

# A Pragmatic Introduction to Secure Multi-Party Computation

---

**Suggested Citation:** David Evans, Vladimir Kolesnikov and Mike Rosulek, *A Pragmatic Introduction to Secure Multi-Party Computation*. NOW Publishers, 2018.

**David Evans**

University of Virginia  
evans@virginia.edu

**Vladimir Kolesnikov**

Georgia Institute of Technology  
kolesnikov@gatech.edu

**Mike Rosulek**

Oregon State University  
rosulekm@eecs.oregonstate.edu

This article may be used only for the purpose of research, teaching, and/or private study. Commercial use or systematic downloading (by robots or other automatic processes) is prohibited without explicit Publisher approval.

**now**

the essence of knowledge

Boston — Delft

## Errata

Last update: July 11, 2019

### 23 June 2019

- Footnote 1 on Page 34 (Patricia Thaine): “will reveal  $x$  to  $P_1$ ” should be “will reveal  $x$  to  $P_2$ ”.
- Section 4.1.2 (p. 67, bottom) (Patricia Thaine): The share reconstruction description didn’t include the semantic indexes. To clarify, it should be:

The share reconstruction procedure on input  $sh_{1i}, sh_{2i}$ , outputs  $sh_{1i} \oplus sh_{2i} = s_i$ .

- Section 6.2 (p. 109) (Patricia Thaine):

"It follows that the parties must always perform the second phase, even when  $P_1$  is honest."

should be

"It follows that the parties must always perform the second phase, even when  $P_1$  is caught cheating."

- Section 6.5.1 (p. 113-114) (Patricia Thaine): The given wording could be interpreted ambiguously,

“In other words, the ZK proof should prevent parties from running  $\pi$  honestly, but with different inputs in different rounds.”

Replaced with:

“In other words, the ZK proof should prevent parties from running  $\pi$  with different inputs in different rounds.”

### 10 July 2019

- Fixes to notation in Section to avoid confusion in  $\Delta$  notation.