Dokumentation

Cloud Kryptographie und deren mögliche Anwendung im E-Government

Version 1.0, 31.12.2015

Bernd Zwattendorfer – bernd.zwattendorfer@egiz.gv.at

Zusammenfassung: Die Erfüllung rechtlicher Rahmenbedingungen, wie z.B. die Sicherung des Datenschutzes, ist meist eines der größten Hindernisse bei der Verwendung von Cloud Computing im E-Government Bereich. Dabei zeigen jedoch Studien, dass Cloud Computing für den öffentlichen Sektor enorme Kostenvorteile mit sich bringen kann. Um diesen Umstand entgegenzuwirken und einen breiteren Einsatz von Cloud Computing im behördlichen Bereich zu ermöglichen, werden in diesem Dokument kryptographische Technologien vorgestellt, die die Erfüllung rechtlicher Rahmenbedingungen auf Basis kryptographischer Technologien in Zukunft ermöglichen könnten. Einziges Hindernis ist dabei der praktische Reifegrad einzelner Technologien, welche derzeit noch nicht für einen Produktivbetrieb geeignet sind.

E-Government Innovationszentrum
Inffeldgasse 16/a, A-8010 Graz
Tel. +43 316 873 5514
Fax. +43 316 873 5520
E-Mail post@egiz.gv.at
www.egiz.gv.at

Das E-Government Innovationszentrum ist eine gemeinsame Einrichtung des Bundeskanzleramtes und der TU-Graz

BUNDESKANZLERAMT ÖSTERREICH
TU Graz
Graz University of Technology

Inhaltsverzeichnis

1 Einleitung

Cloud Computing und sein bedarfs-orientiertes Abrechnungsmodell erlauben es Cloud Service-Konsumenten Kosten zu sparen. Von solch möglichen Kosteneinsparungen können auch Behörden profitieren. Das größte Kosteneinsparungspotential bieten sogenannte Public Clouds, deren Services prinzipiell der Allgemeinheit zur Verfügung gestellt werden. Der große Nachteil von Public Clouds ist jedoch, dass Datenschutzproblematiken auftreten können.

Ein möglicher Ansatz um diesen Datenschutzproblematiken entgegenzuwirken ist die Verwendung von kryptographischen Technologien. Im Rahmen dieses Projekts werden unterschiedliche Technologien der Cloud Kryptographie untersucht und auf deren Eignung für einen möglichen Einsatz im E-Government und Cloud Computing hin bewertet. Der Fokus dabei liegt auf neuen kryptographischen Technologien im Bereich der Authentifizierung, Verschlüsselung und der elektronischen Signaturen. Details über die wichtigsten in diesem Bericht vorgestellten Technologien können in [RaSl14] nachgelesen werden.

2 Authentifizierung

Identifizierung und Authentifizierung sind zwei wesentliche Prozesse zum Absichern von schützenswerten Daten und der Regelung von Zugriffen. Im Rahmen der Identifizierung erfolgt meist eine Identitätsfeststellung, der Nachweis der vorgewiesenen Identität wird als Authentifizierung bezeichnet.

Ein wesentlicher Bestandteil im österreichischen E-Government zur sicheren Identifizierung und Authentifizierung von österreichischen Bürgerinnen und Bürgern ist die österreichischen Bürgerkarte oder Handy-Signatur. Im Rahmen einer Anmeldung mittels Bürgerkarte oder Handy-Signatur erfolgt eine sichere und eindeutige Identitätsfeststellung sowie eine kryptographisch sichere Authentifizierung auf Basis einer qualifizierten elektronischen Signatur.

Die sichere Authentifizierung ist somit ein wesentlicher Bestandteil im österreichischen E-Government. In diesem Abschnitt werden neue Möglichkeiten einer Authentifizierung im Rahmen von Cloud Computing vorgestellt.

2.1 Anonymous Password Authentication

Passwörter sind eines der meist verwendeten Authentifizierungsmechanismen, nicht nur im Cloud Bereich, sondern generell im WWW und im Internet. Der große Vorteil von Passwörtern ist, dass für eine Authentifizierung nur der Faktor „Wissen“ abgefragt werden muss, und beispielsweise kein zusätzlicher Faktor wie z.B. „Besitz“ benötigt wird. Nichtsdestotrotz haben Passwörter klare Nachteile in der Sicherheit. Einerseits werden von Benutzerinnen und Benutzern üblicherweise nur kurze Passwörter gewählt, welche zwar leicht zu merken sind, jedoch anfällig für sogenannte Dictionary-Attacks [RFC 4949] sind. Andererseits sind Passwörter nicht datenschutzfreundlich, da sich eine Benutzerin bzw. ein Benutzer zuvor beim Server registrieren muss. D.h., der Server kennt einerseits die Identität der Benutzerin bzw. des Benutzers, andererseits auch die Passwörter (zumindest den gehashten Wert [CJM+15]).

Um den Datenschutz beim Umgang mit Passwörtern zu erhöhen, können „Anonymous Password Authentication“-Mechanismen [YZW+09][YZW+10] verwendet werden. Diese Mechanismen erlauben die Authentifizierung mittels Passwort, ohne dass ein Server diese einer bestimmten Benutzerin bzw. einem bestimmten Benutzer zuordnen kann. D.h., die Benutzerin bzw. der Benutzer ist nicht „linkbar“ und Login-Transaktionen können vom Server nicht verfolgt werden. Gemäß der Praktikabilität dieser neueren Authentifizierungsmechanismen auf Basis von Passwörtern werden jedoch von [YWB09] bedenken geäußert.

Möglicher Einsatz im Cloud Computing und E-Government

Benutzerinnen bzw. Benutzer können beispielsweise anonym auf einen behördlichen Cloud Speicher zugreifen, ohne ihre wahre Identität Preis geben zu müssen.

2.2 Anonymous Credential Systems

Anonymous Credential Systems wurden bereits in einem früheren EGIZ-Bericht [Zwat13] ausführlicher diskutiert, deswegen wird für Details auf diesen Bericht verwiesen. Um diesen Bericht hinsichtlich Cloud Kryptographie jedoch konsistent zu halten, werden die wichtigsten Punkte aus dem früheren EGIZ-Bericht übernommen.

Anonymous Credential Systems erlauben die Authentifizierung nur auf Basis von anonymen Attributen (Credentials), sprich die komplette Identität einer Person muss nicht Preis gegeben werden. Anonymous Credentials erlauben z.B. nur die Bekanntgabe des Alters als authentisches Attribut, ohne dabei das Geburtsdatum offenzulegen. Die zwei wichtigsten Technologien sind dabei U-Prove und Idemix. U-Prove[1] ist eine von Stefan Brands [Brands00] entwickelte und von Microsoft übernommene Technologie. Identity Mixer[2] (Idemix) ist ein von IBM entwickeltes Anonymous Credential System.

Möglicher Einsatz im Cloud Computing und E-Government

Benutzerinnen bzw. Benutzer können beispielsweise auf behördliche Cloud Applikationen zugreifen, indem sie nur jene Attribute ihrer Identität offenlegen, die auch wirklich relevant für einen erfolgreichen Zugriff sind.

2.3 Anonymous Communication

Anonymous Communication versucht eine Nachricht von einem Sender zu einem Empfänger so zu versenden, dass weder der Empfänger der Nachricht die Identität des Senders kennt, noch ein Knoten entlang des Kommunikationskanals die Identität des Senders oder Empfängers kennt [RaSI14]. Vorteil dieser Technologien ist, dass ein Service Provider weder die Identität einer Benutzerin bzw. eines Benutzers rausfinden noch ein Verhaltensprofil ableiten kann. Anonymous Communication kann auf unterschiedlichen Wegen passieren. [RaSI14] beschreiben in ihrem Buch „Mix networks“ [BFK09], „Crowd Systems“ [ReRu98], oder „Hordes Systems“ [LeSh02] als unterschiedliche Technologien, die alle ihre Vor- und Nachteile besitzen, jedoch hier aus Fokus-Gründen nicht explizit erwähnt werden.

[1] http://research.microsoft.com/en-us/projects/u-prove/
[2] http://idemix.wordpress.com/

Möglicher Einsatz im Cloud Computing und E-Government
Benutzerinnen bzw. Benutzer können beispielsweise auf behördliche Cloud Applikationen zugreifen, ohne ihre Identität Preis geben zu müssen. Auch über Protokoll-Informationen wie z.B. eine IP-Adresse kann keine Identität abgeleitet werden.

3 Verschlüsselung

Elektronische Verschlüsselung wird meist dann eingesetzt, wenn Daten vertraulich übertragen bzw. behandelt werden müssen, sodass unbefugte Personen keinen Zugriff zu diese Daten erhalten können. Klassische Verschlüsselungsverfahren (meist basierend auf asymmetrischen Verfahren) werden auch im E-Government eingesetzt. So können beispielsweise mittels Bürgerkarte Daten für österreichische Bürgerinnen bzw. Bürger einfach verschlüsselt werden.

In diesem Abschnitt werden neuere kryptographische Verschlüsselungsverfahren vorgestellt, die neben dem Schutz von Vertraulichkeit noch andere Eigenschaften besitzen, sodass sie sich für einen Cloud-Einsatz im E-Government eignen könnten.

3.1 Attribute-Based Encryption

Attribute-Based Encryption [SaWa05] ist ein Verschlüsselungsverfahren, welches die Möglichkeit einer Autorisierung bzw. Zugriffskontrolle direkt in den Entschlüsselungsprozess integriert. Daten können dabei nicht nur für eine bestimmte Person verschlüsselt werden, sondern jede Person kann diese Daten entschlüsseln, sofern sie bestimmte Attribute besitzt oder gewisse Policies erfüllen kann. D.h., die einzelnen Schlüssel bzw. die verschlüsselten Daten sind abhängig von bestimmten Attributen oder Policies.

Möglicher Einsatz im Cloud Computing und E-Government
Benutzerinnen bzw. Benutzer können beispielsweise persönliche Daten einem Cloud Provider verschlüsselt zur Verfügung stellen, welcher die Daten selbst nicht einsehen kann. Nur jene Personen haben Zugriff, die auch die entsprechenden Berechtigungen dafür besitzen. Diesen Personen müssen aber nicht alle Daten zur Verfügung gestellt werden, sondern nur ein Subset für welches die Berechtigungen den Zugriff erlauben.

3.2 Proxy Re-Encryption

Proxy Re-Encryption [BBS98] ist ein asymmetrisches Verschlüsselungsverfahren, bei dem ein „halb-vertrauenswürdiger" Proxy (Intermediär) verschlüsselte Daten umschlüsseln kann. In anderen Worten ausgedrückt, kann dieser Proxy einen verschlüsselten Text, welcher z.B. für Person A verschlüsselt ist, mit Hilfe eines sogenannten Re-Encryption Schlüssel so transformieren bzw. umschlüsseln, dass der verschlüsselte Text von einer Person B entschlüsselt werden kann. Obwohl der Proxy diese Umschlüsselungsfunktion durchführen kann, lernt er weder den Klartext noch erhält er Zugriff auf einen der privaten Schlüssel von A oder B.

Gemäß der Richtung der Proxy Re-Encryption Operation kann die Umschlüsselung uni- oder bidirektional erfolgen. D.h., die Umschlüsselung kann entweder nur von A nach B

erfolgen (unidirektional) oder auch vice versa (bidirektional). Zusätzlich gibt es Proxy Re-Encryption Verfahren, die entweder nur eine einfache Umschlüsselung (z. B. von A nach B) oder eine mehrfache Umschlüsselung erlauben (z.B. von A nach B nach C).

Möglicher Einsatz im Cloud Computing und E-Government

Benutzerinnen bzw. Benutzer können beispielsweise persönliche Daten wie z.B. Identitätsdaten einem Cloud Provider verschlüsselt zur Verfügung stellen, welcher die Daten selbst nicht einsehen, jedoch für eine dritte Person umschlüsseln kann.

3.3 Homomorphic Encryption

Homomorphic Enryption erlaubt die Berechnung beliebiger Funktionen auf verschlüsselten Daten. Dabei hat die Partei, die die Berechnung auf den verschlüsselten Daten durchführt, weder Zugriff auf den Klartext noch auf den notwendigen Schlüssel zum Entschlüsseln. Werden die Daten dann entschlüsselt, so enthält der Klartext dann das Ergebnis der Berechnung, welche auf den verschlüsselten Daten durchgeführt wurde.

Prinzipiell wird meist zwischen „Group Homomorphic Encryption", „Somehow Homomorphic Enryption", und „Fully Homomorphic Encryption" unterschieden. Bei der „Group Homomorphic Encryption" können nur binäre Funktionen auf den verschlüsselten Daten angewendet werden, bei der „Somehow Homomorphic Enryption" nur eine limitierte Klasse an Funktionen, und bei der „Fully Homomorphic Encryption" beliebige Funktionen. [Vaik11] gibt einen guten Überblick über all die unterschiedlichen Varianten homomorpher Verschlüsselung.

Möglicher Einsatz im Cloud Computing und E-Government

Benutzerinnen bzw. Benutzer können beispielsweise persönliche Daten (z.B. Medizindaten) einem Cloud Provider verschlüsselt zur Verfügung stellen, welcher die Daten selbst nicht einsehen kann. Der Cloud Provider kann dann mathematische Operationen darauf durchführen, ohne das Ergebnis zu lernen.

3.4 Searchable Encryption

Searchable Encryption [BHJ+15] erlaubt das Suchen von Schlüsselwörtern auf verschlüsselten Daten. So können beispielsweise Daten verschlüsselt auf einem Server gespeichert und nach bestimmten Daten gesucht werden, ohne dass der Server Informationen weder über die Suchanfrage noch über den Inhalt der gespeicherten Daten erhält. Mit Hilfe dieser Algorithmen kann daher der kostenintensive Fall vermieden werden, dass verschlüsselte Daten zuerst auf den Client heruntergeladen und anschließend entschlüsselt werden müssen, bevor die Suchanfrage gestartet werden kann [RaSI14]. Im Wesentlichen kann auch zwischen Volltext-Suche und Index-basierter

Suche unterschieden werden. In der Volltext-Suche wird jedes verschlüsselte Datenelement auf ein bestimmtes Schlüsselwort untersucht. Bei der Index-basierten Suche wird die Suche nur über eine separate verschlüsselte Index-Datei durchgeführt.

Möglicher Einsatz im Cloud Computing und E-Government
Behörden können auch sensible Dokumente in die Cloud auslagern, da diese nur verschlüsselt gespeichert sind. Wird ein bestimmtes Dokument benötigt (z.B. ein bestimmter elektronischer Akt), so kann eine entsprechende Suche auf den verschlüsselten Dokumenten durchgeführt werden.

4 Elektronische Signaturen

Elektronische Signaturen sind ein Kernelement im österreichischen E-Government. Elektronische Signaturen werden sowohl auf Systemebene als auch auf Bürgerebene eingesetzt. So ermöglicht die Bürgerkarte bzw. die Handy-Signatur die sichere Erstellung einer qualifizierten elektronischen Signatur für Bürgerinnen bzw. Bürger.

Elektronische Signaturen schützen einerseits die Authentizität, die Integrität, sowie die Nicht-Abstreitbarkeit von signierten Dokumenten. In diesem Abschnitt werden neuere Signaturverfahren vorgestellt, die zusätzliche Eigenschaften besitzen, welche im E-Government und Cloud-Kontext Verwendung finden könnten.

4.1 Anonymous Signatures

Anonymous Signatures [YWD+06] erlauben Mitgliedern einer Gruppe elektronische Signaturen für die Gruppe zu erzeugen, ohne dass genau festgestellt werden kann, welches Gruppenmitglied die Signatur tatsächlich erstellt hat. Die erstellte Signatur ist daher nur mit der Gruppe und nicht mit einer einzelnen Person verknüpft. Es kann nicht festgestellt werden, wer der eigentliche Signator war.

Prinzipiell kann zwischen „Group Signatures“ [CH91], „List Signatures“ [CSS+06], und „Ring Signatures“ [RST01] unterschieden werden. Bei „Group Signatures“ gibt es einen expliziten Manager der Gruppe, der auch im Bedarfsfall die Anonymität der Signatur aufheben und den Signator identifizieren kann. „List Signatures“ erlauben die Limitierung der Anzahl der erstellten Signaturen pro Benutzerin bzw. Benutzer. Außerdem können Gruppen Signaturen miteinander verknüpft werden, sofern sie vom selben Gruppen-Mitglied erstellt wurden. „Ring Signatures“ sind ähnlich zu „Group Signatures“, jedoch mit dem Unterschied, dass für die Erstellung einer Signatur die Hilfe eines anderen Gruppen-Mitglieds, z.B. dem Manager der Gruppe, nicht nötig ist. [RaSI14]

Möglicher Einsatz im Cloud Computing und E-Government
Petitionen können von Bürgerinnen und Bürgern gemeinsam und authentisch bei einer Behörde eingereicht werden, ohne dass festgestellt werden kann, wer der eigentliche Signator der Petition ist.

4.2 Blind Signatures

Blind Signatures [Chaum82] beschreiben Signaturverfahren, bei denen der Signator das eigentliche Dokument bzw. die Daten, die er signiert, nicht sieht. Das signierte Dokument bzw. die signierten Daten können dann wie bei herkömmlichen Signaturen gegen das Original verifiziert werden. Blinde Signaturen werden üblicherweise dort eingesetzt, wo der Signator und der Dokument-/Daten-Ersteller zwei unterschiedliche Personen sind.

Typische Beispiele für die Verwendung von Blinden Signaturen sind E-Voting, E-Cash, aber auch elektronische Ticket-Systeme, bei denen authentische Tokens ausgestellt werden, die anonym und ohne Transaktionsverknüpfungen genutzt werden können. In manchen Anwendungsbereichen kann es auch Sinn machen, nicht die kompletten Daten vor dem Signator auszublenden, sondern einzelne Teile sichtbar zu lassen (z.B. die Gültigkeitsdauer eines Tickets) [RaSI14]. Solche Arten von Blinden Signaturen werden als „Partially Blind Signatures" [AbFu96] bezeichnet.

Möglicher Einsatz im Cloud Computing und E-Government

Der Einsatz von Blinden Signaturen erfolgt bereits im E-Voting Kontext. Ein weiterer möglicher Einsatz wäre eine Signatur-Service in der Cloud unter Verwendung von blinden Signaturen.

4.3 Redactable Signatures

Digitale Signaturen erlauben üblicherweise keine Veränderung der signierten Daten. In manchen Fällen kann es jedoch wünschenswert sein, dass Teile von signierten Daten entfernt oder verändert werden können, sodass die Original-Signatur trotzdem ihre Gültigkeit behält. Redactable Signatures [JMS+02] ermöglichen diese Funktionalität, ohne dass der Original-Signator dazu nochmals eingreifen muss. Signaturverfahren, die das Entfernen von Teilen einer Signatur von beliebigen Personen bei Beibehaltung der Gültigkeit erlauben, werden als Redactable Signatures bezeichnet. Signaturverfahren, die das Austauschen von bestimmten Teilen von ausgewählten Personen bei Beibehaltung der Gültigkeit erlauben, werden als Sanitizeable Signatures [ACM+05] bezeichnet.

Möglicher Einsatz im Cloud Computing und E-Government

Behördliche Dokumente können trotzdem mit elektronischen Signaturen versehen werden, obwohl Teile daraus beispielsweise geschwärzt worden sind. Bei Verwendung von redigierbaren Signaturen behält das Dokument trotzdem seine Gültigkeit, und der Empfänger erhält nur Einblick in einen bestimmten Bereich des Dokuments.

5 Diskussion und Fazit

Die Erfüllung rechtlicher Rahmenbedingungen, wie z.B. die Sicherung des Datenschutzes, ist meist eines der größten Hindernisse bei der Verwendung von Cloud Computing im E-Government Bereich. Dabei zeigen jedoch Studien, dass Cloud Computing für den öffentlichen Sektor enorme Kostenvorteile mit sich bringen kann. Um diesen Umstand entgegenzuwirken und einen breiteren Einsatz von Cloud Computing im behördlichen Bereich zu ermöglichen, wurden in diesem Dokument kryptographische Technologien vorgestellt, die den nötigen Datenschutz sowie die Erfüllung rechtlicher Rahmenbedingungen auf Basis kryptographischer Technologien in Zukunft ermöglichen könnten.

Neuere, hauptsächlich auf Anonymität bedachte Authentifizierungsverfahren könnten es beispielsweise Bürgerinnen und Bürgern ermöglichen, nicht ihre komplette Identität Preis zu geben, sondern nur die für ein Verfahren relevante Daten wie z.B. das Alter. Die neueren vorgestellten Verschlüsselungsverfahren bringen insgesamt hauptsächlich solche Eigenschaften mit, dass Bearbeitungen oder Prozesse auch auf verschlüsselten Daten durchgeführt werden könnten. Behördliche Daten bzw. Dokumente könnten so einfach in die Cloud ausgelagert werden und müssten nicht explizit für eine Bearbeitung heruntergeladen werden, da eine Bearbeitung direkt auf den verschlüsselten Daten in der Cloud möglich wird. Letztendlich wurden neuere elektronische Signaturverfahren vorgestellt, die hauptsächlich darauf abzielen, die Identität des Signators zu schützen und beispielsweise Verknüpfungen von Transaktionen zu vermeiden. Im Cloud Kontext können solche Verfahren auch eingesetzt werden, um den Signator gegenüber dem Cloud Provider nicht alle Daten Preis geben lassen zu müssen, und trotzdem authentische Daten vorweisen zu können.

Obwohl im Rahmen dieses Projekts gezeigt werden konnte, dass mit Hilfe kryptographischer Technologien durchaus ein breiterer Einsatz von Cloud Computing im behördlichen Umfeld möglich gemacht werden könnte, so ist der praktische Einsatz dieser Technologien in behördlichen Anwendungen noch sehr stark vom technischen Reifegrad dieser Technologien abhängig, welcher sich nicht bei allen im Produktivbereich bewegt.

Dokumentenhistorie

Version	Datum	Autor(en)	Anmerkung
0.1	09.12.2015	Bernd Zwattendorfer	Dokumenterstellung und Kapitel 1
0.2	18.12.2015	Bernd Zwattendorfer	Kapitel 2, 3, 4, 5
1.0	31.12.2015	Bernd Zwattendorfer	Finalisierung

Referenzen

[AbFu96] Abe M., Fujisaki E., "*How to date blind signatures*", 1996, Advances in Cryptology — ASIACRYPT '96, S. 244-251, http://link.springer.com/chapter/10.1007%2FBFb0034851

[ACM+05] Ateniese G., Chou D.H., de Medeiros B., Tsudik G.: "*Sanitizable Signatures*", ESORICS 2005, 2005, S. 159-177, http://link.springer.com/chapter/10.1007%2F11555827_10

[BBS98] Blaze M., Bleumer G., Strauss M., "*Divertible Protocols and Atomic Proxy Cryptography*", Advances in Cryptology - EUROCRYPT '98, Vol. 1403 800 of LNCS, Springer, 1998, S. 127-144.

[BFK09] Berthold O., Federrath H., Köpsell S., "*Web MIXes: A System for Anonymous and Unobservable Internet Access*", 2009, Designing Privacy Enhancing Technologies, S. 115-129, http://link.springer.com/chapter/10.1007%2F3-540-44702-4_7#

[BHJ+15] Bösch C., Hartel P., Jonker W., Peter A., "A Survey of Provably Secure Searchable Encryption", 2015, Journal ACM Computing Surveys (CSUR), 47(2), http://dl.acm.org/citation.cfm?id=2636328

[Brands00] Stefan Brands: "*Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*", 2000, http://www.credentica.com/the_mit_pressbook.html

[Chaum82] Chaum D., "Blind Signatures for Untraceable Payments", 1986, Advances in Cryptology, S. 199-203, http://link.springer.com/chapter/10.1007%2F978-1-4757-0602-4_18

[CH91] Chaum D., van Heyst E., "*Group Signatures*", Advances in Cryptology - EUROCRYPT '91, 1991, http://dl.acm.org/citation.cfm?id=1754897

[CJM+15] Chang D., Jati A., Mishra S., Sanadhya S., "*Rig: A Simple, Secure and Flexible Design for Password Hashing*", 2015, Information Security and Cryptology, S. 361-381, http://link.springer.com/chapter/10.1007/978-3-319-16745-9_20#

[CSS+06] Canard S., Schoenmakers B., Stam M., Traor J., "*List signature schemes*", Discrete Applied Mathematics, 154 (2), 2006, S. 189-201, http://dl.acm.org/citation.cfm?id=1705186

[JMS+02] Johnson R., Molnar D., Song D.X., Wagner D., "*Homomorphic Signature Schemes*". CT-RSA '02, 2002, S. 244-262, http://link.springer.com/chapter/10.1007%2F3-540-45760-7_17

[LeSh02] Levine B., Shields C., "*Hordes: A multicast based protocol for anonymity*", 2002, J. Comput. Secur. 10 (3), S. 213-240, http://dl.acm.org/citation.cfm?id=603406

[RaSl14] Rass S., Slamanig D., "*Cryptography for Security and Privacy in Cloud Computing*", 2014, Artech House

[ReRu98] Reiter M., Rubin A., "Crowds: Anonymity for Web Transactions", 1998, ACM Transactions on Information and System Security (TISSEC), 1(1), S. 66-92, http://avirubin.com/crowds.pdf

[RFC 4949] Shirey R., "*Internet Security Glossary, Version 2*", 2007, RFC 4949, Network Working Group, https://tools.ietf.org/html/rfc4949

[RST01] Rivest R., Shamir A., Tauman Y., "*How to Leak a Secret: Theory and*

Applications of Ring Signatures", ASIACRYPT 2001, 2001, S. 552-565, http://link.springer.com/chapter/10.1007%2F11685654_7

[SaWa05] Sahai A., Waters B., "*Fuzzy Identity-Based Encryption*", EUROCRYPT, 2005, S. 57-473, http://link.springer.com/chapter/10.1007%2F11426639_27

[Vaik11] Vaikuntanathan V., "Computing Blindfolded: New Developments in Fully Homomorphic Encryption", 2011, Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, S. 5-16, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6108145&tag=1

[YWB09] Yang Y., Weng J., Bao F., "*On the Limits of Anonymous Password Authentication*", 2009, Chinacrypt09, S. 246-252, http://icsd.i2r.a-star.edu.sg/staff/yanjiang/papers/yanjiang-limits-anonymous-password.pdf

[YWD+06] Yang G., Wong D., Deng X., Wang H., "*Anonymous Signature Schemes*", 2006, Public Key Cryptography - PKC 2006, S. 347-363, http://link.springer.com/chapter/10.1007%2F11745853_23

[YZW+09] Yang Y., Zhou J., Weng J., Bao F., "*A New Approach for Anonymous Password Authentication*", 2009, ACSAC, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5380508

[YZW+10] Yang Y., Zhou J., Weng J., Bao F., "*Towards Practical Anonymous Password Authentication*", 2010, ACSAC, https://www.acsac.org/2010/openconf/modules/request.php?module=oc_program&action=view.php&a=&id=110&type=2

[Zwat13] Zwattendorfer B., "*Anonymous Credentials – Claim-based authentication*", 2013, EGIZ-Bericht, https://www.egiz.gv.at/files/projekte/2013/anonymous_credentials/Anonymous_Credentials%E2%80%93Claim-based_authentication_v1.0.pdf