Scalable Cryptography

Dennis Hofheinz und Eike Kiltz

Karlsruher Institut für Technologie und Ruhr-Universität Bochum

Motivation

- Gegenwärtige Kryptographie nicht bereit für große Szenarien
  - Gängige **Sicherheitsdefinitionen** auf eine Instanz ausgerichtet
  - **Konstruktionen** verlieren Sicherheit bei Mehrfachbenutzung
- **Beispiel:** Verschlüsselungsstandard PKCS#1
  - (Heuristisch) sicher unter zahlentheoretischer Annahme (RSA)
  - **Genauer:** Angriff $\mathcal{A}$ auf PKCS#1 $\Rightarrow$ RSA-Problemlöser $\mathcal{B}$
  - **Aber:**

$$\text{Erfolg}(\mathcal{B}) \quad \approx \quad \frac{\text{Erfolg}(\mathcal{A})}{n_{\text{PKCS}}}$$

(wobei n_{PKCS} =Anzahl PKCS-Instanzen)

- **Konsequenz:** Schlüssellängen unklar, wenn Szenario unklar

Motivation

- Gegenwärtige Kryptographie nicht bereit für große Szenarien
  - Gängige **Sicherheitsdefinitionen** auf eine Instanz ausgerichtet
  - **Konstruktionen** verlieren Sicherheit bei Mehrfachbenutzung
- **Beispiel:** Verschlüsselungsstandard PKCS#1
  - (Heuristisch) sicher unter zahlentheoretischer Annahme (RSA)
  - **Genauer:** Angriff $\mathcal{A}$ auf PKCS#1 $\Rightarrow$ RSA-Problemlöser $\mathcal{B}$
  - **Aber:**

$$\text{Erfolg}(\mathcal{B}) \quad \approx \quad \frac{\text{Erfolg}(\mathcal{A})}{n_{\text{PKCS}}}$$

(wobei n_{PKCS} =Anzahl PKCS-Instanzen)

- **Konsequenz:** Schlüssellängen unklar, wenn Szenario unklar

Motivation

- Gegenwärtige Kryptographie nicht bereit für große Szenarien
  - Gängige **Sicherheitsdefinitionen** auf eine Instanz ausgerichtet
  - **Konstruktionen** verlieren Sicherheit bei Mehrfachbenutzung
- **Beispiel:** Verschlüsselungsstandard PKCS#1
  - (Heuristisch) sicher unter zahlentheoretischer Annahme (RSA)
  - **Genauer:** Angriff $\mathcal{A}$ auf PKCS#1 $\Rightarrow$ RSA-Problemlöser $\mathcal{B}$
  - **Aber:**

$$\text{Erfolg}(\mathcal{B}) \approx \frac{\text{Erfolg}(\mathcal{A})}{n_{\text{PKCS}}}$$

(wobei n_{PKCS} =Anzahl PKCS-Instanzen)

- **Konsequenz:** Schlüssellängen unklar, wenn Szenario unklar

Motivation

- Gegenwärtige Kryptographie nicht bereit für große Szenarien
  - Gängige **Sicherheitsdefinitionen** auf eine Instanz ausgerichtet
  - **Konstruktionen** verlieren Sicherheit bei Mehrfachbenutzung
- **Beispiel:** Verschlüsselungsstandard PKCS#1
  - (Heuristisch) sicher unter zahlentheoretischer Annahme (RSA)
  - **Genauer:** Angriff $\mathcal{A}$ auf PKCS#1 $\Rightarrow$ RSA-Problemlöser $\mathcal{B}$
  - **Aber:**

$$\text{Erfolg}(\mathcal{B}) \quad \approx \quad \frac{\text{Erfolg}(\mathcal{A})}{n_{\text{PKCS}}}$$

    (wobei n_{PKCS} =Anzahl PKCS-Instanzen)
- **Konsequenz:** Schlüssellängen unklar, wenn Szenario unklar

Motivation

- Gegenwärtige Kryptographie nicht bereit für große Szenarien
  - Gängige **Sicherheitsdefinitionen** auf eine Instanz ausgerichtet
  - **Konstruktionen** verlieren Sicherheit bei Mehrfachbenutzung
- **Beispiel:** Verschlüsselungsstandard PKCS#1
  - (Heuristisch) sicher unter zahlentheoretischer Annahme (RSA)
  - **Genauer:** Angriff $\mathcal{A}$ auf PKCS#1 $\Rightarrow$ RSA-Problemlöser $\mathcal{B}$
  - **Aber:**

$$\text{Erfolg}(\mathcal{B}) \quad \approx \quad \frac{\text{Erfolg}(\mathcal{A})}{n_{\text{PKCS}}}$$

(wobei n_{PKCS} =Anzahl PKCS-Instanzen)

- **Konsequenz:** Schlüssellängen unklar, wenn Szenario unklar

Motivation

- Gegenwärtige Kryptographie nicht bereit für große Szenarien
  - Gängige **Sicherheitsdefinitionen** auf eine Instanz ausgerichtet
  - **Konstruktionen** verlieren Sicherheit bei Mehrfachbenutzung
- **Beispiel:** Verschlüsselungsstandard PKCS#1
  - (Heuristisch) sicher unter zahlentheoretischer Annahme (RSA)
  - **Genauer:** Angriff $\mathcal{A}$ auf PKCS#1 $\Rightarrow$ RSA-Problemlöser $\mathcal{B}$
  - **Aber:**

$$\text{Erfolg}(\mathcal{B}) \quad \approx \quad \frac{\text{Erfolg}(\mathcal{A})}{n_{\text{PKCS}}}$$

(wobei n_{PKCS} =Anzahl PKCS-Instanzen)

- **Konsequenz:** Schlüssellängen unklar, wenn Szenario unklar

Motivation

- Gegenwärtige Kryptographie nicht bereit für große Szenarien
  - Gängige **Sicherheitsdefinitionen** auf eine Instanz ausgerichtet
  - **Konstruktionen** verlieren Sicherheit bei Mehrfachbenutzung
- **Beispiel:** Verschlüsselungsstandard PKCS#1
  - (Heuristisch) sicher unter zahlentheoretischer Annahme (RSA)
  - **Genauer:** Angriff $\mathcal{A}$ auf PKCS#1 $\Rightarrow$ RSA-Problemlöser $\mathcal{B}$
  - **Aber:**

$$\text{Erfolg}(\mathcal{B}) \quad \approx \quad \frac{\text{Erfolg}(\mathcal{A})}{n_{\text{PKCS}}}$$

  (wobei n_{PKCS} =Anzahl PKCS-Instanzen)
- **Konsequenz:** Schlüssellängen unklar, wenn Szenario unklar

Motivation

- Gegenwärtige Kryptographie nicht bereit für große Szenarien
  - Gängige **Sicherheitsdefinitionen** auf eine Instanz ausgerichtet
  - **Konstruktionen** verlieren Sicherheit bei Mehrfachbenutzung
- **Beispiel:** Verschlüsselungsstandard PKCS#1
  - (Heuristisch) sicher unter zahlentheoretischer Annahme (RSA)
  - **Genauer:** Angriff $\mathcal{A}$ auf PKCS#1 $\Rightarrow$ RSA-Problemlöser $\mathcal{B}$
  - **Aber:**

$$\text{Erfolg}(\mathcal{B}) \quad \approx \quad \frac{\text{Erfolg}(\mathcal{A})}{n_{\text{PKCS}}}$$

  (wobei n_{PKCS} =Anzahl PKCS-Instanzen)
- **Konsequenz:** Schlüssellängen unklar, wenn Szenario unklar

Zielsetzung

- **Ziel:** Definitionen und Konstruktionen für große Szenarien
- **Teilziel 1:** tighte Sicherheitsbeweise
  - Sicherheitsgarantien unabhängig von Anzahl Instanzen
  - Schlüssellängen unabhängig von Anwendung/Szenario
- **Teilziel 2:** rekonfigurierbare Sicherheit
  - Sicherheitsgarantien bei Bedarf im Betrieb erhöhbar
  - Kein aufwändiger Austausch von Infrastrukturen nötig
- **Teilziel 3:** asymptotisch extrem effiziente Kryptographie
- **Teilziel 4:** neue Bausteine (non-interactive key exchange)

Zielsetzung

- **Ziel:** Definitionen und Konstruktionen für große Szenarien
- **Teilziel 1:** tighte Sicherheitsbeweise
  - Sicherheitsgarantien unabhängig von Anzahl Instanzen
  - Schlüssellängen unabhängig von Anwendung/Szenario
- **Teilziel 2:** rekonfigurierbare Sicherheit
  - Sicherheitsgarantien bei Bedarf im Betrieb erhöhbar
  - Kein aufwändiger Austausch von Infrastrukturen nötig
- **Teilziel 3:** asymptotisch extrem effiziente Kryptographie
- **Teilziel 4:** neue Bausteine (non-interactive key exchange)

Zielsetzung

- **Ziel:** Definitionen und Konstruktionen für große Szenarien
- **Teilziel 1:** tighte Sicherheitsbeweise
  - Sicherheitsgarantien unabhängig von Anzahl Instanzen
  - Schlüssellängen unabhängig von Anwendung/Szenario
- **Teilziel 2:** rekonfigurierbare Sicherheit
  - Sicherheitsgarantien bei Bedarf im Betrieb erhöhbar
  - Kein aufwändiger Austausch von Infrastrukturen nötig
- **Teilziel 3:** asymptotisch extrem effiziente Kryptographie
- **Teilziel 4:** neue Bausteine (non-interactive key exchange)

Zielsetzung

- **Ziel:** Definitionen und Konstruktionen für große Szenarien
- **Teilziel 1:** tighte Sicherheitsbeweise
  - Sicherheitsgarantien unabhängig von Anzahl Instanzen
  - Schlüssellängen unabhängig von Anwendung/Szenario
- **Teilziel 2:** rekonfigurierbare Sicherheit
  - Sicherheitsgarantien bei Bedarf im Betrieb erhöhbar
  - Kein aufwändiger Austausch von Infrastrukturen nötig
- **Teilziel 3:** asymptotisch extrem effiziente Kryptographie
- **Teilziel 4:** neue Bausteine (non-interactive key exchange)

Zielsetzung

- **Ziel:** Definitionen und Konstruktionen für große Szenarien
- **Teilziel 1:** tighte Sicherheitsbeweise
  - Sicherheitsgarantien unabhängig von Anzahl Instanzen
  - Schlüssellängen unabhängig von Anwendung/Szenario
- **Teilziel 2:** rekonfigurierbare Sicherheit
  - Sicherheitsgarantien bei Bedarf im Betrieb erhöhbar
  - Kein aufwändiger Austausch von Infrastrukturen nötig
- **Teilziel 3:** asymptotisch extrem effiziente Kryptographie
- **Teilziel 4:** neue Bausteine (non-interactive key exchange)

Zielsetzung

- **Ziel:** Definitionen und Konstruktionen für große Szenarien
- **Teilziel 1:** tighte Sicherheitsbeweise
  - Sicherheitsgarantien unabhängig von Anzahl Instanzen
  - Schlüssellängen unabhängig von Anwendung/Szenario
- **Teilziel 2:** rekonfigurierbare Sicherheit
  - Sicherheitsgarantien bei Bedarf im Betrieb erhöhbar
  - Kein aufwändiger Austausch von Infrastrukturen nötig
- **Teilziel 3:** asymptotisch extrem effiziente Kryptographie
- **Teilziel 4:** neue Bausteine (non-interactive key exchange)

Zielsetzung

- **Ziel:** Definitionen und Konstruktionen für große Szenarien
- **Teilziel 1:** tighte Sicherheitsbeweise
  - Sicherheitsgarantien unabhängig von Anzahl Instanzen
  - Schlüssellängen unabhängig von Anwendung/Szenario
- **Teilziel 2:** rekonfigurierbare Sicherheit
  - Sicherheitsgarantien bei Bedarf im Betrieb erhöhbar
  - Kein aufwändiger Austausch von Infrastrukturen nötig
- **Teilziel 3:** asymptotisch extrem effiziente Kryptographie
- **Teilziel 4:** neue Bausteine (non-interactive key exchange)

Zielsetzung

- **Ziel:** Definitionen und Konstruktionen für große Szenarien
- **Teilziel 1:** tighte Sicherheitsbeweise
  - Sicherheitsgarantien unabhängig von Anzahl Instanzen
  - Schlüssellängen unabhängig von Anwendung/Szenario
- **Teilziel 2:** rekonfigurierbare Sicherheit
  - Sicherheitsgarantien bei Bedarf im Betrieb erhöhbar
  - Kein aufwändiger Austausch von Infrastrukturen nötig
- **Teilziel 3:** asymptotisch extrem effiziente Kryptographie
- **Teilziel 4:** neue Bausteine (non-interactive key exchange)

Zielsetzung

- **Ziel:** Definitionen und Konstruktionen für große Szenarien
- **Teilziel 1:** tighte Sicherheitsbeweise
  - Sicherheitsgarantien unabhängig von Anzahl Instanzen
  - Schlüssellängen unabhängig von Anwendung/Szenario
- **Teilziel 2:** rekonfigurierbare Sicherheit
  - Sicherheitsgarantien bei Bedarf im Betrieb erhöhbar
  - Kein aufwändiger Austausch von Infrastrukturen nötig
- **Teilziel 3:** asymptotisch extrem effiziente Kryptographie
- **Teilziel 4:** neue Bausteine (non-interactive key exchange)

Techniken und Zusammenarbeit

- **Techniken:**
  - Komplexitätstheorie (Reduktionen)
  - Zahlentheorie (Gitter)
- **Zusammenarbeit:**
  - Projekt „Security-Preserving Operations of Big Data“
  - Suche nach gemeinsamem Szenario

Techniken und Zusammenarbeit

- **Techniken:**
  - Komplexitätstheorie (Reduktionen)
  - Zahlentheorie (Gitter)
- **Zusammenarbeit:**
  - Projekt „Security-Preserving Operations of Big Data“
  - Suche nach gemeinsamem Szenario

Techniken und Zusammenarbeit

- **Techniken:**
  - Komplexitätstheorie (Reduktionen)
  - Zahlentheorie (Gitter)
- **Zusammenarbeit:**
  - Projekt „Security-Preserving Operations of Big Data“
  - Suche nach gemeinsamem Szenario

Techniken und Zusammenarbeit

- **Techniken:**
  - Komplexitätstheorie (Reduktionen)
  - Zahlentheorie (Gitter)
- **Zusammenarbeit:**
  - Projekt „Security-Preserving Operations of Big Data“
  - Suche nach gemeinsamem Szenario

Techniken und Zusammenarbeit

- **Techniken:**
  - Komplexitätstheorie (Reduktionen)
  - Zahlentheorie (Gitter)
- **Zusammenarbeit:**
  - Projekt „Security-Preserving Operations of Big Data“
  - Suche nach gemeinsamem Szenario

Techniken und Zusammenarbeit

- **Techniken:**
  - Komplexitätstheorie (Reduktionen)
  - Zahlentheorie (Gitter)
- **Zusammenarbeit:**
  - Projekt „Security-Preserving Operations of Big Data“
  - Suche nach gemeinsamem Szenario