Visuelle Kryptographie

14. April 2013

sublab

sublab

Einordnung

Früher

- Ver- und Entschlüsselung nur manuell, z. B. Skytale und CAESAR-Chiffre
- Vorteil: mit primitiver Technik anwendbar
- Nachteile: nur geringe Datenmengen verschlüsselbar, mit Computer leicht zu knacken

Heute

- Kryptographie i. d. R. maschinell, z. B. RSA auf Chipkarten
- Vorteil: praktisch nicht zu knacken, große Datenmengen verschlüsselbar
- Nachteil: nur mit spezieller, moderner Technik anwendbar

Junges Spezialgebiet *Visuelle Kryptographie*

- Vorteile: praktisch nicht zu knacken, ohne Technik entschlüsselbar
- Nachteile: nur geringe Datenmengen verschlüsselbar

Eurocrypt '94: Moni Naor und Adi Shamir stellen visuelle Kryptographie vor

Grundprinzip

- Klartext und Geheimtext liegen als Grafiken vor
- Klartext wird per Computer verschlüsselt
- Geheimtextteile werden auf transparente Folien gedruckt
- Entschlüsselung durch optische Überlagerung der Folien
- Erkennen des Klartexts durch menschliches visuelles System

Ein Pixel des Klartexts ergibt sich durch optische Überlagerung mehrerer Subpixel der Geheimtextteile. Jedes Klartext-Pixel wird unabhängig von anderen Klartext-Pixeln verschlüsselt. Beispiel 2-von-2-Verschlüsselung:

Geheimtext[0]

OR

Geheimtext[1]

=

Klartext

schwarzes Pixel

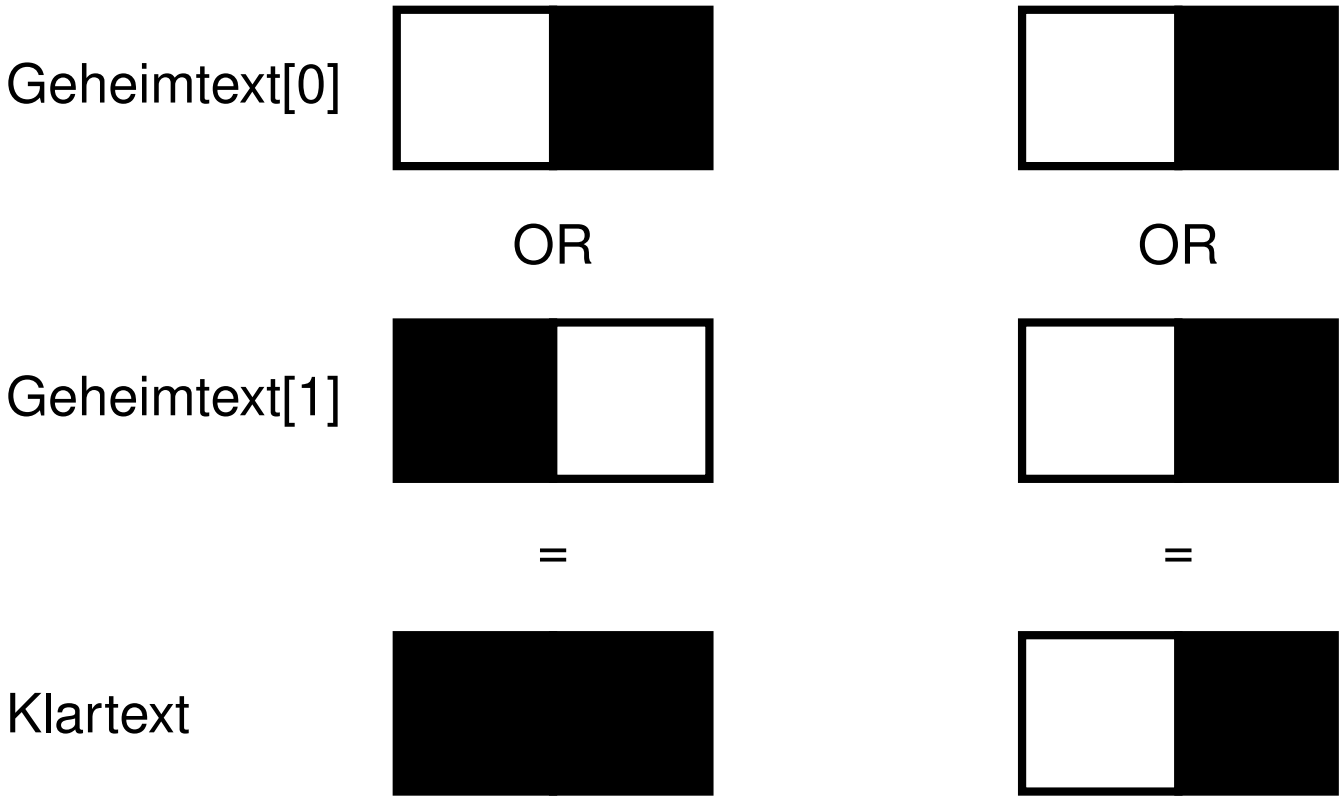
OR

=

»weißes« Pixel

sublab

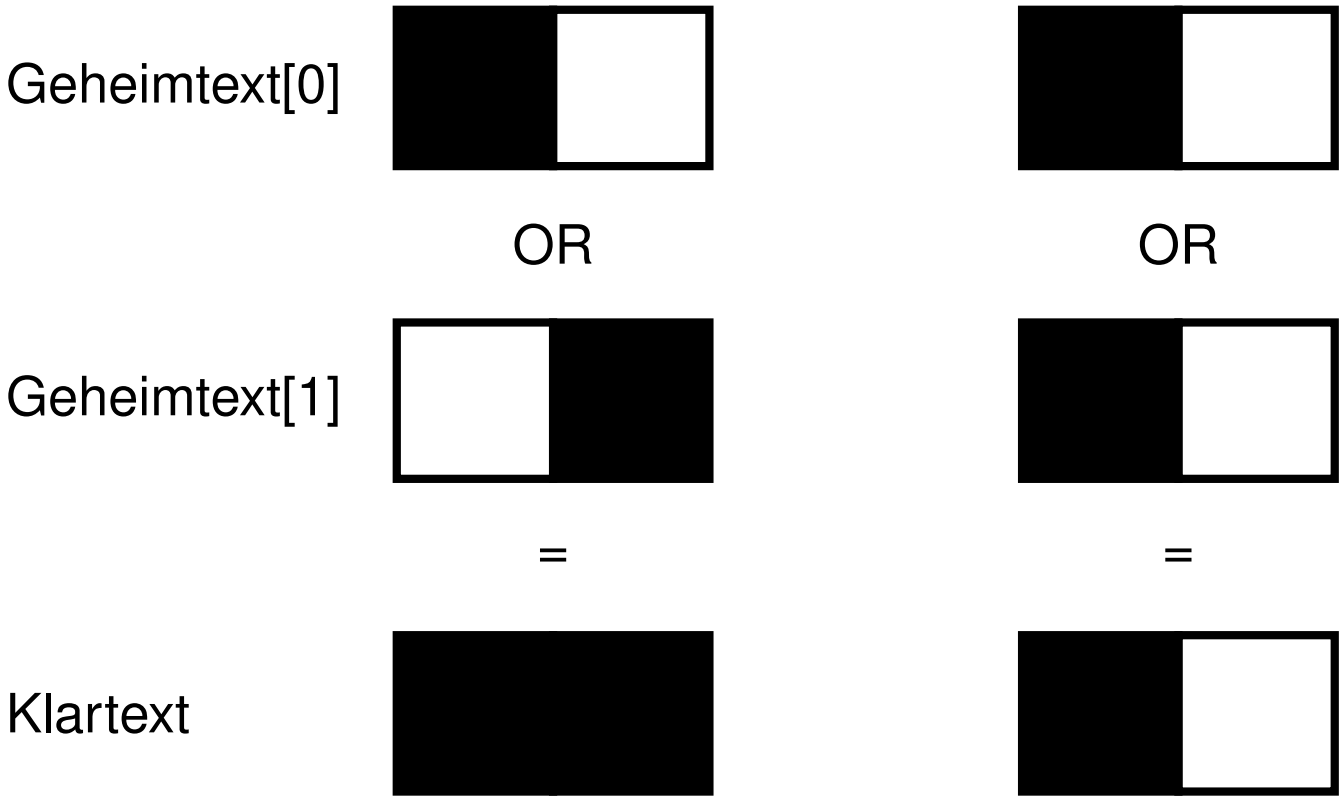
Ein Pixel des Klartexts ergibt sich durch optische Überlagerung mehrerer Subpixel der Geheimtextteile. Jedes Klartext-Pixel wird unabhängig von anderen Klartext-Pixeln verschlüsselt. Beispiel 2-von-2-Verschlüsselung:



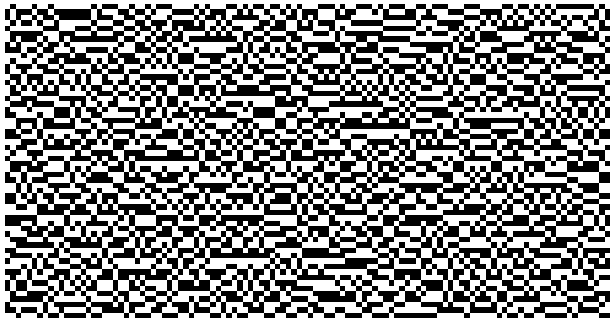
schwarzes Pixel »weißes« Pixel

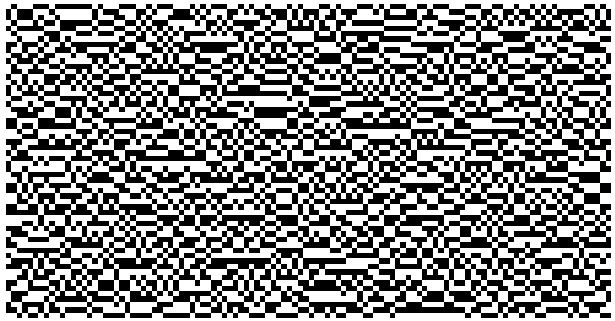
sublab

Ein Pixel des Klartexts ergibt sich durch optische Überlagerung mehrerer Subpixel der Geheimtextteile. Jedes Klartext-Pixel wird unabhängig von anderen Klartext-Pixeln verschlüsselt. Beispiel 2-von-2-Verschlüsselung:

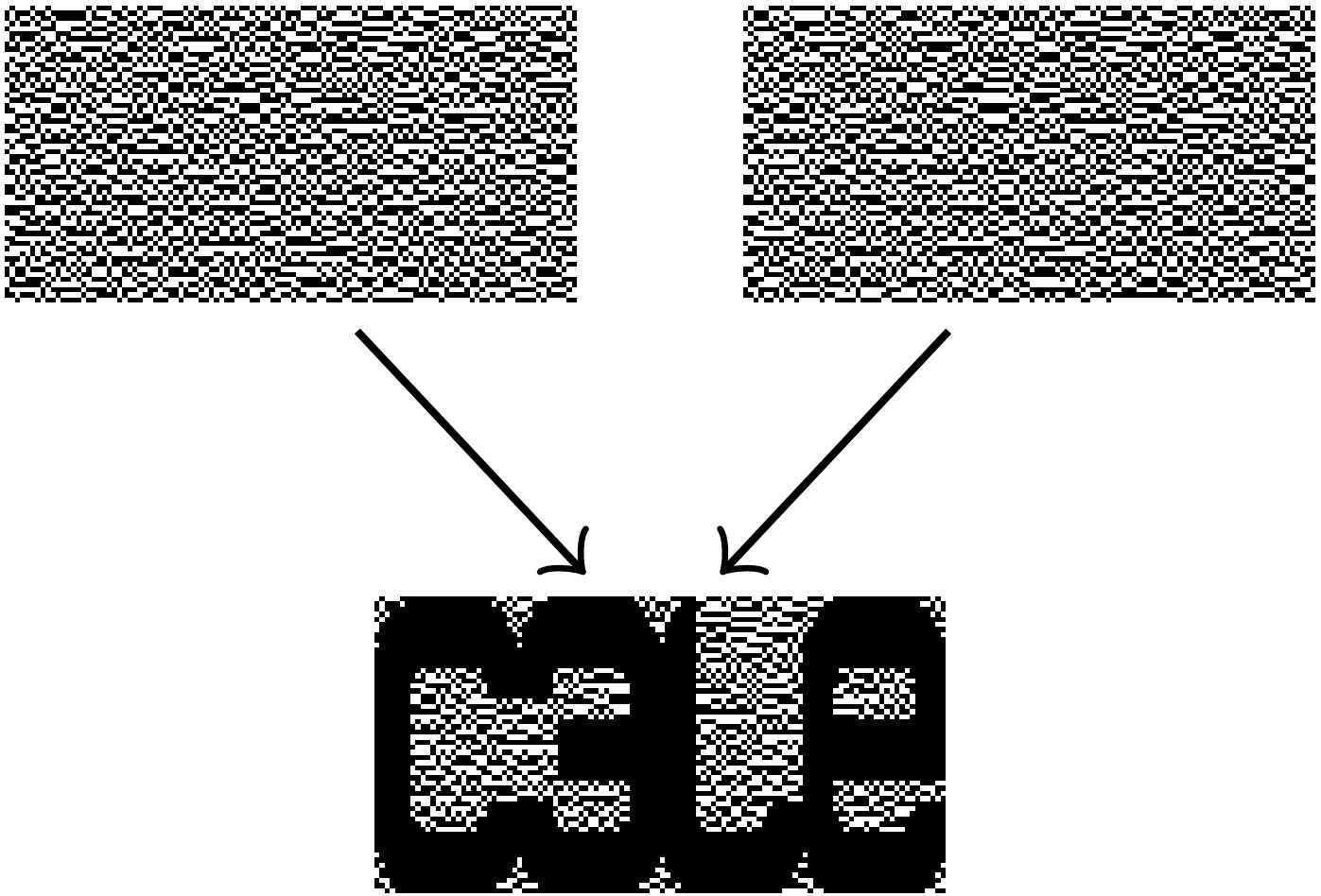


Beispiel: 2-von-2-Verschlüsselung mit VslCrypt





Beispiel: 2-von-2-Verschlüsselung mit VslCrypt



Einschränkungen

- weißes Subpixel kann schwarzes Subpixel nicht aufdecken
  - »weißes« Pixel nicht weiß, sondern im Mittel grau
  - begrenzter Kontrast
  - je mehr Folien (Geheimtextteile), umso geringer der Kontrast
- entschlüsselter Klartext ist beim vorigen 2-von-2-Kryptosystem in einer Längendimension gespreizt

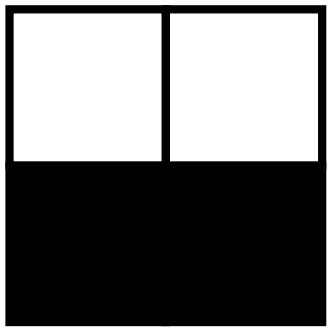
Matrixmodell

- Abbildung der Subpixel eines einzelnen Klartext-Pixels in einem Folienstapel durch eine Matrix
- Matrixelement: Subpixel, weiß = 0, schwarz = 1
- Spalte: Position des Subpixels auf einer Folie (Geheimtextteil)
- Zeile: einzelne Folie

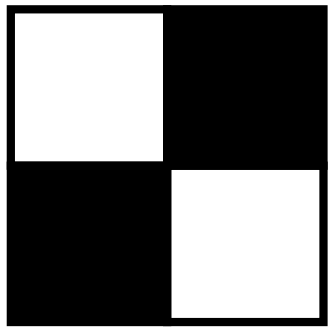
Beispiel:

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

Folie 1



Folie 2



sublab

Visuelles k-von-n-Kryptosystem nach Naor und Shamir

Dieses System ist schwellenbasiert, d. h., durch Überlagerung von mindestens k Geheimtextteilen wird der Klartext sichtbar.

Kontrastkriterien

- Menge aller Matrizen C_0, so daß Überlagerung von irgend-k Zeilen einer jeden Matrix »weißes« Klartext-Pixel ergibt
- Menge aller Matrizen C_1, so daß Überlagerung von irgend-k Zeilen einer jeden Matrix schwarzes Klartext-Pixel ergibt

Sicherheitskriterium

- Überlagerung von weniger als k Zeilen der Matrizen in C_0 und C_1 läßt keine Rückschlüsse auf Zugehörigkeit zu C_0 oder C_1 zu
- $\Rightarrow$ perfekte Sicherheit

Visuelles k-von-n-Kryptosystem nach Naor und Shamir

Dieses System ist schwellenbasiert, d. h., durch Überlagerung von mindestens k Geheimtextteilen wird der Klartext sichtbar.

Kontrastkriterien

- Menge aller Matrizen C_0, so daß Überlagerung von irgend-k Zeilen einer jeden Matrix »weißes« Klartext-Pixel ergibt
- Menge aller Matrizen C_1, so daß Überlagerung von irgend-k Zeilen einer jeden Matrix schwarzes Klartext-Pixel ergibt

Sicherheitskriterium

- Überlagerung von weniger als k Zeilen der Matrizen in C_0 und C_1 läßt keine Rückschlüsse auf Zugehörigkeit zu C_0 oder C_1 zu
- $\Rightarrow$ perfekte Sicherheit

Visuelles k-von-n-Kryptosystem nach Naor und Shamir

Dieses System ist schwellenbasiert, d. h., durch Überlagerung von mindestens k Geheimtextteilen wird der Klartext sichtbar.

Kontrastkriterien

- Menge aller Matrizen C_0, so daß Überlagerung von irgend-k Zeilen einer jeden Matrix »weißes« Klartext-Pixel ergibt
- Menge aller Matrizen C_1, so daß Überlagerung von irgend-k Zeilen einer jeden Matrix schwarzes Klartext-Pixel ergibt

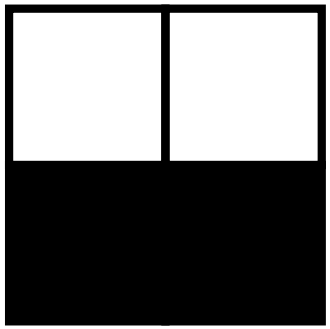
Sicherheitskriterium

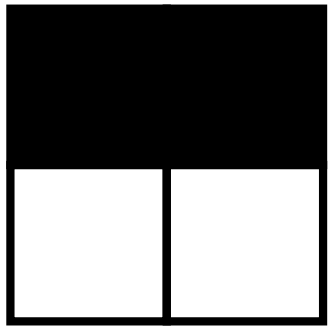
- Überlagerung von weniger als k Zeilen der Matrizen in C_0 und C_1 läßt keine Rückschlüsse auf Zugehörigkeit zu C_0 oder C_1 zu
- $\Rightarrow$ perfekte Sicherheit

sublab

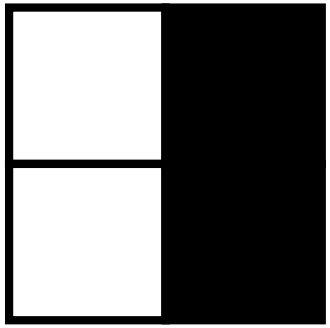
Verbessertes 2-von-2-Kryptosystem (1/3)

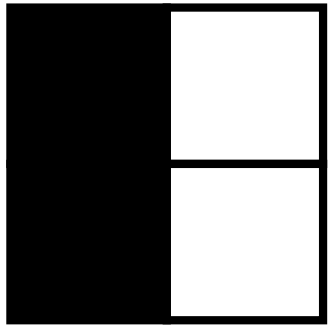
horizontale Teile



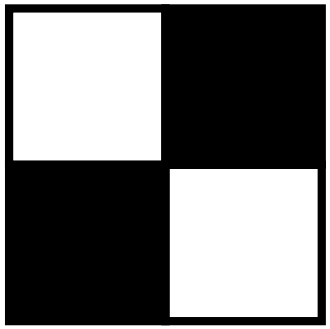


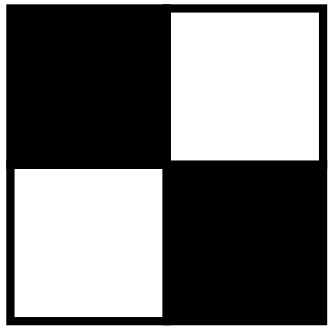
vertikale Teile





diagonale Teile





sublab

Verbessertes 2-von-2-Kryptosystem (2/3)

Verwendung von vier statt zwei Subpixeln:

$$C_0 = \{\text{alle Matrizen, die man durch Permutation der Spalten von } \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \text{ erhält}\}$$

$$C_1 = \{\text{alle Matrizen, die man durch Permutation der Spalten von } \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \text{ erhält}\}$$

sublab

Verbessertes 2-von-2-Kryptosystem (3/3)

Anwendung

Zur Verschlüsselung eines weißen Klartext-Pixels wähle zufällig eine Matrix aus C_0.
Zur Verschlüsselung eines schwarzen Klartext-Pixels wähle zufällig eine Matrix aus C_1.

Eigenschaften

- Entschlüsselung durch zwei Geheimtextteile
- Vermeidung der Verzerrung des Klartextes durch quadratische Subpixelanordnung
- zwei weiße und zwei schwarze Subpixel je Geheimtextteil
- zwei weiße und zwei schwarze Subpixel für »weißes« Klartext-Pixel
- vier schwarze Subpixel für schwarzes Klartext-Pixel

Perfekte Sicherheit

am Beispiel des verbesserten 2-von-2-Kryptosystems

$$C_? = \left\{ \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}, \ldots \right\}$$

$$C_? = \left\{ \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}, \ldots \right\}$$

Perfekte Sicherheit

am Beispiel des verbesserten 2-von-2-Kryptosystems

$$C_? = \left\{ \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}, \ldots \right\}$$

$$C_? = \left\{ \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}, \ldots \right\}$$

sublab

Perfekte Sicherheit

am Beispiel des verbesserten 2-von-2-Kryptosystems

$$C_? = \left\{ \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \dots \right\}$$

$$C_? = \left\{ \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \dots \right\}$$

Perfekte Sicherheit

am Beispiel des verbesserten 2-von-2-Kryptosystems

$$C_1 = \left\{ \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \dots \right\}$$

$$C_0 = \left\{ \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \dots \right\}$$

Konzept der Schlüsselfolie

Anwendung

- erzeuge Folie S, die zufällig alle möglichen Subpixel-Permutationen enthält
- verschlüssele alle Klartexte so, daß ein Geheimtextteil S entspricht
- Es gibt also einen konstanten Geheimtextteil S, die Schlüsselfolie.

Bewertung der Sicherheit

- Klartexte durch Übereinanderlegen der abgefangenen, nicht konstanten Geheimtextteile erkennbar
- genauso unsicher wie mehrfache Verwendung eines Schlüssels bei herkömmlicher Verschlüsselung
- Fazit: unsicher

sublab

Konzept der Schlüsselfolie

Anwendung

- erzeuge Folie S, die zufällig alle möglichen Subpixel-Permutationen enthält
- verschlüssele alle Klartexte so, daß ein Geheimtextteil S entspricht
- Es gibt also einen konstanten Geheimtextteil S, die Schlüsselfolie.

Bewertung der Sicherheit

- Klartexte durch Übereinanderlegen der abgefangenen, nicht konstanten Geheimtextteile erkennbar
- genauso unsicher wie mehrfache Verwendung eines Schlüssels bei herkömmlicher Verschlüsselung
- Fazit: unsicher

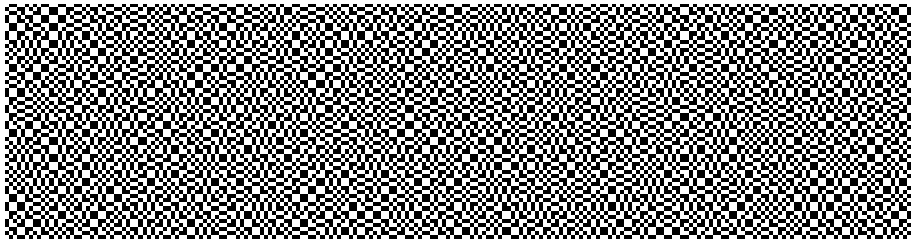
sublab

Ausblick

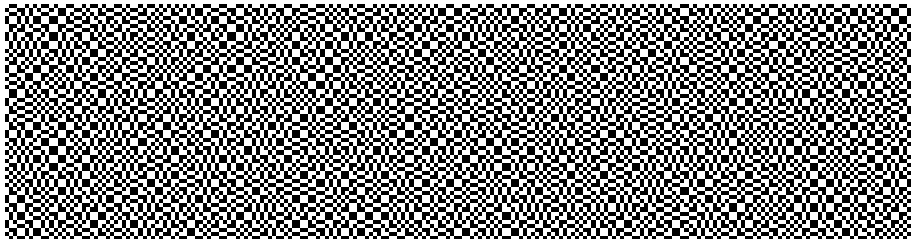
- visuelle Kryptographie relativ junges Forschungsgebiet
- interessante Entwicklungen:
  - Kontrastverbesserung
  - Toleranz gegen Verschiebungen (z. B. Übertragung per Telefax)
  - gruppen- statt schwellenbasierte Verschlüsselung
  - Graustufen-Verschlüsselung
  - farbige Verschlüsselung
  - drei Folien, zwei Klartexte

2-von-2-Kryptosystem mit VCK

```
> python vck-split-mono.py c3le.tif
```



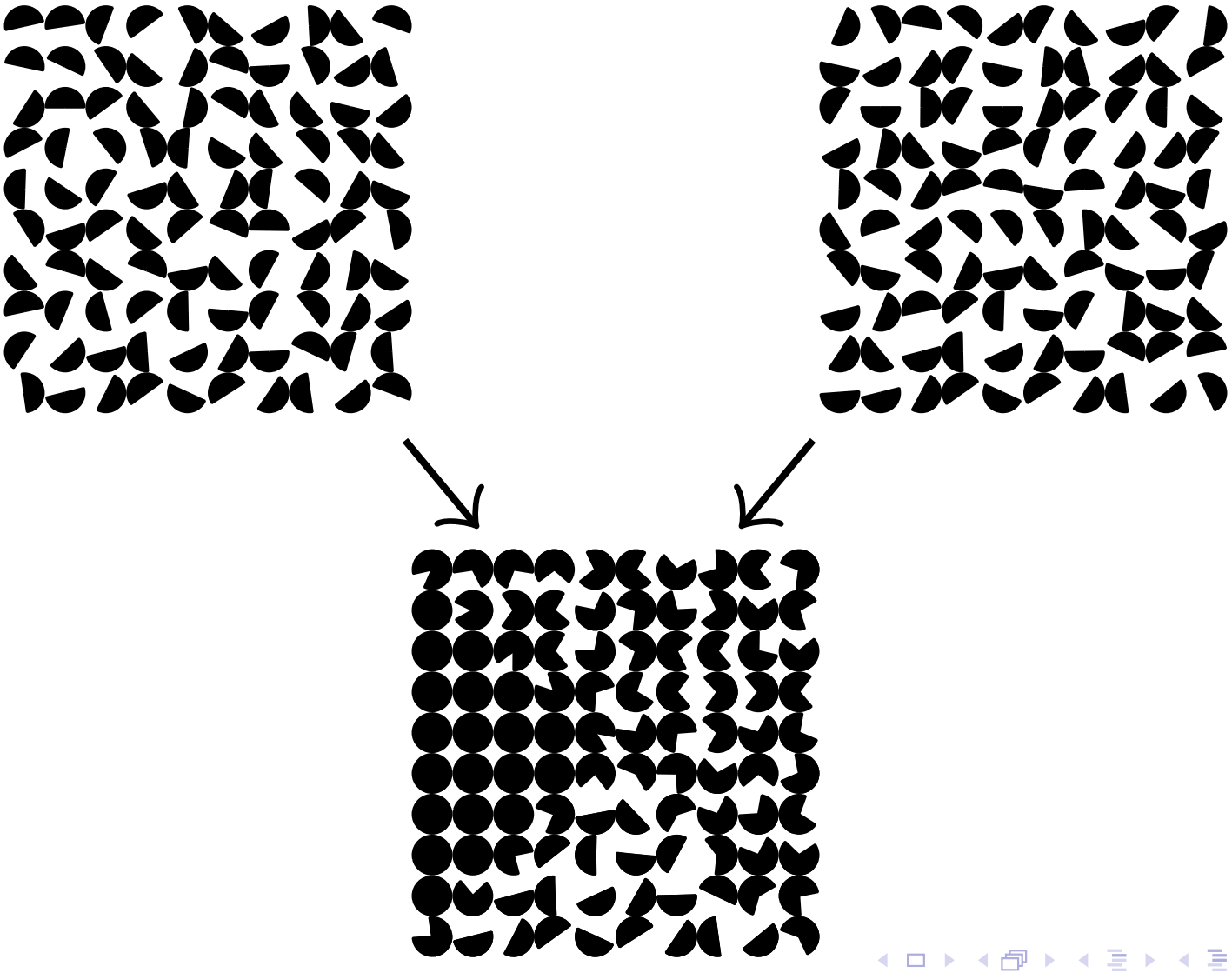
OR



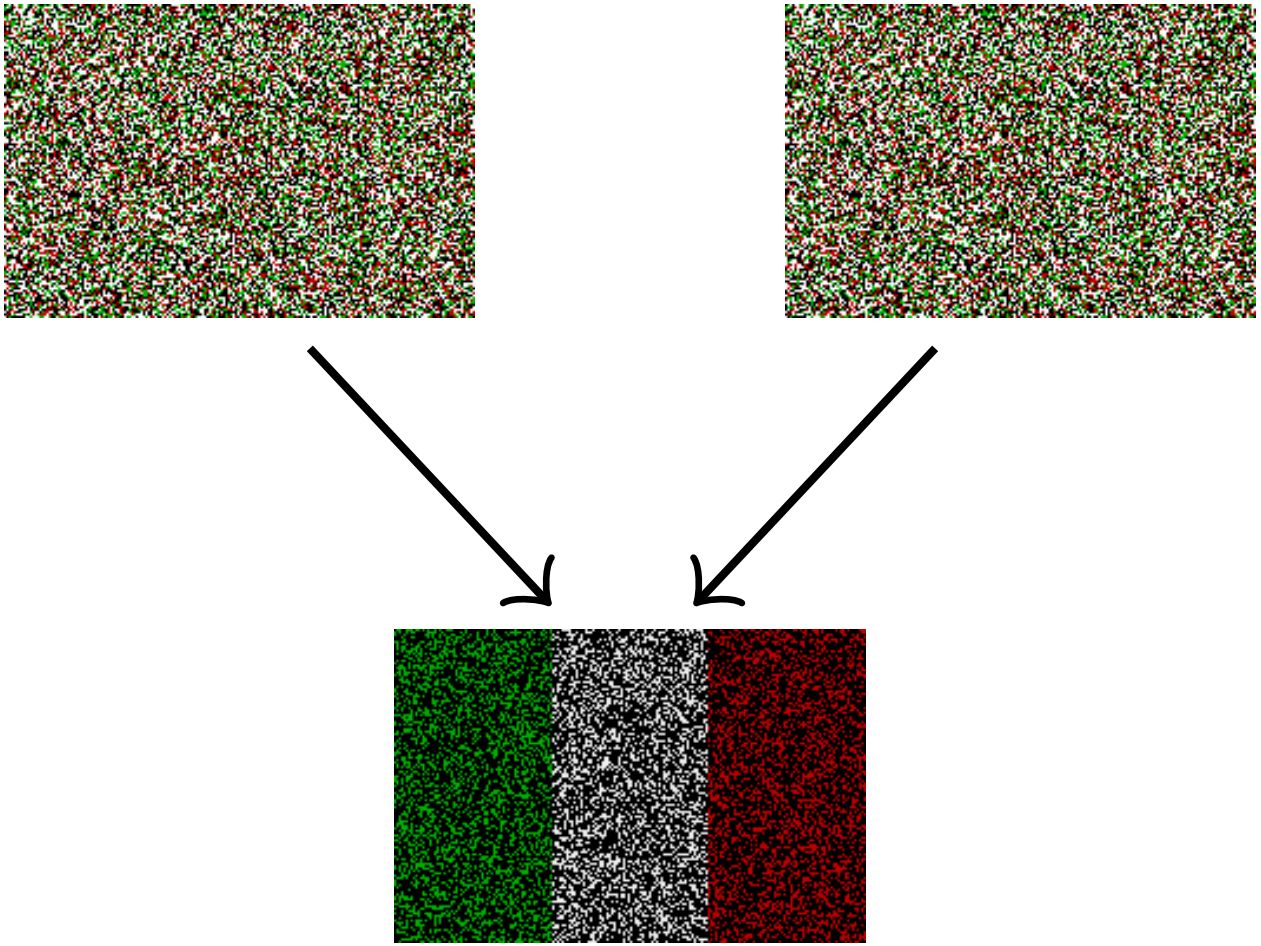
=

Graustufen-Verschlüsselung mit VCK

Überlagerung von gedrehten Halbkreisen ergibt Kreissektoren



Farbige Verschlüsselung mit VES



Weitere Beispiele werden im Anschluß an den Vortrag gezeigt, sind aber wegen Urheberrechten und aufgrund ihrer Größe nicht in dieser Datei veröffentlicht.

Anknüpfungspunkte für Selbststudium

- `http://www.wisdom.weizmann.ac.il/~naor/PAPERS/visual_pap.ps.gz`
- `http://cage.ugent.be/~klein/vis-crypt/`
- VCK: `http://www.cl.cam.ac.uk/~fms27/vck/`
- VslCrypt: `http://www.uni-giessen.de/beutelspacher/programme/vslcrypt.zip`

Lizenz