RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

WISSENSCHAFTSMAGAZIN

GEHEIMNIS

Auf Blei: Verflucht im Römischen Reich

In den Genen: Vererbte Krankheiten

Zwischen den Zeilen: Versteckte Botschaften

#35 Nr. 1 | 2025

Informatik

ONLINE WÄHLEN OHNE MULMIGES GEFÜHL

Wie lassen sich der Komfort einer Internetwahl und die Sicherheit einer Stimmabgabe auf Papier verbinden? Damit experimentieren IT-Sicherheitsprofis.

Wahlbenachrichtigung, Briefwahlunterlagen, Stimmzettel. Eine Bundestagswahl verschlingt tonnenweise Papier. So viel, dass im November 2024 in Deutschland gar Diskussionen entbrannten, wie schnell eine vorgezogene Bundestagswahl nach dem Ampel-Aus überhaupt organisierbar wäre. Diskussionen, die manche andere Länder in dieser Form nicht haben würden. In Estland beispielsweise kann man bereits seit 2005 seine Stimme digital abgeben. „Für eine Internetwahl braucht man großes Vertrauen in die technische Infrastruktur“, weiß Prof. Dr. Karola Marky. Sie leitet an der Ruhr-Universität Bochum das Digital Sovereignty Lab und ist Mitglied im Exzellenzcluster CASA, das sich der Cybersicherheit im Zeitalter großskaliger Angreifer widmet. Seit über zehn Jahren erforscht sie verschiedene Aspekte von Internetwahlen.

„Bei dem Thema gibt es einige spannende Konflikte“, führt die Forscherin aus. „Zum einen muss das Wahlrecht gewahrt werden. Es dürfen also nur Stimmen von wahlberechtigten Personen gezählt werden. Zum anderen muss man das Wahlgeheimnis sicherstellen: Niemand darf wissen, welche Partei ich gewählt habe.“ Beides gleichzeitig zu gewährleisten, liegt nicht in der Natur des Internets. „Es wurde nicht mit Privatsphäre konzipiert, sondern um Menschen zu verbinden. Die Anonymität wurde nachträglich dazu gebaut“, so Karola Marky. „Um eine Internetwahl sicher zu machen, muss man den ganzen Werkzeugkasten der Kryptografie und Privatsphäre-Technologie nutzen.“

Eine gut umgesetzte Internetwahl bietet einige Vorteile: Man kann beispielsweise von zuhause aus wählen, es braucht weniger Papier und weniger Wahlpersonal, und die Auszählung geht schneller. Ein Vorteil der Papierwahl hingegen liegt in der Archivierung. Stimmzettel, Protokolle und Begleitdokumente werden archiviert und können nachträglich nur schwer gefälscht werden. Das ermöglicht im Bedarfsfall auch eine Neuauszählung.

Lässt sich das Beste aus beiden Welten kombinieren? „Wir wollten wissen, ob man das Vertrauen in die Papierdokumentation in eine Internetwahl integrieren kann“, sagt Karola Marky. Die Bochumer Gruppe dachte sich daher ein Verfah- ▸

Rund 60 Millionen Wahlberechtigte gibt es in Deutschland. Etwa 47 Prozent von ihnen gaben bei der Bundestagswahl 2021 ihre Stimme per Briefwahl ab – das erzeugt viel zusätzlichen Aufwand.

„ICH BIN AKTUELL NICHT DAFÜR, BEI POLITISCHEN WAHLEN IN DEUTSCHLAND ONLINE ZU WÄHLEN.“

Karola Marky

Eine herkömmliche Wahl verschlingt tonnenweise Papier.

ren für eine hybride Stimmabgabe aus: Die wahlberechtigte Person füllt online von zuhause ihren Stimmzettel aus. Kommt sie an den Punkt der Stimmabgabe, wird sie zu einem Live-Video weitergeleitet. Hier kann sie beobachten, wie ein Drucker ihre gerade abgegebene Stimme ausdruckt. Natürlich nicht im Klartext. Was aus dem Drucker herauskommt, ist ein QR-Code, der eine Verschlüsselung der gewählten Partei enthält, sowie ein Zahlen-Code, der eine Art Tracking-ID darstellt, welche lediglich die wählende Person kennt.

„Wenn ich den Livestream beobachte, sehe ich also nur, dass eine Stimme abgegeben wurde, aber nicht für welche Partei oder wer gerade abgestimmt hat“, erklärt Karola Marky. Auf diese Weise könnte man den Livestream öffentlich zugänglich machen und maximale Transparenz ermöglichen, während zugleich das Wahlgeheimnis gewahrt wäre.

Verschiedene Verfahren im Vergleich

Vereinfacht gesagt würde wie folgt ausgezählt werden: Das Wahlpersonal würde den QR-Code von der Tracking-ID trennen. Die QR-Codes würden eingescannt und die Stimmen so gezählt, während die IDs separat gesammelt würden. So wäre sowohl die Information, wie viele Personen an der Wahl teilgenommen haben, als auch die Anzahl der Stimmen für die verschiedenen Parteien in Papierform archiviert.

In einer Studie baten die Bochumer Forschenden 150 Personen, an einer simulierten Internetwahl teilzunehmen. 50 von ihnen gaben ihre Stimme ab und sahen am Ende des Prozesses lediglich eine Bestätigungsseite, dass die Stimme gezählt wurde. Weitere 50 wurden in einen Livestream weitergeleitet und konnten den Ausdruck des QR-Codes ihrer Stimme verfolgen. Die letzten 50 sahen ebenfalls einen Livestream, allerdings mit einem 3D-Druck-Verfahren, welches dieselben Informationen wie der oben beschriebene QR-Code 3D-druckt. Anschließend bewerteten die Teilnehmenden beispielsweise, wie vertrauenswürdig, wie sicher und wie gut nutzbar sie den Prozess fanden.

Das System mit Live-Ausdruck des QR-Codes empfanden die Teilnehmenden als signifikant vertrauenswürdiger verglichen mit dem Standardsystem ohne Livestream. Als marginal leichter bedienbar bewerteten sie hingegen das Verfahren ohne Livestream. „Weil das den gewohnten Prozess widerspiegelt“, vermutet Karola Marky. „Grundsätzlich sehen wir in unseren Studien, dass sich um die 60 bis 80 Prozent der Teilnehmenden Internetwahlen wünschen, egal, wie genau das Programm für die Stimmabgabe aussieht. Weil wir das in Deutschland nicht haben, kennen unsere Versuchspersonen im Regelfall auch keine Alternativen.“

Karola Marky betont, dass es noch einige Herausforderungen für das von ihr und ihrem Team erdachte System zu bewältigen gibt: An welchem Ort würden die QR-Codes gedruckt? Was ist, wenn der Strom ausfällt? Wie werden Probleme berichtet? „Dieses System ist noch viel zu unausgereift, und es wird vermutlich niemals genau so bei einer großen Wahl zum Einsatz kommen“, stellt die Informatikerin fest. „Uns ging es darum zu erforschen, ob sich unser Vertrauen in Papier in eine Internetwahl integrieren lässt und wie Menschen auf ein solches hybrides System reagieren würden.“

Ein weiterer wichtiger Schritt sei die Ende-zu-Ende-Verifizierbarkeit. „Wer seine Stimme abgibt, muss die Möglichkeit haben zu überprüfen, ob sie auch in der Server-Wahlurne mit dem richtigen Inhalt angekommen ist“, meint Karola Marky. In Estland beispielsweise ist das gewährleistet. Hier erhält man nach der Wahl einen QR-Code, den man mit einem zweiten Gerät, zum Beispiel einem Smartphone, scannen und so überprüfen kann, dass die Stimme der gewählten Partei entspricht. „Allerdings haben nur rund vier Prozent der Esten diese Möglichkeit in der Vergangenheit genutzt“, weiß Marky. „Das ist relativ wenig.“

Das Bochumer Team arbeitet daher an einer mathematischen Methode, mit der nicht nur Individuen, sondern auch Organisationen überprüfen könnten, ob verschlüsselte Stimmen auf den Wahlservern den richtigen Inhalt haben – ohne das Wahlgeheimnis zu verletzen. „Mit unserer Methode könnte jeder für mich überprüfen, ob ich wirklich Partei XY gewählt habe, ohne zu wissen, dass ich Partei XY gewählt habe – das ist die Magie der kryptografischen Methoden, die wir heute haben“, so Marky.

Ob irgendwelche dieser Verfahren eines Tages in Deutschland zum Einsatz kommen werden, weiß die Forscherin nicht. Ihrer Meinung nach braucht es zunächst mehr Bewusstsein in der Politik für die Bedeutung von Sicherheit bei der Software-Entwicklung. „Auch wenn ich dieses faszinierende Thema mit Begeisterung erforsche, bin ich aktuell nicht dafür, bei politischen Wahlen in Deutschland online zu wählen“, sagt Karola Marky.

Text: jwe, Fotos: tk

Standpunkt

WEG VOM GEHEIMNIS UM DIE **QUELLCODES**

Ob behördliche Software in Deutschland sicher ist oder nicht, ist aktuell Glückssache, meint Informatikerin Karola Marky. Sie fordert mehr Open-Source-Lösungen, damit auch die Guten auf Fehlersuche gehen können.

Wenn wir in Deutschland eines Tages online wählen können wollen, benötigen wir dafür eine Software, deren Quellcode frei verfügbar ist. In Deutschland empfinden Menschen solche Open-Source-Lösungen oft als unsicher. Sie haben Sorge, dass Angreifer in dem offenen Quellcode Sicherheitslücken finden und ausnutzen könnten. Das stimmt so nicht.

Denn auch viele IT-Sicherheits-Experten schauen sich solche Open-Source-Lösungen an, finden Sicherheitslücken, die dann geschlossen werden können. Wie gut das funktionieren kann, zeigt ein Beispiel aus der Schweiz. Dort wurde die Software für Internetwahlen 2019 wegen Software-Entwicklungsproblemen eingestampft. Die Schweizer kauften der Firma den Code ab, veröffentlichten ihn und starteten ein Bounty-Hunting-Programm: Wer Mängel in der Software fand, konnte mit hohen Geldbeträgen belohnt werden. Seit 2023 ist das E-Voting in der Schweiz nun an bestimmten Orten für bestimmte Personengruppen mit verbesserter Software wieder möglich.

Mancherorts ist ein Großteil der öffentlichen Systeme open source. Das sollte auch in Deutschland so sein. Dann könnten wir besser sicherstellen, dass Standards für die Software-Entwicklung eingehalten werden – und dass Software sowohl anwenderfreundlich als auch sicher ist. Aktuell sind die Ausschreibungsprozesse für neue Software bei uns ein Glücksspiel. Leider kommt häufig unsichere Software dabei heraus. Das Problem ist, dass die IT-Sicherheit in den Köpfen vieler Entscheidungsträger nicht den Stellenwert hat, die sie haben müsste, oder dass Vertrauen in die Software von außen auferlegt wird. Oft sagen Politiker Sätze wie „Solche Systeme wurden noch nie angegriffen“ oder „Wir machen vertrauenswürdige Systeme“. Beweise dafür sind ohne den Code und genügend Transparenz aber nicht gegeben.

Wir haben in Deutschland eine große Expertise in der Software-Entwicklung. Es gibt kompetente Firmen, Organisationen wie den Chaos-Computer-Club und die Forschenden. Bislang versackt das Expertenwissen aber häufig in irgendwelchen Fachzeitschriften. Wenn wir eine sichere digitale Demokratie haben wollen, müssen wir alle Hand in Hand arbeiten und die Expertinnen und Experten noch besser einbeziehen.

Text: Prof. Dr. Karola Marky, Foto: tk

Prof. Dr. Karola Marky leitet an der Ruhr-Universität Bochum das Digital Sovereignty Lab und ist Mitglied des Exzellenzclusters CASA.

REDAKTIONSSCHLUSS

Schon im 15. Jahrhundert dachten sich die Menschen trickreiche Lösungen aus, um Geheimnisse sicher weitergeben zu können, zum Beispiel die rechts abgebildete Chiffrierscheibe (mehr dazu ab Seite 26). Mit ihr konnte man einen Klartext in Kauderwelsch verwandeln, indem man die Buchstaben des Klartextes auf dem äußeren Ring durch die Buchstaben auf dem inneren Ring ersetzte. Der innere Ring war drehbar. Um einen verschlüsselten Text zu entschlüsseln, musste man wissen, wie der innere Ring auszurichten ist. Die Ausrichtung wurde von sogenannten Steuerungsbuchstaben bestimmt, also Buchstaben, die keine Entsprechung im Klartext hatten, sondern nur dazu bestimmt waren, die Ausrichtung des inneren Rings anzugeben. War dieser richtig gedreht, konnte man den Klartext auf dem äußeren Ring ablesen.

LUST ZU KNOBELN?

Dann inneren Ring der Scheibe ausschneiden und los geht's:

yuose&azmydbkofxczn&cdeuqmlitokhyds

Hinweise: Unser Beispiel ergibt einen Satz mit sechs Wörtern und beinhaltet acht Steuerungsbuchstaben. Steuerungsbuchstaben müssen auf das Z des äußeren Rings ausgerichtet werden. Der verschlüsselte Text in diesem Beispiel beginnt mit einem Steuerungsbuchstaben. Die anderen sieben Steuerungsbuchstaben sind zufällig im Text verteilt und können auch mitten im Wort auftreten. Immer wenn ein Zeichen aus unserem Kauderwelsch-Beispiel sich nicht in einen sinnvollen Buchstaben übersetzen lässt, handelt es sich um einen Steuerungsbuchstaben. Richten Sie dann den inneren Ring neu aus, indem Sie dieses Zeichen des inneren Rings auf das große Z des äußeren Rings drehen. Achtung: Da der Erfinder der Chiffrierscheibe Latein sprach, fehlt der Buchstabe U im äußeren Ring, der für unseren Lösungssatz erforderlich ist. Ein V im äußeren Ring kann sowohl ein U als auch ein V bedeuten. Viel Spaß!

Die Auflösung finden Sie unten links auf dieser Seite.

IMPRESSUM

HERAUSGEBER: Rektorat der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation der Ruhr-Universität Bochum (Hubert Hundt, v.i.S.d.P.)

WISSENSCHAFTLICHER BEIRAT: Prof. Dr. Birgit Apitzsch (Sozialwissenschaft), Prof. Dr. Thomas Bauer (Fakultät für Wirtschaftswissenschaft), Prof. Dr. Elena Enax-Krumova (Medizin), Prof. Dr. Constantin Goschler (Geschichtswissenschaften), Prof. Dr. Markus Kaltenborn (Jura), Prof. Dr. Achim von Keudell (Physik und Astronomie), Prof. Dr. Günther Meschke (Prorektor für Forschung und Transfer), Prof. Dr. Martin Muhler (Chemie), Prof. Dr. Franz Narberhaus (Biologie), Prof. Dr. Nils Pohl (Elektro- und Informationstechnik), Prof. Dr. Tatjana Scheffler (Philologie), Prof. Dr. Gregor Schöner (Informatik), Prof. Dr. Sabine Seehagen (Psychologie), Prof. Dr. Roland Span (Maschinenbau), Prof. Dr. Marc Wichern (Bau- und Umweltingenieurwissenschaft), Prof. Dr. Peter Wick (Evangelische Theologie)

REDAKTIONSANSCHRIFT: Dezernat Hochschulkommunikation, Redaktion Rubin, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, rubin@rub.de, news.rub.de/rubin

REDAKTION: Dr. Julia Weiler (jwe, Redaktionsleitung); Meike Drießen (md); Dr. Lisa Bischoff (lb); Raffaela Römer (rr)

FOTOGRAFIE: Damian Gorczany (dg), Schiefersburger Weg 105, 50739 Köln, Tel.: 0176/29706008, damiangorczany@yahoo.de, www.damiangorczany.de; Roberto Schirdewahn (rs), Offerkämpe 5, 48163 Münster, Tel.: 0172/4206216, post@people-fotograf.de, www.wasaufdieaugen.de; Tim Kramer (tk), Agentur für Markenkommunikation, Ruhr-Universität Bochum

COVER: RUB, Tim Kramer

BILDNACHWEISE INHALTSVERZEICHNIS: Teaserfoto für Seite 14: Roberto Schirdewahn; Seite 22, 62: RUB, Tim Kramer

GRAFIK, ILLUSTRATION, LAYOUT UND SATZ:
Agentur für Markenkommunikation, Ruhr-Universität Bochum, www.einrichtungen.rub.de/de/agentur-fuer-markenkommunikation. Die Illustrationen wurden mit Adobe Firefly erzeugt.

DRUCK: LD Medienhaus GmbH & Co. KG, Hansaring 118, 48268 Greven, info@ld-medienhaus.de, www.ld-medienhaus.de

ANZEIGEN: Dr. Julia Weiler, Dezernat Hochschulkommunikation, Redaktion Rubin, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, rubin@rub.de

AUFLAGE: 3.900

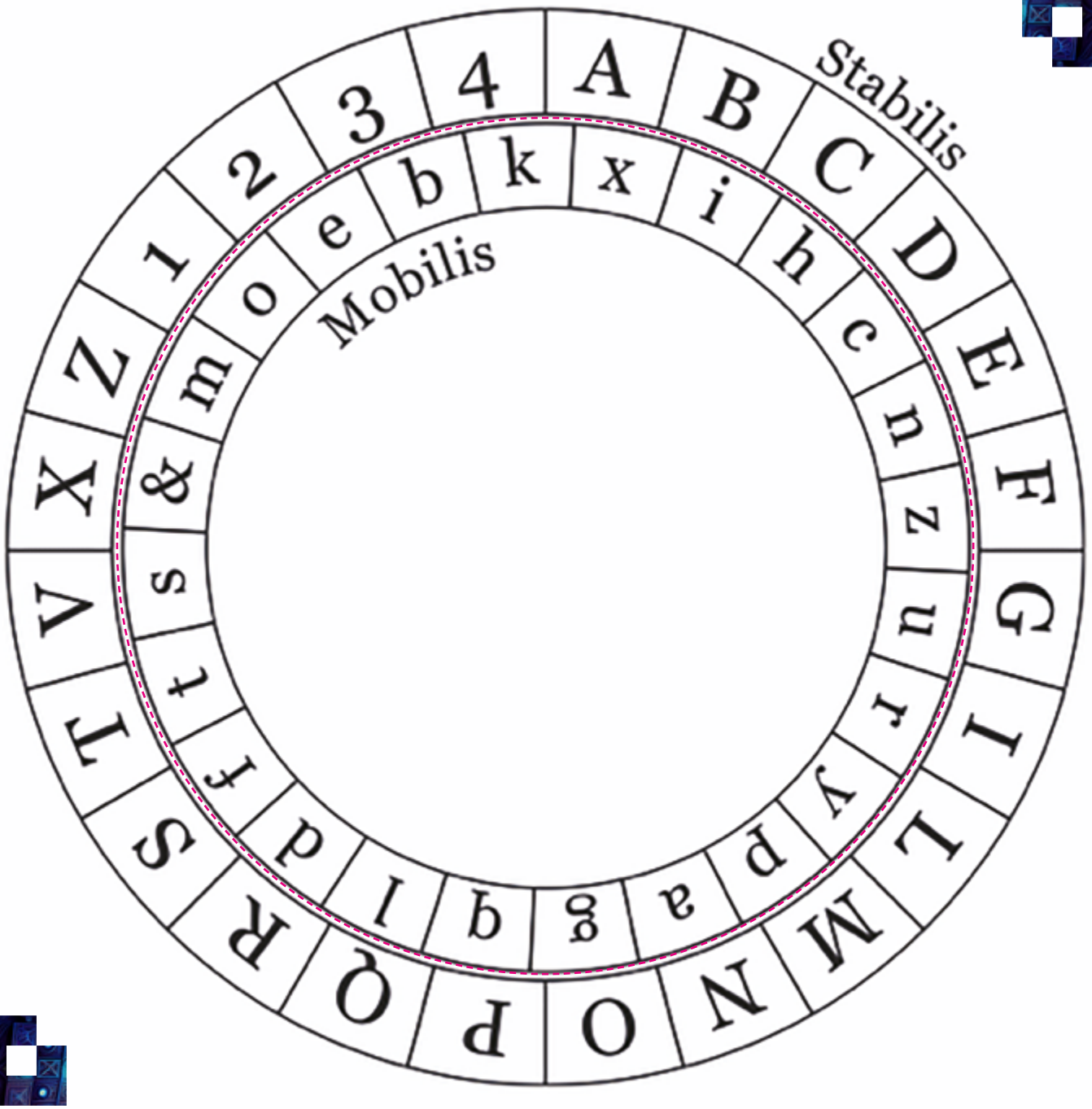
BEZUG: Rubin erscheint zweimal jährlich und ist erhältlich im Dezernat Hochschulkommunikation der Ruhr-Universität Bochum. Das Heft kann kostenlos abonniert werden unter news.rub.de/rubin/abo. Das Abonnement kann per E-Mail an rubin@rub.de gekündigt werden.

ISSN: 0942-6639

Die nächste Ausgabe von RUBIN erscheint am 1. Dezember 2025.

Lösungssatz: Viel Freude beim Lesen von Rubin

CHIFFRIERSCHEIBE



Den inneren Ring der Scheibe ausschneiden und los geht's.