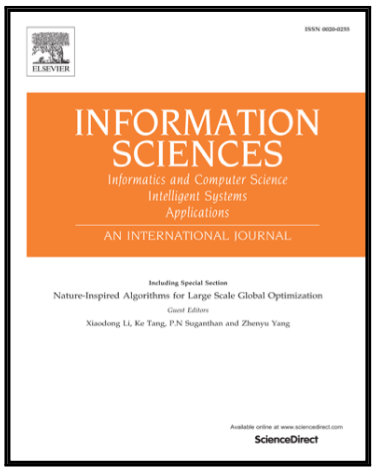


# FAS: Forward Secure Sequential Aggregate Signatures for Secure Logging

Jihye Kim, Hyunok Oh

PII: S0020-0255(17)30040-3
DOI: https://doi.org/10.1016/j.ins.2018.08.044
Reference: INS 13888

To appear in: *Information Sciences*

Received date: 4 January 2017
Revised date: 25 May 2018
Accepted date: 20 August 2018

Please cite this article as: Jihye Kim, Hyunok Oh, FAS: Forward Secure Sequential Aggregate Signatures for Secure Logging, *Information Sciences* (2018), doi: https://doi.org/10.1016/j.ins.2018.08.044

# FAS: Forward Secure Sequential Aggregate Signatures for Secure Logging

Jihye Kim

*Kookmin University, Seoul, Korea*

Hyunok Oh*

*Hanyang University, Seoul, Korea*

**Abstract**

Audit logs are an elemental part of computer systems due to their forensic value. Safeguarding audit logs on a physically unprotected machine are a challenging work, especially in the presence of active adversaries. Forward security is necessary for such a logging system. In this paper, we propose a new Forward secure sequential Aggregate Signature (FAS) scheme with optimal storage and communication for keys and signatures. To the best of our knowledge, our FAS scheme is the only scheme that has constant-sized public and secret keys as well as constant-sized aggregate signatures. Our proposed scheme supports aggregation of consecutive signatures by a third party. We prove the security of our proposed scheme under the hardness of factoring assumption, in the random oracle model.

*Keywords:* Forward security, digital signature, proven security, aggregation

## 1. Introduction

Audit logs are a standard tool for computer system developers and administrators. They record the "what happened when by whom" of the system. This information can record faults and help their diagnosis. It can identify security

*Corresponding author
*Email address:* hoh@hanyang.ac.kr (Hyunok Oh)