Post-Quantum-Kryptographie auf Eingebetteten Systemen
Stand der Technik und Ausblick

Thomas Pöppelmann, Infineon Technologies AG

Quantencomputer besitzen aufgrund ihrer Rechenleistung das Potenzial, verschiedene aktuell verwendete Verschlüsselungsalgorithmen zu brechen oder zu schwächen. Betroffen sind insbesondere asymmetrische Kryptoverfahren wie RSA und Elliptic Curve Cryptography (ECC), welche von zahlreichen Internetstandards wie Transport Layer Security (TLS), S/MIME, PGP, und GPG genutzt werden. Abhilfe verspricht hier die Post-Quantum-Kryptographie (Post-Quantum Cryptography; PQC), bei der es sich um Verfahren handelt, die auf klassischen Computern ausgeführt werden können, aber der Leistung von Quantencomputern standhalten. Aktuell existiert eine große Zahl solcher PQC-Verfahren, welche sich bzgl. ihrer Implementierungseigenschaften stark von RSA und ECC unterscheiden.

Asymmetrische kryptographische Verfahren wie RSA oder ECC sind heutzutage die Basis vieler kryptographischer Sicherheitsprotokolle. Ein bedeutendes Beispiel ist das Transport Layer Security (TLS) Protokoll welches die Kommunikation zwischen Web-Browsern und Servern absichert, aber auch immer mehr Verbreitung im Internet der Dinge oder anderen eingebetteten Systemen findet. Aufgrund der gegenüber RSA effizienteren Arithmetik ist auf eingebetteten Systemen besonders ECC attraktiv. So ist es selbst auf einigen Mikrocontrollern grundsätzlich möglich, ECC ohne dedizierten Hardwarebeschleuniger auszuführen. RSA und ECC gelten dazu heute als sehr sicher, da die zugrundeliegenden mathematischen Probleme wie effizientes Faktorisieren oder das Berechnen des diskreten Logarithmus über elliptischen Kurven auch nach Jahren der Untersuchung als schwer gelten. Allerdings hat Peter Shor bereits im Jahr 1994 einen Algorithmus vorgestellt, der RSA und ECC auf einer theoretischen Maschine - dem Quantencomputer - zu brechen vermag. Da ein leistungsfähiger Quantencomputer mittels Shors Algorithmus den privaten Schlüssel aus dem öffentlichen Schlüssel des RSA oder ECC-Kryptosystems in Polynomialzeit extrahiert, können selbst massiv vergrößerte Parameter diesen Angriff nicht verhindern. Neben asymmetrischen Verfahren wie RSA oder ECC ist auch die symmetrische Kryptographie, wie AES oder Triple-DES, von Quantenalgorithmen betroffen. Allerdings ist ein praktischer Angriff durch den sogenannten Grover Algorithmus weit weniger fatal, da aktuell angenommen wird, dass dieser durch das Verdoppeln der Schlüssellänge von symmetrischen Verfahren kompensiert werden kann (z. B. Einsatz von AES-256 anstelle von AES-128).

Post-Quantum Kryptographie, die NSA und NIST

Seit Jahren wird schon an der Entwicklung eines ausreichend leistungsstarken Quantencomputers gearbeitet, der, neben Fortschritten bei der Kryptoanalyse, auch Einsatz in der Materialentwicklung oder chemischen Simulation finden könnte. Um den negativen Konsequenzen für die Kryptographie entgegenzuwirken arbeiten Forscher schon seit Jahren an der so genannten Post-Quantum-Kryptographie (PQC). Dabei handelt es sich um kryptographische Algorithmen, die auf klassischen Computern ausgeführt werden, aber dabei auf mathematischen Problemen und Strukturen basieren, die selbst für Quantencomputer als extrem schwer lösbar angenommen werden. Trotzdem ist es eine berechtigte Fragestellung, warum man sich als praktischer An-

wender oder Implementierer von Kryptographie und IT-Sicherheitslösungen nun Gedanken über eine theoretische Maschine machen soll. Und weiterhin ist es richtig, dass PQC außerhalb der akademischen Welt lange Zeit ein Nischendasein führte und kaum beachtet wurde. Allerdings hat sich diese Situation spätestens August 2015 durch eine Ankündigung der National Security Agency (NSA) der Vereinigten Statten grundlegend geändert. In einer Veröffentlichung auf ihrer Webseite kündigte die NSA für die „Commercial National Security Algorithm Suite“ (CNSA Suite) an, "in the not too distant future" auf quantencomputer-resistente Algorithmen zu wechseln. Gleichzeitig wurden die Anforderungen bzgl. der Schlüssellänge für neue geheimnisverarbeitende Computersysteme zusätzlich verschärft, zum Beispiel muss nun AES-256 eingesetzt werden. Auch Mitarbeiter des BSI kommen zu dem ähnlichen Schluss, dass es heute Zeit ist zu handeln [1]. Ein weiter Vorstoß kommt vom US National Institut for Standards and Technology (NIST) welches kürzlich ein Post-Quantum-Krypto-Projekt gestartet hat. Das langfristige Ziel ist in einem wettbewerbsähnlichen Prozess neue Schlüsselaustausch-, Public-Key-Verschlüsselungs- und Signaturverfahren zu standardisieren. Aufgrund dieser Initiativen und der damit verbunden Disruption erscheint es außerordentlich wichtig, das Thema PQC nicht zu ignorieren, sondern aktiv zu gestalten.

Implementierung von Post-Quantum Kryptographie

Aktuell existieren fünf fundamentale mathematische Probleme bzw. Klassen von Algorithmen, mit denen Post-Quantum Kryptographie realisiert werden kann. Dies sind Signaturverfahren basierend auf Hashfunktionen oder dem schweren Problem multivariate quadratische Polynomgleichungen zu lösen. Zusätzlich existieren Public-Key-Verschlüsselungs- und Schlüsselaustauschverfahren basierend auf codierungstheoretischen Problemen oder Problemen auf supersingulären elliptischen Kurven. Eine weitere vielversprechende Kategorie ist die sogenannte gitterbasierte Kryptographie. Mir ihr lassen sich asymmetrische Public-Key Verschlüsselungs- und Signaturverfahren realisieren, die ein hohes Sicherheitsniveaus bei moderat großen Schlüsseln und Chiffretexten bieten.

Die praktische Implementierung von PQC-Verfahren auf eingebetteten Systemen ist seit einigen Jahren Gegenstand der Forschung. Es müssen dazu neue Wege zur effizienten Berechnung auf 8-, 16-, oder 32-bit Prozessoren gefunden werden, da die bisherigen RSA oder ECC-orientierten Konzepte nicht mehr angewandt werden können. Ein Beispiel für ein post-quantum Schlüsselaustauschverfahren ist das sogenannte gitterbasierte NewHope Verfahren [2], welches von Alkim, Ducas, Pöppelmann und Schwabe entwickelt wurde. NewHope kann aktuell verfügbare Diffie-Hellman- oder Elliptic Curve Diffie-Hellman-basierte Schlüsselaustauschmechanismen ersetzen oder komplementieren. Für langfristige Sicherheit erreicht NewHope nach aktuellem Stand der Forschung etwa 256 Bits an Sicherheit gegen Angriffe durch Quantencomputer. Beide Seiten müssen für einen Schlüsselaustauch etwa jeweils 2048 Bytes übertragen. Im Jahr 2016 wurde der NewHope -Algorithmus von Google in einer öffentlichen Betaversion des Chrome-Browsers in das TLS Protokoll integriert und erfolgreich getestet.

Die Ausführung des NewHope Algorithmus erfordert drei Schritte. Als ersten Schritt generiert der Server einen öffentlichen Schlüssels (Key generation) aus einem Geheimnis welches nur der Server kennt. Im zweiten Schritt erzeugt der Client einen öffentlichen Schlüssel aus einem nur dem Client zugänglichen Geheimnis. Der Client verknüpft dann sein Geheimnis mit dem öffentlichen Schlüssels des Servers und

erzeugt den symmetrischen Sitzungsschlüssel (Keygen + shared key). Im dritten Schritt erzeugt der Server mit seinem Geheimnis und dem öffentlichen Schlüssels des Clients denselben Sitzungsschlüssel (Shared key). Ein passiver Angreifer, welcher nur die Datenübertragung verfolgt wird durch die mathematische Komplexität der Schlüsselgenerierung daran gehindert, Rückschlüsse auf die individuellen Geheimnisse oder den erzeugt den symmetrischen Sitzungsschlüssel zu ziehen.

Auf einer Intel CPU können mittels der häufig verfügbaren Vektorregister (Advanced Vector Extensions; AVX) mehrere tausend Schlüsselaustauschvorgänge pro Sekunde berechnet werden. Eine öffentlich verfügbare Implementierung des NewHope Verfahrens für eingebettete Systeme wurde bereits von Alkim, Jakubeit und Schwabe vorgestellt [3]. Auf einem Cortex-M0 kann dabei der „Key generation“ Schritt in 1,2 Millionen Zyklen, der „Keygen + shared key“ Schritt in 1,7 Millionen Zyklen und der „Shared key“ Schritt in 0,3 Millionen Zyklen ausgeführt werden. Die Implementierung ist mittels Assembler-Befehlen optimiert und nutzt für die notwendige Polynommultiplikation einen Fast Fourier Transform (FFT) basierten Algorithmus. Ein weiterer wichtiger Schritt in Richtung ausreichend sicherer Implementierungen ist der Schutz gegen physikalische Angriffe. In [4] präsentieren Oder, Schneider und Pöppelmann eine Implementierung eines Public-Key-Verschlüsselungsverfahrens, welches NewHope ähnelt und nach aktuellem Stand 233-Bit Sicherheit bieten soll. Dabei wird durch Randomisierung der internen Daten ein gewisser Schutzlevel gegen eine Stromprofilanalyse erreicht. Auf einem Cortex-M4F benötigt die Verschlüsselung einer Nachricht dann 4,1 Millionen Zyklen während die seitenkanalgeschützte Entschlüsselung 25,6 Millionen Zyklen benötigt.

Infineon hat den NewHope-Ansatz erstmals auf einem kommerziell verfügbaren kontaktlosen Sicherheitschip implementiert. Das belegt, dass PQC auch auf Smart Card-Systemen mit wenig Speicher und kontaktloser Stromversorgung implementiert werden kann und somit praktikabel ist. Weitere Forschungsarbeiten sind erforderlich, um vorhandene Systeme im Hinblick auf einen niedrigen Stromverbrauch, einen geringen Speicherbedarf und hohe Sicherheit zu optimieren. Infineon, als führender Hersteller von Security ICs und Chips für das Internet der Dinge und die Automobilindustrie ist dabei auf mehreren Ebenen aktiv, um zukünftige Lösungen für Kunden und Anwender bereitzustellen. Aktivitäten umfassen wissenschaftliche Beiträge, Teilnahme an der PQC Standardisierung und prototypische Entwicklung und Forschung.

Literatur- und Quellenverzeichnis

[1] Heike Hagemeier, Manfred Lochter: Informationssicherheit im Quantenzeitalter. Mit Sicherheit - BSI-Magazin 2017/01, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2017_01.pdf

[2] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, Peter Schwabe: Post-quantum Key Exchange - A New Hope. USENIX Security Symposium 2016: 327-343, https://eprint.iacr.org/2015/1092.pdf

[3] Erdem Alkim, Philipp Jakubeit, Peter Schwabe: NewHope on ARM Cortex-M. SPACE 2016: 332-349, https://eprint.iacr.org/2016/758.pdf

[4] Tobias Oder, Tobias Schneider, Thomas Pöppelmann, Tim Güneysu: Practical CCA2-Secure and Masked Ring-LWE Implementation. IACR Cryptology ePrint Archive 2016: 1109 (2016), https://eprint.iacr.org/2016/1109.pdf

Autor

Dr. Thomas Pöppelmann ist Ingenieur im Bereich Sicherheit und Kryptographie im Unternehmensbereich Chip Card & Security der Infineon Technologies AG in München. Sein Hauptarbeitsbereich ist die Entwicklung von Konzepten für abgesicherte Kryptographiemodule, die Standardisierung im Bereich Sicherheit und Post-Quantum-Kryptographie. Im Jahr 2015 wurde er an der Ruhr-Universität Bochum zum Doktor-Ingenieur (Dr.-Ing.) promoviert. Für seine Arbeiten an dem Post-Quantum-Schlüsselaustauschsystem NewHope wurde ihm und seinen Co-Autoren der Facebook Internet Defense Prize 2016 verliehen.

Kontakt

Internet: http://www.infineon.com/post-quantum-crypto und http://tpoeppelmann.de
Email: thomas.poeppelmann@infineon.com