実験説明書

2025 年 3 月 10 日

1．実験目的

本実験の目的は、従来暗号（例：RSA、AES）と比較して、より高い機能性や拡張性を持つと総称される**高機能暗号（Advanced Cryptography）**を利用するソフトウェアの安全な開発手法を検証することにあります。具体的には、以下の点を明らかにします。

ソフトウェア開発者による暗号ライブラリ・API の誤用の実態：

従来暗号であっても誤用が発生している事例があるが、より複雑な高機能暗号では誤用の可能性がさらに高いと予想される。

数学的複雑性および関与する当事者の増加：

高機能暗号は従来暗号と比較して、数学的な背景やプロトコルの複雑性が増すため、開発者が正しく実装することが難しくなる可能性がある。

誤用発生の比較と抑制手法の検討：

従来暗号と比較して、どのような点で誤用が生じやすいのか。

誤用を抑えるためのアプローチとして、従来暗号の既存研究の手法が有効か、もしくは高機能暗号に特有な対策が必要かを評価する。

2. 実験内容

実験では、**属性ベース暗号（ABE, Attribute Based Encryption）**に焦点をあて、オープンソースライブラリ「OpenABE」を用いたソフトウェア開発を実施していただきます。以下の条件で作業を進めてください。

対象ライブラリ:

OpenABE（ABE のオープンソースライブラリ）

使用言語:

C++

ソフトウェアの形式:

コンソールで動作するアプリケーション（コンソールアプリ／CUI）

提供されるリソース:

スタブコード: 事前に関数名、引数のデータ型、出力が定められた状態のコード（関数内部は空で、コメントにより実装すべき動作が示される）

完成済みコード:一部のコードはスタブではなく完成済みコードとして提供されます。

ドキュメント: ABE の概要説明、OpenABE の概要説明（OpenABE デザイン・ドキュメント）および機能説明（OpenABE ライブラリ C++ API ガイド）、OpenABE を用いたサンプルコード

※ドキュメントはすべて読む必要はございません。タスク実施にあたり必要と思われるドキュメントを都度ご参照ください。

開発環境:

VSCode を使用し、Microsoft Live Share によりリモートの VSCode サーバに接続。ブラウザ上で VSCode を開き作業を行います。

動作確認:

用意されたテスト関数により、作成したコードの動作確認が可能です。

3. 作成するコード（ソフトウェア）の概要

実験では、ABE の各機能（セットアップ、鍵生成、暗号化、復号）に対応する 4 種類のソースコードを作成していただきます。以下の仕様に沿って実装を行ってください。

仕様:

各ソースコードにおいて、関数名、引数とそのデータ型、出力は事前に定められています。

提供されたスタブコードは、関数内部が空の状態であり、コメントにより各関数で実装すべき動作が記載されています。

OpenABE が利用可能な ABE は CP-ABE と KP-ABE の 2 種類がありますが、今回は CP-ABE の実装を行います。

CP-ABE の実装において、以下のコードを完成させます

- セットアップ（CPABESetup.cpp）<スタブ>
- 鍵生成（CPABEKeyGen.cpp）<スタブ>
- 暗号化
  - 暗号化 1（ポリシ 1 用）（CPABEEncrypt1.cpp）<スタブ>
  - 暗号化 2（ポリシ 2 用）（CPABEEncrypt2.cpp）<完成済み>
  - 暗号化 3（ポリシ 3 用）（CPABEEncrypt3.cpp）<スタブ>
- 復号
  - 復号 1（Alice 用）（CPABEDecryptAlice.cpp）<スタブ>
  - 復号 1（Bob 用）（CPABEDecryptBob.cpp）<完成済み>
  - 復号 1（Carol 用）（CPABEDecryptCarol.cpp）<完成済み>
  - 復号 1（Dave 用）（CPABEDecryptDave.cpp）<スタブ>

目的:

スタブコードに基づいた正確な実装を通して、ABE を用いた暗号処理の実現と、開発者が遭遇する可能性のある誤用の傾向を評価する。

4. 作成の制限時間

計 6 個のプログラムを作成していただきます。1 つあたり 10 分の開発時間を上限とします。

5. 作成後のアンケートおよびインタビュー

コード作成が完了した後、参加者には以下の手順に従っていただきます。

アンケート:

作成したコードに関するアンケートにご回答いただき、実装上の困難点や使用したドキュメントの有用性等についてフィードバックを求めます。

インタビュー:

アンケートの内容を踏まえ、実験担当者によるインタビューを実施します。インタビューは、実装体験や改善点の確認を目的としています。

実験終了:

インタビューの終了をもって、ユーザ実験は正式に終了となります。