Kryptographie und Komplexität

Einheit 6.4

Mehrparteien-Berechnung und Verteilte Geheimnisse

1. Secret-Sharing Protokolle
2. Verifizierbare Geheimnisaufteilung
3. Threshold Signaturverfahren
4. Münzwurf am Telephon
5. Oblivious Transfer
6. Anonymer Vergleich

Verteilung von Information auf eine Gruppe

- **Mehrparteien-Berechnungen**
  - Aktion wird von mehreren Teilnehmer gemeinsam durchgeführt
    Einzelne Teilnehmer dürfen Aktion nicht alleine ausführen können
    - Öffnen eines Schließfachs in einer Bank
    - Verpacken von Bargeld in der Bundesdruckerei
    - Auszählung von Wahlergebnissen / Elektronische Wahlen
    - Kritische militärische Aktionen
- **Secret Sharing**
  - Absicherung eines Geheimnisses gegen Verrat durch einzelne
    - Einzelpersonen haben nur Teilinformationen
    - Geheimnis kann aus Teilinformation rekonstruiert werden
  - Schutz der Gruppe gegen Blockade durch einzelne
    - Geheimnis kann von Teilgruppe rekonstruiert werden
  - Sicherheitsschwelle abhängig von Bedeutung des Geheimnisses
- **Sichere Funktionenauswertung**
  - Auswertung einer Funktion mit Daten aller Gruppenteilnehmer
  - Ein-/Ausgaben einzelner Teilnehmer bleiben vor anderen verborgen

Modell für Mehrparteien-Berechnung

- **Berechnung benötigt mehrere (geheime) Eingaben**
  - Eingaben einzelner Teilnehmer bleiben für alle anderen unsichtbar
  - Ausgaben erlauben keine Rückschlüsse auf geheime Informationen
  - Teilnehmer verhalten sich möglicherweise nicht korrekt
- **Modell möglicher Angreifer**
  - Gesicherte Authentizität: Angreifer kann Nachrichten nicht ändern
  - Unehrliche Teilnehmer: Angreifer kann falsche Nachrichten einstreuen
  - Korrumpierte Teilnehmer: Angreifer kontrolliert Geheimnisse und Verhalten mancher Teilnehmer
  - Unvollständiges Ergebnis: Angreifer kann Protokoll abbrechen
- **Sichere Mehrparteien-Berechnung ist möglich**
  - Wenn Angreifer weniger als die Hälfte der Teilnehmer kontrolliert
  - Wenn Angreifer beliebig viele Teilnehmer nur passiv kontrolliert

Secret-Sharing Verfahren

Sicherheit in einer korrumpierbaren Welt

- **Aufteilung eines Geheimnisses**
  - Geheime Information wird auf n Personen verteilt
  - Geheimnis kann nur durch Zusammenarbeit rekonstruiert werden
  - Geheimnis bleibt sicher, auch wenn einzelne unehrlich sind
- **Schwellenschema (Threshold Schemes)**
  - Geheimnis kann nur wiederhergestellt werden, wenn mindestens t Personen beteiligt sind
  - Handlungsfähigkeit besteht, auch wenn einzelne nicht mitmachen
- **Komplexe Zugriffsstrukturen**
  - Berücksichtigt unterschiedliche Rollen einzelner Personen
  - Geheimnis kann wiederhergestellt werden, wenn eine bestimmte Mindestkonstellation von Personen beteiligt ist
    - z.B. Zwei Abteilungsleiter oder
      Ein Abteilungsleiter und zwei Referenten aus anderen Gruppen

Das Shamir Secret-Sharing Protokoll

- **Verwendet Konstruktion von Polynomsplines**

  Satz: *Ein Polynom $f \in K[x]$ vom Grad $t-1$ ist eindeutig durch t Punkte $y_i = f(x_i)$ bestimmt*

  – Die Lagrange-Interpolationsformel für Polynome liefert die Gleichung

  $$f(x) = \sum_{i=1}^{t} y_i \cdot \prod_{j \neq i} (x - x_j)/(x_i - x_j)$$

  – Bei weniger als t Interpolationspunkten ist eines der y_i unbestimmt und die Gleichung für f hat viele Lösungen

- **Initialisierung für n Personen**

  – Wähle Primzahl $p > n$ und veröffentliche n verschiedene Zahlen $x_i \in \mathbb{Z}_p^*$

- **Verteilung eines Geheimnisses $s \in \mathbb{Z}_p$**

  – Wähle geheime Koeffizienten $a_j \in \mathbb{Z}_p$ und setze $f(x) = s + \sum_{j=1}^{t-1} a_j x^j$

  – Vergebe an den i-ten Geheimnisträger den Geheimnisteil $y_i = f(x_i)$

- **Rekonstruktion des Geheimnisses**

  – Bei t Teilnehmern kann f eindeutig wiederhergestellt werden

  – Das Geheimnis s ist der Wert von f an der Stelle 0

  – Bei weniger als t Teilnehmern gibt es p mögliche Lösungen für s

Wenn Dealer / Teilnehmer sich falsch verhalten

- **Mögliches Fehlverhalten des Dealers**
  - Falsche Berechnung der Teilgeheimnisse y_i
  - Offenlegung der Teilgeheimnisse y_i
  - Ausgabe von weniger als t Teilgeheimnissen
- **Mögliches Fehlverhalten der Teilnehmer**
  - Weigerung, ihr Teilgeheimnis preiszugeben
  - Angabe eines falschen Wertes für das Teilgeheimnis
- **Einfaches Shamir Protokoll bietet keinen Schutz**
  - Fehlverhalten führt zu Geheimnisverrat oder Nichtrekonstruierbarkeit
  - Secret-Sharing Protokolle müssen robust sein
    - Gegen kleine Menge betrügerischer / nichtkooperativer Teilnehmer
    - Gegen betrügerische Dealer

Verifizierbare Geheimnisaufteilung

Identifiziere Fehlverhalten der Beteiligten

- **Dealer muß Geheimnis verschlüsselt preisgeben**
  - Geheimnis und Fragmente werden mit Einwegfunktion chiffriert
  - Für das (t, n) Secret-Sharing Protokoll wählt Dealer geheime Koeffizienten $a_j \in \mathbb{Z}_p$, setzt $f(x) = s + \sum_{j=1}^{t-1} a_j x^j$ und veröffentlicht Werte $u_j = g^{a_j}$, x_i und $z_i = g^{f(x_i)}$ für ein erzeugendes g
  - Der i-te Geheimnisträger erhält Geheimnisteil $y_i = f(x_i)$
- **Kontrolle des Dealers durch die Geheimnisträger**
  - Jeder kann prüfen, ob $g^{s+\sum_{j=1}^{t-1} a_j (x_i)^j} = \prod_{j=0}^{t-1} u_j^{(x_i)^j} = z_i = g^{f(x_i)}$ ist, d.h. ob die veröffentlichten Punkte von f zu den Koeffizienten passen
  - Teilnehmer i kann prüfen, ob $g^{y_i} = z_i$ gilt, d.h. ob sein Teilgeheimnis wirklich $f(x_i)$ ist
- **Kontrolle der Geheimnisträger durch andere**
  - Bei Rekonstruktion des Geheimnisses kann jeder feststellen, ob Teilnehmer i sein Teilgeheimnis korrekt preisgegeben hat

Threshold Signaturverfahren

Secret-Sharing ohne Preisgabe von Teilgeheimnissen

- **Teilgeheimnisse sind nicht wiederverwendbar**
  - Teilnehmer müssen ihr Teilgeheimnis für die Rekonstruktion des Geheimnisses preisgeben
  - Teilnehmerdaten liegen ab dann für alle anderen offen
  - Für nächste Anwendung müsste neues Geheimnis verteilt werden
  - Ungeeignet für viele Anwendungen verteilter Geheimnisse
- **Signatur mit (t, n) Schwellenschemata**
  - Teilnehmer erzeugen Teilunterschrift, ohne ihre Daten preiszugeben
  - Teile werden durch Combiner oder via Broadcast zusammengesetzt

Threshold Signaturschema mit ElGamal

- **Initialisierung für n Personen**
  - Wähle eine kollisionsresistente Hashfunktion h
  - Wähle große Primzahl $p > n$ und ein erzeugendes Element g von $\mathbb{Z}_p^*$
  - Wähle eine weitere Primzahl q, die $p-1$ teilt
  - Veröffentliche n verschiedene Zahlen $x_i \in \mathbb{Z}_q^*$
- **Verteilung eines Geheimnisses $s \in \mathbb{Z}_q$**
  - Wähle geheime Koeffizienten $a_j \in \mathbb{Z}_q$ und setze $f(x) = s + \sum_{j=1}^{t-1} a_j x^j$
  - Veröffentliche $y = g^s \bmod p$ als Verifikationsschlüssel der Signatur
  - Wähle zufällige $u_i \in \mathbb{Z}_q$ und berechne die Geheimnisteile $s_i = u_i + f(x_i)$
  - Veröffentliche $y_i = g^{s_i} \bmod p$ und $z_i = g^{u_i} \bmod p$
    als Verifikationsschlüssel für Teilnehmer i
- **Verteilung der Informationen**
  - Öffentlich: Hashfunktion h, Primzahlen p, q Verifikationsschlüssel y
    Element g, Stützpunkte x_i, Teilnehmerschlüssel y_i und z_i
  - Teilnehmer i: Geheimnisanteil s_i
  - Dealer: Geheimnis s, Koeffizienten a_i, Zufallswerte u_i

Threshold Signaturschema mit ElGamal (II)

- **Signieren einer Nachricht x durch t Teilnehmer**
  - Teilnehmer i wählt ein zufälliges $k_i \in \mathbb{Z}_q$ und berechnet $r_i = g^{k_i} \bmod p$
  - Jeder erhält die r_i und berechnet $r = \prod_{i=1}^{t} r_i \equiv g^{\sum_{i=1}^{t} k_i} \bmod p$
    sowie $e = h(x, r) \bmod q$ und $\sigma_i = s_i \cdot \prod_{j \neq i} x_j \cdot (x_j - x_i)^{-1} + k_i \cdot e \bmod q$
- **Combiner setzt Teilsignaturen zusammen**
  - Prüfe Signatureteile: $g^{\sigma_i} \equiv y_i^{\prod_{j \neq i} x_j \cdot (x_j - x_i)^{-1}} \cdot r_i^e \bmod p$
  - Gesamtsignatur der Nachricht ist $\sigma = \sum_{i=1}^{t} \sigma_i \bmod q$
- **Verifikation einer Signatur**
  - Berechne $t = \prod_{i=1}^{t} z_i^{\prod_{j \neq i} x_j \cdot (x_j - x_i)^{-1}} \bmod p$ sowie $e = h(x, r) \bmod q$
  - Prüfe ob die Kongruenz $g^{\sigma} \equiv y \cdot t \cdot r^e \bmod p$ gilt

Münzwurf am Telephon

Faire Erzeugung eines gemeinsamen Ergebnisses

- **Zufall (Münzwurf) entscheidet über ein Ergebnis**
  - Erfolgswahrscheinlichkeit muß für beide Teilnehmer gleich gross sein
  - Teilnehmer kann Münzwurf des anderen nicht beobachten
    möchte aber Manipulation des Zufalls verhindern
  - Beide Teilnehmer müssen Gesamtergebnis akzeptieren können
- **Einfaches Mehrparteien-Protokoll** vgl. Rabin Verfahren §4.4
  - Alice wählt zwei Primzahlen p und q und berechnet $n = p \cdot q$.
  - Bob wählt zufälliges $r \in \{0, .., p-1\}$ und berechnet $k := r^2 \bmod n$
  - Alice sendet eine der vier möglichen Quadratwurzeln z von k an Bob
  - Ist $z \not\equiv \pm r \bmod n$, so kann Bob die Zahl n faktorisieren und gewinnt
  - Die Erfolgswahrscheinlichkeit für Bob und Alice ist genau 50%
    wenn Alice keine leicht faktorisierbare Zahl n auswählt

Oblivious Transfer

- **Unbemerkte Übertragung von Information**
  - Alice sendet Nachtricht m an Bob
  - Bob erhält Nachricht nur mit 50% Wahrscheinlichkeit
  - Alice weiß nicht, ob Bob m wirklich erhalten hat oder nicht
- **Variante: 1 aus 2 Oblivious Transfer (OT_2^1)**

  Eines von zwei Geheimnissen wird weitergegeben
  - Alice schickt zwei Geheimnisse s_1 und s_2
  - Am Ende hat Bob entweder s_1 oder s_2 erhalten
  - Alice weiß nicht, welches

  Anwendung: Gegenseitiges Unterzeichnen von Verträgen

  Elektronisches Einschreiben (Lesen nur nach Quittieren)

Oblivious Transfer Protokolle

- **Münzwurf am Telephon als OT Protokoll**
  - Die wirkliche Nachricht ist die Faktorisierung von $n = p \cdot q$.
  - Am Ende besitzt Bob diese Information mit 50% Wahrscheinlichkeit
  - Alice weiß nicht, ob Bob n faktorisieren kann oder nicht
- **OT_2^1 Protokoll mit diskreten Logarithmen**
  - Alice wählt Primzahl p und einen Erzeuger g von $\mathbb{Z}_p^*$
  - Alice wählt zufälliges $r \in \mathbb{Z}_p^*$, für das $\log_g r$ unbekannt ist als Schlüssel
  - Bob will s_1 erhalten und wählt zufälliges $b \in \mathbb{Z}_p^*$
    und berechnet $B_1 := g^b$ und $B_2 := r \cdot (g^b)^{-1}$
  - Alice prüft $B_1 \cdot B_2 \equiv r \bmod p$, wählt zufällige $y_1, y_2 \in \mathbb{Z}_p^*$,
    berechnet $\gamma_i = B_i^{y_i}$, $r_i = s_i \oplus \gamma_i$ und $\alpha_i = g^{\gamma_i} \bmod p$
  - Bob berechnet $\alpha_1^b = g^{b \cdot y_1} = B_1^{y_1} = \gamma_1$ und $s_1 = r_1 \oplus \gamma_1$

  Bob kann s_2 nicht berechnen. Alice weiß nicht ob Bob s_1 oder s_2 hat.

Anonymer Vergleich

- **Vergleich zweier Werte, ohne diese offenzulegen**
  - Gebote in Auktionen und offenen Ausschreibungen
    Das unterlegene Gebot sollte geheim bleiben
  - Altersvergleich (wer eröffnet die erste Sitzung im Bundestag?)
  - Rankings, die keine Offenlegung von Details erfordern
  - Vergleich von Firmenwerten mit verfügbarem Kapital für Übernahme
- **Abstrakte Formulierung**
  - Werte a und b von Alice und Bob gehören zur Menge $\{1..n\}$
  - Teste $a < b$, ohne daß Bob a oder Alice b kennenlernt

Protokoll für anonymen Vergleich

- **Basis: Kryptographie mit öffentlichen Schlüsseln**

  Gegeben Ver-/Entschlüsselung e_K, d_k, Primzahl p

  – Alice wählt ein zufälliges x mit $\|x\| \geq \|p\|$

  – Alice berechnet $y = e_K(x) - a$ und schickt y an Bob

  – Bob berechnet $z_u = d_K(y+u) \bmod p$ für alle $u \in W$

  Gilt $|z_u - z_{u'}| < 2$, $z_u = 0$ oder $z_u = p-1$ für ein Paar $u \neq u'$, starte neu

  – Bob schickt Alice die Zahlen $z_1, \ldots z_b, z_{b+1}+1, \ldots z_n+1 \equiv k_1, \ldots, k_n$

  – Alice prüft ob $k_a = x$ gilt. Ist dies der Fall, dann ist $a \leq b$, sonst $a > b$

- **Korrektheit**

  – Gilt $a \leq b$, dann ist $k_a = z_a = d_K(e_K(x) - a + a) \bmod p = x$

  – Gilt $a > b$, dann ist $k_a = z_a + 1 = d_K(e_K(x) - a + a) \bmod p + 1 = x + 1$