論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Cryptographic Obfuscation Based on Secret Key Primitives
著者(和文)	北川冬航
Author(English)	Fuyuki Kitagawa
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11063号, 授与年月日:2019年3月26日, 学位の種別:課程博士, 審査員:田中 圭介,伊藤 利昭,尾形 わかは,鹿島 亮,森 立平,藤崎 英一郎
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第11063号, Conferred date:2019/3/26, 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

系・コース： Department of, Graduate major in	数理・計算科学 系 数理・計算科学 コース	申請学位（専攻分野）： Academic Degree Requested	博士 Doctor of （ 理学 ）
学生氏名： Student's Name	北川 冬航	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 ）

Over the past three decades, cryptographic community has given beautiful solutions to many cryptographic tasks and problems. As a result, we now have many cryptographic tools such as encryption, signature, authentication, protocols, and so on. However, there are still several important cryptographic problems for which we still do not have a solution developed enough. Program obfuscation is one of such cryptographic problems.

Program obfuscation aims to turn programs unintelligible while preserving its functionality.
The goal of program obfuscation is to protect information of program codes against reverse engineering. There are many heuristic approaches to program obfuscation in practice. However, most of such practical attempts had been broken. This fact motivates us to realize program obfuscation whose security is guaranteed in the perspective of cryptography. Program obfuscation is now one of the central topics in cryptography.

The theoretical study of cryptographic program obfuscation was initiated by Barak, Goldreich, Impagliazzo, Rudich, Sahai, Vadhan, and Yang (CRYPTO 2001). They introduced virtual-black-box obfuscation as a formal definition of obfuscation. The definition of virtual black-box obfuscation is intuitive and naturally captures the requirement that obfuscators hide information about programs. However, Barak et al. showed that it is impossible to achieve virtual black-box obfuscation for all circuits. In order to avoid the impossibility result, they also defined a weaker variant of obfuscation called indistinguishability obfuscation (IO). Impossibility of IO for all circuits is not known.

Garg, Gentry, Halevi, Raykova, Sahai, and Waters (FOCS 2013) proposed the first candidate construction of IO for all circuits. Subsequently, many works have shown that IO is powerful enough in the sense that we can achieve a wide variety of cryptographic primitives based on IO though it is weaker than virtual-black-box obfuscation.

While we know the usefulness of IO well, we know very little about how to achieve IO. Although the first candidate construction was demonstrated, we are still at the embryonic stage for constructing IO. All known constructions of IO are based on a little-studied cryptographic tool called multi-linear maps. Moreover, security flaws were discovered in some IO constructions.

Thus, constructing IO based on a standard assumption is still standing as a major open question in the study of cryptography. As a stepping-stone for solving the question, it is important to find a seemingly weaker primitive

that implies IO.

We show that IO for all circuits can be constructed solely from secret-key functional encryption (SKFE). In the construction, SKFE need to be able to issue a-priori unbounded number of functional keys, that is, collusion-resistant. Our strategy is to replace public-key functional encryption (PKFE) in the construction of IO proposed by Bitansky and Vaikuntanathan (FOCS 2015) with puncturable SKFE. Bitansky and Vaikuntanathan introduced the notion of puncturable SKFE and observed that the strategy works. However, it has not been clear whether we can construct puncturable SKFE without assuming PKFE. In particular, it has not been known whether puncturable SKFE is constructed from ordinary SKFE. In this work, we show that a relaxed variant of puncturable SKFE can be constructed from collusion-resistant SKFE. Moreover, we show that the relaxed variant of puncturable SKFE is sufficient for constructing IO.

In addition, we also study the relation of collusion-resistance and succinctness for SKFE. Functional encryption is said to be weakly-succinct if the size of its encryption circuit is sub-linear in the size of functions. We show that collusion-resistant SKFE can be constructed from weakly-succinct SKFE supporting only one functional key. By combining this result with the first result, we show that IO for all circuits can be constructed from weakly-succinct SKFE supporting only one functional key.

（博士課程）
Doctoral Program

東京工業大学
Tokyo Institute of Technology