

Periodische n-fach anonyme Authentifizierung für Sensoren

Jan Camenisch¹ · Susan Hohenberger² · Markulf Kohlweiss³
· Anna Lysyanskaya⁴ · Mira Meyerovich⁴

¹IBM Research, Zurich Research Laboratory,
CH-8803 Rüschlikon, Switzerland,
jca@zurich.ibm.com

²CSAIL, Massachusetts Institute of Technology,
Cambridge, MA 02139, USA,
srhohen@mit.edu

³COSIC, Katholieke Universiteit Leuven,
B-3001 Heverlee-Leuven, Belgium,
markulf.kohlweiss@esat.kuleuven.be

⁴Computer Science Department, Brown University,
Providence, RI 02912, USA,
{anna,mira}@cs.brown.edu

Zusammenfassung

Wie verhindert man, dass ein anonymer Sensor öfter als viermal pro Tag Informationen übermittelt? Mittels E-Cash natürlich! Anonymität ist insbesondere für mobile personengebundene Sensoren wesentlich, die andernfalls den Aufenthaltsort ihrer Besitzer preisgeben. Die Einschränkung der Meldefrequenz ist nötig, um die uneingeschränkte Verbreitung von Roguesensoren zu verhindern.

Wir stellen ein System vor, das es Sensoren erlaubt, Daten bis zu n mal pro Zeitperiode anonym zu authentifizieren. Bei der Initialisierung erhält der Sensor über ein Abhebeprotokoll einen E-Token Spender mit n E-Tokens. Um Daten zu authentifizieren, zeigt der Sensor eines dieser E-Token in einem interaktiven Protokoll mit dem Empfänger. Jedes E-Token kann nur einmal verwendet werden, allerdings werden Spender pro Zeitperiode automatisch neu aufgefüllt. Die einzige bekannte Lösung für dieses Problems für $n = 1$, vorgestellt von Damgård et al. [20], verwendet Protokolle, die um den Faktor k langsamer sind. Der Sicherheitsparameter k bestimmt dabei die Wahrscheinlichkeit 2^{-k} , mit der ein Sensor unerkannt zwei Datensätze verschicken kann.

1. Einleitung

Rechengeräte werden kleiner und billiger. Sie fügen sich natlos in unser tägliches Leben ein. Dadurch wird es möglich, sie beinahe überall zu plazieren, um Information über ihr Umfeld zu sammeln. Beispielsweise können auf Fahrzeugen angebrachte Sensoren Information über den Straßenzustand und die Verkehrssituation an einen zentralen Verkehrsdienst weiterleiten. Dies erlaubt es Benutzern entsprechender Dienste ihre Reise besser zu planen und adequat auf gefährliche Situationen zu reagieren. Andere Vorschläge diskutieren die Verwendung von Sensoren in Kühlschränken, um Gebraucherstatistiken zu erstellen. Diese können neben ihrem Wert als Marketinginstrument auch für öffentliche Gesundheitsstudien herangezogen werden. Selbst die Verwendung von Sensoren zur Messung von Gesundheitswerten, als Mittel der Volksgesundheit, steht zur Diskussion. In all diesen Bereichen könnte die Verfügbarkeit besserer Information letztendlich zu einem besseren Leben für viele führen.

Diese Vision erscheint jedoch inkompatibel mit dem Schutz der Privatsphäre und den Grundsätzen des Datenschutzes. In Autos installierte Sensoren geben den Aufenthaltsort des Fahrzeuges preis. Sensoren in Kühlschränken registrieren die Ess- und Trinkgewohnheiten ihrer Besitzer.

Die naive Lösung besteht darin, dass Sensoren allein die relevante Information, keinesfalls jedoch ihre eigene Identität, übertragen.¹ In diesem Zustand totaler Anonymität gibt es jedoch keine Möglichkeit, um potentielle Angreifer an der Verbreitung irreführender Information zu hindern. Die von einem Sensor zur Verfügung gestellte Information muss authentifiziert werden, jedoch ohne die Identität des Sensors zu verraten. Darüber hinaus benötigen wir einen Mechanismus, um das Aufkommen von Roguesensoren zu verhindern. Roguesensoren sind ehemals ehrliche Sensoren mit gültigem Schlüsselmaterial, die von einem Angreifer übernommen wurden und die von diesem nun zum massiven Aussenden falscher Information verwendet werden.

Das gleiche Problem tritt auch in anderen Szenarien auf, etwa bei interaktiven Computerspielen. Jeder Spieler verfügt über eine Lizenz und beweist deren Besitz jedes Mal, wenn er sich zum zentralen Spielserver verbindet. Zum Schutz seiner Privatsphäre möchte der Spieler jedoch außer der Tatsache, dass er eine Lizenz besitzt, keinerlei weitere Information preisgeben. Wie kann in einem solchen Rahmen verhindert werden, dass Millionen von Nutzern mit einer identischen Lizenz auf das Spiel zugreifen?

Eine Fülle an kryptographischen Primitiven wie etwa Gruppensignaturen [17, 13, 1, 4] und anonyme Credentials [16, 19, 24, 10, 11, 12] wurden entwickelt, um zu beweisen, dass ein Datensatz von einer autorisierten Quelle stammt, ohne jedoch die Identität der jeweiligen Quelle zu offenbaren. Allerdings stellt keines der zitierten Resultate einen Mechanismus bereit, der bei garantierter Anonymität und Unverkettbarkeit der Aktionen ehrlicher Teilnehmer verhindert, dass Roguesensoren unerkannt und unerkennbar massive Falschinformation verbreiten. Es erscheint vielmehr, dass die Fähigkeit zur Verbreitung von Falschinformation eine natürliche Konsequenz von Anonymität ist.

Vor kurzem stellte jedoch Damgård, Dupont und Pedersen [20] ein Verfahren vor, das dieses

¹ Man bemerke, dass diese Information allein schon einen Eingriff in die Privatsphäre darstellen kann. In dieser Arbeit klammern wir diese Aspekte des Problems aus, die vor allem mit statistischen Eigenschaften der jeweiligen Daten selbst zu tun haben. Man konsultiere Sweeney [26] und Chawla et al. [18] als Referenz bezüglich der Problematik welche Daten zuübertragen bzw. geheimzuhalten sind.

scheinbare Paradox überwindet. Es erlaubt die anonyme und unverkettbare Übermittlung von Daten bei niedriger Übertragungsrate (beispielsweise bei einem Verkehrsbericht pro Viertelstunde oder einem Spielzugriff pro Halbestunde). Gleichzeitig können jedoch jene Teilnehmer identifiziert werden, die die Übertragungsrate überschreiten. Dies schränkt die Menge an Falschinformationen ein, die ein Roguesensor übertragen kann – oder viele Roguesensoren mit dem selben Schlüsselmaterial. Analog beschränkt es auch die Anzahl an identischen Softwarelizenzen, die während einer Periode verwendet werden können.

Leider ist der Ansatz von Damgård et al. zu ineffizient für den praktischen Einsatz. Zur Authentifizierung, agiert der Sensor als Beweiser (Prover) in einem zero-knowledge (ZK) Wissensbeweis (Proof-Of-Knowledge) der relevanten Zertifikate. Die zero-knowledge Eigenschaft beruht wesentlich auf den Zufallszahlen des Beweisers; sollte ein Sensor jemals die selben Zufallszahlen doppelt benutzen, so gibt er damit auch sein Schlüsselmaterial und somit seine Identität preis. Die Zufallszahlen des Sensors werden mittels einer Pseudozufallsfunktion von der aktuellen Zeitperiode abgeleitet. Ein zusätzlicher ZK Beweis stellt sicher, dass die vom Prover im Protokoll verwendeten Zufallszahlen korrekt generiert wurden. Sollte ein Roguesensor versuchen mehr als einen Datensatz pro Zeitperiode zu übertragen, so muss er dazu die selben Zufallszahlen erneut benutzen und enthüllt somit seine Identität.

Diese Konstruktion läßt sich jedoch nicht so ohne weiteres effizient umsetzen. Damgård et al. verwenden die effizientesten zur Verfügung stehenden Bausteine und führen sogar einige selbst neu ein. Dennoch benötigt ein Benutzer in ihrem Protokoll $57 + 68r$ Exponentiationen pro Authentifizierung. Der Sicherheitsparameter r fixiert dabei die Wahrscheinlichkeit 2^{-r} , mit der ein Sensor unerkant zwei Datensätze in der selben Zeitperiode verschicken kann.

Wir präsentieren hier eine Zusammenfassung und Diskussion der ersten praktikablen und effizienten Lösung, die in [7] vorgestellt wurde. Das angeführte Problem wird hierzu mit E-Cash [14, 15] und speziell mit kompaktem E-Cash [8] in Bezug gebracht. Jeder Teilnehmer bekommt eine Menge an E-Tokens von einem zentralen Server. Der Server erhält dabei, ähnlich wie in dem Abhebeprotokoll eines E-Cash Verfahrens, keinerlei Information über das Aussehen der ausgestellten E-Tokens. Unser Protokoll erlaubt es einem Teilnehmer, alle jemals benötigten E-Tokens in einer einzigen effizienten Transaktion abzuheben. Der Teilnehmer führt lediglich 3 multi-base Exponentiationen für das Abheben und 35 multi-base Exponentiationen für das Zeigen eines E-Tokens aus. Für den Fall, dass ein Teilnehmer auf ein E-Token pro Zeitperiode beschränkt ist, wie in Damgård et al., werden lediglich 13 multi-base Exponentiationen pro vorgelegten E-Token benötigt.

Verteilte Sensoren verwenden ein E-Token, um einen übermittelten Datensatz zu authentifizieren. Im Falle des Online-Spiels baut jedes E-Token eine neue Verbindung zum Spiel auf. Im Gegensatz zu E-Cash, wo nur eine begrenzte Menge an Geld pro Transaktion abgehoben wird, ist die Anzahl der von einem Teilnehmer erhaltenen E-Tokens unbeschränkt, und der Teilnehmer kann Daten senden oder neue Verbindungen zum Spiel aufbauen, solange dies gewünscht ist. Die E-Tokens sind anonym und sowohl miteinander als auch mit der Ausführung des Abhebeprotokolls, bei dem sie erzeugt wurden, unverkettbar. Die Anzahl der während einer spezifischen Zeitperiode gültigen E-Tokens ist jedoch beschränkt. Ähnlich wie bei E-Cash führt die Wiederverwendung von E-Tokens zur Identifikation von Rogueteilnehmern.

Im Sensorszenario kann ein einzelner Sensor folglich nicht mehr als eine kleine Anzahl an Datensätzen pro Zeitperiode verschicken. Als Resultat kann ein Roguesensor lediglich eine

begrenzte Menge an Falschinformation pro Periode generieren. Sollte er versuchen darüber hinaus Fehlinformation zu verbreiten, so muss er E-Tokens wiederverwenden, was wiederum zu seiner Identifikation führt. Ähnliches gilt für das Szenario des Online-Spieles. Eine Lizenz kann nur eine begrenzte Anzahl pro Tag verwendet werden. Somit wird es unmöglich ein Spiel vielfach gemeinsam zu nutzen.

NOTIZ ZUR TERMINOLOGIE Damgård et al. nennen das angeführte Problem „unclonable group identification,“ mit der Bedeutung, dass, sollte ein Teilnehmer eine Kopie seines Sensors erstellen, sich die Existenz eines solchen Klons manifestiert, sobald beide Sensoren während der selben Zeitperiode Daten übermitteln. Wir verallgemeinern dieses Problem und nennen es periodische n -fach anonyme Authentifizierung. n -fach, da es sich um eine Technik handelt, die es einem Teilnehmer während einer gegebenen Zeitperiode erlaubt n anonyme Authentifizierungen durchzuführen. Für $n = 1$ (also einem E-Token pro Zeitperiode) löst unser Verfahren das gleiche Problem wie das Verfahren von Damgård et al.

2. Funktionalität und Sicherheitsdefinition

Unser System erfüllt die folgende Spezifikation: Im Ausgabeprotokoll erhält jeder Sensor \mathcal{S} einen E-Token-Spender von dem E-Token-Herausgeber \mathcal{H} . Dies kann der Hersteller der Sensoren oder eine von ihm beauftragte Dachorganisation sein. Jeder E-Token-Spender D kann bis zu n anonyme und unverlinkbare E-Tokens pro Zeitperiode erzeugen – aber nicht mehr. Diese E-Tokens werden dann zusammen mit den Messergebnissen des Sensors an einen Prüfer \mathcal{P} übermittelt. Die Prüfer stellen fest, ob es sich um ein gültiges E-Token handelt. Zu einem späteren Zeitpunkt können doppelt ausgegebene E-Tokens erkannt und die Identität des betroffenen Sensors aufgedeckt werden.

\mathcal{S} , \mathcal{P} , und \mathcal{H} interagieren mittels der folgenden Algorithmen:

- **ISchlüErz**(k) ist der Schlüsselgenerierungsalgorithmus des E-Token-Herausgebers. Das erzeugte Schlüsselpaar ist $(pk_{\mathcal{H}}, sk_{\mathcal{H}})$. Der Sicherheitsparameter k gibt das benötigte Sicherheitslevel an.
- **USchlüErz**($k, pk_{\mathcal{H}}$) generiert den Schlüssel des Sensors $(pk_{\mathcal{S}}, sk_{\mathcal{S}})$. Auch hier bestimmt der Sicherheitsparameter k das verlangte Sicherheitslevel.
- **Erhalten**($\mathcal{S}(pk_{\mathcal{H}}, sk_{\mathcal{S}}, n), \mathcal{H}(pk_{\mathcal{S}}, sk_{\mathcal{H}}, n)$) versorgt einen Sensor mit E-Token-Spender D . Der Herausgeber erhält die Revozierungs-Information r_D .
- **Zeigen**($\mathcal{S}(D, pk_{\mathcal{H}}, t, n, m), \mathcal{P}(pk_{\mathcal{H}}, t, n, m)$) überträgt ein E-Token des E-Token-Spenders D für Zeitperiode t an den Prüfer. Das E-Token ist an die Nachricht m gebunden und authentifiziert diese somit. Die Ausgabe auf der Prüferseite ist die Token-Seriennummer TSN S und das Transkript τ des Tokens. Die Ausgabe auf der Sensorseite ist ein aktualisierter E-Token-Spender D' .
- **Identifizieren**($pk_{\mathcal{H}}, S, \tau, \tau'$) identifiziert bei Bereitstellung der beiden Datensätze (S, τ) und (S, τ') , $\tau \neq \tau'$, die bei einer doppelten Verwendung eines E-Tokens anfallen, den verantwortlichen Sensor. Dazu gibt der Algorithmus als Ergebnis den öffentlichen Schlüssel $pk_{\mathcal{S}}$ aus.

Sichere periodische n -fach anonyme Authentifizierung verlangt die folgenden drei Sicherheitseigenschaften:

Korrektheit. Sofern sich Herausgeber und Prüfer spezifikationskonform verhalten, ist garantiert, dass kein Sensor mehr als n unterschiedliche E-Tokens pro E-Token-Spender und Zeitperiode verschicken kann.

Identifikation. Diese Garantie gilt wiederum für korrekt arbeitende Herausgeber und Prüfer. Sollten zu irgendeiner Zeit zwei E-Token mit gleicher Seriennummer in Umlauf kommen, so kann aus (S, τ) und (S, τ') der öffentliche Schlüssel des verantwortlichen Sensors bestimmt werden.

Anonymität. Diese Sicherheitsanforderung garantiert die Anonymität der Sensoren. Ein Angreifer, der sowohl den Herausgeber als auch die Prüfer kontrolliert, kann, selbst wenn er bestimmt, wann Sensoren E-Token-Spender beziehen und E-Tokens zeigen, aus der dabei anfallenden Kommunikation keine Rückschlüsse auf die Identität der Besitzer der gezeigten Tokens ziehen.

Eine weitere Voraussetzung für die Praktikabilität eines solchen Verfahrens ist die Möglichkeit, E-Token-Spender zurückzuziehen. Sollte nämlich die Manipulationssicherheit eines Sensors gebrochen und die enthaltenen Geheimnisse weitere Verbreitung finden, so hilft die Identifizierung des ursprünglichen Sensors alleine nicht weiter. Es bedarf auch eines Mechanismus, um die weitere Verwendung des Spenders einzuschränken, und zwar auch dann, wenn die kopierten Geheimnisse in bestimmten Zeitperioden nur einmal verwendet werden.

- Zurückziehen($pk_{\mathcal{H}}, r_D, RD$) nimmt als Input die Revozierungs-Datenbank RD (anfangs leer) and Revozierungs-Information r_D , die einem bestimmten Sensor entspricht (siehe Erhalten). Das Ergebnis ist eine erweiterte Revozierungs-Datenbank RD . Im Verlauf nehmen wir an, dass RD Teil des $pk_{\mathcal{H}}$ ist.

3. Grundlagen und Werkzeuge

Notation: Seien $\langle g \rangle$ und $\langle \mathbf{g} \rangle$ die jeweils durch die Generatoren g bzw. \mathbf{g} erzeugten Gruppen \mathbb{G} und \mathbf{G} . Obwohl alle verwendeten Bausteine entweder in der Gruppe \mathbb{G} der Primordnung q oder in einer Gruppe zusammengesetzter Ordnung \mathbf{G} arbeiten, bleiben wir bei der Beschreibung unseres Verfahrens zumeist auf Bausteinebene und gehen nicht auf die mathematischen Details ein. Werden jedoch die Ergebnisse oder Eingaben solcher Algorithmen mittels mathematischer Operationen kombiniert, so meinen wir damit die entsprechende Gruppenoperation. Des Weiteren unterstellen wir implizite Konvertierung zwischen binären Strings und Ganzzahlen, wie etwa $\{0, 1\}^l$ und $[0, 2^l - 1]$.

3.1. Komplexitätsannahmen

Die Sicherheit unser E-Token System basiert auf der Voraussetzung, dass gewisse komplexitätstheoretische Probleme nicht in polynomialer Zeit lösbar sind. Wir nehmen an:

Starke RSA-Annahme [2, 23]: Gegeben sei ein RSA-Modulus n und ein zufälliges Element $\mathbf{g} \in \mathbb{Z}_n^*$. Die Berechnung eines $\mathbf{h} \in \mathbb{Z}_n^*$ und eines $e > 1$, so dass $\mathbf{h}^e \equiv \mathbf{g} \pmod{n}$ gilt, ist ein hartes Problem. Der Modulus n ist von der speziellen Form pq , mit sicheren Primzahlen $p = 2p' + 1$ und $q = 2q' + 1$.

Zusätzlich erfordert unsere Konstruktion entweder die y -DDHI- oder die SDDHI-Annahme, abhängig davon wie die Zeitperiodenbezeichner bestimmt werden. Beide Annahmen schließen

DDH (Decisional Diffie-Hellman) und DL (Schwierigkeit der Berechnung des diskreten Logarithmus) in den entsprechenden Gruppen mit ein.

y -Decisional Diffie-Hellman-Inversion (y -DDHI) [3, 21]: Sei $g \in \mathbb{G}$ ein zufälliger Generator der Ordnung $q \in \Theta(2^k)$. Dann gilt für alle probabilistischen Angreifer \mathcal{A} mit polynomialer Rechenzeitbeschränkung,

$$\Pr[a \leftarrow \mathbb{Z}_q^*; x_0 = g^{1/a}; x_1 \leftarrow \mathbb{G}; b \leftarrow \{0, 1\}; b' \leftarrow \mathcal{A}(g, g^a, g^{a^2}, \dots, g^{a^y}, x_b) : \\ b = b'] < 1/2 + 1/\text{poly}(k).$$

Starke DDH-Inversion (SDDHI): Sei $g \in \mathbb{G}$ ein zufälliger Generator der Ordnung $q \in \Theta(2^k)$. Sei des weiteren $\mathcal{O}_a(\cdot)$ ein Orakel, das bei Eingabe $x \in \mathbb{Z}_q^*$ das Ergebnis $g^{1/(a+x)}$ ausgibt. Dann gilt für alle probabilistischen Angreifer $\mathcal{A}^{(\cdot)}$ mit polynomialer Rechenzeitbeschränkung, die das Orakel nicht in x befragen,

$$\Pr[a \leftarrow \mathbb{Z}_q^*; (x, \alpha) \leftarrow \mathcal{A}^{\mathcal{O}_a}(g, g^a); y_0 = g^{1/(a+x)}; y_1 \leftarrow \mathbb{G}; b \leftarrow \{0, 1\}; b' \leftarrow \mathcal{A}^{\mathcal{O}_a}(y_b, \alpha) : \\ b = b'] < 1/2 + 1/\text{poly}(k).$$

3.2. Bausteine

Wir fassen die Eigenschaften und möglichen Instantiierungen der von uns in der Konstruktion eines sicheren E-Token-Systems verwendeten Bausteine zusammen.

Pseudozufallsfunktionen (PZF) mit effizienten Wissensbeweisen Eine Pseudozufallsfunktion lässt sich durch einen effizienten Algorithmus nicht von einer rein zufälligen Funktion unterscheiden. Zusätzlich verlangen wir dass für ein $y = PZF(x; s)$ ein Nachweis der korrekten Herleitung aus dem geheimen Argument x und dem ebenfalls geheimen Seed s effizient möglich ist. Dies entspricht einem Wissensbeweis $PK\{(s, x) : y = PZF(x; s)\}$ in stark verallgemeinerter Camenisch-Stadler-Notation [13].

Eine mögliche Instantiierung einer solchen Pseudozufallsfunktion wurde von Dodis and Yampolskiy [21] vorgeschlagen. Sei $\mathbb{G} = \langle g \rangle$ eine Gruppe der Primordnung q . Sei des weiteren s der zufällige Seed aus \mathbb{Z}_q^* . Dodis and Yampolskiy [21] zeigen, dass $PZF_{DY}(x; s, g) = g^{1/(s+x)}$ eine Pseudozufallsfunktion unter der y -DDHI-Annahme ist, wenn vor der Wahl des Seeds s der Definitionsbereich der Funktion auf eine polynomiale Teilmenge von \mathbb{Z}_q^* eingeschränkt wird. Falls der Definitionsbereich nicht auf diese Weise eingeschränkt werden kann, ist ein Sicherheitsbeweis nur unter die SDDHI-Annahme möglich. Dies gilt etwa dann, wenn Zeitperioden durch beliebige Elemente aus \mathbb{Z}_q^* indiziert werden können.

Commitments mit effizienten Wissensbeweisen Von kryptographischen Commitments wird erwartet, dass sie bindend und geheimhaltend sind. Wir verlangen darüber hinaus, dass ein effizienter Nachweis über die korrekte Erzeugung des Commitments erbracht werden kann. Des weiteren kann ein Wissensbeweis erbracht werden, dass zwei Commitments den selben Wert enthalten, ohne diesen jedoch offen zulegen. Letzteres entspricht einem Wissensbeweis $PK\{(x, r_1, r_2) : C_1 = \text{commit}(x; r_1) \wedge C_2 = \text{commit}(x; r_2)\}$.

Ein weitere Baustein sind Commitments mit effizientem Nachweis, dass der fixierte Wert in einem Intervall $[a, b]$ liegt. Der entsprechende Wissensbeweis ist $PK\{(x, r) : C = \text{commit}(x; r) \wedge a \leq x \leq b\}$.

Eine weitere Eigenschaft, auf die in unseren Protokollen zurückgegriffen wird, ist die additive Verformbarkeit (Malleability) der Commitments. Aus einem Commitment $C_1 = \text{commit}(x; r)$ lässt sich so, ohne Kenntnis von x und r ein Commitment $C_2 = \text{commit}(x + x'; r)$ bestimmen.

Pedersen-Commitments [25] erlauben effiziente Beweise der ersten Art. Eine Gruppe \mathbb{G} der Primordnung q und die Generatoren (g_0, \dots, g_m) sind die öffentlichen Parameter eines solchen Verfahrens. Um sich auf die Werte $(v_1, \dots, v_m) \in \mathbb{Z}_q^m$ festzulegen, wählt man ein zufälliges $r \in \mathbb{Z}_q$ und berechnet $C = \text{commit}(v_1, \dots, v_m; r) = g_0^r \prod_{i=1}^m g_i^{v_i}$.

Fujisaki and Okamoto [23] zeigen wie sich dieses Verfahren auf Gruppen \mathbb{G} zusammengesetzter Ordnung erweitern lässt. Diese Commitments erlauben nun auch effiziente Intervallbeweise [5].

Signaturen mit effizienten Wissensbeweisen Camenisch und Lysyanskaya [11] verwendeten erstmals Signaturverfahren, für die sich effiziente Protokolle definieren lassen, um:

- (1) eine Signatur für die durch ein Pedersen (oder Fujisaki-Okamoto) Commitment [25, 23] fixierten Werte zu erhalten, ohne dass der Unterzeichner etwas über diese Werte lernt;
- (2) die Kenntnis einer solchen Signatur nachzuweisen, ohne die Signatur selbst zu zeigen.

Die Sicherheit der etabliertesten Instantiierungen dieses Verfahrens beruht auf der starken RSA-Annahme. Für elliptische Kurven mit bilinearen Paarungen sind weitere Signaturverfahren [12, 4] mit kürzeren Signaturen bekannt. Wir bezeichnen diese Signaturverfahren im folgenden verkürzt als CL-Signaturen und die beiden Protokolle als CL-Protokoll 1 und 2.

Nicht-interaktive Wissensbeweise Im Zufallsorakelmodell lassen sich Wissensbeweise, in unserem Fall meist Drei-Runden-Protokolle, unter Verwendung der Fiat-Shamir-Heuristik [22] in nicht-interaktive Protokolle überführen. Wird eine Nachricht m , mittels der bei Fiat-Shamir verwendeten Hashfunktion, an den nicht-interaktiven Beweis gebunden, so erhält man ein Signaturverfahren.

Wir benutzen die Notation $SPK\{(Geheimnisse) : \text{Praedikat}(\text{Geheimnisse})\}(m)$, um die so erhaltene Signatur auszudrücken. Der geheime Schlüssel entspricht den bewiesenen Geheimnissen.

3.3. Bestimmung des Zeitperiodenbezeichners

Etwas so anschauliches wie Zeit wird im Kontext eines Systems mit garantieren Sicherheitseigenschaften zur komplexen technischen Herausforderung.

Einerseits verlangen wir, dass der Zeitperiodenbezeichner t für alle Sensoren, die E-Tokens in einer Periode zeigen, der gleiche ist. Des weiteren wird verlangt, dass er einzigartig oder dublettenfrei ist, in dem Sinne, dass er zu keinem späteren Zeitpunkt erneut Verwendung findet. Unsere Konstruktion erlaubt die Verwendung beliebiger Zeitintervallbezeichner, unter den in Abschnitt 3.1 besprochenen Bedingungen. Unter der stärkeren SDDHI Annahme (dies entspricht schwächeren Sicherheitsgarantien) kann somit auch das Hashbaumprotokoll aus [20] verwendet werden.

4. Ein periodisches n -fach anonymes Authentifizierungsverfahren

Stark vereinfacht funktioniert die Konstruktion wie folgt:

Schlüsselmanagement: Zuerst generiert der Herausgeber seine Schlüssel ($\text{ISchlüErz}(k)$). Der geheime Schlüssel besteht aus einem CL-Signaturschlüssel, der öffentliche Schlüssel aus dem entsprechenden Verifikationsschlüssel und dem Setup für die Commitments und die PZF. Darüberhinaus erstellt der Herausgeber einen nicht-interaktiven Beweis, dass all diese Parameter korrekt erzeugt wurden. Der geheime Schlüssel $sk_{\mathcal{H}}$ enthält alle Parameter; der öffentlichen Schlüssel $pk_{\mathcal{H}}$ alle Parameter mit Ausnahme des Signaturschlüssels.

In $\text{USchlüErz}(k, pk_{\mathcal{H}})$ wählt der Sensor einen zufälligen geheimen Schlüssel $sk_{\mathcal{S}} \in \mathbb{Z}_q$ und setzt $pk_{\mathcal{S}} = \text{commit}(sk_{\mathcal{S}}; 0)$. Zusätzlich prüft der Sensor den vom Hersteller erbrachten Beweis der korrekten Erzeugung von $pk_{\mathcal{H}}$. Das Schlüsselpaar des Sensors ist somit $(pk_{\mathcal{S}}, sk_{\mathcal{S}})$, mit $pk_{\mathcal{S}} = \text{commit}(sk_{\mathcal{S}}; 0)$. Dieses Commitment und die Werte der PZF sind beide Elemente der Gruppe G mit Primordnung q .

Ausstellen eines E-Token-Spenders: \mathcal{S} und \mathcal{H} authentifizieren sich gegenseitig. Im Falle eines TPM [27] basierten Sensors könnte dies etwa durch Verwendung des Endorsement-Keys und der im Sensor enthaltenen Zertifikate erfolgen. Während des Erhalten Protokolls bekommt ein Sensor einen E-Token-Spender D zugewiesen, der es ihm erlaubt n Tokens pro Zeitperiode zu zeigen. Der Spender D besteht aus einem Seed s für die PZF, und der CL-Signatur des Herausgebers für s und $sk_{\mathcal{S}}$. Dabei verwenden wir CL-Protokoll 1, um zu verhindern, dass der Herausgeber etwas über s und $sk_{\mathcal{S}}$ lernt.

Verwendung eines E-Tokens: Seien $Serial = 0$ und $Tag = 1$ zwei binäre Konstanten. Im Zeigen Protokoll zeigt ein Sensor sein i tes Token für Zeitperiode t . Der Sensor überträgt dazu die Seriennummer

$$S = PZF(Serial || t || i; s) \quad (1)$$

und den Dublettentag

$$E = pk_{\mathcal{S}} \cdot PZF(Tag || t || i; s)^R \quad (2)$$

für ein vom Prüfer bereitgestelltes zufälliges R . Zusätzlich erbringt der Sensor den Nachweis, dass (S, E) von einem gültigen Spender für Zeitperiode t und für ein i , $0 \leq i < n$, korrekt erzeugt wurde. Hierzu beweist der Sensor, dass er i , s und $pk_{\mathcal{S}} = \text{commit}(sk_{\mathcal{S}}; 0)$ kennt, so dass S und E entsprechend den Gleichungen (1) und (2) geformt sind und der Seed s zusammen mit dem geheimen Schlüssel des Sensors $sk_{\mathcal{S}}$ durch den Hersteller signiert ist. Dazu verwendet er CL-Protokoll 2 und die Wissensbeweise für Commitments und PZF. Der kombinierte Beweis ist nicht-interaktiv und authentifiziert die gehashte Nachricht m .

Da S und E pseudozufällig und da die verwendeten Wissensbeweise Zero-Knowledge-Beweise sind, kann das resultierende E-Token (komplexitätstheoretisch) nicht mit dem Sensor, dem Spender D oder irgendeinem anderen E-Token des selben Spenders verknüpft werden.

Aufdeckung von Missbrauch und Deanonymisierung: Zeigt ein Sensor jedoch $n + 1$ E-Tokens pro Zeitintervall, so haben notwendigerweise zwei E-Token die gleiche TSN. Der Herausgeber kann diesen Verstoß erkennen und $pk_{\mathcal{S}}$ aus zwei Dublettentags berechnen:

$$E = pk_{\mathcal{S}}^R \cdot PZF(Tag || t || i; s), \quad E' = pk_{\mathcal{S}}^{R'} \cdot PZF(Tag || t || i; s).$$

Aus Gleichung (2) folgt

$$pk_S = (E/E')^{(R-R')^{-1}}.$$

Zurücknahme von E-Token-Spendern: Der in [9] vorgestellte, und in [6] optimierte Mechanismus für die Revozierung von CL-Signaturen kann verwendet werden, um E-Token-Spender unbrauchbar zu machen. Der Prüfer verifiziert dabei, ob die vom Sensor in CL-Protokoll 2 gezeigte CL-Signatur noch gültig ist. Die Revozierungs-Information besteht aus der Primzahl e der CL-Signatur, die Revozierungs-Datenbank aus einem dynamischen Akkumulator. Einzelne Primzahlen können zu einem Akkumulator hinzugefügt und entfernt werden.

5. Ausblick

Die Arbeit beschreibt wie aus dem Seed eines E-Token-Spenders, zeitintervallbezogene, verifizierbare und pseudozufällige Seriennummern abgeleitet werden können. Des weiteren wurde ein Mechanismus vorgestellt, um bei doppelter Verwendung einer solchen Seriennummer die Identität des Benutzers aufzudecken. Indem die zu authentifizierende Nachricht kryptographisch an diese Seriennummer gebunden wird, ist es möglich starke Garantien über den Ursprung der Nachricht abzugeben, ohne die Anonymität des Senders zu verletzen. Sender werden wie bei der Verwendung von Gruppensignaturen durch den Herausgeber autorisiert. Zusätzlich wird selbst bei Kompromittierung einzelner Sensoren eine Überflutung des Netzwerkes mit Falschnachrichten vermieden und eine unkoordinierte parallele Verwendung von geklonten Sensoren quasi unmöglich gemacht.

In Abstraktion von den kryptographischen Details dieser Arbeit, läßt sich ihr Ergebnis wie folgt zusammenfassen: Starke Authentifizierung und Anonymität widersprechen sich nicht. Die häufigsten Einwände betreffen die mangelnden Effizienz und der Missbrauchsanfälligkeit anonymer Transaktionen. Schon die Diskussion um den Schutz der Privatsphäre in Trusted-Computing und die Entscheidung DAA (Direct Anonymous Attestation) in die TPM-Spezifikation aufzunehmen, sind ein Indiz, dass solche Verfahren auch bei heutiger Rechenleistung durchaus realisierbar sind. Während es in DAA noch einen Zielkonflikt zwischen Anonymität und Mibrauchserkennung gibt, denn je niedriger der Schwellwert für die Erkennung von Rogue-TPMs gesetzt wird, desto höher ist die Verkettbarkeit der Aktionen, wird dieses Problem von der hier vorgestellten Lösung behoben. Während die Praktikabilität anonymer Transaktionen für E-Kommerz-Szenarien hohe Infrastrukturinvestitionen und eventuell sogar Gesetzesänderungen voraussetzt, erscheint die Realisierung dezidierter Speziallösungen wie der hier vorgestellten anonymen Sensoren auch diesbezüglich praktikabel.

6. Acknowledgement

Part of Jan Camenisch's work reported in this paper is supported by the European Commission through the IST Programme under Contracts IST-2002-507932 ECRYPT and IST-2002-507591 PRIME.² Part of Susan Hohenberger's work is supported by an NDSEG Fellowship. Markulf Kohlweiss is supported by the European Commission through the IST Programme under Contract IST-2002-507591 PRIME.² Anna Lysyanskaya is supported by NSF Career Grant

² The PRIME projects receives research funding from the European Community's Sixth Framework Programme and the Swiss Federal Office for Education and Science.

CNS-0347661. Mira Meyerovich is supported by a U.S. Department of Homeland Security Fellowship and NSF grant CNS-0347661. All opinions expressed in this paper are the authors' and do not necessarily reflect the policies and views of EC, DHS, and NSF.

Literatur

- [1] ATENIESE, GIUSEPPE, JAN CAMENISCH, MARC JOYE und GENE TSUDIK: *A Practical and Provably Secure Coalition-Resistant Group Signature Scheme*. In: BELLARE, MIHIR (Herausgeber): *CRYPTO 2000*, Band 1880 der Reihe LNCS, Seiten 255–270. Springer Verlag, 2000.
- [2] BARIĆ, NIKO und BIRGIT PFITZMANN: *Collision-free accumulators and fail-stop signature schemes without trees*. In: *EUROCRYPT '97*, Band 1233, Seiten 480–494, 1997.
- [3] BONEH, DAN und XAVIER BOYEN: *Short Signatures Without Random Oracles*. In: *EUROCRYPT 2004*, Band 3027 of LNCS, Seiten 56–73, 2004.
- [4] BONEH, DAN, XAVIER BOYEN und HOVAV SHACHAM: *Short Group Signatures using Strong Diffie-Hellman*. In: *CRYPTO*, Band 3152 of LNCS, Seiten 41–55, 2004.
- [5] BOUDOT, FABRICE: *Efficient Proofs that a Committed Number Lies in an Interval*. In: *EUROCRYPT '00*, Band 1807 der Reihe LNCS, Seiten 431–444, 2000.
- [6] CAMENISCH, JAN und JENS GROTH: *Group Signatures: Better Efficiency and New Theoretical Aspects*. In: *proceedings of SCN '04*, Band 3352 of LNCS, Seiten 120–133, 2004.
- [7] CAMENISCH, JAN, SUSAN HOHENBERGER, MARKULF KOHLWEISS, ANNA LYSYANSKAYA und MIRA MEYEROVICH: *How to Win the Clone Wars: Efficient Periodic n-Times Anonymous Authentication*. In: *ACM Conference on Computer and Communications Security*. ACM, 2006.
- [8] CAMENISCH, JAN, SUSAN HOHENBERGER und ANNA LYSYANSKAYA: *Compact E-Cash*. In: *EUROCRYPT*, Band 3494 of LNCS, Seiten 302–321, 2005.
- [9] CAMENISCH, JAN und ANNA LYSYANSKAYA: *Dynamic accumulators and application to efficient revocation of anonymous credentials*. <http://eprint.iacr.org/2001>, 2001.
- [10] CAMENISCH, JAN und ANNA LYSYANSKAYA: *Efficient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation*. In: PFITZMANN, BIRGIT (Herausgeber): *EUROCRYPT 2001*, Band 2045 der Reihe LNCS, Seiten 93–118. Springer Verlag, 2001.
- [11] CAMENISCH, JAN und ANNA LYSYANSKAYA: *A Signature Scheme with Efficient Protocols*. In: *SCN 2002*, Band 2576 der Reihe LNCS, Seiten 268–289, 2003.
- [12] CAMENISCH, JAN und ANNA LYSYANSKAYA: *Signature Schemes and Anonymous Credentials from Bilinear Maps*. In: *CRYPTO 2004*, Band 3152 der Reihe LNCS, Seiten 56–72, 2004.
- [13] CAMENISCH, JAN und MARKUS STADLER: *Efficient Group Signature Schemes for Large Groups*. In: KALISKI, BURT (Herausgeber): *CRYPTO '97*, Band 1296 der Reihe LNCS, Seiten 410–424. Springer Verlag, 1997.
- [14] CHAUM, DAVID: *Blind Signatures for Untraceable Payments*. In: *CRYPTO '82*, Seiten 199–203. Plenum Press, 1982.

-
- [15] CHAUM, DAVID: *Blind Signature Systems*. In: *CRYPTO '83*, Seiten 153–156. Plenum, 1983.
- [16] CHAUM, DAVID: *Security Without Identification: Transaction Systems to Make Big Brother obsolete*. *Communications of the ACM*, 28(10):1030–1044, Oktober 1985.
- [17] CHAUM, DAVID und EUGÈNE VAN HEYST: *Group signatures*. In: DAVIES, DONALD W. (Herausgeber): *EUROCRYPT '91*, Band 547 der Reihe *LNCS*, Seiten 257–265. Springer-Verlag, 1991.
- [18] CHAWLA, SHUCHI, CYNTHIA DWORK, FRANK MCSHERRY, ADAM SMITH und HOE-TECK WEE: *Toward Privacy in Public Databases*. In: KILIAN, JOE (Herausgeber): *Second Theory of Cryptography Conference*, Band 3378 der Reihe *Lecture Notes in Computer Science*, Seiten 363–385. Springer, 2005.
- [19] DAMGÅRD, IVAN BJERRE: *Payment Systems and Credential Mechanism with Provable Security against Abuse by Individuals*. In: GOLDWASSER, SHAFI (Herausgeber): *CRYPTO '88*, Band 403 der Reihe *LNCS*, Seiten 328–335. Springer Verlag, 1990.
- [20] DAMGÅRD, IVAN BJERRE, KASPER DUPONT und MICHAEL OSTERGAARD PEDERSEN: *Unclonable Group Identification*. *Cryptology ePrint Archive*, Report 2005/170, 2005. <http://eprint.iacr.org/2005/170>.
- [21] DODIS, YEVGENIY und ALEKSANDR YAMPOLSKIY: *A Verifiable Random Function with Short Proofs and Keys*. In: *Public Key Cryptography*, Band 3386 of *LNCS*, Seiten 416–431, 2005.
- [22] FIAT, AMOS und ADI SHAMIR: *How to Prove Yourself: Practical Solutions to Identification and Signature Problems*. In: ODLYZKO, ANDREW M. (Herausgeber): *CRYPTO '86*, Band 263 der Reihe *LNCS*, Seiten 186–194. Springer Verlag, 1987.
- [23] FUJISAKI, EIICHIRO und TATSUAKI OKAMOTO: *Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations*. In: *CRYPTO '97*, Band 1294 der Reihe *LNCS*, Seiten 16–30, 1997.
- [24] LYSYANSKAYA, ANNA, RON RIVEST, AMIT SAHAI und STEFAN WOLF: *Pseudonym Systems*. In: HEYS, HOWARD und CARLISLE ADAMS (Herausgeber): *Selected Areas in Cryptography*, Band 1758 der Reihe *LNCS*, 1999.
- [25] PEDERSEN, TORBEN PRYDS: *Non-interactive and information-theoretic secure verifiable secret sharing*. In: *CRYPTO '92*, Band 576 der Reihe *LNCS*, Seiten 129–140, 1992.
- [26] SWEENEY, LATANYA: *k-anonymity: a model for protecting privacy*. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10(5):557–570, 2002.
- [27] TRUSTED COMPUTING GROUP: *TCG TPM Specification 1.2*. Available at www.trustedcomputinggroup.org, 2003.