Quantensichere Zufallszahlen: Fortschritte und Herausforderungen bei der Implementierung von QRNGs in der modernen Kryptographie

Geschrieben von Nicole Kosel, freie Mitarbeiterin der cyberunity AG, in Zusammenarbeit mit Xenia Bogomolec, Information Security Specialist und CEO der Quant-X Security & Coding, Maximiliane Weishäupl, Kryptographie-Doktorandin an der Uni Regensburg, Mehrzad Firoozi, Physik-Doktorand am Fraunhofer IPMS und Peter Kosel, Gründer von cyberunity.

Die Relevanz stochastischer Prozesse hat sich von ihrer initialen Anwendung in der Gaming-Industrie bis hin zur heutigen Nutzung in der Kryptographie signifikant gewandelt und erweitert. Im Zeitalter der Informationstechnologie ist die Generierung von Zufallszahlen unerlässlich für Informationssicherheit, Modellierungen, Simulationen und andere digitale Prozesse. Es ist wichtig, zwischen Zufallszahlen für Modellierungszwecke und denen für kryptographische Anwendungen zu unterscheiden, da im Allgemeinen die Anforderungen an die Qualität der Zufallszahlen bzw. der Zufälligkeit in der Kryptographie wesentlich höher sind. Angesichts des exponentiellen Wachstums des Datenaufkommens und der zunehmenden Konnektivität von Geräten steigt die Anforderung an kryptographische Methoden, die auf einer zuverlässigen Zufälligkeit beruhen. Eine entscheidende Rolle kommt hierbei der Entropie zu, die in der Informationssicherheit die Unvorhersehbarkeit und somit die Qualität der Zufälligkeit indiziert. Quanten-Zufallszahlengeneratoren (QRNGs) repräsentieren eine fortschrittliche Technologie, die die Prinzipien der Quantenmechanik nutzt, um Zufallszahlen mit hoher Entropie zu erzeugen. Diese Zahlen sind aufgrund ihrer ausgeprägten Unvorhersagbarkeit, die durch Quantenphänomene wie beispielsweise die Messung der Polarisierung von Einzelphotonen bedingt ist, für die Kryptographie von besonderer Bedeutung. Die generierte Zufälligkeit ist ein unerlässlicher Bestandteil der Schlüsselerzeugung innerhalb von Verschlüsselungsverfahren und diversen Sicherheitsprotokollen, die darauf abzielen, Informationen gegen unbefugten Zugriff abzusichern. Die Validierung kryptographischer Systeme, einschliesslich Algorithmen, Protokolle und ihrer praktischen Implementierungen, stellt Regierungen weltweit vor immense Herausforderungen. Während der theoretischen Definition und Standardisierung solch kryptographischer Systeme kommt es zu Wettbewerben, in denen diverse interdisziplinäre Forschungsteams Referenzimplementierungen entwickeln, wobei letztere noch nicht für den Markt bestimmt sind. Zur Unterstützung der Überführung in marktreife Produkte haben verschiedene staatliche Institutionen Programme ins Leben gerufen, die eine unabhängige Überprüfung und Zertifizierung von Standards sowie praktischen Implementierungen wie Modulen, Bibliotheken und Geräten nach klar definierten Kriterien ermöglichen. In den Vereinigten Staaten übernimmt das National Institute of Standards and Technology (NIST) eine Vorreiterrolle mit der Etablierung des Cryptographic Module Validation Program (CMVP), einem Rahmenwerk, das die praktische Sicherheit kryptographischer Implementierungen evaluiert und deren Vertrauenswürdigkeit bestätigt. Im Zentrum des CMVP steht die Validierung der Entropiequellen, eine Voraussetzung, die die wesentliche Bedeutung zufälliger Zahlen in der Kryptographie unterstreicht.

Das NIST untermauert diese Notwendigkeit durch das Entropy Source Validation (ESV)-Programm, das speziell entwickelt wurde, um die Qualität und Zuverlässigkeit von Entropiequellen zu bewerten. Es gibt bereits verschiedene Projekte, die den Einsatz von QRNGs (Quanten-Zufallszahlengeneratoren) erforschen und dabei die allgemeinen BSI-Anforderungen für TRNGs (True Random Number Generators) als Basis für Entwicklung und Bewertung verwenden. Während das Bundesamt für Sicherheit in der Informationstechnik (BSI) noch keine spezifischen Richtlinien für QRNGs festgelegt hat und weiterhin die Eignung von QRNGs gegenüber den aktuell zertifizierten TRNGs prüft, zeigt es Interesse daran, die Klassifizierung von QRNGs nach Funktionsklassen des Standards AIS 20/31 vorzunehmen. Entsprechende Forschungsprojekte sind damit beauftragt, an diesen offenen Fragen zu arbeiten und eine solide Grundlage für zukünftige Standards zu schaffen.

"Quant-ID" ist eines davon und zielt darauf ab, quantensichere digitale Identitäten zu schaffen. Unter der Leitung von Quant-X Security & Coding und in Partnerschaft mit dem Fraunhofer IPMS, der MTG AG und der Universität Regensburg, entwickelt das Projekt einen Demonstrator für quantensichere Autorisierung. Diese wird mit einem vom IPMS entwickelten Quantum Random Number Generator (QRNG) und einem von Quant-X implementierten Identity Provider mit Clients realisiert, um hochwertige Zufallswerte für sichere digitale Authentifizierung und Autorisierung in kritischen Infrastrukturen zu generieren. Die MTG AG stellt dabei die post-quanten sichere PKI und die Fakultät für Datensicherheit und Kryptographie der Universität von Regensburg analysiert die Sicherheit des QRNG und der post-quanten Algorithmen in Anwendung. Die jeweiligen Beiträge der einzelnen Partner werden auf https://Quant-ID.de beschrieben. Im Quant-ID werden post-quanten sichere kryptographische Verfahren und Zufallswerte des vom IPMS entwickelten QRNG angewendet, um Netzwerkkommunikation, Webanwendungen und Datenbanken zu sichern, und die Ergebnisse werden auf ihre Eignung für Zertifizierungen geprüft. Drei Mitglieder des Quant-ID-Teams gewähren Einblicke in ihre spezifischen Funktionen und erörtern die Implikationen, die Quantum Random Number Generators (QRNGs) für die IT-Sicherheitslandschaft und die Endnutzer in der nahen Zukunft haben könnten. Unter ihnen sind Maximiliane Weishäupl von der Universität Regensburg und Mehrzad Firoozi vom Fraunhofer Institut für Photonische Mikrosysteme (IPMS), zwei engagierte Doktoranden bei der Verwirklichung dieses Vorhabens.

Maximiliane Weishäupl ist Doktorandin am Lehrstuhl für Datensicherheit und Kryptographie an der Universität Regensburg und widmet sich zum einen der kryptographischen Analyse und zum anderen dem Sicherheitsbeweis des QRNGs. „Die kryptographische Analyse beginnt mit der Identifikation notwendiger Anforderungen, die kryptographische Algorithmen innerhalb der Protokolle erfüllen müssen. Ein Beispiel für eine solche Anforderung ist in unserem Anwendungsfall durch die Tatsache gegeben, dass die Autorisierung von Nutzern schnell sein soll. Auf kryptographischer Ebene, übersetzt sich dies zur Notwendigkeit einer schnellen Verifizierung digitaler Signaturen, was wiederum bei der Auswahl der post-quantum sicheren Verfahren berücksichtigt werden muss", erklärt Weishäupl. Die Analyse befasst sich mit den aktuellen Entwicklungen in der Post-Quantum-Kryptographie und den laufenden NIST Standardisierungsprozessen. Zur Auswahl geeigneter Verfahren für das Projekt Quant-ID werden die NIST-Kandidaten, ergänzt um weitere aussichtsreiche Methoden, im Hinblick auf die identifizierten Anforderungen verglichen. Für die im Projekt verwendete Kryptographie ist es essenziell, dass die Zufälligkeit, die der QRNG produziert, eine sehr gute Qualität hat.

Maximiliane erläutert die Herausforderungen diesbezüglich wie folgt: „Um die Qualität von QRNGs zu bewerten, finden sich in der Literatur verschiedene Ansätze – von der reinen Anwendung vorgefertigter statistischer Testsuiten zu Sicherheitsbeweisen mit mehr oder weniger vielen vereinfachenden Annahmen. Für eine Zertifizierung durch das BSI sind jedoch strikte Bedingungen zu erfüllen: Für den physikalischen QRNG muss ein stochastisches Modell angegeben werden, also eine Familie von Wahrscheinlichkeitsverteilungen, die den QRNG möglichst gut in allen Situationen beschreibt (z.B. verschiedene Umwelt-Bedingungen wie Temperatur) und dabei auch alle erdenklichen Seiteninformationen miteinbezieht (z.B. Störgeräusche von Komponenten). Durch experimentell generierte Daten werden dann die Verteilungsparameter bestimmt, und die Entropie der rohen Daten (also des direkten Outputs des QRNGs) kann berechnet werden. Eine Verbesserung der Entropie kann durch sogenanntes Post-Processing der rohen Daten erreicht werden und kann beispielsweise aus Anwendung einer Hash-Funktion bestehen. Die finale Entropie muss über einer vom BSI festgelegten Schranke liegen und zudem ist die Implementierung von Tests, die die Qualität der Zufallszahlen während des Betriebs des QRNGs gewährleisten, gefordert“.

Mehrzad Firoozi unterstreicht die experimentellen und technischen Aspekte des Projekts. Als wissenschaftlicher Forscher am Fraunhofer IPMS widmet er sich dem makroskopischen Aufbau und der Weiterentwicklung des QRNGs. „In dieser Phase habe ich viele verschiedene konventionelle QRNGs, die auch die Projektanforderung erfüllen können, theoretisch und experimentell miteinander verglichen. Dies konnte uns dabei helfen, den richtigen QRNG-Aufbau für das Projekt auszuwählen. Für den Sicherheitsbeweis ist auch die Beschreibung des QRNGs durch ein mathematisches Modell von grosser Bedeutung", erläutert Firoozi. Seine Arbeit umfasst mit der Implementation des QRNG auch den Aufbau einer Postprocessing-Plattform, die nicht-uniform verteilte Zufallszahlen in uniform verteilte überführt. „Der rohe Output des QRNGs ist normalerweise nicht uniform verteilt (er hat z. B. Gausssche Verteilung). In dieser Phase wird zuerst dieser analoge output von einem Analoge-to-digital Converter (ADC) digitalisiert. Danach werden die digitalen Werte zu einem Field-Programmable Gate Array (FPGA) weitergegeben, damit sie durch eine ‚Randomness Extraction‘ Methode eine uniforme Wahrscheinlichkeitsverteilung bekommen. Dann sind die resultierenden Daten bereit, durch eine geeignete Schnittstelle (z. B. Ethernet) übertragen zu werden", erklärt Firoozi. Ein zentraler Aspekt seiner Arbeit besteht darin, die Technologie so zu optimieren, dass sie für das BSI zertifizierungsfähig wird und anschliessend eine Miniaturisierung des Systems für die praktische Anwendung gewährleistet ist. Das Zusammenwirken von Weishäupl und Firoozi im Projekt Quant-ID ist ein Beispiel für interdisziplinäre Zusammenarbeit. Während Weishäupl die theoretische und analytische Seite der Kryptographie erörtert, bringt Firoozi seine umfangreiche Erfahrung in der experimentellen Physik und Technik ein.

Maximiliane und Mehrzad haben sich aus unterschiedlichen, aber komplementären Gründen für das Projekt in der Quantenkryptographie entschieden. Maximiliane, als Doktorandin mit einem Hintergrund in Mathematik, findet die praktische Anwendung mathematischer Konzepte in der Kryptographie besonders ansprechend. Für sie liegt die Faszination in der interdisziplinären Herausforderung, die Mathematik, Informatik und Physik vereint, was eine umfassende Einarbeitung in diverse Fachgebiete erforderlich macht. Mehrzad hingegen ist von den fundamentalen Quantenphänomenen angezogen, sowohl in theoretischer Hinsicht als auch durch die praktische Beobachtung dieser Phänomene in seinen Experimenten. Die Notwendigkeit, tiefgreifendes Wissen in Quantenoptik und grundlegende Kenntnisse in Informationstheorie zu besitzen, unterstreicht die Komplexität des Fachgebiets.

Sie unterstreichen gemeinsam die Bedeutung von Kreativität und Motivation für ihren Forschungsfortschritt. Mit ihrer Arbeit erweitern sie nicht nur die Grenzen des aktuellen technologischen Wissensstands, sondern legen auch eine solide Basis für die zukünftige Entwicklung sicherer kryptographischer Systeme. „Kryptographie wird bereits heute überall verwendet", bemerkt Weishäupl, „Zufallszahlen sind essenziell und es gibt Beispiele, in welchen schlechte Zufallszahlen ansonsten sichere Kryptographie unsicher gemacht haben. QRNGs mit guten Zufallszahlen sind daher von grossem Interesse." Firoozi ergänzt: „Mit der Entwicklung von Quantencomputern können viel leichter die Verschlüsselungen, die auf mathematischen Algorithmen basieren, geknackt werden. Da die Zufälligkeit in einem QRNG intrinsisch indeterministisch ist, können QRNGs potenziell ein höheres Sicherheitsniveau als klassische RNGs bieten. Demzufolge können Firmen oder Organisationen, bei denen Datensicherheit kritisch ist (Militärische Organisationen, Umspannwerke, Banken, etc.), von dieser Technologie profitieren."

Schematisches Diagramm eines einfachen Quanten-Zufallszahlengenerators (QRNG):

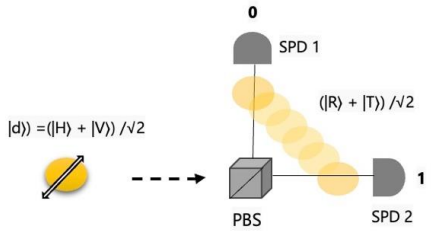

Abb.: Ein Photon wird in diagonaler Polarisation vorbereitet, welche eine Superposition von horizontaler (H) und vertikaler (V) Polarisation ist, (|H⟩ + |V⟩) /√2. Ein polarisierender Strahlteiler (PBS) überträgt die horizontale und reflektiert die vertikale Polarisation. Nach dem Passieren eines symmetrischen Strahlteilers (PBS) existiert dieses Photon in einer Superposition von übertragen (T) und reflektiert (R), (|R⟩ + |T⟩) /√2. Diese Superposition wird in einen klassischen Zustand (|R⟩ oder |T⟩) aufgelöst, wenn es von einem Einzelphotonendetektor (SPD) detektiert wird. Ein Klick auf Detektor SPD1 wird als 0-Bit aufgezeichnet und eine Detektion in SPD2 als 1-Bit.
**PBS= Polarizing Beam Splitter *SPD= Single Photon Detector*

Xenia Bogomolec, CEO der Quant-X Security & Coding betont die kritische Rolle von Zufälligkeit in der Kryptographie: „Die hohe Zufälligkeit eines sogenannten statischen kryptographischen Schlüssels mit langer Gültigkeit ist besonders wichtig. Das kann zum Beispiel ein Zertifikat für Firmwareupdates von Geräten sein, ein Zertifikat im Chip auf dem Deutschen elektronischen Reisepass (ePass) oder Root-Zertifikate von sogenannten Certification Authorities (CAs). Letztere sind die Wurzel der Sicherheit aller damit ausgestellten kryptographischen Zertifikate. Wenn das Root-Zertifikat kompromittiert ist, sind alle damit ausgestellten Zertifikate auch kompromittiert. Root-Zertifikate können über viele Angriffsvektoren kompromittiert werden[1]. Wenn jedoch eine schwache Entropiequelle genutzt wird, deren Determinismus einem bestimmten Angreifer bekannt ist, bräuchte dieser noch nicht einmal die CA zu hacken. Die Auswirkung davon wäre katastrophal, da CAs mit einem Root-Zertifikat unzählige Zertifikate für Anwendungen von Organisationen ausstellen. Ein weiteres Beispiel für die Notwendigkeit hoher Entropiequellen sind Monte Carlo Simulationen, ein Verfahren aus der Wahrscheinlichkeitstheorie, bei dem wiederholt

[1] https://sslmate.com/resources/certificate_authority_failures

Zufallsstichproben einer Verteilung mithilfe von Zufallsexperimenten gezogen werden. Je höher die Entropie ist, desto valider sind die resultierenden Aussagen."

Das Team von Quant-X Security & Coding unterstützt den Sicherheitsbeweis des QRNG aus klassischer Informationssicherheitssicht unter der Leitung von Xenia Bogomolec. Der Hintergrund in Mathematik und Algorithmenentwicklung der entsprechenden Team-Mitglieder ist die Grundvoraussetzung dazu, mit der Kryptographin Maximiliane und dem Physiker Mehrzad eine abgerundete Kommunikation zu pflegen. Ausserdem werden innerhalb der digitalen Verwertung der Quantenentropie verschiedene statistisch relevante Daten gesammelt und ausgewertet. QRNGs sind derzeit schon kommerziell verfügbar, z. B. die Quantis Serie von ID-Quantique. Der Quantis QRNG Chip ist nach NIST Entropy Source Validation (ESV) certified on IID SP 800-90B zertifiziert. Eine Zertifizierung eines QRNG durch das BSI dürfte allerdings noch einige Jahre auf sich warten lassen.

Peter Kosel von der cyberunity AG resümiert, dass das Projekt Quant-ID nicht nur eine beeindruckende Fusion von Expertise und Innovationskraft darstellt, sondern auch den nächsten entscheidenden Schritt in der Entwicklung der Kryptographie und IT-Sicherheit verkörpert.

Alle Interessierten, die einen weiteren Einblick in die Kryptographie und deren Rolle in der Informationssicherheit gewinnen möchten, finden hier einen informativen Artikel über Karrieremöglichkeiten im Kryptographie-Umfeld: Kryptographie-Spezialisten. Schlüsselfiguren in einer sicheren post-quanten Welt. Wenn ihr mehr Informationen zu Wachstumschancen in diesem Bereich wünscht, könnt ihr euch gerne mit Xenia oder Peter in Verbindung setzen.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Das diesem Artikel zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16KISQ108K gefördert.
Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei Quant-ID.