Public-Key-Algorithmen

Lernkontrollfragen zur Klausurvorbereitung

Grundlegende Konzepte

- Welche Schutzziele kann man durch Kryptographie erreichen? (Vertraulichkeit, Integrität, Nachrichtenauthentizität, Teilnehmerauthentizität, Verbindlichkeit)
- Wie lassen sich die Schutzziele erreichen? (Vertraulichkeit durch Verschlüsselung, Nachrichtenauthentizität und Integrität durch Message Authentication Codes und digitale Signatur, Teilnehmerauthentizität durch Challenge-Response, Verbindlichkeit durch digitale Signatur)

- Wie ist die Funktionsweise einer symmetrischen Verschlüsselung und eines Message Authentication Codes?
- Wie ist die Funktionsweise einer asymmetrischen Verschlüsselung und einer digitalen Signatur?
- Was sind die Vorteile der asymmetrischen gegenüber der symmetrischen Kryptographie?

- Welche Public-Key-Algorithmen gibt es? (RSA, Diskreter Logarithmus, Elliptische Kurven)
- Wie funktionieren die Verfahren und worauf beruht die Sicherheit? Wie lässt sich die Sicherheit der drei Verfahren vergleichen?
- Worin unterscheiden sich die verschiedenen Verfahren in der Schlüsselerzeugung? Welche Verfahren sind aufwändiger?

Endliche Körper

- Wie sind endliche Körper definiert?
- Welche Typen gibt es? (Primkörper, binäre Erweiterungskörper)
- Wie lassen sich die verschiedenen Typen im Rechner realisieren?

- Wie funktionieren die grundlegenden Rechenregeln wie Addition, Multiplikation, sowie die Berechnung von additiven und multiplikativen Inversen in Primkörpern bzw. binären Erweiterungskörpern?
- Wie funktioniert Subtraktion und Division im Primkörper bzw. binären Erweiterungskörper?

- Wie funktioniert der Shift-and-Add-Algorithmus und welchen Aufwand hat der Algorithmus? (Algorithmus soll theoretisch beschrieben und praktisch angewendet werden können!)

Elliptische Kurven

- Wie sind elliptische Kurven definiert über den reellen Zahlen? Wie sind elliptische Kurven über einem endlichen Körper (Primkörper bzw. binären Erweiterungskörper) definiert?
- Wie kann man eine elliptische Kurve über einen kleinen Primkörper zeichnen?
- Wie sieht eine elliptische Kurve im Reellen aus?

- Wie kann man auf einer elliptische Kurve rechnen? (Anschauliche Interpretation im Reellen und Übertragung auf endliche Körper)
- Die Formeln für Addition und Verdoppelung müssen nicht auswendig gelernt werden! Falls die Formeln benötigt werden, sind sie angegeben.

- Was sind die Eigenschaften der Rechenregel? (additive Gruppe)
- Wie sind negative Punkte definiert für elliptische Kurven im Reellen, in Primkörpern bzw. Erweiterungskörpern?

- Was ist eine Skalarmultiplikation? Wie lässt sich eine Skalarmultiplikation effizient berechnen? (Double-and-Add, Montgomery-Skalarmultiplikation)
- Die Herleitung der Formeln für Addition und Verdoppelung ohne y-Koordinaten bei der Montgomery-Skalarmultiplikation sowie die Rückgewinnung der y-Koordinate müssen nicht auswendig gelernt werden! Falls die Formeln benötigt werden, sind sie angegeben.

- Wie ist das Diskrete Logarithmus Problem für elliptische Kurven definiert?

Praktikum

- Wie kann man in C/C++ einen binären Schlüssel möglichst effizient bitweise von rechts und von links durchlaufen?
- Was bedeuten Schiebeoperationen bei Bitfolgen, die Polynome darstellen?
- Was bedeuten Schiebeoperationen bei Bitfolgen, die natürliche Zahlen darstellen?

- Wie setzt man die Formeln für die Addition und Verdoppelung in Pseudocode um? (d.h.

  $P_1 := P_1 + P_2$

  $P_2 := P_2$

  bedeuten die Formeln

  $X_1 := X_1Z_2X_2Z_1 + x_P(X_1Z_2+X_2Z_1)^2$

  $Z_1 := (X_1Z_1 + X_2Z_1)^2$

  $X_2 := X_2^4$

  $Z_2 := X_2^4 + Z_2^4 b$

  Wie lassen sich diese Formeln im Rechner umsetzen?)

Eingabe: x-Koordinate x_P eines Punktes P, Parameter b der elliptischen Kurve, k natürliche Zahl
Ausgabe: X_1, Z_1, X_2, Z_2, wobei $x_1 = X_1/Z_1$ die x-Koordinate des Punktes $k \cdot P$ ist und $x_2 = X_2/Z_2$ die x-Koordinate des Punktes $(k+1) \cdot P$.

(1)	$X_1 \leftarrow 1, Z_1 \leftarrow 0$		
(2)	$X_2 \leftarrow x_P, Z_2 \leftarrow 1$		
(3)	**for** $i \leftarrow m-1$ **downto** 0 **do**		
(4)	**if** $k_i = 1$ **do**		
(5)		$T \leftarrow X_1 * Z_2$	X_1Z_2
(6)		$S \leftarrow X_2 * Z_1$	X_2Z_1
(7)		$X_1 \leftarrow T * S$	$X_1Z_2X_2Z_1$
(8)		$S \leftarrow T \oplus S$	$X_1Z_2 + X_2Z_1$
(9)		$Z_1 \leftarrow S * S$	$(X_1Z_2 + X_2Z_1)^2$
(10)		$T \leftarrow x_P * Z_1$	$x_P(X_1Z_2 + X_2Z_1)^2$
(11)		$X_1 \leftarrow X_1 \oplus T$	$X_1Z_2X_2Z_1 + x_P(X_1Z_2 + X_2Z_1)^2$
(12)		$T \leftarrow X_2 * X_2$	X_2^2
(13)		$S \leftarrow Z_2 * Z_2$	Z_2^2
(14)		$Z_2 \leftarrow S * T$	$X_2^2Z_2^2$
(15)		$S \leftarrow S * S$	Z_2^4
(16)		$S \leftarrow S * b$	$Z_2^4 b$
(17)		$X_2 \leftarrow T * T$	X_2^4
(18)		$X_2 \leftarrow X_2 \oplus S$	$X_2^4 + Z_2^4 b$
(19)	**else do**		
(20)		$T \leftarrow X_2 * Z_1$	
(21)		$S \leftarrow X_1 * Z_2$	
(22)		$X_2 \leftarrow T * S$	
(23)		$S \leftarrow T \oplus S$	
(24)		$Z_2 \leftarrow S * S$	
(25)		$T \leftarrow x_P * Z_2$	
(26)		$X_2 \leftarrow X_2 \oplus T$	
(27)		$T \leftarrow X_1 * X_1$	
(28)		$S \leftarrow Z_1 * Z_1$	
(29)		$Z_1 \leftarrow S * T$	
(30)		$S \leftarrow S * S$	
(31)		$S \leftarrow S * b$	
(32)		$X_1 \leftarrow T * T$	
(33)		$X_1 \leftarrow X_1 \oplus S$	
(34)	**return** (X_1, Z_1, X_2, Z_2)		

Protokolle

- Was sind die Systemparameter eines ECC-Systems? Wie werden diese erzeugt?
- Wie werden privater und öffentlicher Schlüssel eines ECC-Systems erzeugt?

- Wie funktioniert das Diffie-Hellman Protokoll für elliptische Kurven? Was kann damit erreicht werden? Worauf basiert die Sicherheit des Protokolls?
- Wie funktioniert eine ElGamal-Verschlüsselung?

Es sind keine Hilfsmittel außer Taschenrechner zugelassen!