論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Multi-Divisible On-Line/Off-Line Cryptography
著者(和文)	山本暖
Author(English)	Dan Yamamoto
出典(和文)	学位:博士(工学), 学位授与機関:東京工業大学, 報告番号:甲第11255号, 授与年月日:2019年9月20日, 学位の種別:課程博士, 審査員:尾形 わかは,植松 友彦,山田 功,田中 圭介,笠井 健太
Citation(English)	Degree:Doctor (Engineering), Conferring organization: Tokyo Institute of Technology, Report number:甲第11255号, Conferred date:2019/9/20, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	要約
Type(English)	Outline

Multi-Divisible On-Line/Off-Line Cryptography

supervisor: Wakaha Ogata

Department of Communications and Integrated Systems
Tokyo Institute of Technology

Dan Yamamoto

August 20, 2019

Outline

In the emerging network environment, e.g., Internet of Things (IoT), more and more computationally-restricted devices as well as bandwidth-restricted devices are connected to each other at any time in any place. Securing their communication is urgently required to make these environment sustainable and scalable. We can use cryptographic schemes as building blocks to achieve security for them, only if it is taken into account that the devices here have restricted resources.

On-line/off-line cryptography, a fundamental concept for many cryptographic systems (e.g., signatures, encryptions, signcryptions, and so forth) is a key to reduce *computational* costs of the devices using the schemes to send their message in confidential and/or authenticated way.

The history of on-line/off-line cryptography began with *on-line/off-line signatures* proposed by Even et al. The signing procedure of on-line/off-line signature scheme is split into the *off-line* phase and the *on-line* phase. The signer can all the computationally-expensive operations in the off-line phase, i.e., in any idle time *before* the sender decides the message to be signed. Then, in on-line phase, i.e., *after* the message is determined, only lightweight operations are required to sign the message so that even low-power devices can handle the signing process.

Gao, Wei, Xie and Tang proposed the notion of *divisible on-line/off-line signatures* later, in which off-line signature tokens can be transmitted to the recipient in the off-line phase so that the senders can save the on-line transmission bandwidth. Hence, it is attractive for not only computationally-restricted devices but also bandwidth-restricted devices.

The other instance of on-line/off-line cryptography, called on-line/off-line encryptions, has been studied mainly in the identity-based settings. An *identity-based on-line/off-line encryption (IBOOE)* scheme has a slightly different feature from (divisible) on-line/off-line signature schemes in the way that *recipient's identity* is regarded as the additional input of the on-line phase. Here, the sender of IBOOE can execute an expensive part of the encryption process even if the identity of the recipient as well as the plaintext is not known.

In this thesis, we propose a general concept of *multi-divisible on-line/off-line cryptography* (MDO cryptography, for short), which covers the above previous on-line/off-line cryptography as well as divisible on-line/off-line signatures.

In general, MDO cryptographic schemes have the following features: (a) Incremental processing: A sender's process can be divided into two or more sub-processes; (b) Incremental sending: Outputs of intermediate sub-processes can be sent prior to all the subsequent sub-processes.

These features enable us to save both computational overhead and transmission bandwidth, on which we can construct secure communication platform for IoT-like environment.

As instances taking full advantage of these two features of MDO cryptography, we introduce notions of multi-divisible on-line/off-line encryptions (MDOEs), incrementally executable signcryptions (IESCs), multi-divisible on-line/off-line signcryptions (MDOSCs), and divisible on-line/off-line tag-based KEMs.

Firstly, we show a notion of *multi-divisible on-line/off-line encryption* (MDOE), which captures the both desirable features of ID-based on-line/off-line encryptions and divisible on-line/off-line signatures. As in the case of ID-based on-line/off-line encryption schemes, a part of encryption process of MDOE can be performed even when the public key of the recipient is unknown. Also as in the case of divisible on-line/off-line signatures, partial ciphertexts in MDOE can be made publicly available for the recipients even when some of the sender's input (e.g., public key or plaintext) is not determined. We define several security notions of MDOEs with regard to three dimensions: the level of divisibility, the number of users, and the number of encryption queries per user. The implications and separations between these security notions are also shown. Furthermore, we present examples of concrete MDOE schemes.

Secondly, we introduce *incrementally executable signcryption* (IESC), a signcryption scheme that supports the incremental processing feature without the incremental sending feature. Here a signcryption process are split into three sub-processes, where the sender can activate each sub-process incrementally by its given sequential input: the sender's key pair, a recipient's public key, and a plaintext message to be sent to the recipient. We can utilize significant intervals between these three sub-processes to perform as much pre-computation as possible.

Thirdly, as a generalized notion of incrementally executable signcryption, we propose a notion of *multi-divisible on-line/off-line signcryption* (MDOSC), here the incremental sending feature is also available for the sender. More specifically, the sender can make partial signed ciphertexts available for the receivers even when some of the sender's input (e.g., public key of the target recipient or plaintext to be signcrypted) is not determined. As with MDOEs, we define several security notions of MDOSCs and show implications and separations between them. Furthermore, we present a generic construction of MDOSC that achieves the strongest security notions.