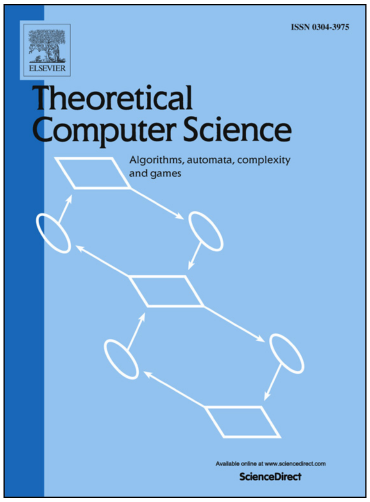
ISSN 0304-3975
ELSEVIER
Theoretical Computer Science
Algorithms, automata, complexity and games
Available online at www.sciencedirect.com
ScienceDirect

Provably Secure Certificate-Based Encryption with Leakage Resilience

Yuyan Guo, Jiguo Li, Yang Lu, Yichen Zhang, Futai Zhang

PII: S0304-3975(17)30748-X
DOI: https://doi.org/10.1016/j.tcs.2017.10.020
Reference: TCS 11358

To appear in: *Theoretical Computer Science*

Received date: 25 December 2015
Revised date: 20 July 2017
Accepted date: 22 October 2017

Please cite this article in press as: Y. Guo et al., Provably Secure Certificate-Based Encryption with Leakage Resilience, *Theoret. Comput. Sci.* (2018), https://doi.org/10.1016/j.tcs.2017.10.020

Provably Secure Certificate-Based Encryption with Leakage Resilience

Yuyan Guo[1,2], Jiguo Li[1], Yang Lu[1], Yichen Zhang[1] and Futai Zhang[3]
[1]College of Computer and Information, Hohai University, 211100, Nanjing, China
[2]School of Computer Science and Technology, Huaibei Normal University, 235000, Anhui, China
[3]School of Computer Science and Technology, Nanjing Normal University, 210096, Nanjing, China

Abstract The security of encryption schemes, in general, has been considered in an ideal environment, where the adversary cannot obtain the secret internal state of the scheme. However, in the real world, an adversary can gain partial information on the secret key through a key leakage attack. To avoid this attack, it is crucial to construct an encryption scheme with leakage resilience. In this paper, we first define a secure leakage-resilient model of certificate-based encryption. In this model, the adversary is permitted to get some information on the secret value through a side-channel attack. Moreover, we put forward a new leakage-resilient certificate-based encryption scheme. This scheme is secure against chosen ciphertext attack under the decisional 3-party Diffie-Hellman assumption in the standard model. Compared with the existing two certificate-based encryption schemes, our scheme enhances the security property, and the execution time of the proposed scheme is less than that of the two certificate-based encryption schemes.

Keywords certificate-based encryption, leakage resilience, side-channel attack

1. Introduction

In public key cryptography (PKC), the users' public keys are not related to their identities. The issue is overcome by a certificate generated by a certificate authority (CA), which provides a trusted link between the users' identities and their public keys. The system uses a public key infrastructure (PKI) that issues and manages the certificates. One of the main efficiency drawbacks of the system is certificate management in PKI when the number of users is very large. To avoid this problem, Shamir [1] proposed the idea of identity-based cryptography (IBC) to reduce the demand of certificates. In IBC, a user's identity is regarded as public key. A trusted third party produces the user's secret key. However, the key escrow problem is inherent in IBC, and the users' secret keys of IBC have to be transmitted through a secure channel. To address the key escrow problem, Al-Riyami and Paterson [2] introduced the idea of certificateless public key cryptography (CL-PKC) in 2003. In CL-PKC, the trusted key generation center provides a partial secret key to a user. This user then merges the partial secret key with a secret value to generate his secret key. Consequently, CL-PKC overcomes the key escrow problem. Nevertheless, the partial secret key should be securely delivered to the user. Thus, the CL-PKC does not avoid the key distribution problem.

In 2003, Gentry [3] first proposed a certificate-based encryption (CBE) scheme, which combines public key encryption (PKE) and identity-based encryption (IBE) while keeping the advantages of each scheme. In CBE scheme, a user produces a pair of public key and secret key and applies to a corresponding certificate, which is generated by the CA. The CBE overcomes the shortcomings of PKE