

Vorrichtung zur Transformation eines Datensatzes mit einem geheimen Schlüssel

Technisches Gebiet

Die Erfindung bezieht sich auf eine Vorrichtung zur Transformation eines Datensatzes mit einem geheimen Schlüssel, wobei eine Abfrageeinheit über eine
5 bidirektionale Kommunikationsschnittstelle mit einer Transformationseinheit verbunden ist, die einen Speicher für den geheimen Schlüssel und einen Prozessor zur Transformation des Datensatzes aufweist.

Stand der Technik

Bei der Abwicklung digitaler Transaktionen liegen der Signatur der
10 Transaktionsdatensätze sowie der Authentifizierung des Benutzers regelmäßig asymmetrische Verschlüsselungsverfahren zugrunde. Um derartige Transaktionen unter möglichst hohen Sicherheitsbedingungen durchführen zu können, ist es insbesondere im Zusammenhang mit Transaktionen auf Basis von Kryptowährungen wesentlich, dass nicht nur die Transformation der
15 entsprechenden Datensätze auf zuverlässige Weise erfolgen kann, sondern dass auch Maßnahmen getroffen werden, die eine sichere Verwahrung der für die Transaktionsabwicklung erforderlichen geheimen Schlüssel sowie der tokenisierten Werte der Kryptowährungen erlauben.

Vor diesem Hintergrund wurden bereits Vorrichtungen vorgeschlagen, die eine
20 Transformationseinheit mit einem Speicher für den geheimen Schlüssel sowie einem Prozessor zur Transformation des Datensatzes vorsehen. Die Transformationseinheit kann beispielsweise als sogenannte mobile Cryptowallet ausgebildet sein, die zur Durchführung der Transaktion über eine USB-Schnittstelle mit einer an einem Netzwerk bzw. am Internet angeschlossenen
25 Abfrageeinheit verbunden werden kann. Obwohl derartige

Transformationseinheiten grundsätzlich die offline-Verwahrung geheimer Schlüssel sowie gegebenenfalls tokenisierter Werte erlauben, sind Benutzer dennoch einem erheblichen Sicherheitsrisiko ausgesetzt. So kann die während der Transaktionsabwicklung zwischen Transformations- und Abfrageeinheit aufgebaute Busverbindung, nicht zuletzt aufgrund der dabei erforderlichen Übertragungssoftware, bislang nicht sinnvoll gegenüber von der Abfrageeinheit ausgehenden Seitenkanalanalysen oder invasiven Attacken zur Schädigung der Transformationseinheit geschützt werden. Darüber hinaus ist an den aus dem Stand der Technik bekannten Vorrichtungen auch nachteilig, dass bei einem Verlust der Transformationseinheit auch die darin gespeicherten geheimen Schlüssel und tokenisierten Werte unwiderruflich verloren gehen.

Es besteht somit ein Bedarf an einer Vorrichtung der eingangs geschilderten Art, die eine zuverlässige und sichere, insbesondere gegenüber Seitenkanalattacken geschützte Abwicklung digitaler Transaktionen bei nachhaltig sicherer Verwahrung der sensiblen geheimen Schlüssel ermöglicht.

Darstellung der Erfindung

Die Erfindung löst die gestellte Aufgabe dadurch, dass die Abfrageeinheit mehrere optische Sender zum parallelen Übertragen von Codewörtern des in zweidimensionale Codewörter übersetzten Datensatzes an mehrere optische Empfänger der Transformationseinheit und die Transformationseinheit mehrere optische Sender zum parallelen Übertragen von Codewörtern des in zweidimensionale Codewörter übersetzten transformierten Datensatzes an mehrere optische Empfänger der Abfrageeinheit aufweist, wobei Sender und Empfänger einer Einheit je in einem zweidimensionalen Raster angeordnet sind und den Empfängern und Sendern der anderen Einheit mit Abstand gegenüberliegen. Zuzufolge dieser Merkmale wird zunächst eine permanente physische Trennung der Transformationseinheit und der darauf gespeicherten sensiblen geheimen Schlüssel von umliegenden, mit der Abfrageeinheit verbundenen Zugangssystemen erreicht. Eine Transformation eines Datensatzes kann beispielsweise bedeuten, dass der Datensatz vollständig verschlüsselt wird

oder dass bei Abwicklung einer Transaktion der Datensatz in der Transformationseinheit signiert wird, wonach der signierte Datensatz über die Abfrageeinheit beispielsweise an die Blockchain übermittelt und nach erfolgreicher Integritätsprüfung in dieser abgespeichert werden kann. Unter einer

5 Signatur kann dabei beispielsweise die Ergänzung des Datensatzes mit einem verschlüsselten Hashwert seiner selbst verstanden werden. Da zur Übertragung keine physische Verbindung zwischen Transformationseinheit und Abfrageeinheit erforderlich ist, die potentiell Seitenkanalattacken zulässt oder gar Schwachstellen besitzt, erzeugen alleine die physischen Möglichkeiten der optischen Übertragung

10 mithilfe der zweidimensionalen Codewörter die sicherheitsrelevanten Begrenzungen. Dabei liegt der Erfindung die Überlegung zugrunde, dass durch die parallele Übertragung zweidimensionaler Codewörter der Informationsgehalt der einzelnen Codewörter verglichen zum Datensatz so hoch ist, dass eine erfolgreiche Manipulation der Übertragung durch einen Eingriff in den

15 Übertragungskanal nicht mehr möglich ist. Je nach verwendeten Codierungsverfahren und entsprechenden Methoden zur Fehlerkorrektur scheitert nämlich die Einschleusung von schadhafte Informationen an der vorgegebenen Integrität bzw. der gleichzeitigen optischen Übertragung der zweidimensionalen Codewörter. Dies ist insbesondere dann der Fall, wenn die in den Codewörtern

20 verwendete Fehlerkorrektur mehr als einen Fehler zulässt, wie dies beispielsweise bei Reed-Solomon-Codes der Fall ist. Grundsätzlich kann jeder zur Transaktion von der Abfrageeinheit an die Transformationseinheit, et vice versa übertragene untransformierte bzw. transformierte Datensatz genau in ein Codewort übersetzt werden. Es ist aber auch denkbar, dass die entsprechenden

25 untransformierten bzw. transformierten Datensätze jeweils in mehrere Codewörter, die nacheinander übertragen werden, übersetzt werden können. Dabei kann auch ein Angriff durch Manipulation eines externen Taktgebers dadurch ausgeschlossen werden, dass der Bildwechsel an den optischen Sendern selbst als Übertragungstakt herangezogen wird. Besonders vorteilhafte

30 Bedingungen ergeben sich in Hinblick auf Übertragungssicherheit und Übertragungsdauer, wenn die Seitenlängen des zweidimensionalen Rasters an optischen Sendern und / oder Empfängern genauso wie die Seitenlängen der zweidimensionalen Codewörter größer als 10, vorzugsweise größer als 20 ist.

Dies bedeutet, dass entlang beider Ausdehnungsrichtungen der Codewörter mehr als 10, vorzugsweise mehr als 20 Codeelemente, beispielsweise schwarze oder weiße Symbolzellen vorgesehen sind, zu deren Übermittlung wenigstens die gleiche Anzahl optischer Sender und Empfänger vorgesehen sein muss. Mit
5 einem Codewort können dabei mehr als 50, bevorzugt mehr als 100, besonders bevorzugt mehr als 200 bit des Datensatzes bzw. des transformierten Datensatzes übertragen werden.

Obwohl jedem optischen Sender genau ein optischer Empfänger zugeordnet werden kann, kann die in einem Codewort parallel übertragbare Information mit
10 geringem Aufwand platzsparend erhöht werden, wenn die optischen Sender die Bildpunkte eines Displays und die optischen Empfänger die Bildpunkte eines Bildsensors sind. Auf diese Weise können vorhandene Standardbauteile zum Einsatz kommen, was eine Produktion der erfindungsgemäßen Vorrichtung in großen Stückzahlen begünstigt.

15 In diesem Zusammenhang wird vorgeschlagen, dass zwischen den Displays und den Bildsensoren eine zentralprojizierende Optik vorgesehen ist. Aufgrund dessen, dass Bildsensoren auch mit hoher Auflösung entsprechend klein gefertigt werden können, sodass die Bildsensoren kleiner als die Displays sind, kann das gesamte, die jeweiligen Sender und Empfänger umfassende bidirektionale
20 Übertragungssystem im Wesentlichen auf die Größe des Displays beschränkt werden, sodass neben einer zuverlässigen optischen Übertragung eine besonders kompakte Bauweise der Vorrichtung ermöglicht wird.

Beispielsweise kann vorgesehen sein, dass die zweidimensionalen Codewörter Matrix-Codes, insbesondere Quick-Response-Codes bilden, wobei die
25 vorgegebenen Codeelemente ein oder mehreren optischen Sendern zugeordnet werden. Dabei können die Codeelemente die, im Falle des Quick-Response-Codes quadratischen, üblicherweise entweder schwarzen oder weißen Symbolzellen der Codematrix sein. Quick-Response-Codes haben aufgrund ihrer weitgehenden Transformationsinvarianz den Vorteil, dass auf eine exakte
30 Ausrichtung zwischen den optischen Sendern und den optischen Empfängern

verzichtet werden kann. Darüber hinaus weisen diese Codes ein hohes Maß an Redundanz auf, was das Einschleusen von schadhafte Informationen weiter erschwert.

- Um einen physischen Eingriff in die optische Schnittstelle zu verhindern, empfiehlt es sich, dass die Transformationseinheit und die Abfrageeinheit in einem gemeinsamen Gehäuse untergebracht sind. Zur weiteren Erhöhung der Sicherheit kann zudem vorgesehen sein, dass das Gehäuse ein Widerstandsmessgerät aufweist. Wird nun die Transformation der Datensätze auf Basis eines vorgegebenen Widerstandswertes durchgeführt und detektiert das Widerstandsmessgerät einen vom vorgegebenen Widerstandswert abweichenden Wert, beispielsweise indem das Gehäuse gewaltsam aufgebrochen wird, werden die Transaktionen unterbrochen und der Zugriff auf das System gesperrt.

- Für besonders gute Sicherheitsbedingungen kann der Zwischenraum zwischen den optischen Sendern und den gegenüberliegenden optischen Empfängern mit einer optisch durchlässigen Vergussmasse versehen sein. Unter einer optischen Durchlässigkeit wird verstanden, dass in Bezug auf die optischen Signale eine verzerrungsfreie Übertragung ermöglicht wird. Beispielsweise können hierfür geeignete Gießharze auf Polyurethanbasis oder Polyacrylate vorgesehen sein. In einer besonders günstigen Ausführungsform können optisch anisotrope, beispielsweise unterschiedliche raumrichtungsabhängige Brechungsindizes aufweisende Vergussmassen eingesetzt werden, sodass lediglich in Übertragungsrichtung eine für eine verzerrungsfreie optische Übertragung erforderliche optische Durchlässigkeit gegeben ist, während quer dazu einfallendes Licht die Übertragung nicht stören kann.

- Die Erfindung bezieht sich auch auf ein Verfahren zur Transformation eines Datensatzes mit einem geheimen Schlüssel, wobei ein Datensatz von einer Abfrageeinheit an eine Transformationseinheit übertragen, anhand eines in der Transformationseinheit hinterlegten Schlüssels transformiert und der transformierte Datensatz an die Abfrageeinheit zurückgegeben wird. Dabei wird der untransformierte Datensatz von der Abfrageeinheit in zweidimensionale

- Codewörter übersetzt, deren Codeelemente werden optisch und parallel an die Transformationseinheit übertragen und dort transformiert. Der transformierte Datensatz wird wiederum von der Transformationseinheit in zweidimensionale Codewörter übersetzt wird und deren Codeelemente werden optisch und parallel
- 5 an die Abfrageeinheit übertragen.

Kurze Beschreibung der Erfindung

In der Zeichnung ist der Erfindungsgegenstand beispielsweise dargestellt und zwar in einer schematischen Draufsicht auf eine erfindungsgemäße Vorrichtung.

Wege zur Ausführung der Erfindung

- 10 Eine erfindungsgemäße Vorrichtung zur Transformation eines Datensatzes mit einem geheimen Schlüssel weist eine Abfrageeinheit 1 auf, die über eine bidirektionale Kommunikationsschnittstelle 2 mit einer Transformationseinheit 3 verbunden ist. Die Transformationseinheit 3 umfasst einen Speicher 4 für den geheimen Schlüssel, beispielsweise einen für asymmetrische
- 15 Verschlüsselungsverfahren erzeugten privaten Schlüssel, sowie einen Prozessor 5 zur Transformation des Datensatzes.

- Sowohl die Abfrageeinheit 1 als auch die Transformationseinheit 3 umfassen jeweils mehrere optische Sender, die beispielsweise mehrere Bildpunkte eines Displays 6 sind, sowie mehrere optische Empfänger, die beispielsweise mehrere
- 20 Bildpunkte eines beispielsweise auf einer Platine 7 angebrachten Bildsensors 8 sind. Das Display 6 und der Bildsensor 8 der Abfrageeinheit 1 liegen dabei dem Display 6 und dem Bildsensor 8 der Transformationseinheit 3 mit Abstand gegenüber. Darüber hinaus ist auf den Bildsensoren 8 je eine zentralprojizierende Optik 9 angeordnet. Die sich zwischen den Displays 6 und den Bildsensoren 8
- 25 bzw. Optiken 9 bildenden Strahlengänge der Bildprojektion werden in der dargestellten Zeichnung durch strichpunktierte Linien schematisch angedeutet.

Die Abfrageeinheit 1 und die Transformationseinheit 3 können in einem gemeinsamen Gehäuse 10 untergebracht sein, wobei der Zwischenraum

zwischen den Displays 6 und den gegenüberliegenden Bildsensoren 7 mit einer optisch durchlässigen Vergussmasse 11 versehen sein kann.

- Zur Transformation eines Datensatzes mit einem geheimen Schlüssel wird ein Datensatz von der Abfrageeinheit 1 an die Transformationseinheit 3 übertragen, sodass der Datensatz anhand eines in der Transformationseinheit 3 hinterlegten Schlüssels transformiert, also beispielsweise signiert wird und der transformierte Datensatz an die Abfrageeinheit 1 zurückgegeben werden kann. Die Abfrageeinheit 1 kann den transformierten Datensatz über eine Netzwerkschnittstelle 12 beispielsweise an eine Blockchain weiterleiten.
- 10 Bei der Übertragung des untransformierten Datensatzes von der Abfrageeinheit 1 wird der Datensatz von der Abfrageeinheit 1 in zweidimensionale Codewörter übersetzt und deren Codeelemente werden optisch und parallel an die Transformationseinheit 3 übertragen, dort rückübersetzt und mithilfe des Prozessors 5 transformiert. Der transformierte Datensatz wird wiederum von der
- 15 Transformationseinheit 3 ebenfalls in zweidimensionale Codewörter übersetzt und deren Codeelemente werden optisch und parallel an die Abfrageeinheit 1 übertragen. Beispielsweise kann vorgesehen sein, dass die zweidimensionalen Codewörter Matrix-Codes, insbesondere Quick-Response-Codes bilden, die auf den Displays 6 abgebildet und von den jeweils gegenüberliegenden Bildsensoren
- 20 8 empfangen werden. Dabei können die Codeelemente die, im Falle des Quick-Response-Codes quadratischen, üblicherweise entweder schwarzen oder weißen Symbolzellen der Codematrix sein. Zur Verbesserung der Übertragungssicherheit können jedem Codeelement wie beispielsweise jeder Symbolzelle mehrere optische Sender und / oder mehrere optische Empfänger für eine parallele
- 25 Übertragung des Codeelements über mehrere Sender und / oder Empfänger zugewiesen werden, sodass die Übertragungssicherheit weiter erhöht wird.