AmorE: Amortized Efficiency for Pairing Delegation

Anonymous Author(s)

ABSTRACT

Bilinear pairings are extensively utilized in cryptography. Despite their widespread use, pairings remain one of the least efficient cryptographic tools in many protocols. In this paper, we explore methods to securely and efficiently outsource pairing computations from a resource-constrained device (client) to an untrusted server. Existing protocols for securely outsourcing pairing computations are either inefficient or achieve efficiency only in the online phase, as they require at least one pairing computation in the offline phase. We take a different approach and focus on Amortized Efficiency (AmorE): leveraging an initial pairing computation to securely verify the correctness of polynomially many outsourced pairing computations on public inputs. AmorE builds on top of LOVE (Aranha et al., Latincrypt21) and essentially chains together an optimized version of LOVE in a manner that maintains the statistical security of the scheme under sequential repetitions. We show that AmorE can bootstrap one trusted pairing computation to sequentially verify multiple outsourced pairing computations efficiently, in a way that does not require the client device to store libraries needed for the pairing computation. This enables to execute pairing-based cryptographic algorithms on IoT devices, which otherwise would not have the storage or computational power to handle the aforementioned libraries. To showcase this feature in a practical scenario, we introduce ProdAmorE, an efficient variant of AmorE that enables the client to verify an arbitrary number of aggregate signatures without executing any pairing computations. The performance achieved by AmorE in our implementation marks it as the first pairing delegation protocol capable of claiming speedups ranging between 9.5% and 36.9% for the *entire* client computation compared to computing the pairing locally.

CCS CONCEPTS

• **Security and privacy**;

KEYWORDS

Delegation of Computation, Bilinear Pairings, Security, Efficiency.

ACM Reference Format:

Anonymous Author(s). 2018. AmorE: Amortized Efficiency for Pairing Delegation. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation emai (Conference acronym 'XX).* ACM, New York, NY, USA, 1 page. https://doi.org/XXXXXXX.XXXXXXX

Conference acronym 'XX, June 03–05, 2018, Woodstock, NY

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/XXXXXXX.XXXXXXX