



Wissenschaftliche Ausarbeitung

PHOABE: Policy-Hidden Outsourced Attribute Based Encryption

Florian Hansen
Hochschule Flensburg

14. April 2020

Zusammenfassung

1 Einleitung

Diese wissenschaftliche Ausarbeitung wird im Rahmen der Hochschulveranstaltung *Hot-Topics in der IT-Security* angefertigt und handelt über den sicheren Datenaustausch zwischen Internet-of-Things-Geräten. Besonders wird hierbei auf die Attribute Based Encryption (ABE) eingegangen, welche ein relativ junges Forschungsgebiet der Kryptographie darstellt. Es existieren zwar einige ABE-Schemata, diese sind jedoch für leistungsschwache Geräte eher ungeeignet.

Diese Ausarbeitung beschäftigt sich hauptsächlich mit der Arbeit von [1], welche ein neues attribut-basiertes Verschlüsselungsschema vorstellt: *PHOABE*. Dieses Schema widmet sich bekannten Problemen der Attribut-basierten Verschlüsselung, wie zum Beispiel das Verstecken der Zugriffsregelungen (*Access-Policies*), die sensitive Daten enthalten können. Zusätzlich fordert das Schema eine Auslagerung des Entschlüsselungsvorganges, welches aufgrund von bilinearen Abbildungen relativ rechenintensiv ist. Hierbei sollen sogenannte *Semi-trusted Cloud Server* den aufwändigen Teil der Berechnung übernehmen, damit auch leistungsschwache Geräte solche attribut-basierte Verschlüsselungen durchführen können.

2 Problembeschreibung

Das *Internet der Dinge*, *Internet of Things* (IoT), hat die Aufgabe, verschiedenste Hardwarekomponenten miteinander zu verbinden und damit einen Datenaustausch zu ermöglichen. Ein gutes Beispiel hierfür sind Smartphones und Sensoren, die ständig miteinander kommunizieren müssen bzw. sollen. Grundsätzlich können IoT-Anwendungen aufgrund ihrer Kommunikationsfähigkeit in zwei Bereiche eingeteilt werden. In Einzelanwendungen benö-

tigen man lediglich eine Autorität während es auch Anwendungsfälle gibt, die über unterschiedliche Bereiche bzw. Domänen kommunizieren müssen. Diese besitzen damit mehrere Autoritäten.

Beide Formen von IoT haben eins gemeinsam. Sie müssen einen sicheren Austausch von Daten und die Sicherung der Privatsphäre gewährleisten. Hierfür werden Daten verschlüsselt und mithilfe von Zugriffskontrollmechanismen nur bestimmten Autoritäten zur Verfügung gestellt. Genau deshalb ist die attribut-basierte Verschlüsselung ein attraktiver Kandidat, da sie Zugriffskontrolle (*Access-Control*) und Verschlüsselung miteinander verknüpft. Ein Problem dabei existiert dennoch. Dieses Verfahren verwendet bilineare Abbildungen, was vor allem in der Entschlüsselung viel Rechenaufwand bedeutet. Für leistungsstarke Desktop-Rechner mag dies weniger eine Rolle spielen, ist jedoch bezogen auf IoT ein großes Problem, denn dort kommunizieren in der Regel Geräte mit sehr eingeschränkten Ressourcen miteinander. Zudem erhöht sich der Rechenaufwand proportional zur Anzahl der Attribute. Das Problem liegt also darin, Daten sicher und effizient zwischen ressourcenarmen Geräten auszutauschen, ohne die Privatsphäre der Benutzer zu verletzen.

3 Motivation

Die attribut-basierte Verschlüsselung ist, wie in der Problembeschreibung bereits erwähnt, ineffizienter, je mehr Attribute verwendet werden. Besonders die Entschlüsselung wird durch die bilinearen Operationen extrem rechenaufwändig, was zur Folge hat, dass dieses Schema auf ressourcenärmeren Geräten und damit auf IoT nur bedingt anwendbar ist. Eine wichtige Frage, die sich also stellt ist, wie man ABE für eben solche Anwendungsfälle anwendbar gestalten kann.

In weiterführenden Arbeiten, so auch der von [2], wird ein neues Konzept in Verbindung mit attribut-basierter Verschlüsselung vorgestellt, um diese effizienter zu gestalten. Für die kostspielige Entschlüsselung ist nun nicht mehr alleine der Benutzer zuständig, sondern eine weitere Instanz. Ein halb vertrauenswürdiger Cloud-Server (*semi-trusted cloud server*, STCS), welcher

den rechenaufwändigen Teil der Entschlüsselung übernehmen soll. Damit der Server keinerlei Informationen über den Entschlüsselten Ciphertext erhält, soll dieser diesen lediglich zum Teil entschlüsseln. Anschließend wird das Ergebnis vom Benutzer selbst entschlüsselt. So soll garantiert werden, dass die rechenaufwändige Arbeit vom STCS und nicht vom Benutzer übernommen wird und trotzdem keinerlei Informationen über die eigentliche Nachricht an dem Server preisgegeben wird.

Eine weitere Überlegung von [1] ist folgende. Was ist, wenn der STCS das teilweise entschlüsselte Chiffre fälscht? Es muss also zusätzlich die Möglichkeit bestehen, dass das Ergebnis der Entschlüsselung des STCS' überprüft werden kann. Einige vergangene Arbeiten haben sich dem Problem gewidmet, jedoch keine effiziente Lösung geboten oder sind inpraktikabel für IoT, da sie sich auf einer einzigen Autorität stützen. Da IoT jedoch hauptsächlich über mehrere Domänen kommuniziert, ist dies keine praktikable Lösung. Die Motivation hinter [1] ist also, ein ausgelagertes, verifizierbares multi-authority ABE-Schema zu entwerfen.

4 Grundlagen

4.1 Zugriffsregeln

Grundsätzlich werden Regeln für den Datenzugriff durch zwei Formate repräsentiert. Zum Einen durch boolsche Funktionen und zum Anderen durch sogenannte Linear Secret Sharing Schemes (LSSS). In diesem Abschnitt sollen beide Repräsentationsmöglichkeiten eingeführt werden.

Definition 1 (Zugriffsstrukturen [3]). *Sei $\{P_1, P_2, \dots, P_n\}$ die Menge der beteiligten Parteien. Eine Sammlung $\mathbb{A} \subseteq 2^{\{P_1, P_2, \dots, P_n\}}$ ist monoton, wenn $\forall B, C. B \in \mathbb{A} \wedge B \subseteq C \implies C \in \mathbb{A}$. Eine Zugriffsstruktur ist damit eine Sammlung \mathbb{A} von nicht-leeren Untermengen von dem Universum $\{P_1, P_2, \dots, P_n\}$. Alle Mengen $A \in \mathbb{A}$ werden als autorisierte Mengen während die nicht in \mathbb{A} vertetenden Mengen als unauthorisierte bezeichnet werden.*

Definition 1 kann dabei so interpretiert werden, als dass alle Obermengen jedes Elements $B \in \mathbb{A}$ vertreten sein müssen. Im Folgenden soll ein Beispiel dies verdeutlichen.

Beispiel (Zugriffsstrukturen). Sei $\mathbb{U} = \{1, 2, 3, 4\}$ ein Universum und $\mathbb{A} \subseteq 2^{\mathbb{U}}$ eine Zugriffsstruktur.

Die Zugriffsstruktur $\mathbb{A} = \{\{1, 2\}, \{3, 4\}\}$ ist nicht monoton, da das Element $\{1, 2, 3\}$ nicht vorhanden ist.

Die Zugriffsstruktur $\mathbb{A} = \{\{3, 4\}, \{1, 3, 4\}, \{1, 2, 3, 4\}\}$ ist monoton, da alle Obermengen der Elemente von \mathbb{A} vorhanden sind.

4.2 Bilineare Abbildungen

5 Attribute Based Encryption (ABE)

5.1 Key-Policy ABE

5.2 Ciphertext-Policy ABE

5.3 Single-Authority

5.4 Multi-Authority

6 Policy-Hidden Outsourced ABE

7 Fazit und Ausblick

Literatur

- [1] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia. PHOABE: Securely outsourcing multi-authority attribute based encryption with po-

- licy hidden for cloud assisted IoT. *Computer Networks*, (133):141–156, 2018.
- [2] M. Green, S. Hohenberger, and B. Waters. Outsourcing the Decryption of ABE Ciphertexts. *USENIX Security Symposium*, 2011.
- [3] R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. Cryptology ePrint Archive, Report 2007/323, 2007. <https://eprint.iacr.org/2007/323>.