Sample or Random Security – A Security Model for Segment-Based Visual Cryptography

Sebastian Pape

Dortmund Technical University

March 5th, 2014

Financial Cryptography and Data Security 2014

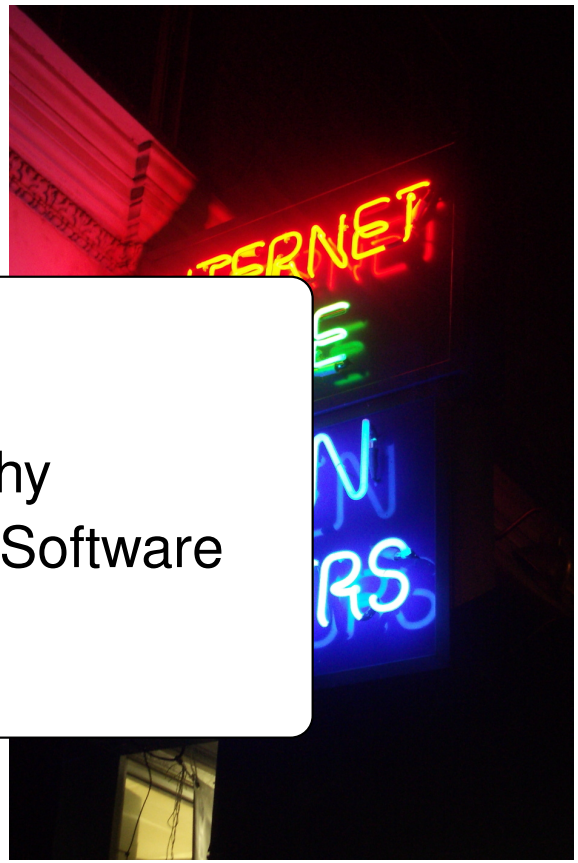
Overview

1 Introduction
- Visual Cryptography

2 Sample-Or-Random Security

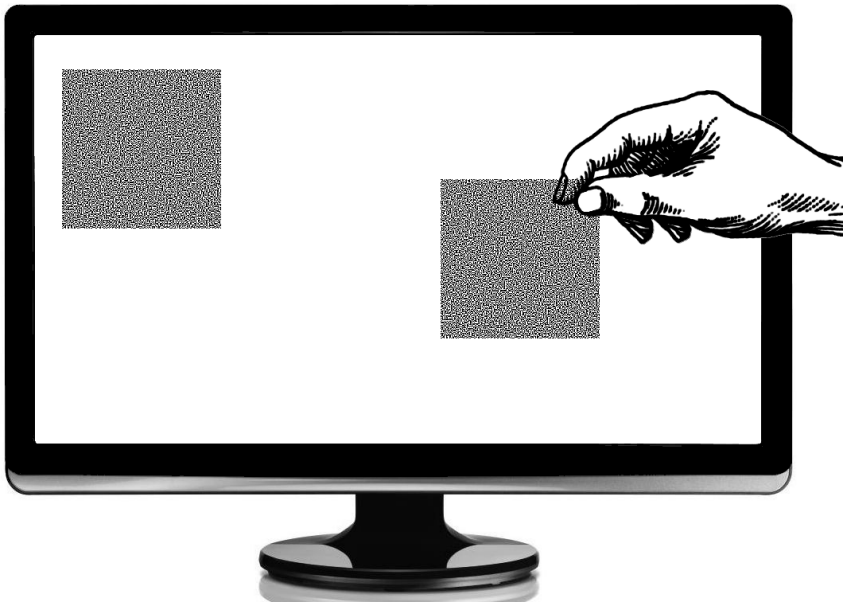
3 Summary and Outlook

Scenario



Untrustworthy
Hardware / Software

Visual Cryptography - Idea



(a) Transparencies side by side

(b) Transparencies stacked

Pixel-based Visual Crypt. (Naor and Shamir, 1994)

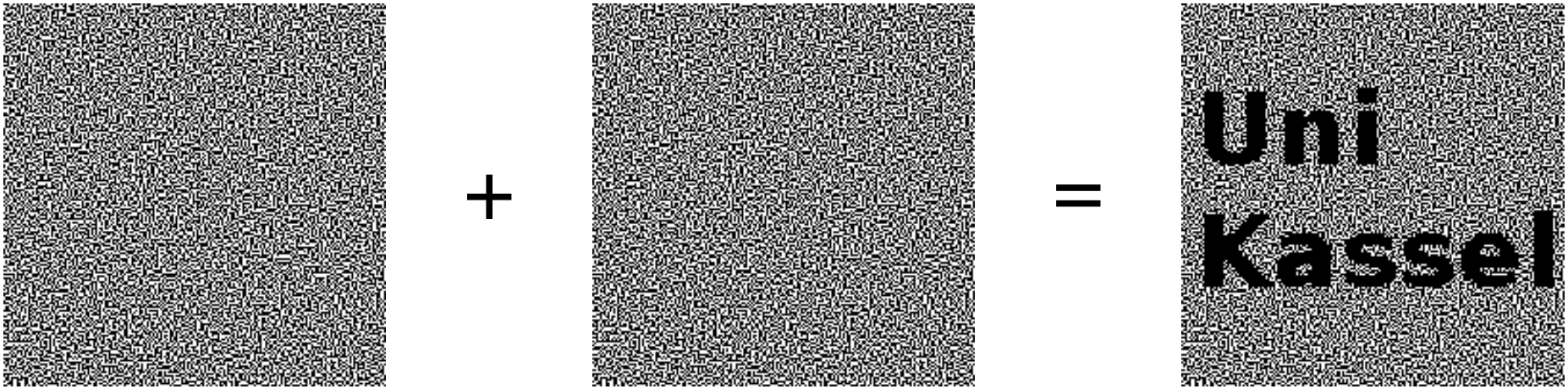


Figure: Example

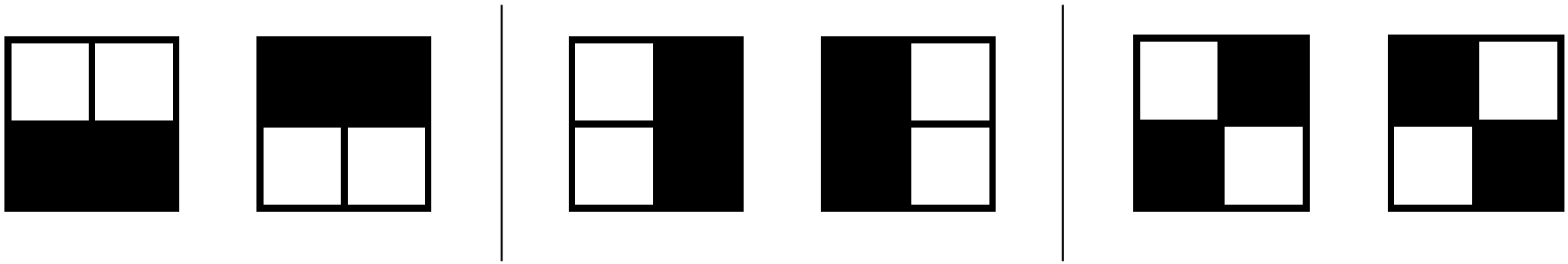
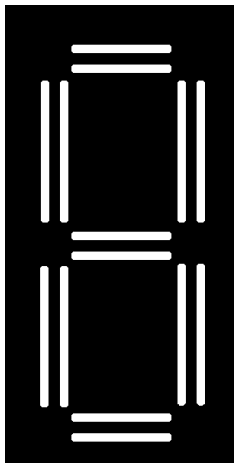
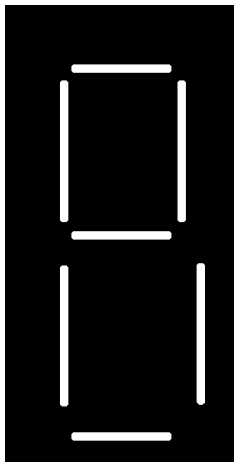


Figure: Shares With 4 Sub-pixels in a 2x2 Matrix

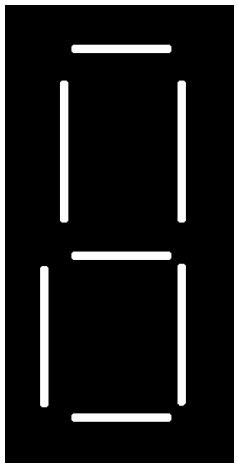
Segment-based Visual Cryptography (Borchert, 2007)



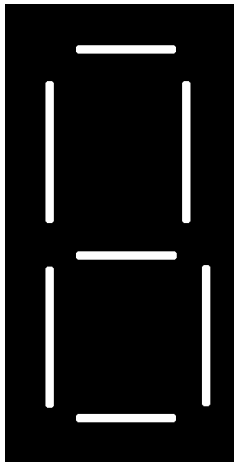
(a) full



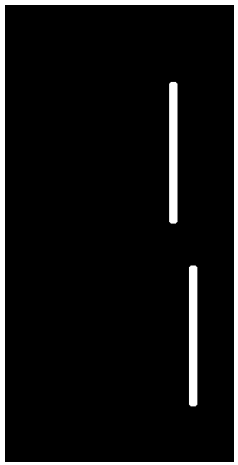
(b) c_1



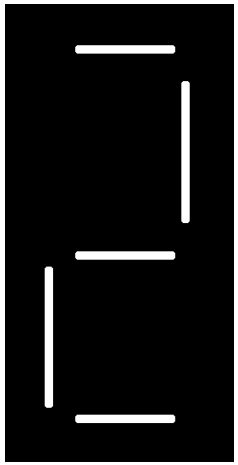
(c) c_2



(d) k



(e) $c_1 \leftrightarrow k$



(f) $c_2 \leftrightarrow k$

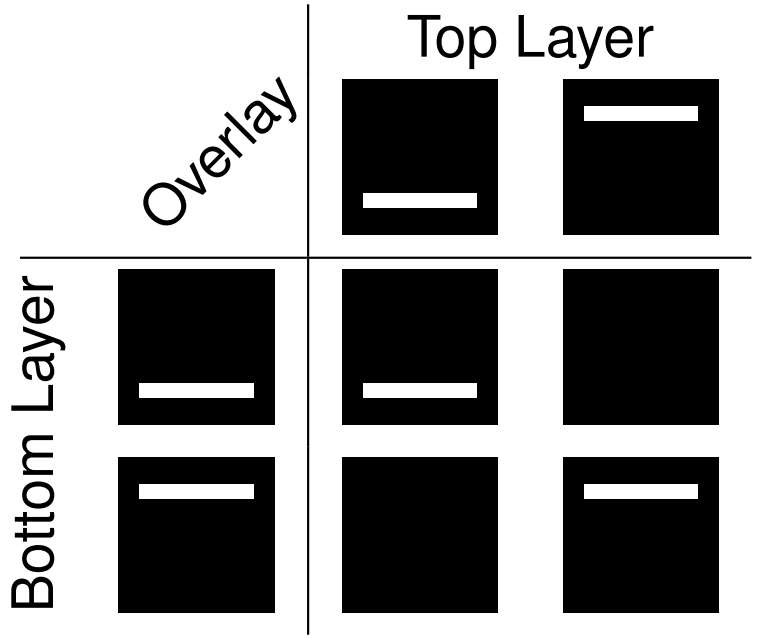
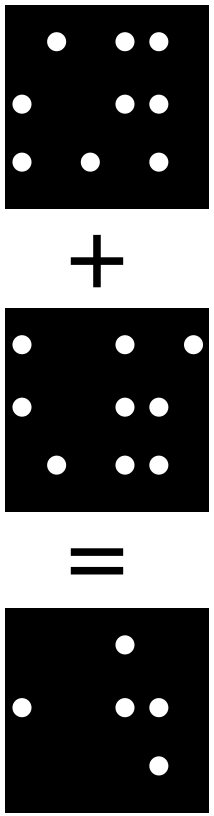


Table: Contingency Table

Dice Codings (Doberitz, 2008)



Ciphertext

\+

Key

=

Plaintext (5)

Cipher \ Dec	Key	
		
		
		

Table: Contingency Table

Visual Cryptography - Application

Figure: Keypad of a cash machine

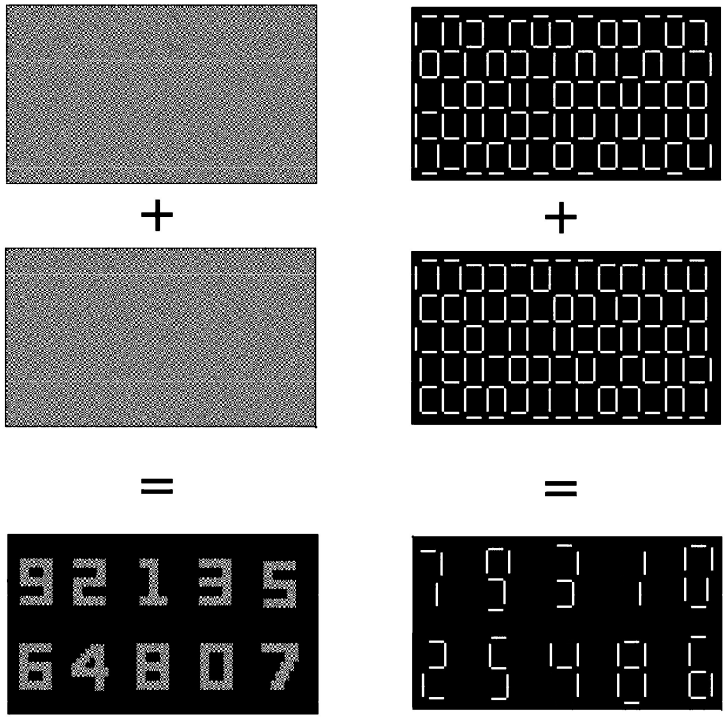


Figure: Keypads in visual Cryptography (Borchert, 2007)

Reminder: Reusing Key-Transparencies

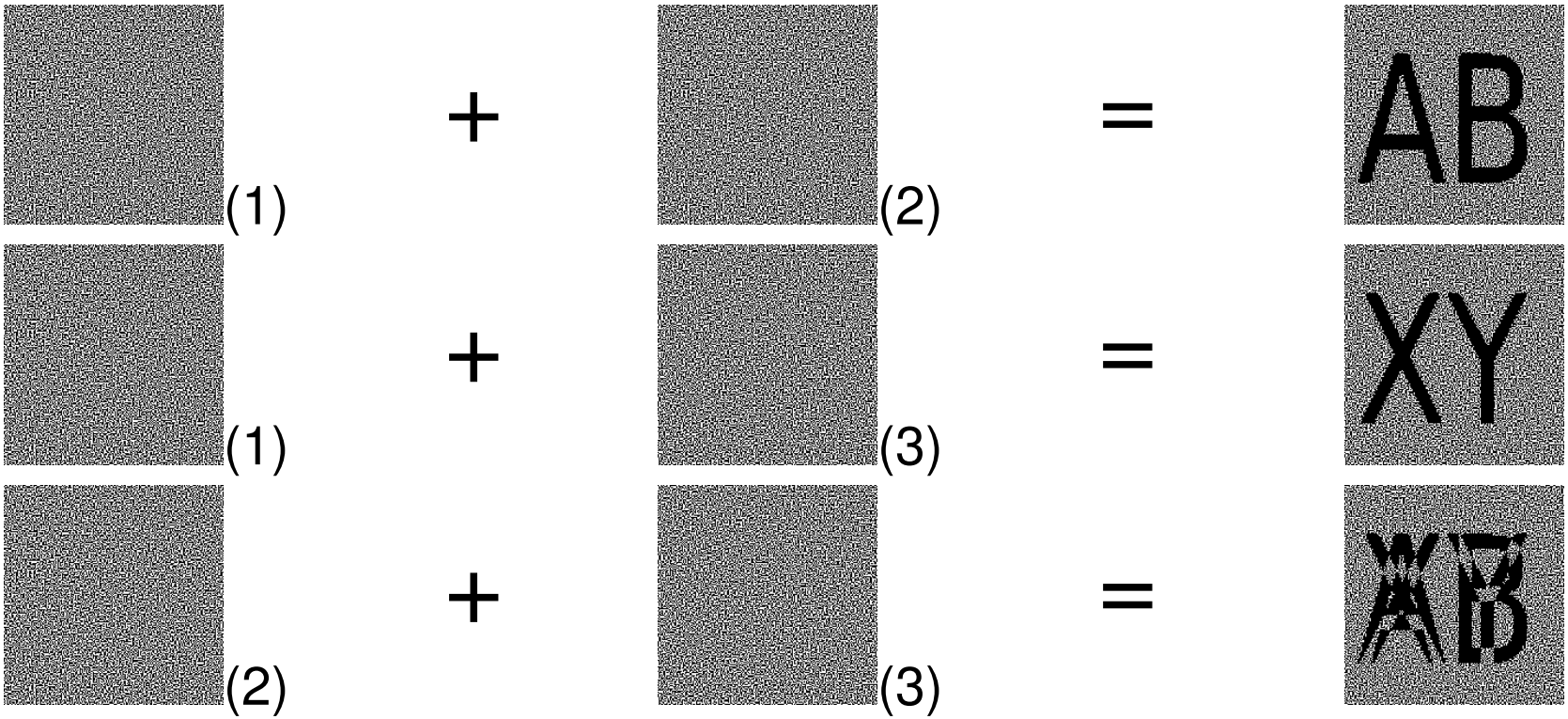


Figure: Combination of 3 transparencies

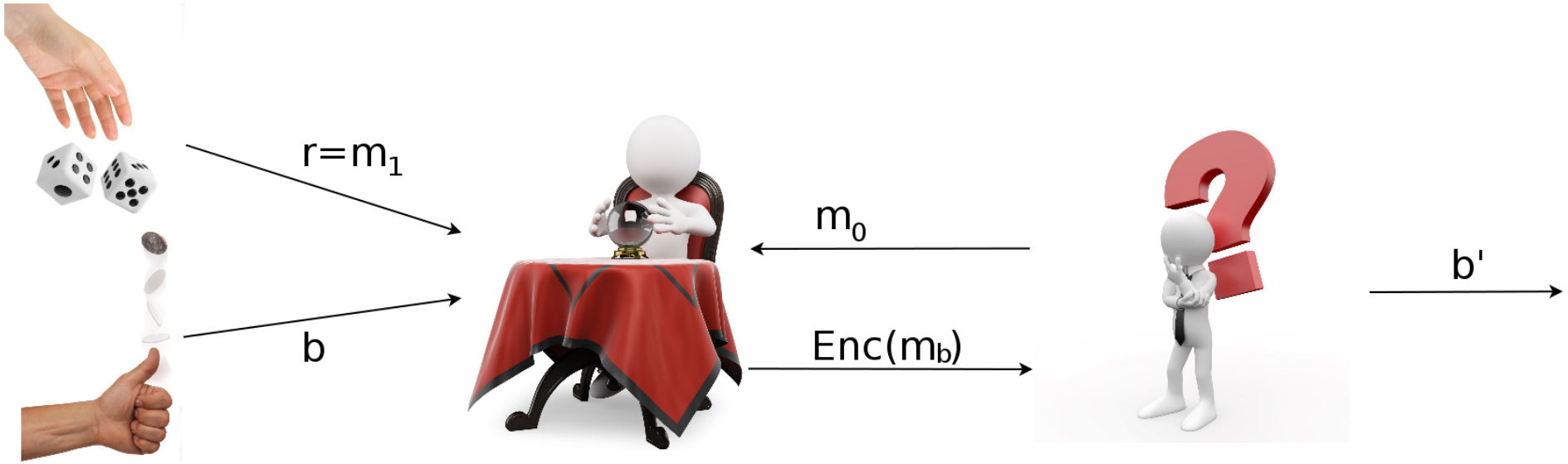
Overview

1 Introduction

2 Sample-Or-Random Security
- Real-Or-Random Security
- Sample-Or-Random Security
- Relation between *ROR – CPA* and *SOR – CO*
- Evaluation

3 Summary and Outlook

Real-Or-Random (*ROR – CPA*) Bellare et al. (1997)



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

k	$\leftarrow$	GenKey(1^n)	Key generation
b	$\in_R$	$\{0,1\}$	Random choice of b
b'	$\leftarrow$	$A^{O_{\mathcal{RR}}(\cdot,b)}$	Adversary tries to determine b

Adversary's advantage $\mathbf{Adv} = Pr[correct] - Pr[false]$

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

Why Ciphertext-Only Securitymodel?

- *CPA* is not suitable for visual cryptography
  - Adversary may not have access to an encryption oracle
- *CPA* is too strong
  - use of XOR allows determining the key
  - e.g. encryptions of □ or 8
- Allow Trade-off: Weaker securitymodel vs. easier key handling

$\Rightarrow$ *CO*-Securitymodel

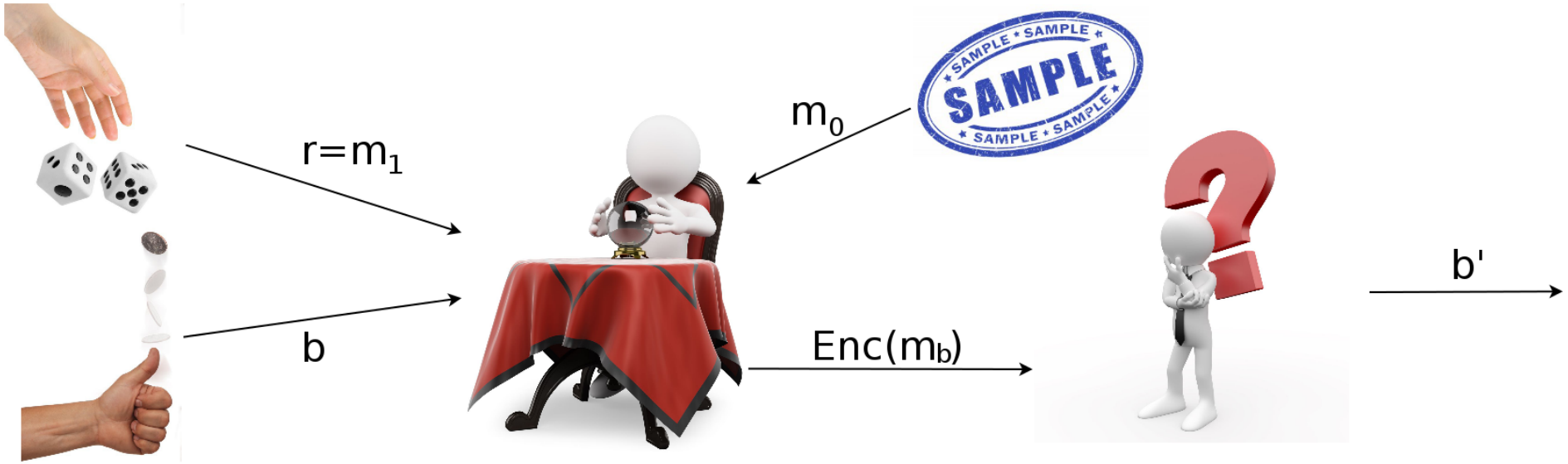
Sample Structure sample_{struct}

sample_{struct} returns a finite set of plaintexts following the pattern of *struct*.

Example for $\Gamma = \{0, 1, \ldots, n\}$ $\Pi(0, 1, \ldots, n)$

$$\text{sample}_{keypad} \in_R \{\gamma \mid \gamma = \gamma_0 \| \gamma_1 \| \ldots \| \gamma_n \ \wedge \ \forall i, j \text{ with } 0 \leq i, j \leq n \ . \ \gamma_i \neq \gamma_j\}$$

Sample-Or-Random (*SOR – CO*)



Experiment

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

k	$\leftarrow$	GenKey(1^n)	Key generation
b	$\in_R$	$\{0,1\}$	Random choice of b
b'	$\leftarrow$	$A^{O_{SR}}(struct)$	Adversary tries to determine b

Adversary's advantage

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

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

Relation between *ROR – CPA* and *SOR – CO*

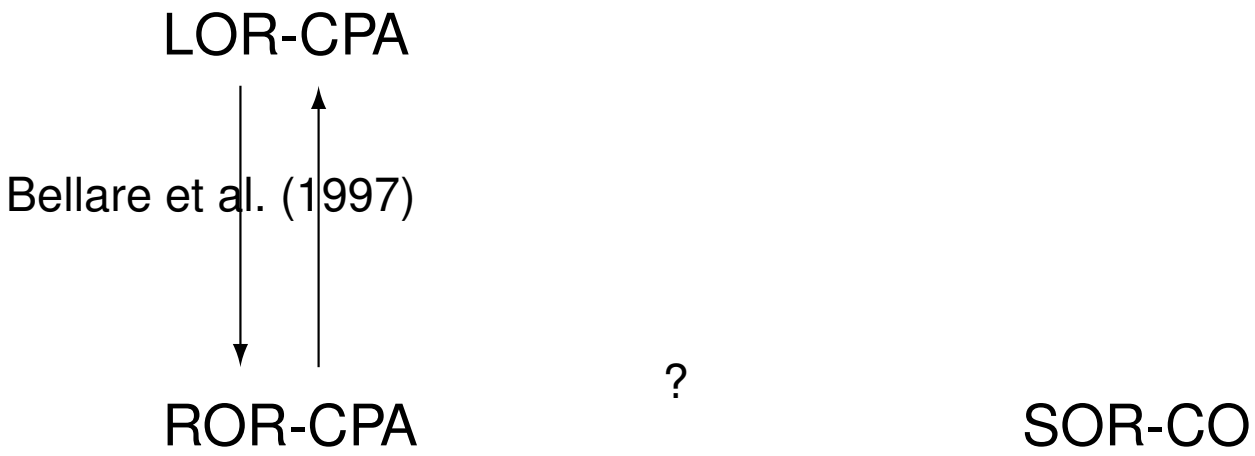


Figure: Relation between Securitymodels for Symmetric Encryption

Relation between *ROR – CPA* and *SOR – CO*

Theorem

Notion of *SOR – CO* is weaker than *ROR – CPA*.

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

If an encryption scheme Π is secure in the sense of *ROR – CPA*, then Π is also secure in the sense of *SOR – CO*.

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

If there exists an encryption scheme Π which is secure in the sense of *SOR – CO*, then there is an encryption scheme Π' which is secure in the sense of *SOR – CO* but not *ROR – CPA*.

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

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

If there exists an encryption scheme Π which is secure in the sense of $SOR - CO$, then there is an encryption scheme Π' which is secure in the sense of $SOR - CO$ but not $ROR - CPA$.

Sketch of Proof

- Assumption: $\Pi = (\text{GenKey}, \text{Enc}, \text{Dec})$, $SOR - CO$-secure exists
- Derive $\Pi' = (\text{GenKey}', \text{Enc}', \text{Dec}')$,
  Lemma 2a: $SOR - CO$-secure,
  Lemma 2b: but not $ROR - CPA$-secure
- Idea: 'mark ciphertexts', to contradict $ROR - CPA$-security

$[SOR - CO \nRightarrow ROR - CPA]$ – derived encryption scheme

Sample struct sample_1

$$\text{sample}_{keypad} \in_R \{\gamma \mid \gamma = \gamma_0 \| \gamma_1 \| \ldots \| \gamma_n \ \wedge \ \forall i, j \text{ with } 0 \leq i, j \leq n \ . \ \gamma_i \neq \gamma_j\}$$

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

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

Algorithm $\text{Enc}'_k(m)$:
$c \leftarrow \text{Enc}_k(c)$
if $m = 0 \ldots 0$
then $c' := 0 \| c$
else
$c' := 1 \| c$
return c'

Algorithm $\text{Dec}'_k(c')$:
$c' = \alpha_1 \| \alpha_2 \| \ldots \| \alpha_{|c'|}$
$c := \alpha_2 \| \ldots \| \alpha_{|c'|}$
$m := \text{Dec}_k(c)$
return m

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

Lemma 2a:

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

Proof.

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

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

□

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

Lemma 2b:

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

Proof.

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

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

□

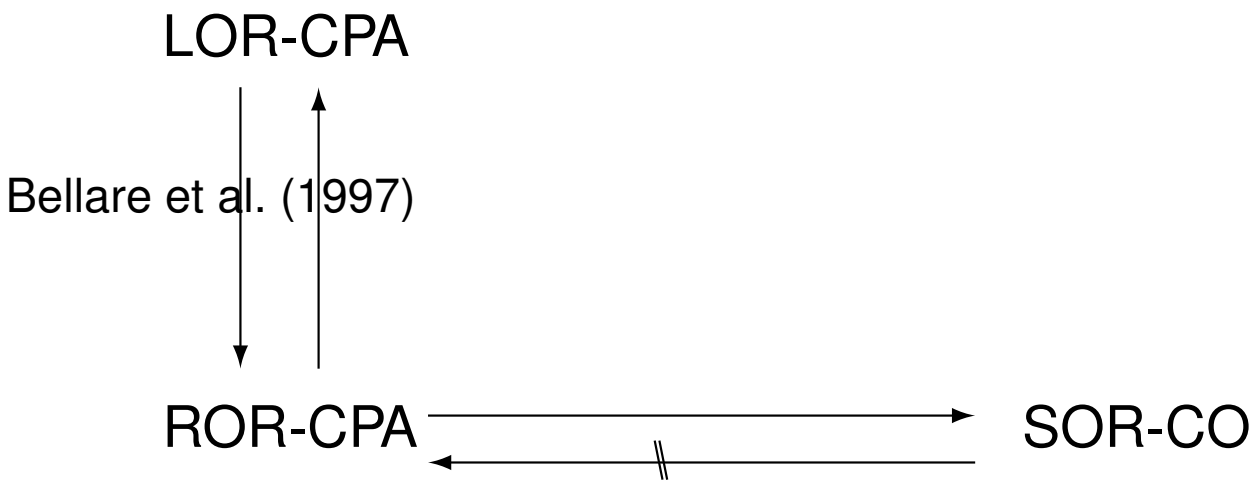
Relation between *ROR – CPA* und *SOR – CO*

⇒ Lemma 2: [*SOR – CO* ⇏ *ROR – CPA*]

If there exists an encryption scheme Π which is secure in the sense of *SOR – CO*, then there is an encryption scheme Π′ which is secure in the sense of *SOR – CO* but not *ROR – CPA*.

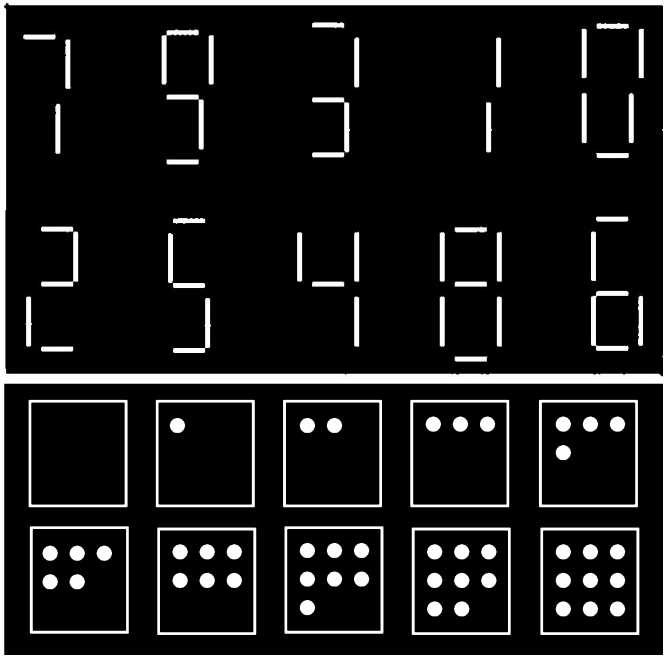
Theorem

SOR – CO is weaker than *ROR – CPA*.



Evaluation: *SOR – CO* at 7-Segment / Dice Codings

- Difference of 2 “Keypad-Ciphertexts” is even
- Adversary
  - asks for 2 ciphertexts
  - if difference is even
    $\Rightarrow b = 0$ (’sample mode’)
  - if difference is odd
    $\Rightarrow b = 1$ (’random mode’)



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

- Idea for countermeasure: add noise to the ciphertexts

Dice Codings with Noise

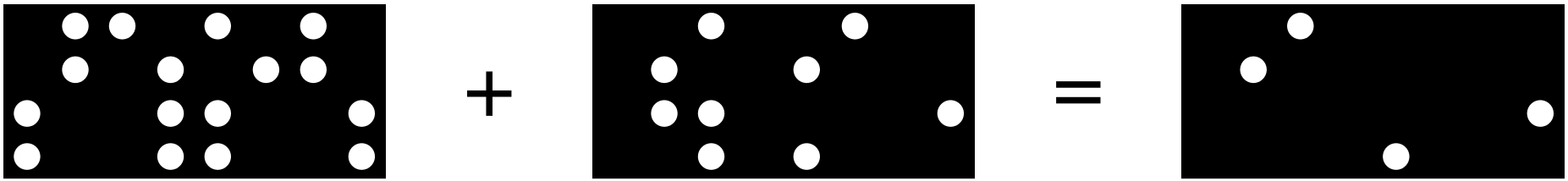


Figure: Visualization for $n = 9$ and $\nu = 7$

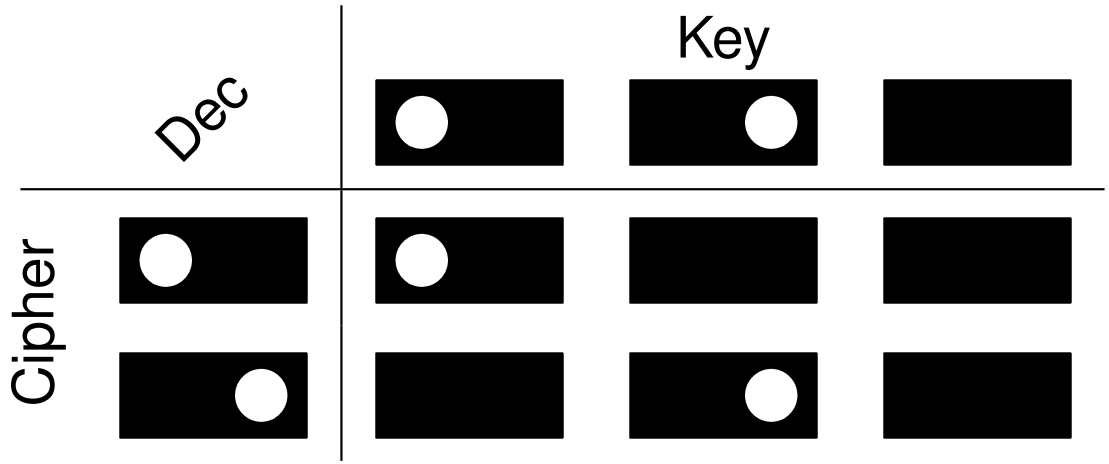


Table: Contingency Table

Overview

1 Introduction

2 Sample-Or-Random Security

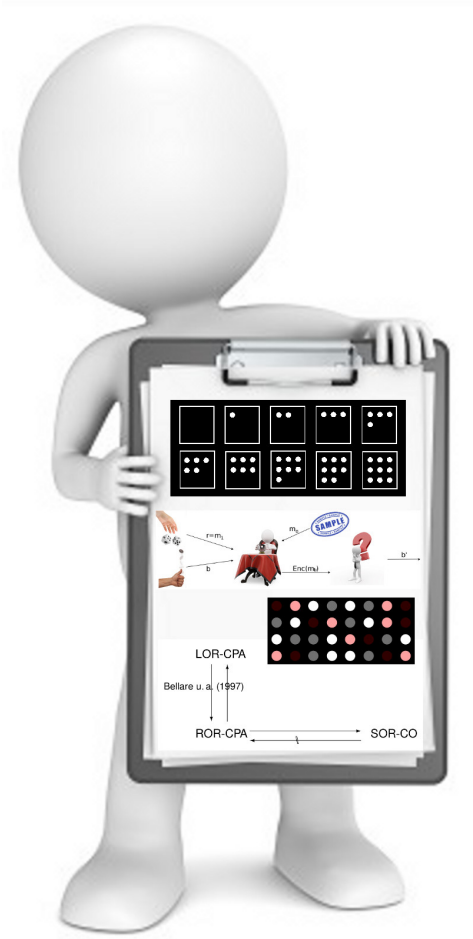
3 Summary and Outlook

Summary and Open Questions

- *SOR – CO* Securitymodel
  - Relation to *ROR – CPA*
- Visual encryption scheme making use of noise
  - Conjecture: SOR-CO-secure if parameters chosen accordingly

---

- *SOR – CO*-security
  - Is Random-or-Sample Security a sufficient choice
  - SampleA-or-SampleB Security?
  - What about active adversaries?
- Dice codings with noise
  - Given n and ν for how many ciphertexts is the scheme SOR-CO-secure?



References

References I

M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption. In *Proceedings of 38th Annual Symposium on Foundations of Computer Science (FOCS 97)*, pages 394–403, 1997.

B. Borchert. Segment-based visual cryptography. Technical Report WSI-2007-04, Wilhelm-Schickard-Institut für Informatik, Tübingen, 2007.

D. Doberitz. Visual cryptography protocols and their deployment against malware. Master's thesis, Ruhr-Universität Bochum, Germany, 2008.

M. Naor and A. Shamir. Visual cryptography. In A. D. Santis, editor, *EUROCRYPT*, volume 950 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 1994. ISBN 3-540-60176-7.