Karlsruher Institut für Technologie

Karlsruhe Reports in Informatics 2010,3
Edited by Karlsruhe Institute of Technology,
Faculty of Informatics
ISSN 2190-4782

Tagungsband des 12. Kryptotags

Workshop der Fachgruppe „Angewandte Kryptographie“
der „Gesellschaft für Informatik e.V.“

Institut für Kryptographie und Sicherheit,
Karlsruher Institut für Technologie (KIT)

2010

KIT – University of the State of Baden-Wuerttemberg and National
Research Center of the Helmholtz Association

Tagungsband des 12. Kryptotags

Workshop der Fachgruppe „Angewandte Kryptographie“
der „Gesellschaft für Informatik e.V.“

Institut für Kryptographie und Sicherheit,
Karlsruher Institut für Technologie (KIT)

Inhaltsverzeichnis

Schlüsselaustausch durch Mehrwegausbreitung **5**
Antonio Almeida, Nico Döttling, Déjan Lazich

SOKEN: Schlüsselaustausch in sozialen Netzwerken **6**
Dirk Achenbach und David Förster

Komfortables und sicheres Einloggen in Online-Accounts **7**
Bernd Borchert

An approach to Completely Searchable Encryption **8**
Rolf Haynberg

On the Soundness of Authenticate-then-Encrypt **9**
Ueli Maurer and Björn Tackmann

Traitor Tracing from Anonymous Attribute-Based Encryption **10**
Mario Strefler

`http://KryptoTag.de` **11**

Schlüsselaustausch durch Mehrwegausbreitung

Antonio Almeida, Nico Döttling, Déjan Lazich

Institut für Kryptographie und Sicherheit
Forschungsgruppe Prof. Dr. J. Müller-Quade
Karlsruher Institut für Technologie

Die Allgegenwärtigkeit von drahtlosen Netzwerken hat die Interesse an physikalischen Schlüsselaustauschverfahren erneuert. Der Ausblick auf informationstheoretische Sicherheit macht diese Schemata zu vielversprechenden Kandidaten für kryptographische Infrastrukturen ohne komplexitätstheoretische Annahmen benutzen zu müssen.

Eine der vielversprechendsten Techniken um kryptographische Schlüssel auf der Bitübertragungsschicht zu erzeugen basiert auf dem Prinzip der Reziprozität von Funkkanälen. Funkkanäle besitzen quasi immer das Phänomen der Mehrwegeausbreitung. In solchen Kanälen werden ausgesendete Radiosignale von verschiedenen physischen Hindernissen wie Automobilen, Gebäuden Bäumen usw. gestreut und reflektiert. Deshalb misst der Empfänger das Originalsignal, das mit mehreren Echos überlagert ist. Die Reziprozität besagt, dass ein Kanal, der durch seine Impulsantwort charakterisiert ist gleich bleibt, wenn Sender und Empfänger die Rollen tauschen. Somit kann ein Sende-und-Empfangssystem aus zwei physikalisch getrennten Sendeempfängern, Alice und Bob, gemeinsamen Zufall extrahieren, indem die Impulsantworten des Funkkanals zwischen ihnen gemessen werden. Der Zufall entsteht durch die unbekannte dynamische elektromagnetische Charakteristik der Umgebung in der Alice und Bob sich befinden. Da die gemessene Impulsantwort des Kanals zwischen Alice und Bob für beide Teilnehmer gleich ist, kann daraus ein gemeinsamer geheimer Schlüssel errechnet werden. Kritisch für die Sicherheit dieses Konzeptes ist dass sich jeder lauschende Angreifer in hinreichend großer Entfernung zu den legitimen Protokollteilnehmern befindet und somit unkorrelierte Messungen erhält.

Wir präsentieren eine prototypische Implementierung eines reziprozitätsbasierten Schlüsselaustauschs, der auf der GNURADIO-Plattform läuft. Wir benutzen Zeitmultiplex um den Kanal auf verschiedenen Trägerfrequenzen zu vermessen und eine breitbandige Frequenzantwort zu synthetisieren. Aus der resultierenden Frequenzantwort extrahieren wir den gemeinsamen Zufall für Alice und Bob. Schließlich werden Methoden der Information Reconciliation benutzt um unvermeidbare Fehler durch Rauschen zu korrigieren und letztlich den kryptographischen Schlüssel zu erhalten.

Wir beschreiben auch einige Schwachstellen dieses Protokolls und schlagen Techniken vor, die die Sicherheit verbessern.

Mit dieser Arbeit wollen wir weitere Untersuchungen praktischer Aspekte von Schlüsselaustauschverfahren fördern, welche auf Kanalreziprozität basieren.

SOKEN: Schlüsselaustausch in sozialen Netzwerken

Dirk Achenbach und David Förster

Institut für Kryptographie und Sicherheit
Forschungsgruppe Prof. Dr. J. Müller-Quade
Karlsruher Institut für Technologie (KIT)

Die Sicherheit von Public-Key-Schlüsselaustauschverfahren wird beständig durch Fortschritte im Bereich der Algorithmik und der Rechenleistung gefährdet. Wir stellen ein alternatives Schlüsselaustauschverfahren vor, dessen Sicherheit nicht auf den Komplexitätsannahmen asymmetrischer Verfahren wie Diffie-Hellman [DH76] beruht. Statt den Schlüssel über den Kommunikationskanal auszuhandeln, schlagen wir ein Schlüsselaustauschnetzwerk vor, das persönliche Begegnungen nutzt, um Schlüssel auszutauschen und weiterzuleiten. Hierzu werden mobile Kommunikationsgeräte mit Kurzstreckenfunkeinrichtungen eingesetzt. Mithilfe dieses Netzwerks können zwei Parteien, die sich persönlich nie getroffen haben, ein gemeinsames Geheimnis erhalten. Diese gemeinsamen Geheimnisse können mit Schlüsseln aus asymmetrischen Verfahren kombiniert werden, um maximale Sicherheit zu erhalten.

Bei jeder Begegnung tauschen Netzwerkteilnehmer neu erzeugte Schlüssel aus und geben zusätzlich im Vorfeld erhaltene Schlüssel weiter. Um die Sicherheit der eigenen Kommunikation nicht zu beeinträchtigen, wird vor der Weitergabe eines Schlüssels eine kryptographische Hashfunktion auf ihn angewandt. Damit ein Schlüssel bei einer Weitergabe an verschiedene Personen unterschiedliche Werte annimmt, wird zum ursprünglichen Schlüsselwert beim Hashen ein zusätzliches Salt beigegeben. Auf diese Weise spannt jeder initiale Schlüssel einen Schlüsselbaum auf, der über das Schlüsselnetzwerk wächst. Zur Etablierung eines gemeinsamen Schlüssels teilt der Empfänger eines abgeleiteten Schlüssels dem Urheber die Liste der verwendeten Salts mit. Dieser kann damit die Modifikationen nachvollziehen und den abgeleiteten Schlüssel berechnen. Der eigentliche Schlüssel wird hierbei nicht übertragen. Besitzen zwei Netzwerkteilnehmer zwei auf diese Weise erhaltene Schlüssel, deren Übertragungswege echt disjunkt sind, und kombinieren sie diese auf geeignete Weise, erhalten sie ein gemeinsames Geheimnis.

Die Sicherheit des SOKEN-Schlüsselaustauschnetzwerks beruht auf der Schwierigkeit, persönliche Begegnungen großflächig zu überwachen. Ein Angreifer müsste eine große Anzahl von Individuen überwachen oder kompromittieren, um die Vertraulichkeit der ausgetauschten Schlüssel signifikant einzuschränken. Da das Verfahren anonym arbeitet, ist es für Angreifer schwer, Bewegungsprofile der Netzwerkteilnehmer zu erstellen.

Laut Milgrams Untersuchungen zum Small-World-Phänomen [Mil67] und einer Analyse des Instant-Messaging-Netzwerks Microsoft Messenger [LH08] sind die meisten Menschen über einen nur kurzen Pfad gemeinsamer Bekannter verbunden. Dies legt nahe, dass je zwei Teilnehmer des SOKEN-Netzwerks mit hoher Wahrscheinlichkeit einen gemeinsamen Schlüssel besäßen.

Literatur

[DH76] W. Diffie und M. Hellman. *New directions in cryptography.* IEEE Transactions on information theory, Seiten 644-654, 1976.

[Mil67] S. Milgram. *The small world problem.* Psychology today, 2(1):6067, 1976.

[LH08] J. Leskovec und E. Horvitz. *Planetary-scale views on a large instant-messaging network.* WWW '08: Proceedings of the 17th international conference on world wide web, ACM, Seiten 915–924, New York, NY, USA, 2008.

Komfortables und sicheres Einloggen in Online-Accounts

Um Passwörter und Benutzernamen kümmert sich das Handy

Bernd Borchert

Universität Tübingen

Viele Internet-Nutzer kennen das Problem, dass man die vielen Passwörter und Benutzernamen für seine Internet Online-Accounts vergisst oder verwechselt. Ein an der Universität Tübingen entwickeltes neues Verfahren erspart dem Benutzer nicht nur das Sich-Merken von Benutzernamen und Passwörtern, sondern auch das Eintippen davon. Alles wird vom Fotohandy erledigt.

Das neue Verfahren löst gleichzeitig ein weiteres Problem, das vielen bekannt ist, das aber gern ignoriert wird: Die üblichen Dauer-Passwörter für Online Accounts können durch Trojaner auf dem Eingabe-Rechner abgehört werden - dagegen gibt es keinen 100-prozentigen Schutz. Die gestohlenen Identitäten werden dann an Sammelstellen im Internet geschickt und von dort aus für kriminelle Zwecke weiterverkauft. Bei dem neuen Verfahren gibt es keine Dauer-Passwörter mehr, d.h. es können auch keine abgehört werden.

Das Verfahren verläuft aus Benutzersicht folgendermaßen. Der Benutzer braucht ein internetfähiges Fotohandy. Für jeden Account ist ein Intialisierungsschritt auf dem Handy nötig. Wenn der Benutzer dann auf einem beliebigen Internet-Rechner in den Account hinein will, geht er mit dem Browser des Internet-Rechners auf die Webseite des Account-Anbieters. Dort wird ein 2D-Code angezeigt, der mit dem Fotohandy abfotografiert wird. Das Handy verarbeitet die gelesenen Daten und kontaktiert anschließend per Handy-Internet den Account-Server. Nach Prüfung der Daten setzt sich der Server mit dem Browserfenster auf dem Bildschirm des Benutzers in Verbindung und schaltet dort den Account frei. *Der Benutzer ist wie von Zauberhand in seinen Online Account hineingekommen: er musste sich Benutzername und Passwort weder merken noch sie eintippen. Das einzige, was er zu tun hatte, war, mit seinem Fotohandy den 2D-Code auf dem Bildschirm zu scannen.*

Die Gefahr, dass auch ein Handy-Dieb auf diese Weise in die Accounts hineinkommen kann, kann der Benutzer für die Accounts, die ihm wichtig sind, durch ein Verfahren abwehren, bei dem zusätzlich eine PIN abgefragt wird, und zwar für Trojaner unabhörbar.

Das Verfahren wurde von der Universität Tübingen zur Patentierung angemeldet. Ein Prototyp wurde von Studenten des Wilhelm-Schickard-Institut programmiert, siehe die unten angegebene Webseite, auf der auch ein Demo-Video zu finden ist. Die entsprechenden Handy-Programme (Apps) stehen für iPhones und Android Handys zur Verfügung. Es wird derzeit nach Account-Providern gesucht, die ihren Benutzern das Verfahren anbieten wollen.
Demoseite:
http://www-fs.informatik.uni-tuebingen.de/~borchert/Troja/Open-Sesame/

An approach to Completely Searchable Encryption

Rolf Haynberg

Institut für Kryptographie und Sicherheit
Forschungsgruppe Prof. Dr. J. Müller-Quade
Karlsruher Institut für Technologie

Cloud-Computing ermöglicht flexible und ressourcen-effiziente Dienstleistungen. Allerdings verhindern zu hohe Sicherheitsrisikos den Einsatz mit sensiblen Daten [1]. Zwar bieten viele Dienstleister Schutz vor Angriffen von außen, aber Insider-Angriffe können für den Kunden ein intolerierbares Risiko darstellen.

Bei der bloßen Speicherung bietet Verschlüsselung einen ausreichenden Schutz, sollen die Daten aber vom Dienstleister durchsucht werden, ist dies mit den meisten Verschlüsselungsverfahren nicht möglich. Lösungen aus der theoretischen Kryptographie[5] haben Kosten die einen praktischen Einsatz bisher verhindert haben. Searchable Encryption bietet einen Kompromiss zwischen dem Schutz der Daten und der Möglichkeit die Daten zu durchsuchen.

Viele bestehende Arbeiten auf diesem Gebiet nutzen invertierte Indizes: Zu Schlüsselwörtern aus einer gegebenen Menge können übereinstimmende Dokumente gefunden werden [2, 3, 4]. Sie verbergen den Klartext der Dokumente, der Schlüsselwörter und das Ergebnis der Suchanfrage. Eine Suchen nach beliebigen Teilworten in einer Zeichenkette ist mit diesen Verfahren jedoch nicht praktikabel, da die Anzahl der Schlüsselwörter quadratisch mit der Textlänge wächst, was sich sowohl auf die Suchzeit als auch den Speicherverbrauch auswirkt.

In diesem Vortrag wird die Arbeit an einer konkreten, verschlüsselten, Datenstruktur beschrieben, die eine schnelle Volltextsuche ermöglicht. Die Datenstruktur basiert auf einer linearen Repräsentation[6] von SCDAWGs [7]. Die Laufzeit der Suche hängt linear von der Länge des Suchwortes ab und ist damit insbesondere unabhängig von der Textlänge. Der Speicherbedarf wächst linear mit der Textlänge. Darüber hinaus bietet die Datenstruktur das Potenzial für eine Vielzahl von weiteren Anwendungsgebieten.

Literatur

[1] C. Henrich, M. Huber, C. Kempka, J. Müller-Quade, M. Strefler. *Towards Secure Cloud Computing.* IKS/IPD Fakultät für Informatik, Universtität Karlsruhe (TH).

[2] D. Xiaodong Song, D. Wagner, and A. Perrig. *Practical techniques for searches on encrypted data.* In IEEE Symposium on Security and Privacy, pages 44–55, 2000. `ttp://citeseer.nj.nec.com/song00practical.tml`.

[3] D. Boneh, G. Di Crescenzo, R. Ostrovsky and G. Persiano. *Public Key Encryption with Keyword Search.* Stanford University and Telcordia and UCLA and Università di Salerno.

[4] Eu-Jin Goh. *Secure Indexes.* Stanford University. 2004.

[5] Craig Gentry. *Fully Homomophic Encryption Using idea Lattices.* In the 41st ACM Symposium on Theory of Computing (STOC), 2009.

[6] K. Monostori, A. Zaslavsky and I. Vajk. *Suffix Vector: A Space-Efficient Suffix Tree Representation.* 2001.

[7] A. Blumer, J. Blumer, D. Haussler, R. McConnell and A. Ehrenfeucht. *Complete Inverted Files for Efficient Text Retrieval and Analysis.* University of Denver, University of Colorado.

On the Soundness of Authenticate-then-Encrypt

Ueli Maurer and Björn Tackmann

ETH Zürich
Switzerland

A communication channel from an honest sender A to an honest receiver B can be described as a system with three interfaces labeled A, B, and E (the adversary), where the security properties of the channel are characterized by the capabilities provided at the E-interface. The two main security guarantees a channel can provide are secrecy and authenticity.

A security mechanism, like encryption or a message authentication code (MAC), can be seen as the transformation of a certain type of channel into a stronger type of channel, where the term "transformation" refers to a natural simulation-based definition as presented in [Mau09]. For example, the main purpose of a MAC can be seen as first transforming an insecure into an authenticated channel, and encryption can be seen as then transforming the authenticated into a fully secure channel. This corresponds to the Encrypt-then-Authenticate (EtA) paradigm, where the reversed occurrence of the terms authentication and encryption is justified by the order of operations applied to the plaintext by the sender.

The dual paradigm, Authenticate-then-Encrypt (AtE), corresponds to using encryption to transform an insecure into a confidential channel, and using a MAC to transform the confidential into a fully secure channel. As pointed out by Bellare and Namprempre [BN00] and Krawczyk [Kra01], this paradigm is not sound in general; there are secure encryption schemes for which AtE is insecure.

There are two reasons for investigating nevertheless the soundness of AtE as a general paradigm. First, this calls for a definition of confidentiality; what separates a confidential from a secure channel is its (potential) malleability. We propose the first systematic analysis of malleability for symmetric encryption, and, in particular, we state a malleability restriction for confidential channels to be transformable into a secure channel by a secure MAC. Second, AtE is used in practice, for example in TLS. We show that the malleability of certain encryption schemes (e.g., the one-time pad and CBC encryption) satisfy the restriction and hence, together with a strongly unforgeable MAC, yield a secure channel. This proves the soundness of AtE and also confirms Krawczyk's results on the security of these specific instantiations of AtE obtained in the game-based setting.

References

[BN00] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In Tatsuaki Okamoto, editor, *ASIACRYPT 2000*, volume 1976 of *LNCS*, pages 531–545. IACR, Springer, 2000.

[Kra01] Hugo Krawczyk. The order of encryption and authentication for protecting communications. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 310–331. IACR, Springer, 2001.

[Mau09] Ueli Maurer. Abstraction in cryptography. In *CRYPTO 2009*, volume 5677 of *LNCS*, page 465. IACR, Springer, 2009.

Traitor Tracing from Anonymous Attribute-Based Encryption

Mario Strefler*

*ENS / INRIA / CNRS

Introduction Traitor tracing (TT) schemes are used to encrypt message broadcasts to a set of N users while providing traceability: Each user is assigned a decryption key. If an adversary uses these keys to construct a pirate decoder which is able to decrypt messages, there is a tracing algorithm that retrieves from this decoder the identifier of one corrupted user using a special tracing key.

The most efficient public-key TT scheme currently known is [BSW], which requires $O(\sqrt{N})$-size ciphertexts. In practical applications, bandwidth is very limited. Therefore, our goal is to reduce ciphertext size even at the cost of longer decryption keys. We divide this task into two steps. The first step is the construction of an anonymous attribute-based encryption (ABE) scheme supporting DNF access policies. This step is still an open problem. In the second step, we use the anonymous ABE from the first step to construct a PuLBE, a publicly traceable analogon to the private linear broadcast encryption (PLBE) presented in [BSW]. This directly implies traitor tracing [BSW].

Construction For our construction we rely on an anonymous ciphertext-policy ABE (CP-ABE) scheme that supports DNF access structures. ABE provides a way to encrypt a message not to a specific user, but to any user whose attributes fulfill certain criteria. In CP-ABE schemes user keys are associated with an attribute list. Then, messages are encrypted to all users whose keys satisfy an access policy that is specified at encryption time. An ABE is *anonymous* if users learns nothing about the policy except whether their key is able to decrypt or not. This is necessary for tracing.

We arrange the N users in a d-dimensional hypercube with sides of length m and write $N = m^d$. Each user is identified by his d coordinates in this cube; therefore we need d attributes and each attribute can take m values. Assume an ABE scheme that fits our requirements and has key and ciphertext length at most polynomial in the number of attribute values (in our case md). Then we will obtain TT key and ciphertext lengths polylogarithmic in N (for $d = m$). Anonymous schemes fulfilling one of our two other main requirements (DNF access policy, polynomial ciphertext and key length) already exist. The anonymous ABE from [NYO] does not allow DNF access formula, while the predicate encryption from [KSW] has a complexity depending on m^d instead of md.

To use the ABE scheme, we must now translate between these structures. The PuLBE expects a linear ordering of the users, provided by a bijection $Index\colon [0, m-1]^d \to [0, m^d - 1]$. To encrypt, we need to convert the receiver set $[i, m^d - 1]$ into a policy in DNF. We choose subspaces of $[0, m-1]^d$ such that their union covers the receiver set. A term containing only conjunctions can be used to describe a subspace in the hypercube and there can be at most m spaces for each dimension. We construct md such terms (empty if necessary) and set the ciphertext policy to be their disjunction.

References

[BSW] D. Boneh, A. Sahai, and B. Waters. Fully collusion resistant traitor tracing with short ciphertexts and private keys. *EUROCRYPT 2006*, vol. 4004 of *LNCS*, pp. 573–592. Springer, 2006.

[KSW] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. *EUROCRYPT 2008*, vol. 4965 of *LNCS*, pp. 146–162. Springer, 2008.

[NYO] T. Nishide, K. Yoneyama, and K. Ohta. Attribute-based encryption with partially hidden encryptor-specified access structures. *ACNS 2008*, vol. 5037 of *LNCS*, pp. 111–129. Springer, 2008.

http://KryptoTag.de

Der Kryptotag ist eine zentrale Aktivität der GI-Fachgruppe „Angewandte Kryptologie“. Er ist eine wissenschaftliche Veranstaltung im Bereich der Kryptologie und von der organisatorischen Arbeit der Fachgruppe getrennt. Grundgedanke des Kryptotages ist, dass er inklusive Anreise wirklich nur einen Tag dauert und Nachwuchswissenschaftlern, etablierten Forschern und Praktikern auf dem Gebiet der Kryptologie die Möglichkeit bieten, Kontakte über die eigene Universität hinaus zu knüpfen.

Die Vorträge können ein breites Spektrum abdecken, von noch laufenden Projekten, die ggf. erstmals einem breiteren Publikum vorgestellt werden, bis zu abgeschlossenen Forschungsarbeiten, die zeitnah auch auf Konferenzen präsentiert wurden bzw. werden sollen oder einen Schwerpunkt der eigenen Diplomarbeit oder Dissertation bilden. Die eingereichten Abstracts werden gesammelt und als technischer Bericht veröffentlicht. Es handelt sich damit um eine zitierfähige Arbeit. Sie können von den Seiten der Fachgruppe herunter geladen werden.

Bisherige Kryptotage

12. Kryptotag: 9. April 2010, Karlsruher Institut für Technologie.
Kontakt: Jörn Müller-Quade und Willi Geiselmann.

11. Kryptotag: 30. November 2009, Universität Trier.
Kontakt: Ralf Küsters und Andreas Vogt.

10. Kryptotag: 20. März 2009, Institut für Mathematik, Technische Universität Berlin.
Kontakt: Florian Heß.

9. Kryptotag: 10. November 2008, Institut für Internet-Sicherheit, Fachhochschule Gelsenkirchen. Kontakt: Markus Linnemann.

8. Kryptotag: 11. April 2008, Universität Tübingen, WSI für Informatik, Diskrete Mathematik.
Kontakt: Michael Beiter, Claudia Schmidt, Anja Korsten.

7. Kryptotag: 9. November 2007, Bonn-Aachen International Center for Information Technology.
Kontakt: Michael Nüsken und Daniel Loebenberger.

6. Kryptotag: 19. Februar 2007, Universität des Saarlandes, Information Security and Cryptography Group und Sirrix AG. Kontakt: Michael Backes und Ammar Alkassar.

5. Kryptotag: 11. September 2006, Universität Kassel, Fachbereich Mathematik/Informatik, Theoretische Informatik. Kontakt: Heiko Stamer.

1. Kryptowochenende: 1.–2. Juli 2006, Tagungszentrum Kloster Bronnbach der Universität Mannheim. Kontakt: Frederik Armknecht und Dirk Stegemann.

4. Kryptotag: 11. Mai 2006, Ruhr Universität Bochum, Horst-Görtz Institut.
Kontakt: Ulrich Greveler.

3. Kryptotag: 15. September 2005, Technische Universität Darmstadt, Theoretische Informatik.
Kontakt: Ralf-Philipp Weinmann.

2. Kryptotag: 31. März 2005, Universität Ulm, Abteilung für Theoretische Informatik.
Kontakt: Wolfgang Lindner und Christopher Wolf.

1. Kryptotag: 1. Dezember 2004, Universität Mannheim, Theoretische Informatik.
Kontakt: Stefan Lucks und Christopher Wolf.

Innerhalb der Fachgruppe für Angewandte Kryptologie sind Stefan Lucks (Bauhaus Universität Weimar) und Christopher Wolf (Ruhr-Universität Bochum) verantwortlich für die Organisation der Kryptotage. Für eventuelle Rückfragen bitte an sie wenden.