Identity-Based Encryption (IBE)

Grundlagen und Forschung

Niklas Julius Müller

19. Januar 2026

Freie Universität Berlin

Überblick

Motivation

Grundidee von IBE

Vorteile und Nachteile

Attribute-Based Encryption (ABE)

Forschung

Fazit

Motivation

Erinnerung: Public-Key Kryptographie

- In klassischer Public-Key Kryptographie:
  - Jeder Benutzer besitzt ein Schlüsselpaar $(\mathsf{pk}, \mathsf{sk})$.
  - Öffentliche Schlüssel müssen verteilt und authentifiziert werden.
- Problem: **Public Key Infrastructure (PKI)**
  - Zertifikate und Certificate Authorities (CAs)
  - Sperrlisten, Ablaufdaten, Verwaltungsaufwand

Warum Identity-Based Encryption?

- Ziel: **Zertifikate überflüssig machen**
- Öffentlicher Schlüssel = Identität (z. B. E-Mail-Adresse)
- Der Sender benötigt nur die Identität des Empfängers, nicht dessen Zertifikat
- Stark vereinfachtes Schlüsselmanagement

Grundidee von IBE

Was ist Identity-Based Encryption?

Informelle Definition

Identity-Based Encryption ist ein Public-Key Verschlüsselungsverfahren, bei dem eine eindeutige Zeichenkette (z. B. `alice@example.com`) direkt als öffentlicher Schlüssel dient.

- Eine vertrauenswürdige Stelle, der **Private Key Generator (PKG)**, erzeugt private Schlüssel.
- Benutzer erhalten ihren privaten Schlüssel vom PKG nach Legitimation.

Systemkomponenten

- **PKG (Private Key Generator)**
  - Besitzt den Master-Secret-Key
  - Generiert private Schlüssel für Identitäten
- **Empfänger**
  - Identität: z. B. E-Mail-Adresse
  - Privater Schlüssel wird vom PKG bereitgestellt
- **Sender**
  - Verschlüsselt nur mithilfe der Identität des Empfängers

IBE-Algorithmen

Setup

- Input: Sicherheitsparameter
- Output: mpk, msk

Extract

- Input: msk, ID
- Output: $\mathsf{sk}_{\mathsf{ID}}$

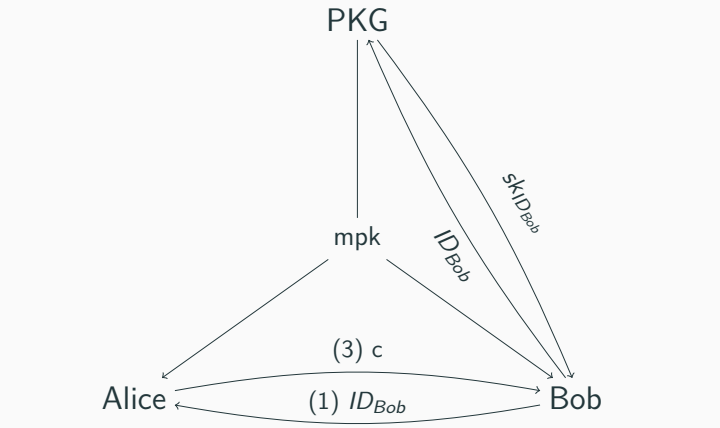
Encrypt

- Input: MPK, ID, Nachricht m
- Output: Ciphertext c

Decrypt

- Input: $\mathsf{sk}_{\mathsf{ID}}$, c
- Output: Klartext m

Ablauf eines Nachrichtenaustauschs



Vorteile und Nachteile

Vorteile von IBE

- Keine Zertifikate notwendig
- Öffentliche Schlüssel sind leicht auffindbar
- Gut geeignet für:
  - E-Mail-Verschlüsselung
  - Dynamische oder große Benutzergruppen
  - Mobile oder IoT-Geräte

Nachteile und Herausforderungen

- **Schlüsselhinterlegungsproblem**
  - PKG kennt alle privaten Schlüssel
  - Hohe zentrale Vertrauensanforderung
- **PKG-Kompromittierung**
  - Kompromittierung = vollständiger Systembruch
- **Skalierbarkeit**
  - Benutzer müssen den PKG kontaktieren

Attribute-Based Encryption (ABE)

Attribute-Based Encryption (ABE)

- Erweiterung der Identity-Based Encryption (IBE)
- Schlüssel und Ciphertexte hängen von **Attributen** ab:
  - Eigenschaften eines Benutzers (z. B. „Student“, „Mitarbeiter“, „Level 3“)
  - Kontext (z. B. „Abteilung: IT“, „Rolle: Admin“)
- Zugriff wird durch eine **Zugriffsstruktur / Policy** definiert
  - ABE ermöglicht feingranulare Zugriffskontrolle.
  - Beispiel: Nur Benutzer mit Attributen „Mitarbeiter“ AND „IT“ dürfen lesen

Forschung

Survey - Stand der Forschung[1]

- **Forschungsfragen:**
  - Gibt es postquantensichere IBE?
  - Auf welchen kryptographischen Annahmen beruhen sie?
- Identifizierte Gebiete:
  - Gitter
  - Codes
  - Multivariate Polynomsysteme
  - Isogenien

[1] Identity-Based Encryption in the Post-Quantum Era, im Review Prozess

Survey - Ergebnisse

- Gitter
  - Quantensichere Schemes sowohl im ROM als auch im Standard Model
- Codes
  - Die Sicherheitsannahme[2] wurde gebrochen.[3]
- Multivariate Polynomsysteme
  - Sicherheitsbeweis nicht vorhanden.
- Isogenien
  - Annahme falsch (Survey)
  - Gebrochen (dazu später mehr)

[2] Das LRPC+ Problem ist schwer bzw. RankPKE ist sicher

[3] Debris-Alazard, Tillich (2018) Two Attacks on Rank Metric Code-Based Schemes: RankSign and an IBE Scheme

Survey - Ergebnistabelle

	multivariate	codes	isogenies	lattices
hash function	no	yes	no	yes/no
bit encryption	multi	multi	multi	single/multi
security proof	no	quantum-broken	quantum-broken	yes

IBE basierend auf Isogenous Pairing Groups

- von Takeshi Koshiba and Katsuyuki Takashima[4].
- Idee: Pre-Challenge quantensicher.
  - Quantencomputer stehen nur begrenzt zur Verfügung. Einzelne Nachrichten müssen nicht quantensicher sein sondern nur die geheimen Schlüssel.

[4] Koshiba, Katsuyuki Takashima (2016) Pairing Cryptography Meets Isogeny: A New Framework of Isogenous Pairing Groups.

Post-Quantum Security[5]

- IBE basierend auf Isogenous Pairing Groups
- Auch Generation der geheimen Schlüssel der Nutzer sk_{ID} lässt sich auf das Elliptic Curve Discrete Logairthm Problem reduzieren.
- Ist somit vollständig nicht quantensicher.

[5] A Note on the Post-Quantum Security of Identity-Based Encryption on Isogenous Pairing Groups, im Reviewprozess

Fazit

Zusammenfassung

- IBE nutzt Identitäten statt einer PKI zur Verschlüsselung
- Trusted Entity ist notwendig
- Anwendungen in E-Mail, IoT und Organisationen
- Quantensichere Gitter IBEs existieren
- Weitere Schemes befinden sich aktuell in der Entwicklung

Offene Fragen

- Können quantensichere IBEs abseits von Gitter-Kryptographie gefunden werden?
  - Welche Basis-Schemata kommen in Frage?
  - Sind die Basis-Schemata quantensicher?
  - Kann die Sicherheit im Standard Model gezeigt werden?
- Gibt es weitere Angriffe auf Gitter-Verfahren?

Vielen Dank!

Quellen

- Boneh, Franklin (2001) Identity-Based Encryption from the Weil Pairing https://doi.org/10.1007/3-540-44647-8_13
- Gentry, Peikert, Vaikuntanathan (2008) Trapdoors for Hard Lattices and New Cryptographic Constructions https://doi.org/10.1145/1374376.1374407
- Koshiba, Takashima (2016) Pairing Cryptography Meets Isogeny: A New Framework of Isogenous Pairing Groups https://ia.cr/2016/1138
- Debris-Alazard, Tillich (2018) Two Attacks on Rank Metric Code-Based Schemes: RankSign and an IBE Schemedoi:10.1007/978-3-030-03326-2_3
- Andersch, Pilaszewicz, Margraf (2025) A Note on the Post-Quantum Security of Identity-Based Encryption on Isogenous Pairing Groups https://ia.cr/2025/1439 (preprint)
- Pilaszewicz, Müller, Andersch, Margraf (2025) Identity-Based Encryption in the Post-Quantum Era (im Reviewporzess)