The Challenge of Authentication in Insecure Environments

Sebastian Pape

Fachbereich Elektrotechnik / Informatik der Universität Kassel

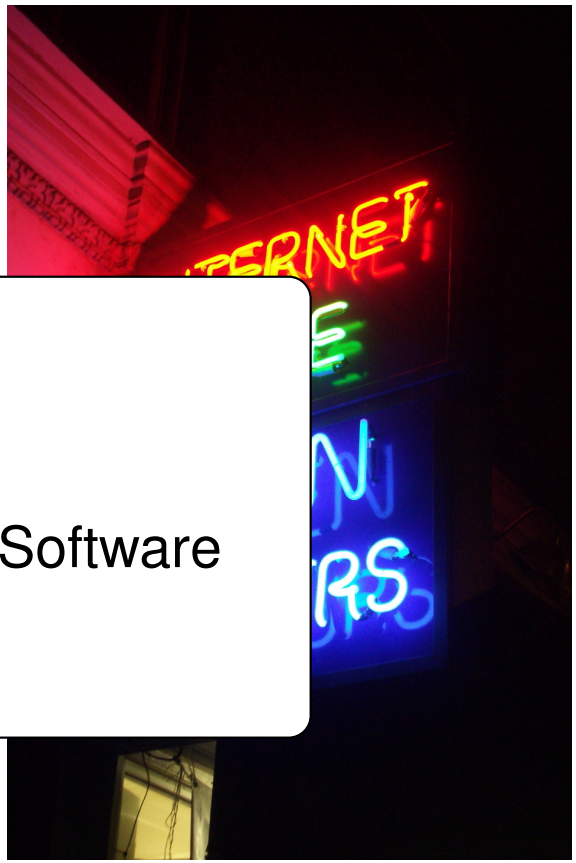
2. September 2013

Disputation zur Erlangung des akademisches Grades
Doktor der Naturwissenschaften (Dr. rer. nat.)

Übersicht

Was heißt unsichere Umgebung?

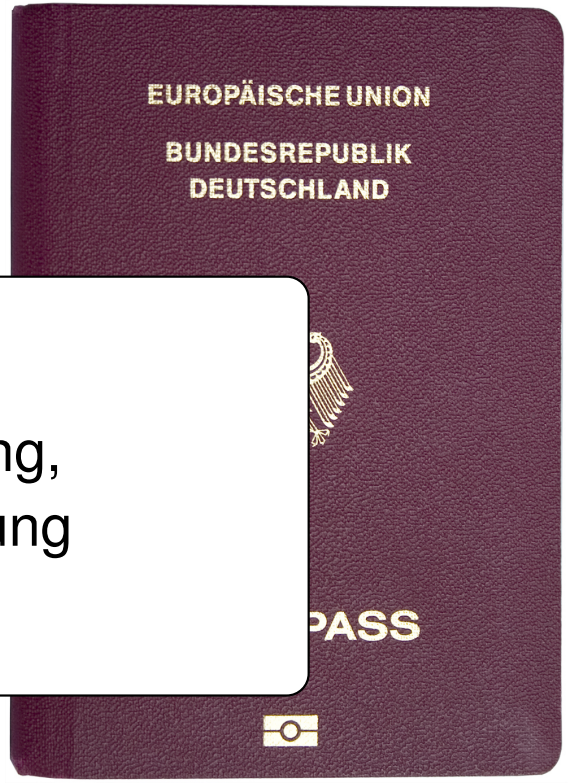
Was heißt unsichere Umgebung?



Unsichere
Hardware / Software

Was heißt unsichere Umgebung?

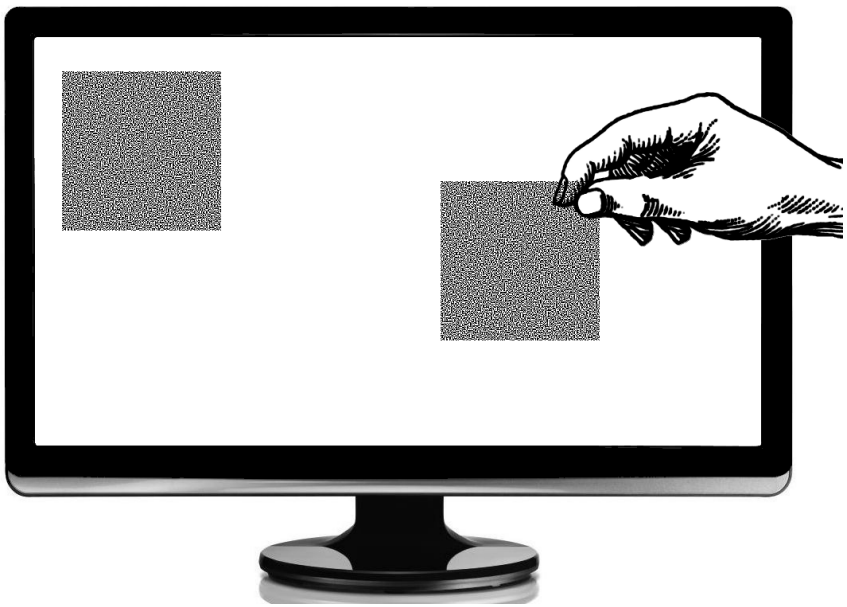
Was heißt unsichere Umgebung?



Überwachung,
Profilerstellung

Übersicht

Visuelle Kryptographie - Idee



(a) Folien nebeneinander

(b) Folien übereinander angeordnet

Verwendung von Keypads

Abbildung: Keypad eines Geldautomaten

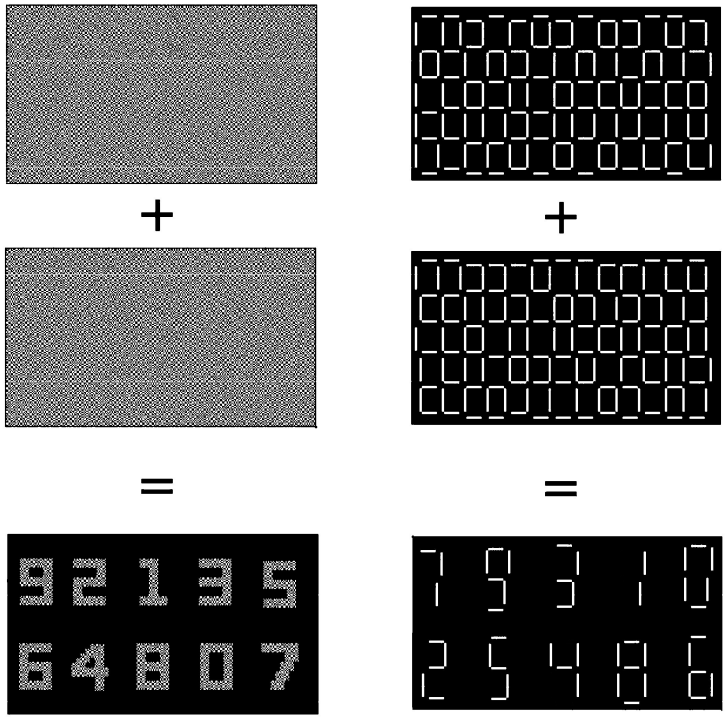


Abbildung: Keypads in der visuellen Kryptographie (Borchert, 2007)

Pixelbasierte visuelle Kryptogr. (Naor und Shamir, 1994)

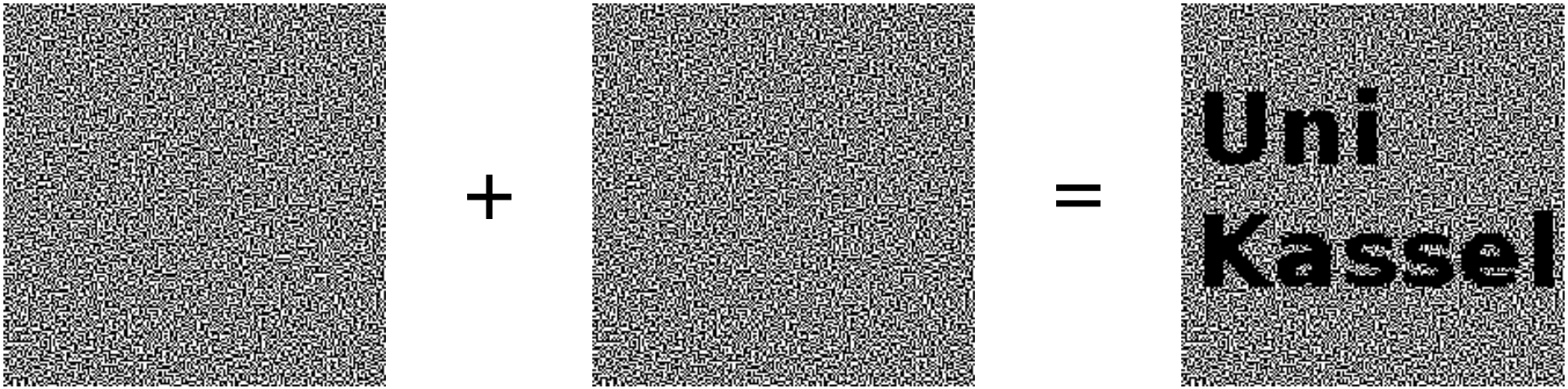


Abbildung: Beispiel pixelbasierter visueller Kryptographie

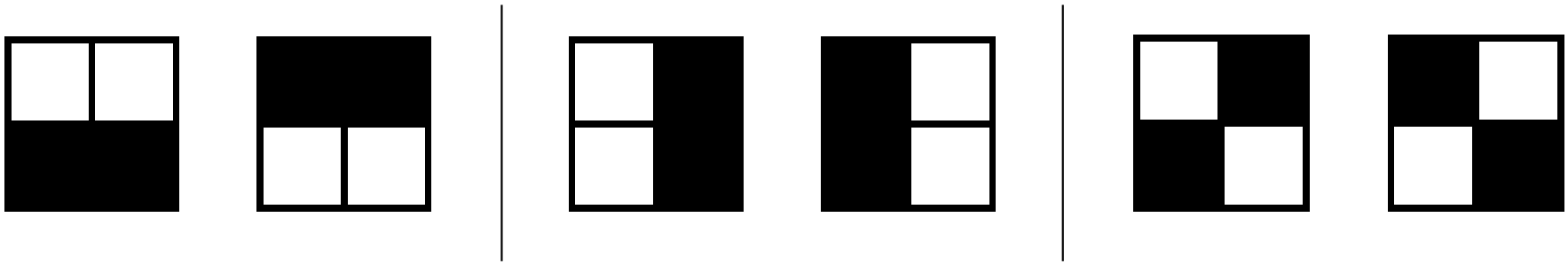


Abbildung: Shares mit jeweils 4 Subpixeln in einer 2x2 Matrix

Überlagerung von zwei Pixeln (Naor und Shamir, 1994)

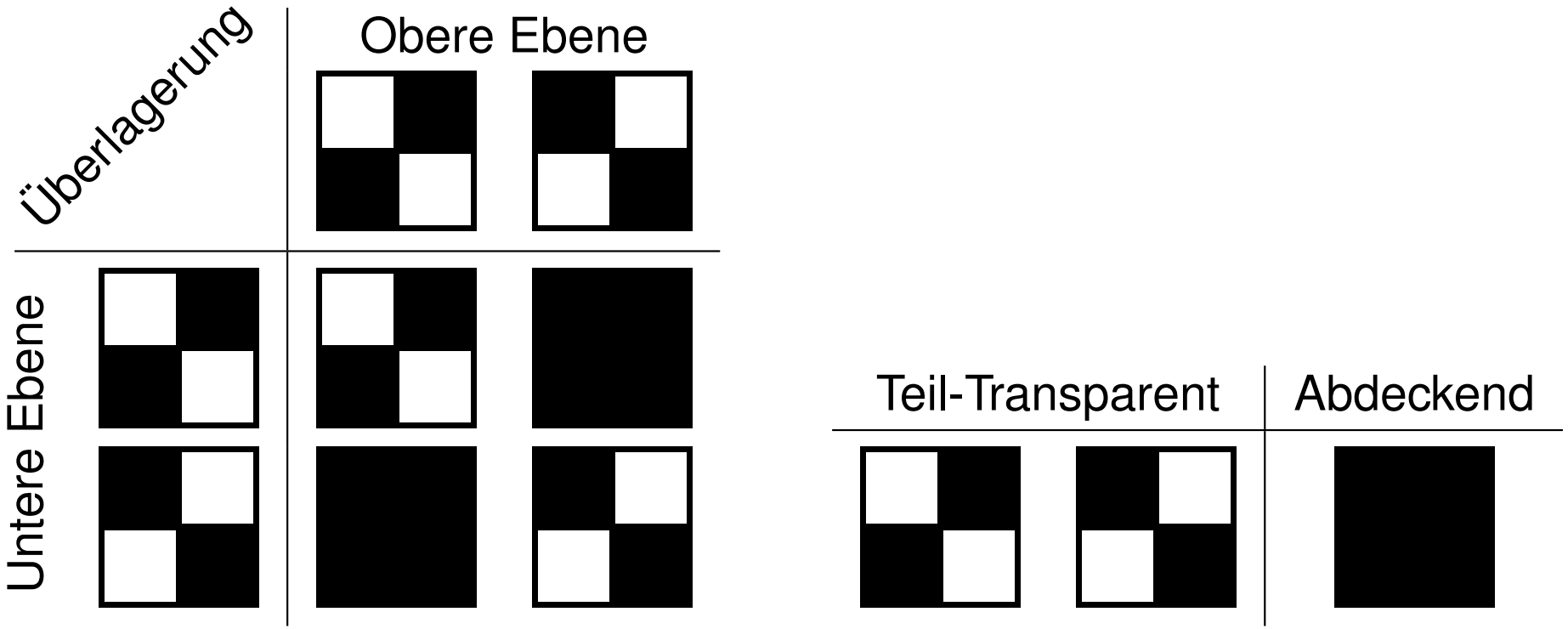


Abbildung: Kreuz- und Auswertungstabelle

Wiederverwendung von Schlüsselfolien (pixelbasiert)

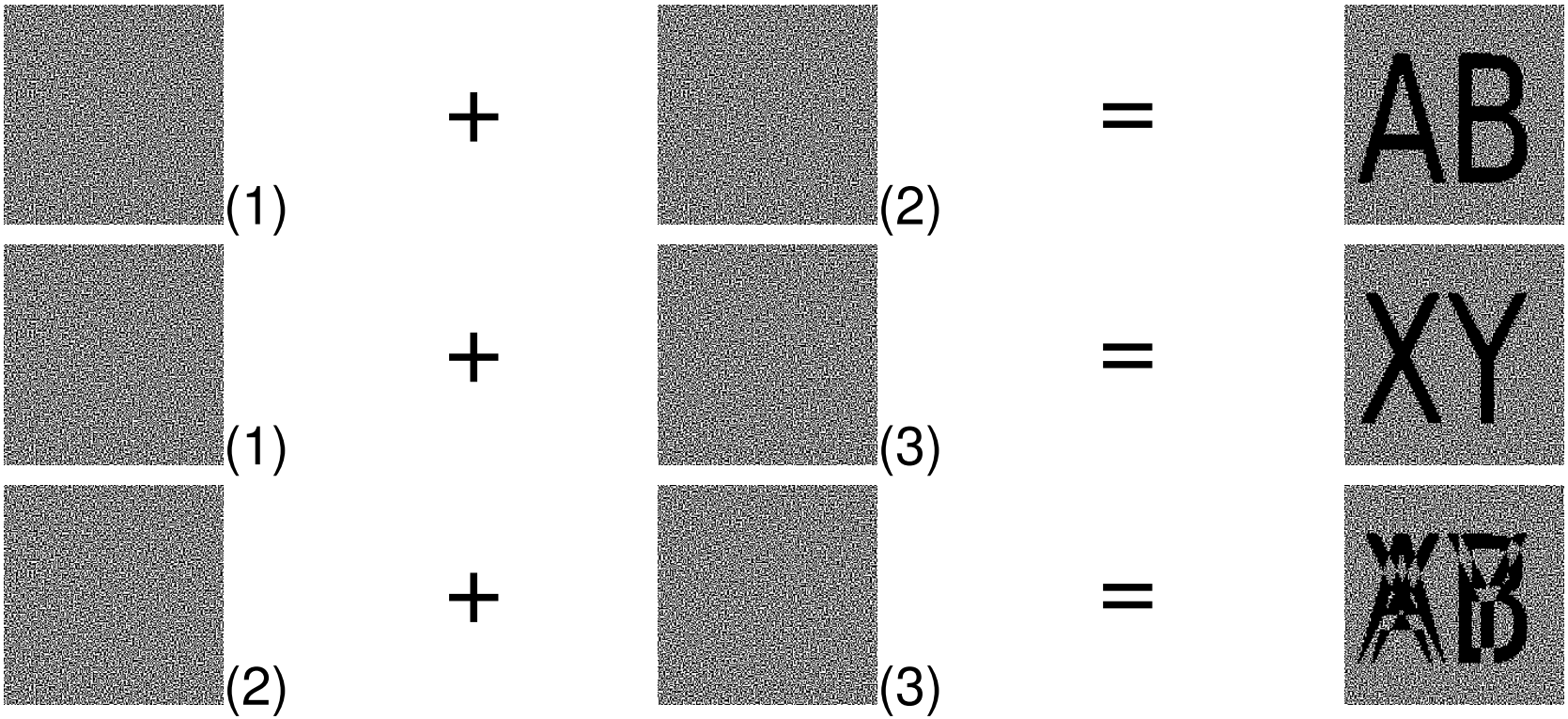
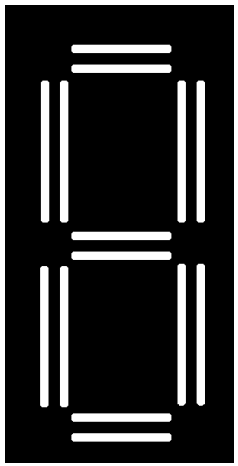
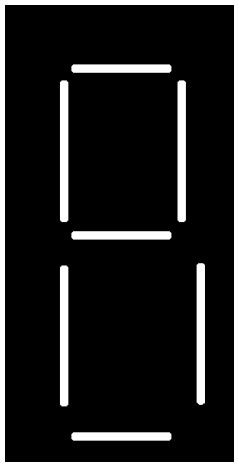


Abbildung: Kombination von drei verschiedenen Folien

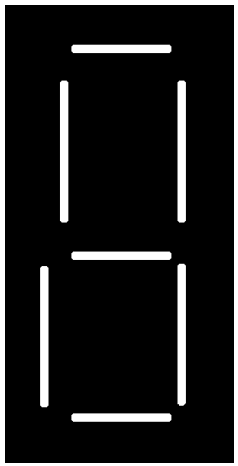
Segmentbasierte visuelle Kryptographie (Borchert, 2007)



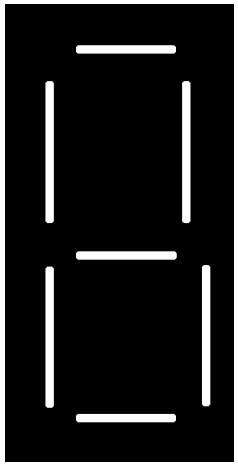
(a) full



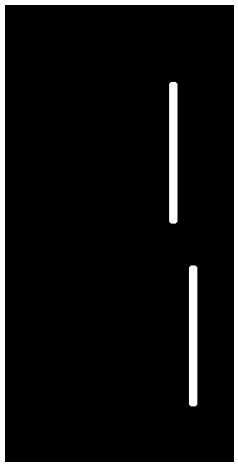
(b) c_1



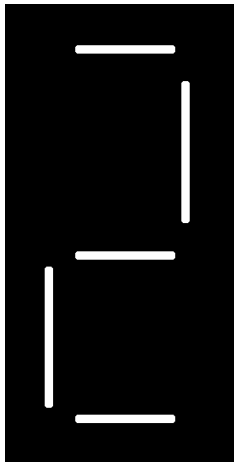
(c) c_2



(d) k



(e) $c_1 \leftrightarrow k$

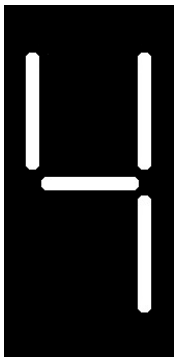


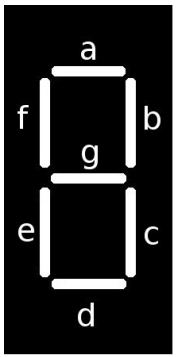
(f) $c_2 \leftrightarrow k$

Vorteile gegenüber pixelbasierter VC

- Ausrichtung der Folien leichter
- Kein Kontrastverlust
  $\Rightarrow$ Symbole leichter zu erkennen
- Weniger Bits notwendig
- Leichter für Laien zu verstehen

Wiederverwendung von Schlüsselfolien (7-Segment)





- $2^7 = 128$ mögliche Schlüssel
- 1 Ciphertext bekannt
  $\Rightarrow$ 10 Schlüssel möglich

- Theorie: 1.9 Ciphertexte notwendig
- Praxis: 3-5 Ciphertexte notwendig

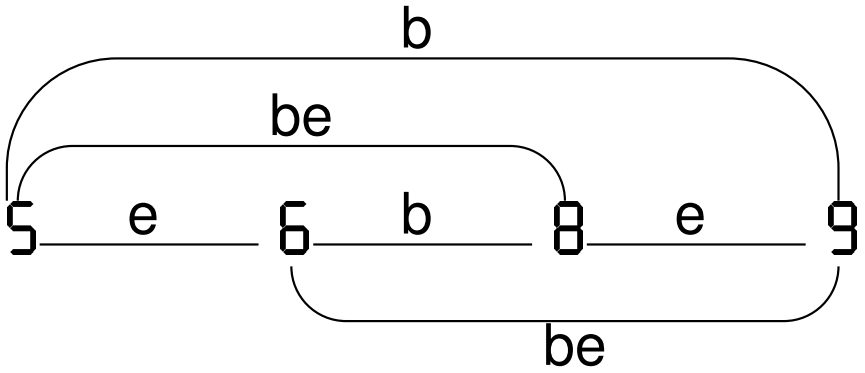


Abbildung: Abgeschlossene Untergruppe: 5, 6, 8, 9

Dice Codings (Doberitz, 2008)

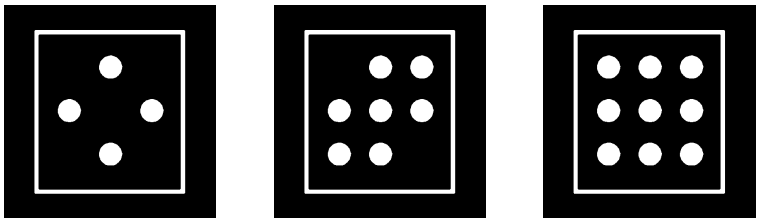
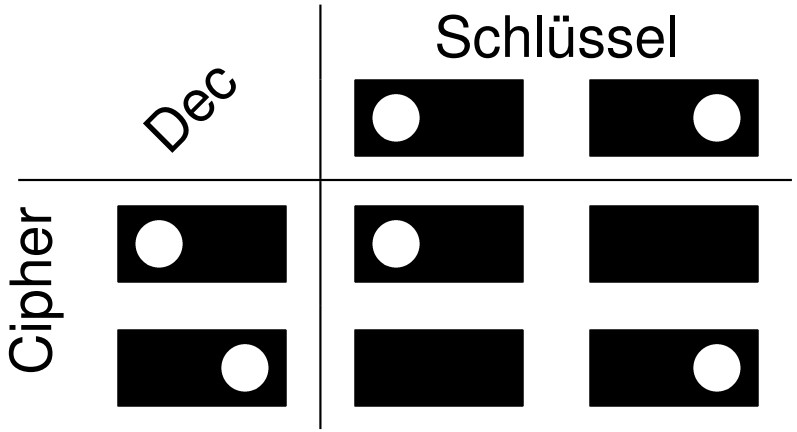


Abbildung: Encodings von 4, 7, 9



- Abgeschlossen
- User-Studie von Doberitz (2008)

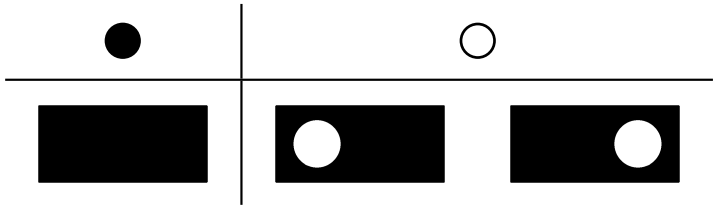
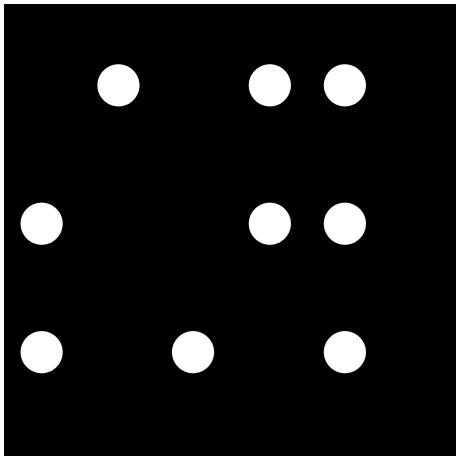


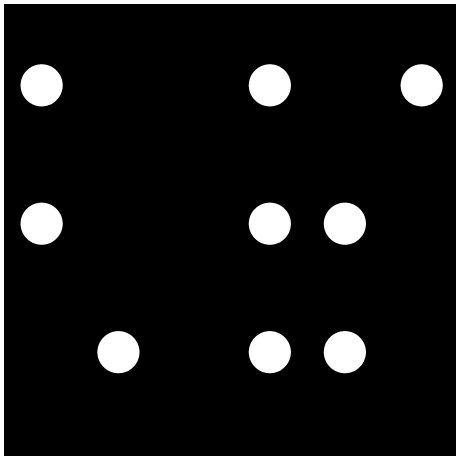
Abbildung: Kreuz- und Auswertungstabelle

Dice Codings - Beispiel



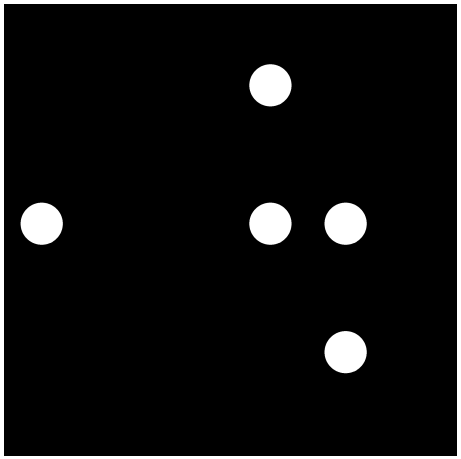
Ciphertext c

+



Schlüssel k

=

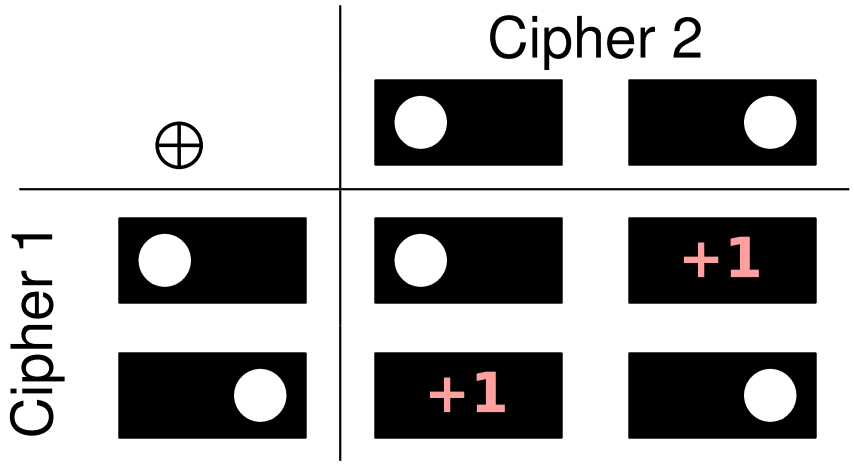


Symbol s (5)

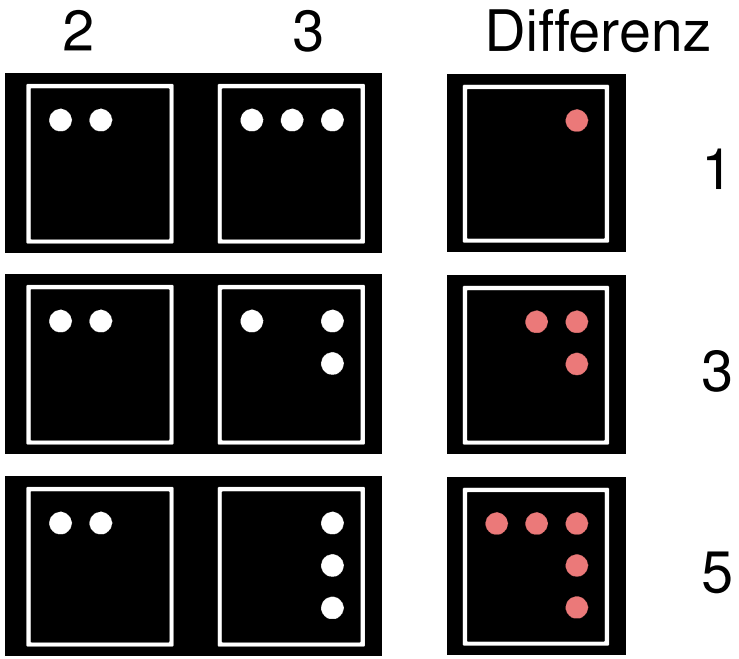
Wiederverwendung von Schlüsselfolien (Dice Codings)

$$C_1 \oplus C_2 = (S_1 \leftrightarrow K) \oplus (S_2 \leftrightarrow K) = S_1 \oplus S_2$$

- Informationsgewinn durch XOR

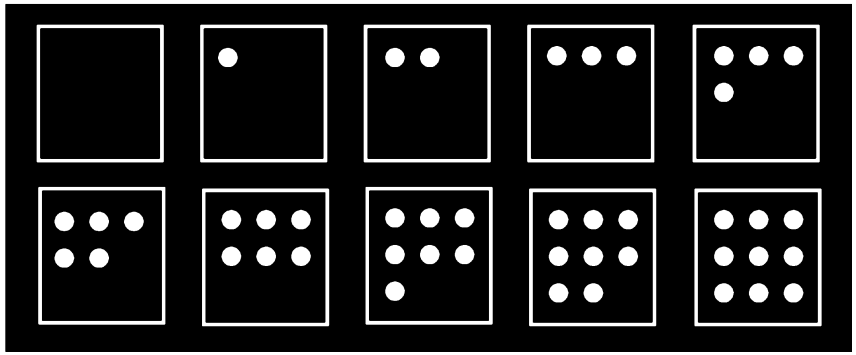


- XOR von 2 Encodings



Wiederverwendung von Schlüsselfolien (Dice Codings)

- Dices
  - Unterschiedliche Anzahl von Encodings
  - 0 und n haben nur ein Encoding
  - Inverses von k ist $n - k$
    - auch bei Ciphertext
- Keypads
  - Dices paarweise verschieden
  - 22 bis 26 Ciphertexte erlauben den Schlüssel einzuschränken

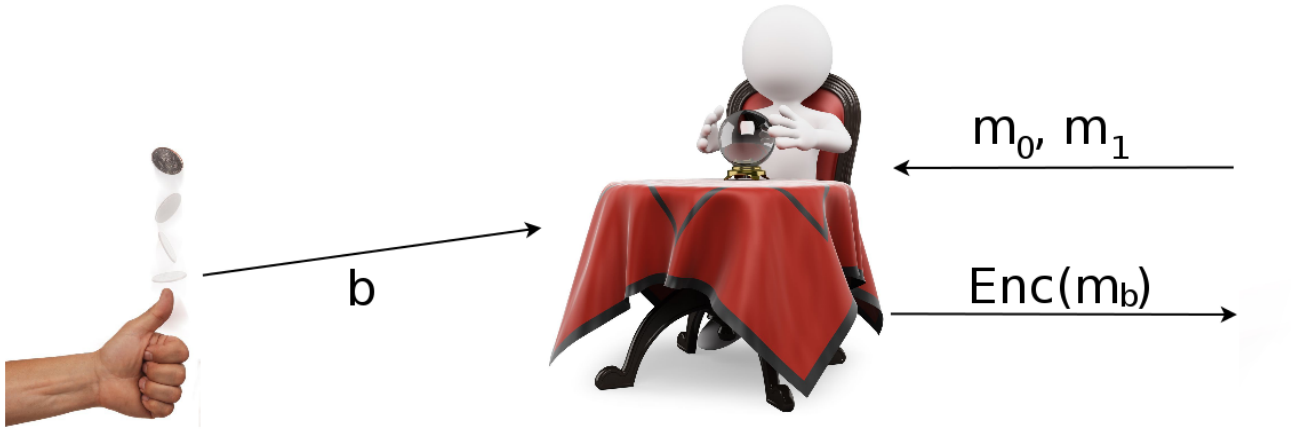


m	$\lvert\mathcal{S}_m\rvert$	m	$\lvert\mathcal{S}_m\rvert$
0	1	5	126
1	9	6	84
2	36	7	36
3	84	8	9
4	126	9	1

Tabelle: Anzahl unterschiedlicher Encodings eines 9-Dots Dice Coding

Übersicht

Left-Or-Right (*LOR – CPA*) Bellare u. a. (1997)



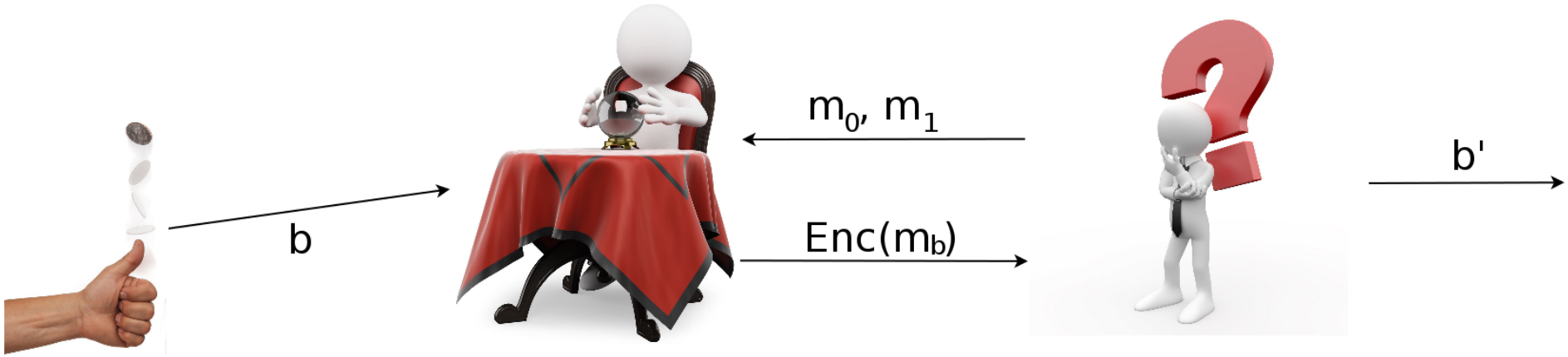
Experiment $\mathbf{Exp}_{A,\Pi}^{lor-cpa-b}(n) = b'$

k	$\leftarrow$	$\text{GenKey}(1^n)$	Schlüsselerzeugung
b	$\in_R$	$\{0,1\}$	zufällige Wahl von b
b'	$\leftarrow$	$A^{O_{\mathcal{LR}}(\cdot,\cdot,b)}$	Angreifer versucht b zu bestimmen

Vorteil des Angreifers $\mathbf{Adv} = Pr[correct] - Pr[false]$

$$\mathbf{Adv}_{A,\Pi}^{lor-cpa}(n) \stackrel{def}{=} Pr[\mathbf{Exp}_{A,\Pi}^{lor-cpa-1}(n) = 1] - Pr[\mathbf{Exp}_{A,\Pi}^{lor-cpa-0}(n) = 1]$$

Left-Or-Right (*LOR – CPA*) Bellare u. a. (1997)



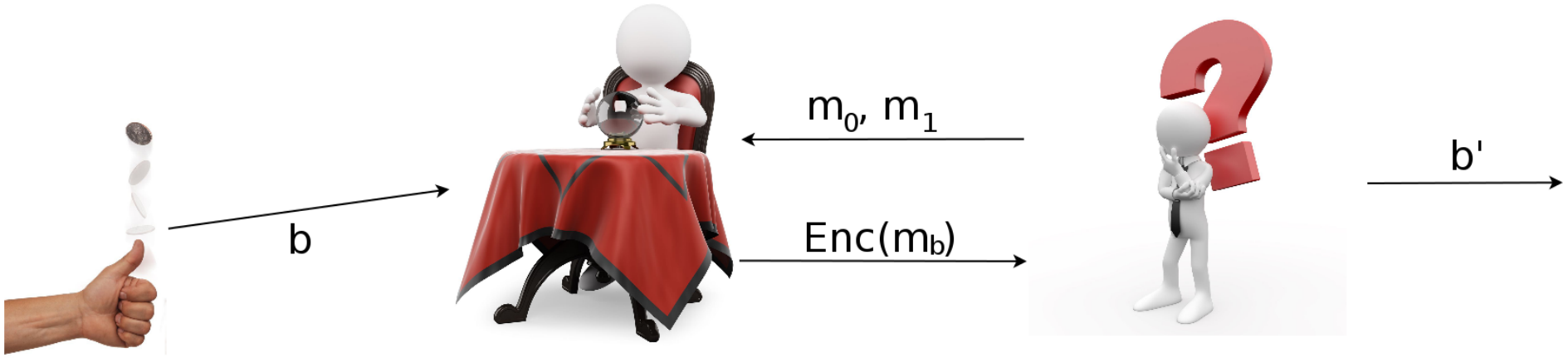
Experiment $\mathbf{Exp}^{lor-cpa-b}_{A,\Pi}(n) = b'$

k	$\leftarrow$	GenKey(1^n)	Schlüsselerzeugung
b	$\in_R$	$\{0,1\}$	zufällige Wahl von b
b'	$\leftarrow$	$A^{O_{\mathcal{LR}}(\cdot,\cdot,b)}$	Angreifer versucht b zu bestimmen

Vorteil des Angreifers $\mathbf{Adv} = Pr[correct] - Pr[false]$

$$\mathbf{Adv}^{lor-cpa}_{A,\Pi}(n) \stackrel{def}{=} Pr[\mathbf{Exp}^{lor-cpa-1}_{A,\Pi}(n) = 1] - Pr[\mathbf{Exp}^{lor-cpa-0}_{A,\Pi}(n) = 1]$$

Left-Or-Right (*LOR – CPA*) Bellare u. a. (1997)



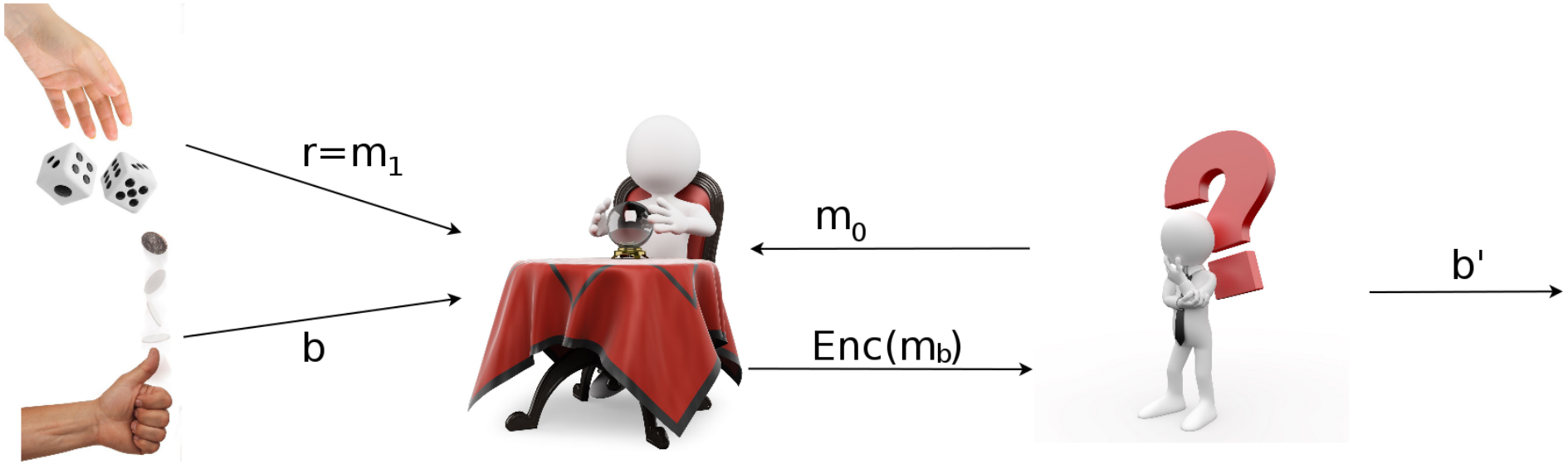
Experiment $\mathbf{Exp}^{lor-cpa-b}_{A,\Pi}(n) = b'$

k	$\leftarrow$	GenKey(1^n)	Schlüsselerzeugung
b	$\in_R$	$\{0,1\}$	zufällige Wahl von b
b'	$\leftarrow$	$A^{O_{\mathcal{LR}}(\cdot,\cdot,b)}$	Angreifer versucht b zu bestimmen

Vorteil des Angreifers $\mathbf{Adv} = Pr[correct] - Pr[false]$

$$\mathbf{Adv}^{lor-cpa}_{A,\Pi}(n) \stackrel{def}{=} Pr[\mathbf{Exp}^{lor-cpa-1}_{A,\Pi}(n) = 1] - Pr[\mathbf{Exp}^{lor-cpa-0}_{A,\Pi}(n) = 1]$$

Real-Or-Random (*ROR – CPA*) Bellare u. a. (1997)



Experiment

$$\mathbf{Exp}^{ror-cpa-b}_{A,\Pi}(n) = b'$$

k	$\leftarrow$	GenKey(1^n)	Schlüsselerzeugung
b	$\in_R$	$\{0,1\}$	zufällige Wahl von b
b'	$\leftarrow$	$A^{O_{\mathcal{RR}}(\cdot,b)}$	Angreifer versucht b zu bestimmen

Vorteil des Angreifers

$$\mathbf{Adv} = Pr[correct] - Pr[false]$$

$$\mathbf{Adv}^{ror-cpa}_{A,\Pi}(n) \stackrel{def}{=} Pr[\mathbf{Exp}^{ror-cpa-1}_{A,\Pi}(n) = 1] - Pr[\mathbf{Exp}^{ror-cpa-0}_{A,\Pi}(n) = 1]$$

Ciphertext-Only Sicherheitsmodell

- *CPA* gibt die eigentlichen Umstände nur unzureichend wieder
  - Angreifer hat nicht immer ein Verschlüsselungsorakel
- *CPA* ist zu stark
  - XOR + geringer Zufall erlauben Bestimmung des Schlüssels
  - z.B. Verschlüsselungen von □, 8 oder 9 (n dots)

$\Rightarrow$ *CO*-Sicherheitsmodell

Sample Structure sample_{struct}

Jeder Aufruf von sample_{struct} liefert eine endliche Menge Klartexte, die dem Muster *struct* folgen.

Beispiel für $\Gamma = \{0, 1, \ldots, n\}$ $\Pi(0, 1, \ldots, n)$

$\text{sample}_1 \in_R \{m \mid m = m_0 m_1 \ldots m_n \ \wedge \ \forall i, j \text{ mit } 0 \leq i, j \leq n \ . \ \exists m_i = j\}$

Ciphertext-Only Sicherheitsmodell

- *CPA* gibt die eigentlichen Umstände nur unzureichend wieder
  - Angreifer hat nicht immer ein Verschlüsselungsorakel
- *CPA* ist zu stark
  - XOR + geringer Zufall erlauben Bestimmung des Schlüssels
  - z.B. Verschlüsselungen von □, 8 oder 9 (n dots)

$\Rightarrow$ *CO*-Sicherheitsmodell

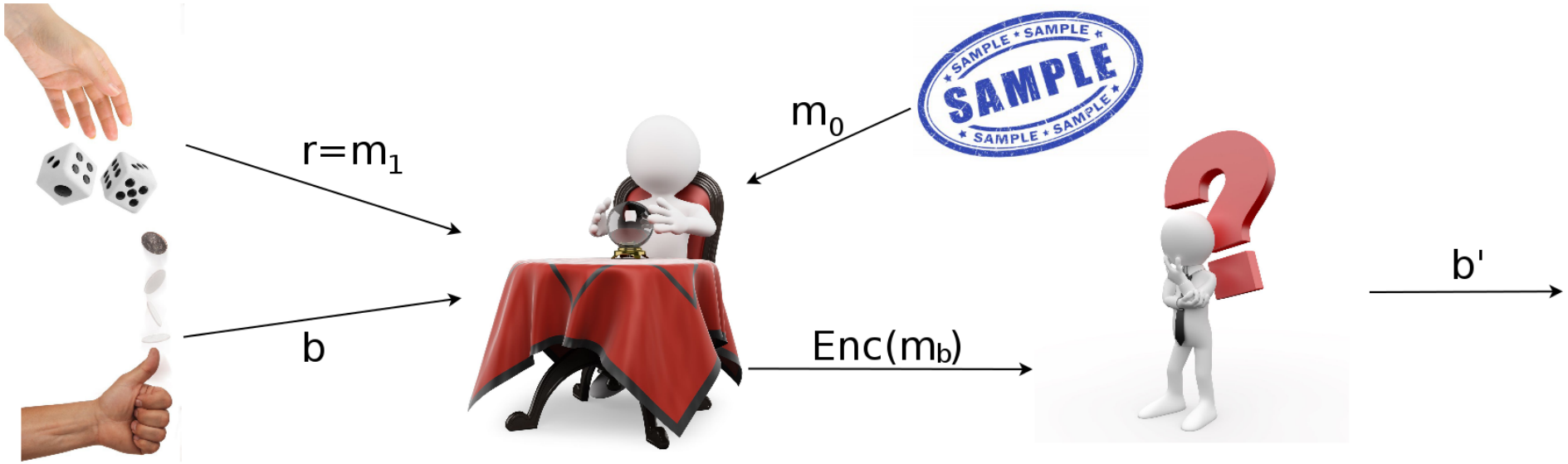
Sample Structure sample_{struct}

Jeder Aufruf von sample_{struct} liefert eine endliche Menge Klartexte, die dem Muster *struct* folgen.

Beispiel für $\Gamma = \{0, 1, \ldots, n\}$ $\Pi(0, 1, \ldots, n)$

$\text{sample}_1 \in_R \{m \mid m = m_0 m_1 \ldots m_n \ \wedge \ \forall i, j \text{ mit } 0 \leq i, j \leq n \ . \ \exists m_i = j\}$

Sample-Or-Random (*SOR – CO*)



Experiment

$\mathbf{Exp}^{sor-co-b}_{A,\Pi}(n) = b'$

k	$\leftarrow$	GenKey(1^n)	Schlüsselerzeugung
b	$\in_R$	$\{0,1\}$	zufällige Wahl von b
b'	$\leftarrow$	$A^{O_{SR}}(struct)$	Angreifer versucht b zu bestimmen

Vorteil des Angreifers

Adv $= Pr[correct] - Pr[false]$

$$\mathbf{Adv}^{sor-co}_{A,\Pi}(n) \stackrel{def}{=} Pr[\mathbf{Exp}^{sor-co-1}_{A,\Pi}(n) = 1] - Pr[\mathbf{Exp}^{sor-co-0}_{A,\Pi}(n) = 1]$$

Beziehung zwischen *ROR – CPA* und *SOR – CO*

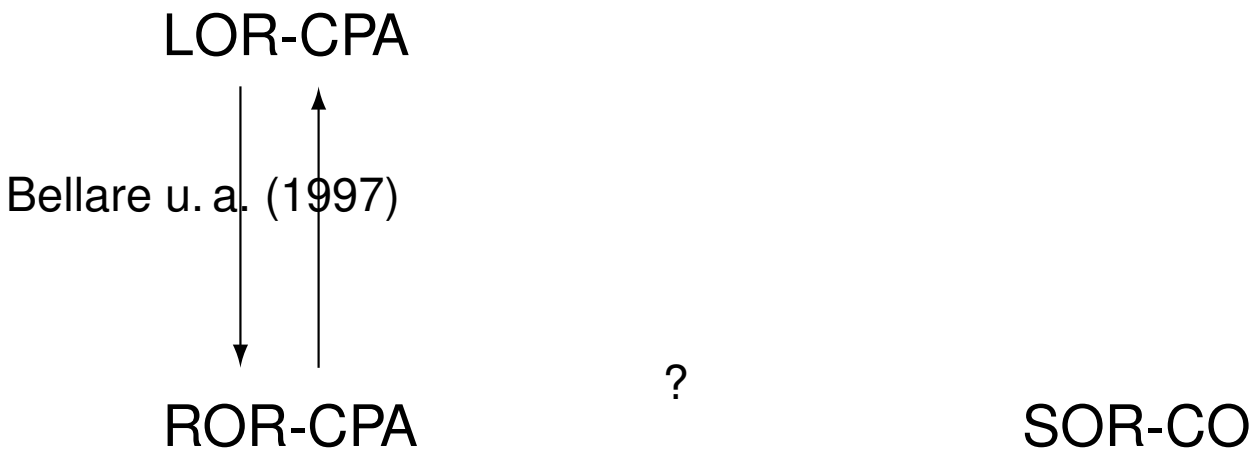


Abbildung: Beziehungen zwischen Sicherheitsmodellen für symmetrische Verschlüsselung

Beziehung zwischen *ROR – CPA* und *SOR – CO*

Theorem

SOR – CO ist schwächer als *ROR – CPA*.

Lemma 1: $[ROR - CPA \Rightarrow SOR - CO]$

Falls ein Verschlüsselungsschema Π sicher im Sinne von *ROR – CPA* ist, dann ist Π auch sicher im Sinne von *SOR – CO*.

Lemma 2: $[SOR - CO \not\Rightarrow ROR - CPA]$

Existiert ein Verschlüsselungsschema Π, das sicher im Sinne von *SOR – CO* ist, dann gibt es ein Verschlüsselungsschema Π', das sicher im Sinne von *SOR – CO* ist, aber nicht sicher im Sinne von *ROR – CPA* ist.

Beziehung zwischen *ROR – CPA* und *SOR – CO*

Theorem

SOR – CO ist schwächer als *ROR – CPA*.

Lemma 1: $[ROR - CPA \Rightarrow SOR - CO]$

Falls ein Verschlüsselungsschema Π sicher im Sinne von *ROR – CPA* ist, dann ist Π auch sicher im Sinne von *SOR – CO*.

Lemma 2: $[SOR - CO \not\Rightarrow ROR - CPA]$

Existiert ein Verschlüsselungsschema Π, das sicher im Sinne von *SOR – CO* ist, dann gibt es ein Verschlüsselungsschema Π′, das sicher im Sinne von *SOR – CO* ist, aber nicht sicher im Sinne von *ROR – CPA* ist.

Beziehung zwischen *ROR – CPA* und *SOR – CO*

Theorem

SOR – CO ist schwächer als *ROR – CPA*.

Lemma 1: $[ROR - CPA \Rightarrow SOR - CO]$

Falls ein Verschlüsselungsschema Π sicher im Sinne von *ROR – CPA* ist, dann ist Π auch sicher im Sinne von *SOR – CO*.

Lemma 2: $[SOR - CO \not\Rightarrow ROR - CPA]$

Existiert ein Verschlüsselungsschema Π, das sicher im Sinne von *SOR – CO* ist, dann gibt es ein Verschlüsselungsschema Π′, das sicher im Sinne von *SOR – CO* ist, aber nicht sicher im Sinne von *ROR – CPA* ist.

$[SOR - CO \nRightarrow ROR - CPA]$ – Beweisskizze

Lemma 2: $[SOR - CO \nRightarrow ROR - CPA]$

Existiert ein Verschlüsselungsschema Π, das sicher im Sinne von $SOR - CO$ ist, dann gibt es ein Verschlüsselungsschema Π', das sicher im Sinne von $SOR - CO$ ist, aber nicht sicher im Sinne von $ROR - CPA$ ist.

Beweis.

- Annahme: $\Pi = (\text{GenKey}, \text{Enc}, \text{Dec})$, $SOR - CO$-sicher existiert
- Abgeleitet davon: $\Pi' = (\text{GenKey}', \text{Enc}', \text{Dec}')$, $SOR - CO$-sicher, aber nicht $ROR - CPA$-sicher
- Idee: 'spezieller Ciphertext', der $ROR - CPA$-Sicherheit widerspricht

□

$[SOR - CO \nRightarrow ROR - CPA]$ – abgeleitetes Kryptosystem

Sample struct — sample_1

$$\text{sample}_1 \in_R \{m \mid m = m_0 m_1 \dots m_n \ \wedge \ \forall i, j \text{ with } 0 \leq i, j \leq n \ . \ \exists m_i = j\}$$

Algorithms $\Pi' = (\text{GenKey}', \text{Enc}', \text{Dec}')$:

Algorithm $\text{GenKey}'(1^n)$:
- $k \leftarrow \text{GenKey}(1^n)$
- return k

Algorithm $\text{Enc}'_k(m)$:
- if $m = 0 \dots 0$
  - then $c := \sharp$
- else
  - $c \leftarrow \text{Enc}_k(m)$
- return c

Algorithm $\text{Dec}'_k(c)$:
- if $c = \sharp$
  - then $m := 0 \dots 0$
- else
  - $m := \text{Dec}_k(c)$
- return m

Beziehung zwischen *ROR – CPA* und *SOR – CO*

Theorem

SOR – CO ist schwächer als *ROR – CPA*.

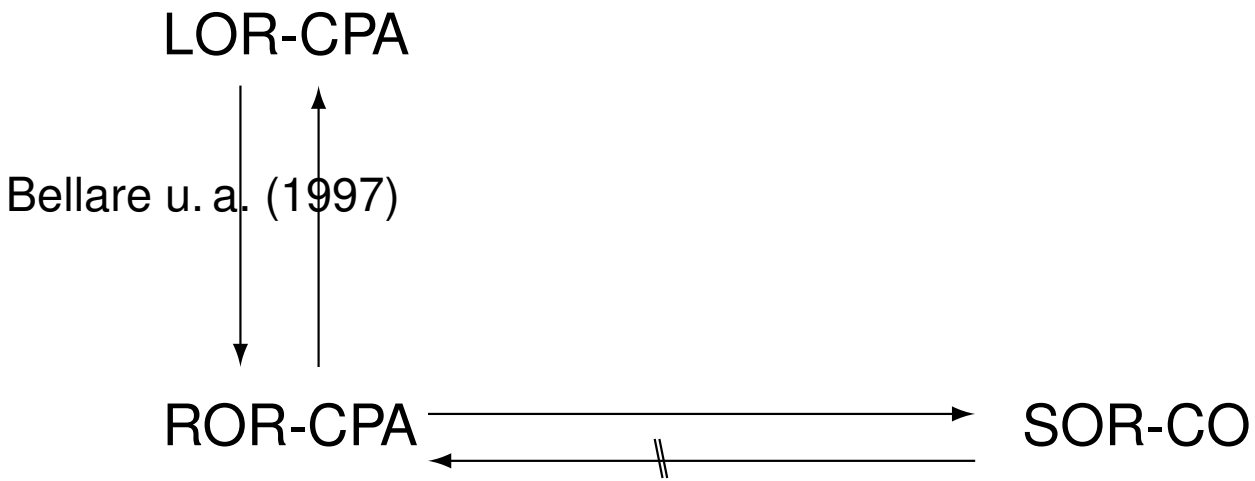
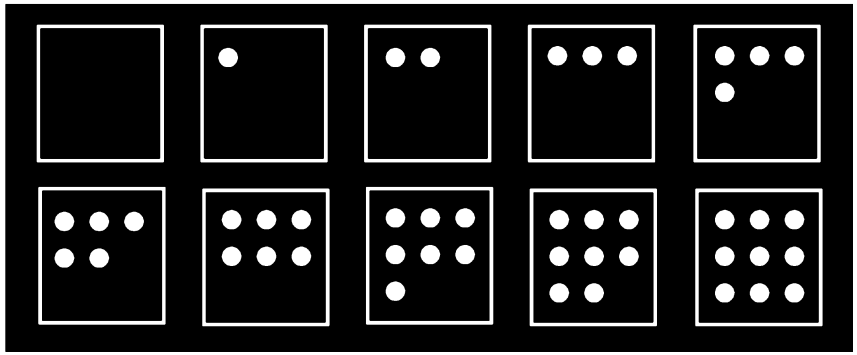


Abbildung: Beziehungen zwischen Sicherheitsmodellen für symmetrische Verschlüsselung

SOR – CO bei Dice Codings

- Differenz von 2 “Keypad-Ciphertexten” ist gerade
- Angreifer
  - Fragt nach 2 Ciphertexten
  - Falls Differenz gerade
    $\Rightarrow b = 0$ (’sample mode’)
  - Falls Differenz ungerade
    $\Rightarrow b = 1$ (’random mode’)

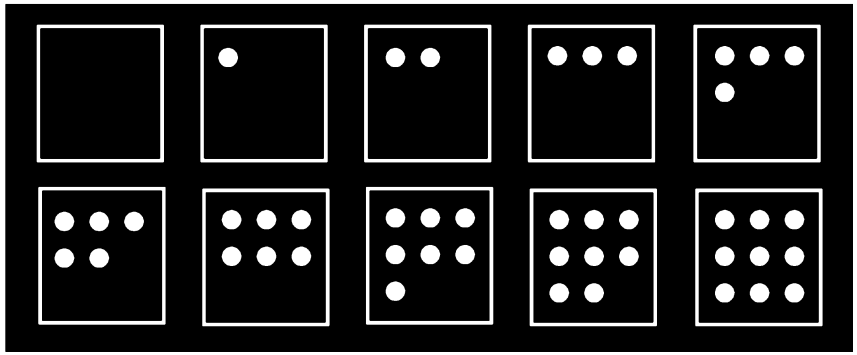


$$\begin{aligned}
\mathbf{Adv}^{sor-co}_{A,\Pi'}(n) &= Pr[\mathbf{Exp}^{sor-co-1}_{A,\Pi'}(n) = 1] && - Pr[\mathbf{Exp}^{sor-co-0}_{A,\Pi'}(n) = 1] \\
&= Pr[A = rand | O = rand] && - Pr[A = rand | O = samp] \\
&= \frac{1}{2} && - 0
\end{aligned}$$

- Idee Gegenmaßnahme: Rauschen in die Ciphertexte einfügen

SOR – CO bei Dice Codings

- Differenz von 2 “Keypad-Ciphertexten” ist gerade
- Angreifer
  - Fragt nach 2 Ciphertexten
  - Falls Differenz gerade
    $\Rightarrow b = 0$ (’sample mode’)
  - Falls Differenz ungerade
    $\Rightarrow b = 1$ (’random mode’)

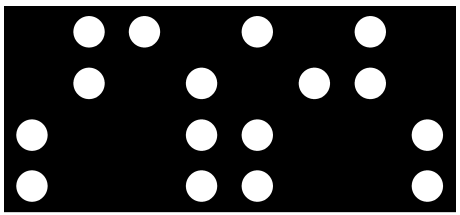


$$\begin{aligned}
\mathbf{Adv}^{sor-co}_{A,\Pi'}(n) &= Pr[\mathbf{Exp}^{sor-co-1}_{A,\Pi'}(n) = 1] && - Pr[\mathbf{Exp}^{sor-co-0}_{A,\Pi'}(n) = 1] \\
&= Pr[A = rand | O = rand] && - Pr[A = rand | O = samp] \\
&= \frac{1}{2} && - 0
\end{aligned}$$

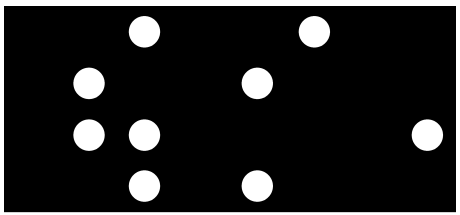
- Idee Gegenmaßnahme: Rauschen in die Ciphertexte einfügen

Dice Codings mit Rauschen – Beispiele

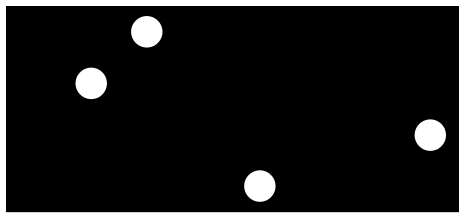
- Idee: Rauschen in die Ciphertexte einfügen

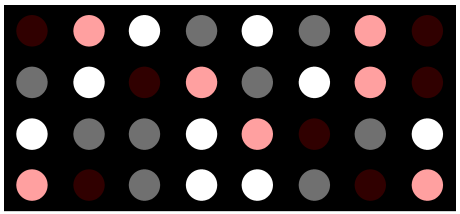

Ciphertext $c^\star$

+

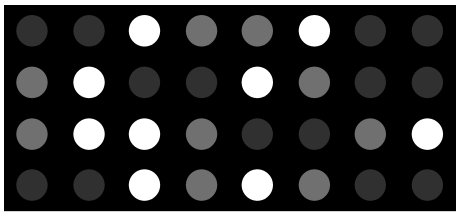

Key $k^\star$

=


Symbol $s^\star$ (4)


Ciphertext $c^\star$

+


Key $k^\star$

=

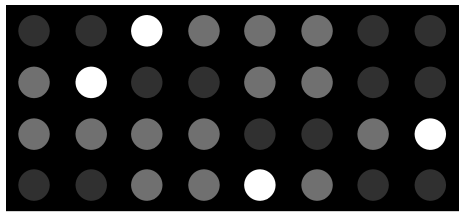
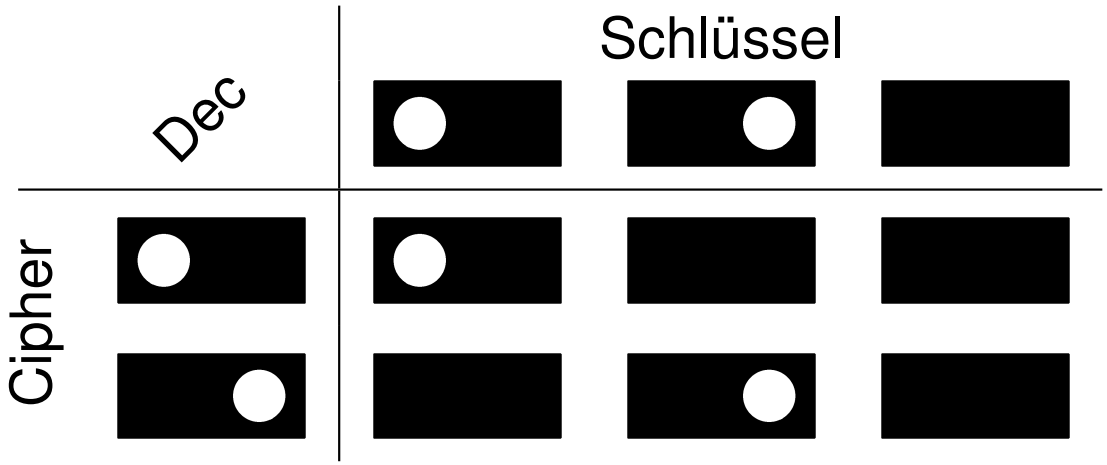

Symbol $s^\star$ (4)

Abbildung: Beispielvisualisierungen für $n = 9$ und $\nu = 7$

Dice Codings mit Rauschen – Details

$$\mathrm{Enc}^{\star}_{k^{\star}}(s) = \mathrm{Noise}_{k^{\star}}(\mathrm{Enc}_k(s)) := s \leftsquigarrow k^{\star}$$
$$\mathrm{Dec}^{\star}_{k^{\star}}(c^{\star}) = \mathrm{Dec}_k(\mathrm{Noise}^{-1}_{k^{\star}}(c^{\star})) := c^{\star} \leftrightarrow k^{\star}$$



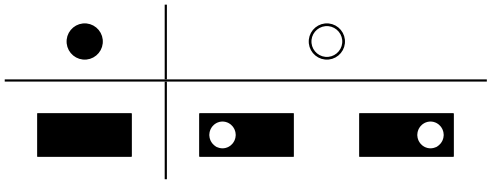
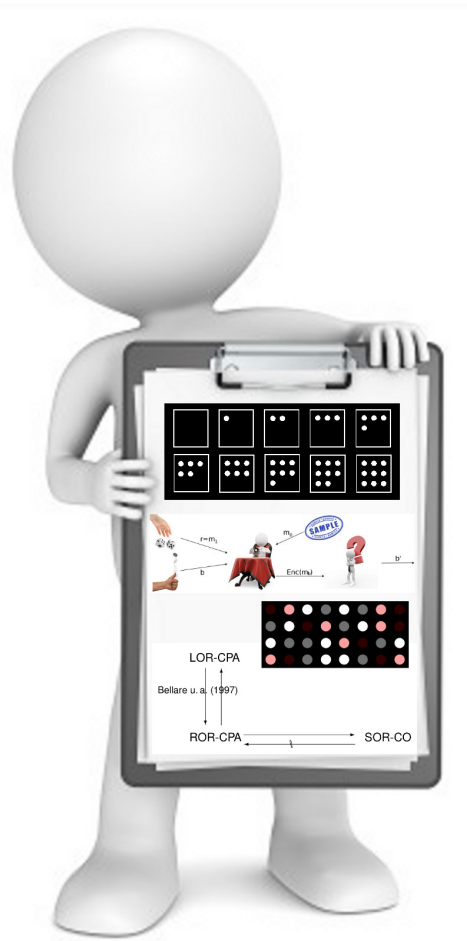


Abbildung: Kreuz und Auswertungstabelle

Zusammenfassung Teil 1

- Idee der visuellen Kryptographie
- Abgeschlossenes Encoding (Dice Codings)
- *SOR – CO* Sicherheitsmodell
  - Relation zu *ROR – CPA*
- Angriffe / Bewertung von VC basierend auf Dice Codings
- Erweiterte Version mit Rauschen



Ausblick Teil 1 – Dice Codings

- *SOR* – *CO*-Sicherheit von Dice Codings with Noise
- Vermutung: Mehr Rauschen erschwert es dem Angreifer
- Offene Frage: Bis zu wievielen Ciphertexten ist das System noch SOR-CO-sicher?
- Ziel: Anzahl der Ciphertexte abhängig von n und ν

Ausblick Teil 1 – Andere Sinne

- Ansprechen anderer Sinne
- Andere Encodings?
- Bessere Verschlüsselung?

Abbildung: Braille Anzeige

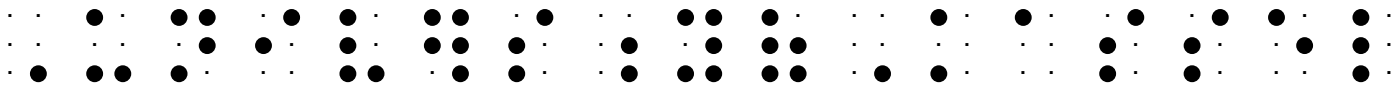


Abbildung: 'University of Kassel' in Grade 2 Braille

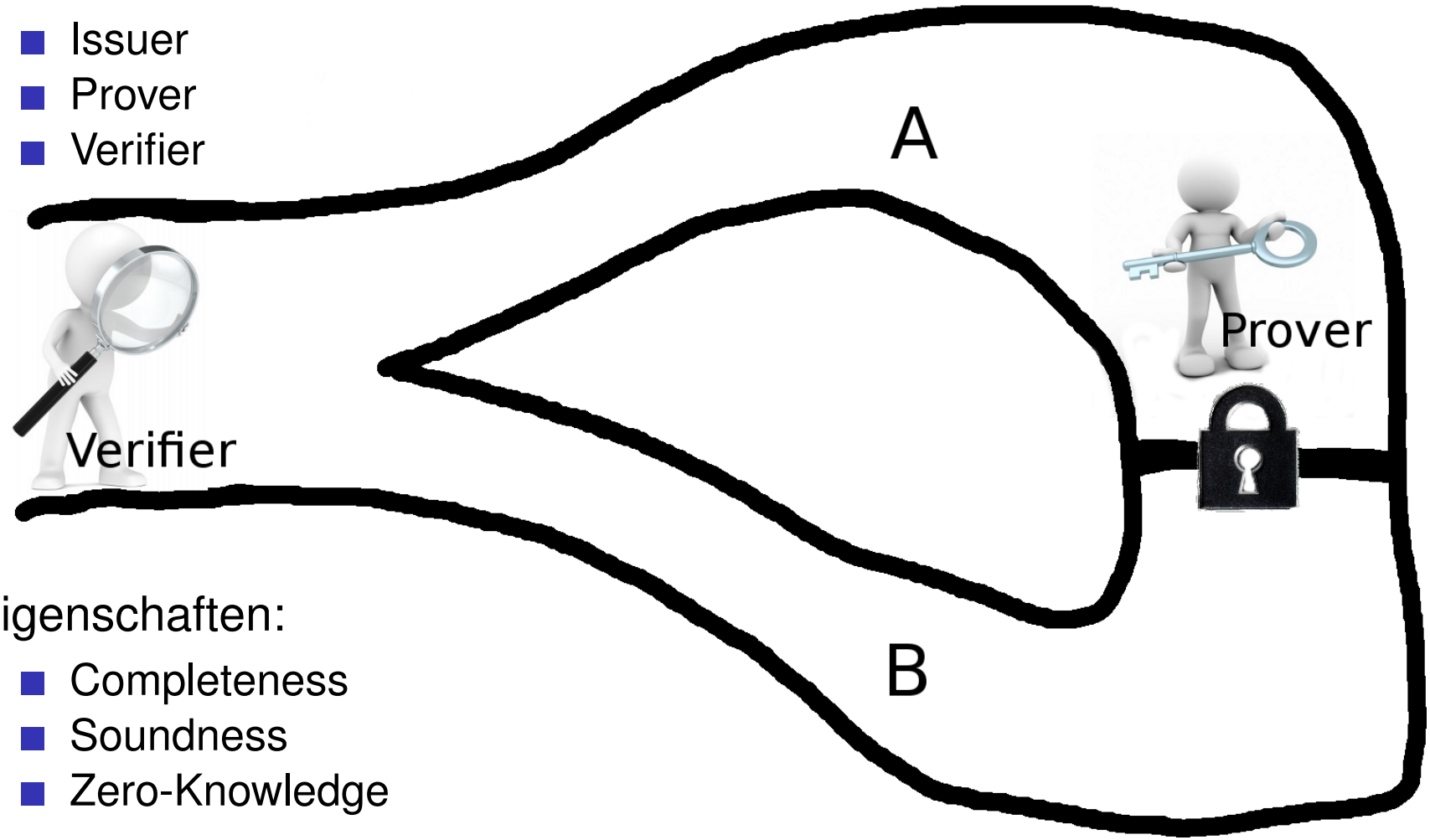
Übersicht

Anonyme Credentials - Einführung

- Anonym Attribute nachweisen
  - z.B. Altersnachweis, Nahverkehrstickets, Gesundheitssystem
- Idee von Chaum (1985)
- Gewinnt durch EDV an Bedeutung
- Aktionen eines Benutzers können nicht in Verbindung miteinander gebracht werden
- Nicht-Übertragbarkeit kann gewünscht sein

Zero-Knowledge-Proof (Quisquater u. a., 1990)

- Idee von Goldwasser, Micali und Rackoff (1989)
- 3 Beteiligte:
  - Issuer
  - Prover
  - Verifier



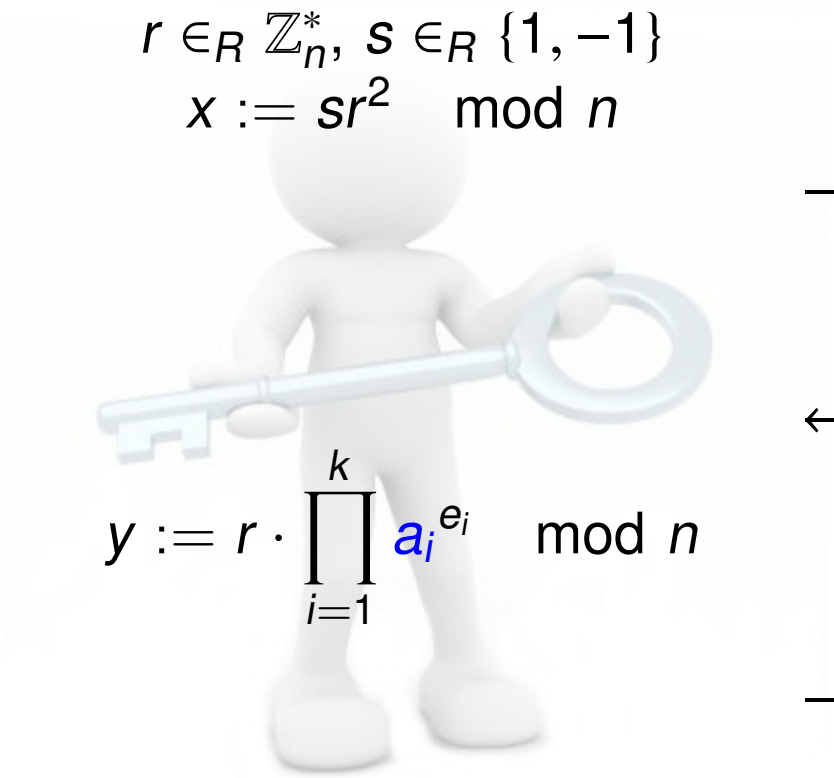
- Eigenschaften:
  - Completeness
  - Soundness
  - Zero-Knowledge

Feige-Fiat-Shamir Identification Scheme (Initialisierung)

Der Issuer ...

- ... wählt zwei Primzahlen p, q und berechnet $n = pq$
- ... wählt $a_1, \ldots, a_k \in \mathbb{Z}_n^*$
- ... berechnet $b_i = a_i^2 \mod n$
- ... sendet n und $a_1, \ldots, a_k$ an Prover
- ... sendet n und $b_1, \ldots, b_k$ an Verifier
- ... hält p, q geheim

Feige-Fiat-Shamir Identification Scheme (Protocol Run)



Prover

$r \in_R \mathbb{Z}_n^*,\ s \in_R \{1, -1\}$

$x := sr^2 \mod n$

$x \longrightarrow$

Verifier

wählt

$e_1, \ldots, e_k$ with $e_i \in \{0, 1\}$

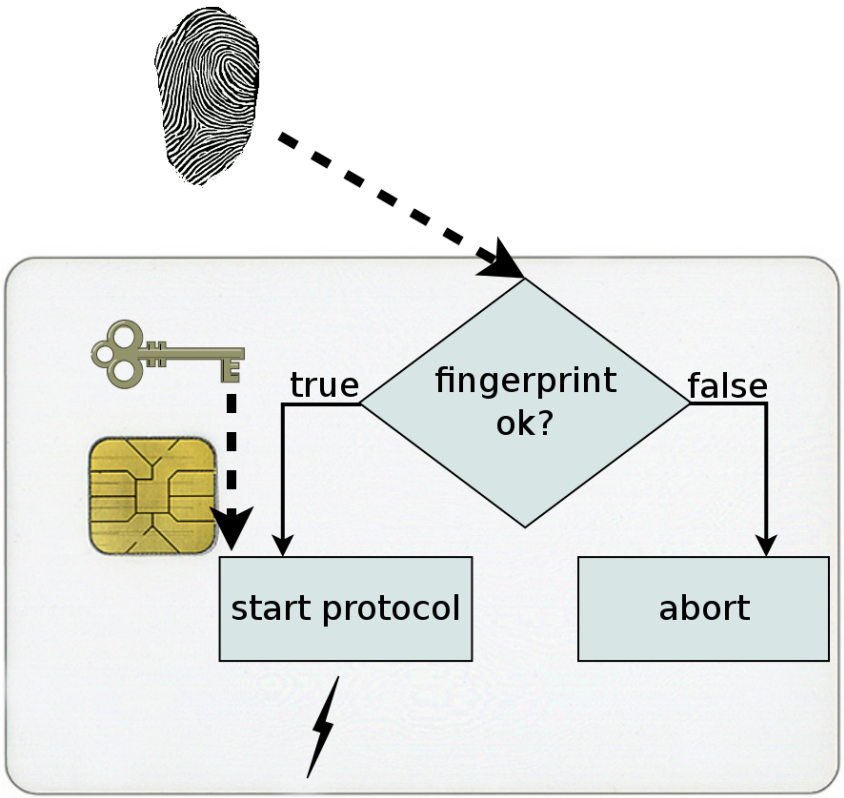
$\longleftarrow e_1, \ldots, e_k$

$y := r \cdot \prod_{i=1}^{k} a_i^{e_i} \mod n$

$y \longrightarrow$

$y^2 \stackrel{?}{=} \pm x \cdot \prod_{i=1}^{k} b_i^{e_i} \mod n$

Biometrische Zugangskontrolle + Zero-Knowledge-Proof



Biometrische Zugangskontrolle

$$y := r \cdot \prod_{i=1}^{k} a_i^{e_i} \mod n$$

- a_i auf Karte gespeichert

Bleumer (1998),
Impagliazzo und More (2003)

Abbildung: Nicht-Übertragbarkeit durch Benutzung biometrischer Zugangskontrolle

Angriffe auf das biometrische System

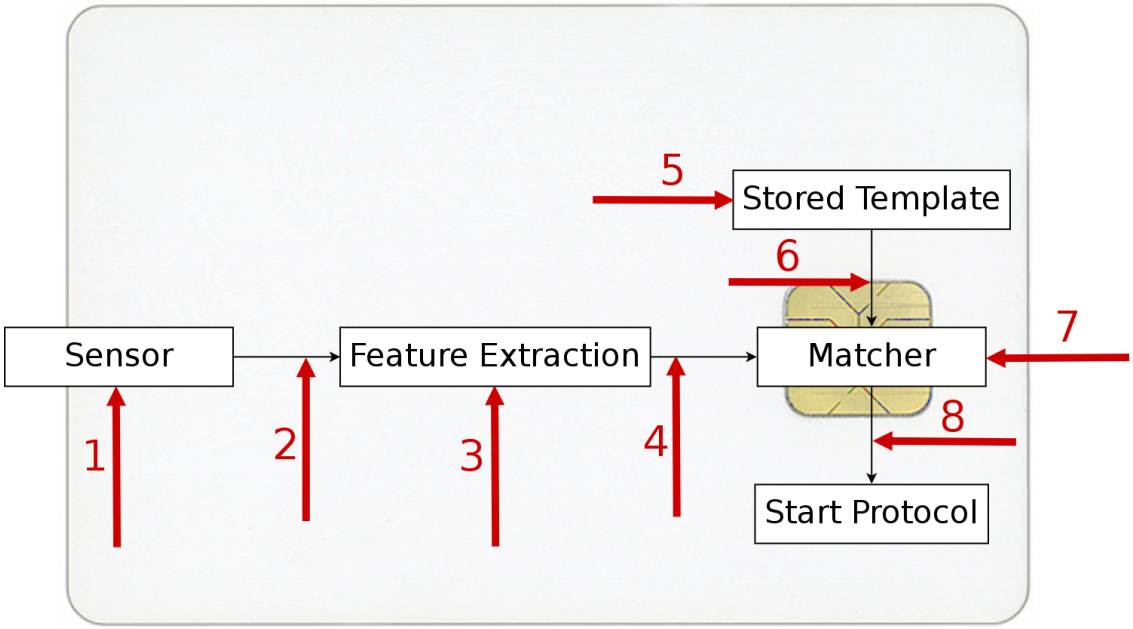
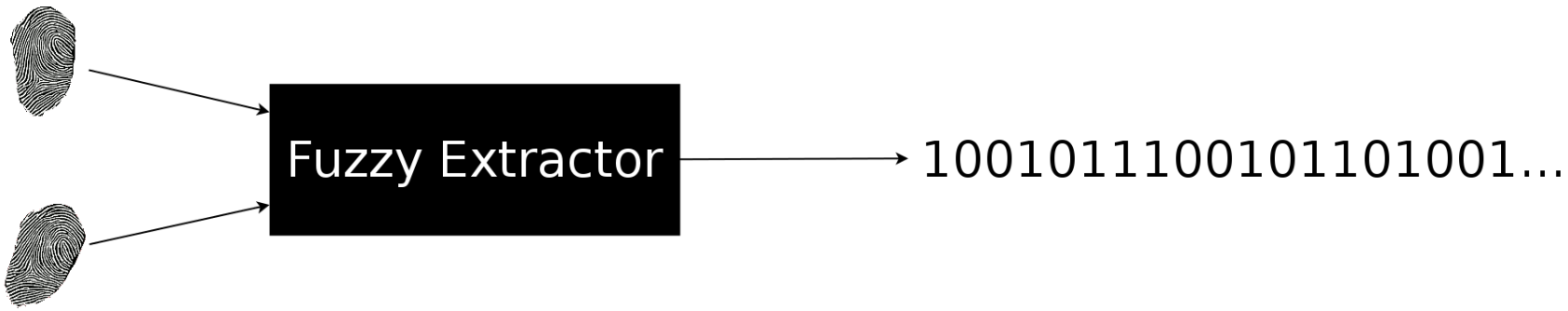


Abbildung: Angriffspunkte auf ein biometrisches System (nach Ratha, Connell und Bolle (2001))

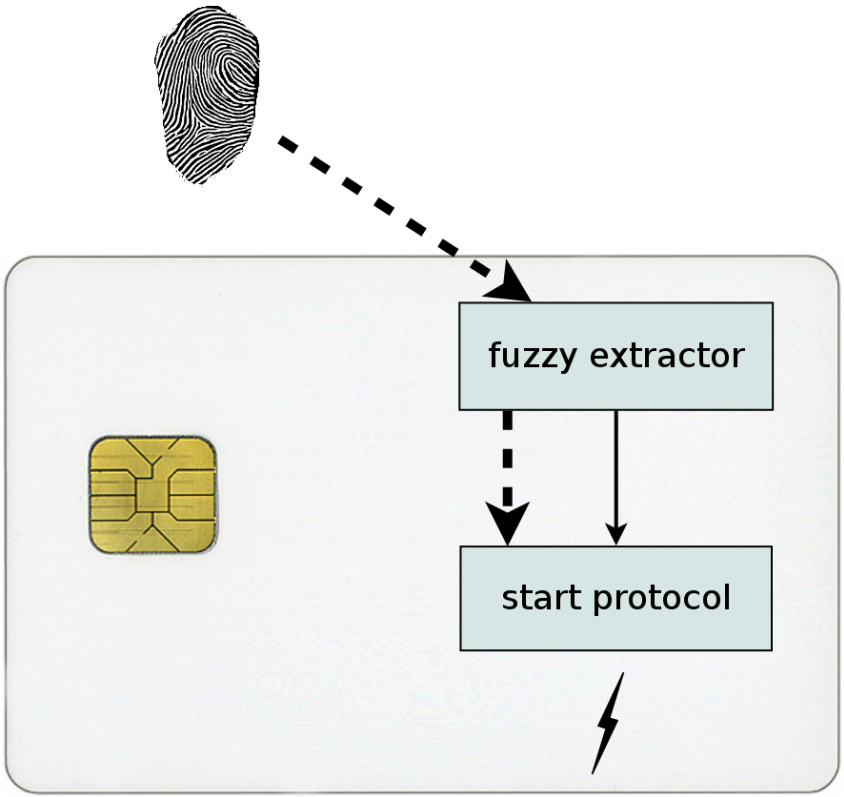
- Biometrische Daten vom Sensor ändern (2-4)
- Template auslesen (5)
- Template ändern (5,6)
- Matcher beeinflussen (7)
- Entscheidung des Matchers ändern (8)

Fuzzy Extractor

- Fuzzy vault schemes von Juels und Wattenberg (1999)
- Kryptographische Schlüssel aus biometrischen Daten ableiten
- “Fehler-korrigierende Hash-Funktion”



Fuzzy Extractor + Zero-Knowledge-Proof



Fuzzy Extractor

$$y := r \cdot \prod_{i=1}^{k} a_i^{e_i} \mod n$$

- a_i durch Fuzzy Extractor f_i

Bhargav-Spantzel, Squicciarini und Bertino (2006)

Abbildung: Nicht-Übertragbarkeit mittels Fuzzy Extractor

Angriffe auf den Fuzzy Extractor

- Falls Biometrische Daten bekannt: Geheimnis ableitbar
- Fingerabdrücke auf der Karte finden?
- Falls System schlecht aufgesetzt:
  - Unzureichende Bitlänge
  - Wiederverwendung von Werten

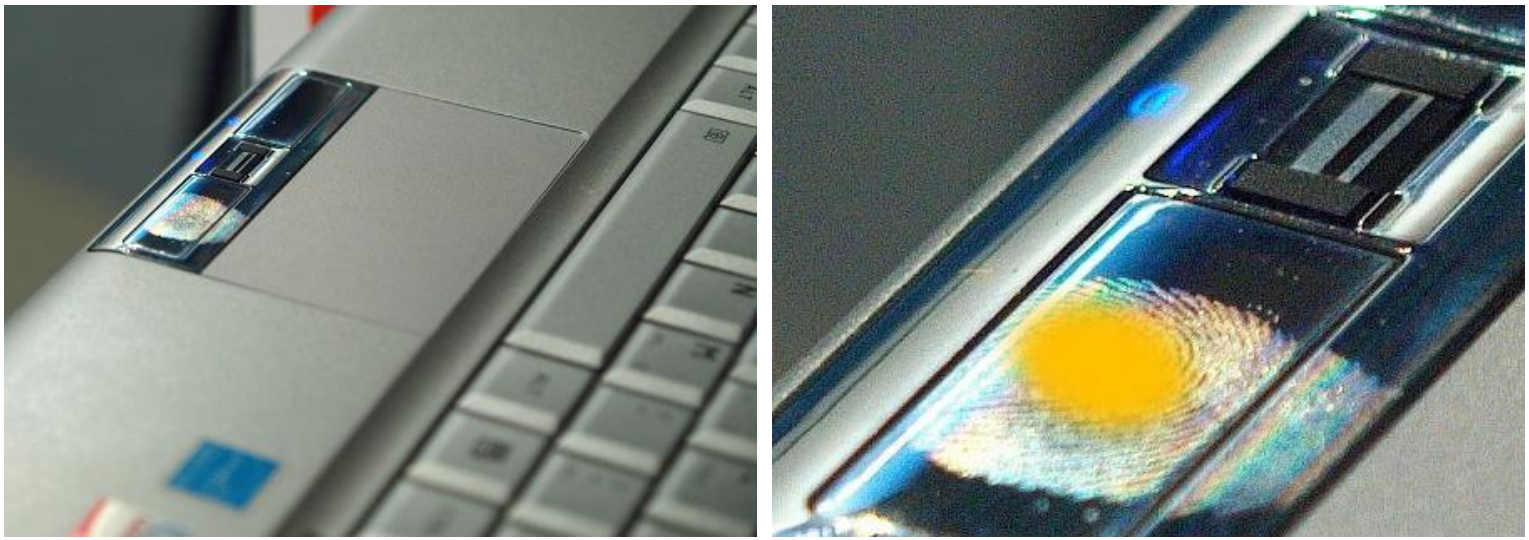
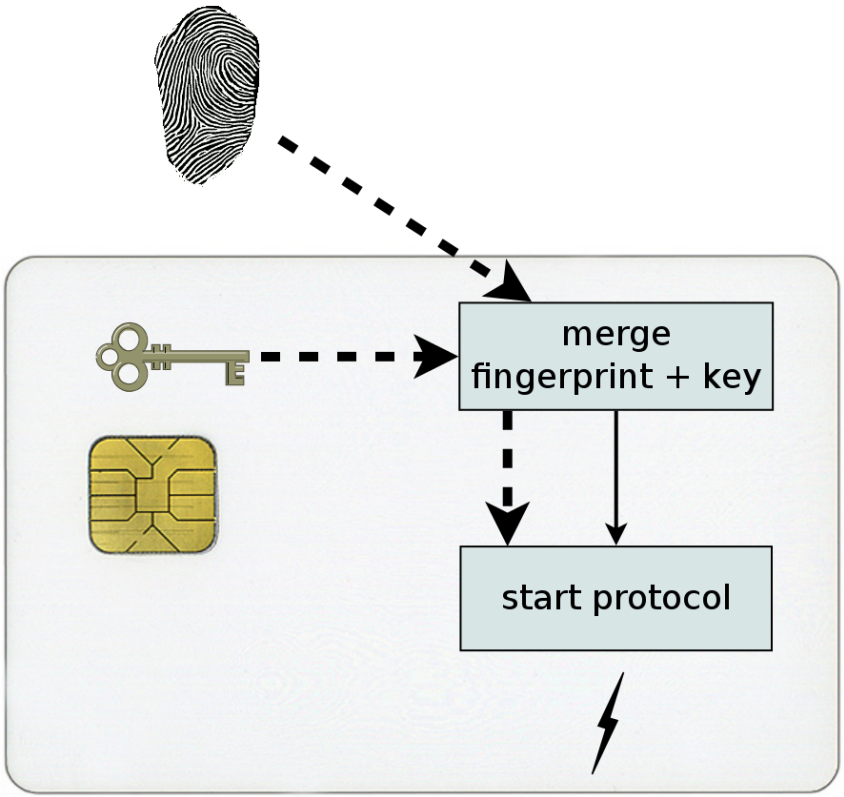


Abbildung: Fingerabdruck Cameron (2008)

Fuzzy Extractor + Geheimnis + Zero-Knowledge-Proof



Fuzzy Extractor + Geheimnis

$$y := r \cdot \prod_{i=1}^{k} a_i{}^{e_i} \mod n$$

- a_i durch Kombination von
  - Fuzzy Extractor f_i
  - Geheimnis s_i auf der Karte
- z.B. $a_i := f_i + s_i \mod n$

Abbildung: Nicht-Übertragbarkeit mittels Fuzzy Extractor + Geheimnis

Sicherheitsmodell Variation nach Wang u. a. (2012)

- Ursprünglich für Passwort-Authentifizierung mit Smartcards
- Angreifer hat entweder
  - Passwort / Biometrie des Benutzers oder
  - Smartcard

Verfahren	Angreifer kennt Biometrische Daten	Angreifer hat Smartcard
Biometrische Zugangskontrolle	keine	Umgehen der Zugriffskontrolle, Credent. benutzen Credentials auslesen Biometr. Daten auslesen
Fuzzy Extractor	Credential ableiten, falls Verfahren bekannt	keine
Fuzzy Extractor und Schlüssel	keine	keine

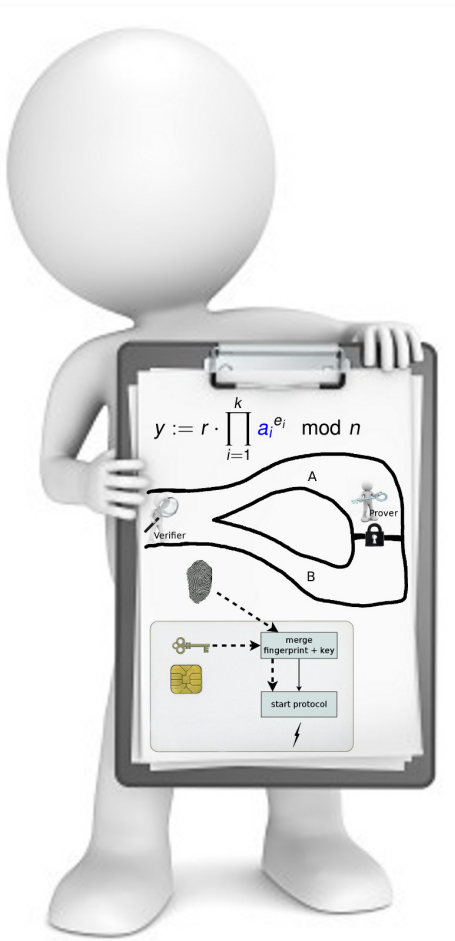
Sicherheitsmodell Variation nach Wang u. a. (2012)

- Ursprünglich für Passwort-Authentifizierung mit Smartcards
- Angreifer hat entweder
  - Passwort / Biometrie des Benutzers oder
  - Smartcard

Verfahren	Angreifer kennt Biometrische Daten	Angreifer hat Smartcard
Biometrische Zugangskontrolle	keine	Umgehen der Zugriffskontrolle, Credent. benutzen Credentials auslesen Biometr. Daten auslesen
Fuzzy Extractor	Credential ableiten, falls Verfahren bekannt	keine
Fuzzy Extractor und Schlüssel	keine	keine

Zusammenfassung Teil 2

- Nicht-Übertragbare anonyme Credentials
- Kombination mit Biometrie
- Vergleich verschiedener Ansätze
- Neuer Ansatz: Kombination Fuzzy Extractor mit Geheimnis auf Smartcard



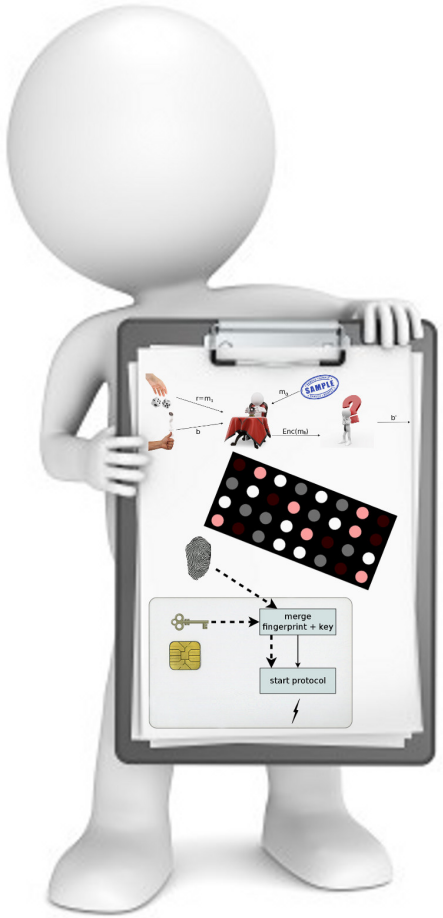
Ausblick Teil 2

- Prototyp erstellen
  - Smartcards nicht verfügbar
  - Bestimmung von false accept/reject Raten
  - Welche Geräte geeignet?
- Gibt es andere geeignete biometrische Merkmale?
- Wie Anonymität aufheben, wenn Fingerabdruck falsch?

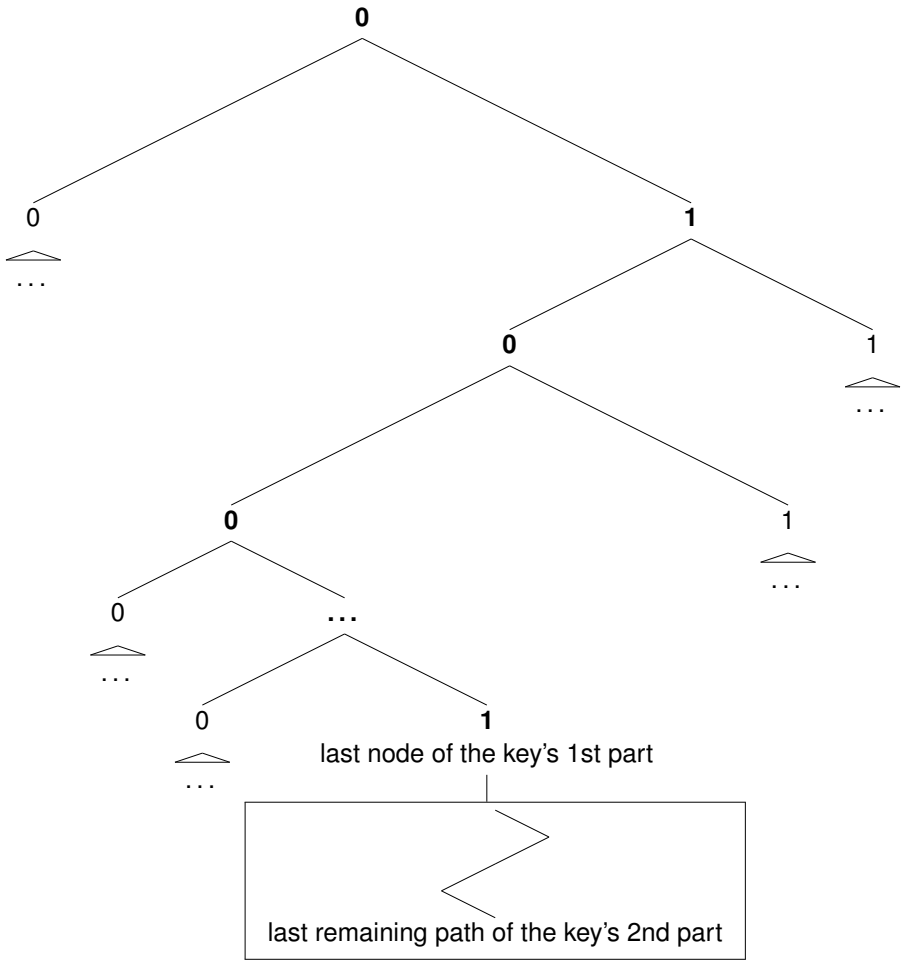
Übersicht

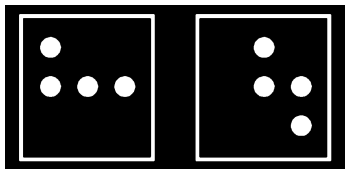
Zusammenfassung

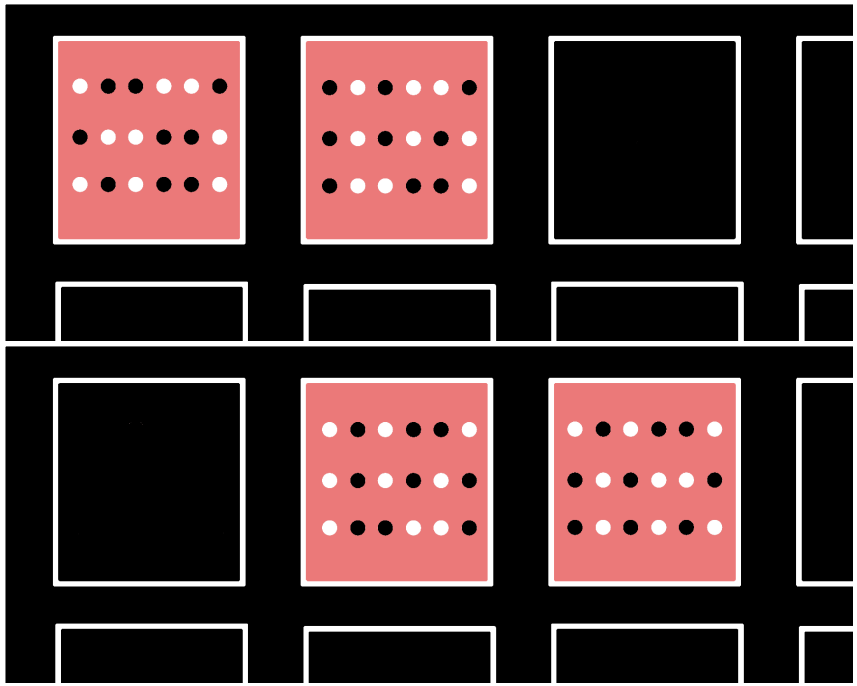
- Von Menschen entschlüsselbare Verschlüsselungssysteme
  - Getrennte Betrachtung von Enkodierung und Verschlüsselung
  - Verallgemeinerung von visueller Kryptographie
  - Definition Sicherheitsmodell *SOR – CO*
    - Relation zu *ROR – CPA*
  - Dice Codings
    - Sicherheitsanalyse
    - Verbesserung durch Rauschen
- Nicht-Übertragbare Anonyme Credentials
  - Vergleich und Sicherheitsanalyse
    Biometrische Authentifizierung / Geheimnisse
  - Kombination Fuzzy Extractor mit Geheimnis auf Smartcard

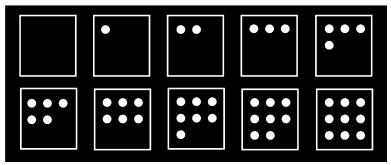


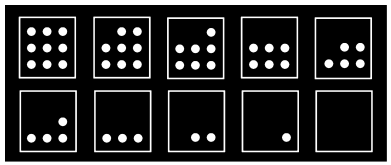
HDES - Angriff auf Ciphertext-Paare











HDES - Kombination von Folien

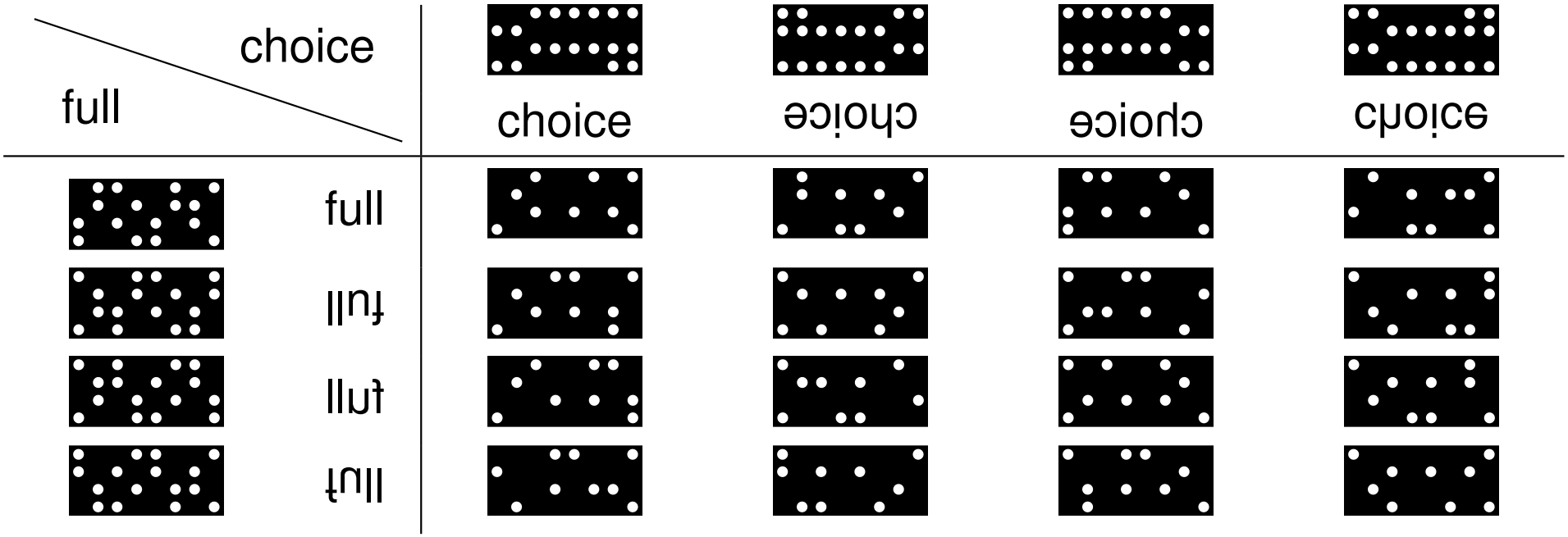
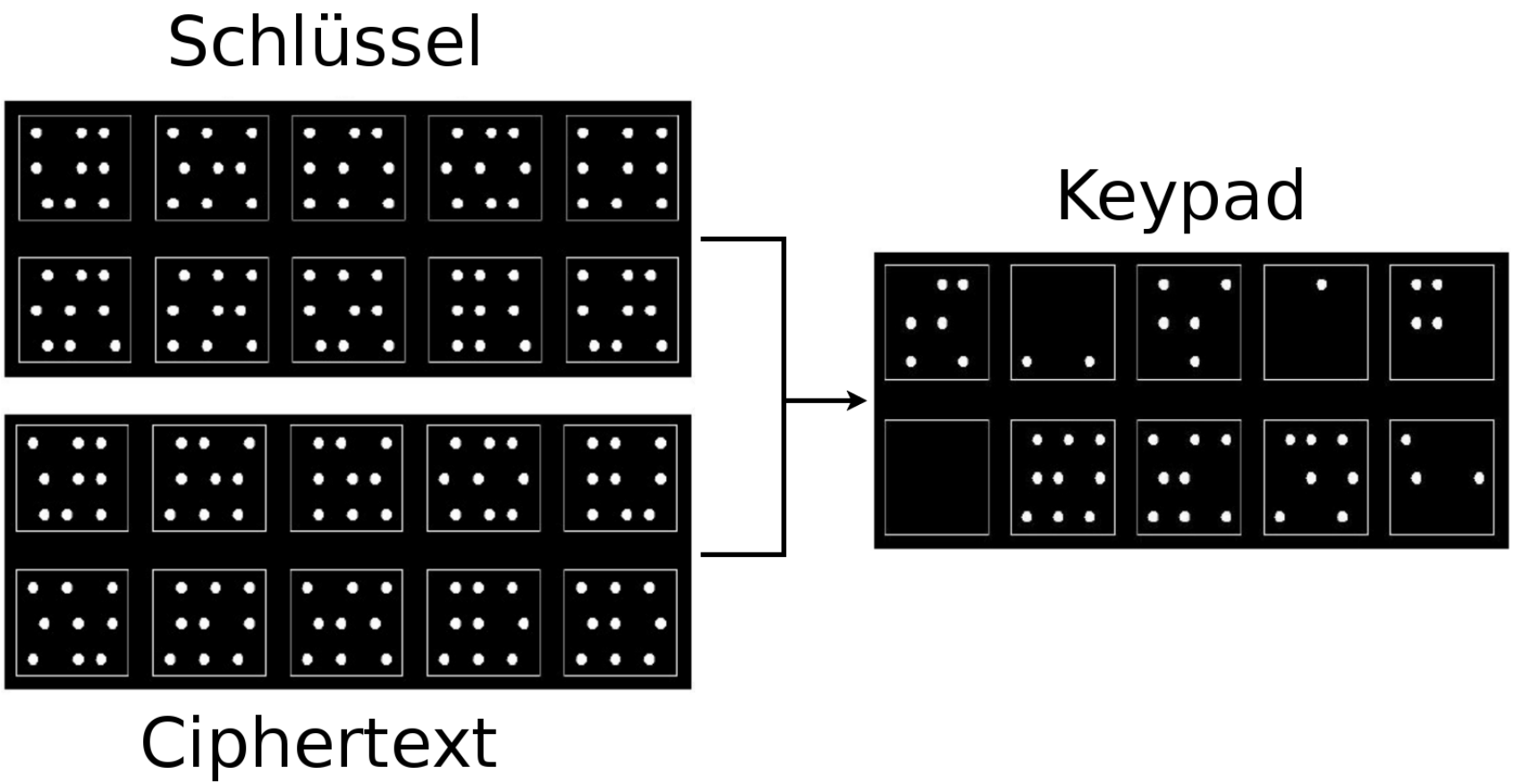


Abbildung: Komposition von Schlüsseln

Dice Codings - Beispiel Keypad



[$SOR - CO \nRightarrow ROR - CPA$] Lemma 2a - Details

Lemma 2a

$\Pi' = (\text{GenKey}', \text{Enc}', \text{Dec}')$ is not secure in the sense of $ROR - CPA$.

Beweis.

- Adversary asks $\mathcal{O}_{\mathcal{RR}}(\cdot, b)$ for encryption of '0 . . . 0'.
- If $\mathcal{O}_{\mathcal{RR}} \rightarrow \sharp \quad \Rightarrow \quad b = 0$ ('real mode')
- If $\mathcal{O}_{\mathcal{RR}} \nrightarrow \sharp \quad \Rightarrow \quad b = 1$ ('random mode')

$$\begin{aligned}\mathbf{Adv}^{ror-cpa}_{A_{cpa},\Pi'}(n) &= Pr[\mathbf{Exp}^{ror-cpa-1}_{A_{cpa},\Pi'}(n) = 1] \quad - Pr[\mathbf{Exp}^{ror-cpa-0}_{A_{cpa},\Pi'}(n) = 1] \\ &= 1 - \frac{1}{(n+1)^{n+1}} \qquad\qquad - 0\end{aligned}$$

□

[$SOR - CO \nRightarrow ROR - CPA$] Lemma 2b - Details

Lemma 2b

$\Pi' = (\text{GenKey}', \text{Enc}', \text{Dec}')$ is secure in the sense of $SOR - CO$ given the sample structure sample_1.

Beweis.

- $b = 0$ ('sample mode'): No change, $0 \ldots 0$ never appears
- $b = 1$ ('random mode'): Negligible $Adv_\sharp$, $Pr[0 \ldots 0] = \frac{1}{(n+1)^{n+1}}$

$$\begin{aligned}
\mathbf{Adv}^{sor-co}_{A,\Pi'}(n) &= Pr[\mathbf{Exp}^{sor-co-1}_{A,\Pi'}(n) = 1] && - Pr[\mathbf{Exp}^{sor-co-0}_{A,\Pi'}(n) = 1] \\
&\leq Pr[\mathbf{Exp}^{sor-co-1}_{A,\Pi}(n) = 1] + Adv_\sharp && - Pr[\mathbf{Exp}^{sor-co-0}_{A,\Pi}(n) = 1] \\
&= \mathbf{Adv}^{sor-co}_{A,\Pi}(n) + Adv_\sharp
\end{aligned}$$

□

Dice Codings with Noise – Ext

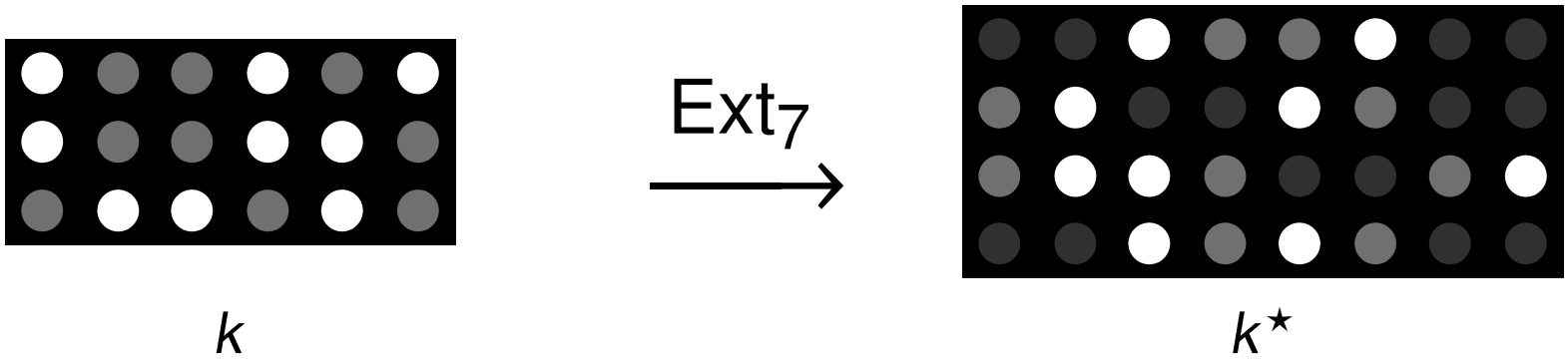


Abbildung: Sample Visualisation of the Ext Function for $n = 9$ and $\nu = 7$ with Black Segments Shown in Dark Grey

Dice Codings with Noise – Noise

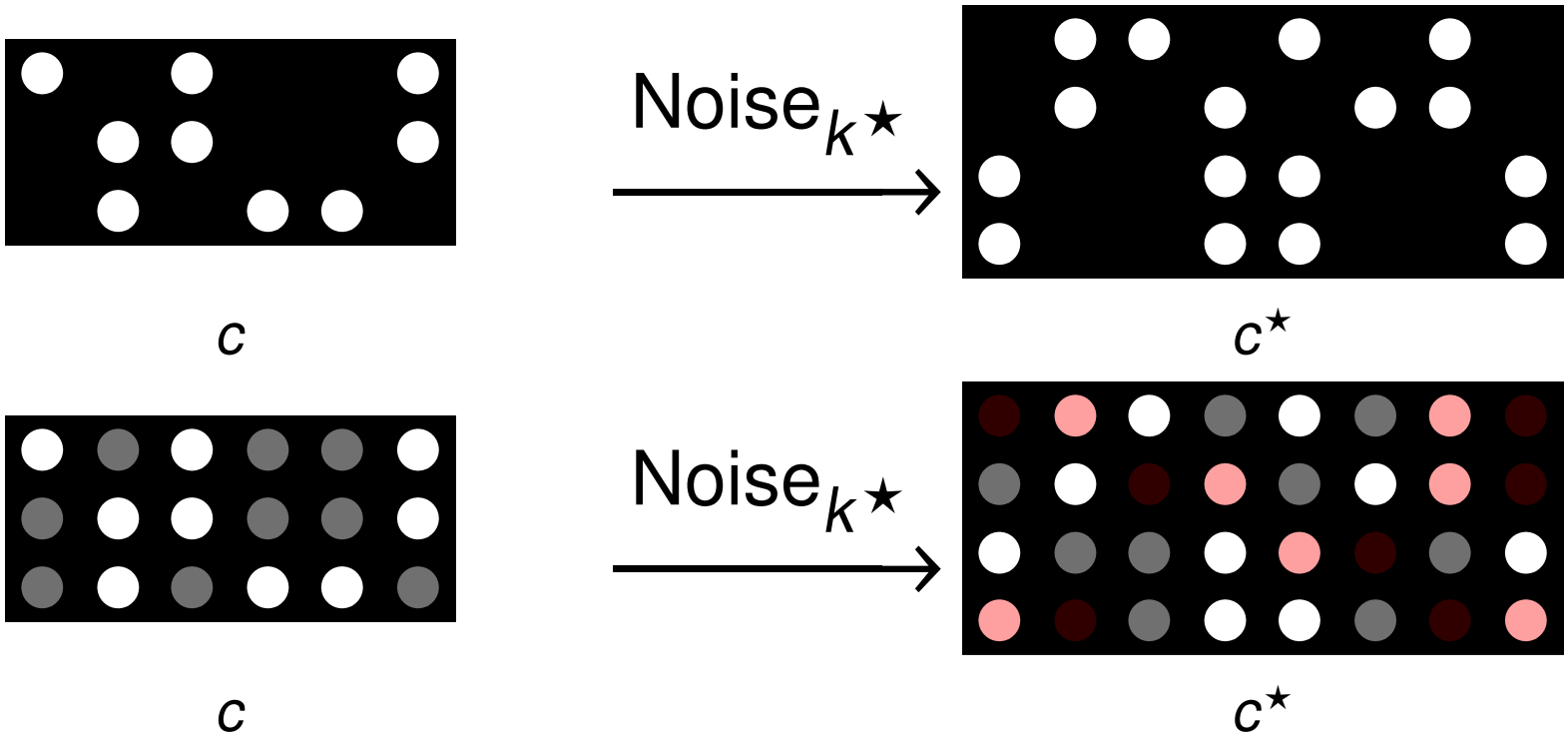


Abbildung: Sample Visualisations of the Noise Function with $k^\star$ from Fig. 22 for $n = 9$ and $\nu = 7$

Dice Codings with Noise – Noise^{-1}

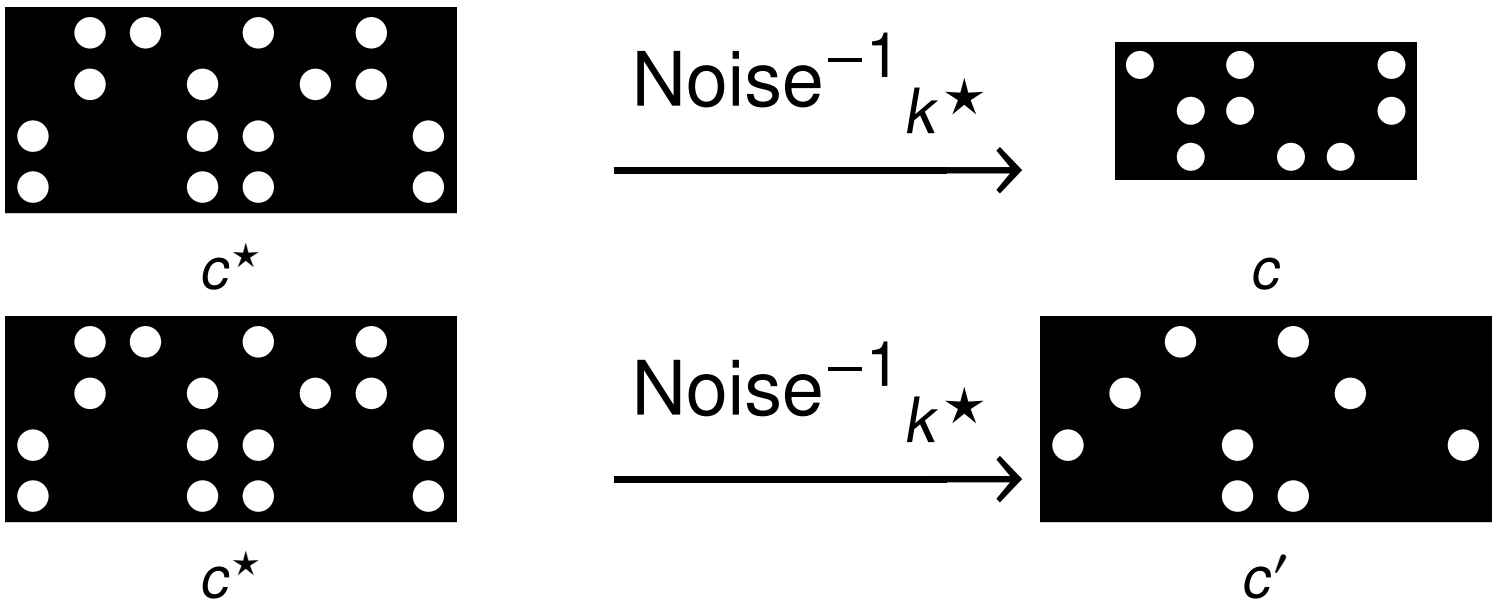


Abbildung: Sample Visualisations of the Noise^{-1} Function with $k^\star$ from Fig. 22 for $n = 9$ and $\nu = 7$

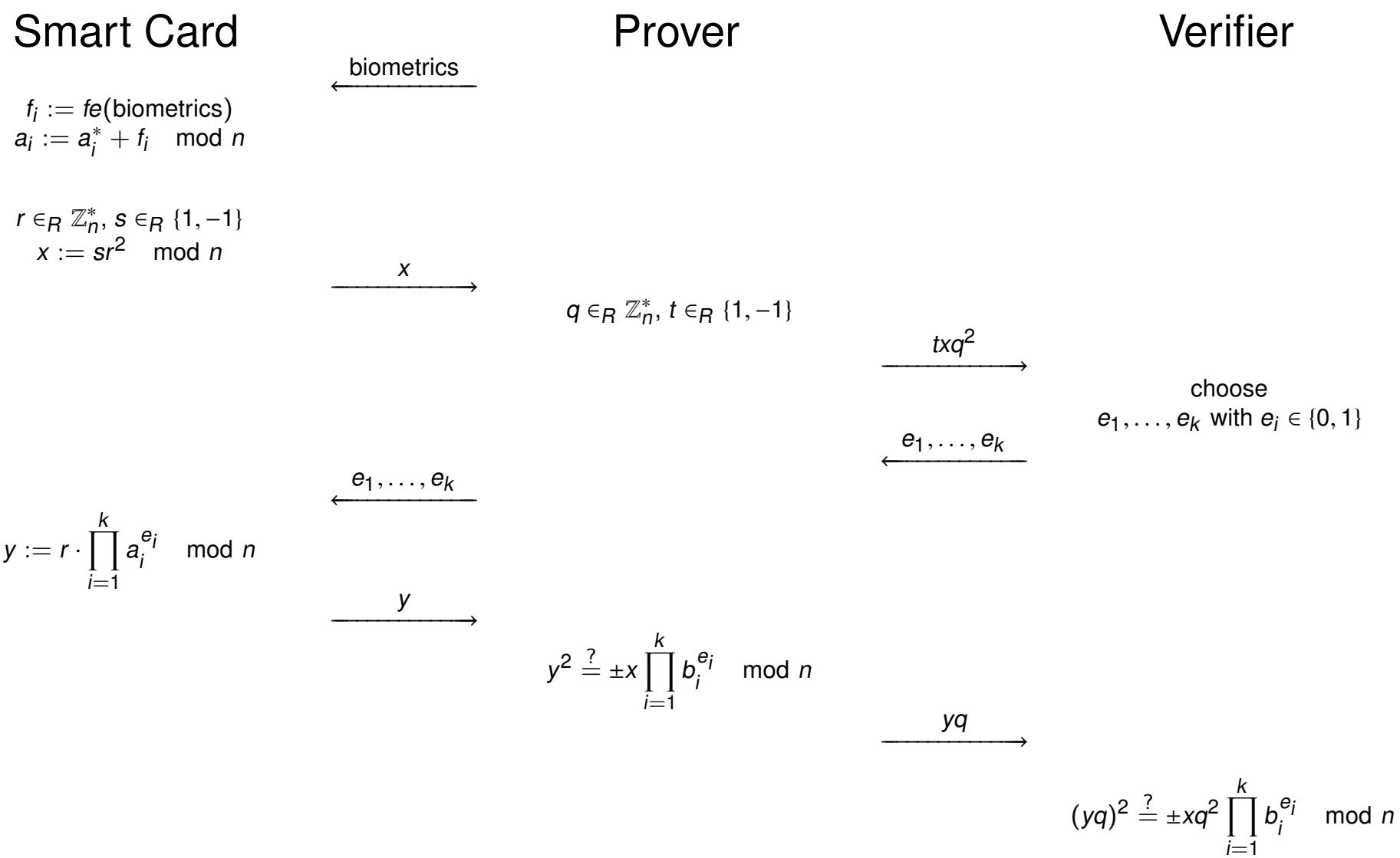


Abbildung: Modified Feige-Fiat-Shamir Identification Scheme

References I

[Bellare u. a. 1997] Bellare, Mihir ; Desai, Anand ; Jokipii, E. ; Rogaway, Phillip: A Concrete Security Treatment of Symmetric Encryption. In: *Proceedings of 38th Annual Symposium on Foundations of Computer Science (FOCS 97)*, 1997, S. 394–403

[Bhargav-Spantzel u. a. 2006] Bhargav-Spantzel, Abhilasha ; Squicciarini, Anna ; Bertino, Elisa: Privacy preserving multi-factor authentication with biometrics. In: *DIM '06: Proceedings of the second ACM workshop on Digital identity management*. New York, NY, USA : ACM, 2006, S. 63–72. – ISBN 1-59593-547-9

[Bleumer 1998] Bleumer, Gerrit: Biometric yet Privacy Protecting Person Authentication. In: *Lecture Notes in Computer Science* 1525 (1998), S. 99–110. – URL citeseer.ist.psu.edu/article/bleumer98biometric.html

[Borchert 2007] Borchert, Bernd: Segment-based Visual Cryptography / Wilhelm-Schickard-Institut für Informatik, Tübingen. 2007 (WSI-2007-04). – Forschungsbericht

[Cameron 2008] Cameron, Kim: *Fingerprint charade*. Kim Cameron's Identity Weblog, http://www.identityblog.com/?p=981. May 2008. – last access 2013/05/21

[Chaum 1985] Chaum, David: Security without identification: transaction systems to make big brother obsolete. In: *Communications of the ACM* 28 (1985), Nr. 10, S. 1030–1044

[Doberitz 2008] Doberitz, Denise: *Visual Cryptography Protocols and their Deployment against Malware*, Ruhr-Universität Bochum, Germany, Diplomarbeit, 2008

[Goldwasser u. a. 1989] Goldwasser, Shafi ; Micali, Silvio ; Rackoff, Charles: The knowledge complexity of interactive proof systems. In: *SIAM J. Comput.* 18 (1989), Nr. 1, S. 186–208. – ISSN 0097-5397

[Impagliazzo und More 2003] Impagliazzo, Russell ; More, Sara M.: Anonymous Credentials with Biometrically-Enforced Non-Transferability. In: *Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society (WPES '03)* ACM (Veranst.), 2003, S. 60–71

[Juels und Wattenberg 1999] Juels, Ari ; Wattenberg, Martin: A fuzzy commitment scheme. In: *Proceedings of the 6th ACM conference on Computer and communications security*. New York, NY, USA : ACM, 1999 (CCS '99), S. 28–36. – URL http://doi.acm.org/10.1145/319709.319714. – ISBN 1-58113-148-8

References II

[Naor und Shamir 1994] Naor, Moni ; Shamir, Adi: Visual Cryptography. In: Santis, Alfredo D. (Hrsg.): *EUROCRYPT* Bd. 950, Springer, 1994, S. 1–12. – ISBN 3-540-60176-7

[Quisquater u. a. 1990] Quisquater, Jean-Jacques ; Guillou, Louis C. ; Berson, Thomas A.: How to Explain Zero-Knowledge Protocols to Your Children. In: *Advances in Cryptology - CRYPTO '89: Proceedings* Bd. 435, 1990, S. 628–631

[Ratha u. a. 2001] Ratha, Nalini K. ; Connell, Jonathan H. ; Bolle, Ruud M.: Enhancing security and privacy in biometrics-based authentication systems. In: *IBM Systems Journal* 40 (2001), March, Nr. 3, S. 614–634. – URL `http://dx.doi.org/10.1147/sj.403.0614`. – ISSN 0018-8670

[Wang u. a. 2012] Wang, Ding ; Ma, Chun guang ; Wang, Ping ; Chen, Zhong: *Robust Smart Card based Password Authentication Scheme against Smart Card Security Breach*. Cryptology ePrint Archive, Report 2012/439. 2012. – `http://eprint.iacr.org/`