Cryptographic Protocols for Privacy-Preserving Access Control in Databases

DISS. ETH NO. 21835

CRYPTOGRAPHIC PROTOCOLS FOR PRIVACY-PRESERVING ACCESS CONTROL IN DATABASES

A thesis submitted to attain the degree of

DOCTOR OF SCIENCES of ETH ZURICH
(Dr. sc. ETH Zurich)

presented by

MARIA DUBOVITSKAYA

Dipl. Information Security & Dipl. Econ. Management
Moscow Engineering Physics Institute (State University)

born on 22 June 1984
citizen of Russian Federation

accepted on the recommendation of
Prof. Dr. Ueli Maurer, examiner
Dr. Jan Camenisch, co-examiner
Prof. Dr. Anna Lysyanskaya, co-examiner

2014

Abstract

A large number of electronic transactions involve querying databases. While service providers need to have access controls in place to ensure that data is properly protected, users are concerned about the amount of information that service providers and also third parties can infer from a transaction. For example, statistics about patent search queries can reveal sensitive information about the company's research strategy. Therefore, privacy-preserving access control protocols are a key ingredient of the modern IT infrastructure. In this dissertation, we provide new efficient cryptographic protocols for privacy-preserving access control.

First, we present protocols that provide anonymous and oblivious access to databases. We consider a database, where every record has an access control policy. We propose an oblivious transfer with access control protocol that allows only authorized users to access a record, while the database provider does not learn which record was accessed and by whom. Moreover, the users' access rights can be revoked. We further extend this work for a practical application of buying records from a database in a privacy-preserving way with the first unlinkable priced oblivious transfer protocol with rechargeable wallets. We also provide an option of hiding the access control policies from the users and propose the first oblivious transfer protocol that supports hidden access control policies.

Second, we improve our protocols to provide strong security guarantees. We develop efficient oblivious transfer protocols that guarantee security under concurrent composition in the standard model and under well-established cryptographic assumptions. To achieve that, instead of using discrete logarithm based primitives, including interactive Schnorr proofs, we employ a recent framework that makes use of the non-interactive Groth-Sahai proofs and compatible cryptographic primitives that are called structure-preserving.

Third, we contribute to the above framework by developing new methods and primitives and proving a number of impossibility results. Namely, we present new methods for performing multiplicative homomorphisms and proof optimizations for Groth-Sahai proofs. We propose a new structure-preserving signature scheme, a new vector commitment scheme, and an unlinkable quotable signature scheme. The latter we use to construct an efficient non-interactive anonymous credential system, where a presentation proof is independent of the number of attributes in a credential. Finally, we show that it is impossible to construct structure-preserving

verifiable unpredictable functions, or more precise, algebraic structure-preserving deterministic primitives that satisfy provability, uniqueness, and unpredictability. This result extends to structure-preserving verifiable random functions, unique signatures, pseudorandom functions and deterministic public key encryption that are key building blocks in many cryptographic protocols.

Zusammenfassung

Heutzutage involviert eine grosse Anzahl elektronischer Transaktionen Datenbankabfragen. Während Dienstanbieter den Zugang zu den Daten vor unberechtigem Zugriff schützen wollen, liegt die Sorge der Benutzer in der Information, welche die Dienstanbieter aus den durchgeführten Transaktionen herleiten können. Statistische Informationen die aus Suchanfragen auf Patentdatenbanken extrahiert werden, können beispielsweise Informationen über die Forschungsstrategie des zugreifenden Unternehmens enthüllen. Daher sind datenschutzerhaltende Zugriffskontrollprotokolle ein wichtiger Baustein moderner IT-Infrastrukturen. In dieser Dissertation präsentieren wir neuartige effiziente Algorithmen für Zugriffskontrolle in Datenbanken, welche die Privatsphäre schützen.

Erstens zeigen wir Protokolle zum anonymen Zugriff auf Datenbanken, die vergessliche Datenbankabfragen ermöglichen, also Oblivious-Transfer-Protokolle zulassen. Wir legen dabei die Annahme zugrunde, dass in den entsprechenden Datenbanken jeder Eintrag eine Zugriffskontrollregel assoziiert hat. Wir schlagen ein Oblivious-Transfer-Protokoll mit Zugriffskontrolle vor, welches nur autorisierten Benutzern erlaubt, einen Eintrag abzufragen. Gleichzeitig lernt der Datenbankanbieter keinerlei Information (nach informationstheoretischer Definition) darüber, auf welchen Eintrag oder von welchem Benutzer zugegriffen wurde. Die Zugriffsrechte von Benutzern können dabei durch den Anbieter wiederrufen werden. Wir erweitern dieses Resultat für den praktischen Anwendungsfall des datenschutzerhaltenden kommerziellen Zugriffes auf Datenbankeinträge im Rahmen des ersten unverknüpf-baren Oblivious-Transfer-Protokolles mit Preisangaben und wiederaufladbaren Geld-börsen. Wir ermöglichen das optionale Geheimhalten der Zugriffskontrollregeln vor den Benut-zern und schlagen das erste Oblivious-Transfer-Protokoll mit geheimgehaltenen Zugriffskontrollregeln vor.

Zweitens verbessern wir unsere Protokolle dahingehend, dass sie stärkere Sicherheitseigenschaften aufweisen. Wir entwickeln effiziente Oblivious-Transfer-Protokolle, welche Sicherheit unter nebenläufiger Protokollkomposition im Standardmodell und unter wohletablierten kryptographischen Annahmen garantieren. Um dies zu erreichen, haben wir anstelle von diskreten-Logarithmus-basierten Primitiven, wie beispielsweise interaktiven Schnorr-Beweisen, ein neues Framework verwendet, welches nichtinteraktive Groth-Sahai-Beweise und damit kompatible kryptographische Primitive, welche als strukturerhaltend bezeichnet werden, nutzt.

Drittens erweitern wir obengenanntes Framework durch neue Methoden und Primitive und beweisen eine Reihe von Unmöglichkeitsresultaten. Konkret präsentieren wir neue Methoden zum Berechnen von multiplikativen Homomorphismen und zeigen Optimierungen von Groth-Sahai-Beweisen. Wir präsentieren ein neues strukturerhaltendes Signaturverfahren, ein neues Vektor-Commitmentverfahren und ein unverknüpfbares zitierbares Signaturverfahren. Letzteres benutzen wir dazu, ein effizientes nichtinteraktives anonymes Zertifikatssystem zu konstruieren, welches sich dadurch auszeichnet, dass ein Präsentationsbeweis unabhängig von der Anzahl der Attribute des zu präsentierenden Zertifikats ist. Schliesslich zeigen wir, dass es unmöglich ist, strukturerhaltende verifizierbare unvorhersagbare Funktionen zu konstruieren, oder, präziser ausgedrückt, algebraische strukturerhaltende deterministische Primitive, welche die Eigenschaften der Beweisbarkeit, Einzigartigkeit und Unvorhersagbarkeit aufweisen. Dieses Resultat kann auf strukturerhaltende verifizierbare Zufallsfunktionen, einzigartige Signaturen, Pseudozufallsfunktionen und deterministische Public-Key-Kryptosysteme erweitert werden, welche wichtige Bausteine von vielen kryptographischen Protokollen sind.