論文 / 著書情報
Article / Book Information

題目(和文)	完全構造保持署名と耐不可逆漏洩署名に関する構成
Title(English)	Constructions for Fully Structure-Preserving Signature and Uninvertible Leakage Resilient Signature
著者(和文)	王煜宇
Author(English)	Yuyu Wang
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第10754号, 授与年月日:2018年3月26日, 学位の種別:課程博士, 審査員:田中 圭介,伊東 利哉,尾形 わかは,渡辺 治,鹿島 亮
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第10754号, Conferred date:2018/3/26, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	論文要旨
Type(English)	Summary

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

専攻： Department of	数理・計算科学　専攻	申請学位（専攻分野）： Academic Degree Requested	博士 Doctor of　（　理学　）
学生氏名： Student's Name	王 煜宇 (Yuyu Wang)	指導教員（主）： Academic Supervisor(main)	田中　圭介
		指導教員（副）： Academic Supervisor(sub)	

要旨（英文 800 語程度）
Thesis Summary（approx.800 English Words ）

Digital signatures are fundamental cryptographic primitives that give receivers the reason to believe that messages are admitted by claimed senders. Specifically, by using a signature scheme, senders can sign messages by using secret keys only known by themselves, and receivers can verify the validity of the signatures by using the corresponding public information. Roughly, the security of signature schemes ensures that an adversary who does not know secret keys cannot forge signatures. They are used as building blocks in many cryptographic protocols, and also exploited in many digital services where authenticity of digital messages is necessary, such as smart cards, ID cards, digital transactions, and digital contracts. Therefore, signatures compatible with other cryptographic elements and ones that can tolerate powerful attacks in the real world are desirable.

In this thesis, we focus on fully structure-preserving signatures (FSPSs), the notion of which was firstly proposed by Abe Kohlweiss, Ohkubo, and Tibouchi in Eurocrypt 2015, and signatures resilient to uninvertible leakage. The former ones play important roles in many efficient modular protocols, and the latter ones provide strong security guarantee against side-channel attacks. Concretely, we achieve the following results.

Firstly, we propose a general way to obtain FSPSs. More specifically, we bridge the gap between standard structure-preserving signatures (SPSs), which have already been widely studied in prior works, and FSPSs. In FSPSs, all the messages, signatures, verification keys, and signing keys consist only of group elements, while in SPSs, signing keys are not required to be a collection of group elements. To achieve our goal, we introduce two new primitives called trapdoor signature (TS) and signature with auxiliary key (AKS), both of which can be derived from SPSs. By carefully combining both primitives, we obtain generic constructions of FSPS from SPSs. Upon instantiating the above two primitives, we get many instantiations of FSPS with unilateral and bilateral message spaces. Different from previously proposed FSPSs, many of our instantiations also have the automorphic property, which enables a signer to sign his own verification key. As by-product results, one of our instantiations has the shortest verification key size, signature size, and lowest verification cost among all previous constructions based on standard assumptions, and one of them is the first FSPS scheme in the type I bilinear group.

Our main contributions for FSPSs lie in two aspects. First, we formalize the notions of TS and AKS in order to adapt the well-known EGM paradigm to construct FSPSs. Second, we show that most of existing SPS schemes can be cast as TSs and AKSs, and consequently we can obtain a number of FSPSs and FASs based on existing SPSs. Perhaps interestingly, although most of the previously proposed SPS schemes with a unilateral message space are not automorphic (since their verification keys and messages usually consist of elements in different source groups), when some of them are converted into FSPSs by using our method, the resulting schemes become automorphic.

Then we propose a fully leakage-resilient (FLR) signature scheme in the selective auxiliary input model, which captures an extremely wide class of side-channel attacks that are based on physical implementations of algorithms rather than public

parameters chosen. Our signature scheme keeps existential unforgeability under chosen message attacks as long as the adversary cannot completely recover the entire secret state from leakage in polynomial time with non-negligible probability. Formally speaking, the leakage is allowed to be any computable uninvertible function on input the secret state, without any additional restriction. We instantiate such a signature scheme by exploiting a point-function obfuscator with auxiliary input (AIPO) and a differing-inputs obfuscator (diO). As far as we know, this is the first signature scheme secure against uninvertible leakage. Furthermore, our signature scheme is public-coin, in the sense that the randomness used in the signing procedure is a part of a signature and no additional secret randomness is used. Additionally, we provide a variant of the above signature scheme, for which leakage functions are additionally required to be injective, and the sizes of the circuits representing leakage functions are upper bounded. This scheme is resilient to uninvertible leakage that information-theoretically determines the secret information, and can be constructed based only on diO, without exploiting AIPO.

Although our constructions are based on strong assumptions, they show that signature schemes resilient to uninvertible leakage are achievable. Furthermore, they can be treated as a solution to the open problem mentioned by Boyle, Segev, and Wichs in Eurocrypt 2011, which is whether it is possible to achieve public-coin (or deterministic) constructions of FLR signature.