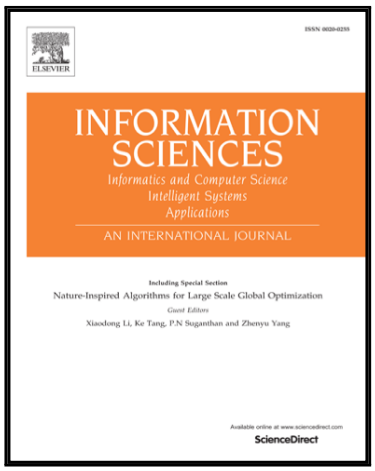

Forward-Secure ID based Digital Signature Scheme with Forward-Secure Private Key Generator

Hyunok Oh, Jihye Kim, Ji Sun Shin

PII: S0020-0255(16)32010-2
DOI: 10.1016/j.ins.2018.04.049
Reference: INS 13592

To appear in: *Information Sciences*

Received date: 14 December 2016
Revised date: 28 March 2018
Accepted date: 14 April 2018

Please cite this article as: Hyunok Oh, Jihye Kim, Ji Sun Shin, Forward-Secure ID based Digital Signature Scheme with Forward-Secure Private Key Generator, *Information Sciences* (2018), doi: 10.1016/j.ins.2018.04.049

Forward-Secure ID based Digital Signature Scheme with Forward-Secure Private Key Generator

Hyunok Oh

Hanyang University, Seoul, Korea

Jihye Kim

Kookmin University, Seoul, Korea

Ji Sun Shin*

Sejong University, Seoul, Korea

Abstract

In an identity based digital signature scheme, a private key generator (PKG) uses its master secret key to issue a user private key to an ID. Thus, forward secrecy of the system is not retained unless forward secrecy of the master secret key is provided. However, current forward secure identity based digital signature schemes only focus on forward secrecy of *user* private keys.

In this paper, we capture forward secrecy of *both* PKG's master secret and user private keys, and formalize a new definition of "forward-secure ID based signature schemes with forward-secure PKG". Then, we design a scheme and prove its security under the BDHI assumption in the standard model (without random oracles).

Keywords: forward security, digital signature, private key generator, ID based

1. Introduction

Forward security of digital signatures limits the damage upon key exposure by dividing the lifetime into several time periods and using a different key every

*Corresponding author
Email address: jisun.shin@gmail.com (Ji Sun Shin)