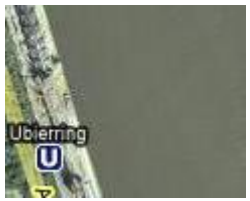
Das Teilen von Geheimnissen (Secret Sharing)

Prof. Dr. Wolfgang Konen
FH Köln

Fachhochschule Köln
University of Applied Sciences Cologne

Aktivierung / Motivation



- Aktivierung: Piraten, Schatzkarte …
  - Nachteile beim Durchreißen Schatzkarte:
    Ein Teil verrät bereits viel (alles?) über den Schatz

- Ernsteres Problem: Sicherheitscode für Aktivierung
  Atombomben (hoffentlich!) auf N Personen verteilt
  - Wieviel wissen N-1 Personen bereits über Geheimnis?
  - Was passiert, wenn 1 aus N stirbt / verschwindet?
  - Prozessorientierte Fragen (behandeln wir hier nicht)
    - Was ist mit dem, der den Code verteilt hat?

Fragestellungen Secret Sharing

1. Wie kann ich ein Geheimnis / einen Zugang so auf N Personen aufteilen, dass …
   - … das Geheimnis rekonstruiert werden kann, wenn alle N zusammenkommen
   - … nichts / wenig über das Geheimnis bekannt wird, wenn N-1, N-2, … , 2, 1 Personen zusammenkommen

2. Wie kann ich ein Geheimnis / einen Zugang so auf N Personen verteilen, dass …
   - … bereits K aus N das Geheimnis rekonstruieren können
   - … nichts / wenig über das Geheimnis bekannt wird, wenn K-1, K-2, … , 2, 1 Personen zusammenkommen

Fragestellungen (2)

- Welches Problem löst die 2. Fragestellung?
  - Das Problem, dass Geheimnis nicht verlorengeht, wenn N-K der N Personen ausfallen.
  - Anwendungsfall: Internet-Sicherheitspasswort über **N multiple Server** verteilen.
    - Beispiel: N=10, K=8
    - Auch wenn 1,2=N-K der multiplen Server ausfallen, kann sich der Hauptserver noch das Geheimnis verschaffen
    - Trotzdem ist der Einbruch von Hackern auf 1,2,…,7=K-1 der multiplen Server noch nicht kompromittierend
  - Wir nennen solche Verfahren **K-aus-N-Verfahren**

Lösungsraum / Lösungen für N-aus-N

- Beim Tresor: N Schlüssel bzw. N Vorhängeschlösser:



….

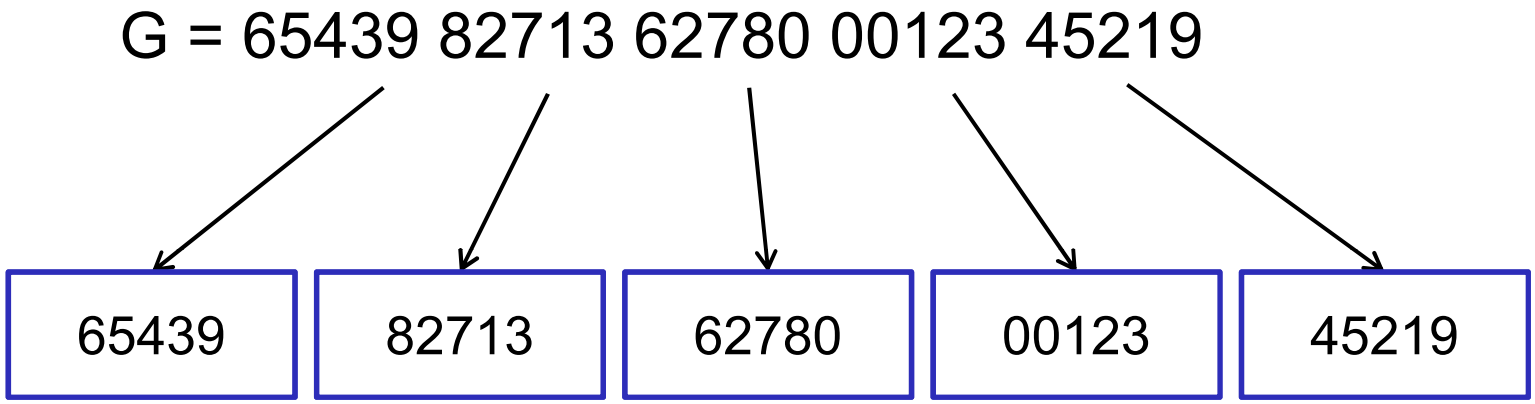

- Diskrete Mathe / Kryptographie
  - Geheimnis = Zahl G (möglicherweise sehr lang)
  - Beispiel:

G = 65439 82713 62780 00123 45219

- Wir beschäftigen uns im Folgenden nur mit den Zahl-Lösungen

(K)eine Lösung

- Aufteilen von G auf N=5 Person:



  - Warum keine Lösung?
    - Wenn 4 Personen zusammenkommen, gibt es nur noch 10^5 statt 10^{25} Möglichkeiten für Geheimnis G >> leicht zu knacken
    - Allgemeiner: Der Raum für G wurde auf den Anteil $10^5/10^{25} = 1/10^{20}$ des ursprünglichen Raums eingeschränkt >> dramatische Reduktion!

Bessere Lösung: Summe

- Verteile Geheimnis G=129 auf N=5 Personen, indem jeder eine Zahl $\in \mathbf{Z}_{40}$ erhält, sodass die Summe G ergibt.
  - Beispiel: 17+32+39+11+30 = 129
- Um wieviel wird der Raum für G eingeschränkt, wenn N-1=4 Personen zusammenkommen?
  - Minimalzahl für G ist 0
  - Maximalzahl für G ist (40-1)·5 = 195
  - Wenn die Personen 1,…4 zusammenkommen, ist 17+32+39+11 = 99. G kann also nur 99,…,138 sein
  - Im Allgemeinen wird der Raum für G auf den Anteil $40/[(40-1)\cdot N] \approx 1/N$ eingeschränkt >> deutliche Reduktion

(Noch) Bessere Lösung: Summe mod m

- Algorithmus, um Geheimnis G auf N Personen zu verteilen
  - Wähle Modul m mit m>G und N-1 zufällige Zahlen $t_1,\ldots,t_{N-1} \in \mathbf{Z}_m$ für Personen 1,2,…,N-1
  - Berechne $R = (t_1+\ldots+t_{N-1}) \bmod m$
  - Die Zahl für die N. Person ist $t_N=(G-R) \bmod m$
- Wieso richtig?
  - $t_1+\ldots+t_{N-1}+t_N = R + (G-R) = G \pmod m$
- Um wieviel wird der Raum für G eingeschränkt, wenn N-1 Personen zusammenkommen?

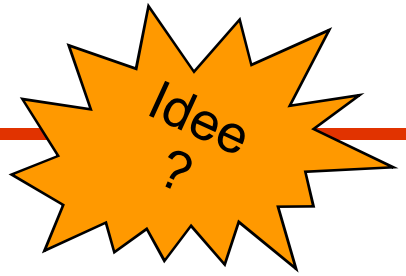
(Noch) Bessere Lösung: Summe mod m

- Um wieviel wird der Raum für G eingeschränkt, wenn N-1 Personen zusammenkommen?
  - Gar nicht!
  - Denn:
    - Wenn G=R, ist t_N=0 die richtige Zahl
    - Wenn G=R+1, ist t_N=1 die richtige Zahl

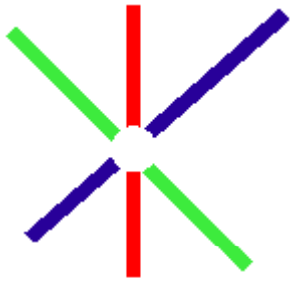
      ...
    - Wenn G=m-1, ist t_N=G-R-1 die richtige Zahl
    - Wenn G=0 , ist t_N=G-R die richtige Zahl, usw.

      ...
    - Wenn G=R-1, ist t_N=m-1 die richtige Zahl
  - Insgesamt: Für t_N und G sind alle Zahlen $\in \mathbf{Z}_m$ möglich
  - Wenn N-1 Personen zusammenkommen, ist der Raum für G um NICHTS eingeschränkt (!)

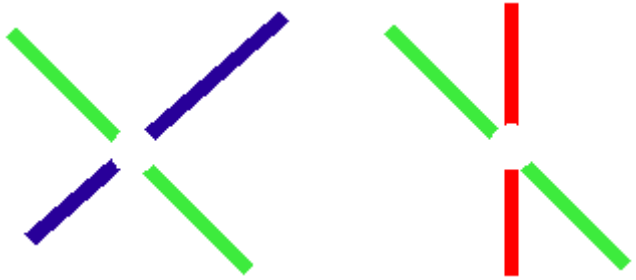
Geheimnis teilen: K-aus-N-Verfahren



- Idee aus Geometrie: 2-aus-N: Geraden in Ebene $\mathbf{R}^2$



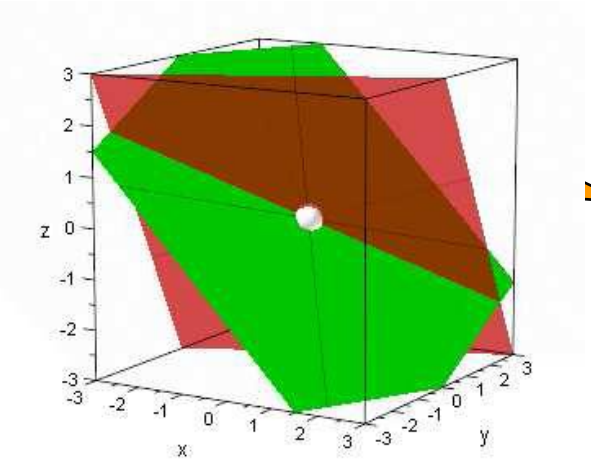
- Jede Person erhält eine Gerade, das Geheimnis ist Schnittpunkt
- Bereits 2 Personen können Geheimnis rekonstruieren:



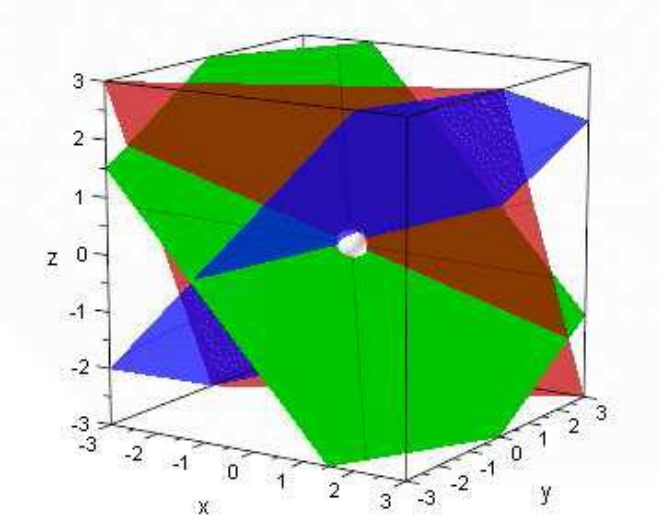
usw.

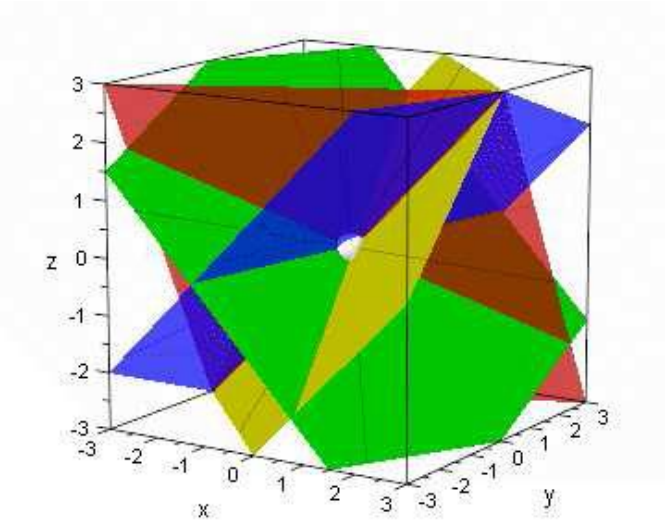
Geheimnis teilen: K-aus-N-Verfahren

Wie verallgemeinern auf 3-aus-N?



- Richtig, Ebenen im Raum $\mathbf{R}^3$
- Jede Person erhält eine Ebene,
  Geheimnis = Schnittpunkt
- Bereits 3 Personen können Geheimnis rekonstruieren:





s. Notizen

Vor- und Nachteil des Geraden-Ebenen - Verfahrens

Vorteil: K-aus-N überhaupt möglich

Welche Nachteile?

- Bereits jeder Teilnehmer (jede Gerade oder Ebene) weiß etwas über Geheimnis, K-1 Teilnehmer wissen noch mehr.
- Beispiel 2 Ebenen im Raum $\mathbf{R}^3$: Wenn die Box die Kantenlänge 10^2 (Gitterpunkte) hat, dann sind initial $10^{2\cdot 3} = 10^6$ Gitterpunkte möglich
- Wenn 2 Personen zusammenkommen, wissen sie, dass Geheimnis auf „ihrer“ Schnittgeraden liegt >> nur noch 10^2 Gitterpunkte
- Reduktion auf Anteil $10^2/10^6 = 1/10^4$ des ursprünglichen Geheimnisraumes
- Allgemein: Bei Kantenlänge L und K Personen ist die Reduktion bei K-1 Personen mindestens L^{1-K}, was besonders für große K erheblich ist

s. Notizen

Shamirs Secret Sharing: Beispiel für K=3

Adi Shamir: das „S“ von RSA, israelischer Kryptologieexperte

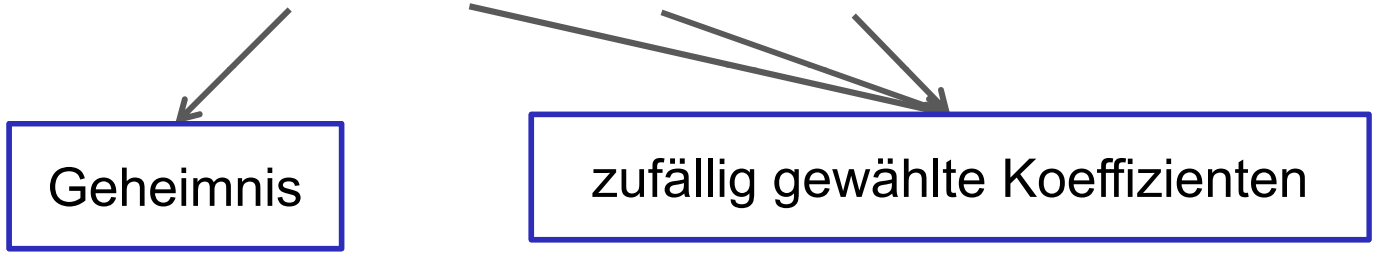
- Shamir legte 1979 ein neues Verfahren vor:
  - das K-aus-N Secret Sharing erlaubt,
  - bei dem K-1 Teilnehmer NICHTS über das Geheimnis erfahren,
  - (auch patentiert).
  - Das Verfahren ist in [1] beschrieben. Ausnahmsweise ein Krypto-Paper, das auch für Nicht-Mathematiker **sehr gut** lesbar ist. Es ist auch nur 2 Seiten lang! (1979 konnte man noch kurze und trotzdem gehaltvolle Paper schreiben.)
  - Weiteres gutes Anwendungsbeispiel: elektronische Überweisung in einer Firma nur nach dem 4,6,8,…,-Augen-Prinzip

Shamirs Secret Sharing

Adi Shamir: das „S“ von RSA

- Idee: Nehme ein Polynom vom Grad K-1, wenn ein Geheimnis unter K Personen geteilt werden soll:

$$f(x) = a_0 + a_1 x + \ldots + a_{K-1} x^{K-1}$$

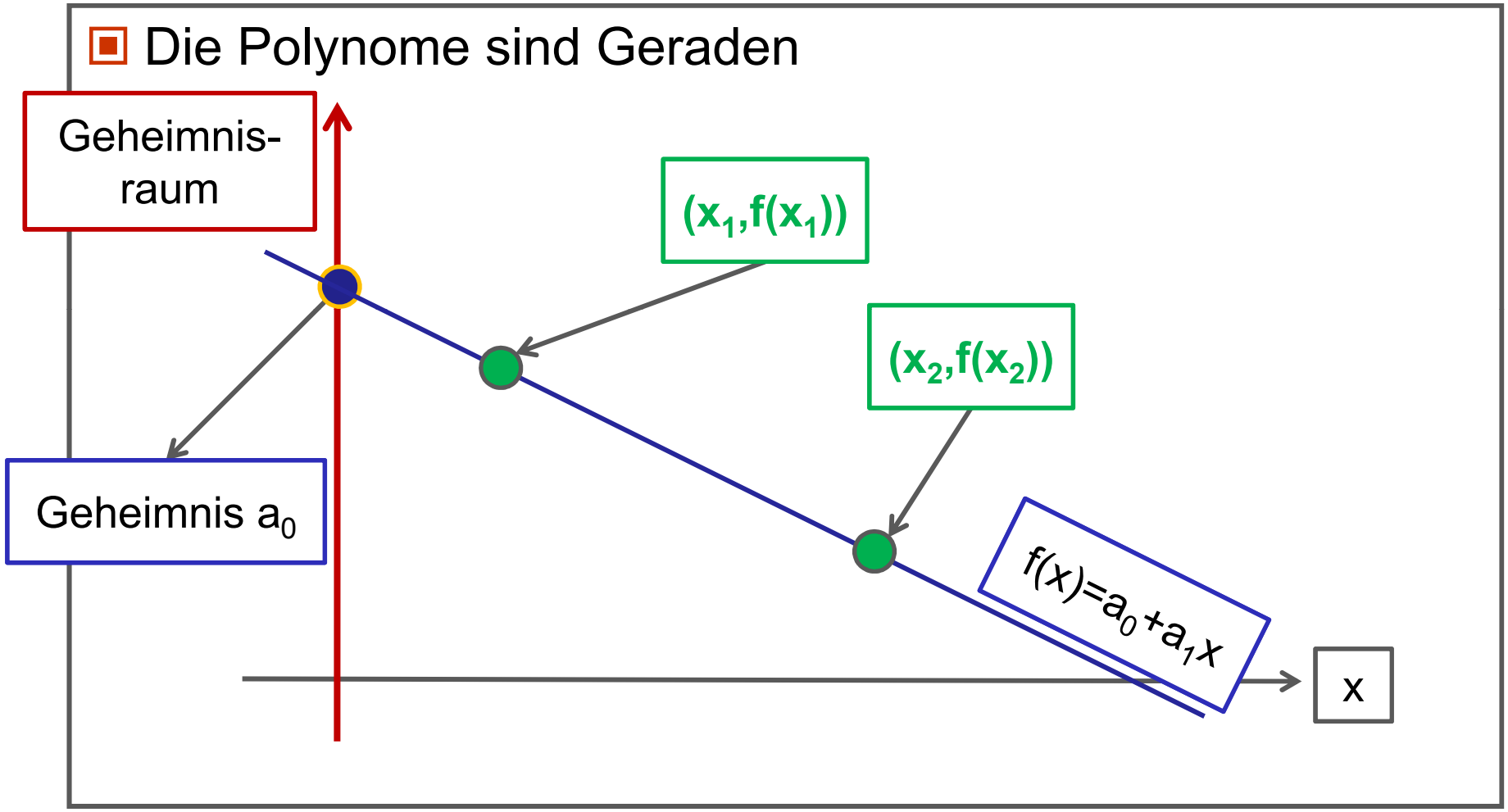


- Ein Polynom vom Grad K-1 ist eindeutig durch beliebige K Punkte festgelegt $\Rightarrow$
- Verteile N Punkte $(x_n, f(x_n))$ an N Personen [n=1,…,N] für ein K-aus-N-Verfahren [1]

[1] Damit wir nicht durch Rundungsfehler gestört werden, rechnen wir nur mit ganzen Zahlen x_n, a_i.

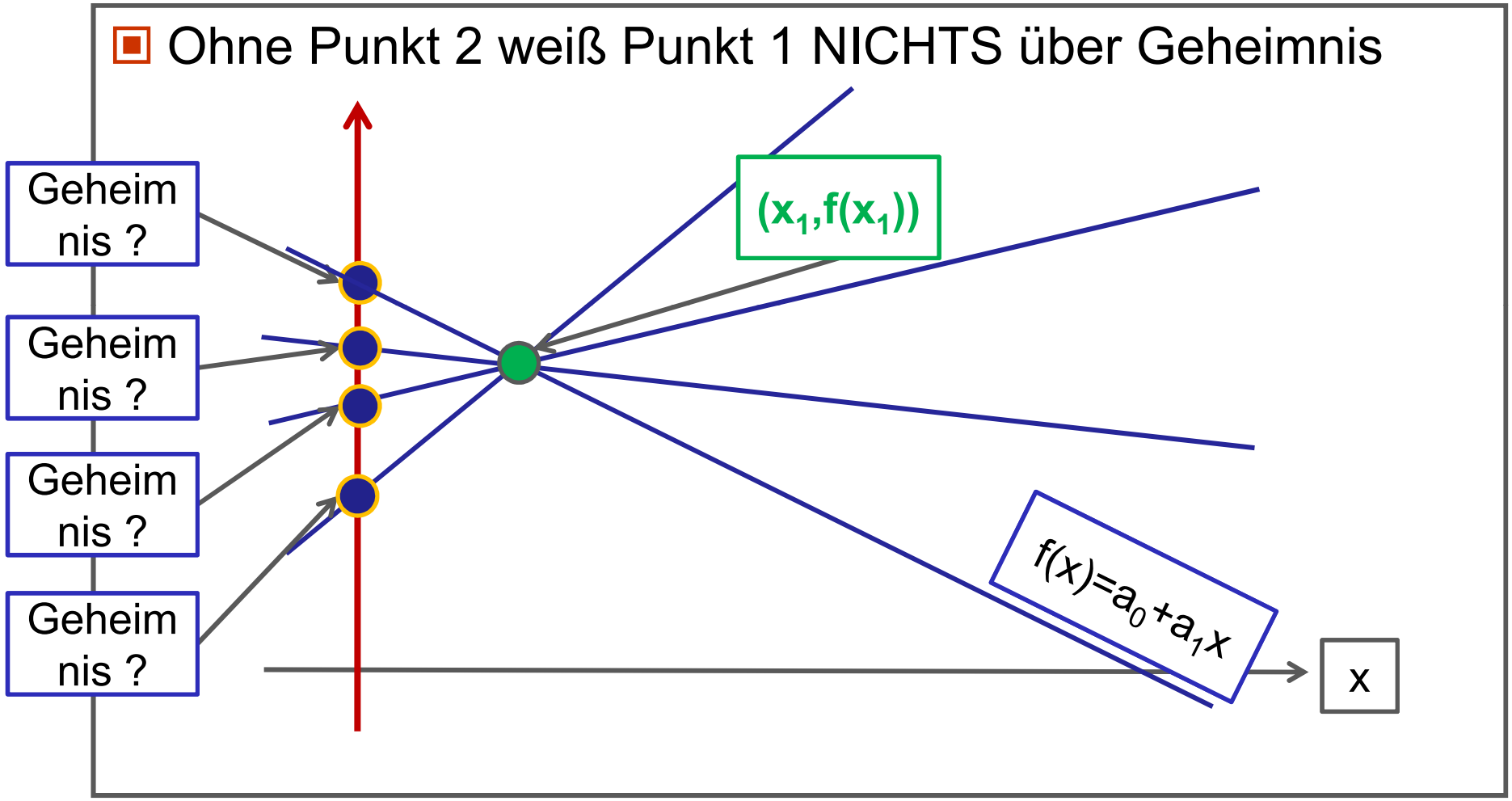
Shamirs Secret Sharing: Beispiel für K=2

Adi Shamir: das „S“ von RSA



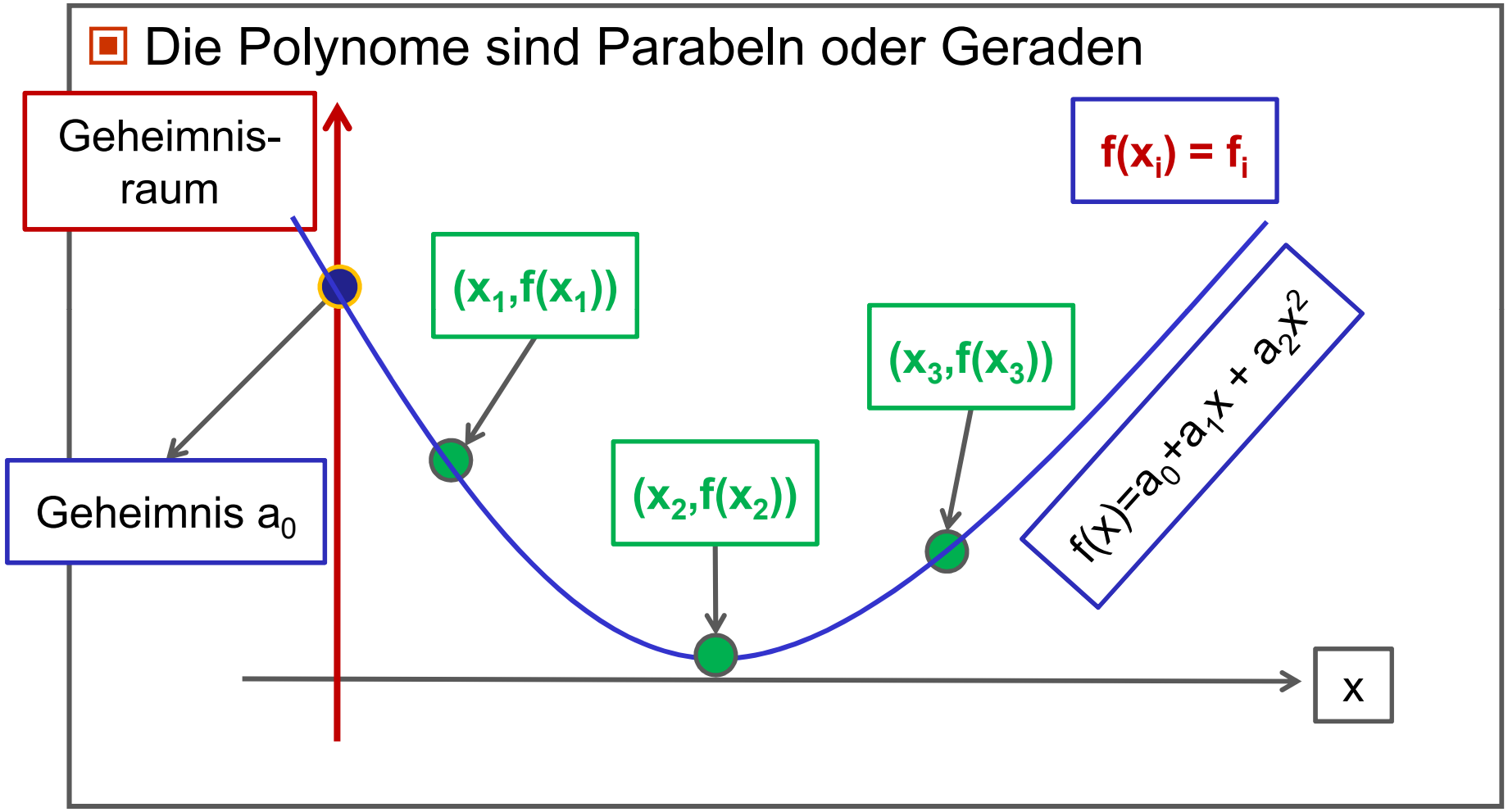
Shamirs Secret Sharing: Beispiel für K=2

Adi Shamir: das „S“ von RSA



Shamirs Secret Sharing: Beispiel für K=3

Adi Shamir: das „S“ von RSA



Shamirs Secret Sharing: Beispiel für K=3

Adi Shamir: das „S“ von RSA

- Wie berechnet man aus den Punkten (x_i, f_i) direkt f(0) ?
- Mit der Lagrange-Interpolationsformel
  (sieht kompliziert aus, ist aber einfach zu programmieren ;-))

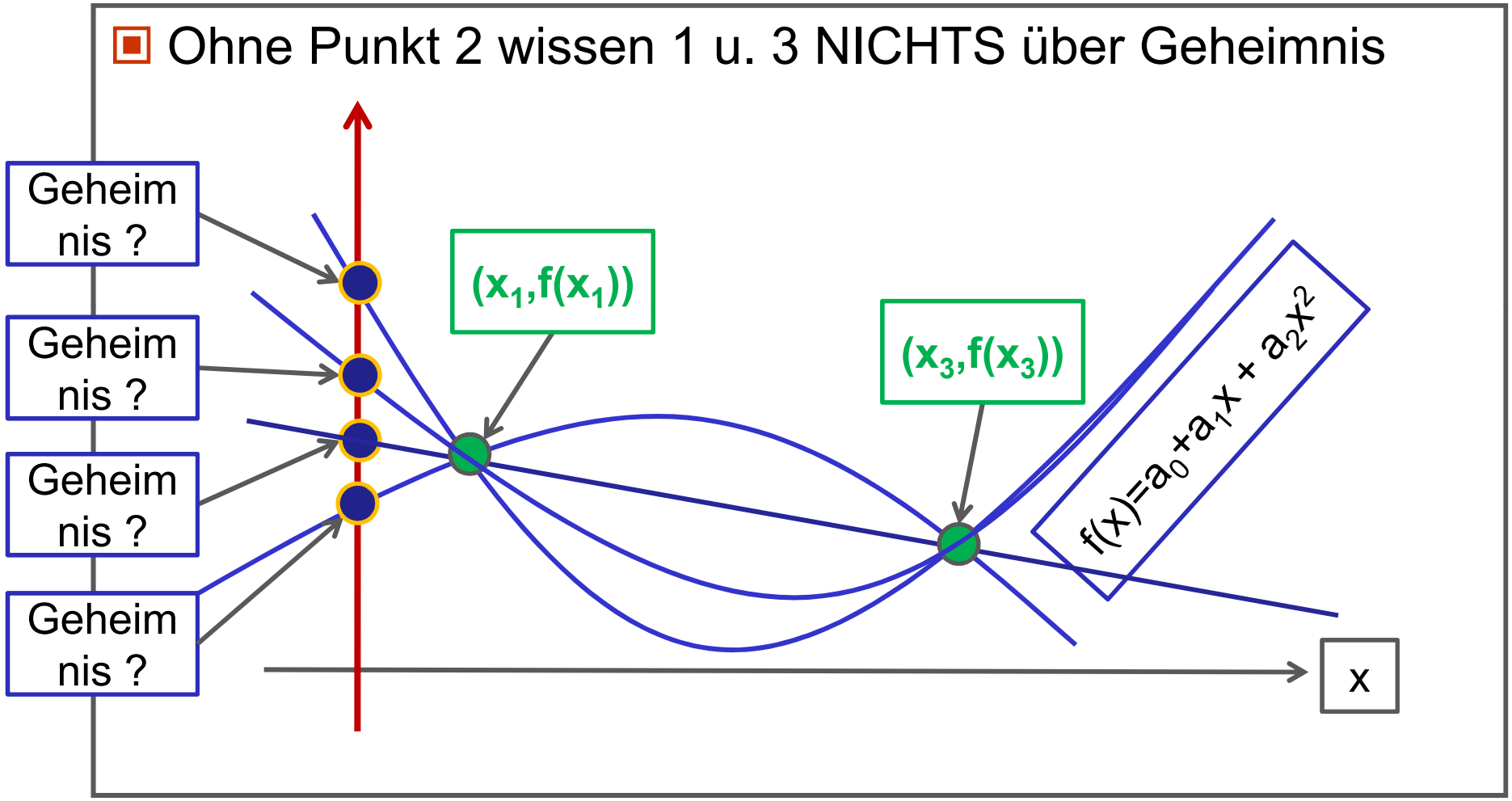
$$f(x) = \sum_{i=1}^{K} f_i \prod_{\substack{j=1,\\ j\neq i}}^{K} \frac{x - x_j}{x_i - x_j}$$

- Spezialfall x=0:

$$f(0) = \sum_{i=1}^{K} f_i \prod_{\substack{j=1,\\ j\neq i}}^{K} \frac{-x_j}{x_i - x_j}$$

Shamirs Secret Sharing: Beispiel für K=3

Adi Shamir: das „S“ von RSA



Shamirs Secret Sharing: Beispiel für K=3

Adi Shamir: das „S“ von RSA

- VORSICHT: Die Aussage, dass 2 von 3 Personen NICHTS über das Geheimnis wissen, gilt im bisher gezeigten Bild noch nicht: In [3] wird gezeigt, dass in einem bestimmten Beispiel aus 2 von 3 Punkten auf $a_0=5k+4$, $k \in Z$, geschlossen werden kann.
- Also Reduktion des Geheimnisraumes um 80% (!)
- Was fehlt?
- Ähnlich wie bei Summe, muss man alle Berechnungen **mod p** durchführen (p: Primzahl)
- Dann ist wahr, dass 2 von 3 Punkten nichts über a_0 verraten (genauer erklärt in [4])

ausführlicher in sss.mw

s. Notizen

Fazit Secret Sharing

- „Summe mod m“ ist gutes und einfaches Verfahren für N-aus-N Secret Sharing
- Shamirs Secret Sharing mit **mod p** ist gutes Verfahren für K-aus-N Secret Sharing
- In beiden Fällen spielt Modulare Arithmetik und damit Diskrete Mathematik eine entscheidende Rolle, damit Teile des Puzzles keinerlei Rückschlüsse auf das Ganze erlauben.

Literatur

(1) Shamir, A.: How to share a secret, Comm. of the ACM, 22, p. 612-613, Nov. 1979.
http://lardbucket.org/blog/wp-content/uploads/2007/10/shamir_how_to_share_a_secret.pdf

(2) Wikipedia (engl.) http://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing
(leider mit einem Fehler im Beispiel, auf Discussion-Page diskutiert >> warum man bei Wikipedia-Beiträgen immer auch weiterlesen sollte!!)

(3) Der (vermeintliche) „Flaw“ (Fehler) von Andy Schmitz
http://lardbucket.org/blog/archives/2007/10/30/a-flaw-in-shamirs-secret-sharing-method/

(4) Die (korrekte) Antwort darauf von A.J. Bromage:
http://andrew.bromage.org/blog/archive/2007/11/shamirs_secret_sharin.html