

# Practical Approaches to Secure Computation

Ronald Cramer<sup>1</sup>, Eike Kiltz<sup>1</sup>, Berry Schoenmakers<sup>2</sup>, Tomas Toft<sup>1,2</sup>, Pim Tuyls<sup>3</sup>, José Villegas<sup>2</sup>

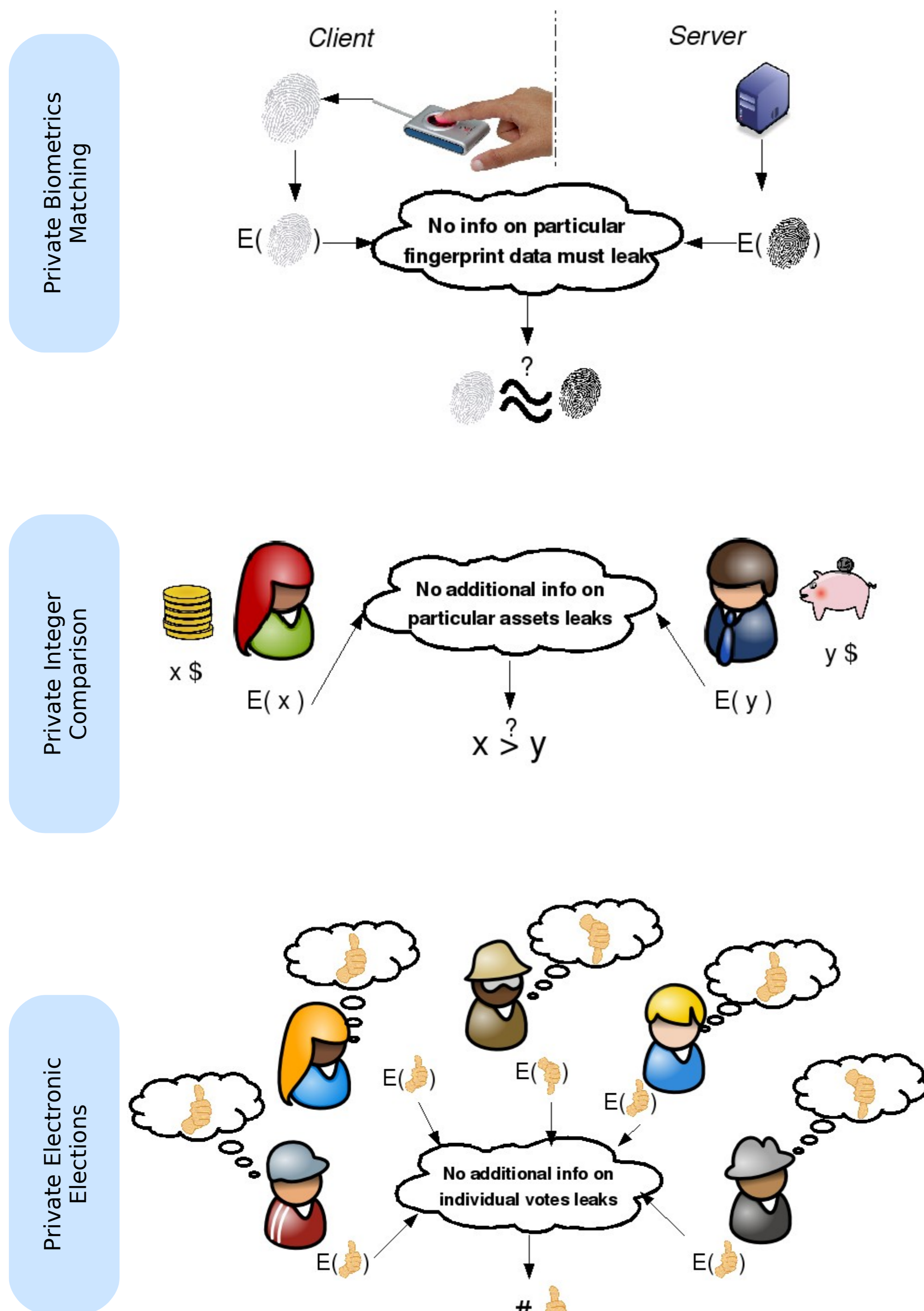
<sup>1</sup> CWI, <sup>2</sup> TU Eindhoven, <sup>3</sup> Philips Research Labs

ronald.cramer@cwi.nl, kiltz@cwi.nl, berry@win.tue.nl, t.toft@tue.nl, pim.tuyls@philips.com, j.a.villegas@tue.nl

**Secure Computation** deals with the following situation: Two (or more) parties want to perform a computation jointly. Each party needs to contribute its private input to this computation, but no party wants to disclose its private inputs to the other parties, or to any third party.

## Motivating Examples

Computing with encrypted data



## General Setting

- Mutually distrusting parties jointly perform a given task

### Requirements



#### Integrity

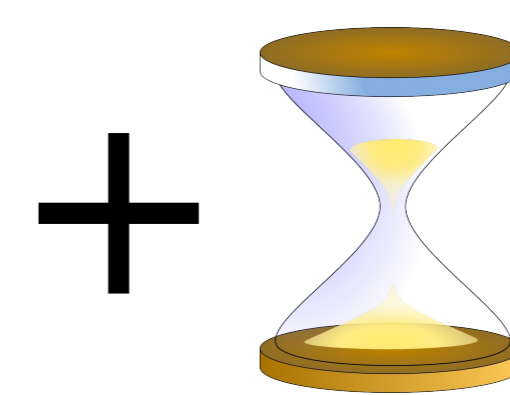
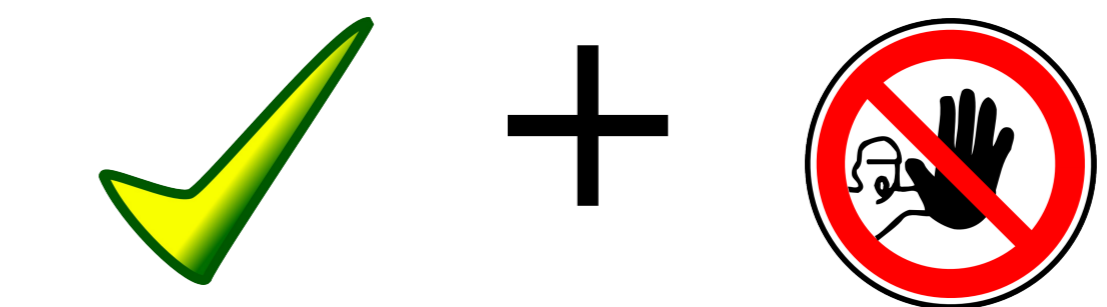
Parties want to be sure that the output of the function is computed correctly



#### Privacy

No more information should be released than what follows from output

## Our Goals



#### Efficiency

Resulting protocols must be applicable in real-life scenarios using reasonable amounts of resources



#### Implementation

Prototyping and executing building blocks to have concrete performance figures, and compare different approaches.

## Some Recent Project Results

### Integer Comparison

This is an important building block for MPC protocols.

- Theoretical:** Constant communication round protocols, solving a long-standing open problem [1].
- Practical:** Simple and computationally efficient protocol with non-constant, yet practical low round complexity [2].

### Test-bed implementation

- The **number of rounds** between parties has been traditionally believed to be *the* time-consuming parameter.
- Important but preliminary tests show that actually **computational cost** is also a bottleneck in time execution of MPC protocols.

## References

- [1] I. Damgård, M. Fitzi, E. Kiltz, J. Nielsen, and T. Toft. *Unconditionally secure constant-rounds multiparty computation for equality, comparison and exponentiation*. In Proc. TCC 2006, volume 3876 of Lecture Notes in Computer Science, pages 285-304.
- [2] J. Garay, B. Schoenmakers, and J. Villegas. *Practical and secure solutions for integer comparison*. In Proc. PKC 2007, volume 4450 of Lecture Notes in Computer Science, pages 330-342.