Funktionsweise der Honey Encryption

Konstantin Kobs
Tom Petersen

20. Januar 2015

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

1. Einleitung

2. Honey Encryption - Ein Beispiel

3. Verfahren der Honey Encryption
   - Distribution Transforming Encoder
   - Verschlüsselung

4. Einschränkungen

5. Fazit

Brute-Force-Angriff auf klassische Verfahren

$$K_1 \rightarrow \text{yxV\#U}$$
$$K_2 \rightarrow \text{Katze}$$
$$K_3 \rightarrow \text{-CPK9}$$
$$\ldots \rightarrow \ldots$$

Verwendete Passwörter

https://xato.net/wp-content/xup/passwordscloud.png

Honey Encryption - Idee

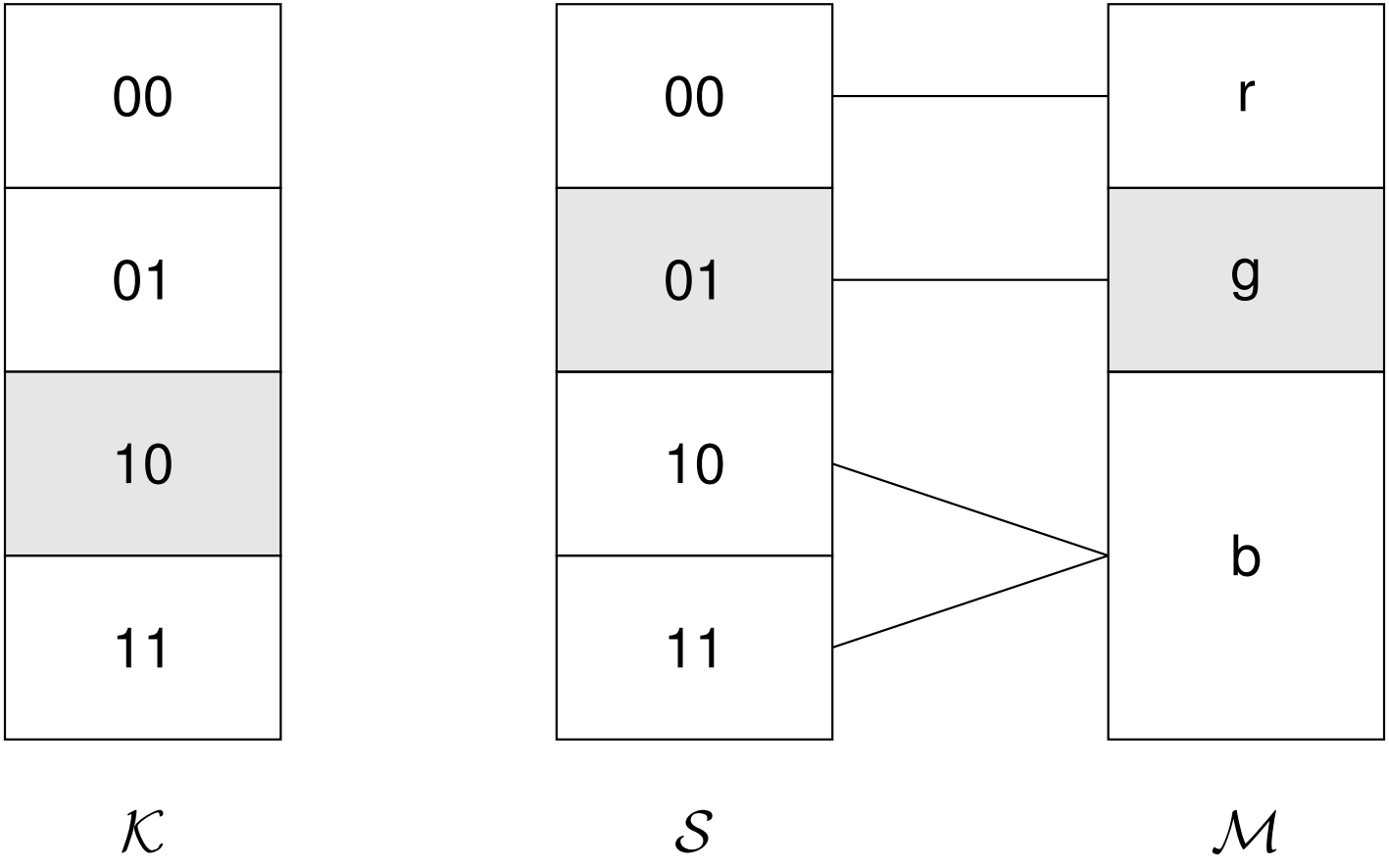
$$K_1 \rightarrow \text{Hund}$$
$$K_2 \rightarrow \text{Katze}$$
$$K_3 \rightarrow \text{Maus}$$
$$\ldots \rightarrow \ldots$$

Honey Encryption

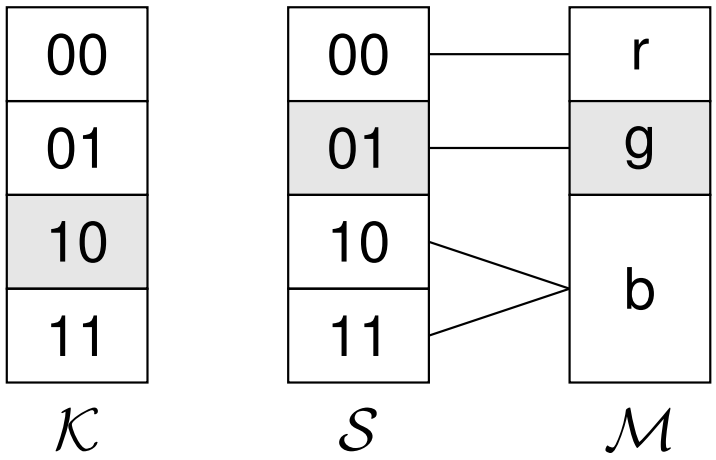
Honey Encryption wurde entwickelt, um Ciphertexte zu generieren, die bei Entschlüsselung mit einem falschen Schlüssel zu einem plausibel wirkenden, aber unechten Klartext führen.

- A. Juels, T. Ristenpart

Honey Encryption - Ein Beispiel



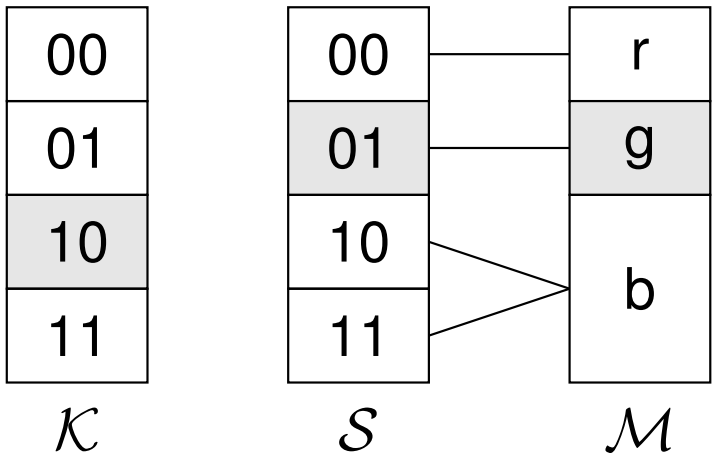
Honey Encryption - Ein Beispiel



Verschlüsselung

$$\begin{aligned} 01 &\leftarrow \text{Nachricht } M \textit{ (grün)} \\ \oplus\underline{10} &\leftarrow \text{Schlüssel } K \\ 11 &\leftarrow \text{Ciphertext } C \end{aligned}$$

Honey Encryption - Ein Beispiel



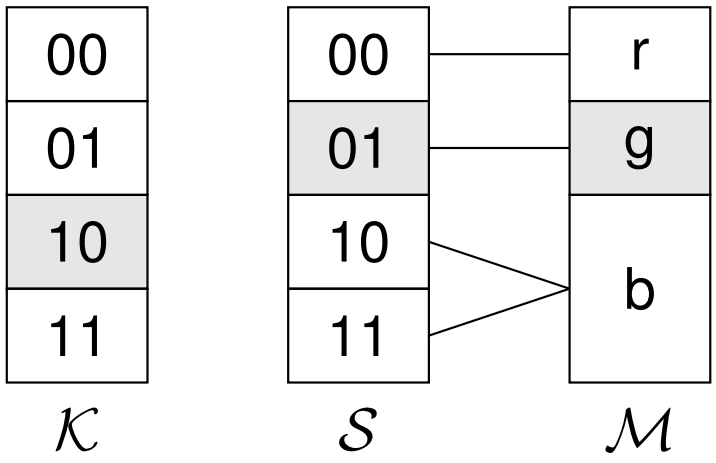
Entschlüsselung

$$\begin{aligned} 11 &\leftarrow \text{Ciphertext } C \\ \oplus\underline{10} &\leftarrow \text{Schlüssel } K \\ 01 &\leftarrow \text{Nachricht } M \textit{ (grün)} \end{aligned}$$

Verschlüsselung

$$\begin{aligned} 01 &\leftarrow \text{Nachricht } M \textit{ (grün)} \\ \oplus\underline{10} &\leftarrow \text{Schlüssel } K \\ 11 &\leftarrow \text{Ciphertext } C \end{aligned}$$

Honey Encryption - Ein Beispiel



Verschlüsselung

$$\begin{aligned} 01 &\leftarrow \text{Nachricht } M \text{ (grün)} \\ \oplus\underline{10} &\leftarrow \text{Schlüssel } K \\ 11 &\leftarrow \text{Ciphertext } C \end{aligned}$$

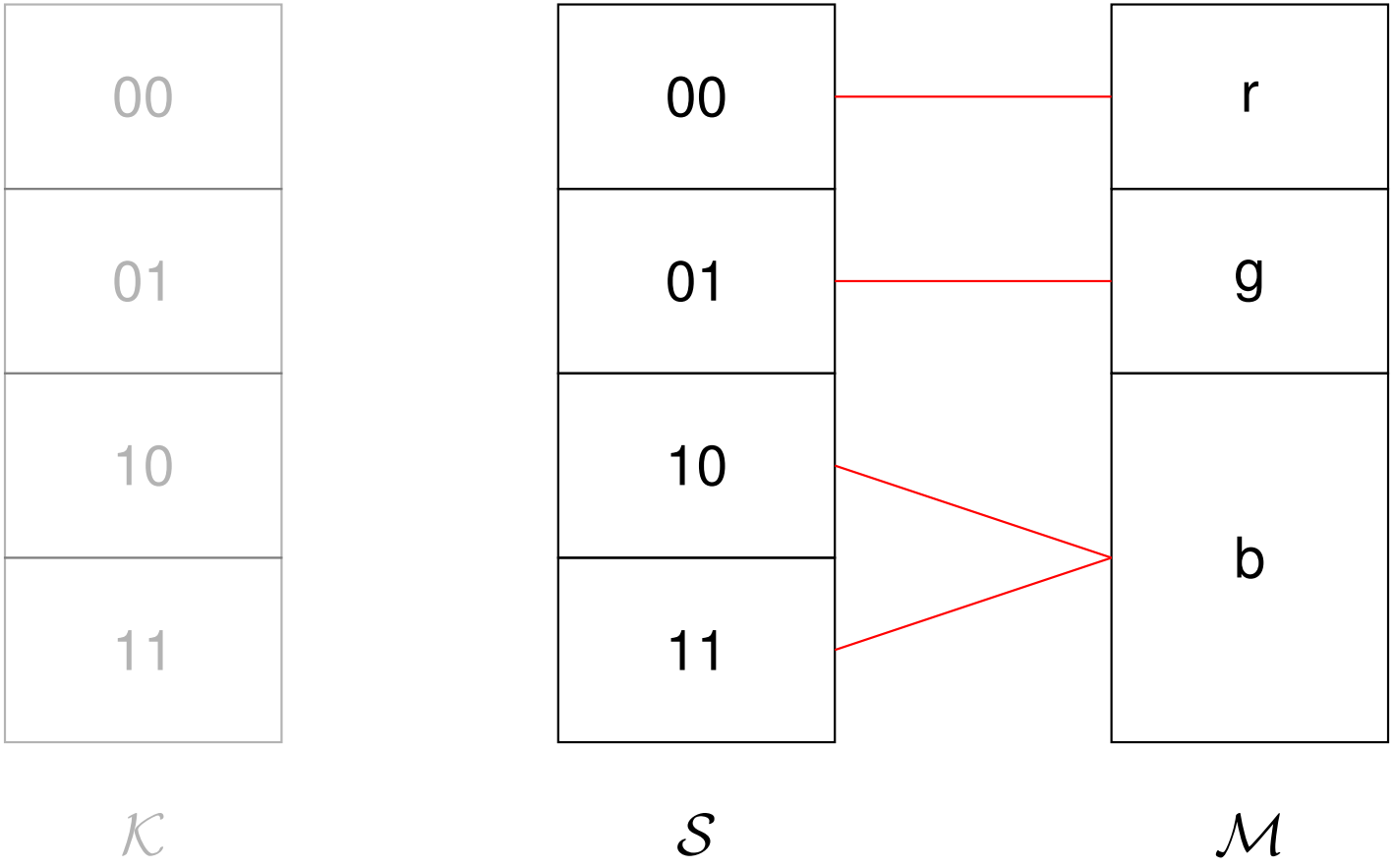
Entschlüsselung

$$\begin{aligned} 11 &\leftarrow \text{Ciphertext } C \\ \oplus\underline{10} &\leftarrow \text{Schlüssel } K \\ 01 &\leftarrow \text{Nachricht } M \text{ (grün)} \end{aligned}$$

Brute-Force-Angriff

$$\begin{aligned} 11 &\leftarrow \text{Ciphertext } C \\ \oplus\underline{11} &\leftarrow \text{Schlüssel } K' \\ 00 &\leftarrow \text{Nachricht } M' \text{ (rot)} \end{aligned}$$

DTE - Distribution Transforming Encoder

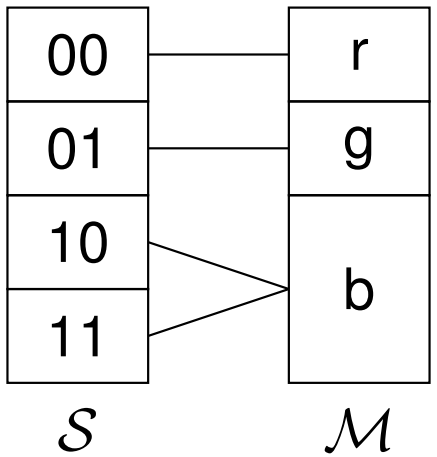


DTE - Schema

$$DTE = (encode, decode)$$

$$encode(Nachricht) \overset{<r>}{=} Seed$$

$$decode(Seed) = Nachricht$$



DTE - Speicherung

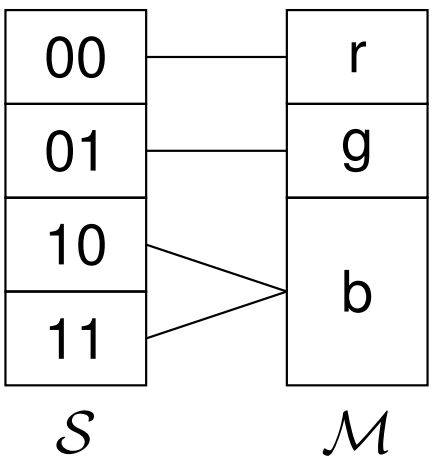
- Datenstruktur (z.B. Tabelle)

Seed	Nachricht
00	rot
01	grün
10, 11	blau

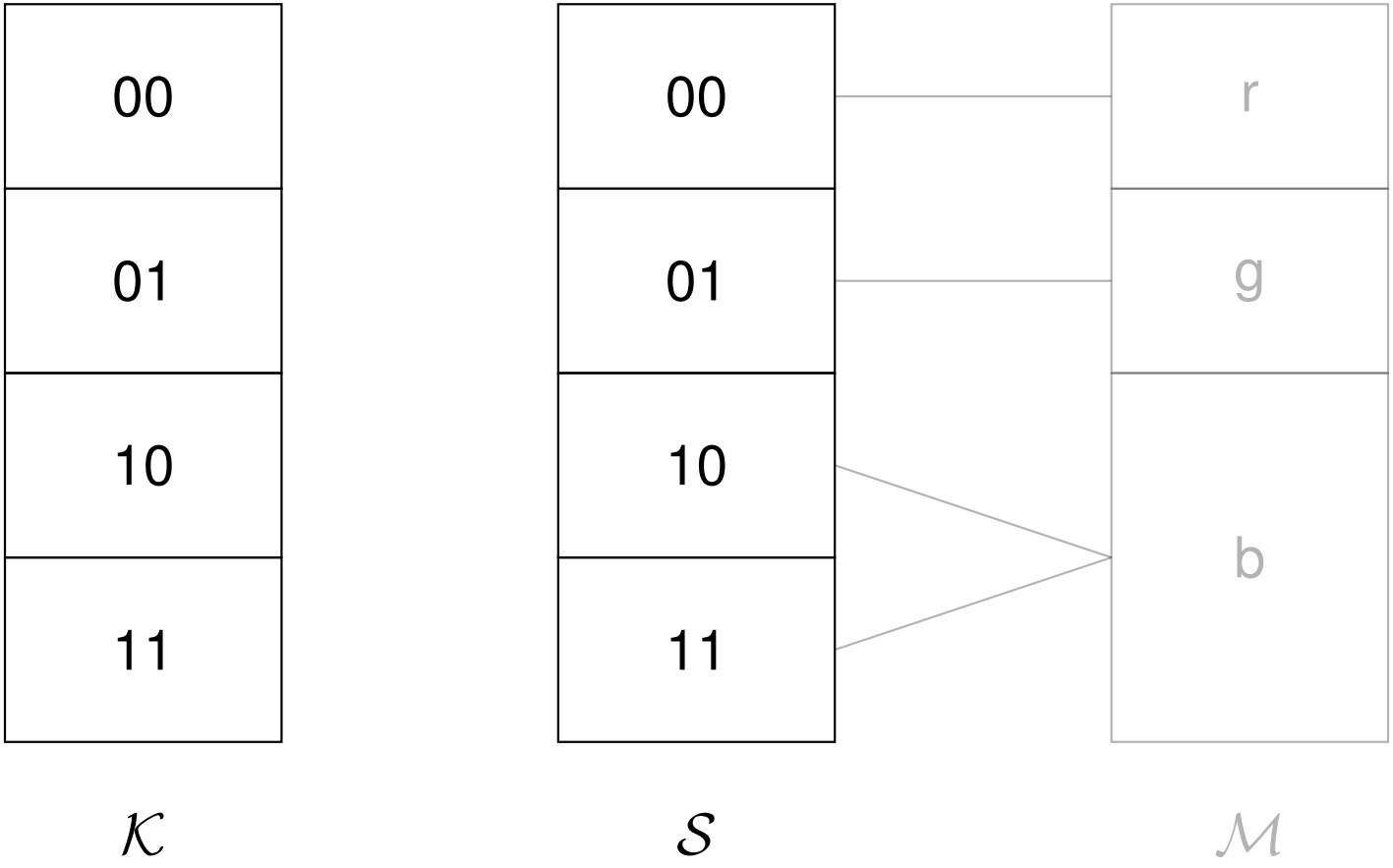
- Algorithmus zur direkten Berechnung
  - PINs
  - Kreditkarten-Nummern

DTE - Voraussetzungen

- Struktur/Menge der Nachrichten
  - Klartexte sollen plausibel sein!
- Verteilung der Nachrichten
  - Nachricht wahrscheinlicher $\Rightarrow$ mehr Seeds



Verschlüsselung



Hashbasierte Verschlüsselung

Verschlüsselung

$\mathrm{HEnc}_{\mathrm{Hash}}(M, K)$

$S \xleftarrow{<r>} \mathrm{DTE}_{\mathrm{encode}}(M)$

$R \xleftarrow{<r>} \{0,1\}^k$

$H = \mathrm{HF}(K, R)$

$C = H \oplus S$

Return (C, R)

Hashbasierte Verschlüsselung

Verschlüsselung

$\mathrm{HEnc}_{\mathrm{Hash}}(M, K)$

$S \xleftarrow{<r>} \mathrm{DTE}_{\mathrm{encode}}(M)$

$R \xleftarrow{<r>} \{0,1\}^k$

$H = \mathrm{HF}(K, R)$

$C = H \oplus S$

Return (C, R)

Entschlüsselung

$\mathrm{HDec}_{\mathrm{Hash}}((C, R), K)$

$H = \mathrm{HF}(K, R)$

$S = H \oplus C$

$M = \mathrm{DTE}_{\mathrm{decode}}(S)$

Return M

Einschränkungen der Honey Encryption

- Freitext nicht möglich
  - *Menge der Nachrichten* unendlich groß
  - Verteilung nicht bekannt

Einschränkungen der Honey Encryption

- Freitext nicht möglich
  - *Menge der Nachrichten* unendlich groß
  - Verteilung nicht bekannt
- Vorab bekannte Informationen
  - Angreifer hat Zusatzinformationen $\Rightarrow$ Verifizierung des Ergebnisses
  - Sicherheit der Verschlüsselung

Einschränkungen der Honey Encryption

- Freitext nicht möglich
  - *Menge der Nachrichten* unendlich groß
  - Verteilung nicht bekannt
- Vorab bekannte Informationen
  - Angreifer hat Zusatzinformationen $\Rightarrow$ Verifizierung des Ergebnisses
  - Sicherheit der Verschlüsselung
- *Typo-Safety*
  - Tippfehler führt zu falschen Daten
  - große Stärke $\Rightarrow$ große Schwäche

Fazit

- Sehr sicher
- Nicht universal anwendbar
- Forschungsgebiete:
  - Natural Language Processing
  - Stochastik
  - User Experience
- Nächstes Ziel: Passwort-Manager