Erratum to the paper "Protocol composition for arbitrary primitives" (CSF 2010)

Véronique Cortier, Loria - CNRS

April 23, 2017

Theorem 3 of paper [1] (obtained as a corollary to the main result, Theorem 1) is unfortunately wrong. Indeed, consider a protocol P (using the notations of [1]) that always binds x_k and y_k to the same value (no freshness). Consider a protocol Q that is insecure as soon as x_k and y_k are bound to the same value in two different sessions. Then Q is secure but the composed protocol R is not.

This issue was actually pointed in Section III.A (key freshness) of our paper.

Acknowledgments

I would like to thank Myrto Arapinis, Stéphanie Delaune, Vincent Delaune as well as Rohit Chadha, Mahesh Viswanathan, Matt Bauer for having independently pointed me the flaw.

References

[1] Ş. Ciobâcă and V. Cortier. Protocol composition for arbitrary primitives. In *Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10)*, pages 322–336, Edinburgh, Scotland, UK, July 2010. IEEE Computer Society Press.