UNIKASSEL VERSITÄT

Sebastian Pape

Some Observations on Reusing One-Time Pads within Dice Codings

Overview

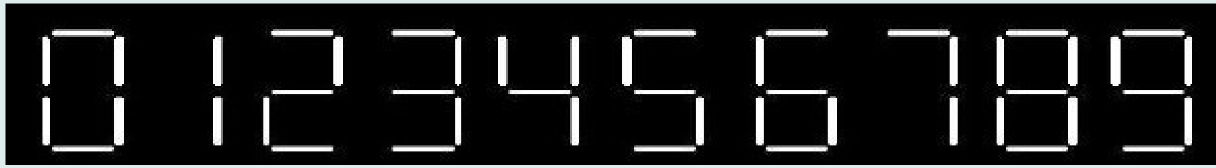
- Dice Codings
- Invalid Keys
- Attacking the Key Pad
- Countermeasures

Introduction / Scenario

- Scope: Online-Banking
- Computer is controlled by attacker
- Visual Cryptography
- Key-transparencies are used in conjunction with monitor

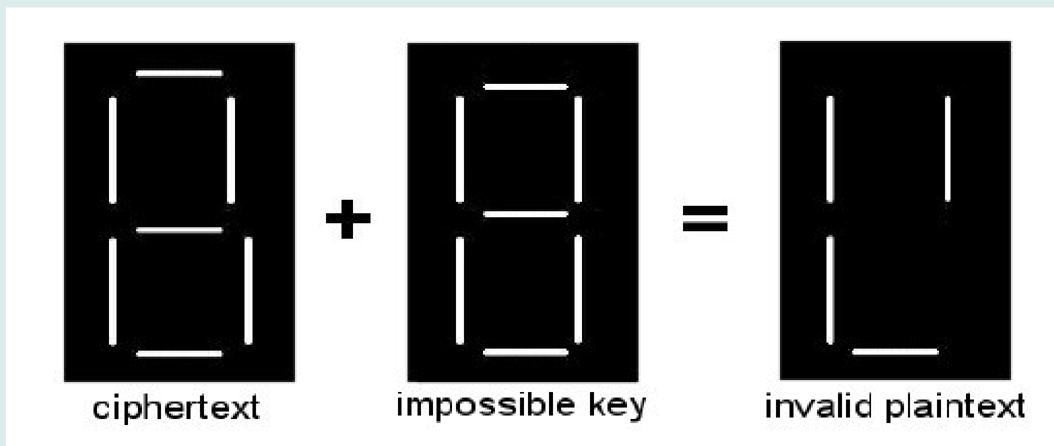
Introduction / Visual Coding

- Digits:



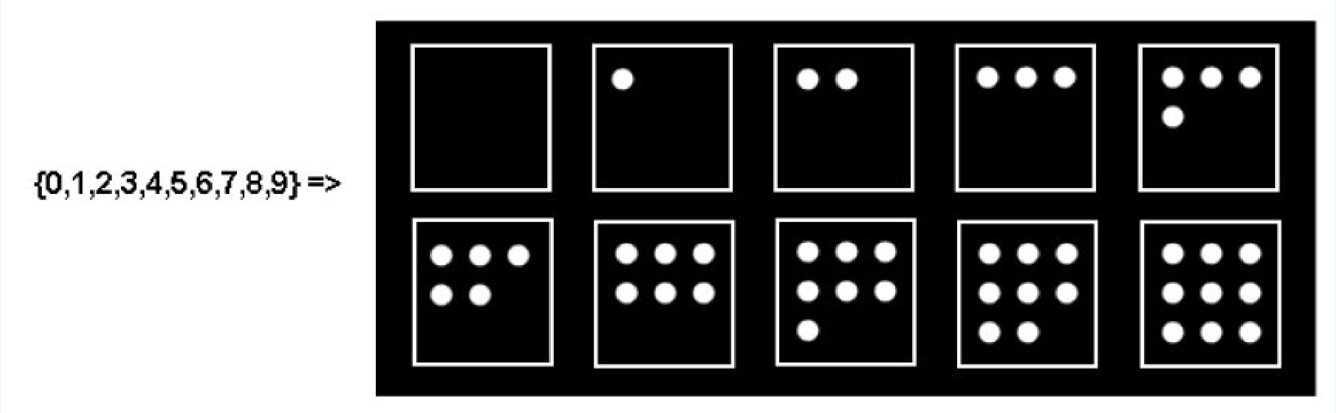
From [DD08]

- Not complete:



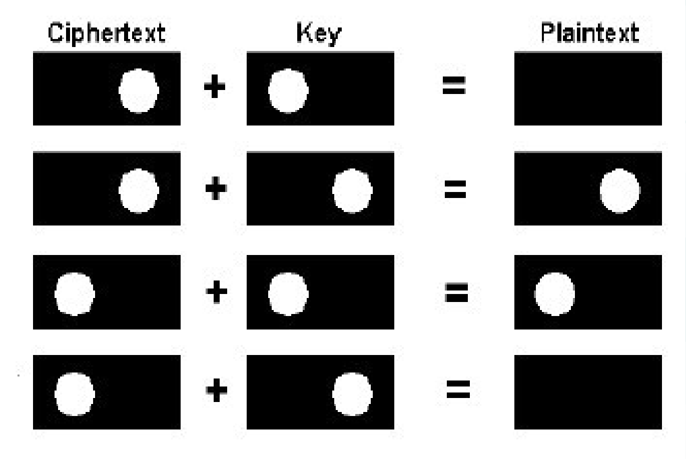
From [DD08]

Dice Codings



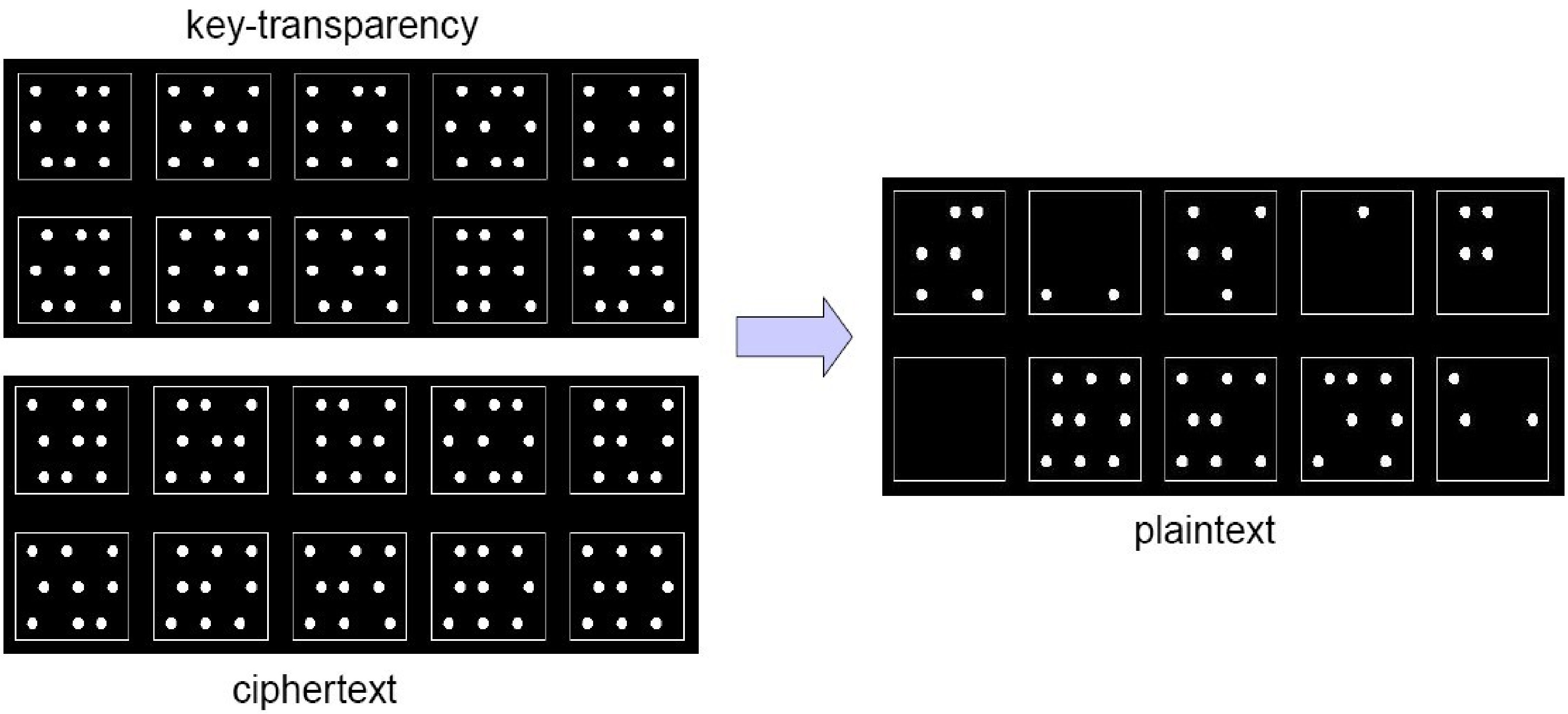
From [DD08]

- Identity / NOT XOR



From [DD08]

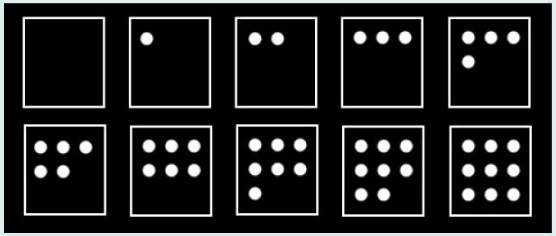
Dice Codings Example



From [DD08]

Invalid Keys (10 dices)

- Number of points per segment: 9
- Keysize for 10 segments: $2^{90} \approx 1{,}23 * 10^{27}$
- Valid keys:



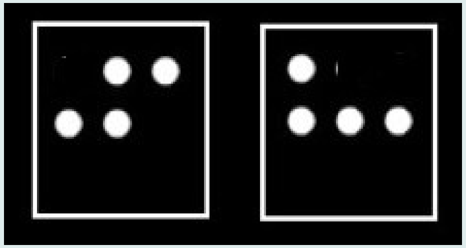
From [DD08]

$$\binom{9}{0} * \binom{9}{1} * \ldots * \binom{9}{9} * 10! \approx 4{,}26 * 10^{19} < 2^{66}$$

Quotient: $\frac{\text{valid keys}}{\text{number of keys}} \approx 3 * 10^{-8}$

Invalid Keys (2 dices)

- Number of points per segment: 9
- Keysize for 2 segments: 2^{18}
- Invalid keys per Ciphertext:

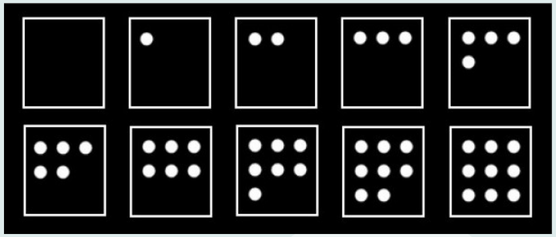


$$\binom{9}{0}^2+\binom{9}{1}^2+\ldots+\binom{9}{9}^2=\sum_{i=0}^{9}\binom{9}{i}^2=48.620$$

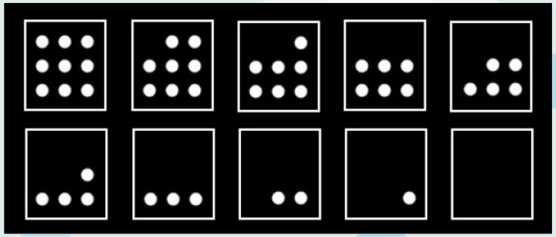
- Quotient: $\frac{\text{invalid keys}}{\text{number of keys}}=\frac{48.620}{262.144}\approx 18{,}5\,\%$

Questions

- Is it possible to extract the OTP / key-transparency?
  ⇒ almost
- d(Cipher, key) →



- d(Cipher, inverse(key)) →



- So, how many ciphertexts do we need?

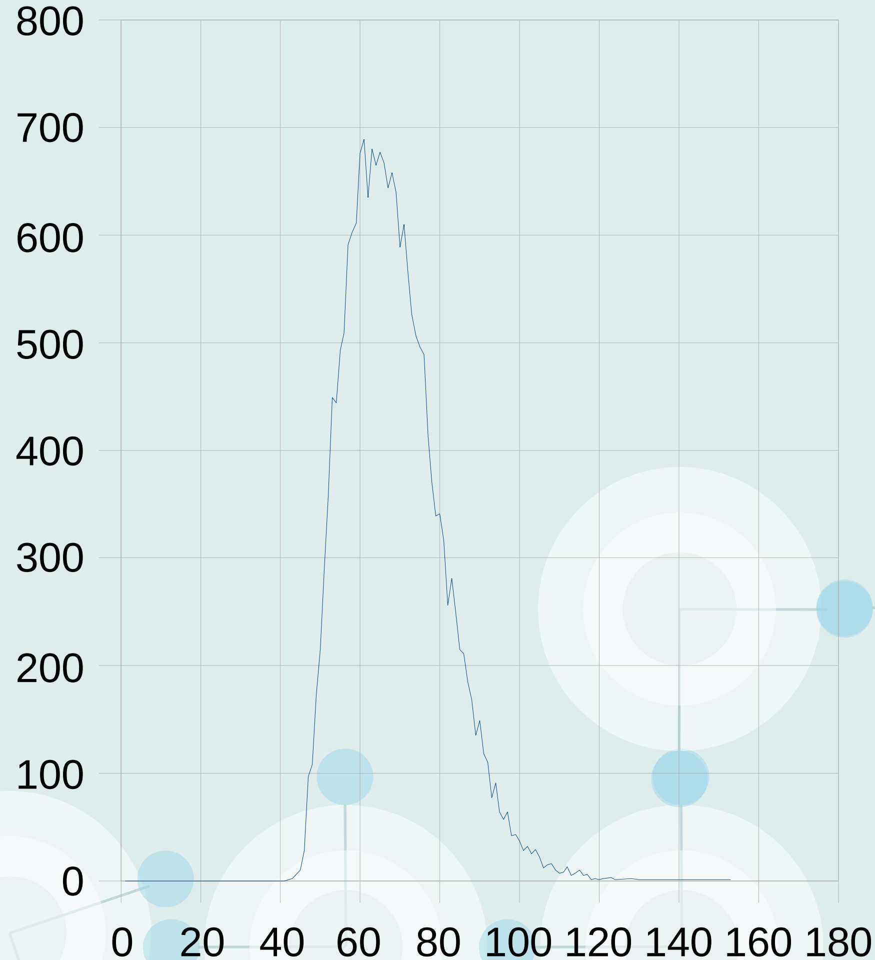
Algorithm's Idea

U N I K A S S E L
V E R S I T Ä T

- Keep track of invalid keys
  - Binary Decision Tree with half of all possible keys
  - Delete invalid keys
  - Until only one key is left
- Result: Secret Key or its inverse
- Runtime: Several times 2^{17} =131.072

Test Data (Ciphers)

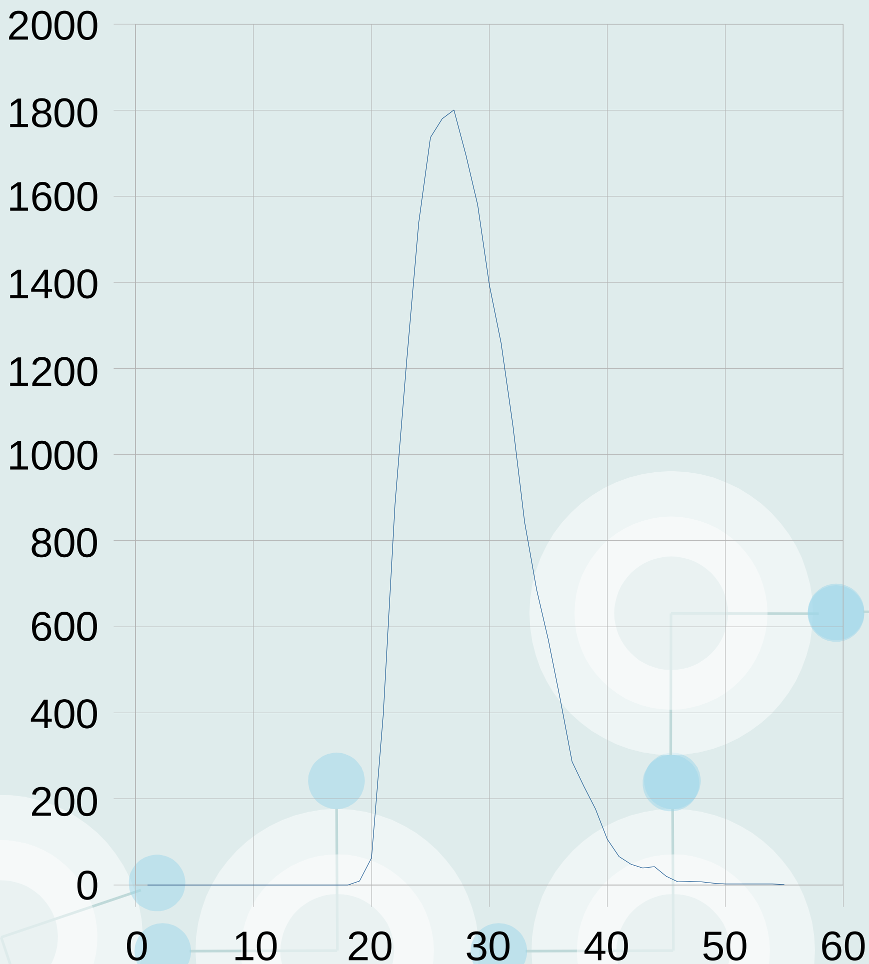
- 20.000 runs
- 70 ciphers >= 60%
- 90 ciphers >= 95%



U N I KASSEL
V E R S I T Ä T

Test Data (CPU time(s))

- 20.000 runs
- 1 Core 3.00GHz (Intel E8400)
- Feasible
- Victims CPU can be used



Global View

- Easy Implementation: Run Algorithm 5 times (pairs: 0+1, 2+3, ..., 8+9)
- But: we have 45 pairs and as soon as parts of the key are recovered additional information is gained
- Not tested in practice
- Complete key or its inverse is recovered

Countermeasures

- More points on the dices (0 to n)
- More dices
  (lower restrictions)
- Similar procedure to iTAN
  (lower restrictions)

Number of Points

- Number of points per segment: n
- Keysize for 2 segments: 2^{2n}
- Invalid keys per Ciphertext:

$$\sum_{i=0}^{n} \binom{n}{i}^2 = \frac{2n!}{n!n!}$$ (using Vandermonde's identity)

$$\frac{2n!}{n!n!} \approx \frac{1}{\sqrt{\pi n}} 2^{2n}$$ (using Stirling's formula)

- Quotient: $\frac{\text{invalid keys}}{\text{number ob keys}} \approx \frac{1}{\sqrt{\pi n}}$
- Bad impact on UI

Number of Dices

- 0 additional dices:
  - 18,5% invalid keys, keysize: 2^{18}
- 1 additional dice (1 doubled dice allowed):
  - 3,9% invalid keys, keysize: 2^{27}
- 2 additional dices (1 tripple dice allowed):
  - <1% invalid keys, keysize: 2^{36}
- $\binom{9}{0}^{2+a}+\binom{9}{1}^{2+a}+\ldots+\binom{9}{9}^{2+a}=\sum_{i=0}^{9}\binom{9}{i}^{2+a}$
- Impact on UI

Similar to iTAN

- Ask for a specific TAN
- Allows to add more redundancy
- Only 4 (6) Digits have to be contained
- Worst case: $3{,}76 * 10^{24}$ (digits: 0189)
- Versus: $2^{90} \approx 1{,}23 * 10^{27}$
- But now any combination can be possible
- Statistical attacks? / digits 0,9 expose key

Conclusions

- It is possible to attack Dice Codings if the key-transparency is used multiple times
- By Improvements attack can be countered
- Procedure similar to iTan may solve this and is probably acceptable by users
- Statistical attack may be possible
- User manipulation not regarded here
  - Influence User (0,9) to leak parts of the key

Thank you

for your attention

References

- [DD08] Denise Doberitz, Complete Codings for Visual Cryptography, 9. Kryptotag, Gelsenkirchen