Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K27: Angriffe auf ECC

Stichworte: Verwendung elliptischer Kurven, Patente, Standards, Sicherheitsbedenken, NSA-Hintertür, Angriffe durch Quantencomputer u.a.

27.1. Einleitung: Wir beenden die Vorlesung mit Gedanken über Patente, Standards, Sicherheitsfragen und einigen Schlussbemerkungen.

Verwendung elliptischer Kurven

27.2. Die sehr praktische Nutzbarkeit elliptischer Kurven ist mittlerweile sehr vielseitig. Elliptische Kurven können außer für kryptographische Anwendungen auch für pseudo-Zufallsgeneratoren oder das Faktorisierungsproblem eingesetzt werden. Kryptographie-Anwendungen gehören aber zu ihrem Haupteinsatzgebiet. Man bezeichnet die Kryptographie-Anwendungen elliptischer Kurven zusammenfassend mit ECC (= "elliptic curve cryptography").

27.3. Die in Österreich gängigen Bürgerkarten (e-card oder Bankomat-karte) verwenden schon seit 2004/2005 ECC. Die meisten Reisepässe europäischer Staaten verwenden ECC zumindest als Zugriffsschutz für den Chip, manche Länder (u.a. Deutschland und Schweiz) auch, um die gespeicherten Daten mit "Passive Authentification" zu schützen. Auch die deutsche Gesundheits-Karte hat auf ihrem Speicherchip ECC implementiert.

27.4. Die Firma Sony benutzte ECDSA zur digitalen Signierung von Software für die Playstation 3.

Patente

27.5 Die allgemeine Idee zu ECC wurde nicht patentiert, d.h. ECC selbst ist prinzipiell patentfrei. (Im Gegensatz zu RSA oder DH.) Es gibt aber eine Reihe von Patenten zu effizienten Implementationen. Daher sind Implementierungen mit Patentproblemen konfrontiert.

27.6. Die kanadische Firma Certicom (vgl. www.certicom.com) besitzt hunderte Patente, die für ECC oder Public-key-Kryptographie benötigt werden. Davon wurden 26 von der NSA (die US-amerikanische National Security Agency) im Wert von 25 Millionen US-Dollar lizenziert, um ECC-Verfahren zu Zwecken der nationalen Sicherheit zu implementieren; davon Kurven über $\mathbb{F}_p$ für Primzahlen p mit 256, 384 und 521 Bit. ($2^{512} \approx 10^{154}$) (Angeblich sind einige dieser Lizenzen abgelaufen, weil die NSA die Lizenzbeträge dafür nicht mehr bezahlt hat.)

27.7. Die patent-bedingte Unsicherheit bzgl. der ECC ist mit ein Grund dafür, dass die ECC nicht in jederlei Hinsicht als empfehlenswert akzeptiert wird.

27.8. Patentstreit certicom gegen Sony 2007: Certicom klagte Sony wegen der Verwendung zweier ihrer US-Patente zur ECC an. Die Anklage wurde 2009 abgewiesen.

27.9. Die Firma certicom wurde 2009 von RIM (Research in Motion, heute: blackberry) zum Preis von 130 Millionen US-Dollar als Tochterfirma übernommen.

Standards und Sicherheit

27.10. Eine elliptische Kurve wird zur Benutzung für gewöhnlich nicht jedesmal neu erzeugt: Die Berechnung von $\#E(\mathbb{F}_p)$ ist zeitaufwendig und kompliziert zu implementieren. Daher werden Kurvenparameter geeigneter elliptischer Kurven zur praktischen Verwendung von verschiedenen Organisationen veröffentlicht ("Standardkurven"/"benannte Kurven"), z.B. von der NIST (U.S. National Institute of Standards and Technology) oder SECG (Standards for Efficient Cryptography Group).

27.11. Man kann Kurven selbst zur Nutzung erzeugen, wenn u.a. die in K25 genannten Kriterien für die kryptographische Eignung nachprüfbar erfüllt sind. Diese Liste ist nicht vollständig; die Kriterien sollten dem aktuellen Stand der Forschung angepasst sein. Auch Patentfragen werden dann wichtig.

27.12. Verschiedene Organisationen geben Sicherheitsstandards für den Gebrauch des ECC heraus. In Deutschland gibt etwa das BSI (Bundesamt für Sicherheit in der Informationstechnik) technische Vorgaben und Empfehlungen zur ECC-Implementierung auf der Basis des ISO/IEC 15946 - Standards heraus. So halten sich z.B. deutsche Banken an diese Vorgaben.

27.13. Im Jahr 2013 meldete die New York Times auf Grundlage eines Snowden-Dokuments, dass der vom NIST als Standard gesetzte ECC-Algorithmus "Dual_EC_DRBG" zur Erzeugung von Pseudo-Zufallszahlen eine von der NSA eingeschleuste Schwäche im Algorithmus und der empfohlenen elliptischen Kurve besitzen würde. Die Firma RSA-Security gab daraufhin die Empfehlung, darauf basierende Algorithmen nicht weiter zu verwenden. Das NIST hat die Empfehlung des Algorithmus inzwischen zurückgezogen. Kryptographie-Experten äußerten aufgrund dieser "NSA Hintertür" auch Bedenken gegenüber mancher der vom NIST empfohlenen elliptischen Kurven und rieten wieder zur Nutzung EC-freier Kryptographie.

→ vgl. Artikel "Nach Snowden: Wenig Schlaf für Kryptoforscher" 17.09.2014 auf www.heise.de/security

Dabei hatte certicom bereits 2006 eine Patentanmeldung eingereicht, in der die Hintertür beschrieben wurde.

→ vgl. Artikel "NSA-Skandale: So funktionieren Kryptographie-Hintertüren" auf Spiegel online

→ vgl. Artikel "Konkurrenz für die NIST: Bernsteins elliptische Kurven auf dem Weg zum Standard" bei heise.de,

→ auch: wikipedia "krypto-Handy": Absatz "Mobiltelefone der deutschen Bundesregierung"

Mögliche und bekannte Angriffe auf ECC

27.14. Das DL-Problem auf elliptischen Kurven ist mittlerweile auch gegenüber einem Angriff mit einem Quantencomputer nicht mehr resistent: der Shor-Algorithmus konnte auf elliptische Kurven-Gruppen übertragen werden, vgl. Proos und Zalka, auf arXiv: quant-ph/0301141 (2004). Ein solcher Angriff braucht nur etwa halb so lange wie der klassische Shor-Algorithmus zur Lösung des Faktorisierungsproblems bei einem RSA-Verfahren mit vergleichbarer Sicherheit. Auch der Speicheraufwand eines Quantencomputers (Anzahl benötigter Qubits) ist dabei um (grob) den Faktor 2/3 geringer. → vgl. die Ausführungen in K11.5.
Bei Aufkommen von Quantencomputern werden die ECC-Verfahren daher Jahre vor den entsprechenden RSA-Verfahren geknackt sein.
An Kryptographie-Alternativen wird derzeit geforscht ("post-quantum-cryptology").

27.15. Mai 2011 veröffentlichten Brumley/Tuveri eine Arbeit zu einem erfolgreichen Timing-Angriff auf ECDSA in Form eines "Seitenkanalangriffs": Weil Ver- und Entschlüsseln mit verschiedenen Schlüsseln unterschiedlich viel Zeit in Anspruch nimmt, konnte durch Abhören der verschlüsselten Kommunikation (über einen "Seitenkanal") auf die privaten Schlüssel geschlossen werden.

27.16. Im Jahr 2010 gelang es einer Hackergruppe, den private key bei der von Sony für die Playstation 3 benutzten ECDSA zu erbeuten und damit das Sicherheitssystem fast vollständig zu unterwandern. Dies war aber vor allem auf Implementierungsfehler von Sony zurückzuführen und beruhte nicht auf etwaige Sicherheitslücken des verwendeten ECC-Systems.

Ende der Vorlesung