

Tarnkappe.info > Artikel > Interviews > Theo Tenzer im Interview zum Thema Verschlüsselung





Theo Tenzer

# Theo Tenzer im Interview zum Thema Verschlüsselung

3.4.24 12:24 von Lars Sobiraj Lesezeit: 21 Min.

Unser Gesprächspartner Theo Tenzer betreibt Erwachsenenbildung. Er ist Journalist und Autor mehrerer Bücher zum Thema Kryptographie.

## INHALT

Quanten-Computer überholten längst die Super-Computer

Neue Algorithmen sollen unsere Privatsphäre schützen

Wie können wir sicher kommunizieren?

Theo Tenzer: Alle wollen Hintertüren zu den Daten besitzen

Systematische Überwachung & einfachere Strafverfolgung

Theo Tenzer: Rolle der Steganographie nimmt zu

Verschlüsselungstechniken stehen vor großen Herausforderungen

Theo Tenzer: Quantencomputer als ernsthafte Bedrohung

Multi-Verschlüsselung als vielversprechender Ansatz

Smoke Crypto beinhaltet McEliece-Algorithmus gleich mehrfach

Theo Tenzer über kryptographische Innovationen

Open Source als Treiber

Interoperabilität: Versand von Nachrichten über verschiedene Messenger

Aufklärung bitte nicht nur am Global Encryption Day

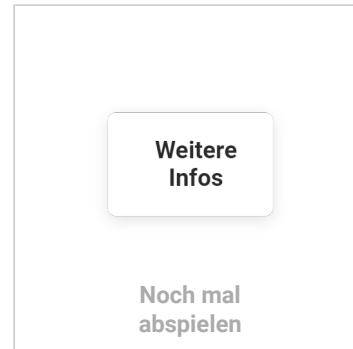
Theo Tenzer: Datenschutz und Kryptographie können sich gegenseitig unterstützen

Jeder trägt die Verantwortung, seine Privatsphäre zu sichern

**Lars Sobiraj: Hallo Theo Tenzer! Schön, dass es mit dem Interview geklappt hat. Der kryptographische Wandel ist ja ein Thema von zunehmender Bedeutung in unserem heutigen digitalen Alltag. Dazu braucht es gar keinen Vorfall an entschlüsselten Informationen aus Politik oder dem Militär. Kürzlich ging der Taurus-Leak durch die Medien. Dabei haben Offiziere der Bundeswehr in einer Videokonferenz teils unverschlüsselt über den Einsatz des Marschflugkörpers Taurus in der Ukraine diskutiert. Du hast Dich als Publizist eingehend mit dem kryptographischen Wandel beschäftigt. Was wandelt sich denn da?**

**Theo Tenzer:** Ja, vielen Dank Dir und Euch in der Redaktion, für die Anfrage und Möglichkeit zu diesem Interview. Ich gebe euch gerne Auskunft zu meiner Einschätzung.

- Anzeige -



## Quanten-Computer überholten längst die Super-Computer

Mein Interesse am Thema Kryptographie entstand eher beiläufig im Zusammenhang mit den verschlüsselnden Messengern und ich begann, dazu zu recherchieren. Meine Aufmerksamkeit hat sich aber vor ein paar Jahren intensiviert, als die Aussicht aufkam, dass Quanten-Computer möglicherweise leistungsfähiger werden könnten als die bisherigen hochleistungsfähigen Super-Computer.

Und es wurde im diesem Zusammenhang dabei öffentlicher und vertiefter betrachtet, dass damit auch der weit verbreitete Algorithmus RSA und ein weiterer möglicherweise gebrochen werden kann.

Das fand ich ganz spannend, weil es eine technologische Revolution ist. So, als wenn Bücher nicht mehr abgeschrieben werden müssen, sondern stattdessen in Serie gedruckt werden können. Und es erzeugte in mir – wie ggf. bei jedem – eine Neugier, was denn nun daran ist. So fingen meine Recherchen an.

Seit 2016 hat die amerikanische Normungsbehörde **NIST** ja auch schon von RSA inzwischen mehr Abstand genommen als früher, um es mal so auszudrücken. Man ist dabei, einige Algorithmen nach vorne zu bringen und zu standardisieren, die gegen die Quanten-Computer sicherer zu sein scheinen.

## Neue Algorithmen sollen unsere Privatsphäre schützen

Das war eine persönliche Einstiegsmotivation in das Thema der **Verschlüsselung**, und so wird auch jede Leserin und jeder Leser dieses Interviews insgesamt für sich ebenso feststellen können, dass die Entwicklung der Informationstechnologie der letzten Jahre inhaltlich zu einer Vielzahl neuer Verschlüsselungsmethoden und -techniken geführt hat, die unsere Kommunikation und unsere Daten, unsere Sicherheit und Privatsphäre schützen sollen.



Denn auch Bürgerinnen und Bürger wollen bei zunehmender Kommunikation über das Internet ihre Daten geschützt und verschlüsselt wissen. Nicht erst seit der sogenannten „Handy-Generation“, also denjenigen Jahrgängen, die mit dem Smartphone aufgewachsen, hat sich die Kryptographie zu einem entscheidenden Thema der digitalen Online-Welt entwickelt:

Die steigende Bedrohung durch Cyberkriminalität, aber auch staatliche Überwachung hat das Bewusstsein für die Notwendigkeit von Verschlüsselung bei allen Bürgerinnen und Bürgern erhöht. Entsprechende Vereine, soziale Gruppen und Datenschützer weisen immer wieder darauf hin. Es sollte Verschlüsselung als Standard gesetzt sein, was man im Englischen als „*Security by Default*“ bzw. „*by Design*“ bezeichnet.

Unternehmen und Privatpersonen suchen somit nach sicheren Lösungen, um ihre Kommunikation und ihre Daten vor unbefugtem Zugriff zu schützen.

Der kryptographische Wandel betrifft daher nicht nur IT- und Sicherheits-Expertinnen und - Experten, die direkt mit der Materie beschäftigt sind, sondern die gesamte Gesellschaft. Wir alle, die digitale Geräte und das Internet nutzen, sind von den neuen Anforderungen und Auswirkungen des kryptographischen Wandels betroffen. Es ist daher wichtig, dass wir uns über die aktuellen Entwicklungen informieren und verstehen, wie wir unsere Privatsphäre besser schützen können – das kann man nicht nur den Fachexpertinnen und Fachexperten überlassen.

## Wie können wir sicher kommunizieren?

**Lars Sobiraj aka Ghandy:** Die Offiziere der Bundeswehr sind nach dem Lapsus, bei einer Verbindung nicht auf die Verschlüsselung geachtet zu haben, sicherlich auch gebrandmarkt. Das Bewusstsein für notwendige Verschlüsselung wird noch eine Weile anhalten. Wie können wir als Bürgerinnen und Bürger denn sicherstellen, dass unsere Kommunikation geschützt ist? Welche Bedeutung hat die Ende-zu-Ende-Verschlüsselung in modernen Chat-Messengern?

**Theo Tenzer:** Eine der wichtigsten Entwicklungen im kryptographischen Wandel ist die verstärkte Anwendung von Ende-zu-Ende-Verschlüsselung in Chat-Messengern. Große Tech-Unternehmen bieten kostenfreie Messenger-Dienste an, die eine sichere Kommunikation zwischen den Nutzerinnen und Nutzern ermöglichen sollen. Diese Ende-zu-Ende-Verschlüsselung garantiert, dass nur jeweilige Absendende und Empfangende einer Nachricht diese lesen können – und niemand sonst!

Allerdings gibt es auch Bedenken hinsichtlich möglicher Hintertüren in den Verschlüsselungssystemen, die es staatlichen Akteuren ermöglichen könnten, die Kommunikation von Millionen von Nutzerinnen und Nutzern zu überwachen – oder zumindest durch die anbietenden Gatekeeper-Dienste Zugang dazu zu erhalten. Als reguläres Monitoring oder nur im Bedarfsfall sei mal dahingestellt.



# Theo Tenzer: Alle wollen Hintertüren zu den Daten besitzen

- Die Otto-Normal-Verbraucherinnen und -Verbraucher sind erstmal froh, dass ihnen Ende-zu-Ende-Verschlüsselung angeboten wird. Auf diesen Markt-Standard kann heute kein Anbieter mehr verzichten.

Kritische Verbraucherinnen und Verbraucher zweifeln sicherlich, ob die Dienste wirklich auch selbst nicht in die Kommunikation reinschauen können.

- Und expertierte Nutzerinnen und Nutzer werden sicherlich darauf hinweisen, dass es wichtig ist, dass die Verschlüsselungstechnologien in den Applikationen und Servern quell-offen und damit transparent sein sollen, damit unabhängige Expertinnen und Experten für Sicherheit sie überprüfen können.
- Und die ggf. paranoiden Nutzerinnen und Nutzer fragen sich, warum der ganze Chat für Millionen von Menschen kostenfrei angeboten wird. Denn auch Chat-Daten sind ja ein wesentlich begehrtes Objekt der Kontrolle für Sicherheitsmaßnahmen.
- Sicherheits-Nerds fordern ggf., dass die Kommunikation nicht über die oft US-amerikanischen Gatekeeper-Server läuft, sondern über souveräne, eigene und quelloffene Chat-Server.

Dass die „Gatekeeper“ – welch ein Begriff – gerade deshalb als solche klassifiziert wurden, und sich für den Austausch mit anderen großen Anbieter auch mit der Verschlüsselung interoperabel zeigen, kann ein Hinweis darauf sein, dass man ggf. mit weniger Hürden und weniger Schnittstellen auch technische Überwachungen der Kommunikation durchführen will. Sei es direkt auf den Endgeräten der Nutzerinnen und Nutzer oder auch zentral auf den Servern eines

Gatekeepers. Das ist der Fall immer dann, wenn ein vorhandener Schlüssel an zentraler Stelle doch die Verschlüsselung aufbrechen können sollte.

Alternativen sind wie bei jeder Wahl also gut. Und, sie sollten auch aus einer anderen „Bubble“ oder einem anderen „Fahrwasser“ kommen als die Gatekeeper. Quelloffene und kleinere Serveranbieter von verschlüsselten Messengern versuchen sich ja bewusst von den Gatekeepern zu differenzieren mit ihren Sicherheitsmerkmalen. Interoperable Gatekeeper werden sicherlich bald keinen Unterschied mehr in der Ende-zu-Ende-Verschlüsselung machen. „Unite the Cows“ – war schon vor vielem Jahren eine bekannte Internetplattform, deren Namen auf das Bild einer großen „Schafssherde“ vor den „Toren der Kommunikation“ – also den Gatekeepern – bildlich passen könnte?

## Systematische Überwachung & einfachere Strafverfolgung

**Tarnkappe.info:** Die Interoperabilität wurde ja politisch erzwungen. Wie beeinflusst die politische Diskussion den kryptographischen Wandel und welche Auswirkungen hat sie auf die Privatsphäre?

**Theo Tenzer:** Richtig, ein weiterer wichtiger Aspekt des kryptographischen Wandels ist natürlich die politische Diskussion um die Regulierung von Verschlüsselungstechnologien und die zunehmende Überwachung der Bevölkerung. Es ist kein technisches Thema allein. Forderungen nach Vorratsdatenspeicherung und einer Einschränkung von Verschlüsselung stehen im Konflikt mit dem Schutz der Privatsphäre.



Einige argumentieren, dass Verschlüsselung ein Hindernis für die Strafverfolgung darstelle und dass Zugang zu den verschlüsselten Nachrichten benötigt werde, um Verbrechen zu bekämpfen. Es gibt daher Bestrebungen, Verschlüsselung einzuschränken und Chat-Kontrollen auf allen internetfähigen Geräten einzuführen.

Auf der anderen Seite stehen Datenschützerinnen und Datenschützer sowie Bürgerrechtsaktivistinnen und -aktivisten, die die Privatsphäre der Menschen schützen wollen. Sie warnen vor einer totalen Überwachung und fordern eine umfassende Debatte über die Auswirkungen der Überwachung und eines Verzichts von Verschlüsselung auf die Gesellschaft.

Eine umfassende gesellschaftliche Diskussion über staatliche Überwachung und das Recht auf Verschlüsselung und Wahrung des Briefgeheimnisses im digitalen Raum ist daher notwendig, um

die Auswirkungen auf die Bürgerinnen und Bürger und unsere Gesellschaft insgesamt zu beleuchten.

## Theo Tenzer: Rolle der Steganographie nimmt zu

**Lars Sobiraj aka Ghandy:** Wie kann die **computergestützte Steganographie**, also das **Verstecken einer geheimen Botschaft, in der modernen kryptographischen Landschaft eingesetzt werden?** Welche Vorteile bietet sie gegenüber herkömmlichen **Verschlüsselungsmethoden?**

**Theo Tenzer:** Eine tatsächlich weitere interessante Entwicklung im kryptographischen Wandel ist die Wiederbelebung der Steganographie. Bei der Steganographie handelt es sich um eine Methode zur verdeckten Kommunikation, bei der Informationen in anderen Daten versteckt werden. Es ist also eine Methode, Informationen so zu übermitteln, dass sie nicht sofort auffällig sind und somit „unter dem Radar“ bleiben.

Die Steganographie kann eine wichtige Rolle bei der Sicherung der Kommunikation spielen, insbesondere wenn Verschlüsselungstechnologien durch staatliche Überwachungsmaßnahmen beeinträchtigt werden.

Es ist zumindest in den theoretischen Ansätzen eine Renaissance der Steganographie zu verzeichnen, wenn es z.B. um „Deniable Cipher-Text“ oder „verleugnungsfähige Einmal-Signaturen“ oder „abstreitbare Datei-Speicherungen“ geht.

Einige wissen vielleicht, dass vor vielen Jahren schon Julian Assange zusammen mit Suelette Dreyfus und Ralf Weinmann an einem Datei-System gearbeitet hat, dass man abstreiten kann,

selbst wenn man gefoltert würde. Ein zweites, alternatives Passwort sollte dann in eine weitere Daten-Umgebung führen – quasi als doppelten Boden, wie es bei der Software VeraCrypt oder Offsystem heute möglich ist. Es sind interessante Ansätze, die aktuell wieder stärker aufgegriffen werden und – voraussichtlich – werden würden angesichts einer Reduzierung oder gar eines Verbots von Cipher-Text in den Datennetzen.

-----BEGIN PGP MESSAGE-----  
Version: GnuPG v1.4.12 (GNU/Linux)

```
hQIMA1tQ1At53r41AQ//eKt3jrQ2KqHfp+k4f8YpZWsDLDLX40SEo1L6j0cb7+op  
wM5OzHMZO17dG2uNXi6rW24PpX1VvyokI6lzzkiWprbNZblv+i1x13OX21yOR3jl  
f16UtR2iHpGumwBILVExAxBRFp177+ykfnrd1WTIX/qFQcFbjrdlobBIARqtxqXyr  
MNTJ1s6hDmnnLD5D8hLyA/e7U9HAcXDJ1YQsrbs5hcnu4FhZtfKm8uiSyPTfqSwY  
A9W1PQ+pjZVRJPW9XB5dyh73hs+eOSfQ7G1bUXErKX+ygGIU8NvA12cTtZAKjL6R  
d11MYEAXYIj782mDunvGEi1+pyEDCXbqpnAydcxEOmPHrEA6ddfrir75x292N27W  
fx7aQBRaCfb0SPO3xbvuLqjnd493JkrUvhUy+k4IEAPCaIVbyPLFPOcNmYmA6Cbs  
qWTvoy428gl/dvOh29BOKR06Tj9J22VwotydzHmW2e1N81fQgMT4BhcUIsxnGYw  
HuZTkDksmRoAtioxYQt2HJuvNL3edHcGGcs4Gy2JKVUAWfa0SyUhmSTD6Cc+lq82Z  
AeBbLzo3v3kQWYxyGTPerLVE/TWk9BAjZ/ErlyYbb/JXe7i1u9SQ4ZUJwEYE7vKD  
FzAFji71cd0Q/zRlqyHGyUiOD692tBKzOZfEYQqB2fxn9GIMa7YoxTdxCRI7RzvS  
wFMBfMA/WMGOT3lwPPfBocfQJY JPGPUFAq6SceMLPNJ0vsLDtDXoetzR1/P3e/d  
EmQCrgsrEAmREeiupAeylIWFSmAfju+/ddAhGCzJd8qUR6BN0A+6Uicf9oq4NEFp  
a3YEd8zJ12921ulzuFZpVdo0LDvuY2KTfUj+1gOEjn6H7GznLsXsafg0jCPG12v5  
iFGuzJ9HWj9W5Wb81gUUFBQzleYDFLlb8WiHjfZWjMx/FayfoNfx/AaEXm9XjGQ  
ql4TEel+ip9JRxFOS5McR7/crTm8pDZYzGohwmZxtTwww7d4+PWJ8J8ceWqI4ZMW  
1hsk6Cugn+kKCDBe+WqtINQwFLYJte5Xv1KWTJeO7K6V8+xDRg==  
=fxMY
```

-----END PGP MESSAGE-----

Grafik Elsamuko, thx! (CC BY-SA 2.0)

# Verschlüsselungstechniken stehen vor großen Herausforderungen

**Lars Sobiraj aka Ghandy:** Du hast es ebenso schon kurz angesprochen: Wie beeinflusst der Durchbruch der Quanten-Computer den kryptographischen Wandel und welche neuen Verschlüsselungsmethoden sind entstanden? Sind die Quanten-Computer das neue Macht-Instrument der forschenden Spezialisten?

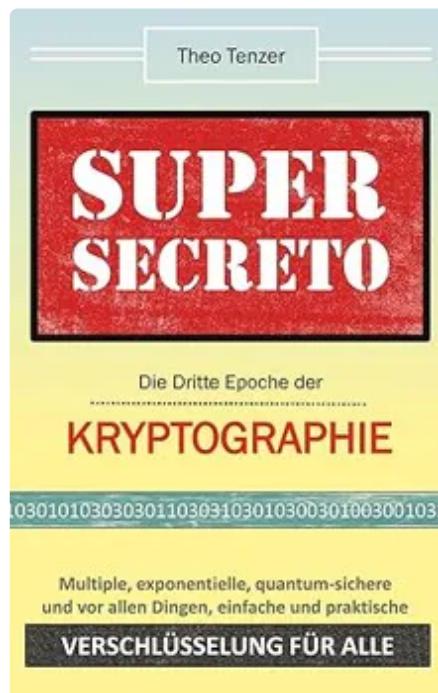
**Theo Tenzer:** Ein wichtiger Meilenstein im kryptographischen Wandel ist oder war natürlich der Durchbruch der Quanten-Computer. Sie sind jetzt da. Diese neue Art von Computern stellt herkömmliche Verschlüsselungstechniken vor große Herausforderungen, da sie in der Lage sind, Primzahlen schnell zu knacken. Verschlüsselung beruht auf einer Zerlegung bzw. Faktorisierung von Primzahlen. Entwicklerinnen und Entwickler können sich mit einem Abo auf entsprechende Plattformen buchen.

Schon im Jahr 2019 verkündete Google den Durchbruch der „Quantum Supremacy“, bei dem ein Quanten-Computer schneller als ein herkömmlicher Super-Computer rechnete. Dieser Meilenstein verändert nicht nur das Forschungsfeld, sondern führt auch dazu, dass Regierungen verstärkt in die Erforschung von Quanten-Computern investieren. Es ist absehbar, dass einige bisherige Verschlüsselungsmethoden aufgrund der steigenden Rechenkapazität von Quanten-Computern in Zukunft nicht mehr sicher sein könnten.

## Theo Tenzer: Quantencomputer als ernsthafte Bedrohung

Diese neuen Computer haben eine enorme Rechenleistung und könnten herkömmliche Verschlüsselungsmethoden schnell und einfach knacken. Dies stellt eine ernsthafte Bedrohung für

die Sicherheit unserer Daten und Kommunikation dar.



Es ist wichtig, dass wir uns weiterhin mit den Auswirkungen von Quanten-Computern auf die Kryptographie auseinandersetzen und alternative Verschlüsselungsmethoden entwickeln: Ein vielversprechender Ansatz ist der [McEliece-Algorithmus](#), der als sicher gegenüber Quanten-Computern gilt. Er ist im quell-offenen Crypto Messenger Smoke bei F-Droid.org [verbaut](#). Aber auch Crystals Kyber ist als neuer Algorithmus inzwischen standardisiert.

Die NIST hatte ja bereits 2016 mitgeteilt, das RSA und elliptische Kurven zukünftig nicht mehr als sicher gelten können. Drei Jahre später ging Google dann an die Öffentlichkeit, dass die Quanten die Nase vorn haben. Und das ist auch schon wieder fünf Jahre her.

Der McEliece Algorithmus wird derzeit standardisiert und erste deutsche Mail-Anbieter kümmern sich sogar um die Sicherheit der verschlüsselten Kommunikation vor den Quanten-Computern. Das ist eine rasante Entwicklung.

Die weitere Implementierung dieser Algorithmen in Verschlüsselungs-Tools und Messengern könnte also eine Lösung für die Sicherheitsprobleme darstellen, die durch Quanten-Computer entstanden sind.

## Multi-Verschlüsselung als vielversprechender Ansatz

**Lars Sobiraj aka Ghandy:** Neben der Quantum-Computing-sicheren Verschlüsselung gibt es ja auch noch die Mehrfach- oder Multiverschlüsselung. Wie funktioniert die Multi-Verschlüsselung und welche Vorteile bietet sie gegenüber herkömmlichen Verschlüsselungsmethoden?

**Theo Tenzer:** Ja, ein weiterer, vielversprechender Ansatz im kryptographischen Wandel ist die Multi-Verschlüsselung.

Dabei wird ein verschlüsselter Text mit einem weiteren Algorithmus oder durch einen verschlüsselten Kanal gesendet. Dies erhöht die Sicherheit der Verschlüsselung und erschwert es Angreifenden, den verschlüsselten Text zu entschlüsseln.

Die Applikation und Verschlüsselungs-Suite Spot-On gilt quasi seit mehr als ein Jahrzehnt als Innovator in der Multiverschlüsselung. Auch, wenn sie gar nicht so bekannt ist wie z.B. VeraCrypt, gehört sie zu den umfassend ausgearbeiteten Werkzeugen. Sie kann vieles verbinden: verschiedene Algorithmen, AES und RSA oder auch NTRU und McEliece oder symmetrische mit

asymmetrischen Verschlüsselungsverfahren. Und halt eben auch die erneute Verschlüsselung von bereits bestehendem Cipher-Text mit einem AES bevor der neue Cipher-Text nochmal durch einen mit temporären Schlüsseln erstellten Kanal gesendet wird. Temporäre Schlüssel werden mit Langzeitschlüsseln gemischt oder auch mit ganz vielen Schlüsseln. Den Schlüssel aus dem Fiasco Forwarding (statt nur eines Schlüssels (wie bei OTR oder Double Ratchet) wird hier gleich ein ganzes Dutzend an Schlüsseln gesandt, um Analysen und Attacken zu erschweren).

Wie haben die alten Schneiderlein immer gesagt: Doppelt genäht hält halt besser. Die Forschung bemüht sich, mit ihren theoretischen Annahmen dazu nachzukommen. Ob Quanten-Computer solche Dreifach- bzw. Mehrfach-Verschachtelungen auflösen können, bleibt ein interessantes Zukunftsfeld.

Die Multiverschlüsselung ist also noch ein relativ unerforschtes Konzept. Sie wird bisher nur von wenigen Unternehmen, Applikationen und Entwicklerinnen und Entwicklern eingesetzt. Es ist jedoch zu erwarten, dass „Super-Encipherment“, wie „Multi-Verschlüsselung“ im Englischen auch genannt wird, in Zukunft eine wichtige Rolle bei der Sicherung unserer Kommunikation und Daten spielen wird.



**Smoke Crypto beinhaltet McEliece-Algorithmus gleich mehrfach**

## Lars Sobiraj: Wie kann der McEliece-Algorithmus in der Praxis angewendet werden und wie wird er derzeit standardisiert?

**Theo Tenzer:** Das McEliece-Messaging ist ein interessantes Beispiel für den kryptographischen Wandel. Es ist im [Smoke Crypto Chat Messenger](#) mit vier verschiedenen Moduli implementiert. Fach-Expertinnen und -Experten, die dazu theoretisch geforscht haben, und Modelle vorgelegt haben, finden ihr theoretisches Einstellungs-Modell dort als Pre-Set „ready-to-use“ implementiert. Denn dieser Messenger implementierte den McEliece-Algorithmus als einer der ersten und schuf somit eine innovative Anwendung im Bereich der sicheren Kommunikation.

Organisationen wie das National Institute of Standards and Technology (NIST) in den USA und das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland spielen eine wichtige Rolle bei der Festlegung von Verschlüsselungsstandards. Um den kryptographischen Wandel zu flankieren und zu unterstützen, ist es zentral, dass solche Verschlüsselungsstandards wie im Fall des McEliece-Messagings entwickelt und standardisiert werden. Derzeit erfolgt ja die NIST-Normung und damit Empfehlung dieses Algorithmus mit vielen öffentlichen Materialien dokumentiert auch unter der Webseite [mceliece.org](#). Welche Pre-Set-Einstellungen letztlich empfohlen werden und ob es einer der vier Moduli der Forschenden aus dem Praxismodell des Smoke-Messengers ist, wird man dann vergleichen können.

## Theo Tenzer über kryptographische Innovationen

### Tarnkappe.info: Was ist noch an weiteren kryptographischen Innovationen zu nennen?

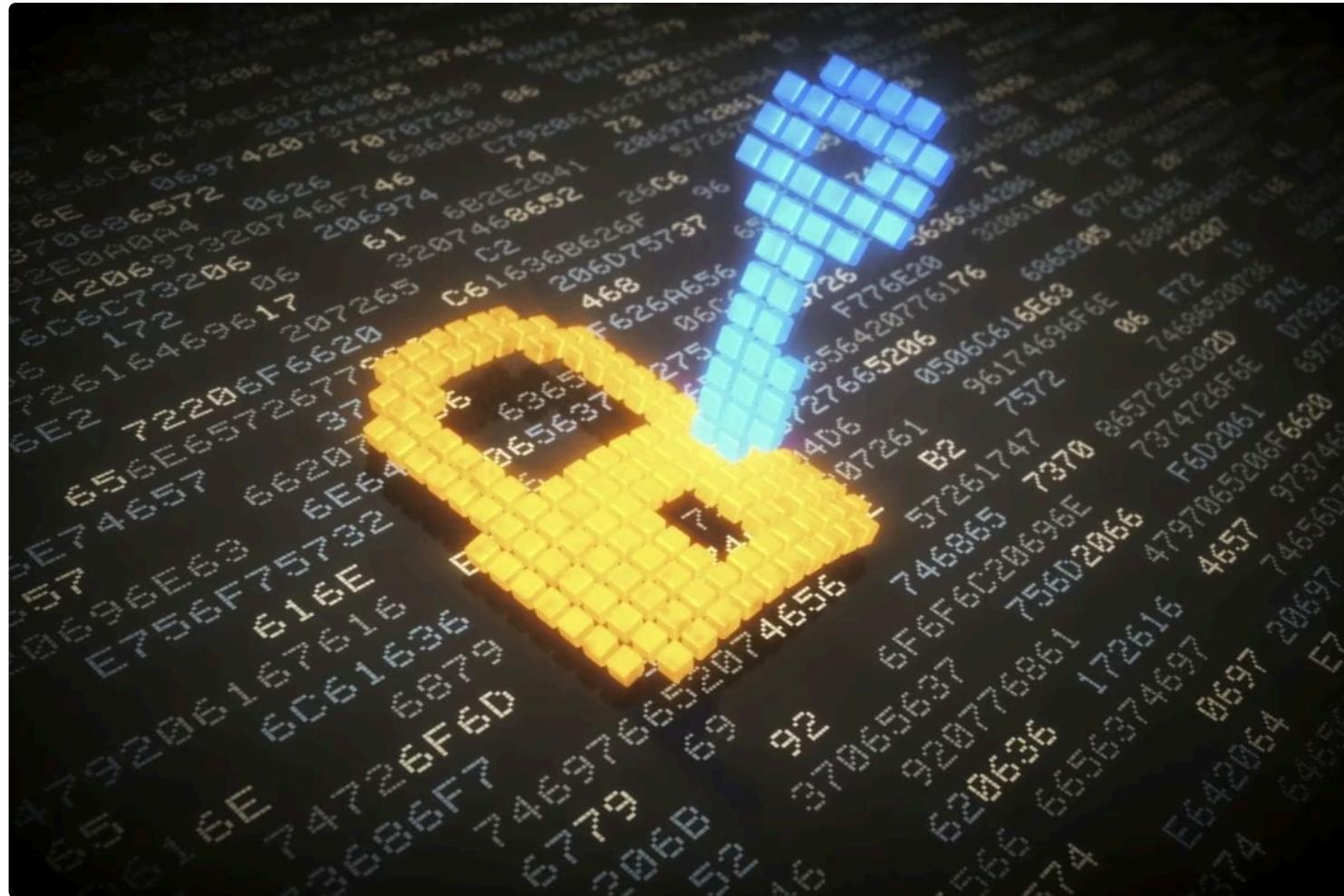
**Theo Tenzer:** Ein weiterer interessanter Aspekt des kryptographischen Wandels sind die transdisziplinären Forschungsfragen. Sie ergeben sich aus der Verbindung beispielsweise von

Graphentheorie, Chaos- und Komplexitätstheorie mit der Kryptographie. Das sogenannte „[Beyond Cryptographic Routing](#)“ bereichert herkömmliche Routing-Protokolle um kryptographische Komponenten (wie es bei dem Echo-Protokoll gegeben ist). Sie bietet eine neue Form der Datensicherheit in Kombination mit der spezifischen Weiterleitung im Netzwerk, die auch vor der Analyse von Metadaten schützen kann.

Ebenso ist die derivative Kryptographie zu nennen, die auf einen Austausch von Schlüsseln komplett verzichtet, in dem die Schlüssel auf beiden Seiten einfach abgeleitet werden. Das erhöht die Sicherheit enorm und verändert die kryptographischen Prozesse. Wenn Alice und Bob keine Schlüssel mehr tauschen (müssen), wie beispielsweise bei den Juggernaut Schlüsseln oder auch mit weiteren Schlüsselaustauschprotokollen, und wir das im Messenger konkret anwenden können, dann ist das schon sehr innovativ.

Im Zuge des kryptographischen Wandels entstehen somit auch zahlreiche neue Anwendungen und Protokolle. Es gibt eine Vielzahl von Open-Source-Verschlüsselungsprogrammen, die eine sichere Kommunikation ermöglichen. Einige bekannte Beispiele haben wir ja bereits benannt. Und auch der Messenger [Delta-Chat](#) setzt Verschlüsselung und bestehende POPTASTIC-E-Mail-Server sehr nativ ein. D.h. der Nutzer muss sich gar nicht mehr um viel kümmern, um einfach und sicher verschlüsselt kommunizieren zu können.

Das Steam-Protokoll ermöglicht ein Ende-zu-Ende verschlüsseltes Filesharing und damit auch ein „[Swarming](#)“, also das Downloaden von mehreren Quellen, obwohl eine Verschlüsselung vorliegt. Das bekannte Filesharing mit [RetroShare](#) kann dieses nur Punkt-zu-Punkt verschlüsselt. Steam geht mit dieser spezifischen Verschlüsselung noch einen Evolutions-Schritt weiter: Aus Peer-to-Peer-Sharing wurde Friend-to-Friend-Sharing. Und dieses nicht mit einer Punkt-zu-Punkt-Verschlüsselung, sondern einer interoperablen Ende-zu-Ende-Verschlüsselung.



## Open Source als Treiber

**Lars Sobiraj aka Ghandy:** Welche Rolle spielt Open Source bei der Verschlüsselung?

**Theo Tenzer:** Die Bedeutung von quell-offenen Werkzeugen zur Verschlüsselung ist ein weiterer wichtiger Aspekt des kryptographischen Wandels. Denn diese Werkzeuge stehen allen

Nutzerinnen und Nutzern frei zur Verfügung und ermöglichen eine sichere Kommunikation und Datenübertragung. Sie bieten eine Alternative zu proprietären Verschlüsselungstechnologien, bei denen die Funktionsweise nicht für unabhängige Sicherheitsprüfungen offen ist.

Open-Source-Verschlüsselungs-Tools bieten also auch die Möglichkeit, das Vertrauen der Nutzerinnen und Nutzer in die Sicherheit ihrer Kommunikation nachweislich wiederherzustellen. Indem sie ihre Programmierung und Funktionsweise öffentlich machen und unabhängige Sicherheitsaudits ermöglichen, stellen diese Entwicklerinnen, Entwickler und deren Projekte sicher, dass keine Hintertüren oder Schwachstellen vorhanden sind. Insbesondere im Messaging sollte Quelloffenheit ein Qualitätsmerkmal sein.

## Interoperabilität: Versand von Nachrichten über verschiedene Messenger

**Tarnkappe.info: Wie können wir die Interoperabilität von verschlüsselnden Chat-Klienten verbessern und welche Vorteile bietet dies für die Sicherheit unserer Kommunikation?**



**Theo Tenzer:** Die Evaluierung der Interoperabilität von verschlüsselnden Chat-Klienten sowie die Vernetzbarkeit von Chat-Servern ist ein ebenso aktueller Schwerpunkt im kryptographischen

Wandel. Es wird daran gearbeitet, sichere Kommunikation zwischen verschiedenen Anwendungen zu ermöglichen und die Nutzung von verschlüsselten Chat-Diensten zu erleichtern. Das bietet sicherlich noch mehr Annehmlichkeiten für Nutzerinnen und Nutzer. Auch wenn Kritikerinnen und Kritiker wittern, dass Verschlüsselungsstandards herabgesetzt werden sollen, um sie besser brechen zu können und Kommunikation einfacher, d.h. mit ggf. nur einer technischen Vorrichtung, besser abhören zu können.

**Lars Sobiraj aka Ghandy:** Warum ist Zusammenarbeit in der Kryptographie wichtig? Wie können die Akteurinnen und Akteure die Öffentlichkeit über die Bedeutung von Verschlüsselung informieren?

**Theo Tenzer:** Im Zuge der kryptographischen Veränderungen der letzten Jahre hat sich eine „Global Encryption Coalition“ gebildet. Sie besteht aus führenden Instituten, Organisationen, Open-Source-Projekten, Einzelpersonen und Unternehmen mit Verschlüsselungslösungen. Diese Koalition hat das Ziel, Nutzerinnen und Nutzer, Politik und die breite Öffentlichkeit über Kryptographie und Verschlüsselung zu informieren. Zudem wollen sie ihre Arbeitsergebnisse und Forschungsfragen einer größeren Öffentlichkeit zugänglich machen.

**Aufklärung bitte nicht nur am Global Encryption Day**



Und: Der jährliche „Global Encryption Day“ ist dabei immer zum dritten Oktober-Wochenende ein wichtiger Termin im Kalender der kryptographisch Tätigen und der Medien. Interessierte können mitmachen. An diesem Tag bzw. Wochenende bieten zahlreiche Organisationen, Institute und Vereine in Kooperation mit der „Global Encryption Coalition“ weltweit Veranstaltungen, Workshops, Informations- und „Lern-Nuggets“ sowie Kampagnen zum Thema Verschlüsselung an. Ziel ist es, die Bedeutung von Verschlüsselung in der Öffentlichkeit zu stärken. Wir wollen Werkzeuge erläutern und präsentieren und damit das Bewusstsein für Datenschutz und Privatsphäre zu schärfen.

**Lars Sobiraj aka Ghandy: Du hast gerade ein kleines Heft aus Deinem Band „Verschlüsselung für alle“ mit Beschreibungen zu verschiedenen und den wichtigsten quell-offenen Software-Applikationen ausgekoppelt. Es erschien im Band „Open-Source Verschlüsselung“ als Sonderausgabe. Herausgegeben gemeinsam mit dem Verein Aktion Freiheit statt Angst e.V., die darin auch ein Geleitwort veröffentlicht haben und Mitglied im Arbeitskreis Vorratsdatenspeicherung sind. Wie kam es zu der Kooperation?**

- Anzeige -

## Theo Tenzer: Datenschutz und Kryptographie können sich gegenseitig unterstützen

**Theo Tenzer:** Es liegt und lag nahe, dass sich Datenschutz und Kryptographie gegenseitig befreunden. Nur durch eine enge Zusammenarbeit und einen aktiven Themenauftausch aller Beteiligten können wir die Bedeutung von Kryptographie und Verschlüsselung in der Gesellschaft vermitteln und den Schutz der Privatsphäre gewährleisten. Digitale Computer-Chips begleiten und überwachen den Menschen immer mehr.

Insgesamt ist der kryptographische Wandel ein komplexes und vielschichtiges Thema. Dieser hat große Auswirkungen auf die Sicherheit und Privatsphäre in der digitalen Welt. Es erfordert eine umfassende Auseinandersetzung mit den aktuellen Entwicklungen. Dazu kommt eine kontinuierliche Anpassung der Verschlüsselungstechnologien, um den neuen Herausforderungen gerecht zu werden.

Es war daher sinnvoll, die Applikationen, die quelloffen verschlüsseln, einmal alle zu listen und in einem Überblicksband kurz zu beschreiben. (ISBN 9783757853150).

Das haben wir mit dem Verein aktualisiert und über 30 Werkzeuge zur Verschlüsselung einmal in einem kleinen Band beschrieben. Darüber hinaus gibt es neben der Software und zahlreicher Fach- und Sachbücher vieler Autorinnen und Autoren natürlich auch einige Online-Tutorials und Lernplattformen. Dazu kommen hochschulbezogene Lehrveranstaltungen und betriebliche wie schulische Ausbildungen im Informatikunterricht.

# Jeder trägt die Verantwortung, seine Privatsphäre zu sichern



Es liegt in unserer und jedem eigener Verantwortung, sich aktiv an dem Schutz der Privatsphäre zu beteiligen. Und natürlich auch, die mit Verschlüsselung bestehenden Risiken zu besprechen. Das wird immer der Zwiespalt in der Abwägung bei Verschlüsselung bleiben.

Denn Verschlüsselung ist eine mathematische Option, die immer für alle besteht. Wie weit wollte man den Schutz der Freiheit und ein Menschenrecht auf Verschlüsselung sowie Privatheit und Briefgeheimnis in der digitalen Welt für wie viel Erfolg von Ermittlungsoptionen bei wenigen Fällen in der Verbrechensbekämpfung opfern? Denn: „Ein bisschen verschlüsselt“ gibt es nicht. Entweder es ist „zu“ oder „auf“ – wenn die Verschlüsselung sicher ist und sein soll! Auch das ist Chance und Risiko zugleich, je nach Betrachtung.

**Lars Sobiraj aka Ghandy: Vielen Dank für die Auskünfte und Deine Einschätzungen, Theo.**