UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Attributbasierte Verschlüsselung mittels Gittermethoden

Kathlén Kohn

Fakultät für Elektrotechnik, Informatik und Mathematik
Universität Paderborn

1. März 2013

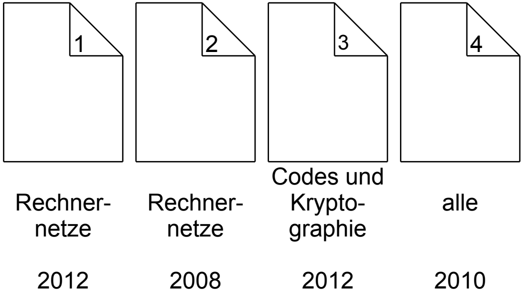
Inhaltsverzeichnis

Begriffe

Attributbasierte Verschlüsselung

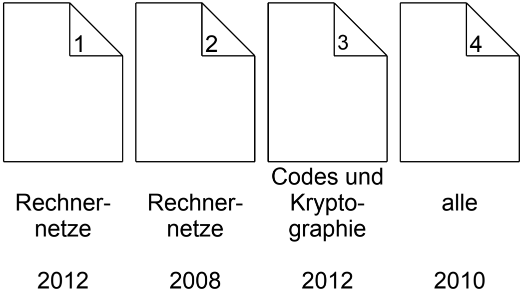
Begriffe

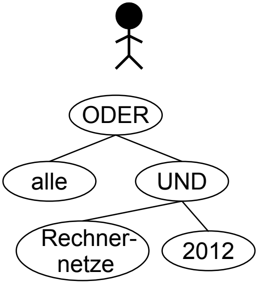
Attributbasierte Verschlüsselung



Begriffe

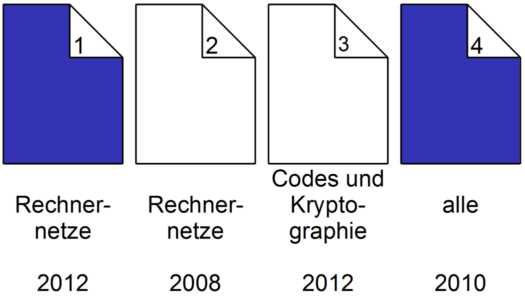
Attributbasierte Verschlüsselung

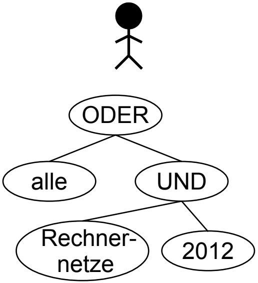




Begriffe

Attributbasierte Verschlüsselung



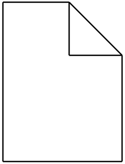


Begriffe

Fuzzy Identitätsbasierte Verschlüsselung

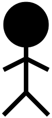
Begriffe

Fuzzy Identitätsbasierte Verschlüsselung



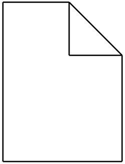
(**1**,1,0,**1**,...)

(**1**,0,0,**1**,...)



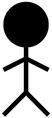
Begriffe

Fuzzy Identitätsbasierte Verschlüsselung



Gespeicherte Aufnahme:
(**1**,1,0,**1**,...)

Aktuelle Aufnahme:
(**1**,0,0,**1**,...)



Begriffe

Fuzzy Identitätsbasierte Verschlüsselung

- Nutzer:
  - hat Identität $\mathrm{id}^{(N)} \in \{0,1\}^l$
  - erhält geheimen Schlüssel zu $\mathrm{id}^{(N)}$

Begriffe

Fuzzy Identitätsbasierte Verschlüsselung

- Nutzer:
  - hat Identität $\mathrm{id}^{(N)} \in \{0,1\}^l$
  - erhält geheimen Schlüssel zu $\mathrm{id}^{(N)}$
- Datei:
  - hat Identität $\mathrm{id}^{(D)} \in \{0,1\}^l$
  - wird unter $\mathrm{id}^{(D)}$ verschlüsselt

Begriffe

Fuzzy Identitätsbasierte Verschlüsselung

- Nutzer:
  - hat Identität $\mathrm{id}^{(N)} \in \{0,1\}^l$
  - erhält geheimen Schlüssel zu $\mathrm{id}^{(N)}$
- Datei:
  - hat Identität $\mathrm{id}^{(D)} \in \{0,1\}^l$
  - wird unter $\mathrm{id}^{(D)}$ verschlüsselt
- Grenzwert $k \in \mathbb{N}, k \leq l$

Begriffe

Fuzzy Identitätsbasierte Verschlüsselung

- Nutzer:
  - hat Identität $\mathrm{id}^{(N)} \in \{0,1\}^l$
  - erhält geheimen Schlüssel zu $\mathrm{id}^{(N)}$
- Datei:
  - hat Identität $\mathrm{id}^{(D)} \in \{0,1\}^l$
  - wird unter $\mathrm{id}^{(D)}$ verschlüsselt
- Grenzwert $k \in \mathbb{N}, k \leq l$
- Nutzer kann Datei entschlüsseln

$$\Leftrightarrow \left| \left\{ j \in \{1,\ldots,l\} \;\middle|\; \mathrm{id}_j^{(N)} = \mathrm{id}_j^{(D)} = 1 \right\} \right| \geq k$$

Begriffe

k aus n Geheimnisteilung

Begriffe

k aus n Geheimnisteilung

- Geheimnis G auf n Teilnehmer aufteilen

Begriffe

k aus n Geheimnisteilung

- Geheimnis G auf n Teilnehmer aufteilen
- k Teilnehmer (oder mehr) können G rekonstruieren

Begriffe

k aus n Geheimnisteilung

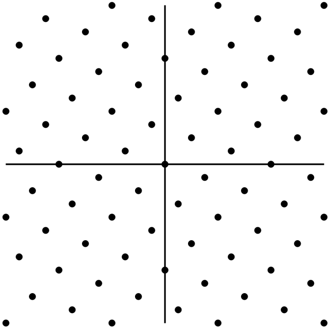
- Geheimnis G auf n Teilnehmer aufteilen
- k Teilnehmer (oder mehr) können G rekonstruieren
- Weniger als k Teilnehmer nicht

Begriffe

Verschlüsselung mittels Gittermethoden

Begriffe

Verschlüsselung mittels Gittermethoden

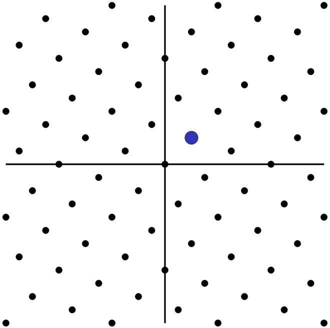


Definition

Sei $B \in \mathbb{R}^{m \times n}$ mit $\mathrm{rk}(B) = n$. Dann ist $\{Bz \mid z \in \mathbb{Z}^n\}$ ein Gitter mit Basis B.

Begriffe

Verschlüsselung mittels Gittermethoden



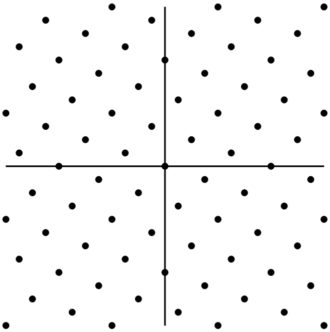
Definition

Sei $B \in \mathbb{R}^{m \times n}$ mit $\mathrm{rk}(B) = n$. Dann ist $\{Bz \mid z \in \mathbb{Z}^n\}$ ein Gitter mit Basis B.

Shortest Vector Problem: Finde kürzesten Gittervektor ungleich Null.

Begriffe

Verschlüsselung mittels Gittermethoden



Definition

Sei $B \in \mathbb{R}^{m \times n}$ mit $\mathrm{rk}(B) = n$. Dann ist $\{Bz \mid z \in \mathbb{Z}^n\}$ ein Gitter mit Basis B.

Lemma

Sei $q \in \mathbb{N}$ Primzahl, $A \in \mathbb{Z}_q^{n \times m}$. Dann ist $\Lambda(A) := \{e \in \mathbb{Z}^m \mid Ae = 0\}$ ein Gitter.

Verschlüsselungsverfahren

Verschlüsselungsverfahren

- l: Länge von Identitäten
- k: Zur Entschlüsselung notwendige Anzahl an Übereinstimmungen

Verschlüsselungsverfahren

- l: Länge von Identitäten
- k: Zur Entschlüsselung notwendige Anzahl an Übereinstimmungen

1. Setup:

Verschlüsselungsverfahren

- l: Länge von Identitäten
- k: Zur Entschlüsselung notwendige Anzahl an Übereinstimmungen

1. Setup:
    - Öffentlich: $u \in \mathbb{Z}_q^n$, $A_1, \ldots, A_l \in \mathbb{Z}_q^{n \times m}$

Verschlüsselungsverfahren

- l: Länge von Identitäten
- k: Zur Entschlüsselung notwendige Anzahl an Übereinstimmungen

1. Setup:
   - Öffentlich: $u \in \mathbb{Z}_q^n$, $A_1, \ldots, A_l \in \mathbb{Z}_q^{n \times m}$
   - Geheimer Hauptschlüssel: „kurze“ Gitterbasen zu $\Lambda(A_1), \ldots, \Lambda(A_l)$

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: u, $\Lambda(A_1), \ldots, \Lambda(A_l)$

2. Geheimer Schlüssel zu id $\in \{0, 1\}^l$:

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: u, $\Lambda(A_1), \ldots, \Lambda(A_l)$

2. Geheimer Schlüssel zu id $\in \{0,1\}^l$:
   Erstelle $e_j \in \mathbb{Z}^m$: $\text{id} = \begin{array}{cccccc} (& 1, & 0, & 0, & 1, & \ldots) \\ & \downarrow & & & \downarrow & \\ & e_1 & & & e_4 & \end{array}$

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: $u, \Lambda(A_1), \ldots, \Lambda(A_l)$

2. Geheimer Schlüssel zu id $\in \{0,1\}^l$:
   Erstelle $e_j \in \mathbb{Z}^m$: $\text{id} = \begin{array}{cccccc} (& 1, & 0, & 0, & 1, & \ldots) \\ & \downarrow & & & \downarrow & \\ & e_1 & & & e_4 & \end{array}$
   - Für alle k-elementigen Teilmengen S der e_j: $\sum_{j \in S} z_j A_j e_j = u$

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: u, $\Lambda(A_1), \ldots, \Lambda(A_l)$

2. Geheimer Schlüssel zu id $\in \{0,1\}^l$:
   Erstelle $e_j \in \mathbb{Z}^m$: $\text{id} = \begin{array}{cccccc} (& 1, & 0, & 0, & 1, & \ldots) \\ & \downarrow & & & \downarrow & \\ & e_1 & & & e_4 & \end{array}$
   - Für alle k-elementigen Teilmengen S der e_j: $\sum_{j \in S} z_j A_j e_j = u$
   - Weniger als k Vektoren e_j reichen für obige Summe nicht aus

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: u, $\Lambda(A_1), \ldots, \Lambda(A_l)$

2. Geheimer Schlüssel zu id $\in \{0,1\}^l$:
   Erstelle $e_j \in \mathbb{Z}^m$: $\text{id} = \begin{array}{cccccc} (& 1, & 0, & 0, & 1, & \ldots) \\ & \downarrow & & & \downarrow & \\ & e_1 & & & e_4 & \end{array}$
   - Für alle k-elementigen Teilmengen S der e_j: $\sum_{j \in S} z_j A_j e_j = u$
   - Weniger als k Vektoren e_j reichen für obige Summe nicht aus
   - $\|e_j\|$ nicht zu groß

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: u, $\Lambda(A_1), \ldots, \Lambda(A_l)$
2. Geheimer Schlüssel zu id: $\sum z_j A_j e_j = u$, $\|e_j\|$ klein

3. Verschlüsselung von $b \in \{0, 1\}$ unter $\mathrm{id}' \in \{0, 1\}^l$:

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: u, $\Lambda(A_1), \ldots, \Lambda(A_l)$
2. Geheimer Schlüssel zu id: $\sum z_j A_j e_j = u$, $\|e_j\|$ klein
3. Verschlüsselung von $b \in \{0,1\}$ unter $\mathrm{id}' \in \{0,1\}^l$:
   - $s \in \mathbb{Z}_q^n$ zufällig gleichverteilt
   - $c := b \left\lfloor \frac{q}{2} \right\rfloor + u^T s$

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: $u, \Lambda(A_1), \ldots, \Lambda(A_l)$
2. Geheimer Schlüssel zu id: $\sum z_j A_j e_j = u$, $\|e_j\|$ klein

3. Verschlüsselung von $b \in \{0,1\}$ unter $\mathrm{id}' \in \{0,1\}^l$:
   - $s \in \mathbb{Z}_q^n$ zufällig gleichverteilt
   - $c := b \left\lfloor \frac{q}{2} \right\rfloor + u^T s$
   - $$\begin{array}{lccccc} \mathrm{id}' = (& 1, & 1, & 0, & 1, & \ldots) \\ & \downarrow & \downarrow & & \downarrow & \\ & c_1 := A_1^T s & c_2 := A_2^T s & & c_4 := A_4^T s & \end{array}$$

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: $u, \Lambda(A_1), \ldots, \Lambda(A_l)$
2. Geheimer Schlüssel zu id: $\sum z_j A_j e_j = u$, $\|e_j\|$ klein
3. Verschlüsselung von b unter id$'$: $c = b\left\lfloor \frac{q}{2} \right\rfloor + u^T s$, $c_j = A_j^T s$

4. Entschlüsselung mit Menge S von k Übereinstimmungen:

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: u, $\Lambda(A_1), \ldots, \Lambda(A_l)$
2. Geheimer Schlüssel zu id: $\sum z_j A_j e_j = u$, $\|e_j\|$ klein
3. Verschlüsselung von b unter id$'$: $c = b\left\lfloor \frac{q}{2} \right\rfloor + u^T s$, $c_j = A_j^T s$

4. Entschlüsselung mit Menge S von k Übereinstimmungen:

$$\begin{aligned} c - \sum_{j \in S} z_j e_j^T c_j &= b\left\lfloor \frac{q}{2} \right\rfloor + u^T s - \sum_{j \in S} z_j e_j^T A_j^T s \\ &= b\left\lfloor \frac{q}{2} \right\rfloor \end{aligned}$$

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: u, $\Lambda(A_1), \ldots, \Lambda(A_l)$
2. Geheimer Schlüssel zu id: $\sum z_j A_j e_j = u$, $\|e_j\|$ klein
3. Verschlüsselung von $b \in \{0,1\}$ unter $\mathrm{id}' \in \{0,1\}^l$:
   - $s \in \mathbb{Z}_q^n$ zufällig gleichverteilt
   - $c := b \left\lfloor \frac{q}{2} \right\rfloor + u^T s$
   - $$\begin{array}{lccccc} \mathrm{id}' = (& 1, & 1, & 0, & 1, & \ldots) \\ & \downarrow & \downarrow & & \downarrow & \\ & c_1 := A_1^T s & c_2 := A_2^T s & & c_4 := A_4^T s & \end{array}$$

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: u, $\Lambda(A_1), \ldots, \Lambda(A_l)$
2. Geheimer Schlüssel zu id: $\sum z_j A_j e_j = u$, $\|e_j\|$ klein

3. Verschlüsselung von $b \in \{0, 1\}$ unter $\mathrm{id}' \in \{0, 1\}^l$:
   - $s \in \mathbb{Z}_q^n$ zufällig gleichverteilt
   - $c := b \left\lfloor \frac{q}{2} \right\rfloor + u^T s$
   - $$\begin{array}{cccccc} \mathrm{id}' = (& 1, & 1, & 0, & 1, & \ldots) \\ & \downarrow & \downarrow & & \downarrow & \\ & c_1 := A_1^T s & c_2 := A_2^T s & & c_4 := A_4^T s & \end{array}$$

Rekonstruktion von s soll schwierig sein!

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: u, $\Lambda(A_1), \ldots, \Lambda(A_l)$
2. Geheimer Schlüssel zu id: $\sum z_j A_j e_j = u$, $\|e_j\|$ klein

3. Verschlüsselung von $b \in \{0,1\}$ unter $\mathrm{id}' \in \{0,1\}^l$:
   - $s \in \mathbb{Z}_q^n$ zufällig gleichverteilt
   - $c := b \left\lfloor \frac{q}{2} \right\rfloor + u^T s + \boldsymbol{x}$
   - $\mathrm{id}' =$

$$\begin{array}{ccccc} (& 1, & 1, & 0, & 1, & \ldots) \\ & \downarrow & \downarrow & & \downarrow & \\ & c_1 := A_1^T s + \boldsymbol{x_1} & c_2 := A_2^T s + \boldsymbol{x_2} & & c_4 := A_4^T s + \boldsymbol{x_4} & \end{array}$$

Rekonstruktion von s soll schwierig sein!

Verschlüsselungsverfahren

l: Länge, k: #Übereinstimmungen

1. Setup: u, $\Lambda(A_1), \ldots, \Lambda(A_l)$
2. Geheimer Schlüssel zu id: $\sum z_j A_j e_j = u$, $\|e_j\|$ klein
3. Verschlüsselung von b unter id′: $c = b \left\lfloor \frac{q}{2} \right\rfloor + u^T s + \boldsymbol{x}$, $c_j = A_j^T s + \boldsymbol{x_j}$

4. Entschlüsselung mit Menge S von k Übereinstimmungen:

$$c - \sum_{j \in S} z_j e_j^T c_j = b \left\lfloor \frac{q}{2} \right\rfloor + u^T s + \boldsymbol{x} - \sum_{j \in S} z_j e_j^T \left(A_j^T s + \boldsymbol{x_j} \right)$$
$$= b \left\lfloor \frac{q}{2} \right\rfloor + \boldsymbol{x} - \sum_{\boldsymbol{j \in S}} \boldsymbol{z_j e_j^T x_j}$$

Learning with Errors

Learning with Errors

l: Länge, k: #Übereinstimmungen

1. Setup: u, $\Lambda(A_1), \ldots, \Lambda(A_l)$
2. Geheimer Schlüssel zu id: $\sum z_j A_j e_j = u$, $\|e_j\|$ klein
3. Verschlüsselung von $b \in \{0,1\}$ unter $\text{id}' \in \{0,1\}^l$:
   - $s \in \mathbb{Z}_q^n$ zufällig gleichverteilt
   - $c := b \left\lfloor \frac{q}{2} \right\rfloor + u^T s + \boldsymbol{x}$
   - $\text{id}' =$

$$
\begin{array}{ccccc}
(\quad 1, & 1, & 0, & 1, & \ldots) \\
\downarrow & \downarrow & & \downarrow & \\
c_1 := A_1^T s + \boldsymbol{x_1} & c_2 := A_2^T s + \boldsymbol{x_2} & & c_4 := A_4^T s + \boldsymbol{x_4} &
\end{array}
$$

Rekonstruktion von s soll schwierig sein!

Learning with Errors

l: Länge, k: #Übereinstimmungen

1. Setup: u, $\Lambda(A_1), \ldots, \Lambda(A_l)$
2. Geheimer Schlüssel zu id: $\sum z_j A_j e_j = u$, $\|e_j\|$ klein
3. Verschlüsselung von $b \in \{0,1\}$ unter $\mathrm{id}' \in \{0,1\}^l$:
   - $s \in \mathbb{Z}_q^n$ zufällig gleichverteilt
   - $c := b \left\lfloor \frac{q}{2} \right\rfloor + u^T s + \boldsymbol{x}$
   - $\mathrm{id}' =$

$$\begin{array}{ccccc} (\quad 1, & 1, & 0, & 1, & \ldots) \\ \downarrow & \downarrow & & \downarrow & \\ c_1 := A_1^T s + \boldsymbol{x_1} & c_2 := A_2^T s + \boldsymbol{x_2} & & c_4 := A_4^T s + \boldsymbol{x_4} & \end{array}$$

Rekonstruktion von s soll schwierig sein!
Sei χ Verteilung auf $\mathbb{Z}_q$ mit $x \sim \chi$, $x_j \sim \chi^m$.

Learning with Errors

Definition

Sei $s \in \mathbb{Z}_q^n$. Dann ist $\mathcal{A}_{s,\chi}$ Verteilung auf $\mathbb{Z}_q^n \times \mathbb{Z}_q$ mit Samples der Form: $(a, a^T s + x)$.

$a \sim \mathcal{U}_{\mathbb{Z}_q^n}$ $\qquad$ $x \sim \chi$

Learning with Errors

Definition

Sei $s \in \mathbb{Z}_q^n$. Dann ist $\mathcal{A}_{s,\chi}$ Verteilung auf $\mathbb{Z}_q^n \times \mathbb{Z}_q$ mit Samples

der Form: $(a, a^T s + x)$.

$a \sim \mathcal{U}_{\mathbb{Z}_q^n}$ $\qquad$ $x \sim \chi$

Definition

Algorithmus $\mathcal{B}$ löst Unterscheidungs-LWE$_{q,\chi}$, falls

$$\left| \Pr(\mathcal{B}(\mathcal{A}_{s,\chi}) = 1) - \Pr(\mathcal{B}(\mathcal{U}_{\mathbb{Z}_q^n \times \mathbb{Z}_q}) = 1) \right|$$

nicht vernachlässigbar ist mit $s \sim \mathcal{U}_{\mathbb{Z}_q^n}$.

Learning with Errors

Sicherheitsannahme: Kein Polynomialzeitalgorithmus löst Unterscheidungs-LWE$_{q,\chi}$.

Learning with Errors

Sicherheitsannahme: Kein Polynomialzeitalgorithmus löst Unterscheidungs-LWE$_{q,\chi}$.

- Nur Algorithmen mit (leicht sub-)exponentieller Laufzeit bekannt
- Wahrscheinlich keine Verbesserungen auf Quantencomputern

Learning with Errors

Sicherheitsannahme: Kein Polynomialzeitalgorithmus löst Unterscheidungs-LWE$_{q,\chi}$.

- Nur Algorithmen mit (leicht sub-)exponentieller Laufzeit bekannt
- Wahrscheinlich keine Verbesserungen auf Quantencomputern
- Entscheidungsvariante NP-vollständig

Learning with Errors

Sicherheitsannahme: Kein Polynomialzeitalgorithmus löst Unterscheidungs-LWE$_{q,\chi}$.

- Nur Algorithmen mit (leicht sub-)exponentieller Laufzeit bekannt
- Wahrscheinlich keine Verbesserungen auf Quantencomputern
- Entscheidungsvariante NP-vollständig
- Regev: Löst ein Polynomialzeitalgorithmus Unterscheidungs-LWE$_{q,\chi}$, so löst ein Quantenalgorithmus mit Laufzeit $q \cdot \mathrm{poly}(n)$ die approximative Entscheidungsvariante des Shortest Vector Problem mit Approximationsfaktor $\tilde{O}(q\sqrt{n})$ auf Gittern im $\mathbb{R}^n$.

Ausblick

Ausblick

- Erreicht: Attributbasierte Verschlüsselung mittels Gittermethoden für Zugriffsrechte ohne „NOT“

Ausblick

- Erreicht: Attributbasierte Verschlüsselung mittels Gittermethoden für Zugriffsrechte ohne „NOT“
- Offen: Attributbasierte Verschlüsselung mittels Gittermethoden für allgemeine Zugriffsrechte