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

Sebastian Pape

Department of Computer Science, Technical University Dortmund,
Research Group: Software Engineering for Critical Systems,
Otto-Hahn Str. 14, 44225 Dortmund, Germany

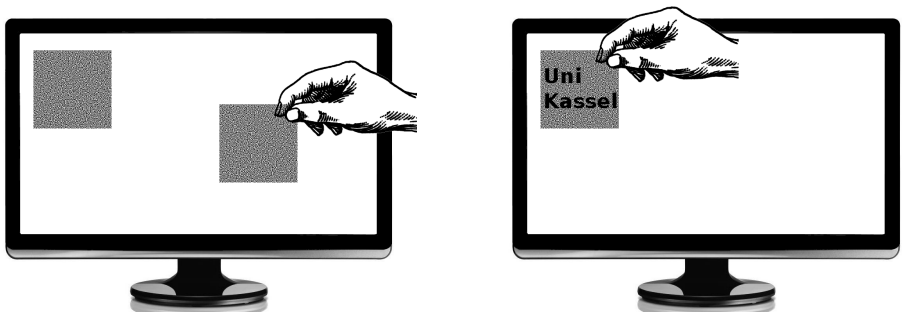
Abstract. In some scenarios, especially when visual cryptography [1] is used, the attacker has no access to an encryption oracle, and thus is not able to mount chosen-plaintext attacks. Based on the notion of real-or-random security under chosen-plaintext attacks (ROR-CPA) given by Bellare et al. [2], we propose the notion of sample-or-random security under ciphertext-only attacks (SOR-CO). We prove that the notion of SOR-CO is fundamentally weaker than the notion of ROR-CPA security and demonstrate the usefulness of our notion by applying it to segment-based visual cryptography [3]. An additional contribution of this paper is the construction of a new segment-based visual encryption scheme with noise based on work by Doberitz [4]. To our knowledge, this is the first visual encryption scheme which makes use of noise. We conjecture that it is secure in the sense of SOR-CO security if the key is not used too often and if the encryption schemes security parameters are chosen accordingly.

Keywords: authentication, visual cryptography, security model

1 Introduction

In online banking, many banks have come up with several approaches of authentication derived from variations of transaction authentication numbers (TAN). The user receives a list of TANs beforehand (e.g. by letter post) and has to authenticate each transaction with one of the numbers from his list. This at least ensures that an adversary cannot perform transactions by knowing the user's login and password. However, this attack is vulnerable to client side attacks such as Trojan horses or phishing. There are various attempts of banks to overcome this, such as indexed TANs (iTAN) where the user was asked for a specific TAN from his list or mobile TANs (mTAN) where a single TAN is created from transaction data and transmitted via a separate channel. In practice those variations helped against phishing, but did not succeed against Trojan horses, since the assumption that the user's mobile phone is a trusted device did not hold due to sophisticated Trojan horses which also affected the mobile devices [5]. Other approaches include special devices which are assumed to be trustworthy, but cause additional costs. Furthermore, the adversary may try to gain also control over the trusted devices by simulating to the user that the devices need to updated and connected to the computer already taken over.

Another proposal for secure authentication on untrusted computers is visual cryptography. Visual cryptography was introduced by Naor and Shamir [1, 6, 7] and allows to encrypt a picture by splitting it into n shares in such a way that someone with k shares is able to reconstruct the image, while $k-1$ shares reveal no information about the original image. They proposed to print each share on a transparency, so that its re-composition can be easily done by humans by stacking their transparencies without the aid of computers. By using only two shares, this approach could have one physical transparency which is put in front of the display of a possibly compromised computer as shown in Fig. 1. By solving



transparencies side by side transparencies stacked

Fig. 1: Example for Visual Cryptography with a Transparency Displayed on a Monitor and a Transparency which is Physically Put in front of the Monitor

a challenge which is only solvable seeing the composed image it is ensured that a Trojan horse would only notice the points which the user clicked, but the malware cannot associate any meaning with it. Specific approaches for online banking were proposed by Greveler [8] and Bochert [3]. They propose to encrypt a virtual keypad with visual cryptography. The user has to decrypt the keypad by aligning a key-transparency on his screen and then has to input his TAN by clicking on the digits of the virtual keypad.

However, all existing approaches are closely related to encryptions based on the XOR function which is due to humans not being able to do complex operations "on the fly". Thus, for many approaches, the key-transparency may be used only once in a secure manner. Although there are a number of schemes allowing to reuse the key-transparency, a satisfying solution for real world scenarios has not yet been found. Leaving the user in practice with plenty of key-transparencies and the hassle of finding the appropriate one.

The general idea of this paper is to examine how key-transparencies for segment-based visual cryptography can securely be used a couple of times. We concentrate on the secure transmission of virtual keypads and do not consider the further protocol for authentication.

1.1 Related Work

Segment-Based Visual Cryptography The idea of segment-based visual cryptography was described by Borchert in 2007. He describes a variation of visual cryptography, where – instead of pixels – segments of a 7-segment display are encrypted [3]. The most significant advantage of segment-based on pixel-based visual cryptography is the easier alignment of the key-transparency. Borchert also gives a more detailed comparison of both variants.

Real-or-Random Security The idea of real-or-random security originates from Bellare et al. [2]. The basic idea is that an oracle, the real-or-random oracle, answers either the encryption of the queried message or an encryption of a randomly chosen string of the same length. If the adversary is not able to determine the oracles operation mode, it is assumed that she is not able to derive any insights from observing encryptions and the encryption scheme is considered to be secure in the sense of real-or-random security. The formal definition of real-or-random security is heavily based on the original work of Bellare et al. [2].

Definition 1. ***(Real-or-Random Oracle $\mathcal{O}_{\mathcal{RR}}$)*** *The real-or-random oracle $\mathcal{O}_{\mathcal{RR}}(\cdot, b)$ takes as input a message m from the plaintext space $\mathcal{M}$ and depending on b it returns either the encryption $\mathsf{Enc}(m)$ of the message m (if $b = 1$) or an encryption $\mathsf{Enc}(r)$ of an equal-length randomly chosen string $r \xleftarrow{R} \mathcal{M}$ (if $b = 0$).*

It is understood that the oracle picks any coins that Enc might need if Enc is randomized, or updates its state appropriately if Enc is stateful.

Definition 2. ***(ROR-CPA)*** *Let $\Pi = (\mathsf{GenKey}, \mathsf{Enc}, \mathsf{Dec})$ be a symmetric encryption scheme, $b \in \{0,1\}$ and $n \in \mathbb{N}$. Let A_{cpa} be an adversary with access to the real-or-random oracle $\mathcal{O}_{\mathcal{RR}}(\cdot, b)$. For the security parameter n the adversary's success probability is*

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

where the experiment $\boldsymbol{Exp}^{ror-atk-b}_{A_{cpa},\Pi}(n) = b'$ for $b \in \{0,1\}$ is given as follows:

$$\begin{array}{l|l} k \leftarrow \mathsf{GenKey}(1^n) & \textit{key-generation} \\ b \in_R \{0,1\} & \textit{random selection of } b \\ b' \leftarrow A^{\mathcal{O}_{\mathcal{RR}}(\cdot,b)}_{cpa} & \textit{adversary tries to determine } b' \end{array}$$

We define the advantage function of the scheme Π as follows:

$$\boldsymbol{Adv}^{ror-cpa}_{\Pi}(n, t, q_e, \mu_e) \stackrel{def}{=} \max_{A_{cpa}} \left\{ \boldsymbol{Adv}^{ror-cpa}_{A_{cpa},\Pi}(n) \right\}$$

where the maximum is over all A_{cpa} with time complexity t, each making at most q_e queries to the real-or-random oracle $\mathcal{O}_{\mathcal{RR}}(\cdot, b)$, totaling at most μ_e bits. If the success probability $\boldsymbol{Adv}^{ror-cpa}_{\Pi}(n)$ for any polynomial (in n) bound adversary is negligible in n, we say the encryption scheme Π is secure in the sense of *$ROR - cpa$.*

2 Sample-or-Random Security

The idea of sample-or-random security is based on real-or-random security and thus also game-based and considering indistinguishability. Since the adversary is not always capable of chosen-plaintext attacks, ciphertext-only attacks are considered. It is only assumed that the encrypted messages follow a certain format known to the adversary, e.g. a virtual keypad contains the digits from '0' to '9'. The same idea as for real-or-random security applies. If the adversary is not able to distinguish encryptions from samples and encryptions from random strings, it is assumed that she is not able to derive any insights from observing encryptions and the encryption scheme is considered to be secure in the sense of sample-or-random security.

Definition 3. ***(Sample-or-Random Oracle $\mathcal{O}_{\mathcal{SR}}$)*** *The sample-or-random oracle $\mathcal{O}_{\mathcal{SR}}(b)$ takes no input and depending on b returns either a set of encryptions $\mathsf{Enc}(m_i)$ of the messages $(m_0, \ldots, m_j) \leftarrow \mathsf{sample}_{struct}$ given by sample_{struct} (if $b = 1$) or an encryption $\mathsf{Enc}(r_i)$ of an equal-size set of uniformly at random chosen strings $r_i \xleftarrow{R} \mathcal{M}$ with the same length than the corresponding messages m_i (if $b = 0$).*

Before we give the definition of sample-or-random security, we introduce the sample structure sample_{kbd}, which represents a randomized virtual keypad:

Definition 4. ***(Sample Structure sample_{kbd})*** *Let $a \| b$ denote the concatenation of the strings a and b. We denote the sample composed of one plaintext message m containing each character γ_i of the alphabet Γ (with size $|\Gamma|$) once with:*

$$\mathsf{sample}_{kbd} \in_R \{m \mid m = \gamma_0 \| \gamma_1 \| \ldots \| \gamma_{|\Gamma|} \ \wedge \ \forall i, j \text{ with } 0 \leq i, j \leq |\Gamma| \ . \ \gamma_i \neq \gamma_j\}$$

Definition 5. *$(SOR - CO)$ Let $\Pi = (\mathsf{GenKey}, \mathsf{Enc}, \mathsf{Dec})$ be a symmetric encryption scheme, $b \in \{0, 1\}$ and $n \in \mathbb{N}$. Let A_{co} be an adversary with access to the sample-or-random oracle $\mathcal{O}_{\mathcal{SR}}(b)$. Let sample_{struct} be a function which returns a finite set of sample plaintexts following the underlying structure struct for each invocation. For the security parameter n the adversary's success probability is*

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

where the experiment $\boldsymbol{Exp}^{sor-co-b}_{A_{co},\Pi}(n) = b'$ for $b \in \{0, 1\}$ is given as follows:

$k \leftarrow \mathsf{GenKey}(1^n)$	*key-generation*
$b \in_R \{0, 1\}$	*random selection of b*
$b' \leftarrow A_{co}^{\mathcal{O}_{\mathcal{SR}}(b)}(struct)$	*adversary tries to determine b′*

We define the advantage function of the scheme Π as follows:

$$\boldsymbol{Adv}^{sor-co}_{\Pi}(n, t, q_e, \mu_e) \stackrel{def}{=} \max_{A_{co}} \left\{ \boldsymbol{Adv}^{sor-co}_{A_{co},\Pi}(n) \right\}$$

where the maximum is over all A_{co} with time complexity t, each making at most q_e queries to the sample-or-random oracle $\mathcal{O}_{\mathcal{SR}}(b)$, totaling at most μ_e bits. If the success probability $\boldsymbol{Adv}_{\Pi}^{sor-co}(n)$ for any polynomial (in n) bound adversary is negligible in n, we say the encryption scheme Π is secure in the sense of $SOR - co$ given the sample structure *struct.*

3 Relation to Real-or-Random Security

We prove that $SOR - CO$ has a weaker notion of security than $ROR - CPA$ by showing that: On the one hand, $ROR - CPA$ (see Def. 2) is at least as strong as $SOR - CO$. On the other hand, given an encryption scheme Π secure in the sense of $SOR - CO$ we show how to construct an encryption scheme Π, which is still secure in the sense of $SOR - CO$, but not in the sense of $ROR - CPA$. The proofs are in general along the lines of the proofs given by Bellare et al. [2].

Corollary 1. $[ROR{-}CPA \Rightarrow SOR{-}CO]$ *If Π is an encryption scheme, which is secure in the sense of $ROR{-}CPA$, then Π is secure in the sense of $SOR{-}CO$.*

Proof. Let m be a plaintext message from the encryption system's plaintext space $\mathcal{M}$ and sample_{struct} be the sample function which returns a set $(m_0, \ldots, m_j)$ of sample plaintexts following an underlying structure *struct* for each invocation of the sample-or-random oracle $\mathcal{O}_{\mathcal{SR}}(b)$. With a real-or-random oracle $\mathcal{O}_{\mathcal{RR}}(\cdot, b)$ the sample-or-random oracle $\mathcal{O}_{\mathcal{SR}}(b)$ may be simulated by producing a sample of messages $(m_0, \ldots, m_j) \leftarrow \mathsf{sample}_{struct}$ and then asking $\mathcal{O}_{\mathcal{RR}}(\cdot, b)$ for their encryption. Thus, security in the sense of $ROR - CPA$ can be seen as security in the sense of $SOR - CO$ with an additional real-or-random oracle available.

The more challenging part is to show that if there exist encryption schemes which are secure in the sense of $SOR - CO$ that these are not automatically secure in the sense of $ROR - CPA$. To proof this we exploit that the adversaries considered by $SOR - CO$ are not able to choose the plaintexts for encryption. We assume there is an encryption scheme $\Pi = (\mathsf{GenKey}, \mathsf{Enc}, \mathsf{Dec})$ which is secure in the sense of $SOR - CO$. Then, based on Π, we construct an encryption scheme $\Pi' = (\mathsf{GenKey}', \mathsf{Enc}', \mathsf{Dec}')$ which is also secure in the sense of $SOR{-}CO$, but can easily be broken in the sense of $ROR - CPA$. For that purpose, we construct Enc' such that it marks the encryption of a particular message m'. This gives the adversary an advantage when asking the real-or-random oracle. To ensure that Π' is still secure in the sense of $SOR - CO$, the message m' should only occur very rarely if strings are chosen either randomly or by the sample structure *struct*. Otherwise an adversary may get an additional advantage to attack the encryption scheme which renders it insecure in the sense of $SOR{-}CO$. We illustrate the idea by regarding the sample structure sample_{kbd} for which we assume, that our alphabet Γ for plaintexts consists of $n+1$ characters represented by numbers from 0 to n and that the ciphertexts' alphabet includes '0' and '1'. We regard the following algorithms for $\Pi' = (\mathsf{GenKey}', \mathsf{Enc}', \mathsf{Dec}')$, assumed $\Pi = (\mathsf{GenKey}, \mathsf{Enc}, \mathsf{Dec})$ is secure in the sense of $SOR - CO$ given the sample structure sample_{kbd}.

Algorithm $\mathsf{GenKey}'(1^n)$:	Algorithm $\mathsf{Enc}'_k(m)$:	Algorithm $\mathsf{Dec}'_k(c')$:
$k \leftarrow \mathsf{GenKey}(1^n)$	$c \leftarrow \mathsf{Enc}_k(c)$	$c' = \alpha_1 \| \alpha_2 \| \ldots \| \alpha_{\|c'\|}$
return k	if $m = 0 \ldots 0$	$c := \alpha_2 \| \ldots \| \alpha_{\|c'\|}$
	then $c' := 0 \| c$	$m := \mathsf{Dec}_k(c)$
	else	return m
	$c' := 1 \| c$	
	return c'	

Π' works almost like Π. When the encryption function is invoked with the particular message m' – here $n+1$ zeros – the decryption is prefixed with '0'. The encryption of all other messages is prefixed with '1'. While this does almost not effect the security in the sense of $SOR-CO$, an adversary of the $ROR-CPA$ security model is able to explicitly ask the encryption oracle for m' and determine the oracle's operation mode. It remains to show the two emerging lemmas:

Lemma 1. *$\Pi' = (\mathsf{GenKey}', \mathsf{Enc}', \mathsf{Dec}')$ is not secure in the sense of $ROR-CPA$.*

Proof. We exploit the built-in weakness of Π' by asking the oracle for the encryption of the message m'. If the encryption is prefixed with '0' we conclude that the oracle is in 'real mode' otherwise we conclude it encrypts random strings. If the encryption is prefixed with '1' we can be sure. However, if the encryption is prefixed with '0', the oracle may nevertheless operate in random mode with a probability of $\frac{1}{(n+1)^{n+1}}$. Thus, the resulting probabilities lead to the adversary's non-negligible advantage and Π' is not secure in the sense of $ROR-CPA$:

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

Lemma 2. *$\Pi' = (\mathsf{GenKey}', \mathsf{Enc}', \mathsf{Dec}')$ is secure in the sense of $SOR-CO$ given the sample structure sample_{kbd}.*

Proof. When the oracle is in 'sample mode' the modification does not come to play, since m' is not part of the sample. Otherwise, we already concluded that the probability that a 'random mode' oracle prefixes an encryption with '0' is $\frac{1}{(n+1)^{n+1}}$. That means when the oracle is in 'random mode', an adversary has an additional chance of receiving m'. However, since the probability is negligible and the adversary is polynomially limited, her additional advantage $Adv_\sharp$ is negligible which leads to the estimation:

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

Due to the assumption that Π is secure in the sense of $SOR-CO$, $\mathbf{Adv}^{sor-co}_{A,\Pi}(n)$ is negligible and so is $Adv_\sharp$. Therefore, $\mathbf{Adv}^{sor-co}_{A,\Pi'}(n)$ is also negligible and Π' secure in the sense of $SOR-CO$ given the sample structure sample_{kbd}.

The message m' needs to be chosen depending on the given sample structure. However, depending on the sample, it is not always possible to come back to strings of a certain length. E.g. when the sample structure consists of a set of messages. Then it is possible to add stages to the encryption function in such a way that a special combination of plaintexts – which is not part of the sample – triggers the oracle's special answer.

Corollary 2. [$SOR-CO \nRightarrow ROR-CPA$] *If there exists an encryption scheme Π which is secure in the sense of $SOR-CO$, then there exists an encryption scheme Π' which is secure in the sense of $SOR-CO$ but not secure in the sense of $ROR-CPA$.*

Proof. Cor. 2 follows from Lem. 1 and Lem. 2.

Theorem 1. *Security in the sense of $SOR-CO$ is a weaker notion than security in the sense of $ROR-CPA$.*

Proof. Th. 1 follows from Cor. 1 and Cor. 2.

Thus, we have shown that the two security models give different notions of security and $SOR-CO$ is weaker than $ROR-CPA$.

4 Application of Sample-or-Random Security to Encryption Schemes

In this section we take a look at some segment-based visual encryption schemes and evaluate if the result from applying the sample-or-random security model is in agreement with the intuitive notion of security. We focus on the encryption of virtual keypads with the corresponding sample $sample_{kbd}$ (cf. Def. 4).

4.1 7-Segment Displays

Borchert [3] describes a variation of visual cryptography, where – instead of pixels – segments of a 7-segment display (cf. Fig. 2a) were encrypted. Each digit can be displayed by switching the appropriate individual segments 'on' and 'off'. Applying visual cryptography, each segment has two representations (left/right or lower/upper) and the segment is visible if the segment's positions match on cipher and key (cf. Fig. 2b). Figures 2c to 2e show a ciphertext, a key and the corresponding plaintext message '1' when stacking the slides on top of each other. It is easy to see that if the plaintext message is '8', key and ciphertext have to be identical, e.g. both Fig. 2c or 2d. We denote this encryption scheme with Π_{7seg}.

Intuitive Notion of Security Since there are only 10 possible digits, after eavesdropping a valid ciphertext, an adversary is able to reduce the number of possible keys from 128 (2^7, the size of the key space) to 10 for each segment. Decrypting with any other key would not result in a valid digit, because the 7-segment coding is not a closed encoding scheme. Thus, as in pixel-based visual cryptography it should not be secure to re-use a key twice.

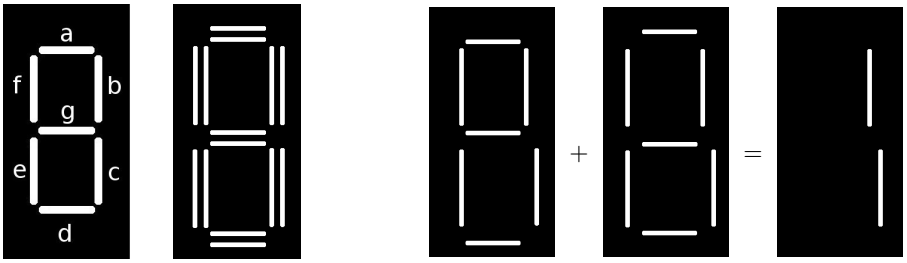


Fig. 2: Segment-Based Visual Cryptography on 7-segment Displays

Sample-or-Random Security We notice that when using the same key and regarding the number of different segments of two encryptions based on 7-segment displays of the sample structure sample_{kbd} they differ in an even number of positions:

Lemma 3. *Let $m = \gamma_0, \ldots, \gamma_n$ and $m' = \gamma'_0, \ldots, \gamma'_n$ be two messages from the sample structure sample_{kbd} and let $c = \alpha_0, \ldots, \alpha_n$ respectively $c' = \alpha'_0, \ldots, \alpha'_n$ be their encryptions with Π_{7seg}. Then the number of different segments of the ciphertexts is always even: $\sum_{i=0}^{n} \alpha_i \oplus \alpha'_i = 0 \mod 2$.*

Proof. Let s respectively s' denote the 7-segment encodings of the messages m respectively m' and let $\leftrightarrow$ denote the identity function. If both segments are equal, the segment is visible. Obviously $c \oplus c' = (s \leftrightarrow K) \oplus (s' \leftrightarrow K) = s \oplus s'$ holds. Thus, the difference of two ciphertexts encrypted with the same key is independent of the key. Since each sample message contains the same encodings, s is a permutation of s'. It can easily be seen that when changing the position of two characters in s, for each segment switched off, another segment needs to be switched on. Thus the difference's parity of two messages from the sample structure sample_{kbd} is independent of the character's permutation of the message and therefore always even.

Theorem 2. *The segment-based visual encryption scheme based 7-segment displays is not secure in the sense of $SOR - CO$ for two ciphertexts ($q_e = 2$) given the sample structure sample_{kbd}.*

Proof. The adversary succeeds with the following strategy. She asks the oracle for two ciphertexts and determines the sum of segmental XORing them. If the sum is even, she guesses that the oracle is in 'sample mode', if it is odd she guesses it is in 'random mode'. The corresponding probabilities are as follows:

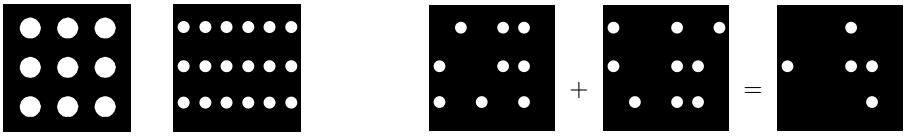
If the oracle is in 'sample mode' ($b = 1$), the sum will always be even and thus the adversary will always be right (cf. Lem. 3).

If the oracle is in 'random mode' ($b = 0$), the sum will be odd only in half of the cases. Thus, the adversary's guess is in half of the cases correct: $\mathbf{Adv}^{sor-co}_{A_{co},\Pi_{7seg}}(n) = Pr[\mathbf{Exp}^{sor-co-1}_{A_{co},\Pi_{7seg}}(n) = 1] - Pr[\mathbf{Exp}^{sor-co-0}_{A_{co},\Pi_{7seg}}(n) = 1] = 1 - \frac{1}{2}$.

Thus, her advantage is not negligible and appropriate to our intuition, Π_{7seg} is not secure in the sense of $SOR - CO$ given the sample structure sample_{kbd}.

4.2 Encryptions Based on Dice Codings

Doberitz [4] describes a variation of segment-based visual cryptography, where – instead of a 7-segment display – a coding based on dots is chosen. The user has to count the number of visible dots – like counting dots from game dices, hence the name *dice coding*. She also presented a user study showing that users get well along with 9 dots. Since this allows us to build a virtual keypad, in the following we regard dice codings with 9 dots. Figure 3a shows the full dot matrix. When the principles of visual cryptography are applied, each dot has two representations (left/right) and the dot is visible if the dot's positions match on cipher and key (cf. Fig. 3b). Figures 3c to 3e show a ciphertext, a key and the corresponding plaintext message '5' when stacking the slides on top of each other. It is easy to see that if the plaintext message is '9', key and ciphertext have to be identical, e.g. both Fig. 3c or 3d. We denote this encryption scheme with Π_{dice}.



9-Dice VC 9-Dice Cipher c Key k Message m

Fig. 3: Segment-Based Visual Cryptography Based on Dice Codings

Intuitive Notion of Security The scheme based on dice codings is closed, there are no undecodable plaintext results. However, the number of possible encodings follows a binomial distribution, there is only one possibility to encode '0' or '9', but there are 126 possibilities to encode '4' or '5' (cf. $\binom{9}{4}$).

Moreover, if virtual keypads are regarded, the segments itself are still closed, but since each segment has to be an encoding of a different digit, the plaintext message itself does not cover the complete message space. Therefore, for a virtual keypad containing each digit from '0' to '9' once, 26 ciphertexts are sufficient to reduce the number of possible keys to two [9].

Sample-or-Random Security In fact, it shows that it does not make a big difference if the virtual keypad is encoded with a 7-segment display or with a 9-dice coding.

Lemma 4. *Let m and m' be two messages from the sample structure sample_{kbd} and let c respectively c' be their encryptions with Π_{DICE}. Then the number of different dots of the ciphertexts c and c' is always even.*

Proof. The proof essentially goes along the lines of the proof of Lem. 3.

Theorem 3. *The segment-based visual encryption scheme based on dice codings* Π_{DICE} *is not secure in the sense of* $SOR-CO$ *for two ciphertexts* ($q_e = 2$) *given the sample structure* sample_{kbd}.

Proof. The proof is analog to the proof of The. 2.

4.3 Encryptions Based on Dice Codings with Noise

The enhanced version of a visual encryption scheme based on dice codings aims to enlarge the amount of information an adversary needs to recover information from eavesdropped ciphertexts. The basic idea is to add noise to the ciphertexts. If both possible positions of a dot are covered by the key, noise is taken out. Since the adversary does not know which of the dots is noise, this renders an additional difficulty for her. To our knowledge, this is the first visual encryption scheme which makes use of noise.

The full dot matrix for the encoding stays unchanged (cf. Fig. 3a). Figure 4a shows the enlarged matrix which is the basis for constructing ciphertexts and keys. Figures 4b to 4d show a ciphertext, a key and the corresponding plaintext message '4' when stacking the slides on top of each other. The ciphertext still consists of a dot at each pair of positions. The key still contains dots with two representations (left/right), but additional contains blackened blocks without any dots. When deciphering, the dot is visible if the key does not contain a blackened block at the considered position and the dot's positions match on cipher and key. If the plaintext message is '9', key and ciphertext have to be identical for all positions where the key contains dots. For the blackened blocks, the ciphertext may contain a dot either on the left or the right position. We denote this encryption scheme with $\Pi^{\star}_{dice}$, the maximum number of visible dots with the encoding parameter n, and the number of blackened blocks with the security parameter ν.

VC 9-dice + Cipher c Key k Message m

Fig. 4: Segment-Based Visual Cryptography Based on Dice Codings with Noise for $n = 9$ and $\nu = 7$

Intuitive Notion of Security The security of the segment-based visual encryption scheme based on dice codings with noise $\Pi^{\star}_{\mathsf{DICE}}(\nu)$ strongly depends on the amount of noise added. If $\nu = 0$ no noise is added and thus $\Pi_{\mathsf{DICE}} = \Pi^{\star}_{\mathsf{DICE}}(0)$. For all other values of ν, the noise additionally stretches the binomial distribution

of the different encodings by the factor 2^ν (e.g. for digit d to $\binom{9}{d} \cdot 2^\nu$). Since the number of possible encodings of all digits are multiplied, this does not concern its ratio, but makes it more difficult to discover encryptions of '0' and '9'.

Sample-or-Random Security If the security parameter $\nu > 0$, the attack of considering the parity of changed dots does not work anymore. Assumed $\nu = 1$ then the parity is flipped if the noise dots of the ciphertexts do not match, which is true in half of the cases. Thus, if the oracle is in 'sample mode' ($b = 1$), the sum will be even in half of the cases and be odd in the other half of the cases. If the oracle is in 'random mode' ($b = 0$), the sum will still be in half of the cases odd and half of the cases even. Therefore, the adversary has no advantage following the described attack. However, for a formal proof, it would be necessary to regard all possible attacks. Therefore, we conclude with a conjecture.

Conjecture 1. Let $\Pi^\star_{\mathsf{DICE}}(\nu)$ be a segment-based visual encryption scheme based on dice codings with noise with the encoding parameter n and the security parameter ν, let q_e be a number of ciphertexts and let sample_{struct} be a sample function. Then there exists a N so that $\forall \nu \geq N$ the encryption scheme $\Pi^\star_{\mathsf{DICE}}(\nu)$ is secure for q_e ciphertexts in the sense of $SOR - CO$ security.

It is reasonable to assume the conjecture is true, because even for a sample which consists of a fixed message string m, the adversary has to determine where in the ciphertext the corresponding encryption of this string is located. The probability to determine the noise, when the dots containing the encryption of the message are fixed, depends on the number of ciphertexts q_e and the security parameter ν. If q_e is fixed, there is a certain point N and for all $\nu \geq N$ the position of the noise is indeterminable.

Remark 1. Assume an application for $\Pi^\star_{\mathsf{DICE}}$, such as online banking. Then N denotes how much noise one has to add to securely use the key transparency q_e times. After the key transparency is used that often, it is thrown away and a new one is used for the next q_e ciphertexts. The usability of the scheme for $\nu \geq N$ is unconsidered here. However, given a certain amount of noise ν, one may derive the closely related question how often a key transparency may securely reused.

5 Conclusion and Future Work

Based on the observation that existing game-based security models for indistinguishability are too strong and do not suit the requirements for visual encryption schemes, we defined the notion of *sample-or-random ciphertext-only* ($SOR-CO$) security. We also showed that the $SOR-CO$ security model gives a weaker notion of security than the real-or-random under chosen-plaintext attacks ($ROR-CPA$) security model. Another security model which comes to mind is to require the attacker to distinguish two different sample structures. Then sample-or-random security may be seen as a special case of sampleA-or-sampleB security. Thus, an

open question is whether there are other notions of security when CPA-security seems to be out of reach and which of them is the 'most meaningful'.

Another open question is, whether the notion of $SOR - CO$ security may be useful for pixel-based cryptography. Since it is difficult to formally model the representation of symbols by pixels, it is unclear whether a more formal notion of security may be useful.

It would also be desirable, given a sample structure sample_{struct} to have a proof for all n, ν, q_e that encryption schemes from the class of segment-based visual encryption schemes based on dice codings with noise are secure/insecure in the sense of sample-or-random ciphertext-only indistinguishability ($SOR - CO$). Where n is the encoding parameter (maximum number of visible dots), ν is the the security parameter (number of noise dots), and the number q_e represents the number of samples available to the adversary.

Another interesting question is whether there are displays similar to the 7-segment display which only have meaningful configurations. A more user-friendly encoding scheme would ease the user's task. However, it is unclear how to construct such a display without the need that the user has to learn new symbols.

Further research is needed, when embedding the encrypted virtual keypad in secure protocols. For example, if the last account numbers and the transfer's amount are encrypted, the adversary may not be able to mount a chosen-plaintext attack, but may have plaintext/ciphertext pairs for certain parts of the ciphertext. Thus, an extended security model may be necessary to judge on the full protocol.

References

1. M. Naor and A. Shamir, "Visual cryptography," in *EUROCRYPT* (A. D. Santis, ed.), vol. 950 of *LNCS*, pp. 1–12, Springer, 1994.
2. 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)*, pp. 394–403, 1997.
3. B. Borchert, "Segment-based visual cryptography," Tech. Rep. WSI-2007-04, Wilhelm-Schickard-Institut für Informatik, Tübingen, 2007.
4. D. Doberitz, "Visual cryptography protocols and their deployment against malware," Master's thesis, Ruhr-Universität Bochum, Germany, 2008.
5. R. Unucheck, "The most sophisticated Android trojan." `https://www.securelist.com/en/blog/8106/The_most_sophisticated_Android_Trojan`, June 2013. last access 2013/06/10.
6. M. Naor and A. Shamir, "Visual cryptography ii: Improving the contrast via the cover base," in *Security Protocols Workshop* (T. M. A. Lomas, ed.), vol. 1189 of *LNCS*, pp. 197–202, Springer, 1996.
7. M. Naor and B. Pinkas, "Visual authentication and identification," in *CRYPTO* (B. S. Kaliski Jr., ed.), vol. 1294 of *LNCS*, pp. 322–336, Springer, 1997.
8. U. Greveler, "VTANs - Eine Anwendung visueller Kryptographie in der Online-Sicherheit," in *GI Jahrestagung (2)* (R. Koschke, O. Herzog, K.-H. Rödiger, and M. Ronthaler, eds.), vol. 110 of *LNI*, pp. 210–214, GI, 2007.
9. S. Pape, *The Challenge of Authentication in Insecure Environments.* PhD thesis, Universität Kassel, 2013. (defended, September 2nd, 2013).