Diss. ETH No. 23415

Non-Malleable Codes and Public-Key Encryption

A thesis submitted to attain the degree of

Doctor of Sciences of ETH Zurich

(Dr. sc. ETH Zurich)

presented by

Sandro Coretti
MSc in Computer Science, ETH Zurich

born on 23 December 1986
citizen of Bregaglia GR, Switzerland

accepted on the recommendation of

Prof. Dr. Ueli Maurer, examiner
Prof. Dr. Yevgeniy Dodis, co-examiner

2016

Abstract

A constructive perspective on public-key encryption. *Public-key encryption (PKE)* is an extremely important and fundamental cryptographic primitive. The security of PKE has received much attention in the cryptographic literature, and many security notions for PKE have been proposed.

When a PKE scheme is used in a larger protocol, the security of this protocol is proved by showing a reduction of breaking a certain security property of the PKE scheme to breaking the security of the protocol. Consequently, each protocol requires in principle its own tailor-made security reduction. Moreover, which PKE security notion should be used in a given context is a priori not evident: PKE security notions are usually defined in terms of a certain game that an efficient adversary cannot win with non-negligible advantage; the employed games model the use of the scheme implicitly through oracle access to its algorithms, and the sufficiency for specific applications is neither explicitly stated nor proven.

The first part of this thesis proposes a new approach to investigating the application of PKE, following the constructive cryptography (CC) paradigm of Maurer and Renner [MR11]: The basic use of PKE is to enable confidential communication from a sender A to a receiver B, assuming A is in possession of B's public key. One can distinguish two relevant cases: The (non-confidential) communication channel from A to B can be authenticated (e.g., because messages are signed) or non-authenticated. The application of PKE is shown to provide the construction of a secure channel from A to B from two assumed authenticated channels, one in each direction, or, alternatively, if the channel from A to B is completely insecure, the construction of a confidential channel without authenticity.

The composition theorem of CC implies that the assumed channels can either be physically realized or can themselves be constructed cryptographically, and also that the constructed channels can directly be used

in any applications that require such a channel. In other words, several construction steps can be composed, which guarantees the soundness of this approach and eliminates the need for separate reduction proofs.

In addition to the above, several popular game-based security notions (and variants thereof) are revisited and given constructive semantics by demonstrating which type of construction is achieved by a PKE scheme satisfying which notion.

Domain extension for public-key encryption. One approach towards basing public-key encryption (PKE) schemes on weak and credible assumptions is to build "stronger" or more general schemes generically from "weaker" or more restricted ones. One particular line of work in this context was initiated by Myers and shelat [MS09] and continued by Hohenberger, Lewko, and Waters [HLW12], who investigated *domain extension* for CCA-secure PKE—which is the strongest standard PKE security notion, requiring security against attackers with access to a decryption oracle—that is, they provide constructions of multi-bit CCA-secure PKE from single-bit CCA-secure PKE.

It is well-known that encrypting each bit of a plaintext string independently is not CCA-secure—the resulting scheme is *malleable*. The second part of this thesis investigates whether this malleability can be dealt with using the conceptually simple approach—suggesting itself when one takes a constructive view on the issue of PKE domain extension—of applying a suitable non-malleable code (a notion introduced by Dziembowski *et al.* [DPW10]) to the plaintext and subsequently encrypting the resulting codeword bit-by-bit. The attacker's ability to ask multiple decryption queries requires that the underlying code be *continuously* non-malleable (as defined by Faust *et al.* [FMNV14]). Since, as is also shown in this thesis, this flavor of non-malleability can only be achieved if the code is allowed to "self-destruct," the resulting scheme inherits this property and therefore only achieves a weaker variant of CCA security.

The second main contribution of this thesis is formalizing this notion of so-called *indistinguishability under (chosen-ciphertext) self-destruct attacks* (IND-SDA) as CCA security with the restriction that the decryption oracle stops working once the attacker submits an invalid ciphertext. First, it is shown that the above approach based on non-malleable codes yields a solution to the problem of domain extension for IND-SDA-secure PKE, provided that the underlying code is continuously non-malleable against a *reduced* form of bit-wise tampering. Then, it is proved that the code by [DPW10] is actually already continuously non-malleable against (even

full) bit-wise tampering; this constitutes an *information-theoretically* secure continuously non-malleable code, a technical contribution that may be of independent interest. Compared to the previous approaches to PKE domain extension, the resulting scheme is more efficient and intuitive, at the cost of not achieving full CCA security. This result is also one of the first applications of non-malleable codes in a context other than memory tampering.

Self-destruct attacks. The third contribution of this thesis is a thorough investigation of security against self-destruct attacks. A new security notion for PKE dubbed *non-malleability under (chosen-ciphertext) self-destruct attacks* (NM-SDA), which is a natural generalization of IND-SDA security and the so-called (standard) notion of *non-malleability under chosen-plaintext attacks* (NM-CPA), is introduced. The notions of IND-SDA and NM-CPA are shown to be incomparable, which implies that NM-SDA is a *strictly* stronger notion than either of them. A black-box construction by Choi *et al.* [CDMW08] of NM-CPA PKE from basic IND-CPA PKE is shown to also achieve NM-SDA security. As such, NM-SDA is a strongest PKE security notion currently known to be implied by IND-CPA security.

Finally, the thesis treats the domain-extension problem for NM-SDA PKE. It turns out that the approach based on non-malleable codes outlined above cannot work with standard non-malleable codes. Therefore, a novel notion of non-malleable codes with *secret state* is introduced and a code strong enough for the domain extension is constructed.

Zusammenfassung

Public-Key Encryption: Eine konstruktive Perspektive. Public-Key Encryption (PKE) ist eine extrem wichtige und fundamentale kryptographische Primitive. Der Sicherheit von PKE ist bereits viel Aufmerksamkeit gewidmet worden und es gibt dementsprechend eine grosse Anzahl an Sicherheitsdefinitionen für PKE.

Wird PKE in einem Protokoll verwendet, so muss die Sicherheit des Protokolls durch eine Reduktion vom Brechen der PKE auf das Brechen des Protokolls bewiesen werden. Im Prinzip benötigt man deswegen für jedes neue Protokoll eine massgeschneiderte Sicherheitsreduktion. Zudem ist a priori meist unklar, welcher Typ Sicherheit für einen gegebenen Kontext angemessen ist: PKE-Sicherheitsdefinitionen basieren für gewöhnlich auf sogenannten Games, die effiziente Angreifer nur mit vernachlässigender Wahrscheinlichkeit gewinnen können sollen. Solche Games modellieren die Anwendung von PKE bloss implizit durch sogenannte Orakel und im Allgemeinen wird weder die Anwendbarkeit in bestimmten Szenarien bewiesen, noch wird definiert, was Anwendbarkeit überhaupt bedeutet.

Der erste Teil dieser Arbeit schlägt einen neuen Ansatz, basierend auf dem Konzept der Constructive Cryptography (CC) von Maurer und Renner [MR11], vor: Die Standardanwendung von PKE ist es, vertrauliche Kommunikation zwischen einem Sender A und einem Empfänger B zu ermöglichen, falls B den öffentlichen Schlüssel von A besitzt. Man kann zwei relevante Fälle unterscheiden: Der (nicht-vertrauliche) Kanal von A zu B kann authentifiziert oder nicht-authentifiziert sein. Es wird beweisen, dass die Anwendung von PKE die Konstruktion eines sicheren Kanals von A zu B von zwei angenommenen authentifizierten Kanälen – einem pro Richtung – erreicht oder, falls der Kanal von A zu B vollständig unsicher ist, die Konstruktion eines vertraulichen, jedoch nicht-authentifizierten Kanals.

Das Kompositionstheorem von CC impliziert, dass die angenommenen Kanäle entweder physisch implementiert oder ihrerseits selbst mittels

kryptographischen Protokollen realisiert werden können, und auch, dass die konstruierten Kanäle direkt in jeder Anwendung eingesetzt werden können, die solche Kanäle erfordert. Anders gesagt: Konstruktionsschritte im obigen Sinn können aneinandergefügt – komponiert – werden. Dies macht den auf CC basierenden Ansatz solide und eliminiert die Notwendigkeit von separaten Reduktionsbeweisen.

Zusätzlich zu oben beschriebenem analysiert diese Arbeit mehrere häufig verwendete game-basierte Sicherheitsdefinitionen (sowie Varianten davon) und zeigt, welche Sicherheitsdefinition welche Konstruktion erreicht. Dadurch erhalten die game-basierten Definitionen eine konstruktive Semantik.

Domain Extension für PKE. Eine Art, die Sicherheit von PKE auf schwache und glaubwürdige Annahmen aufzubauen, besteht darin „stärkere“, allgemeinere Verfahren aus „schwächeren“, spezifischeren zu konstruieren. Eine Reihe von Arbeiten, beginnend mit Myers und shelat [MS09] und fortgeführt von Hohenberger, Lewko und Waters [HLW12], untersucht in diesem Sinne das Problem der *Domain Extension* für CCA-Sicherheit, die die stärkste PKE-Sicherheitsstufe darstellt und Sicherheit gegen Angreifer, die Zugriff auf ein sogenanntes Decryption-Orakel haben, erfordert. Domain Extension ist das Problem, aus ein-bit CCA-sicherer PKE, generisch multi-bit CCA-sichere PKE zu erreichen.

Es ist bekannt, dass, wenn jedes Bit einer Nachricht einzeln verschlüsselt wird, das daraus resultierende Verfahren nicht CCA-sicher ist – es ist sogenannt *malleable (verformbar)*. Der zweite Teil dieser Arbeit untersucht daher folgenden, einfachen, von dem CC-Paradigma inspirierten Ansatz: Um eine multi-bit Nachricht zu verschlüsseln, wird diese zunächst mit einem Non-Malleable Code kodiert (ein Konzept, das von Dziembowski *et al.* [DPW10] eingeführt wurde) und anschliessend wird jedes Bit des Codewortes einzeln verschlüsselt. Da der Angreifer Zugriff auf ein Decryption-Orakel hat, muss der zugrundeliegende Code sogenannt *continuously* non-malleable sein (wie von Faust *et al.* [FMNV14] definiert). Die vorliegende Arbeit zeigt, dass diese Art der Non-Malleability jedoch nur erreicht werden kann, wenn der Code einen sogenannten *„self-destruct“*-Modus hat. Dieses Verhalten findet sich im daraus resultierenden PKE-Verfahren wieder, weshalb dieses lediglich eine schwächere CCA-Variante erreicht.

Der zweite Hauptbeitrag dieser Arbeit besteht in der Formalisierung dieses Sicherheitsbegriffs, der sogenannten *indistinguishability under (chosen-ciphertext) self-destruct attacks* (IND-SDA) als CCA-Sicherheit mit der Einschränkung, dass das Decryption-Orakel nur solange funktioniert, bis

der Angreifer die erste ungültige Anfrage macht. Es wird gezeigt, dass der obige auf Non-Malleable Codes basierende Ansatz für die Domain Extension von IND-SDA-sicherer PKE geeignet ist, falls der verwendete Code gegen eine bestimmte Form von *reduziertem* bit-weisem Tampering non-malleable ist. Danach wird bewiesen, dass der Code von [DPW10] bereits continuously non-malleable ist, sogar gegen *vollwertiges* bit-weises Tampering. Dies stellt einen *informations-theoretisch* sicheren continuously non-malleable Code dar, was ein technischer Beitrag von unabhängigem Interesse sein mag. Im Vergleich zu den vorhergehenden Lösungen im Bereich der Domain Extension für PKE ist das hier vorgestellte Verfahren effizienter und intuitiver, erreicht jedoch nicht die volle IND-CCA-Sicherheitsstufe. Das beschriebene Resultat ist ebenfalls eine der ersten Anwendungen von Non-Malleable Codes ausserhalb des Bereichs des sogenannten Memory Tampering.

Self-Destruct-Attacken. Der dritte Beitrag dieser Arbeit ist eine Analyse der Sicherheit unter Self-Destruct-Attacken. Eine zusätzliche Sicherheitsdefinition, genannt *non-malleability under (chosen-ciphertext) self-destruct attacks* (NM-SDA), wird präsentiert. Es handelt sich dabei um eine natürliche Verallgemeinerung von IND-SDA und der sogenannten (in der Literatur bekannten) *non-malleability under chosen-plaintext attacks* (NM-CPA). Es wird gezeigt, dass IND-SDA- und NM-SDA-Sicherheit nicht vergleichbar sind, was bedeutet, dass NM-SDA *strikt* stärker als die beiden ist. Eine black-box Konstruktion von Choi *et al.* [CDMW08], ursprünglich von NM-CPA PKE basierend auf PKE der grundlegendsten Sicherhietsstufe IND-CPA, ist sogar NM-SDA-sicher, wie in dieser Arbeit bewiesen wird. Dadurch ist NM-SDA eine stärkste derjenigen Sicherheitsstufen, über die bekannt ist, dass sie von IND-CPA aus erreicht werden können.

Schliesslich betrachtet diese Arbeit das Domain Extension-Problem auch für NM-SDA-Sicherheit. Dabei stellt sich heraus, dass dieser Ansatz basierend auf gewöhnlichen Non-Malleable Codes nicht funktionieren kann. Deshalb wird ein neues Konzept von Non-Malleable Codes mit *geheimem Zustand* eingeführt und ein Code vorgestellt, der genügend stark für NM-SDA-Domain Extension ist.