Vorteile der Post Quanten Signatur

Elektronische Signaturen spielen bei IT-Sicherheitslösungen eine entscheidende Rolle. Sie ermöglichen die Echtheitsverifizierung von Kommunikationspartnern im Internet, z.B. in E-Commerce- und E-Banking-Lösungen. Zudem sollen sie die Echtheit von E-Mails, SSL-Zertifikaten oder Software-Updates gewährleisten und gehören zu den asymmetrischen kryptographischen Verfahren.

Zusammenfassung

Das neue e***X***tended ***M***erkle ***S***ignature ***S***cheme (XMSS) Signatur-Verfahren wurde in RFC 8391 als offener Internet-Standard definiert. Somit ist es eines der ersten standardisierten asymmetrischen Kryptographie-Verfahren, welches sich gegen Angriffe von Quantencomputern behaupten kann.
In der asymmetrischen Kryptographie gibt es zwei Schlüssel: einen privaten und einen öffentlichen Schlüssel. Der öffentliche Schlüssel, auch *„Public Key"* genannt, ist für jeden frei zugänglich. Die Sicherheit von *„Public Key"*-Krypto-Verfahren hängt davon ab, ob sich ein komplexes mathematisches Problem in einem bestimmten Zeitraum lösen lässt (wie z.B. der diskrete Logarithmus oder das Zerlegen von Zahlen in ihre Primfaktoren). Was für herkömmliche Computer unlösbar ist, stellt für die neuen Quantencomputer jedoch kein Problem dar – sie können die mathematischen Probleme in kürzester Zeit lösen. Somit sind bisherige *„Public Key"*-Verfahren nicht mehr sicher und digitale Unterschriften können gefälscht werden. Deshalb sind neue Verfahren gefragt, um auch in der Zukunft sichere Kommunikation zu ermöglichen.

Funktionsweise - XMSS

XMSS basiert auf dem Merkle-Signaturverfahren, welches sogenannte Merkle-Bäume und Einmal-Signaturen (Hashfunktionen) verwendet. Die Sicherheit dieses Signaturverfahrens hängt von den gewählten Hashfunktionen ab.

Bei dem XMSS-Verfahren wird zunächst eine Signatur mit dem ***W****interni*tz⁺ ***O****ne-****T****ime* ***S****ignature Scheme* (W-OTS⁺) gebildet. Anschließend wird ein leicht abgewandelter Merkle-Hash Baum verwendet. Dieser kann eine limitierte Anzahl von Nachrichten ($N = 2^n$) verifizieren. Dies funktioniert folgendermaßen:

Wenn Alice eine Nachricht an Bob schickt, hat Bob Zugriff auf den öffentlichen Schlüssel K_{pub} von Alice. Dieser kann durch den öffentlichen Schlüssel X und dem privaten Schlüssel (Y)2^n - verschiedene Einmal-Signaturen verifizieren. Für die privaten Schlüssel Y_i wird eine Einweg-Funktion, eine sogenannte Hash-Funktion (H) angewendet, so dass $h_i = H(Y_i)$. Das entspricht dem Blatt $a_{0,i}$ im Merkle Hash-Baum. Der Baum selber hat die Knoten $a_{j,i}$ – wobei i von links nach rechts durchnummeriert wird. Die Ebene des Baumes wird von j dargestellt und startet bei den Blättern mit 0 und endet bei n. H(Y[0]) wäre demensprechen a[0,0], und ist Bob als gesendete Nachricht bekannt.

> ***"The science of today is the technology of tomorrow."***
>
> ***// Edward Teller, Physiker***

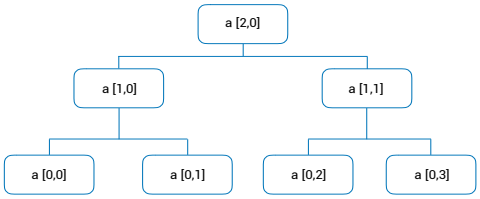
Um den nächsten Knoten a[1,0] zu verifizieren, muss Alice a[0,1] schicken, so dass der Knoten berechnet werden kann: $a[1,0] = H(a[0,0] \,||\, a[0,1])$

Dies geschieht nach der folgenden Formel:

$$a_{i,j} = H(a_{i-1,j} \,||\, a_{i-1,j-1})$$

Der Schritt wird so oft wiederholt, bis der Knoten a[n,0] erreicht wurde, welcher unser K_{pub} ist. Dieser ist der Wurzelknoten. Sind beide Werte, gegebener und errechneter, identisch, so ist die Signatur gültig.

XMSS nutzt zusätzlich Zufallszahlen bei der Verifizierung einzelner Knotenpunkte. Dies erhöht die Sicherheit des Verfahrens.



Post-Quanten Sicherheit durch XMSS

Dadurch, dass das XMSS-Verfahren seine Sicherheit nicht aus der mathematischen Aufgabenstellung (wie diskrete Logarithmen oder die Primfaktorzerlegung) gewinnt, sondern aus der Schwierigkeit der Umkehrbarkeit der Hashfunktion, verliert ein Quanten-Computer seinen mathematischen Vorteil. Denn ein Quanten-Computer kann, im Vergleich zu einem herkömmlichen Rechner, viele Ergebnisse parallel bearbeiten. Folglich erlauben die verwendeten Hashfunktionen durch den Einsatz des Merkle-Baums die digitale Signatur. Dies ist nun die Voraussetzung für eine post-quanten sichere digitale Signatur.

Profitieren Sie von qualifizierten Lösungen

Die mVISE AG bietet ein umfassendes Leistungsspektrum rund um das Thema Informationssicherheit. Kunden profitieren von einem ganzheitlichen Lösungsansatz. mVISE unterstützt, berät und realisiert IT-Security-Projekte von der Konzeption bis zur Umsetzung in allen Phasen. Die Herausforderungen der Digitalisierung löst mVISE gemeinsam mit den Kunden.

ÜBER DEN AUTOR

Bernhard Borsch ist seit 2014 für die mVISE AG tätig. Als Manager für das IT-Security Consulting beraten sein Team und er Kunden zum Thema IT-Security im Zuge der Herausforderungen der Digitalisierung. Zu seinen persönlichen Themenfeldern gehört neben den klassischen Themen, wie Enterprise- & Cloud-Security, PKI und Kryptographie, auch Zukunftsthemen der IT Security, wie Blockchain und Deception Technology. Professionelle und fachkompetente Beratung sind sein Schlüssel zum Erfolg.

Referenzen

Buchmann, Johannes, Erik Dahmen, and Andreas Hülsing.
„XMSS-a practical forward secure signa-ture scheme based on minimal security assump-tions."
International Workshop on Post-Quantum Cryptography. Springer, Berlin, Heidelberg, 2011.

Huelsing, A., Butin, D., Gazdag, S., Rijneveld, J., & Mohaisen, A. (2018).
XMSS: eXtended Merkle Signature Scheme (No. RFC 8391).

mVISE

Wir unterstützen mittelständische und große Unternehmen aller Branchen dabei, von der digitalen Revolution zu profitieren. Die besondere Kombination aus firmeneigenen Software-Lösungen mit ausgewählten Experten-Teams in den relevanten und aktuellen IT-Themengebieten schafft nachhaltige Wettbewerbsvorteile für unsere Kunden.

Unsere Experten bestimmen, gestalten, kreieren und steuern IT-Infrastrukturen und Software-Lösungen für Datenintegrations- und Enterprise-Data-Management-Projekte, mit dem Ziel, die aktuellen Geschäftsmodelle unserer Kunden zukunftssicher zu machen und gleichzeitig neue Geschäftsmodelle zu identifizieren.

Sprechen Sie uns an – gerne stellen wir Ihnen unser Angebot
in einem persönlichen Gespräch näher vor.
service@mvise.de | www.mvise.de

mVISE AG
Wahler Straße 2
40472 Düsseldorf
Fon: +49 211 78 17 80 – 0