Dresden Database
Systems Group

Entwicklung eines konzeptuellen Modells für Verschlüsselungsalgorithmen

Marie-Christin Kloß

Verteidigung Bachelorarbeit, 27. September 2016

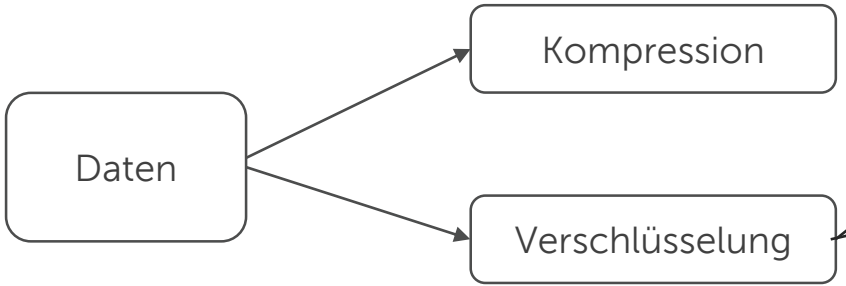
Motivation

Dresden Database Systems Group

Daten im Umfeld von Datenbanksystemen

- Daten werden in der Regel komprimiert ablegt
  - Vielzahl von Algorithmen existieren
  - Konzeptuelles Modell für diesen Bereich existiert (Arbeit von Juliana)

- Neben Kompression spielt Verschlüsselung auch eine große Rolle
  - Auch hier existiert eine Vielzahl von Ansätzen



Ziel der Arbeit:

- Aufarbeitung verschiedener Verschlüsselungsalgorithmen
- Entwicklung eines konzeptuellen Modell zur einheitlichen Beschreibung

Vorstellung XSX-Algorithmus

XSX-Algorithmus

Dresden Database Systems Group

Allgemein

- Algorithmus für Tabellen
- Ziel: maximale Datenvermischung bei minimaler Anzahl von Schritten
- Verwendung von 2 Schlüsseln für XOR, 1 Schlüssel für Bit Swichting

Schlüsselerstellung

- MasterKey: universeller Schlüssel
- RowKey mit Tabelle innerhalb der Datenbank

→Zufallszahl ⊕ MasterKey

- ColumnKey: Zufallszahl
- Skey: Zufallszahl

	Column1	Column2	Column3	RowKey
Row1	a1	a2	a3	RK1
Row2	b1	b2	b3	RK2
Row3	c1	c2	c3	RK3

Skey:	SK1	SK2	SK3
Ckey:	CK1	CK2	CK3
MasterKey			

XSX(2)

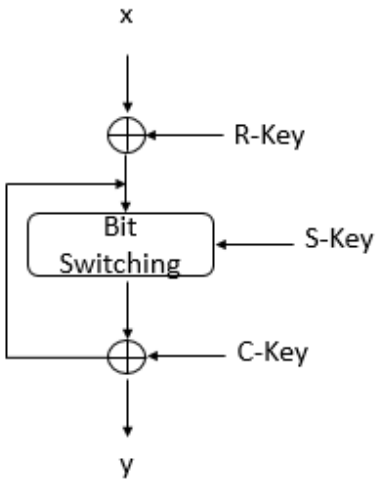
Dresden Database Systems Group

Verschlüsselung

- Plaintext x ⊕ RK
- Bitswitching (SK) ⊕ Ckey → Chiffrentext y

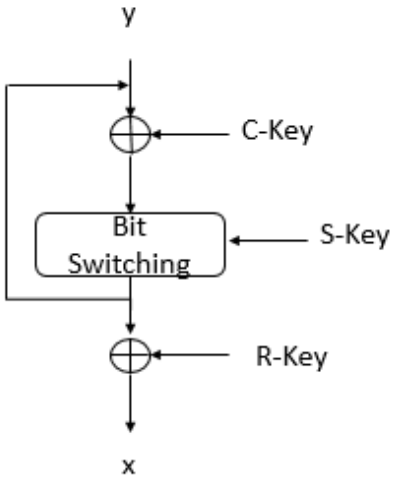
Entschlüsselung

- Chiffrentext y ⊕ CK, Bitswitching (SK)
- Zwischenergebnis ⊕ RK → Chiffrentext x



	Column1	Column2	Column3	RowKey
Row1	a1	a2	a3	RK1
Row2	b1	b2	b3	RK2
Row3	c1	c2	c3	RK3

Skey:	SK1	SK2	SK3
Ckey:	CK1	CK2	CK3
MasterKey			



Bestehende konzeptuelle Modelle

TS-Modell

Dresden Database Systems Group

Allgemein

- Konfiguration der Sicherheitseinstellung
- S- {Sicherheitskonfiguration}
- U- {Benutzervorlieben}
- E- {Anwendungs-/ Umgebungseinstellung}

Funktionsweise

- Pro Parameter Vorgabe mehrerer Werte und durch Benutzer Auswahl
- Einstellbar, wie sicher bzw. nutzerfreundlich bzw. Kompromiss aus beiden

Anwendbar

- Nein: bei Verschlüsselung keine Auswahl von Mengen
- Nein: hierarchische Strukturen lassen sich nicht als Menge darstellen

Kompressionsmodell

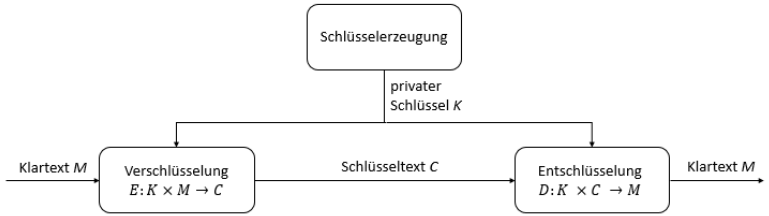
Dresden Database Systems Group

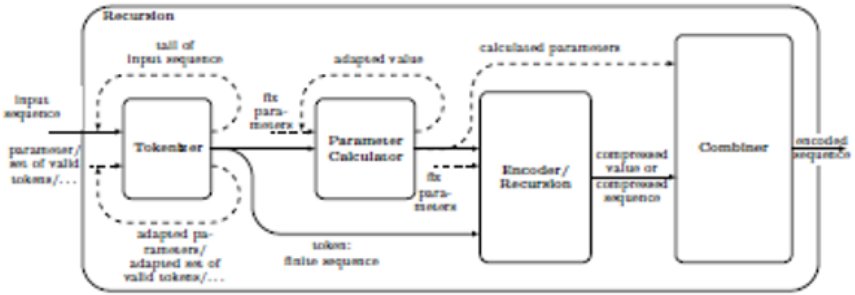
Funktionsweise

- Tokenizer: teilt Input in gewünschte Größe
- ParameterCalculator: Berechnung benötigter Werte/Parameter für Komprimierung
- Rekursion: Rekursion, in der die Kompression für einzelne Werte berechnet wird
- Encoder: führt eigentliche Kompression durch
- Combiner: fügt komprimierte Werte zur gewünschten Form zusammen

Anwendbar

- Ja, aber mit Modifikationen
- Umsetzung von 3 Konzepten (Schlüsselerstellung, Verschlüsselung, Entschlüsselung)





konzeptuelles Modell für Kompressionsalgorithmen [8]

Konzeptuelles Modell für Verschlüsselung

Schlüsselerstellung XSX

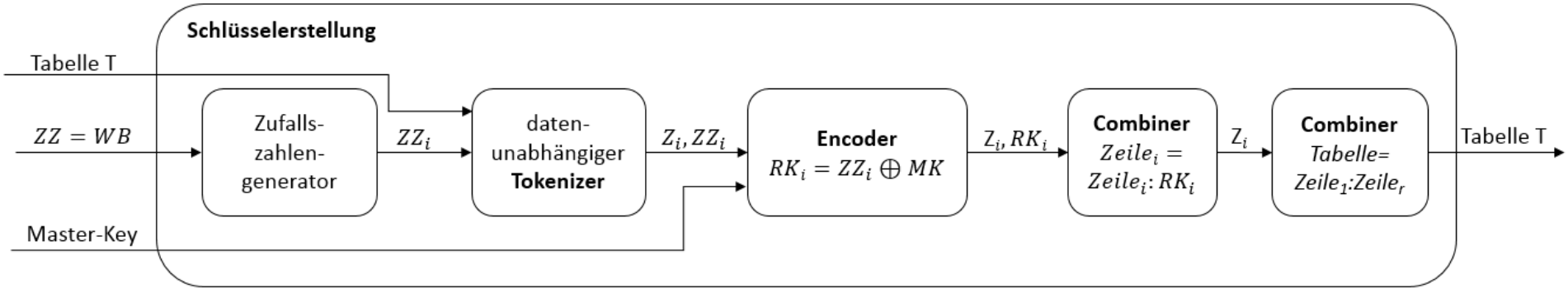
Dresden Database Systems Group

Modifikation

- Hinzufügen eines Zahlengenerators, 2. Combiners
- Zerteilen der Tabelle im Tokenizer
- Berechnung im Encoder
- Zusammenbauen der Tabelle in den beiden Combiner

	Column1	Column2	Column3	RowKey
Row1	a1	a2	a3	RK1
Row2	b1	b2	b3	RK2
Row3	c1	c2	c3	RK3

Skey:	SK1	SK2	SK3
Ckey:	CK1	CK2	CK3
MasterKey			



Verschlüsselung XSX

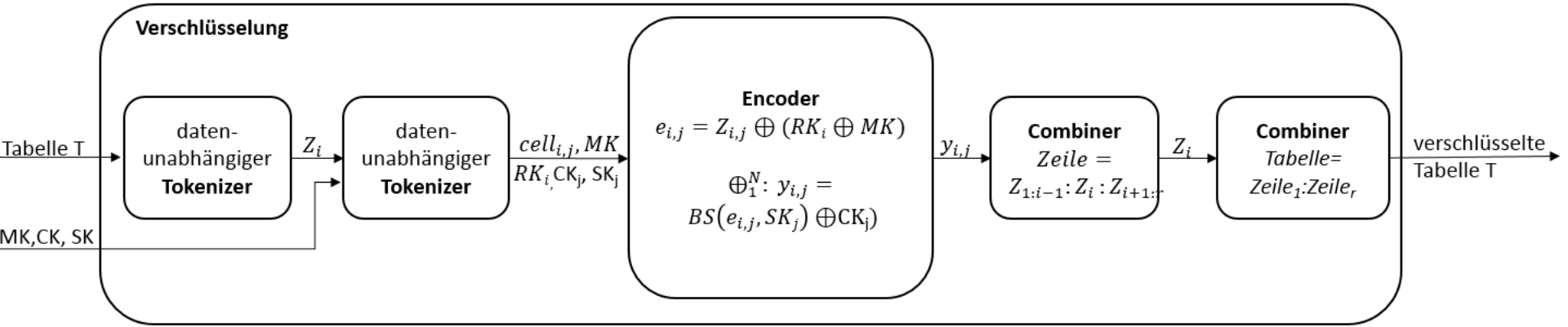
Dresden Database Systems Group

Funktionsweise

- 2 Tokenizer und 2 Combiner
- Verschlüsselung der einzelnen Zellen im Encoder
- Ausgabe verschlüsselter Tabelle

	Column1	Column2	Column3	RowKey
Row1	a1	a2	a3	RK1
Row2	b1	b2	b3	RK2
Row3	c1	c2	c3	RK3

Skey:	SK1	SK2	SK3
Ckey:	CK1	CK2	CK3
MasterKey			



Entschlüsselung XSX

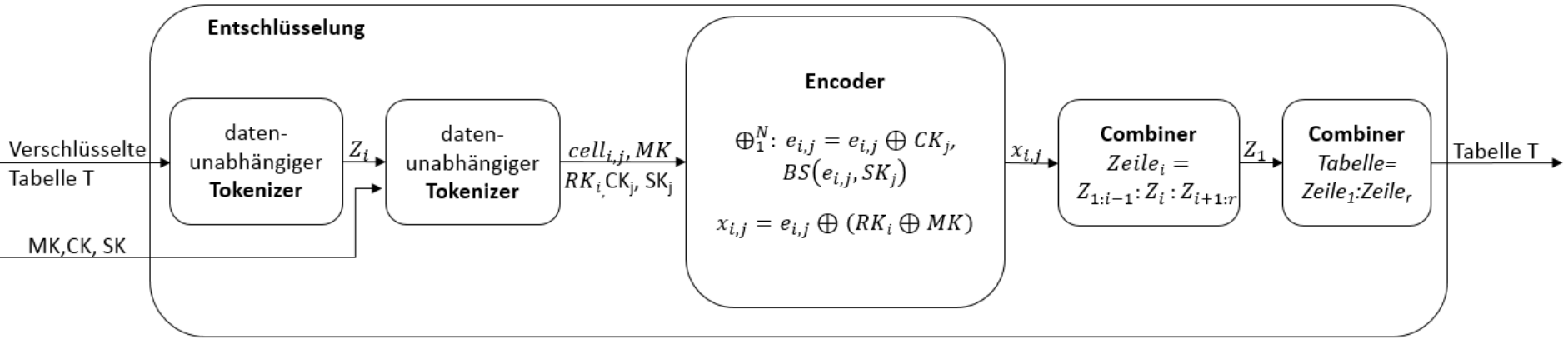
Dresden Database Systems Group

Funktionsweise

- 2 Tokenizer und 2 Combiner
- Entschlüsselung im Encoder
- Ausgabe der entschlüsselten Tabelle

	Column1	Column2	Column3	RowKey
Row1	a1	a2	a3	RK1
Row2	b1	b2	b3	RK2
Row3	c1	c2	c3	RK3

Skey:	SK1	SK2	SK3
Ckey:	CK1	CK2	CK3
MasterKey			



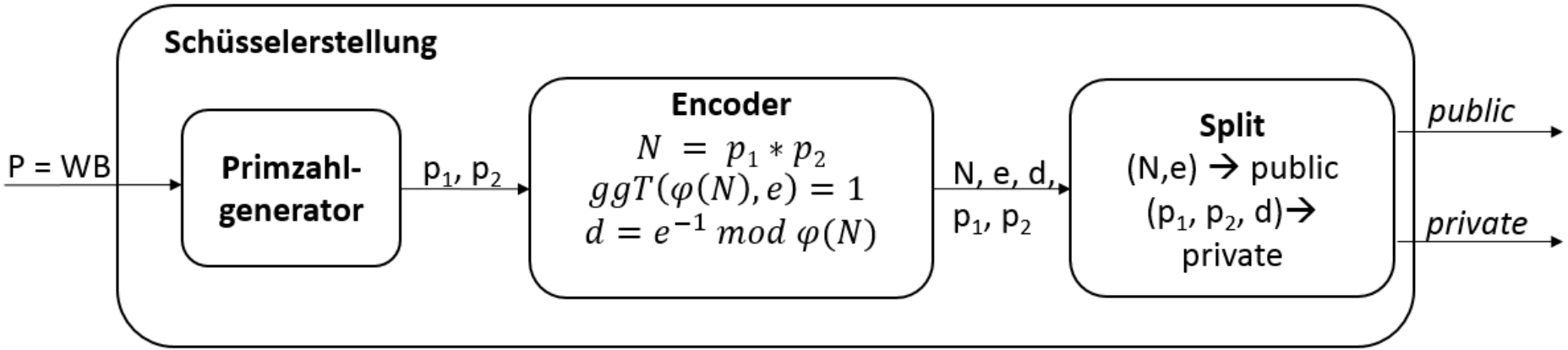
Evaluation

Anwendung RSA(1)

Dresden Database Systems Group

Schlüsselerstellung

- Zahlengenerator als Primzahlengenerator modifiziert
- Berechnung im Encoder
- Split: Aufteilung der Werte auf die Schlüssel

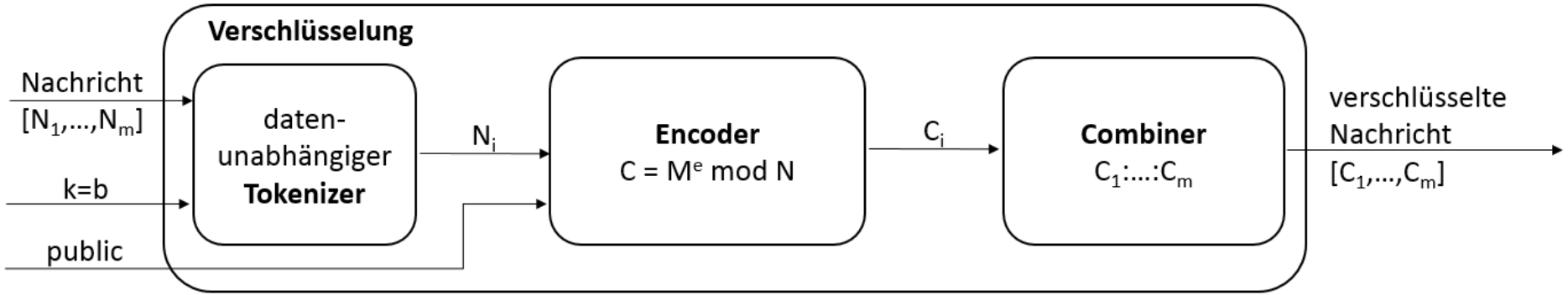


Anwendung RSA(2)

Dresden Database Systems Group

Verschlüsselung

- Gegebenenfalls Teilung der Nachricht
- Öffentliche Schlüssel *public = (N, e)* für Verschlüsselung
- Verschlüsselung im Encoder
- Konkatenation zur Ausgangsform

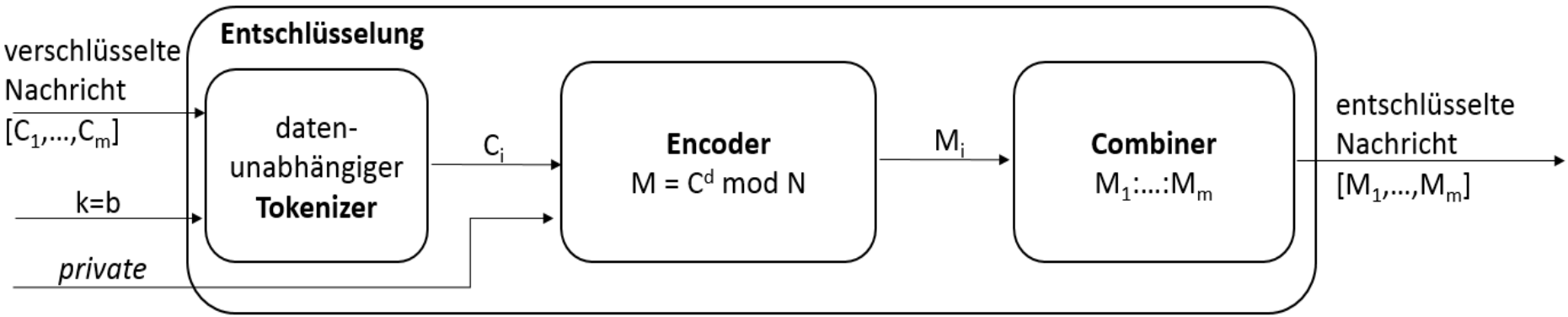


Anwendung RSA(3)

Dresden Database Systems Group

Entschlüsselung

- Gegebenenfalls Teilung der Nachricht
- Privater Schlüssel *private = (p_1, p_2, d)* für Verschlüsselung
- Verschlüsselung im Encoder
- Konkatenation zur Ausgangsform



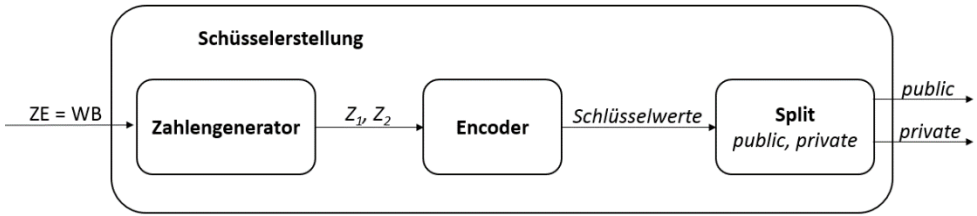
Zusammenfassung

Zusammenfassung

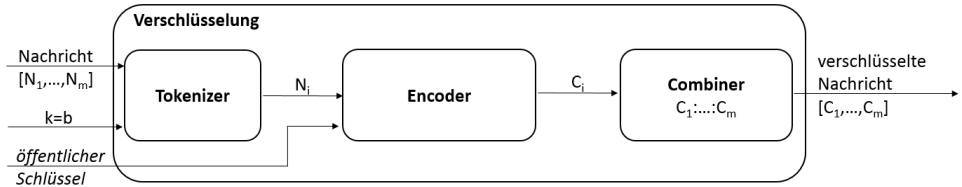
Dresden Database Systems Group

Grundmodelle

- Für Schlüsselerstellung, ja nach symmetrischen oder asymmetrischen Verfahren



- Für Verschlüsselung & Entschlüsselung



Ergänzungen

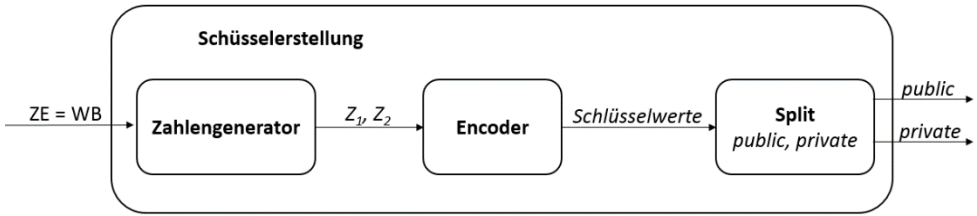
- Manche Konzepte nur manchmal:
  - Split bei asymmetrischer Schlüsselerstellung
  - Combiner bei symmetrischer Schlüsselerstellung
  - 2. Tokenizer & 2. Combiner bei Tabellen
  - ParameterCalculator & Rekursion nur bei datenabhängigen Algorithmen

Zusammenfassung

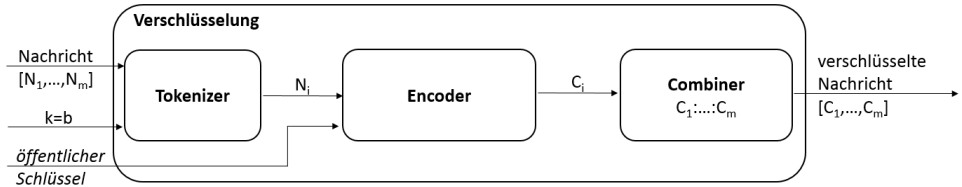
Dresden Database Systems Group

Grundmodelle

- Für Schlüsselerstellung, ja nach symmetrischen oder asymmetrischen Verfahren



- Für Verschlüsselung & Entschlüsselung



Ergänzungen

- Manche Konzepte nur manchmal:
  - Split bei asymmetrischer Schlüsselerstellung
  - Combiner bei symmetrischer Schlüsselerstellung
  - 2. Tokenizer & 2. Combiner bei Tabellen
  - ParameterCalculator & Rekursion nur bei datenabhängigen Algorithmen

Dresden Database Systems Group

Entwicklung eines konzeptuellen Modells für Verschlüsselungsalgorithmen

Marie-Christin Kloß