SOMMER AKADEMIE NIZZA 2009

APPLIED CRYPTOGRAPHY AND SECURITY ENGINEERING

Verteilte Geheimnisse (Secret Sharing)

-Welche Möglichkeiten gibt es ein Geheimnis zu verteilen?

-Wie lässt sich ein Schlüssel möglichst sicher aufteilen?

-Welche verschiedenen Schemata gibt es?

Von Frauke Tabert

GLIEDERUNG

- **1. How to Share a Secret**
  - Einleitung
  - Beschreibung des Verfahrens
  - Vorteile

- **2. Secret Sharing Made Short**
  - Einleitung
  - Krawczyk‘s Verfahren
  - Robuste Schemata
  - Ausblick

EINFÜHRENDES BEISPIEL

- Situation:
  - In der F&E Abteilung eines Autoherstellers wird von 11 Forschern an einem neuen Antrieb geforscht.
  - Aufgrund der strengen Geheimhaltung werden die Ergebnisse in einem Safe verschlossen.
  - Die Wissenschaftler sollen diesen nur öffnen können, wenn mindestens 6 der 11 Personen anwesend sind.
  - Das führt auf 462 Schlösser und 252 Schlüssel für jeden Forscher.

GENERALISIERUNG

- Gegeben: Daten/Geheimnis D (Schlüssel, …)

- Problem:

  Wie lässt sich D in n Teile aufteilen, sodass:
  - D aus k der n Teile rekonstruiert werden kann
  - Kenntnis von bis zu k-1 Teilen bei der Rekonstruktion nicht weiter hilft

→ ein (k,n)-Schwellwert-Schema

(engl. (k,n) threshold scheme)

NUTZEN DER AUFTEILUNG EINES GEHEIMNISSES

- Ein einzelner Ort ist zu gefährlich.

  (Computer können abstürzen, Menschen können sterben, ein Safe kann geknackt werden)
- Mehrere identische Schlüssel an verschiedenen Orten lösen das Problem auch nicht, verteilen es nur und machen angreifbarer.

- daher: Benutzung eines Schwellwert Schemas

- weitere Anwendung: z.B. digitale Signatur von Schecks, RFID

SCHWELLWERT SCHEMATA:

- Sind ideal für eine Gruppe von Personen, die kooperieren müssen

- Bei passender Wahl von k und n
  - kann eine genügend große Mehrheit das Geheimnis D rekonstruieren
  - kann eine genügend große Minderheit diese Rekonstruktion blockieren

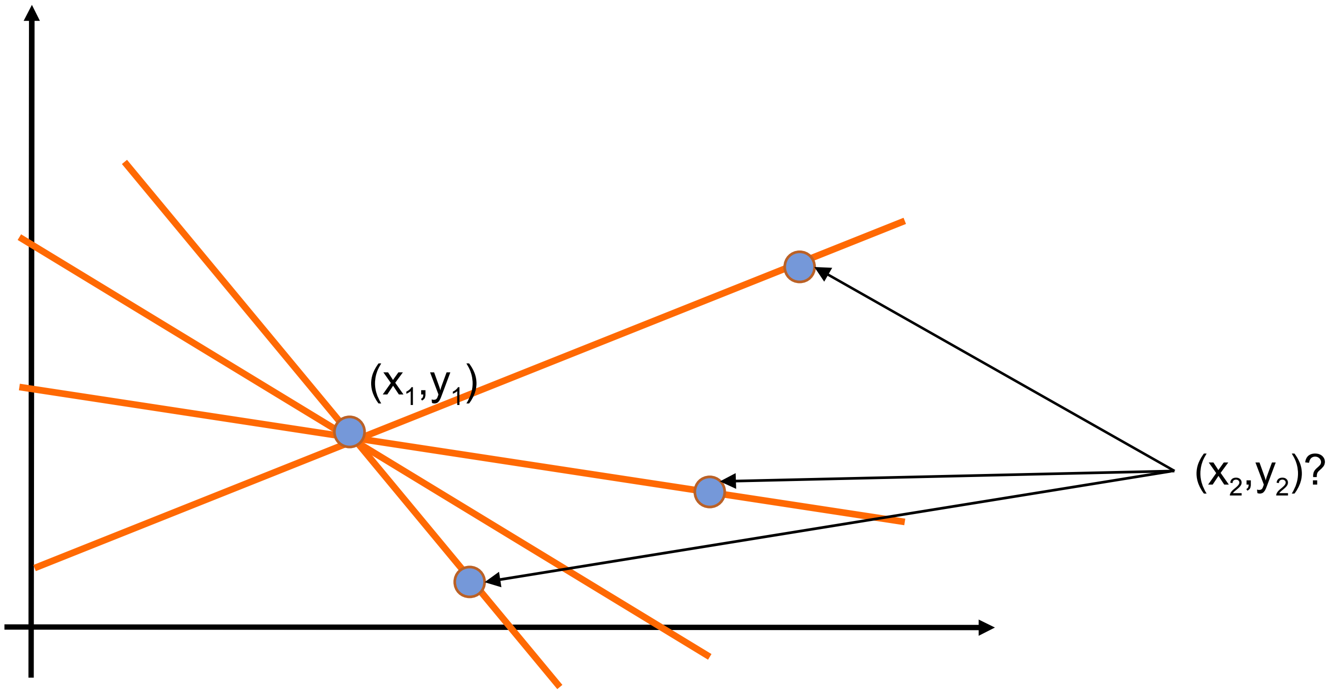
BESCHREIBUNG VON SHAMIRS VERFAHREN

- Basiert auf Polynominterpolation
- Jedem der n Teilnehmer wird ein Wertepaar (x_i, y_i) gegeben
- Es gibt für k Punkte nur ein einziges Polynom vom Grad k-1, für das gilt: $q(x_i) = y_i$.
- Es wird angenommen, dass sich D ohne Verluste in eine Zahl umwandeln lässt.
- D wird mit Hilfe des Polynoms in n Teile geteilt.

GRAPHISCHE DARSTELLUNG

- Einfaches Beispiel:

  eine Gerade wird durch zwei Punkte eindeutig festgelegt (k=2), d.h. man benötigt ein Polynom 1.Grades



- Das Polynom hat die Form:

  $q(x) = a_0 + a_1\, x + a_2\, x^2 + \ldots + a_{k-1}\, x^{k-1}$

  wobei $D = a_0$.

- $D_i = y_i = q(x_i)$ für alle $1 \leq i \leq n$

- Hat man nun k Wertepaare gegeben, lässt sich das Polynom berechnen und mit $a_0 = D = q(0)$, dem ursprünglichen Datensatz, ist das Geheimnis rekonstruiert. (durch k Punkte lässt sich das Polynom eindeutig bestimmen)

- k-1 Wertepaare reichen nicht aus um q(x) zu berechnen.

DETAILS

- Es wird Modulo Rechnung verwendet :
  - Man erreicht dadurch eine Gleichverteilung über einen bestimmten Zahlenbereich.
  - Die Koeffizienten $a_1, \ldots, a_{k-1}$ werden zufällig und gleichverteilt über $[0,p)$ ausgewählt.
  - Dann werden die Werte von $D_1, \ldots, D_n$ modulo p berechnet.
  - Dadurch sind alle möglichen Werte für D gleich wahrscheinlich.

VORTEILE DES SCHWELLWERT SCHEMAS

- Die Größe der verteilten Wertepaare geht nie über die des original Geheimnisses hinaus.

- Wenn k konstant gehalten wird, können beliebig viele weitere „Teilschlüssel“ D_i hinzugefügt oder gelöscht werden.

- Das Polynom kann einfach geändert werden. Gleich bleiben muss nur a_0. Bei häufiger Änderung erhöht dies die Sicherheit.

- Indem mehrere Wertepaare an einen Teilnehmer vergeben werden, kann eine hierarchische Struktur erreicht werden.

SECRET SHARING MADE SHORT

- Bekannt: die Teile eines Geheimnisses müssen immer so groß sein, wie das Geheimnis selbst
- Wann kann diese Grenze erreicht werden?
- Wann muss sie überschritten werden?

- Problem: ineffizient, wenn das Geheimnis groß ist

- Wie kann man die „Teilgeheimnisse“ verkürzen? (→ Effizienzverbesserung)

  (dargestellt in einem Paper von Krawzyk)

- Zuerst zu klären: Wie sicher soll das Geheimnis geschützt sein?
  - **Informationstheoretisch sicher**

    → egal wie viel Rechenzeit investiert wird, aus weniger als k Teilen kann das Geheimnis nicht wieder hergestellt werden

  - **Rechnerisch sicher**

    → mit exponentiellem Aufwand (daher sehr unwahrscheinlich) könnte das Geheimnis auch aus weniger als k Teilen errechnet werden

ZIEL VON KRAWZYKS PAPER

- Verkleinerung der Teilgeheimnisse
- Realisierung eines:
  - einfachen, praktischen und sicheren Schemas, das ein sicheres, symmetrisches Kryptosystem voraussetzt (eine Einweg-Funktion)
    - Einweg-Funktion: Komplexitätstheoretisch ist diese Funktion schwer umzukehren (die Berechnung der Inversen einer Funktion erfolgt nicht in Polynomialzeit)
  - zusätzlich robusten Schemas, das begrenzt die Veränderung der Teilgeheimnisse tolerieren kann

K-SCHWELLWERT-SCHEMA

- Das Geheimnis D wird in n Teile geteilt, von denen k zur Rekonstruktion benötigt werden:
  jedes Teil D_i hat die Größe $\frac{|D|}{k}$ plus eine kurze Information, die nicht von der Geheimnisgröße, sondern von den Sicherheitsparametern abhängt.

- In diesem Fall ist die Grenze optimal, wenn das Geheimnis mit k Teilen rekonstruierbar sein soll.

BEISPIEL FÜR DIE ANWENDUNG

- Gegeben:
  - 5 Server, die sich eine Datenbank mit geheimen Informationen teilen
  - Es sollen immer mindestens 3 Server gleichzeitig Informationen abrufen können
- Mit einem regulären Geheimnisteilungs-Schema würde die Größe der auf jedem Server zu speichernden Informationen gerade der gesamten Datenbank entsprechen.
- Mit dem neuen Schema muss auf jedem Server nur noch 1/3 der Datenbank gespeichert werden.
- Die Menge der Daten nimmt dann nur um 66%, anstatt um 400% zu.

- Weitere Anwendung im Bereich der sicheren Übertragungen von Mitteilungen
  - Zwei Parteien wollen in einem unvollständigen Netzwerk kommunizieren; sie wissen, dass ein Teil dieses Netzwerks von einem Feind kontrolliert wird.
  - Gibt es n unterschiedliche Wege zwischen den beiden Parteien, so kann ein Schwellwert-Schema verwendet werden, um die Nachricht „möglichst" sicher zu übertragen.
  - Kosten liegen im Berechnen, Übertragen und Speichern dieser Teilstücke.

RECHNERISCHE GEHEIMNISTEILUNG (COMPUTATIONAL SECRET SHARING)

- Gegeben (k,n)-Schwellwert-Schema
- 2 Prozesse:
  - Verteilungsprozess:
    - Input: Geheimnis D
    - Aufteilung in n Teile ($D_1,\dots D_n$)
    - private /geheime Verteilung an die Teilnehmer
  - Rekonstruktionsprozess:
    - Input: mind. k Teilstücke
- $A(D) = \{D_1,\dots D_n\}$

A: ein Geheimnisteilungs-Algorithmus

SICHERE VERSCHLÜSSELUNGSSYSTEME

- Definition:

  Eine Verschlüsselungsfunktion ENC ist sicher, wenn ein Paar Geheimnisse D‘ und D‘‘ derselben Länge polynomiell ununterscheidbar sind

- Polynomiell ununterscheidbar:

  Zwei Verteilungen sind nicht unterscheidbar, so lange einem nur polynomielle Ressourcen zur Verfügung stehen.

  (z.B. polynomiell viel Rechenzeit, Speicherplatz,...)

KRAWCZYK‘S SCHWELLWERT-SCHEMA

- Gesucht:

Speicherplatzeffizientes Geheimnisteilungs-Schema

- Idee: Kombination aus
  1. Informationsverbreitungs-Schema
     (information dispersal scheme)
  2. Sicheres Verschlüsselungs-Schema
     (secure enryption function)
  3. Perfektes Geheimnisteilungs-Schema
     (perfect secret sharing scheme, z.B. Shamir)

KRAWCZYK‘S SCHWELLWERT-SCHEMA

- Verteilung:
  1) Wähle einen Schlüssel K. Verschlüssle das Geheimnis D mit der Funktion ENC und dem Schlüssel K. $E = ENC_K(D)$
  2) Benutze IDA, um die verschlüsselte Datei in n Teile aufzuteilen.
  3) Benutze PSS, um n Teile des Schlüssels K herzustellen.
  4) Sende an jeden Teilnehmer P_i , $i = 1, 2,..n$ das Teilgeheimnis $D_i = (E_i , K_i)$.

IDA: information dispersal algorithm

ENC: private key encryption function

PSS: perfect secret sharing scheme

KRAWCZYK'S SCHWELLWERT-SCHEMA

- Rekonstruktion:
  1) Sammle die Teilstücke $D_i = (E_i, K_i)$ von k Teilnehmern.
  2) Rekonstruiere E aus E_{i_j}, j= 1, …, k mit IDA.
  3) Nutze PSS, um K aus K_{i_j}, j= 1, …, k zu rekonstruieren.
  4) Entschlüssle E mit Hilfe von K um D zu rekonstruieren.

- Länge der Teilstücke D_i ist $\frac{|D|}{k} + |K|$

  (Annahme: jeder Teilschlüssel von K ist genauso lang wie K, gegeben wenn log (n) < |K|)

ROBUSTE GEHEIMNISTEILUNG

- Gesucht: ein Schema, das ein Geheimnis rekonstruieren kann, auch wenn ein paar der Teilstücke manipuliert wurden.

- Anwendung eines Schwellwert-Schemas mit ein paar Modifikationen:
  - t: Obergrenze der Anzahl manipulierter Teile

    Es gilt: $t < k$, $k \leq n - t$
  - $\rightarrow 2t < n$

- Jede Teilmenge von n, die mindestens k nicht manipulierte Teilstücke enthält, kann D rekonstruieren.

- Authentifizierung durch Signatur des Erstellers

WEITERFÜHRENDE ASPEKTE

- Zugangsstrukturen
  - Kann die Speicherplatz-Effizienz auch auf generellere Schemata ausgeweitet werden?
- Überprüfbare Geheimnisteilung
  - Was passiert, wenn der Geheimnisteiler korrupt ist?
  - Wie lässt sich dies verhindern?

QUELLEN

- “How to share a secret” by A. Shamir [Sha79]
- „Secret sharing made short” by H. Krawczyk [Kra94]
- Wikipedia:
  - http://en.wikipedia.org/wiki/Secret_sharing
  - http://de.wikipedia.org/wiki/Secret_Sharing
  - http://en.wikipedia.org/wiki/Lagrange_polynomial