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

now
the essence of knowledge
Boston — Delft

Errata

Last update: October 2, 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 P1 is honest."

  should be

  > "It follows that the parties must always perform the second phase, even when P1 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 π honestly, but with different inputs in different rounds.”

  Replaced with:

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

10 July 2019

- Fixes to notation in Section 4.1 (the GESS construction) to avoid confusion in the Δ notation. (Shengchao Ding)

23 Aug 2019

- Section 4.1.3, p. 71, line 2-3 (Shengchao Ding): "when v_a is false, $v_c = v_b$" should be "when v_a is true, $v_c = v_b$"
- Section 4.2.2, several instances (Shengchao Ding): "CMBC-GC" should be "CBMC-GC"

2 October 2019

- Figure 3.4 (BMR Multi-Party GC Generation) (Kelong Cong): line 23 of the figure has $w_{c,1}^0$, but it should be $w_{c,1}^1$.