Sicherheitsanalyse der Lichtbrechungskryptographie

BACHELORARBEIT PHILIPP WOLTER
BETREUER: BERND BORCHERT
GUTACHTER: KLAUS REINHARDT

Gliederung

I. Motivation: iTAN und MITM
II. VC und die Mehrfachverwendung
III. Lichtbrechungskryptographie
    I. Prinzip
    II. Beispiel
    III. Mehrfachverwendung
IV. Ausblick

Take-Home-Messages

- iTAN –Verfahren nicht sicher

Take-Home-Messages

- iTAN –Verfahren nicht sicher
- VC nicht optimal für Onlinebanking

Take-Home-Messages

- iTAN –Verfahren nicht sicher
- VC nicht optimal für Onlinebanking
- Wie funktioniert LBK?

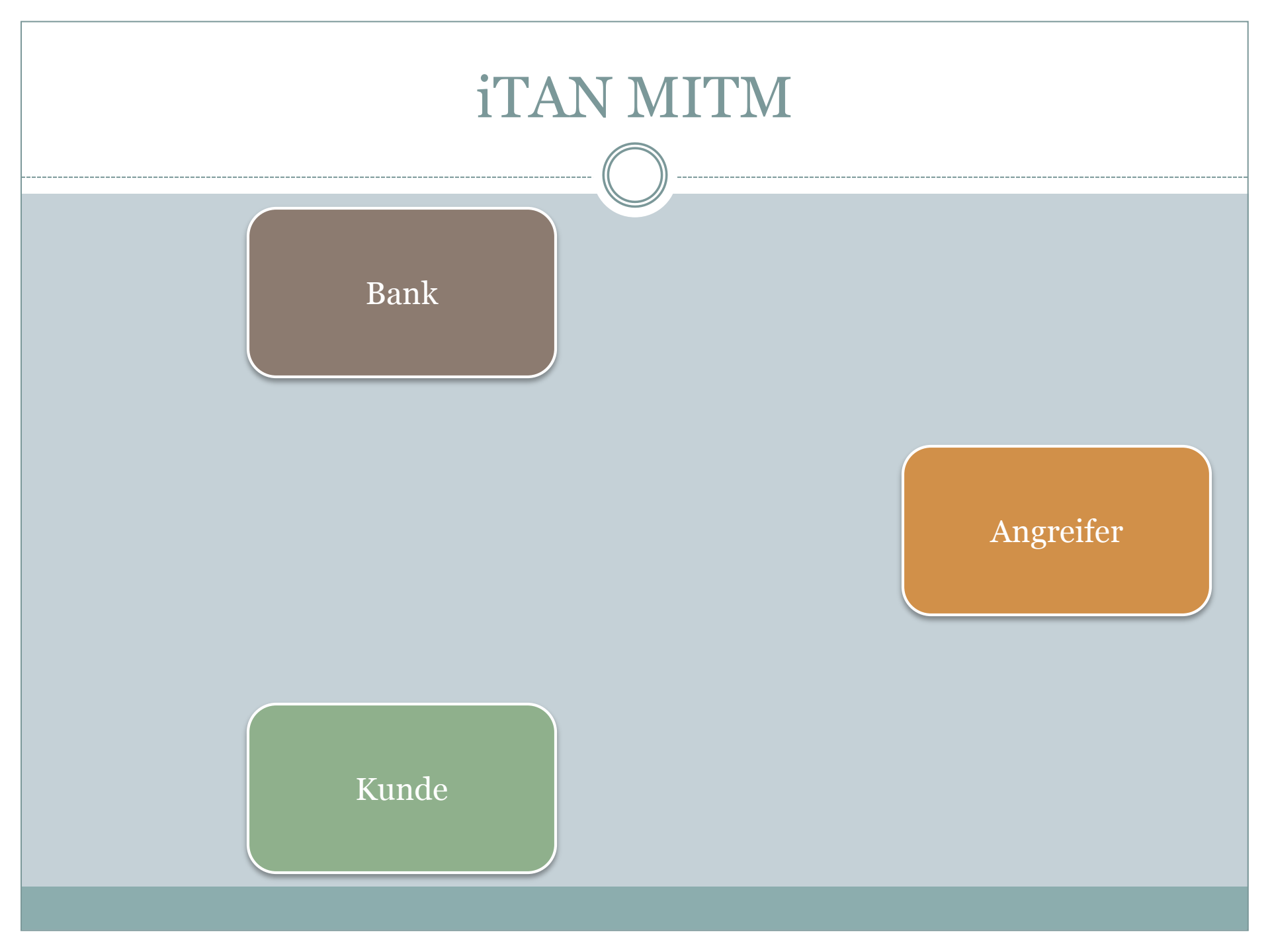
Take-Home-Messages

- iTAN –Verfahren nicht sicher
- VC nicht optimal für Onlinebanking
- Wie funktioniert LBK?
- konkretes Anwendungsbeispiel

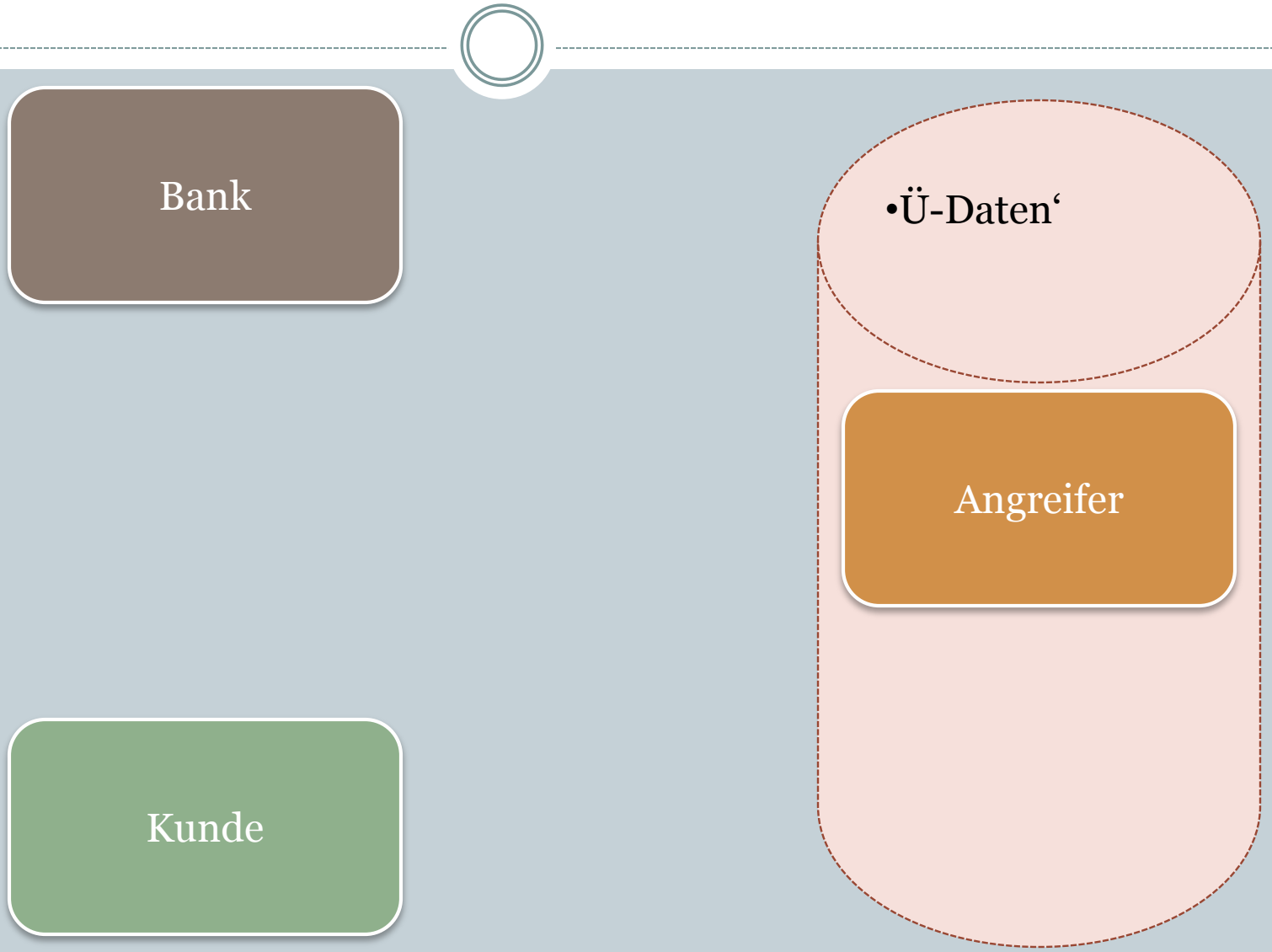
Take-Home-Messages

- iTAN –Verfahren nicht sicher
- VC nicht optimal für Onlinebanking
- Wie funktioniert LBK?
- konkretes Anwendungsbeispiel
- LBK Mehrfachverwendung

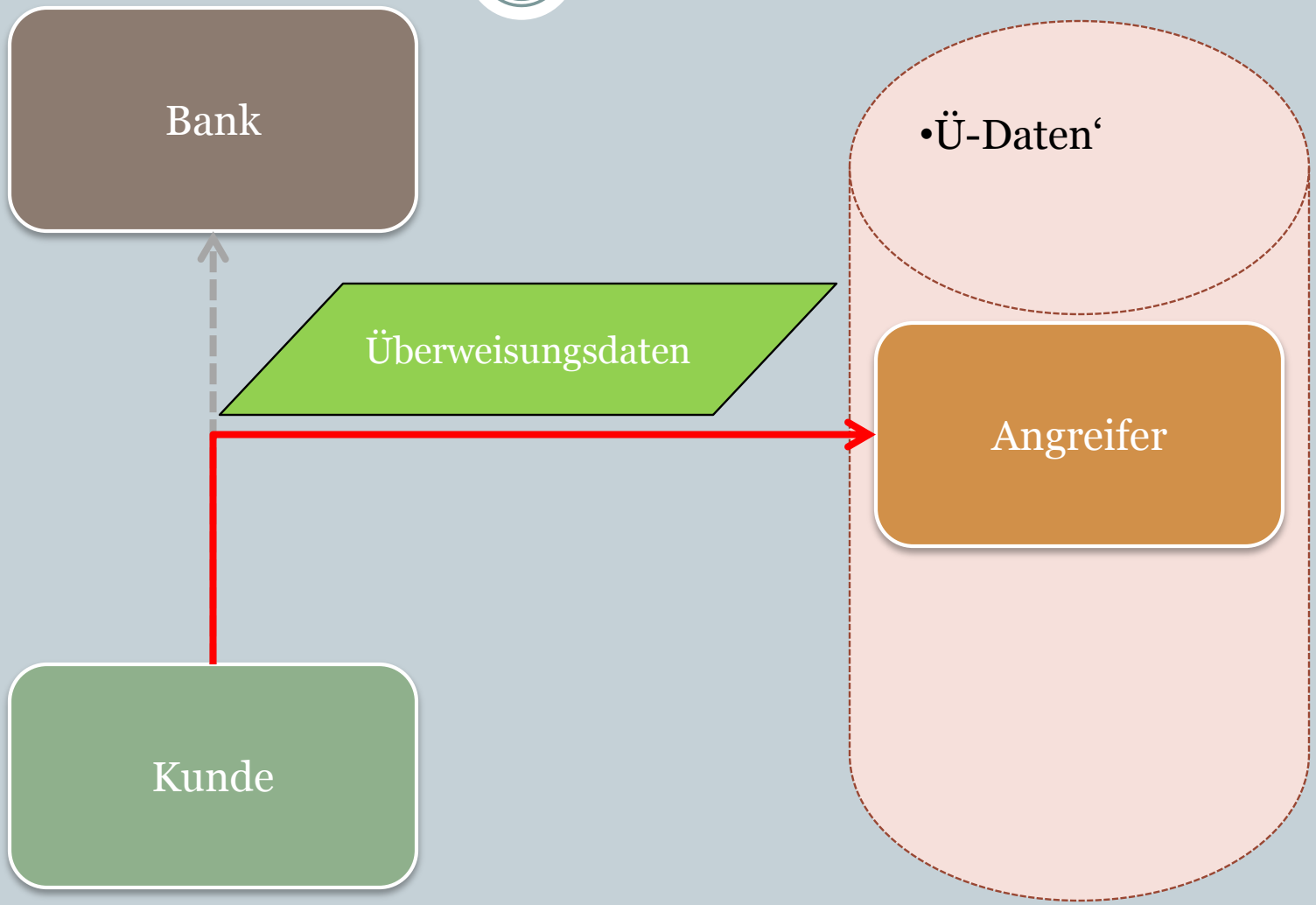
iTAN MITM



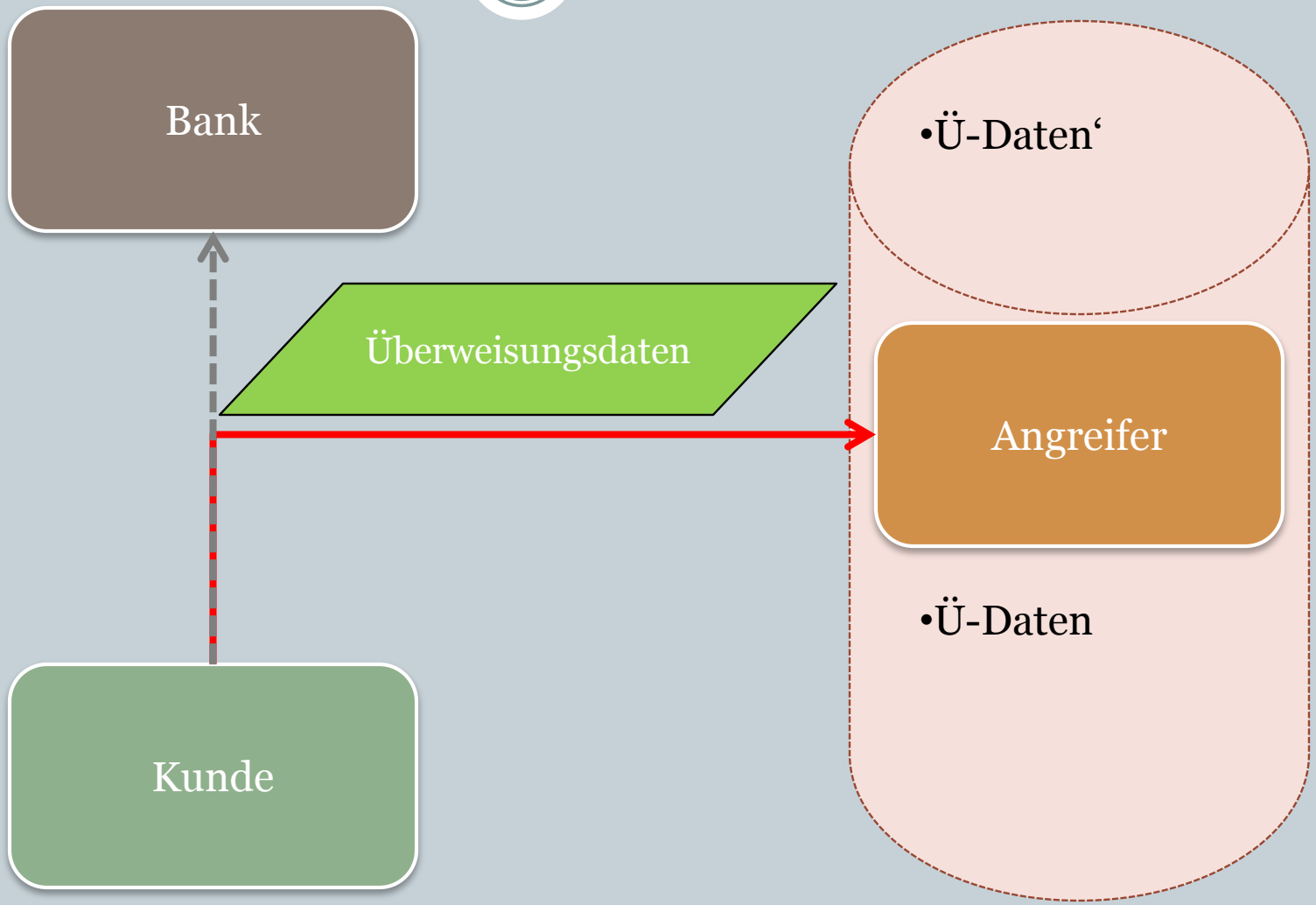
iTAN MITM



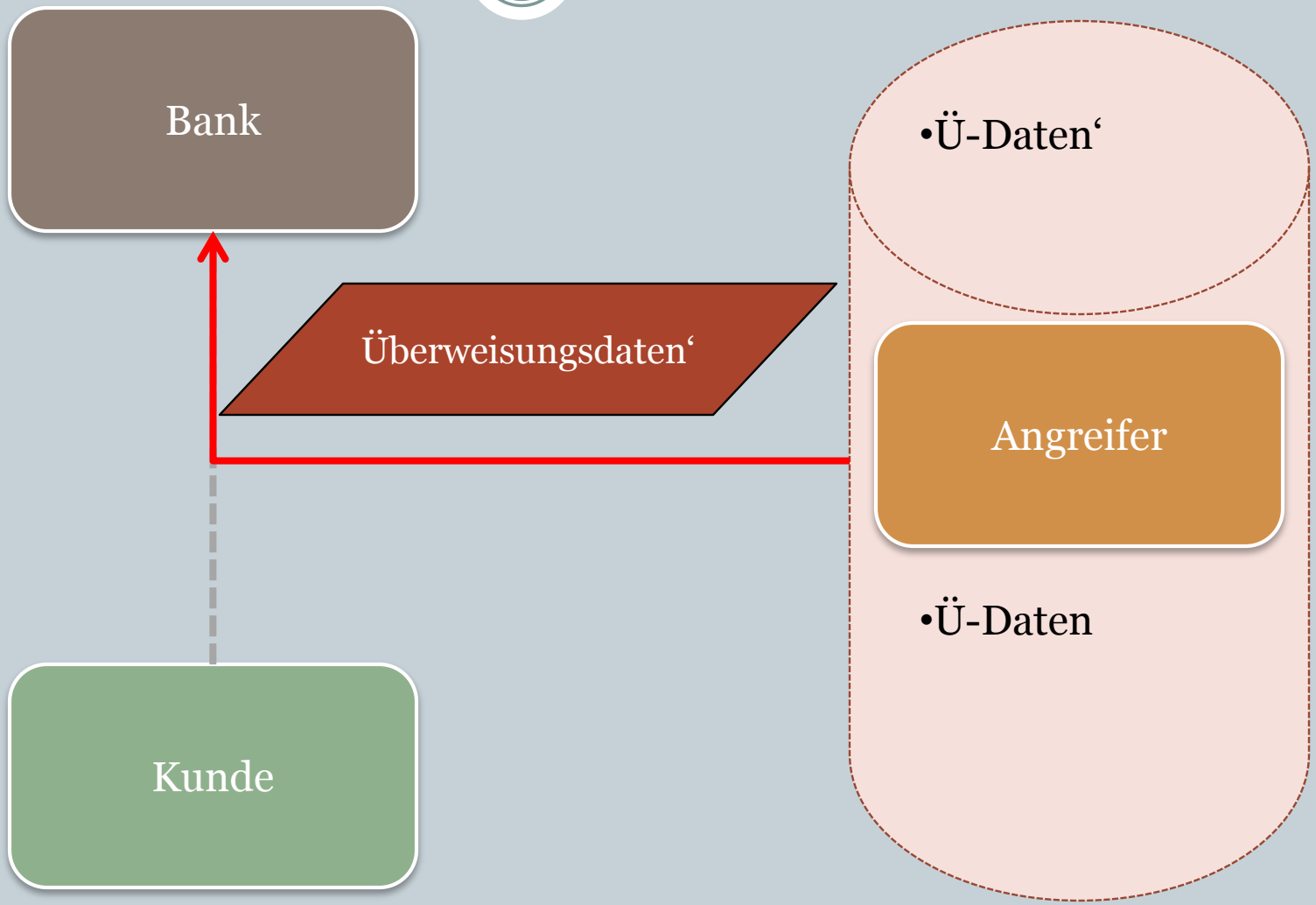
iTAN MITM



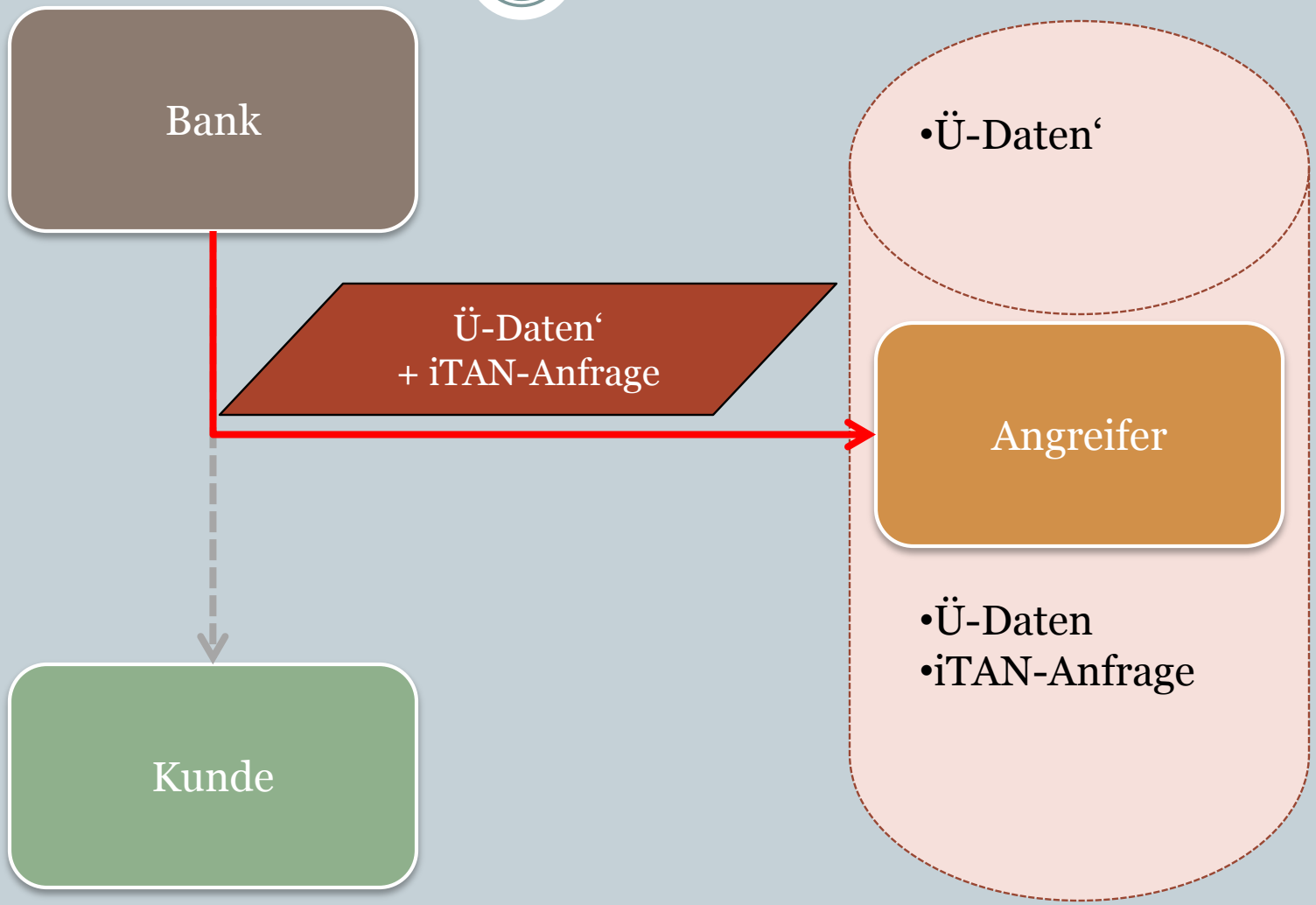
iTAN MITM



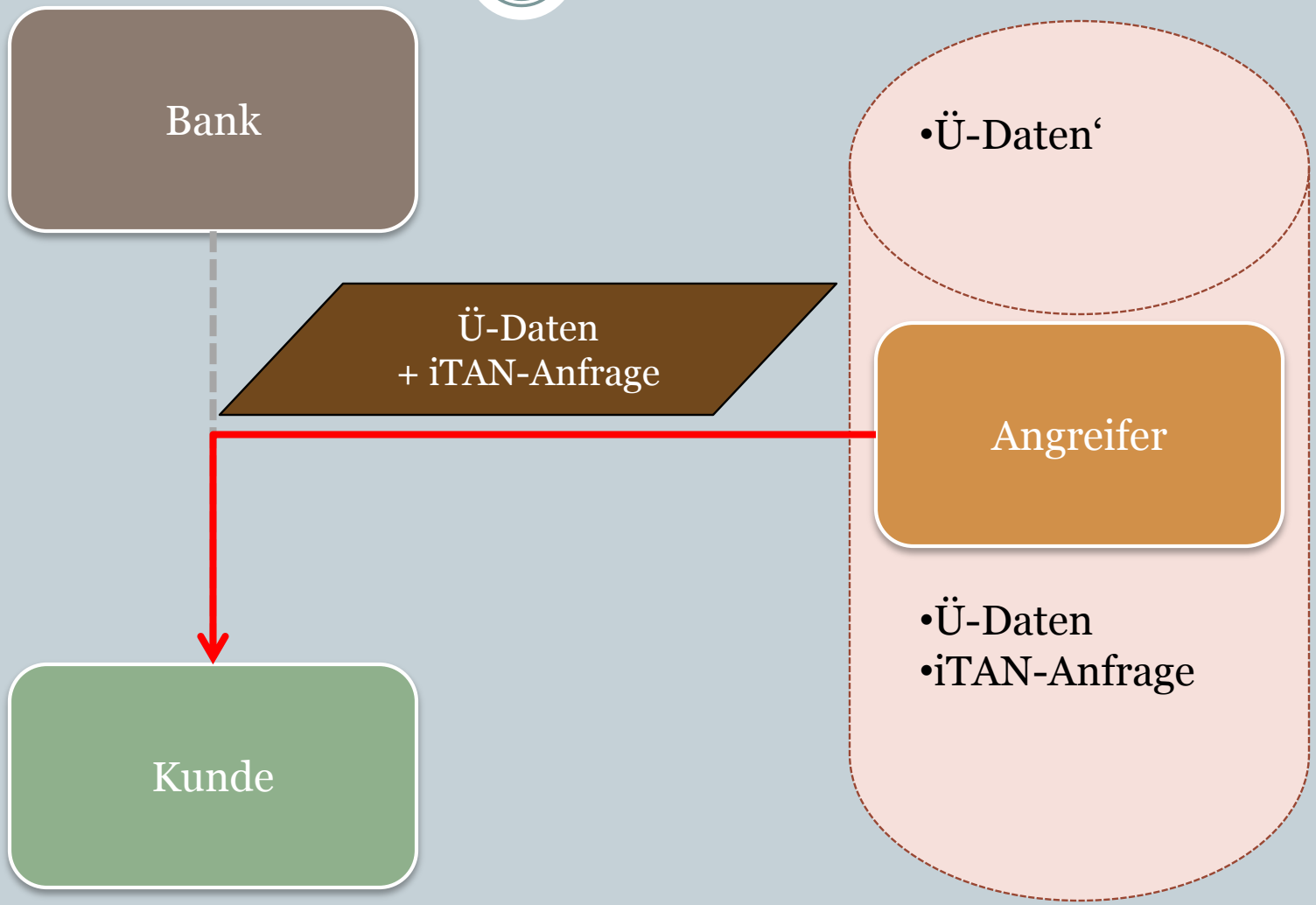
iTAN MITM



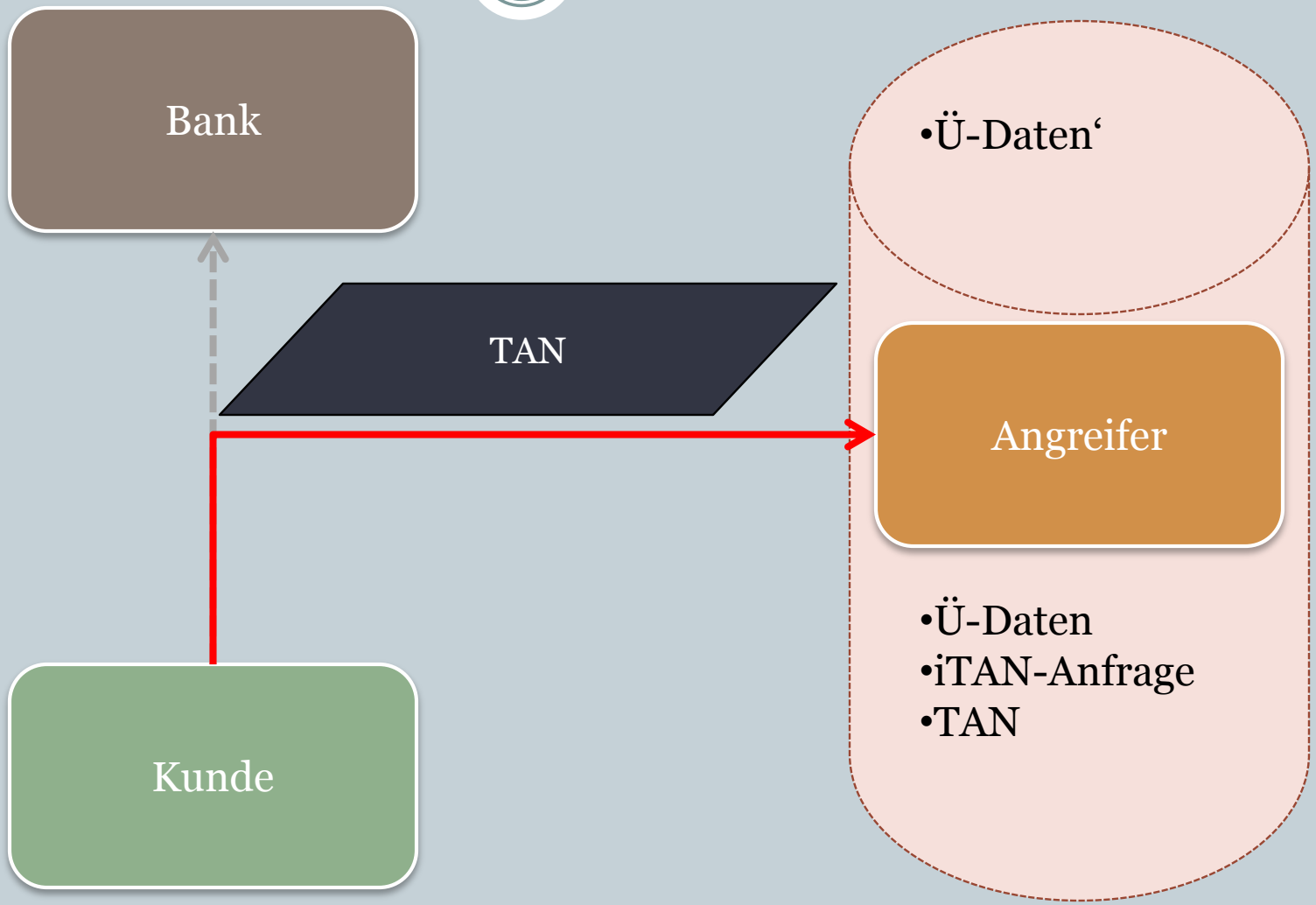
iTAN MITM


Bank
Ü-Daten‘
+ iTAN-Anfrage
Kunde
•Ü-Daten‘
Angreifer
•Ü-Daten
•iTAN-Anfrage

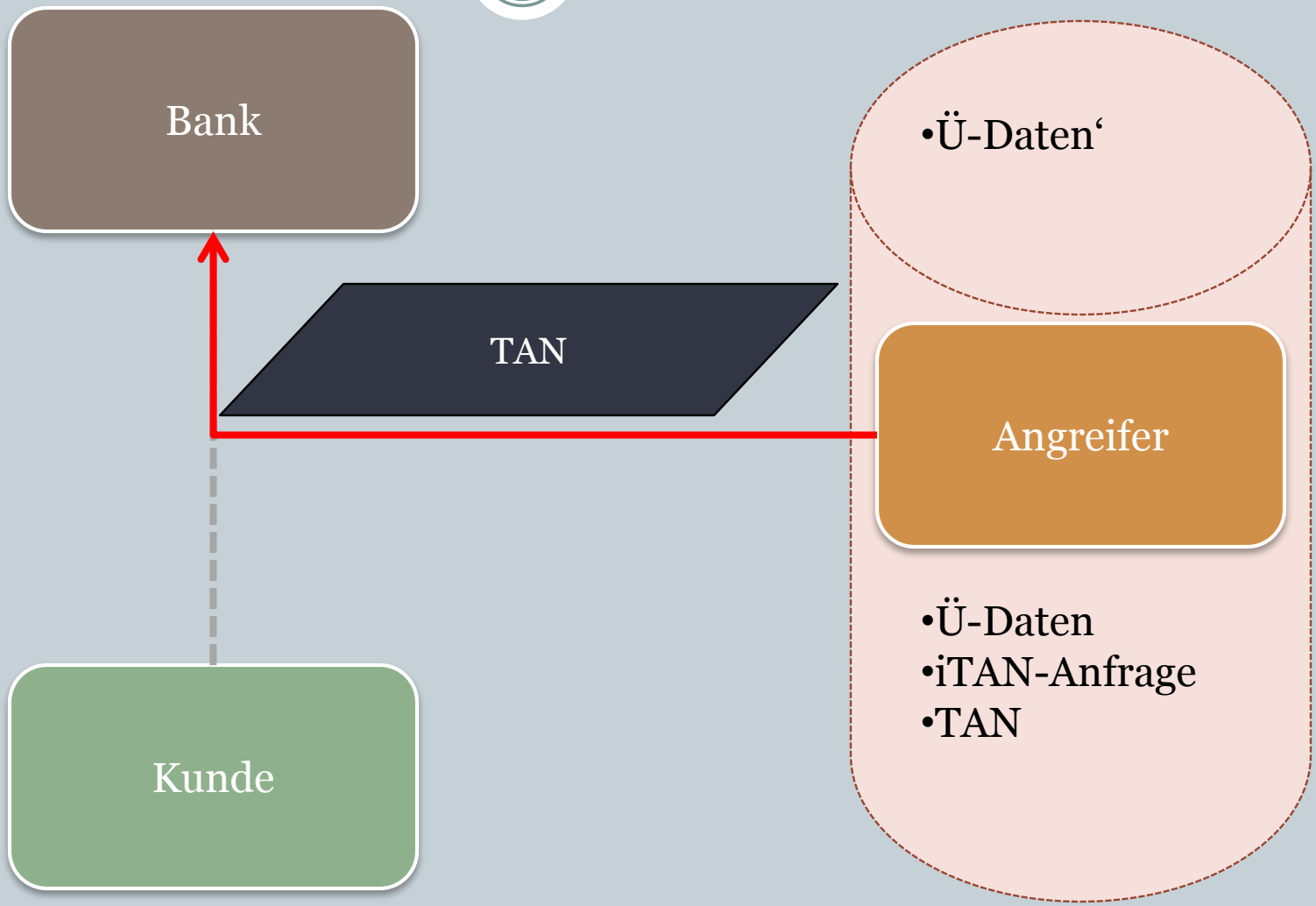
iTAN MITM


Bank
Kunde
Ü-Daten
+ iTAN-Anfrage
Angreifer
•Ü-Daten‘
•Ü-Daten
•iTAN-Anfrage

iTAN MITM



iTAN MITM



Visuelle Kryptographie

- Naor und Shamir EUROCRYPT 1994

Visuelle Kryptographie

- Naor und Shamir EUROCRYPT 1994
- k-aus-n VCS

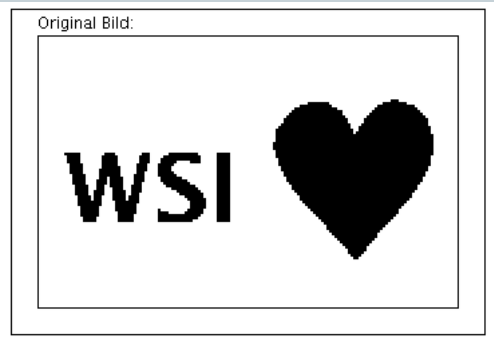
Visuelle Kryptographie

- Naor und Shamir EUROCRYPT 1994
- k-aus-n VCS
- perfekte Sicherheit

Visuelle Kryptographie

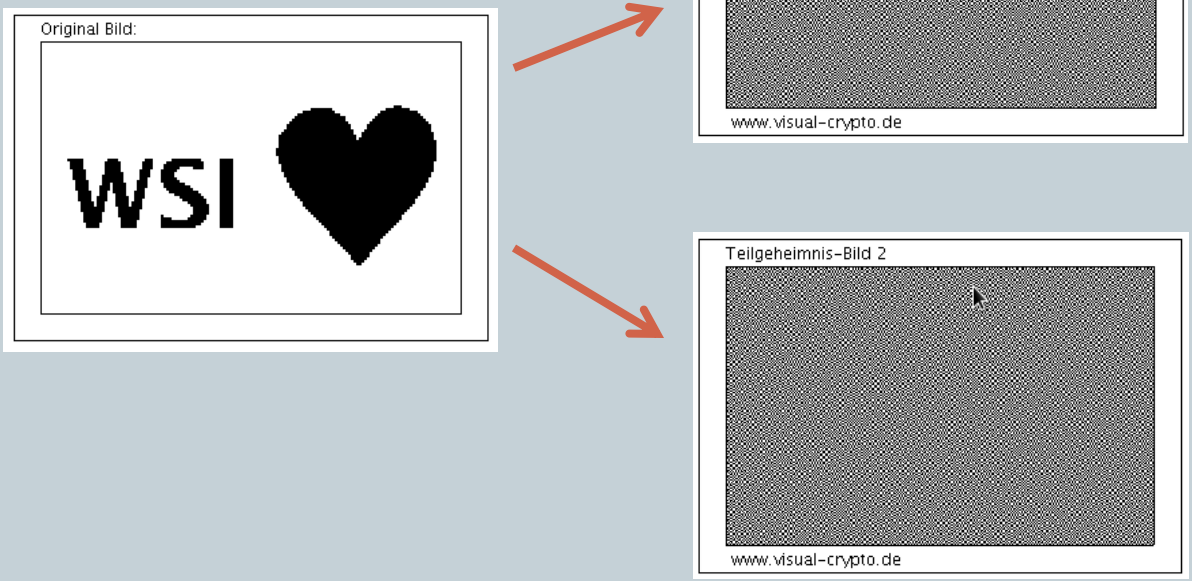
- Naor und Shamir EUROCRYPT 1994
- k-aus-n VCS
- perfekte Sicherheit (bei einmaliger Verwendung)

Visuelle Kryptographie

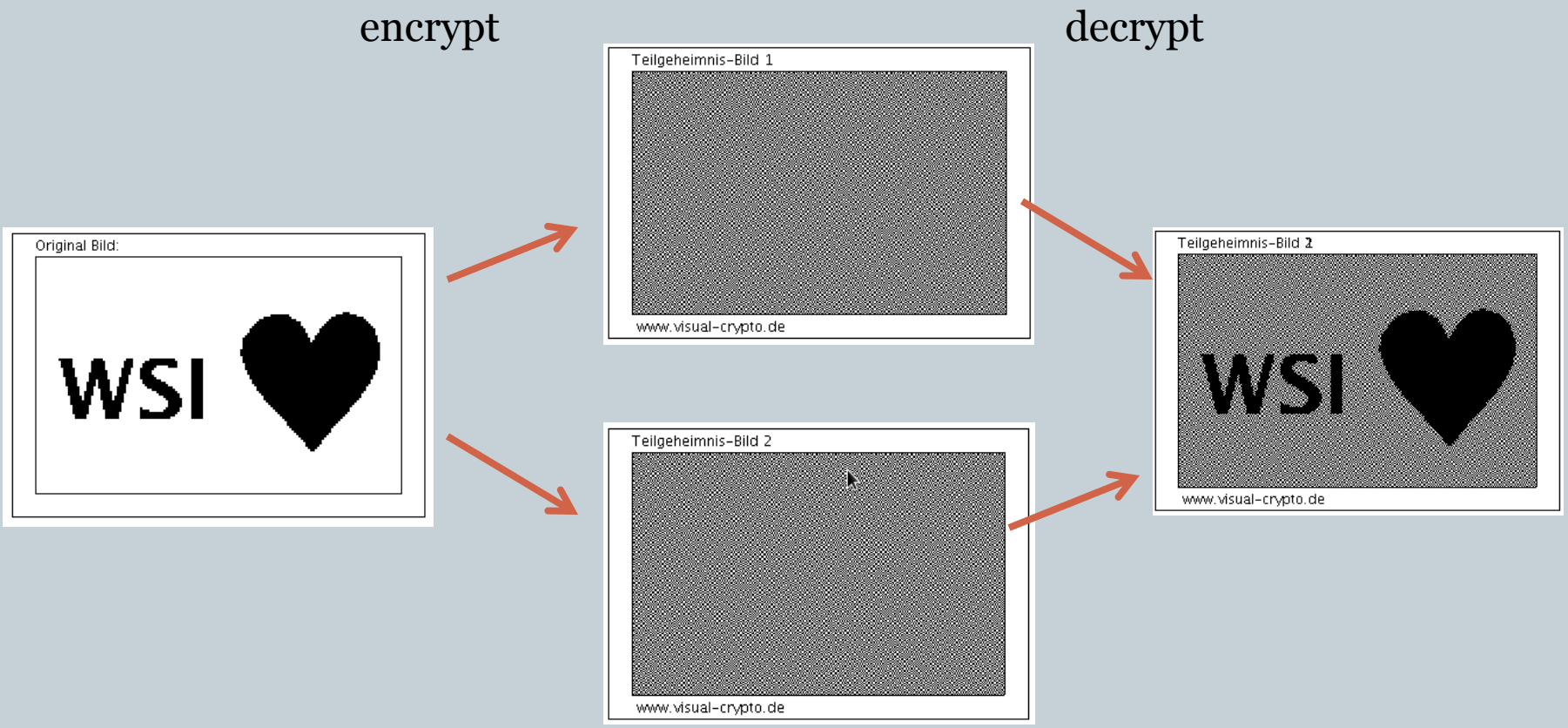


Visuelle Kryptographie

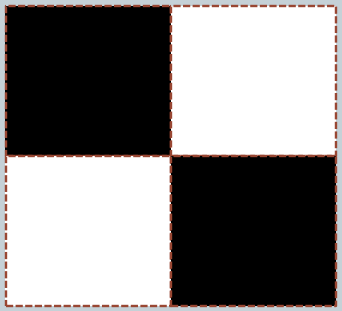
encrypt

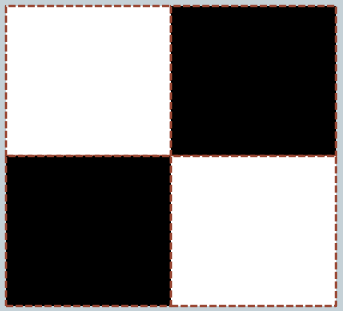


Visuelle Kryptographie



Visuelle Kryptographie

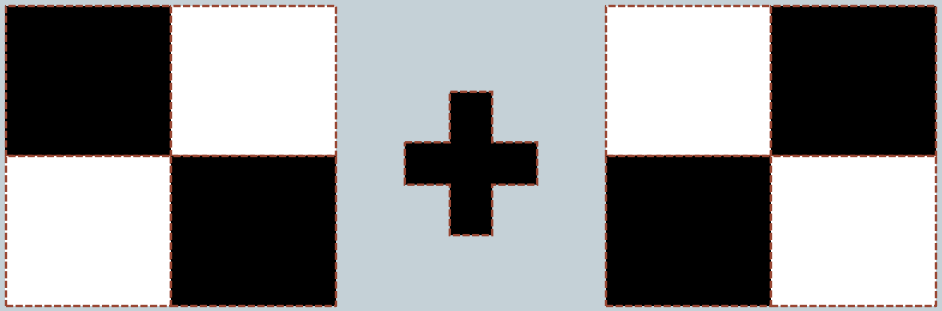




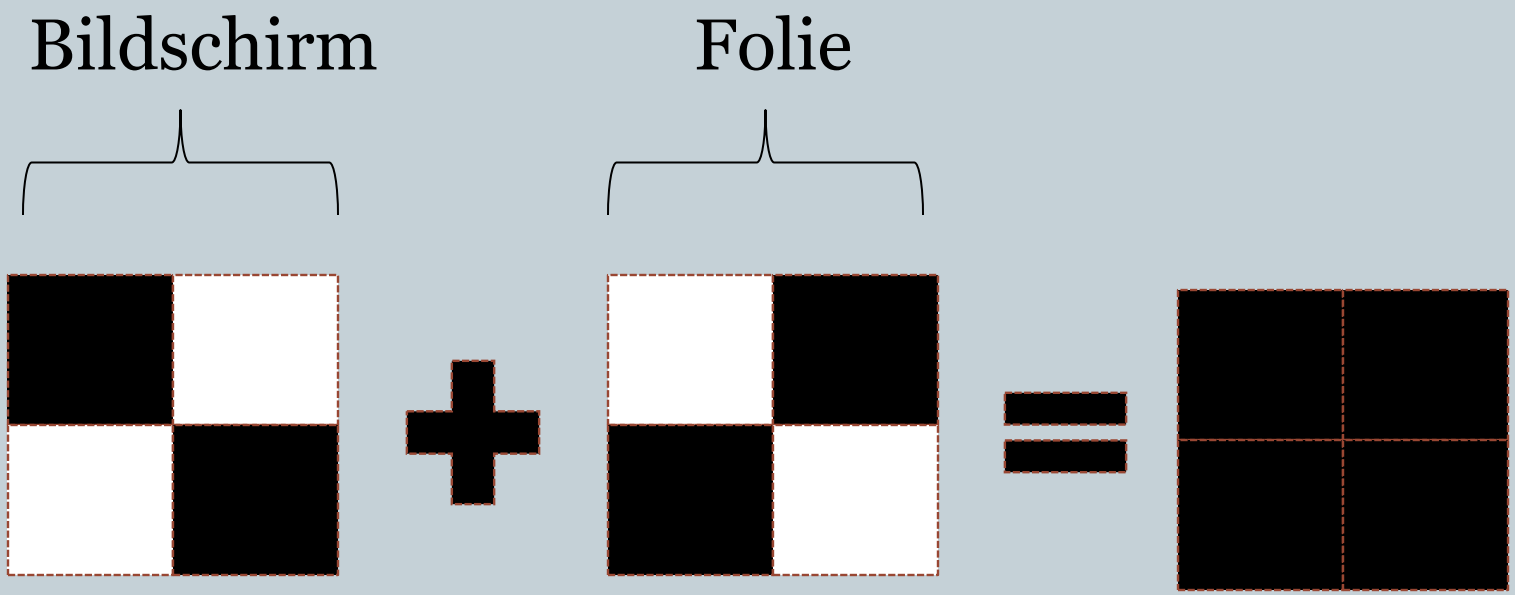
Visuelle Kryptographie

Bildschirm

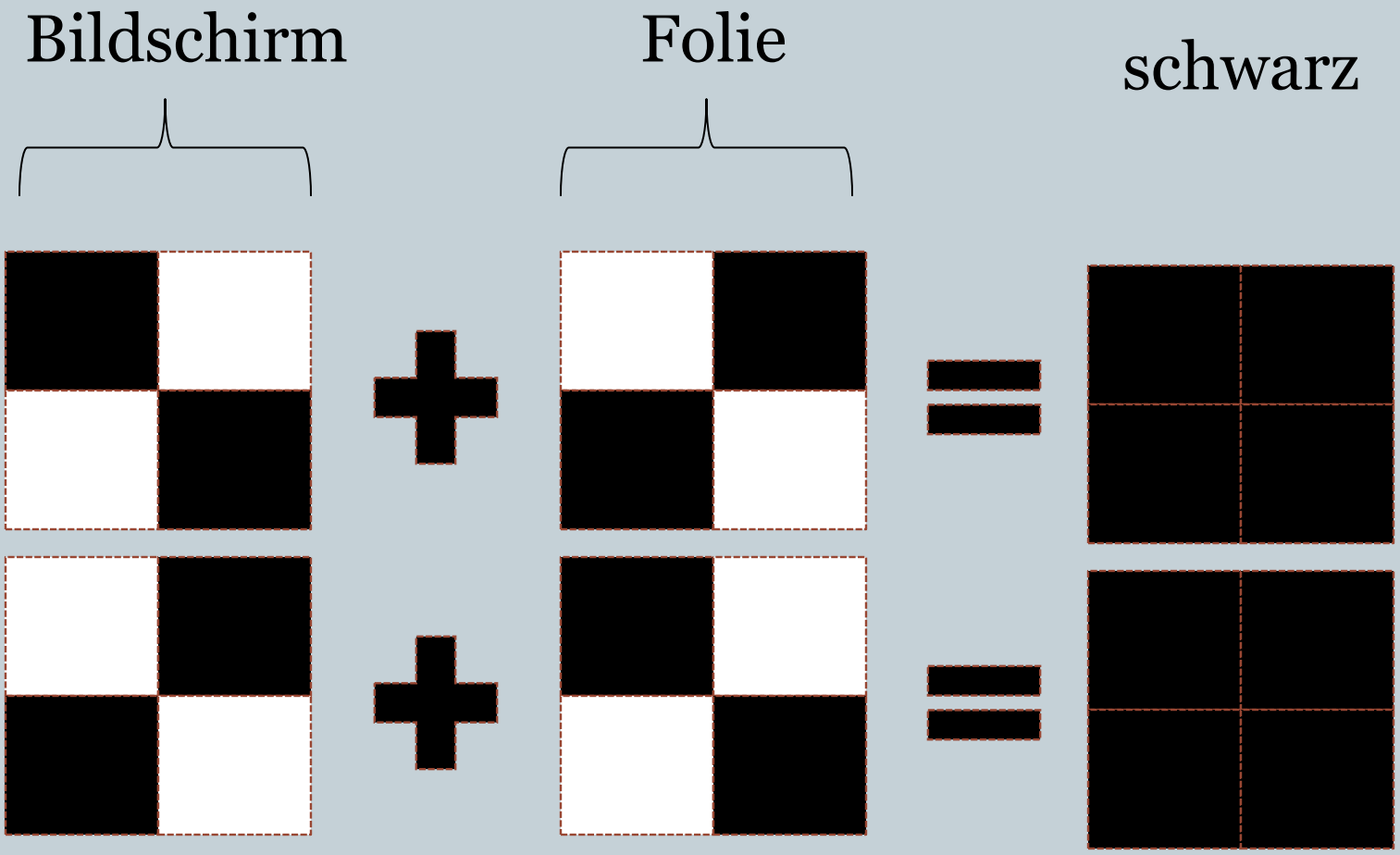
Folie



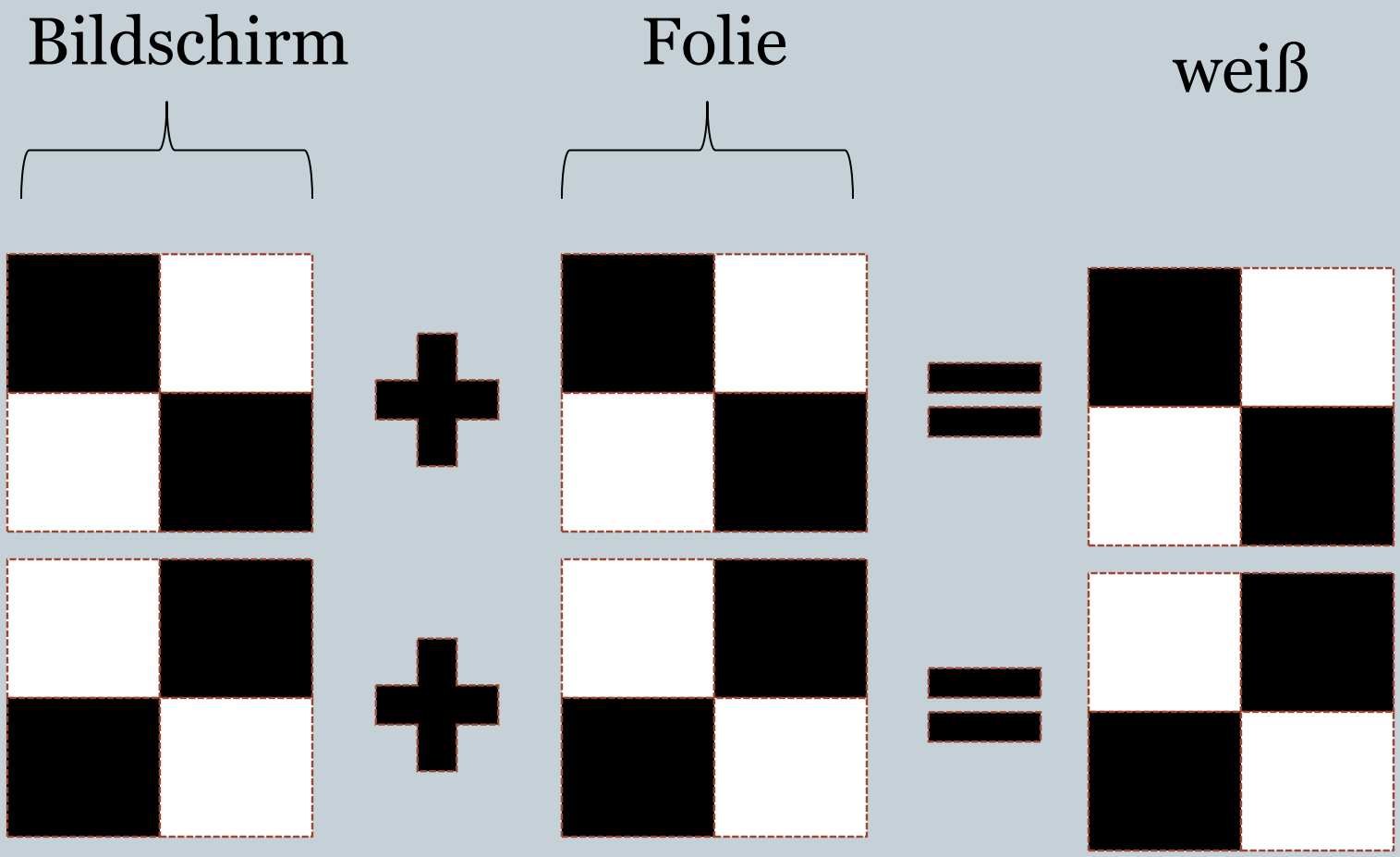
Visuelle Kryptographie



Visuelle Kryptographie



Visuelle Kryptographie

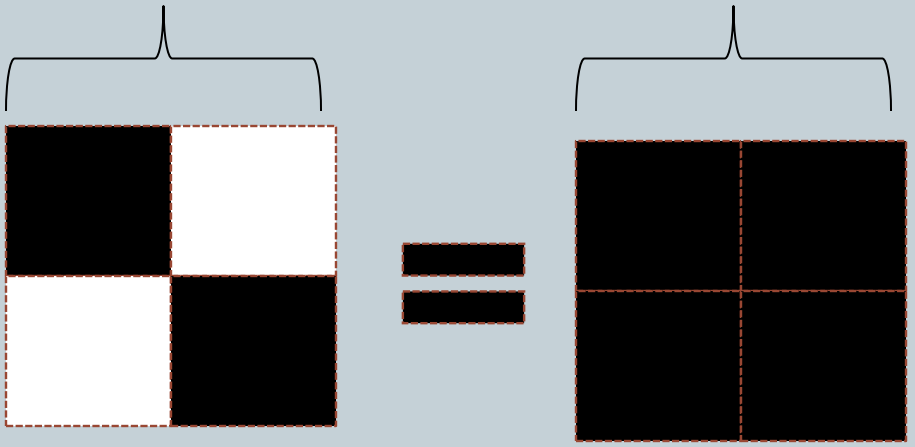


Visuelle Kryptographie

Bank

Bildschirm

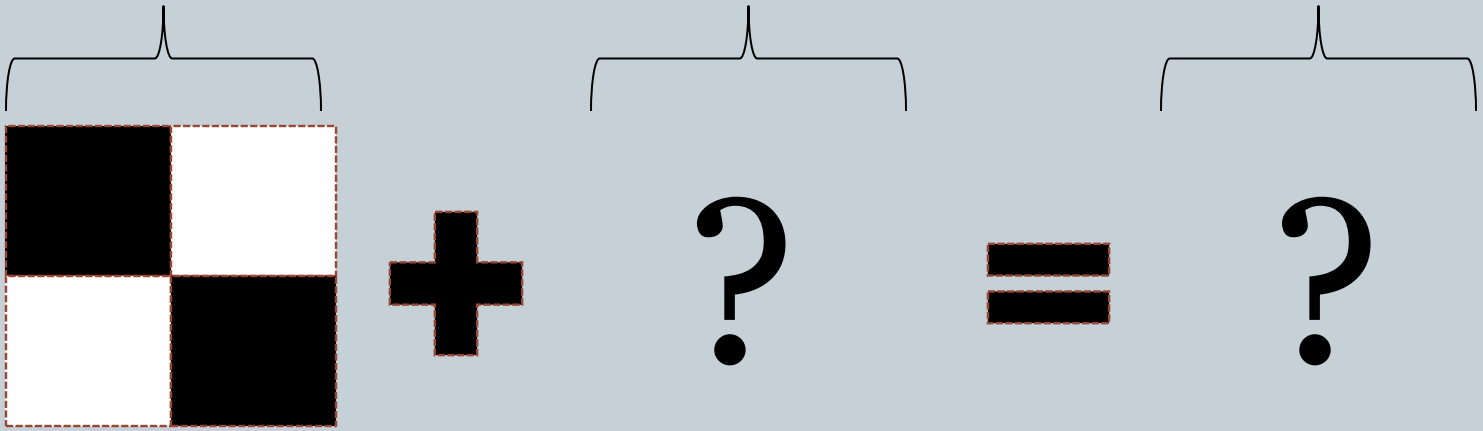
?!



Visuelle Kryptographie

Angreifer

Bildschirm + Folie = Original



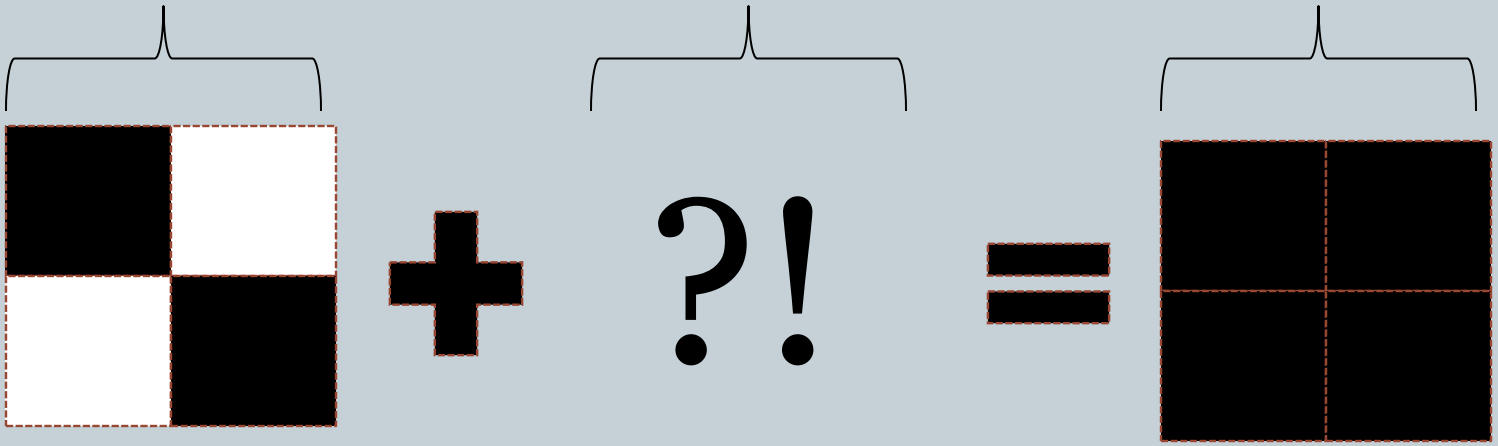
Visuelle Kryptographie

Angriff bei Known-Plaintext

Bildschirm

Folie

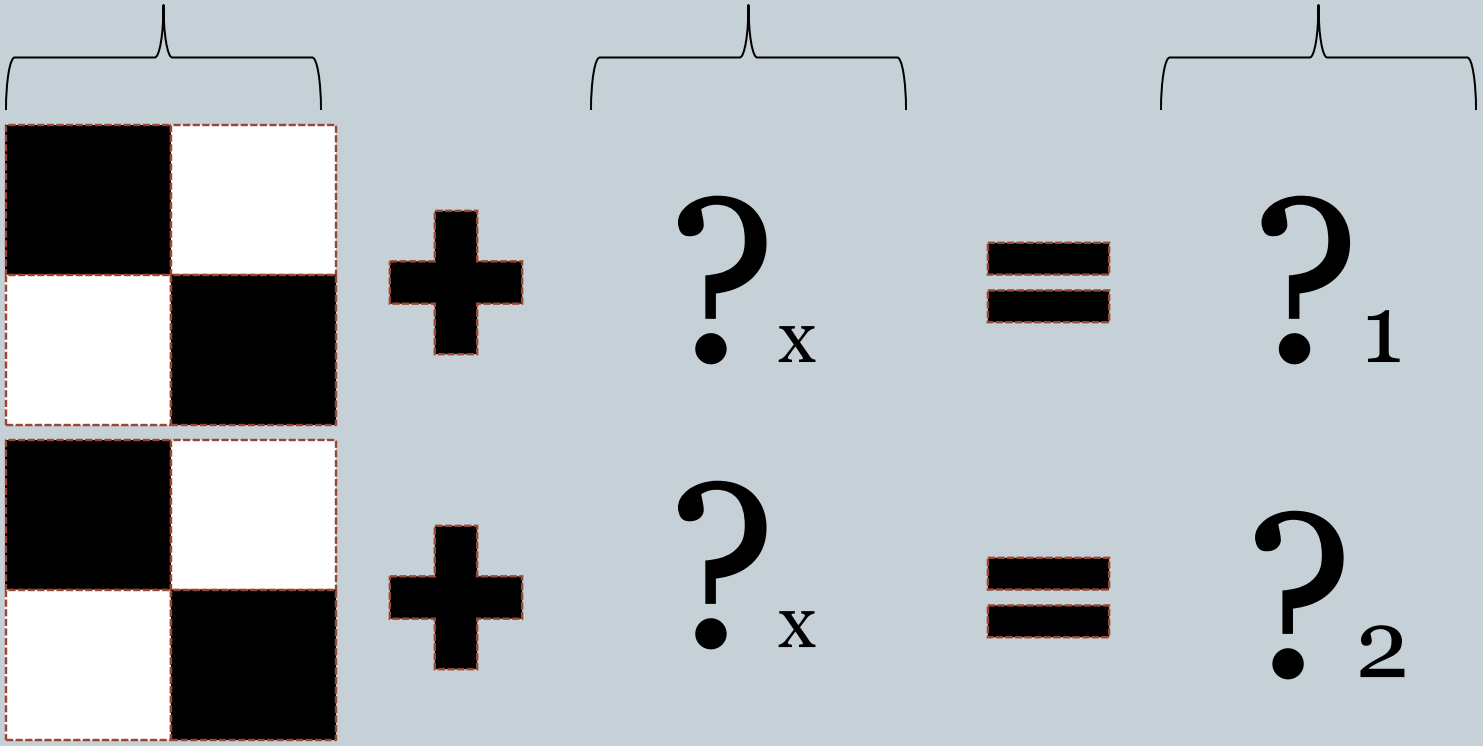
Original



Visuelle Kryptographie

Angriff bei 2-maliger Verwendung

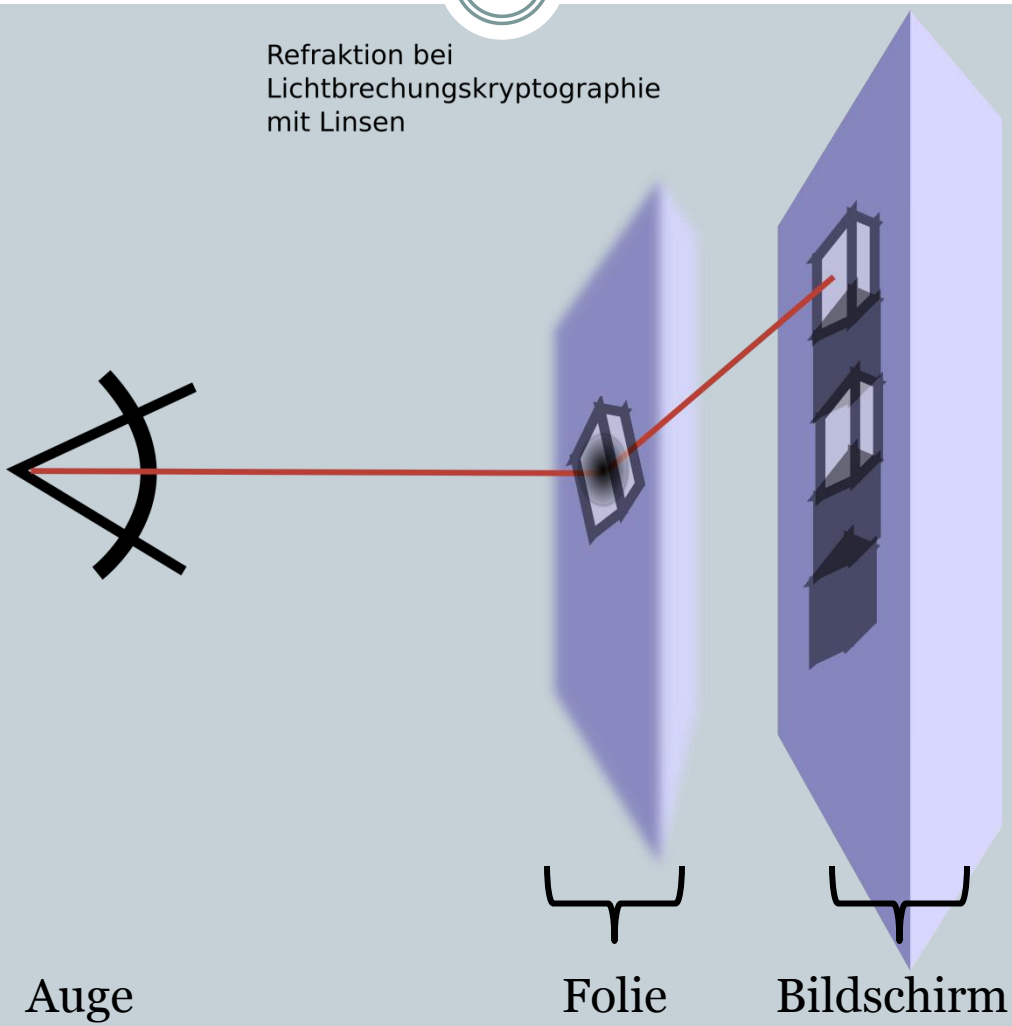
Bildschirm | Folie | Original



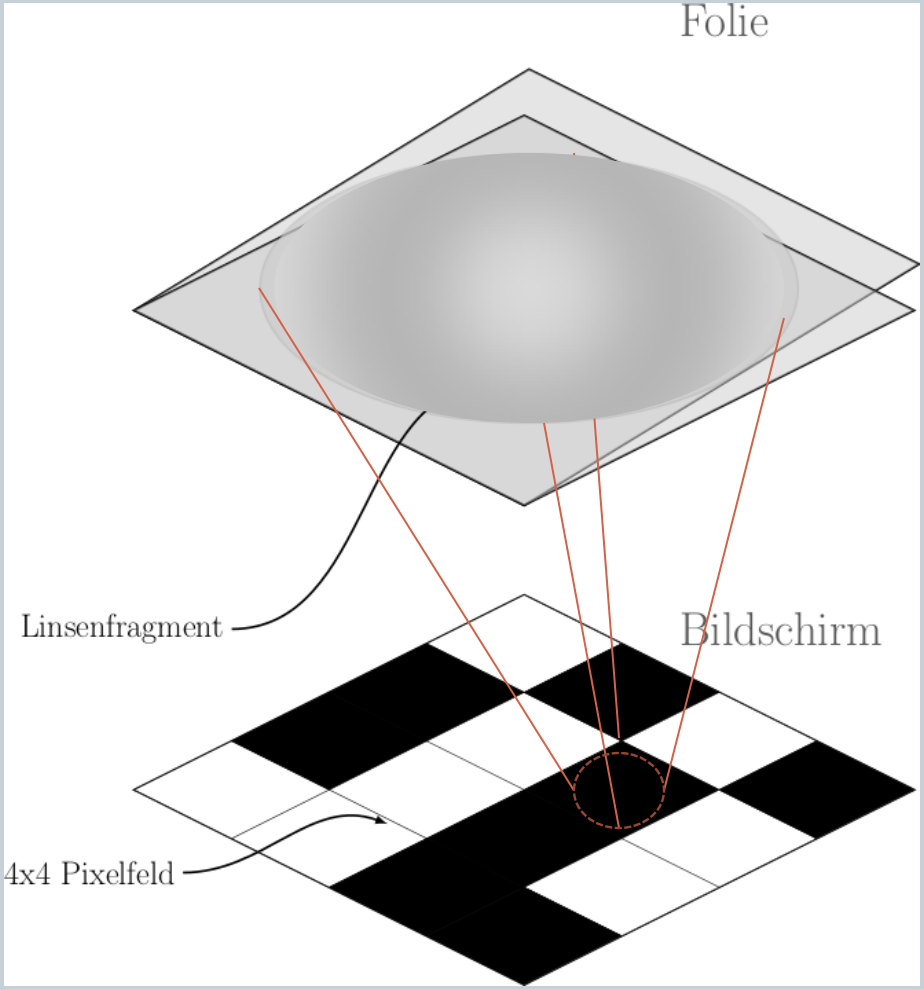
Visuelle Kryptographie

- **VC einmal verwenden ist sicher**
- **Known-Plaintext unsicher**
- **Mehrfachverwendung unsicher**
- **Kontrast schlecht**

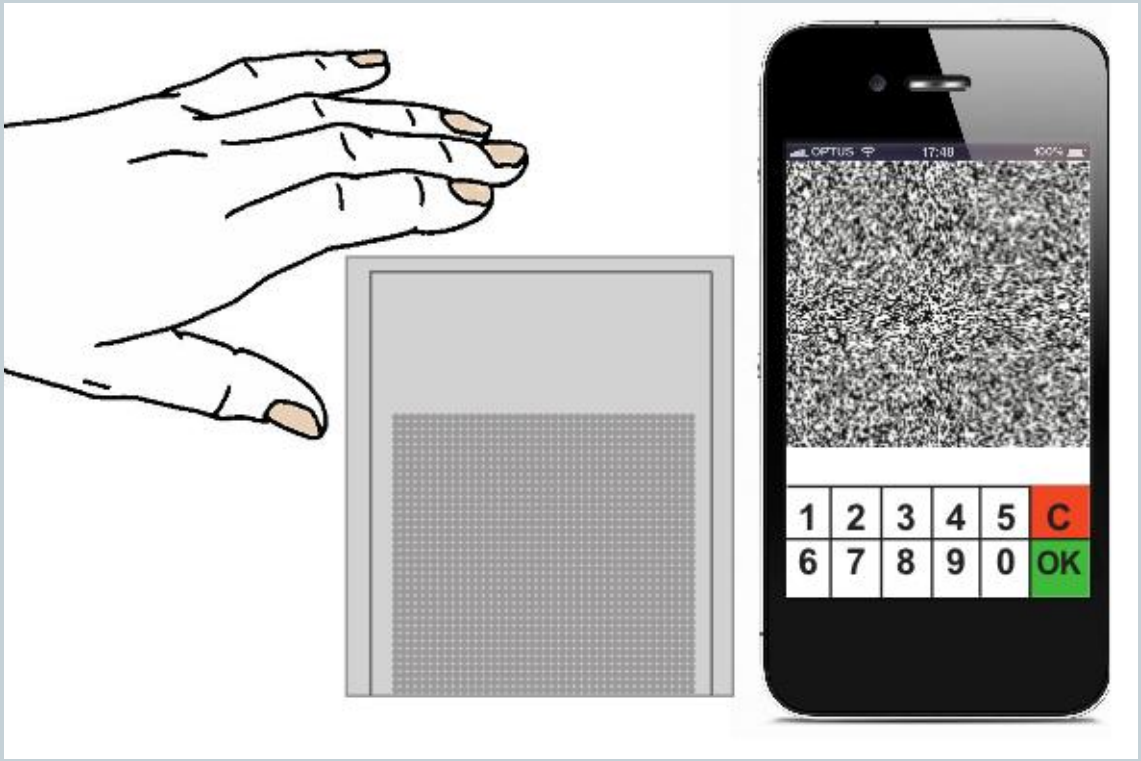
Lichtbrechungs-Kryptographie



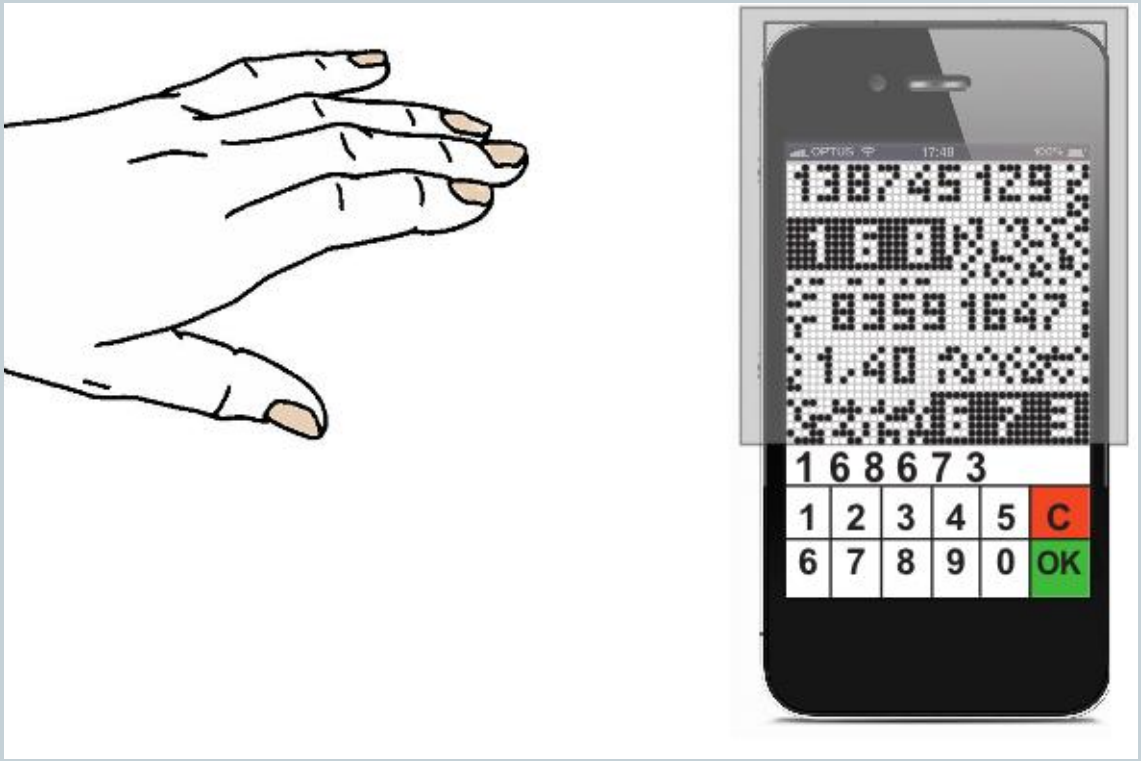
Lichtbrechungs-Kryptographie



Lichtbrechungs-Kryptographie

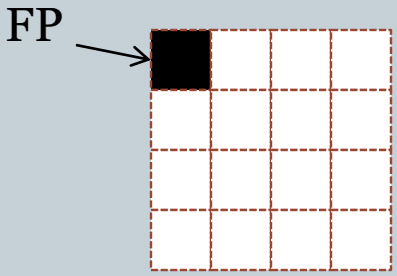


Lichtbrechungs-Kryptographie



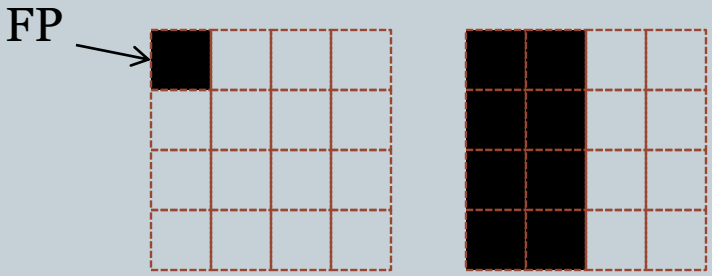
Lichtbrechungs-Kryptographie

Das Belegungsverfahren (Einfachverwendung)



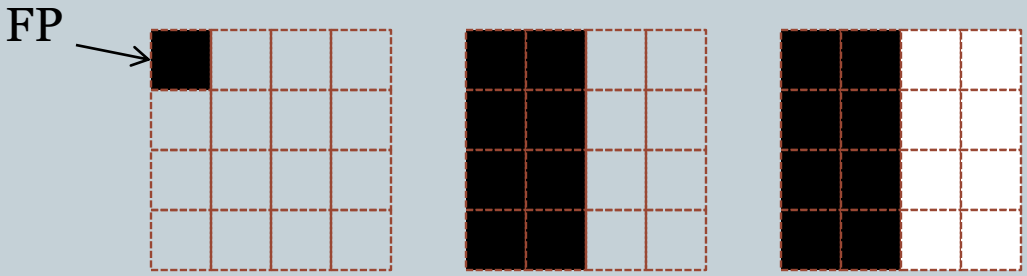
Lichtbrechungs-Kryptographie

Das Belegungsverfahren (Einfachverwendung)



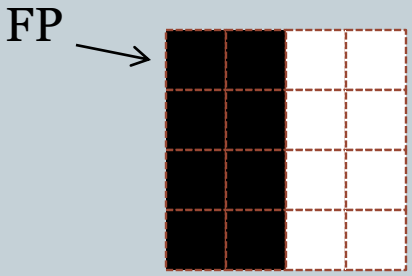
Lichtbrechungs-Kryptographie

Das Belegungsverfahren (Einfachverwendung)



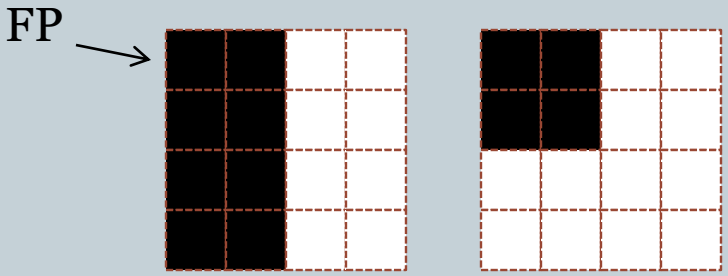
Lichtbrechungs-Kryptographie

Das Belegungsverfahren (Mehrfachverwendung)



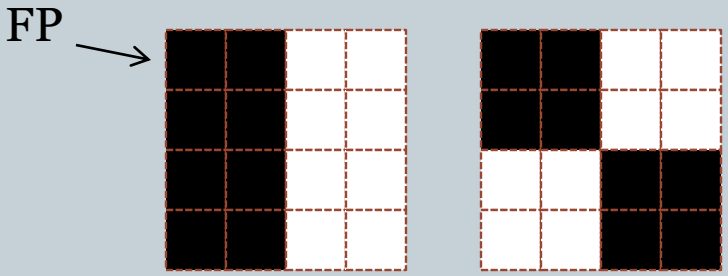
Lichtbrechungs-Kryptographie

Das Belegungsverfahren (Mehrfachverwendung)



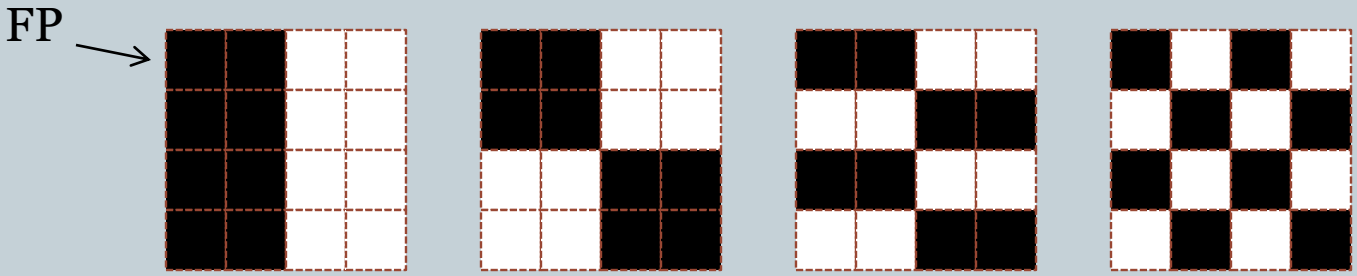
Lichtbrechungs-Kryptographie

Das Belegungsverfahren (Mehrfachverwendung)

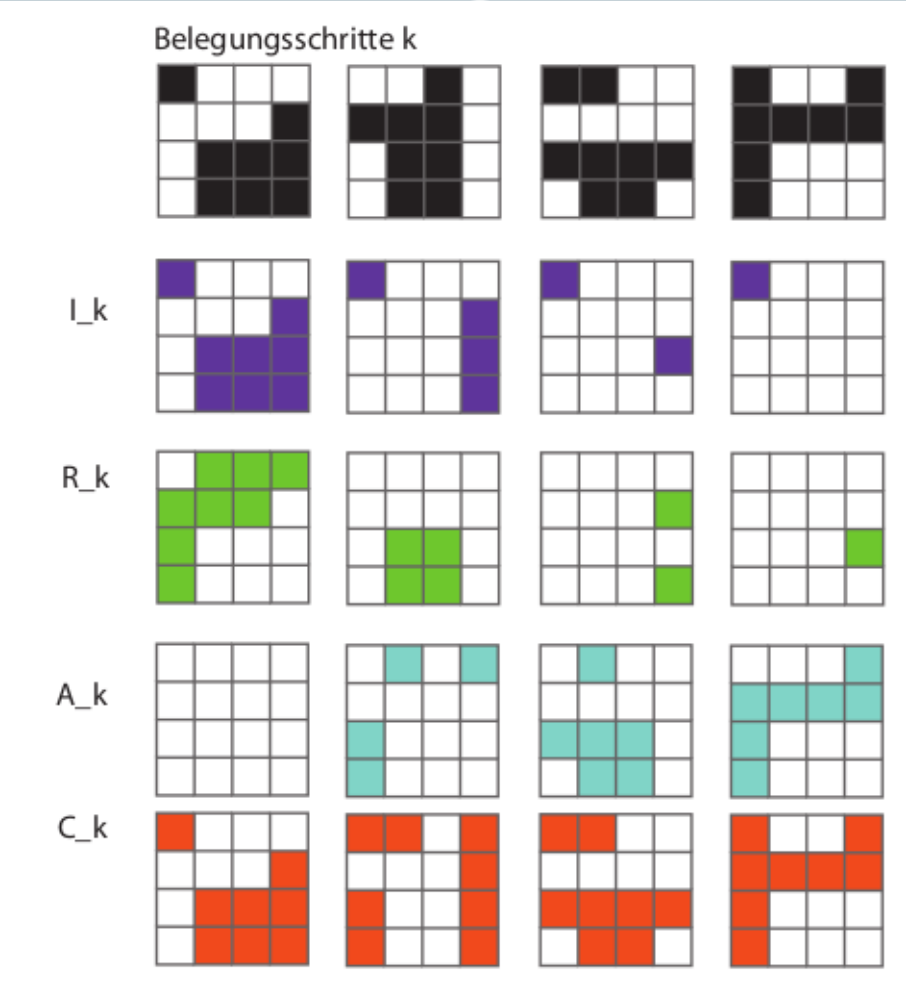


Lichtbrechungs-Kryptographie

Das Belegungsverfahren (Mehrfachverwendung)



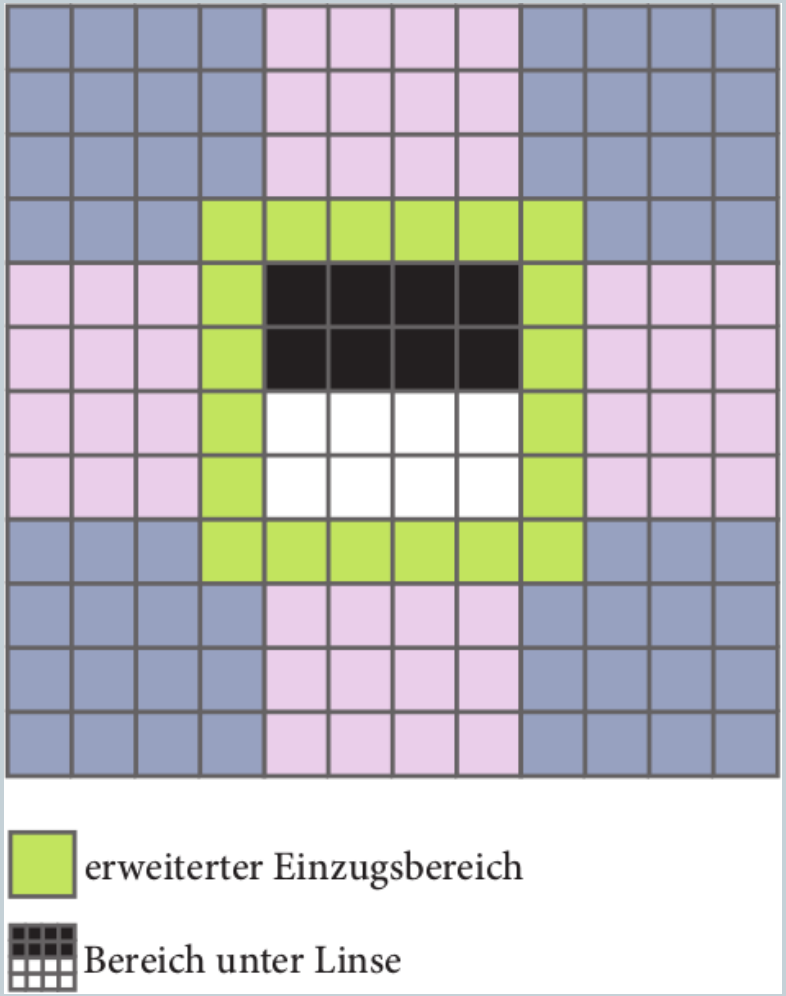
Lichtbrechungs-Kryptographie



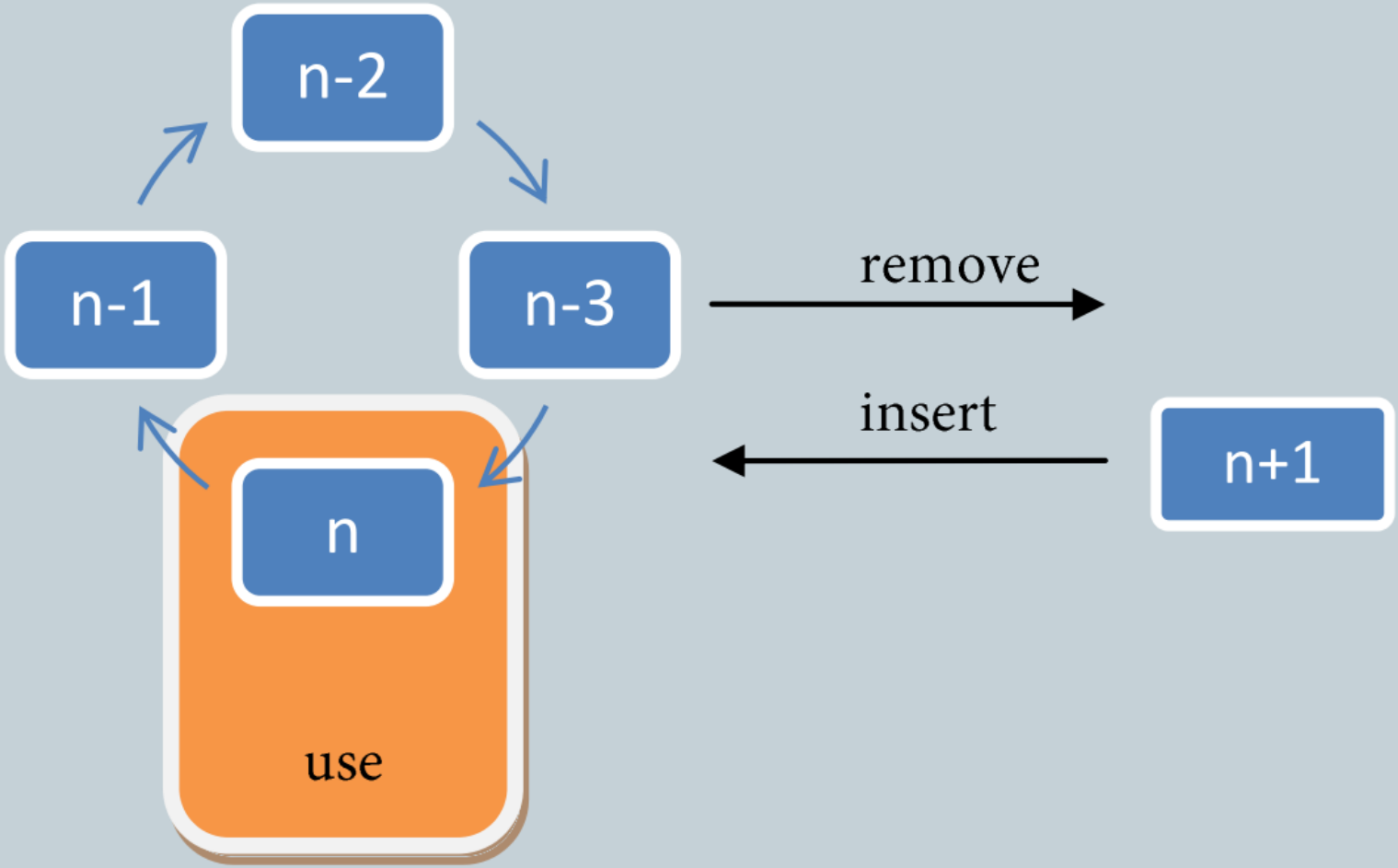
Lichtbrechungskryptographie

- für Onlinebanking nutzbar
- hoher Kontrast, gute Ergonomie
- Einfachverwendung sicher
- $\log_2 n$ Mehrfachverwendungen sicher

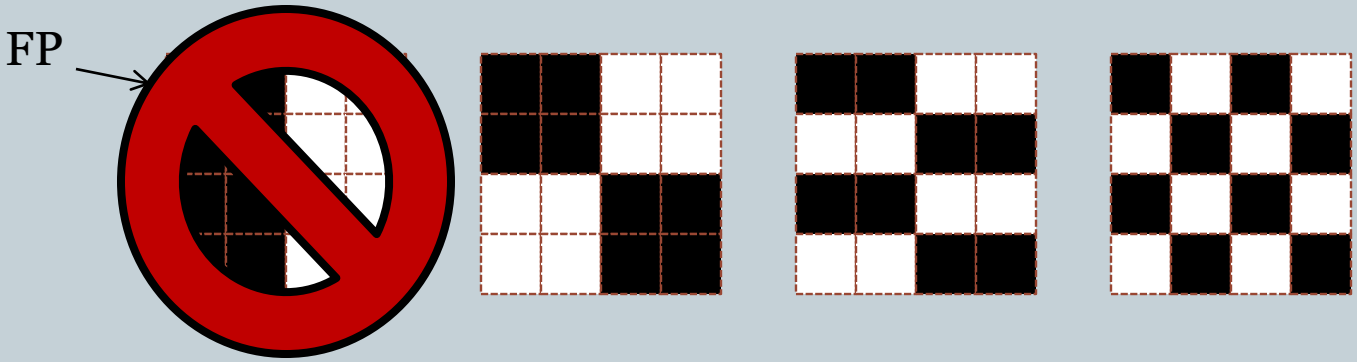
Fokusbereich Erweiterung



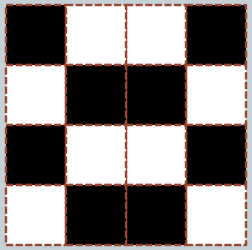
FIFO Erweiterung



FIFO Erweiterung



Schritt V:



Take-Home-Messages

- iTAN –Verfahren nicht sicher
- VC nicht optimal für Onlinebanking
- Wie funktioniert LBK?
- konkretes Anwendungsbeispiel
- LBK mehrfach verwendbar

- Erweiterungen denkbar
- mehr Verwendungen nötig

Danke!