Visuelle Kryptografie

Kathlén Kohn
Universität Paderborn

4. Februar 2010

Gliederung

- Geheimnisteilung
  - Blakley
  - Shamir
- Visuelle Geheimnisteilung
  - Einführungsbeispiel
  - Definition und Vorgehensweise
  - Beispiele

k aus n Geheimnisteilung

- Geheimnis G auf n Teilnehmer aufteilen
- k Teilnehmer (oder mehr) können G rekonstruieren
- Weniger als k Teilnehmer nicht

- 1979: zwei verschiedene Methoden von Blakley und Shamir

Blakley (3 aus 4)

- G Geheimnis
- $p > G$ Primzahl (allen bekannt)
- u und v Zufallszahlen mod p
- Punkt $Q=(G,u,v)$
- Verteile an Teilnehmer Gleichungen der Form $z=ax+by+c$ für Ebenen durch Q
- a und b zufällig wählen
  $\Rightarrow c \equiv v - aG - bu \pmod{p}$

Blakley (3 aus 4)

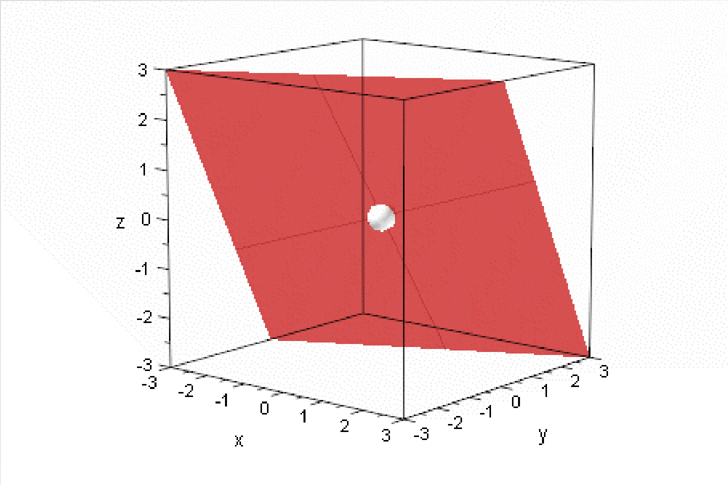
- Bsp.: $G=1$
- Wähle $p=11$, $u=v=2$ => $Q=(1,2,2)$
- $c \equiv v - aG - bu \pmod{p}$
- $a_1=b_1=1$ => $c_1 \equiv 2-1-2 \pmod{11} \equiv 10 \pmod{11}$
- $a_2=b_2=2$ => $c_2 \equiv 2-2-4 \pmod{11} \equiv 7 \pmod{11}$
- $a_3=b_3=3$ => $c_3 \equiv 2-3-6 \pmod{11} \equiv 4 \pmod{11}$
- $a_4=b_4=4$ => $c_4 \equiv 2-4-8 \pmod{11} \equiv 1 \pmod{11}$

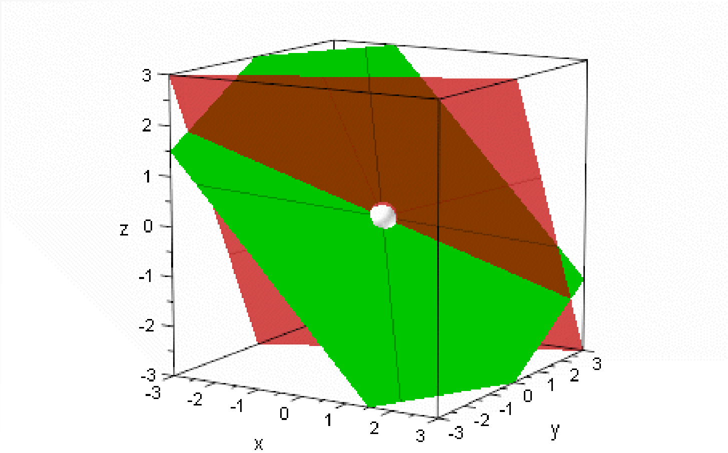
Blakley (3 aus 4)

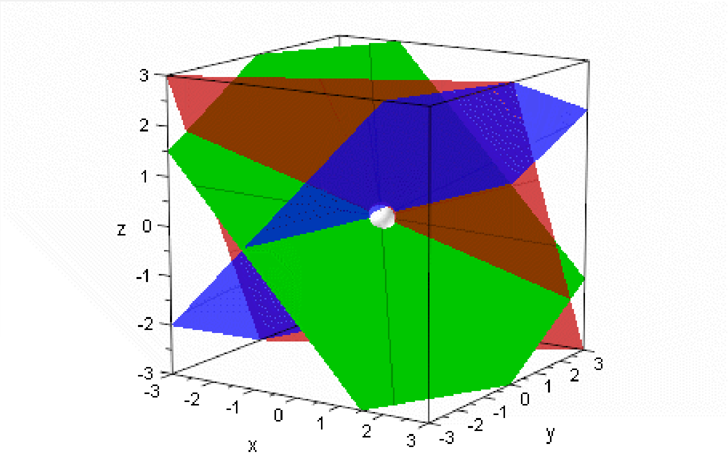
- Alle Rechnungen mod 11
- $z_1 \equiv x+y+10$ $\quad z_2 \equiv 2x+2y+7$

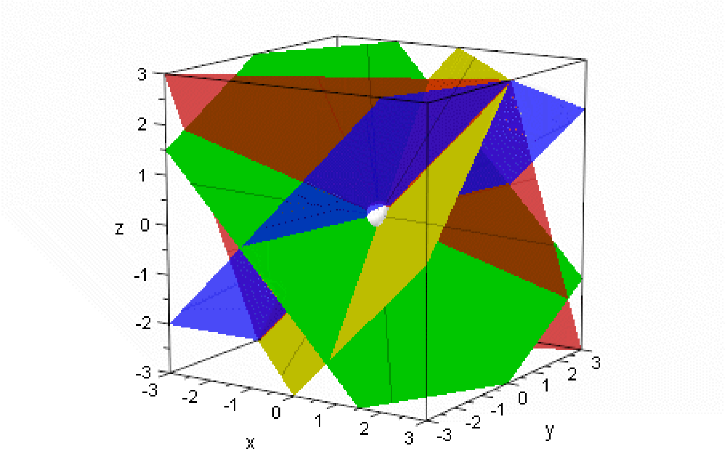
  $z_3 \equiv 3x+3y+4$ $\quad z_4 \equiv 4x+4y+1$
- $z_2 \equiv z_4$: $2x+2y+7 \equiv 4x+4y+1 \;<=>\; x \equiv 10y+3$
- Schon 2 Teilnehmer können die Anzahl der möglichen Werte für G erheblich einschränken!

Blakley (3 aus 4)









Blakley (k aus n)

- k-dimensionalen Raum
- (k-1)-dimensionale Hyperflächen an Teilnehmer verteilen
- Hyperflächen haben gemeinsamen Punkt, dessen erste Koordinate das Geheimnis ist

- Problem: weniger als k Hyperflächen liefern zwar nicht Geheimnis, aber Einschränkung

Shamir (k aus n)

- $p > G$, $p > n$ Primzahl (allen bekannt)
- $s_1, \ldots, s_{k-1}$ mod p unabhängig gleichverteilt gewählt
- $s(x) \equiv G + s_1 x + \ldots + s_{k-1} x^{k-1} \pmod{p}$
- Verteile an Teilnehmer Paare der Form
  $(x_i, s(x_i))$ für $i = 1, \ldots, n$
  aber: $x_i \neq 0$, da $s(0) \equiv G \pmod{p}$
  $x_i \neq x_j$, für alle $i,j = 1, \ldots, n$

Shamir (k aus n)

- s(x) ist Polynom vom Grad k-1

  => wird durch k gegebene Wertpaare (x_i, s(x_i)) eindeutig bestimmt (oBdA seien dies die ersten k: i = 1, ..., k)

- z.B. Lineares Gleichungssystem mit k Gleichungen und k Unbekannten
- z.B. Lagrange-Interpolation:

$$l_i(x) := \prod_{j=1,\, j\neq i}^{k} \frac{x - x_j}{x_i - x_j} \Rightarrow s(x) = \sum_{i=1}^{k} s(x_i)\, l_i(x)$$

Shamir (3 aus 4)

- Bsp.: G=1
- Wähle p=11, $s_1=s_2=2$
  => $s(x)\equiv 1+2x+2x^2 \pmod{11}$
- Verteile an 4 Teilnehmer:
  $(1, s(1)\equiv 5 \pmod{11})$
  $(2, s(2)\equiv 2 \pmod{11})$
  $(3, s(3)\equiv 3 \pmod{11})$
  $(4, s(4)\equiv 8 \pmod{11})$

Shamir (3 aus 4)

- Alle Rechnungen mod 11
- Die ersten 3 Teilnehmer tun sich zusammen
  Wertpaare: (1, 5) (2, 2) (3, 3)
- Gesucht: Koeffizienten von $s(x) \equiv a+bx+cx^2$
  => Erweiterte Koeffizientenmatrix:

$$\begin{pmatrix} 1 & 1 & 1 & 5 \\ 1 & 2 & 4 & 2 \\ 1 & 3 & 9 & 3 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 5 \\ 0 & 1 & 3 & 8 \\ 0 & 2 & 8 & 9 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 5 \\ 0 & 1 & 3 & 8 \\ 0 & 0 & 2 & 4 \end{pmatrix}$$

- c=2, b=2, a=1 => $s(x) \equiv 1+2x+2x^2$ => G=1

Shamir (3 aus 4)

- Wertpaare: (1, 5) (2, 2) (3, 3)
- Lagrange-Interpolation:

$$l_i(x) := \prod_{j=1,\, j\neq i}^{k} \frac{x - x_j}{x_i - x_j} \Rightarrow s(x) = \sum_{i=1}^{k} s(x_i)\, l_i(x)$$

$$l_1(x) = \frac{x-2}{1-2}\,\frac{x-3}{1-3} = \frac{x^2-5+6}{2};$$

$$l_2(x) = -x^2 + 4\mathrm{x} - 3;\; l_3(x) = \frac{x^2-3\mathrm{x}+2}{2}$$

$$\Rightarrow s(x) = 5\,\frac{x^2-5+6}{2} + 2\left(-x^2+4\mathrm{x}-3\right) + 3\,\frac{x^2-3\mathrm{x}+2}{2}$$

$$= 2\mathrm{x}^2 - 9\mathrm{x} + 12 \equiv 2\mathrm{x}^2 + 2\mathrm{x} + 1 \;(mod\; 11)$$

Shamir (3 aus 4)

- Die ersten 2 Teilnehmer tun sich zusammen
  Wertpaare: (1, 5)   (2, 2)
- Gesucht: Koeffizienten von $s(x) \equiv a+bx+cx^2$
  => Aber: 3 Unbekannte lassen sich mit 2
  Gleichungen nicht lösen
- Für k aus n heißt das:
  Bei weniger als k gegebenen Wertpaaren keine Informationen über das Geheimnis bekannt

Shamir (3 aus 4)

- Alle Rechnungen mod 11
- Die ersten 2 Teilnehmer tun sich zusammen
  Wertpaare: (1, 5)   (2, 2)
- Gesucht: Koeffizienten von $s(x) \equiv a+bx+cx^2$
  => Erweiterte Koeffizientenmatrix:

$$\begin{pmatrix} 1 & 1 & 1 & 5 \\ 1 & 2 & 4 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 5 \\ 0 & 1 & 3 & 8 \end{pmatrix}$$

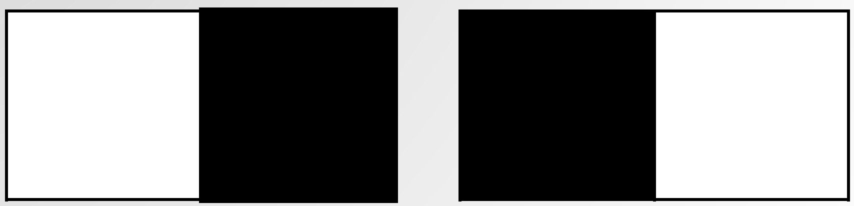
k aus n visuelle Geheimnisteilung

- Adi Shamir und Moni Naor: 1994 „Visual Cryptography"

- Einführungsbeispiel: 2 aus 2
- Teile jeden Pixel in 2 Subpixel:

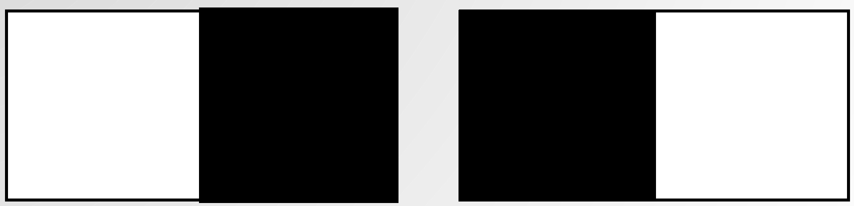
  Schemata:

2 aus 2



- Für weißen Pixel: lege dasselbe Schema übereinander
- Für schwarzen Pixel: lege verschiedene Schemata übereinander

2 aus 2



- Drücke als Boolsche Matrizen aus:

  0: Weiß; 1: Schwarz

  Jede Zeile entspricht Pixel auf einer Folie

- (2 x 2) Matrix W:= $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$

- (2 x 2) Matrix S:= $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

2 aus 2

- H(V): Hamming-Gewicht des Vektors V (Abstand zum Nullvektor)
- W = $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ Hamming-Gewicht einzelner Zeile ist 1
  Hamming-Gewicht der durch oder verknüpften Zeilen ist 1
- S = $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ Hamming-Gewicht einzelner Zeile ist 1
  Hamming-Gewicht der durch oder verknüpften Zeilen ist 2

k aus n visuelle Geheimnisteilung

- pro Pixel:
  - m Subpixel
  - (n x m) Boolsche Matrix $S=(s_{ij})$:

    $s_{ij}=1$ <=> j-tes Subpixel auf i-ter Folie schwarz
- 2 Sammlungen von (n x m) Boolschen Matrizen:
  - C_0 für weiße Pixel
  - C_1 für schwarze Pixel

k aus n visuelle Geheimnisteilung

- H(V): Hamming-Gewicht des Vektors V (Abstand zum Nullvektor)
- $H(V) \geq d$: schwarz ($1 \leq d \leq m$ Grenzwert)
- $H(V) \leq d - \alpha m$: weiß ($\alpha > 0$ relative Differenz)

k aus n visuelle Geheimnisteilung

- 2 Sammlungen von (n x m) Boolschen Matrizen:
  - C_0 für weiße Pixel
  - C_1 für schwarze Pixel
- 3 Bedingungen (Vektor V entsteht durch oder-Verknüpfung von k Zeilen):
  - Für jede Matrix in C_0: $H(V) \leq d-\alpha m$
  - Für jede Matrix in C_1: $H(V) \geq d$
  - Matrizen in C_0 und C_1 auf $q<k$ Zeilen gekürzt
    => ununterscheidbar

2 aus n

- C_0: alle Permutationen der Spalten von

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix} \quad (n \times n)$$

- C_1: alle Permutationen der Spalten von

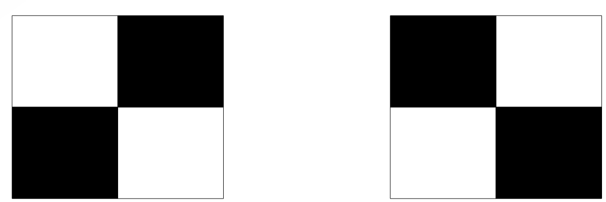
$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \quad (n \times n)$$

2 aus 2

- 4 Subpixel
- Horizontal:

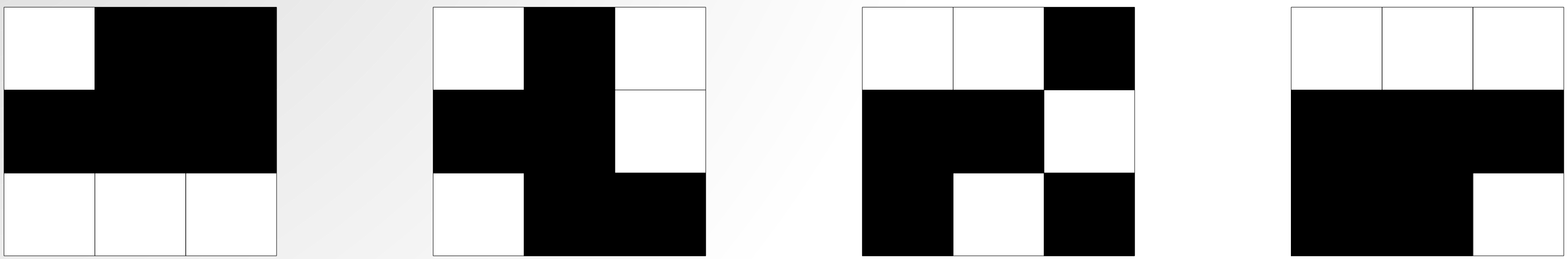
- Vertikal:

- Diagonal:

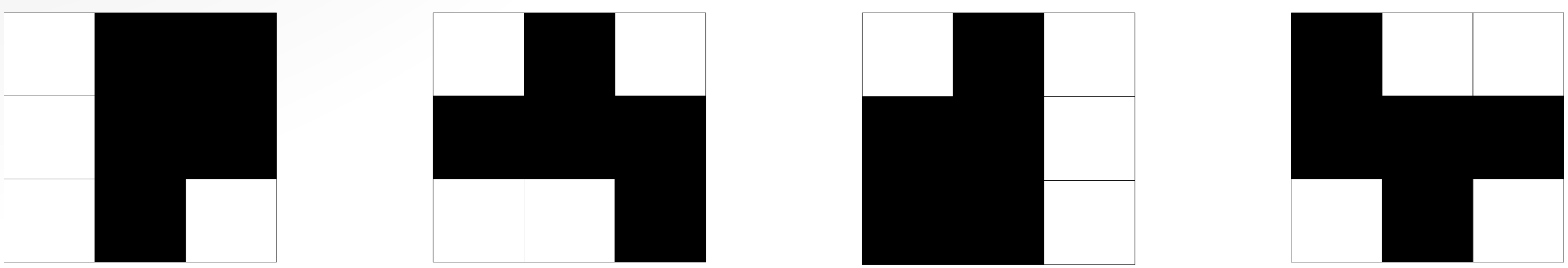


4 aus 4

- Weiß:



- Schwarz:



Quellen

- Moni Naor / Adi Shamir: *Visual Cryptography.* Berlin Heidelberg: Springer-Verlag, 1995
- Wade Trappe / Lawrence Washington: *Introduction to Cryptography with Coding Theory.* Zweite Auflage. New Jersey: Pearson Education, Inc., Pearson Prentice Hall, 2006
- Johannes Blömer: *How to share a secret* in *Algorithmis Unplugged.* Springer Verlag, 2011

k aus k

- 2 Listen von Boolschen Vektoren der Länge k:
  - $J_1^0, J_2^0, \ldots, J_k^0$: k-1 Vektoren linear unabhängig, alle k Vektoren linear abhängig
  - $J_1^1, J_2^1, \ldots, J_k^1$: linear unabhängig
- $(k \times 2^k)$ Matrizen S^0 und S^1, deren Spalten durch alle Boolschen Vektoren der Länge k indiziert werden

k aus k

- $S^t(i, x) := \langle J_i^t, x \rangle$ für alle $i=1, \ldots, k$, $t=0,1$ und alle Boolschen Vektoren x der Länge k
- C_t beinhaltet alle Matrizen, die durch Spaltenpermutation von S^t entstehen