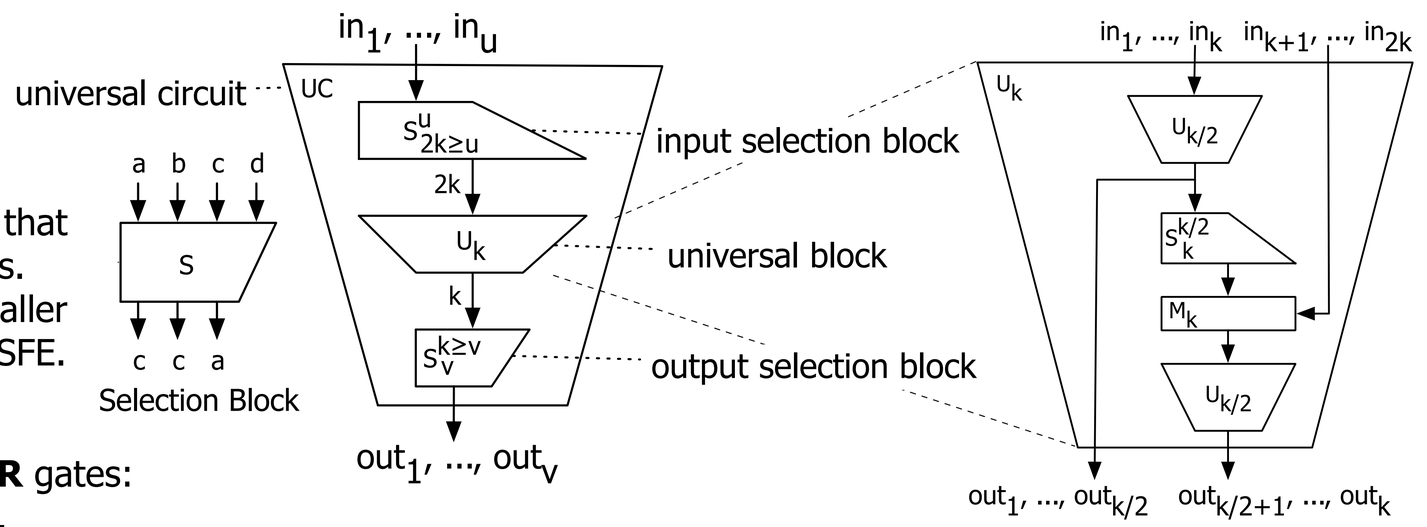
Summary and comparison of **known SFE protocols** with different representations of the boolean function f as boolean circuit or ordered binary decision diagram (OBDD).

parties follow protocol but try to learn additional information | parties may cheat arbitrarily | usage of Random Oracles

Function Represent.	SFE Protocol	Proof of Security: semi-honest	malicious	RO	Evaluation Speed (Encryption Scheme)
Circuit	Yao [Yao86]	X			slow (E_{spec})
	Fairplay [MNPS04]	X	X	X	medium (H)
	GESS [Kol05]	X			very fast (XOR)
	improved SFE	X	X	X	medium/very fast (H/XOR)
OBDD	OBDD SFE [KJGB06]	X			slow (E_{spec})
	improved OBDD SFE	X	X		fast (E)

Extension of OBDD-based SFE protocol [KJGB06] (secure in semi-honest model) to malicious model and **OBDD-based PF-SFE protocol** with small overhead.

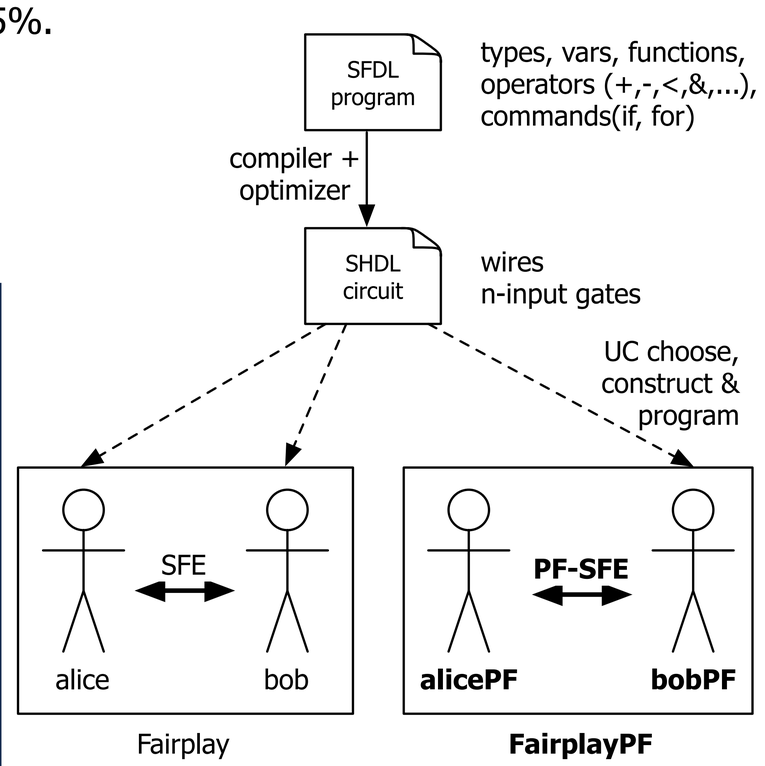
PF-SFE can be reduced to SFE of a Universal Circuit (UC) that can be programmed to compute any function f of size k gates. Our **practical UC construction*** [KS08] is up to 50% smaller than the best UC of Valiant [Val76] when used in today's PF-SFE.



Our **improved SFE protocol*** allows **free** evaluation of **XOR** gates:
- Based on SFE protocols Fairplay [MNPS04] & GESS [Kol05].
- Improves many important functions (e.g. addition, equality test) to 50%.
- UC-based PF-SFE protocols can be improved to even 25%.

Implementation of **FairplayPF**, an extension of the well-known Fairplay SFE system for practical PF-SFE.

http://thomaschneider.de/FairplayPF



Bibliography

[KJGB06] Louis Kruger, Somesh Jha, Eu-Jin Goh, and Dan Boneh. **Secure function evaluation with ordered binary decision diagrams.** In Proc. ACM CCS, pages 410–420. ACM Press, 2006.

[Kol05] Vladimir Kolesnikov. **Gate evaluation secret sharing and secure one-round two-party computation**. In Advances in Cryptology – ASIACRYPT 2005, volume 3788 of LNCS, pages 136–155. Springer, 2005.

[KS08] Vladimir Kolesnikov and Thomas Schneider. **A practical universal circuit construction and secure evaluation of private functions**. In Financial Cryptography and Data Security, FC08, LNCS. Springer, 2008.

[MNPS04] Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella. **Fairplay - a secure two-party computation system**. In USENIX, 2004.

[Val76] Leslie G. Valiant. **Universal circuits (preliminary report)**. In Proc. 8th ACM Symp. on Theory of Computing, pages 196–203, New York, NY, USA, 1976. ACM Press.

[Yao86] Andrew C. Yao. **How to generate and exchange secrets**. In Proc. 27th IEEE Symp. on Foundations of Comp. Science, pages 162–167, Toronto, 1986. IEEE.

Friedrich-Alexander-Universität Erlangen-Nürnberg