Gruppenbasierte Kryptographie

Das RSA und Rabin Verfahren basieren auf dem Restklassenring $\mathbb{Z}/n\mathbb{Z}$ und der Einheitengruppe darin.

Wir betrachten nun Kryptosysteme, welche auf beliebigen abelschen Gruppen basieren. Wir nehmen im folgenden an, daß G eine zyklische Gruppe der Ordnung ℓ ist ($\ell = c\ell_0$ mit c klein und ℓ_0 prim).

Sei G erzeugt von g. Für jedes Element $b \in G$ gibt es ein eindeutig bestimmtes $x \in \mathbb{Z}$ mit $0 \le x \le \ell - 1$ und $b = g^x$. Wir nennen x den diskreten Logarithmus von b zur Basis g.

Die Berechnung diskreter Logarithmen in geeigneten Gruppen ist (vermutlich) ein schwieriges Problem (ähnlich wie das Faktorisieren von n). Die Abbildung $x \mapsto g^x$ ist dann eine Einwegfunktion.

Beispiel: $(\mathbb{Z}/p\mathbb{Z}, +)$ leicht, $(\mathbb{Z}/p\mathbb{Z})^\times$ (normalerweise) schwer.

ElGamal Verschlüsselung

Schlüsselerzeugung:
- Wähle $x \in \mathbb{Z}$ mit $0 \le x \le \ell - 1$ zufällig.
- Berechne $y = g^x$.
- Der geheime Schlüssel ist x, der öffentliche Schlüssel ist y.

Verschlüsselung von $m \in G$:
- Wähle $r \in \mathbb{Z}$ zufällig.
- Berechne $u = g^r$ und $v = my^r$.
- Der Chiffretext ist (u, v).

Entschlüsselung von $(u, v) \in G \times G$:
- Berechne $m = vu^{-x}$.
- Der Klartext ist m.

ElGamal Verschlüsselung

Die Abbildung $x \mapsto g^x$ ist keine Einwegfunktion mit Falltür. Dies ist im Verfahren auch nicht erforderlich.

Für G kann man allgemeiner eine Untergruppe der multiplikativen Gruppe von endlichen Körpern $\mathbb{F}_q^\times$ verwenden.

Das ElGamal Verfahren ist randomisiert. Chiffretexte zu zufälligen Nachrichten sind wie zufällige Elemente aus $G \times G$.

Man maskiert eine Nachricht m mit einem zufälligen Wert y^r. Durch die Angabe von g^r versetzt man den Empfänger in die Lage, $y^r = (g^r)^x$ auszurechnen und so m wiederzuerhalten.

ElGamal Sicherheit

Das Diffie-Hellman Problem ist, zu g, g^a, g^b den Wert g^{ab} auszurechnen.

Thm: Das ElGamal Verfahren ist OW-CPA sicher, wenn das Diffie-Hellman Problem schwierig ist.

Bew: Zu g, g^a, g^b wählen wir zufällig $s, r \in \mathbb{Z}$ modulo ℓ und $z \in G$ und wenden einen Angreifer auf g, den öffentlichen Schlüssel $y = g^{as}$ und den Ciffretext (g^{br}, z) an. Wir erhalten $m = zg^{-bras}$, daraus $z/m = g^{absr}$ und schließlich $g^{ab} = (g^{absr})^{1/(sr)}$. $\square$

Bemerkung: Ist $\gcd\{r, \ell\} = 1$, gibt es $\lambda, \mu \in \mathbb{Z}$ mit $1 = \lambda r + \mu\ell$. Damit ist g^λ die eindeutig bestimmte r-te Wurzel von g.

ElGamal Sicherheit

Das Diffie-Hellman Entscheidungsproblem ist, zu g, g^a, g^b, h zu entscheiden, ob $h = g^{ab}$ oder nicht.

Thm: Das ElGamal Verfahren ist IND-CPA sicher, wenn das Diffie-Hellman Entscheidungsproblem schwierig ist.

Bew: Sei A ein polynomieller Angreifer gegen IND. A liefert also nach Eingabe zweier Klartexte m_1, m_2 und eines Chiffretext c von m_1 oder m_2 in einer Zeit polynomiell in $\log_2(\#G)$ einen Klartext m_i zurück, welcher mit Wahrscheinlichkeit $> 2/3$ der zu c gehörige Klartext ist. Wir nehmen zuerst zusätzlich an, daß A einen Fehler ausgibt, wenn c weder zu m_1 noch zu m_2 gehört.

ElGamal Sicherheit

Bew (ctd.):

Dann gehen wir wie folgt vor: Zu g, g^a, g^b, h wählen wir zwei zufällige $m_1, m_2 \in G$ und wenden A bezüglich des Basiswerts g und des öffentlichen Schlüssels g^a auf m_1, m_2 und den „Chiffretext" $c = (g^b, m_1 h)$ an. Gilt $h = g^{ab}$, so ist der Chiffretext eine Verschlüsselung von m_1, ansonsten nicht. Die Wahrscheinlichkeit, daß c ein Chiffretext zu m_2 ist, ist vernachlässigbar. Gibt A also m_1 aus, so geben wir „$h = g^{ab}$" aus. Gibt A einen Fehler aus, so geben wir „$h \neq g^{ab}$". Dies liefert einen polynomiellen Algorithmus, welcher das DDH mit Wahrscheinlichkeit $> 2/3$ korrekt löst.

Probleme entstehen, wenn das Verhalten von A undefiniert ist, falls c weder zu m_1 noch zu m_2 gehört. Da die Diskussion hier etwas technisch wird, lassen wir sie aus. $\square$