2019-01640 - PhD Position F/M [Campagne Cordi-S] Searchable Encryption

Niveau de diplôme exigé : Bac + 5 ou équivalent
Fonction : Doctorant

Contexte et atouts du poste

The PhD will be co-supervised by:
- Brice Minaud, CR Inria, 80%, https://www.di.ens.fr/brice.minaud/
- Michel Abdalla, DR C2SIS, 20%, https://www.di.ens.fr/michel.abdalla/
within the CASCADE project-team.

Summary. The PhD topic belongs to the field of cryptography. Searchable encryption enables clients to outsource the storage of their data, and issue search queries over the data, while hiding the contents of the data and queries from the server hosting the data and processing the queries. The goal of the PhD is to further our understanding of the practical security of searchable encryption schemes, and to build new solutions, that offer more thorough security guarantees, and a richer functionality.

Motivation. It has become commonplace for individuals and businesses to outsource large amounts of their data to the cloud. The benefits cloud storage brings in areas such as scalability, availability, and persistence, are universally acknowledged. Outsourcing data, however, means sending it to an external service provider, which the user may not trust. Even if the service provider is fully trusted, high-profile breaches into the databases of major companies, where hackers are able to steal clients' data, occur all too frequently. The Snowden mass surveillance revelations compound the problem. Moreover, by nature of cloud storage, it is often difficult for the service provider to offer strong guarantees regarding who is able to access the data, as it is replicated across several data centers in various geographical regions. In addition, in cases such as medical data, ensuring that the data remains private is mandated by law in many countries. The General Data Protection Regulation (GDPR) recently adopted by the European Union is a case in point. All these factors highlight the need to encrypt sensitive data whenever it is stored in the cloud.

Encryption, however, comes at a cost. The promise of standard modern encryption is to make encrypted data essentially indistinguishable from random bits by design, it cannot be searched, or otherwise meaningfully interacted with. This represents a huge loss of functionality relative to plain local storage, and a major drawback of encrypted cloud storage.

As an example, an email provider may wish to store its users' emails in an encrypted form to provide privacy, but it is obviously highly desirable that users should still be able to search for emails that contain a given word, or whose date falls within a given range. Businesses may also want to outsource databases containing sensitive information, such as client data, to dispense with having to maintain their own infrastructure. To be usable at all, the outsourced encrypted database should still offer some form of search functionality. Failing that, the entire database must be downloaded to process each query, defeating the purpose of cloud storage.

At the core of the issues outlined above lies a conflict between security, which asks that encrypted data should be completely opaque, and functionality, which requires that it can still be interacted with, at least in controlled ways. These problems constitute a major challenge at the intersection of two areas: cryptography and data science. Convincing solutions to these issues would allow users to take full advantage of modern cloud technologies, without sacrificing security, privacy, or usability.

Mission confiée

The PhD candidate will carry out research on searchable encryption. Within that topic, we highlight two main objectives.

First objective: understanding leakage functions.

Current works in the cryptographic literature tackle searchable encryption by offering trade-offs between security and efficiency. The server is able to efficiently process queries on encrypted data at the cost of learning some information on the encrypted data. This information is captured by a leakage function. Searchable encryption schemes come with security proofs showing that under standard cryptographic assumptions, what the server is able to learn from processing queries is no more than the output of the leakage function. The leakage function varies with each proposed scheme. It is a critical parameter of its security model.

In our view, the history of encrypted databases shows that proving the security of a construction with respect to a seemingly reasonable leakage function is unsatisfactory. Indeed, so-called leakage-abuse attacks are able to recover sensitive information from the database (including in some cases reconstructing the entire plaintext database) without contradicting the security proofs of the targeted constructions. Instead, the attack only uses the leakage allowed by the scheme. Thus, it is vital to better understand the concrete implications of various leakage functions as regards the practical security of a scheme. Our ultimate goal along this avenue of research is to propose a classification of leakage functions that paints a clear picture of their concrete security implications, and allows for a better overall understanding of the area. More concretely, due to its generality, the line of work that starts with [1], and continues with [2,3], is a stop in that direction. Part of the goal of the thesis is to continue on that path.

Second objective: building new solutions.

Leakage-abuse attacks act as a powerful guide to build more secure schemes. This is exemplified by the rise of forward-private SSE schemes following file-injection attacks [4]. Likewise, attacks such as [3] imply the need to hide access pattern leakage when handling range queries. More generally, our goal is to leverage the deeper understanding of the implications of leakage functions afforded by the previous objective in order to propose new constructions. Of particular interest would be to propose constructions that not only include security proofs with respect to a particular leakage function, but also take into account the implications of that leakage, in order to offer a truly comprehensive security analysis. Here, a natural starting point is to hide access pattern leakage by adapting oblivious

Informations générales

- Thème/Domaine : Algorithmique, calcul formel et cryptologie
- Systèmes d’information (BAP E)
- Ville : Paris
- Centre Inria : CRI de Paris
- Date de prise de fonction souhaitée : 2019-09-01
- Durée de contrat : 3 ans
- Date limite pour postuler : 2019-05-26

Contacts

- Equipe Inria : CASCADE
- Directeur de thèse : Minaud Brice / brice.minaud@inria.fr

À propos d’Inria

Inria, l’institut national de recherche dédié aux sciences du numérique, promeut l’excellence scientifique et le transfert pour avoir le plus grand impact. Il emploie 2400 personnes. Ses 200 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3000 scientifiques pour relever les défis des sciences informatiques et mathématiques, souvent à l’interface d’autres disciplines. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 160 start-up. L’institut s’efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l’économie.

Consignes pour postuler

La candidature doit contenir :

- CV lettre de motivation
- notes de master
- Des lettres de recommandation peuvent être envoyées directement à la personne au recruteur.
- The application must contain:
- CV cover letter
- master's notes
- Letters of recommendation can be sent directly to the recruter.

Sécurité défense :
Ce poste est susceptible d’être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L’autorisation d’accès à une zone est délivrée par le chef d’établissement, après avis ministériel favorable, tel que défini dans l’arrêté du 03 juillet 2012, relatif à la PPST Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l’annulation du recrutement.

Politique de recrutement :
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.

Attention : Les candidatures doivent être déposées en ligne sur le site Inria.
Le traitement des candidatures adressées par d’autres canaux n’est pas garanti.
RAM techniques to searchable encryption schemes, as is done (in a special case) in a recent work by Mishra et al. (S&P 2018).

Further, while relational databases (and the associated query language, SQL) are the mainstream approach, other types of databases (such as graph databases and associated query languages) exist and are deployed in practice for applications such as social networks and knowledge graphs. However, they have received little attention in the cryptographic community. This leaves open another promising avenue of research.


Principales activités
The PhD candidate will conduct research, and engage in related activities, such as collaborations with other researchers, writing research articles, and participating in international conferences. Beyond searchable encryption, the candidate will have opportunities to learn about research in cryptography more broadly. He or she is also welcome to apply for complementary teaching activities if desired.

Compétences
The applicant should have a Master’s degree in Computer Science or Mathematics, preferably related to Cryptology or Computer Security.

As part of their application, candidates should submit the following documents: a résumé (CV), a grade report from their Master’s degree, and a motivation letter. If available, recommendation letters should be sent to: brice.minaud@inria.fr

Avantages
- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Rémunération
1982 € bruts la première et la deuxième année, 2085 € bruts la troisième année.

1982 € gross salary during the first and second years, 2085 € gross salary the last year.