# Cryptology ePrint Archive: Report 2011/231

**History-Free Sequential Aggregate Signatures**

*Marc Fischlin and Anja Lehmann and Dominique Schröder*

**Abstract:** Aggregation schemes allow to combine several cryptographic values like message authentication codes or signatures into a shorter value such that, despite compression, some notion of unforgeability is preserved. Recently, Eikemeier et al. (SCN 2010) considered the notion of *history-free* sequential aggregation for message authentication codes, where the sequentially-executed aggregation algorithm does not need to receive the previous messages in the sequence as input. Here we discuss the idea for signatures where the new aggregate does not rely on the previous messages and public keys either, thus inhibiting the costly verifications in each aggregation step as in previous schemes by Lysyanskaya et al. (Eurocrypt 2004) and Neven (Eurocrypt 2008). Analogously to MACs we argue about new security definitions for such schemes and compare them to previous notions for history-dependent schemes. We finally give a construction based on the BLS signature scheme which satisfies our notion.

**Category / Keywords:** public-key cryptography / Aggregation, Signature, History-Freeness

**Date:** received 10 May 2011, last revised 30 Jun 2011

**Contact author:** marc fischlin at gmail com