2017 IEEE 41st Annual Computer Software and Applications Conference

A Lightweight Multi-receiver Encryption Scheme with Mutual Authentication

Ei Khaing Win[†], Tomoki Yoshihisa[†], Yoshimasa Ishi[†], Tomoya Kawakami[‡]
Yuuichi Teranishi[*†], Shinji Shimojo[†*]
[*]*National Institute of Information and Communications Technology, Tokyo, Japan*
[†]*Osaka University, Osaka, Japan*
[‡]*,Nara Institute of Science and Technology, Nara, Japan*
Email: {ei.khaing.win@ais., yoshihisa@, ishi.yoshimasa@, teranisi@, shimojo@}cmc.osaka-u.ac.jp, kawakami@is.naist.jp

***Abstract*—In this paper, we propose a lightweight multi-receiver encryption scheme for the device to device communications on Internet of Things (IoT) applications. In order for the individual user to control the disclosure range of his/her own data directly and to prevent sensitive personal data disclosure to the trusted third party, the proposed scheme uses device-generated public keys. For mutual authentication, third party generates Schnorr-like lightweight identity-based partial private keys for users. The proposed scheme provides source authentication, message integrity, replay-attack prevention and implicit user authentication. In addition to more security properties, computation expensive pairing operations are eliminated to achieve less time usage for both sender and receiver, which is favourable property for IoT applications. In this paper, we showed a proof of security of our scheme, computational cost comparison and experimental performance evaluations. We implemented our proposed scheme on real embedded Android devices and confirmed that it achieves less time cost for both encryption and decryption comparing with the existing most efficient certificate-based multi-receiver encryption scheme and certificateless multi-receiver encryption scheme.**

1. Introduction

Due to the emergence and popularity of small devices such as smartphones, sensors, and wearable devices, the role of Internet of Things (IoT) becomes very important. In IoT applications such as healthcare, smart homes and group communications, multi-receiver encryption scheme to ensure confidentiality, integrity, and authenticity is necessary for sensitive data exchanges. Although sensitive data is protected from others, it is sometimes shared with trustworthy and previously known or unknown devices for different purposes. For example, pedestrians who feel concerns of their health around a station would like to consult with nearby doctors or nurses with the purpose of improving experience, getting advice or healthcare. Locations detected by GPS, and vital data generated by body sensors attached to the smartphones are some examples of sensitive personal data.

To securely exchange information with fast computing speed, symmetric encryption scheme can be used. Although it uses only one secret key for two communicating parties, key agreement protocol to agree on a shared key or key distribution protocol is required. These protocols introduce security requirements such as authentication of parties in key agreement protocol or secure and integrity-assured key distribution to prevent man-in-the-middle attacks and other attacks. Without the use of public-key cryptography, symmetric key scheme is not sufficient to get secure communication features such as confidentiality, integrity, authentication, and non-repudiation.

Although the conventional public key infrastructure (PKI) is widely used in the current ICT systems, it is not suitable for resource-constrained devices due to its certificate overhead [1]. In identity-based cryptography, unique strings such as identities are used as public keys to simplify certificate management. However, unconditionally trusted third party called key generation center (KGC) or (PKG) exists to generate system parameters and private keys for all users. As private key generator knows all users' private keys, it can eavesdrop all exchanged messages. This problem is called key escrow problem. For multi-receiver setting, several identity-based schemes ([2]- [12]) have been proposed. However, key escrow problem exists in those schemes. There are some identity-based encryption schemes without key escrow problem ([13], [14]) for single-receiver setting and [15] for multi-receiver setting. However, multi-receiver encryption scheme [15] does not achieve source authentication, implicit user authentication and reply attack prevention that are required for secure data exchanges.

Contribution: We propose a novel multi-receiver lightweight encryption scheme with key escrow avoidance and certificate-less nature using elliptic curve cryptography. It provides not only implicit user authentication but also more security properties such as source authentication, and replay attack prevention. Moreover, computation expensive pairing operations are eliminated to achieve less time usage for both sender and receiver. In this paper, we provide security proof for the proposed scheme based on the intractability of the Elliptic Curve Discrete Logarithm problem. According to computational cost comparison and

0730-3157/17 $31.00 © 2017 IEEE
DOI 10.1109/COMPSAC.2017.20