IP Multicast

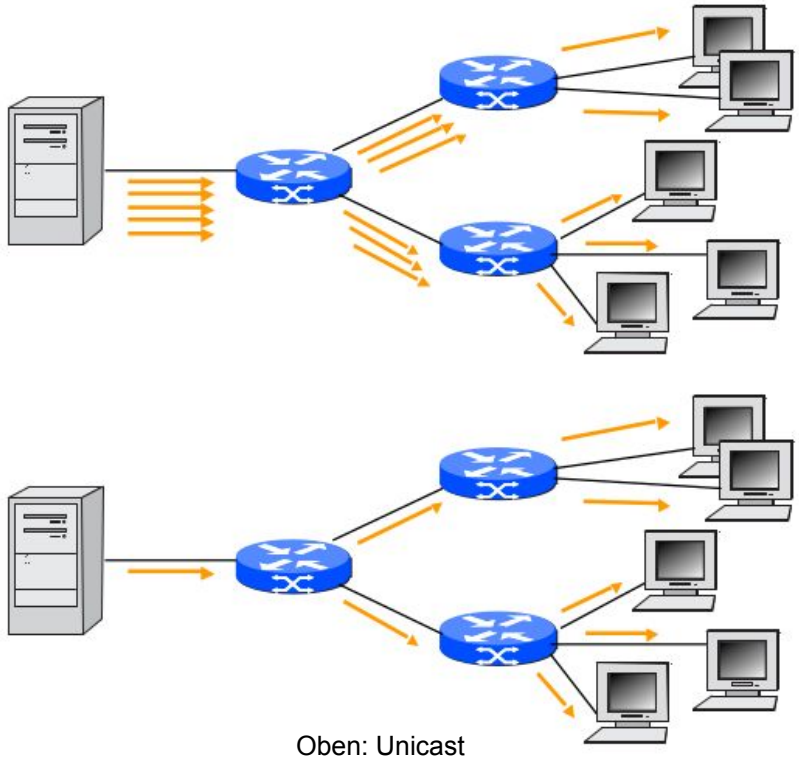
Kryptographie

Julian Götz, Philipp Kleinhenz

31.01.2019

IP Multicast

- Technik zum effizienten Senden von Nachrichten
- Weiterleitende Router duplizieren Nachrichten
- Transport per UDP
    - Reliable Multicast



Oben: Unicast
Unten: Multicast [1]

IP Multicast

- Unterschied zu normalen IP-Paketen liegt in Zieladresse
  - reservierte IP-Adressbereiche 224.0.0.0 bis 239.255.255.255
  - Adressen sind Gruppen von Hosts
- Empfangen von Nachrichten: Anmeldung in Gruppe nötig
- Inhalt lässt sich mit bekannten Verfahren verschlüsseln

- Problem: Schlüsselaustausch
  - Diffie-Hellman nur für zwei Teilnehmer definiert

Zentralisierte Schlüsselvereinbarung

- Zentrale Einheit zuständig für
  - Schlüsselvereinbarung
  - Aufnahme und Ausschluss von Teilnehmern
- Conditional Access Systeme
  - Beispiel Pay-TV: nur zahlende Kunden dürfen Programm empfangen
- Logical Key Hierarchy (IETF)
  - **Group Controller und Key Server** als zentrale Einheit
  - Verschlüsselung der Daten mittels **Traffic Encryption Key (TEK)**

Zentralisierte Schlüsselvereinbarung

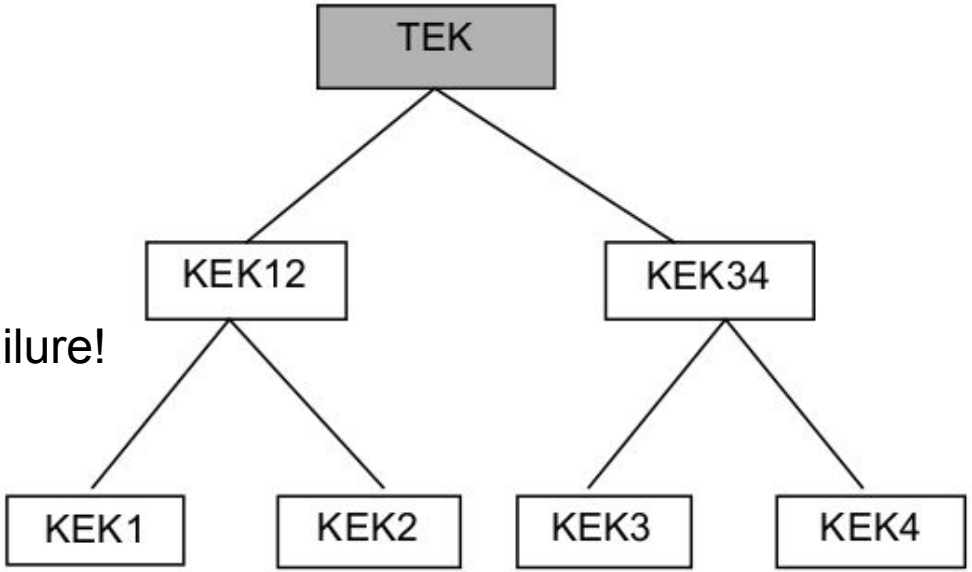
- Übertragen der Traffic Encryption Keys (**TEK**)
  - Teilnehmer: individuelle **Key Encryption Keys (KEK)**
  - Zusammenfassung der Teilnehmer zu **Gruppen** mit **Gruppenschlüsseln**
    - **Gruppenschlüssel** ergibt sich aus KEKs
  - **TEK** wird mit allen **Gruppenschlüsseln** verschlüsselt
    - Teilnehmer entschlüsseln **Gruppenschlüssel** mit **KEK**

- Bei Ausschluss von Bob:
  - **Gruppenschlüssel** wird nicht mehr mit Bob’s **KEK** verschlüsselt
  - Bob kann nicht mehr Gruppenschlüssel entschlüsseln

Zentralisierte Schlüsselvereinbarung

- Logical Key Hierarchy (LKH)
  - binäre Schlüsselhierarchie
  - Nutzung bei dynamischen Gruppen

- Zentralisierung: Single Point Of Failure!



Logical Key Hierarchy [1]

PSA:

“Die modulo p-Reduktionen wurden der leichteren Lesbarkeit halber weggelassen, sind aber in jedem Rechenschritt vorzunehmen.” [1]

Diffie-Hellman Schlüsselaustausch

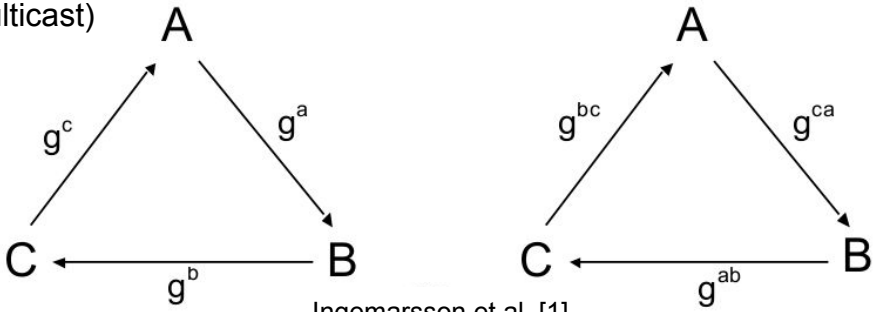
$$g^{f(a,b)} = g^{a \cdot b} = g^{b \cdot a} = g^{f(b,a)}$$

- kurze Wiederholung (s. Vorlesung/Skript):
  - asymmetrische Schlüsselvereinbarung
  - Alice & Bob:
    - vereinbaren gemeinsame Zahl g (z.B. Primzahl)
    - Alice an Bob: g^a
    - Bob an Alice: g^b
    - Alice berechnet Schlüssel: $K_A = (g^b)^a = g^{ab}$
    - Bob berechnet Schlüssel: $K_B = (g^a)^b = g^{ab}$
    - Gemeinsamer Schlüssel: $K = K_A = K_B$
  - symmetrisch verschlüsselte Kommunikation

Generalisierung: Diffie-Hellman für Gruppen (3+)

$$g^{f(a,b)} = g^{a \cdot b} = g^{b \cdot a} = g^{f(b,a)}$$

- **Ingemarsson, Tang und Wong** [2]
  - Eigenschaft von f: Symmetrisch → Permutierbar
  - $a \cdot b \cdot c = a \cdot c \cdot b = \ \ldots \ = c \cdot b \cdot a$
  - Teilnehmer A exponiert gemeinsame Zahl mit privatem Schlüssel: g^a
  - übermittelt Ergebnis an Nachfolger B, erhält Zahl g^n von Vorgänger N
  - exponiert erhaltene Zahl mit privatem Schlüssel: $\left(g^n\right)^a = g^{na}$
  - Wiederholung bis jeder Teilnehmer Gruppenschlüssel $g^{ab\ldots n}$ berechnet hat
  - Insgesamt $n \cdot (n-1)$ Nachrichten in $n-1$ Runden
  - (Alternativ: in jedem Schritt an alle Teilnehmer via Multicast)



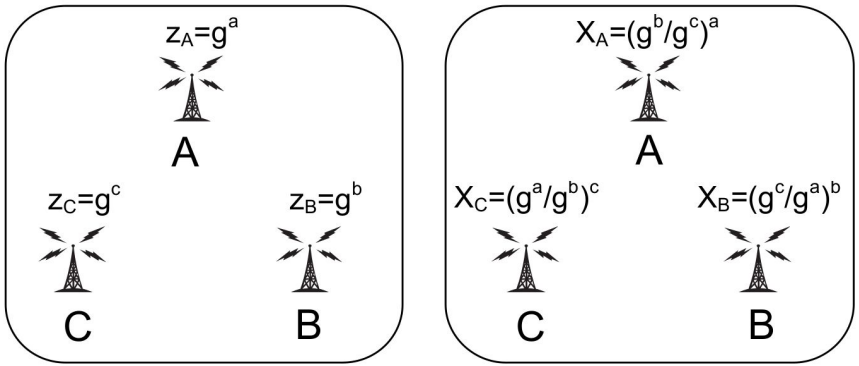
Ingemarsson et al. [1]

Generalisierung: Diffie-Hellman für Gruppen (3+)

$$g^{f(a,b)} = g^{a \cdot b} = g^{b \cdot a} = g^{f(b,a)}$$

- **Burmester und Desmedt** [3]
  - Eigenschaft von f: Zyklisch → Rotierbar
  - $ab + bc + ca = ca + ab + bc = bc + ca + ab$
  - Teilnehmer A exponiert gemeinsame Zahl mit privatem Schlüssel: g^a
  - übermittelt Ergebnis an Vorgänger N und Nachfolger B, erhält g^n und g^b
  - potenziert Quotient aus Vorgänger- und Nachfolgerzahl: $(g^b / g^n)^a$
  - übermittelt Ergebnis an alle Teilnehmer
  - Gruppenschlüssel (3 Teilnehmer A B C):

$$\begin{aligned} K_A &= (g^c)^{3a} \cdot (g^b/g^c)^{2a} \cdot (g^c/g^a)^b \\ &= g^{3ca} \cdot g^{2ab-ac} \cdot g^{cb-ab} \\ &= g^{3ca+2ab-2ac+cb-ab} \\ &= g^{\mathbf{ab+bc+ca}} \\ &= K_B = K_C \end{aligned}$$



Burmester-Desmedt [1]

  - Multicast: Insgesamt $2n$ Nachrichten in 2 Runden (vgl. ITW: $n^2 - n$)

IKA und AKA

- IKA - Initial Key Agreement
  - wie zuvor: Schlüsselvereinbarung innerhalb einer Gruppe mit allen Teilnehmern

- AKA - Auxiliary Key Agreement
  - Ausschluss und Aufnahme neuer Teilnehmer
  - Vereinigen und Teilen von Gruppen
  - **Optimierung**sverfahren: nicht jeder Teilnehmer muss neuen Schlüssel generieren!

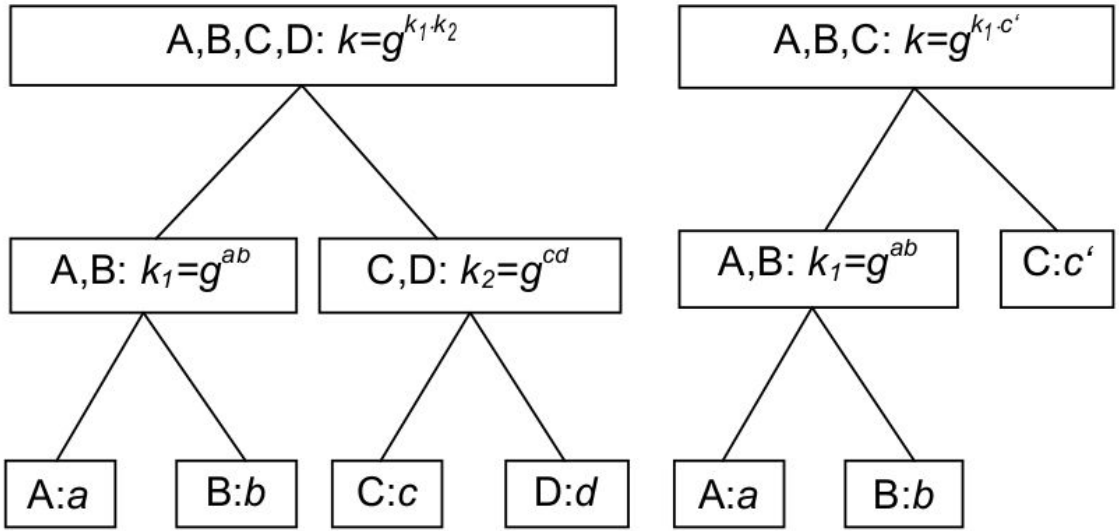
IKA und AKA: Burmester-Desmedt Protokoll

- IKA: Group Controller
  - ein Teilnehmer behält alle erhaltene Zahlen
  - wird im folgenden AKA benötigt
- AKA: Aufnahme eines Teilnehmers (Ausschluss ineffizient, stattdessen IKA)
  - Anzahl Runden, wie zuvor: 2
  - Anzahl Nachrichten: $\mathbf{5}$ (vgl. IKA: $2n$, d.h. in jedem Fall bei $3+$ Teilnehmern: $5 < 2n$)
  - Gruppe $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C})$, neuer Teilnehmer $\boldsymbol{D}$ zwischen $\boldsymbol{C}$ und $\boldsymbol{A}$, folgende Nachrichten:
    - $\boldsymbol{D}$ an alle: g^d
    - $\boldsymbol{D}$ an alle: $\left(g^a / g^c\right)^d$
    - Nachfolger $\boldsymbol{A}$ an alle: $\left(g^b / g^d\right)^a$
    - Vorgänger $\boldsymbol{C}$ an alle: $\left(g^d / g^b\right)^c$
    - Group Controller an $\boldsymbol{D}$: Zahlen von nicht-Nachbarn

    Neuer Gruppenschlüssel kann nun von allen berechnet werden

Iterierter Diffie-Hellman Schlüsselaustausch

- Geeignet bei dynamischen Gruppen
- Kombination Diffie-Hellman mit Binärbäumen der Logical Key Hierarchy
- Iteratives Einsetzen des Diffie-Hellman Schlüsselaustauschs



Iterierter Diffie-Hellman Schlüsselaustausch [1]

Iterierter Diffie-Hellman Schlüsselaustausch

- gemeinsamer Schlüssel wird Gruppenschlüssel
- Vereinbarung mehrerer Gruppen: ein Teilnehmer pro Gruppe muss aktiv sein

Iterierter Diffie-Hellman Schlüsselaustausch

- Verwendung im **AKA**

Quellen

[1] J. Schwenk, “Sicherheit und Kryptographie im Internet”. Wiesbaden: Springer Vieweg, 2014. ISBN 978-3-658-06543-0.

[2] I. Ingemarsson, D. Tang und C. Wong, “A conference key distribution system”, *IEEE Transactions on Information Theory*, vol. 28, no. 5, S. 714-720, 1982. DOI 10.1109/tit.1982.1056542.

[3] M. Burmester und Y. Desmedt, “A secure and efficient conference key distribution system”, *Advances in Cryptology - EUROCRYPT'94*, S. 275-286, 1995. DOI 10.1007/bfb0053443