SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Fiat–Shamir Bulletproofs are Non-Malleable (in the Algebraic Group Model)

Chaya Ganesh [*] Claudio Orlandi [†] Mahak Pancholi [*] Akira Takahashi [*]
Daniel Tschudi [‡]

Keywords: Non-interactive Zero-knowledge, Simulation-extractability, Fiat-Shamir, Algebraic Group Model

Abstract

Bulletproofs (Bünz et al. IEEE S&P 2018) are a celebrated ZK proof system that allows for short and efficient proofs, and have been implemented and deployed in several real-world systems.

In practice, they are most often implemented in their *non-interactive* version obtained using the Fiat-Shamir transform, despite the lack of a formal proof of security for this setting.

Prior to this work, there was no evidence that *malleability attacks* were not possible against Fiat-Shamir Bulletproofs. Malleability attacks can lead to very severe vulnerabilities, as they allow an adversary to forge proofs re-using or modifying parts of the proofs provided by the honest parties.

In this paper, we show for the first time that Bulletproofs (or any other similar multi-round proof system satisfying some form of *weak unique response* property) achieve *simulation-extractability* in the *algebraic group model.* This implies that Fiat-Shamir Bulletproofs are *non-malleable.*

The full version of the paper is available at [GOP$^+$21].

References

[GOP$^+$21] C. Ganesh, C. Orlandi, M. Pancholi, A. Takahashi, and D. Tschudi. Fiat–shamir bulletproofs are non-malleable (in the algebraic group model). Cryptology ePrint Archive, Report 2021/1393, 2021. https://ia.cr/2021/1393.

[*] Indian Institute of Science, CSA IISc, Bengaluru 560012, India
[†] Aarhus University, Åbogade 34, 8200 Aarhus N, Denmark
[‡] Concordium, Rennweg 57, 8001 Zurich, Switzerland