EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN

Private Schnittmengenberechnung

Gemeinsame Daten schnell, sicher und bequem herausfiltern

Kontakt:
TU Darmstadt/EC SPRIDE
Thomas Schneider
thomas.schneider@ec-spride.de
Michael Zohner
michael.zohner@ec-spride.de
Telefon +49 61 51 16-75 424

Die Informationstechnik expandiert unaufhaltbar in viele Bereiche des alltäglichen Lebens. Allerdings geht die Nutzung moderner Technologien häufig mit der unvermeidbaren Herausgabe privater Daten einher. Für viele Anwendungen kann diese Herausgabe von Daten durch eine kryptographische Technik namens „Private Set Intersection“ (PSI, zu deutsch Private Schnittmengenberechnung) vermieden werden. PSI erlaubt es, gemeinsame Daten schnell, sicher und einfach in einer privatsphären-schützenden Weise zu identifizieren und zugleich alle anderen Daten geheim zu halten.

Viele Aktionen in der digitalen Welt verlangen vom Benutzer die Herausgabe seiner privaten Daten an einen Dienst-Anbieter, um einen Dienst zu nutzen. Ein Beispiel hierfür sind mobile Nachrichten-Apps, die Zugriff auf das Adressbuch eines Benutzers benötigen, um die Kontakte zu finden, die diese Apps ebenfalls nutzen. Die derzeit häufig verwendete Lösung schießt jedoch über das Ziel heraus, da der Dienst-Anbieter alle Kontakte erhält, obwohl er nur die gemeinsamen Daten benötigt. Die Alternative, den Dienst-Anbieter die Liste aller seiner Dienst-Nutzer an den Benutzer schicken zu lassen, ist ebenfalls nicht möglich, da der Dienst-Anbieter dadurch die Privatsphäre seiner Nutzer verletzen würde. Somit befinden sich der Dienst-Anbieter und der Benutzer in einer Pattsituation, die beide daran hindert, die Vorteile einer gemeinsamen Vereinbarung zu nutzen.

Bereitstellung der Funktionalität unter Einhaltung der Privatsphäre

Private Set Intersection ist eine kryptographische Technik die es ermöglicht, diese Pattsituation zu überwinden. PSI ermöglicht es, gemeinsame Daten schnell, sicher und bequem heraus zu filtern, ohne die restlichen Daten offen zu legen. Auf diese Weise erhalten beide Parteien nur die Informationen, die unbedingt zur Bereitstellung der Funktionalität benötigt werden (z.B. alle gemeinsamen Kontakte).

Effiziente Berechnung

Die von der EC SPRIDE Forschungsgruppe an der TU Darmstadt entwickelten PSI-Protokolle nutzen kürzlich entwickelte Innovationen im Gebiet der Kryptographie und bauen auf einer hoch effizienten kryptographischen Technik namens „Oblivious Transfer“ auf. Die resultierenden PSI-Protokolle übertreffen die Effizienz vorheriger sicherer Lösungen um zwei Größenordnungen und sind bereit für den Einsatz in zahlreichen Anwendungen.

Flexibler Einsatz

Aufgrund seiner generischen Funktionalität kann PSI für eine Vielzahl verschiedener Anwendungen eingesetzt werden, z.B.:

- Identifizierung gemeinsamer Kontakte oder Kunden,
- Messung der Effektivität von Werbung,
- Sicherstellung der Exklusivität von Verträgen

Der Quellcode ist verfügbar unter http://encrypto.de/PSI.

PSI

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN

Private Set Intersection

Identifying common data fast, secure, and easy

Contact:
TU Darmstadt/EC SPRIDE
Thomas Schneider
thomas.schneider@ec-spride.de
Michael Zohner
michael.zohner@ec-spride.de
Phone +49 61 51 16-75 424

Modern information technology is expanding into many aspects of everyday life. However, often the use of modern technology goes along with an inevitable loss of data privacy. For many applications, this loss can be avoided using a cryptographic technique called "Private Set Intersection" (PSI). PSI allows fast, secure, and easy identification of common data in a user-controlled and privacy-preserving way.

Many actions in the digital world require the user to reveal a lot of private data to a service provider when using its service. An example are mobile messaging apps, where the service provider gets access to the user's address book in order to identify the contacts that also use this service. However, this solution overachieves the goal as the service provider learns all information although he only needs the common contacts to provide his service. On the other hand, the service provider does not want to disclose its database to the user to preserve the privacy of its clients. Thereby, both parties end up in a stalemate, which hinders both of them to enjoy the benefits of a mutual agreement.

Providing Functionality while Retaining Privacy

Private Set Intersection (PSI) is a cryptographic technique that allows to overcome this stalemate. PSI provides fast, secure, and easy identification of common data while keeping all remaining data hidden. Thereby, both parties can use PSI to reveal only the minimal amount of information that is required in order to provide the functionality (e.g., all common contacts).

Efficient Computation

The protocols for PSI that were developed by the EC SPRIDE research team at TU Darmstadt make use of recent developments in the area of cryptography and use a very efficient underlying cryptographic technique called "oblivious transfer". The resulting PSI protocols are very efficient and improve on existing work by two orders of magnitude and are ready for use on large-scale real-world problems.

Flexible Use

Due to its general functionality,
PSI can be used for several applications such as:

- identification of common contacts or customers,
- measuring efficiency of advertising,
- ensuring exclusivity of contracts.

EC SPRIDE researchers at TU Darmstadt have implemented these protocols with a generic and easy-to-use interface. The source code is available at http://encrypto.de/PSI.

PSI

SPONSORED BY THE
Federal Ministry
of Education
and Research