令和 2 年度 東邦大学理学部情報科学科 卒業研究

Android アプリケーションにおけるサードパーティー製 API での暗号技術利用動向の調査

学籍番号　5517097

山口千尋

金岡研究室

目 次

1　はじめに

近年開発者向けユーザブルセキュリティ、ユーザブルプライバシーの研究分野においてソフトウェア開発者の暗号技術の利用に関する研究が活発になっている。これまでの研究では、そういった暗号技術の利用が適切にされておらず脆弱性を生み出しているソフトウェアが多数存在することが判明している。
しかしこれらの研究は SSL/TLS や DES、AES など特定の暗号技術、ソフトウェア開発者の開発時の誤使用など特定の状況に限った調査だけであり、実際にどの程度のソフトウェアでどのように暗号技術が利用されているのかなどの暗号技術全般の網羅的な調査は行われていなかった。Android アプリケーションにおいても同様に、SSL/TLS などの暗号技術の利用がされているケースが多くあると考えられている。

そこで本研究ではソフトウェアの暗号技術の利用状況の網羅的な調査の一環として、Apktool や Baksmali といったツールによる静的解析が容易であること、世界のモバイル端末における OS のシェア率が高いこと [1] から Java で開発された Android アプリケーションを調査対象とする。

Android アプリケーションを静的解析し、暗号で用いられるメソッド名の抽出、API の利用傾向分析を行う。

Android アプリケーションの現状はどのような暗号技術が利用され、どの程度暗号技術が利用されているのか、その時のアルゴリズムはどのようなものが利用されているのかまた暗号技術の利用には何らかの傾向があるのかなどを明らかにすることを目的とする。

調査には Android アプリケーションのサードパーティ配布ストアの 1 つである AndroZoo より取得した 307,587 個の Android アプリケーションと、Google 社のサードパーティ製 API である Tink から抽出した暗号・セキュリティに関するメソッド 705 個のリストを使用する。

調査の結果、調査対象の Android アプリケーション群における暗号・セキュリティに関するメソッドの利用数が判明した。

本稿の構成は以下の通りである。始めに第 2 章で、本研究に関連する技術などについての解説を行い、次の第 3 章では関連研究の紹介を行う。第 4 章では本研究を始めるにあたっての前段階の準備と調査方法や環境についての説明をし、第 6 章では結果と考察を行う。第 7 章で残課題について説明し、第 8 章でまとめる。

2　前提知識

本研究における前提知識を解説する。

2.1　Android

Android とは、Googel 社が 2007 年に開発したスマートフォンやタブレット端末など携帯情報機器向けの Operating System、あるいは Android OS が搭載された端末を指す。主にスマートフォンの OS として広く普及しており、世界的に Apple 社の携帯機器向け iOS と市場を二分している [**?**]。

2.2　Operating System

Operating System(以後 OS) とは、ソフトウェアの種類の 1 つで、機器の基本的な管理や制御のための機能や、多くのソフトウェアが共通して利用する基本的な機能などを実装したシステム全体を管理するソフトウェアのことである。

2.3　Android アプリケーション

Android アプリケーションとは、Android にインストール可能なアプリケーションである。主に、Java や Kotlin などのプログラミング言語で作成されている。Java プログラムをコンパイルして機械語に変換し、画像などのリソースと合わせてパッケージにすることでインストール可能である。

2.4　APK

APK とは、Android Application Package の略であり、Android 向けのを Android 端末にインストールできる形式にパッケージにしたもの、もしくはそのファイルのことである。入手方法は APK ストアからダウンロードする方法や、単体で公開されている APK ファイルをダウンロードする方法等が存在する。一般的に APK は“.apk”拡張子を持つ。ただし、.apk ファイル自体は zip 形式で圧縮されており、その中にはアプリケーションの動作に必要なさまざまなファイルが納められている。.apk ファイルに対して zip ファイルと同様の解凍処理を行い、得られるファイルのうち本研究に関連する項目を解説する。

- AndroidManifest.xml
  - Android アプリケーションの必要要件や、最初に起動されるアクティビティの記述がされている
  - zip の解凍処理により得られる AndroifManifest.xml はバイナリファイルの状態であるため、テキストエディタ等で内容を閲覧するためにはデコード処理が必要である
- classes.dex
  - Android アプリケーションのソースファイルを変換して Android で実行可能なようにまとめたファイルである

– 1つの dex ファイルに含められるメソッドの数は 65,536 が上限であり、それ以上の数のメソッドが 1 つの Android アプリケーションに含まれる場合は、classes2.dex、classes3.dex …と複数ファイルに分割される

2.5 バイナリファイル

バイナリファイルとは、コンピュータプログラムによって読み書きや処理を行うことを前提に、文字コードの規約を用いずに任意のビット列によって構成されるデータを格納するものである。バイナリファイルはその形式に対応したソフトウェア以外で内容を知ることは不可能である。ただし、バイナリエディタによってどのようなバイト列が並んでいるかを見ることが可能である。

2.6 APK ストア

APK ストアとは、Android アプリケーション開発者の作成した Android アプリケーションの配信を代行するサービス、およびそれを行っている Web サイトのことである。Android の公式 APK ストアは、Android の公式 APK ストアである GooglePlay[2]1 つのみであり、非公式の APK ストアは数多く存在する。

2.7 Android Developers

Android Developers とは、Android アプリケーション開発者向けの Android 公式 Web サイトのことである [3]。Android の詳細やドキュメントが提供されている。公式ドキュメントといった場合 Android Developers を指す。

2.8 smali ファイル

smali ファイルとは、Android の Dalvik 仮想マシンで使用される開発者ファイルである。通常、Android アプリケーションに含まれている実行可能ファイルである。DEX(Dalvik Executable)（Dalvik 実行可能）ファイル（.apk ファイル）を逆コンパイルすることによって作成される。smali ファイルの取得には、Apktool[4] を用いる方法と、Baksmali[5] を用いる方法がある。

2.9 中間言語

中間言語とは、計算機が実行するコードを人間が理解できる形式で表現するための言語である。以下に本研究に関連する Dalvik バイトコードについての詳細な説明を述べる。

2.9.1 Dalvik バイトコード

Dalvik バイトコードとは、Android における中間言語である。Apktool 等を用いて APK より取得できる smali ファイルは、Dalvik バイトコードで記述されている。以下のソースコード 1、ソースコード 2 に、Dalvik バイトコードの例と対応するソースコードを示す。

Listing 1: Dalvik バイトコードの例

```
# virtual methods
.method public add(II)I
    .locals 2
    .param p1, "a"    # I
    .param p2, "b"    # I

    .prologue
    .line 3
    add-int v0, p1, p2

    .line 4
    .local v0, "c":I
    sget-object v1, Ljava/lang/System;->out:Ljava/io/PrintStream;

    invoke-virtual {v1, v0}, Ljava/io/PrintStream;->print(I)V

    .line 5
    return v0
.end method
```

Listing 2: 対応するソースコード

```
public int add(int a, int b) {
    int c = a + b;
    System.out.print(c);
    return c;
}
```

2.10 CUI

CUI とは、Character User Interface の略であり、コンピュータやソフトウェアが利用者に情報を提示したり操作を受け付けたりする方法の 1 つで、すべてのやり取りを文字によって行う方式のことである。

2.11 Linux

Linux とは、Linux カーネルを利用している UNIX 系の OS である。主にネットワーク上で他のコンピュータに機能やサービスを提供するサーバコンピュータ用として利用されるほか、スマートフォンなどの携帯端末から一般的なパソコン、家庭用ゲーム機やデジタル家電、スーパーコンピュータまで、様々な種類や用途のコンピュータ製品に組み込まれ広く普及している。

2.12 Linux カーネル

Linux カーネルとは、OS に必要な基本機能を集めた核となるソフトウェアのことである。

2.13 Linux ディストリービューション

Linux ディストリービューションとは、Linux カーネルに加えて OS として機能するよう必要なプログラム群を合わせた配布パッケージを指す。カーネルを利用者がコンピュータに導入して操作可能な状態にするために作成されている。Linux ディストリビューションは自由に開発・配布できるため、個人や数人のグループから企業、大規模オープンソースプロジェクトまで様々な開発主体が様々な機種・用途向けのものを提供している。その中の 1 つに、パソコン向けやサーバ向けとして Ubuntu がある。Ubuntu は、シェルスクリプトや smali ファイル解析に用いる環境が整っていることから本研究では Ubuntu を利用した。

2.14 シェル

シェルとは、オペレーティングシステムと対話するためのインターフェイスであり、コマンドなどを制御する環境のことである。シェルがあることでコマンドを受付、OS との対話が可能である。CUI 環境においてシェルは最も身近なインターフェイスである。

2.15 UNIX コマンド

UNIX コマンドとは、Linux OS 等の UNIX マシンにおいて CUI 上からコンピュータを操作するために使用するコマンドを指す。ファイルのコピーを行う cp、ファイルの内容を表示する cat、ディレクトリの内容を表示する ls などが存在する。

2.16 シェルスプリクト

シェルスプリクトとは、OS を操作するためのシェル上で実行できる簡易なプログラム言語（スプリクト言語）のことを言う。また、スプリクト言語によって書かれた、複数の OS コマンドや制御文などを組み合わせたプログラムを指す。sh コマンドの引数としてシェルスクリプトのファイルを与えて実行すると、ファイルに記述された UNIX コマンドが上から順に実行される。以下のシェルスクリプトを実行すると、a.txt が b.txt にコピーされ、a.txt の末尾に “ hoge ” の文字列が追加される。

Listing 3: シェルスクリプトの例

```
cp a.txt b.txt
echo "hoge" > a.txt
```

2.17 正規表現

正規表現とは，ある文字列の規則を表現する方法である。正規表現ではメタ文字と呼ばれる特別な意味を持つ文字や記号が存在する。基本的なメタ文字を表 1 に示す。ある文字列の中から通常の文字とメタ文字によって作られた特定の規則に当てはまる文字列を検索するときに利用される。正規表現の例を表 2 に示す。

表 1: 正規表現における基本的なメタ文字の一覧

.	任意の 1 文字
∗	直前のパターンの 0 回以上繰り返し (最長一致)
+	直前のパターンの 1 回以上繰り返し (最長一致)
?	直前のパターンの 0〜1 回繰り返し (最長一致)

表 2: 正規表現の例

正規表現の例	正規表現の例の意味	マッチする例
.	任意の 1 文字	a
and∗roid	an と d の 0 回以上の繰り返しと roid からなる文字列	anroid
and+roid	an と d の 1 回以上の繰り返しと roid からなる文字列	andddddroid
and?roid	an と d の 0 回〜1 回の繰り返しと roid からなる文字列	android

2.18 暗号技術

2.18.1 MD5

MD5 とは、Message Digest algorithm 5 の略であり、ハッシュ値を計算するためのハッシュ関数の 1 つである。RSA 暗号の開発者の 1 人、ロン・リベスト氏らによって開発された。IPsec や、POP before SMTP など、さまざまなセキュリティプロトコルで使われている一方、最近になって脆弱性も指摘されている。ハッシュ関数により生成された値は「ハッシュ値」と呼ばれる。MD5 のハッシュ値は、128bit である。

2.18.2 SHA-1

SHA-1 とは、アメリカ国家安全保障局が考案し、1995 年から米国政府の標準として使用されているハッシュ関数である。任意のデータから 160bit のハッシュ値を生成する。2017 年、Google が SHA-1 でハッシュ値が衝突する事例 [6] を発見したため、より安全なハッシュ関数を使用することが推奨されている。

2.18.3 SHA-2

SHA-2 とは、SHA-1 を改良したハッシュ関数である。このハッシュ関数は、バリエーション豊富であり以下を総称して SHA-2 と呼ばれている。

- SHA-224（ハッシュ値：224bit）
- SHA-256（ハッシュ値：256bit）
- SHA-384（ハッシュ値：384bit）
- SHA-512（ハッシュ値：512bit）
- SHA-512/224（ハッシュ値：224bit）

- SHA-512/256（ハッシュ値：256bit）

基本となるアルゴリズムは、SHA-256 と SHA-512 である。SHA-224 は SHA-256 で出力されたハッシュ値を 224bit に切り詰めたものであり、SHA-384 は SHA-512 で出力されたハッシュ値を 384bit に切り詰めたものである。SHA-512/224 と SHA-512/256 についても SHA-512 で出力されたハッシュ値を 224bit、256bit に切り詰めたものである。大きな違いとしては、SHA-256 は 32bitCPU、SHA-512 は 64bitCPU に最適化されている点がある。ハッシュ長が長い方がセキュリティ的な強度が高いが、負荷が高くなる。ただし、現状 SHA-256 でも必要十分な強度となっているため、SHA-256 が利用されている。

2.19 API

API とは、Application Programming Interface の略であり、あるコンピュータプログラム（ソフトウェア）の機能や管理するデータなどを、外部の他のプログラムから呼び出して利用するための手順やデータ形式などを定めた規約である。
APK に使用されている API は大きく分けて 3 種類存在する。詳細は、4.1 で説明する。

2.20 API ドキュメント

API ドキュメントとは、API による開発方法やクラス内のメソッドの使用方法を解説した説明書である。API リファレンス [7] とも呼ばれる。

3　関連研究

本研究における関連研究を紹介する。

3.1　河合らの調査

河合は、Android アプリケーションを調査対象とし、Android アプリケーションの暗号技術利用に関する現状を明らかにするために、401,971 個の APK を展開し得られた smali ファイルと、4,324 個の Android Developers の API リファレンスに記載されている API より取得した暗号・セキュリティに関するクラスが持つメソッドのリストを使用し、暗号で用いられるメソッド名や特徴のある用語によるフィルタリングアルゴリズムが指定可能な代表的箇所の抽出や API の利用傾向分析の調査を行った。
本研究と関連高い調査結果を抜粋し下記に示す。

- アルゴリズムが指定可能であるメソッドにおける、指定されたアルゴリズムの分析

  調査対象の APK 群に最も利用された数が多かったメソッドは android.net.Uri.parse(java.lang.String) の 248,145 個であり、次が java.net.URL.URL(java.lang.String) の 120,601 個であった。
  調査対象の APK 群に利用された数が多かったメソッドの上位は java.net や android.net といったネットワークに関わるものであり、調査対象の APK 群のうち 61.73%の APK が android.net.Uri.parse(java.lang.String) を使用しており、何かしらの通信を行っていると河合は推測した。

  各 API における調査対象の APK 群の中でその API を少なくとも 1 回は利用した回数とその API が少なくとも 1 回は利用されている確率の上位 10 件を表 3 に示す。

表 3: 各 API における調査対象の APK 群の中でその API を少なくとも 1 回は利用した回数とその API が少なくとも 1 回は利用されている確率の上位 10 件 (河合による調査結果)

メソッド名	APK 数 (個)	メソッド利用確率 P(A)(%)
android.net.Uri.parse(java.lang.String)	248,145	61.73
java.net.URL.URL(java.lang.String)	120,601	30.00
java.net.URL.openConnection()	104,936	26.11
android.net.ConnectivityManager .getActiveNetworkInfo()	83,050	20.66
android.net.Uri.fromFile(java.io.File)	82,428	20.51
java.net.HttpURLConnection .getResponseCode()	63,770	15.86
android.net.NetworkInfo.isConnected()	61,452	15.29
android.net.Uri.toString()	58,250	14.49
java.net.HttpURLConnection.disconnect()	53,782	13.38
java.net.HttpURLConnection .setRequestMethod(java.lang.String)	52,515	13.06

- 利用される API の傾向の分析

  暗号・セキュリティに関するメソッドとして、java.security.MessageDigest.digest() の 43,418 個が最も利用されており、次に java.security.MessageDigest.getInstance(java.lang.String) の 37,405 個であった。
  java.security.MessageDigest クラスは主に SHA-1 や SHA-256 といったアルゴリズムを使用したハッシュ値を提供するものである。河合の調査結果より、調査対象の APK 群のうち 10.80% がハッシュ値を利用していることが河合により判明した。
  また、javax.crypto.spec.SecretKeySpec.SecretKeySpec(byte[],java.lang.String) 表 4 でメッセージダイジェストに関するクラスの次に利用数が多い。javax.crypto.spec.SecretKeySpec クラスは秘密鍵に関する機能を提供するクラスである。調査対象の APK 群において最も利用されている暗号化方式は公開鍵暗号であることが考えられる使用しており、何かしらの通信を行っていると河合は推測した。

  android.net.Uri.parse(java.lang.String) を暗号・セキュリティに関する各 API における調査対象の APK 群の中でその API を少なくとも 1 回は利用した回数とその API が少なくとも 1 回は利用されている確率の上位 10 件を表 4 に示す。

表 4: 暗号・セキュリティに関する各 API における調査対象の APK 群の中でその API を少なくとも 1 回は利用した回数とその API が少なくとも 1 回は利用されている確率の上位 10 件 (河合による調査結果)

メソッド名	APK 数 (個)	メソッド利用確率 P(A)(%)
java.security.MessageDigest.digest()	43,418	10.80
java.security.MessageDigest .getInstance(java.lang.String)	37,405	9.31
java.security.MessageDigest.reset()	28,357	7.05
java.security.MessageDigest.update(byte[],int,int)	20,004	4.98
javax.crypto.spec.SecretKeySpec .SecretKeySpec(byte[],java.lang.String)	15,829	3.94
java.security.KeyFactory .generatePublic(java.security.spec.KeySpec)	15,009	3.73
java.security.spec.X509EncodedKeySpec .X509EncodedKeySpec(byte[])	14,662	3.65
java.security.SecureRandom.SecureRandom()	13,759	3.42
java.security.MessageDigest.digest(byte[])	13,414	3.34
javax.crypto.Cipher.doFinal(byte[])	13,009	3.24

河合による先行研究では上記のような結果が得られたが、 暗号利用動向の更なる調査、分析のために Android Developers の API リファレンスに記載されている API 以外の API の調査も必要であると河合は考察した。

4　調査対象と手法

4.1　Android API の分類

APK に使われている API は大きく分けて 3 種類存在する。

4.1.1　公式 API

Android の開発者向け公式 Web サイトである Android Developers の API リファレンスに記載されている API のことを本研究では公式 API と呼ぶこととする。Android では、ソフトウェア開発のために必要なプログラムやライブラリを Google 社が Android SDK として提供してる。SDK で提供されるライブラリは Android 開発者向けサイト Android Developers に API リファレンスとして記載されてる。

4.1.2　サードパーティー製 API

サードパーティー製 API とは、サードパーティが提供する API のことである。サードパーティとは、特定のハードウェア、OS、ソフトウェア、あるいはサービスなどを対象として、それに対応する製品を販売、提供している組織や企業のことを指す。

4.1.3　独自実装等の API

API 開発者が既存の API を利用せずに独自に実装した API や、先述 2 つに含まれないものを独自実装等の API と本論文では呼ぶこととする。

4.2　API の分析

河合による先行研究で公式 API が調査対象とされていたので、ここではサードパーティ製 API と独自実装等の API の分析を行う。
独自実装等の API はドキュメントが公開されている可能性が低いため API のリスト化が困難である。これは、RSA や ECC、Crypto といった暗号、セキュリティに関するキーワードを API のリストの代わりとし検索する必要があるため APK の網羅的調査を行う上で困難である。
比較して、サードパーティー製 API ではドキュメントが公開されているものもあるのでリスト化の困難性が少ない。サードパーティ製の API の分析ではまず API のリスト化を行う必要があるが、サードパーティー製 API は公式 API とは違いドキュメントが作成されていないものがある。存在しない場合はサードパーティ製の API のソースコードを解析し、API のドキュメントを作成してから API のリストの作成を行う。
そこで、本研究では特にサードパーティ製 API を分析対象とし、独自実装等の API は今後の課題とする。

表 5: Tink のドキュメントページより取得した暗号・セキュリティに関するクラスが持つメソッドのリストの一部抜粋

クラス名	メソッド名 (引数)
AesEaxKeyManager	validateKey()
AndroidKeysetManager	getKeysetHandle()
AndroidKeystoreAesGcm	encrypt

4.3 サードパーティ製 API の分析

4.3.1 サードパーティ製 API の例

- Tink[8]

  Tink は、Google の暗号技術者とセキュリティエンジニアのグループが開発した、多言語でクロスプラットフォームな暗号ライブラリである。

- Conceal[9]

  Conceal は、Facebook が開発したライブラリである。共通鍵暗号アルゴリズム AES(256bit) と暗号利用モード GCM を用いた暗号化処理を代行している。

この中でも Tink は、Android OS を提供している Google 社によるサードパーティ製 API であるため、Android アプリケーション開発者にも利用されている可能性は高いと考えられる。本研究では Tink を調査対象とする。

4.3.2 Tink の分析

Tink は現在、それぞれのプリミティブを使って実装された、4 つの暗号化操作を提供している。

- 関連データを備えた認証付き暗号 (プリミティブ: AEAD)
- メッセージ認証コード (プリミティブ: MAC)
- ディジタル署名 (プリミティブ: PublicKeySign と PublicKeyVerify)
- ハイブリッド暗号化 (プリミティブ: HybridEncrypt と HybridDecrypt)

プリミティブとは、単純あるいは基本的な構造や要素のことを言う。
Tink には、ドキュメントが存在するので、ドキュメントが存在しないサードパーティ製 API よりリスト化の困難性が少ない。

4.4 API の取得方法

Tink のドキュメント [10] から API を抽出する。その 167 個のクラスが持つメソッド 705 個のリスト化を行った。このリストは、2020 年 12 月のものである。リストの 1 部を抜粋し、表 5 に示す。リスト全体は付録 A に示す。

4.5 API リストと smali ファイルで利用されるメソッドのマッチング調査

調査対象となる APK 群は、AndroZoo[11] のデータセットより 307,587 個の APK から展開された smali ファイルを使用する。

API リストと smali ファイルで利用されるメソッドのマッチングは、まず smali ファイルに記述された情報から ”invoke ”が記述された行を以下の正規表現にて抽出する。

.* invoke-.*, L

(任意の文字列と”invoke-” と”L”)

抽出された行の例を以下に示す。

invoke-virtual {p0}, Lcom/google/crypto/tink/integration/android/AndroidKeysetManager;->getKeysetHandle()Lcom/google/crypto/tink/KeysetHandle;

抽出された行と API リストのマッチングはクラス名、メソッド名で行う。ソースコード 4 に Tink を利用している APK を数える Python 関数を示す。

Listing 4: API リストと smali ファイルで利用されるメソッドのマッチング Python スクリプト

```
#!/bin/bash
while read line
do
        csvpart=(${line//,/ })
        grep -r -E ".* invoke-.*, L${csvpart[1]};->${csvpart[2]}" ${1} >> "
            ${1}_${2}_result";
done < ${2}
```

5　調査結果と考察

API リストと smali ファイルで利用されるメソッドのマッチング結果を下記に示す。
調査の結果、Tink を利用しているのはパッケージ名が ”mobi.zapzap ” の APK1 つだけであった。この APK では、AndroidKeysetManager クラスとそのメソッドが使用されている。このアプリケーション名は、” ZapZap - Mobile Wallet ” [12] であり日本ではサービスしていない Android 版モバイルアプリケーションである。
使用されている API の分析から設定値を保存する SharedPreferences へのアクセスに Tink 上の AndroidKeysetManager クラスとそのメソッドを使用しているため、暗号技術そのものとして Tink は使用されていないと考えられる。
Tink 利用が Android 公式 API よりも大幅に少ない理由として、Tink1.0.0 のリリース開始が 2017 年 9 月と最近である点と、Android では公式 API の利用が中心的である点が考えられる。

Listing 5: API リストと smali ファイルで利用されるメソッドのマッチング結果

```
172_apks011_smali/16
    CFF2C83B4B4550D446C4BD60890BA6C43B047FC2D9D81120EFFF05CE69884D/mobi/
    zapzap/utils/AppUtil.smali:      invoke-virtual {p0}, Lcom/google/crypto/
    tink/integration/android/AndroidKeysetManager$Builder;->build()Lcom/
    google/crypto/tink/integration/android/AndroidKeysetManager;
172_apks011_smali/16
    CFF2C83B4B4550D446C4BD60890BA6C43B047FC2D9D81120EFFF05CE69884D/mobi/
    zapzap/utils/AppUtil.smali:      invoke-virtual {p0, v0}, Lcom/google/
    crypto/tink/integration/android/AndroidKeysetManager$Builder;->
    withKeyTemplate(Lcom/google/crypto/tink/proto/KeyTemplate;)Lcom/google/
    crypto/tink/integration/android/AndroidKeysetManager$Builder;
172_apks011_smali/16
    CFF2C83B4B4550D446C4BD60890BA6C43B047FC2D9D81120EFFF05CE69884D/mobi/
    zapzap/utils/AppUtil.smali:      invoke-virtual {p0, v0}, Lcom/google/
    crypto/tink/integration/android/AndroidKeysetManager$Builder;->
    withKeyTemplate(Lcom/google/crypto/tink/proto/KeyTemplate;)Lcom/google/
    crypto/tink/integration/android/AndroidKeysetManager$Builder;
172_apks011_smali/16
    CFF2C83B4B4550D446C4BD60890BA6C43B047FC2D9D81120EFFF05CE69884D/mobi/
    zapzap/utils/AppUtil.smali:      invoke-virtual {p0, v0}, Lcom/google/
    crypto/tink/integration/android/AndroidKeysetManager$Builder;->
    withMasterKeyUri(Ljava/lang/String;)Lcom/google/crypto/tink/integration
    /android/AndroidKeysetManager$Builder;
172_apks011_smali/16
    CFF2C83B4B4550D446C4BD60890BA6C43B047FC2D9D81120EFFF05CE69884D/mobi/
    zapzap/utils/AppUtil.smali:      invoke-virtual {v0, p0, v1, v2}, Lcom/
    google/crypto/tink/integration/android/AndroidKeysetManager$Builder;->
    withSharedPref(Landroid/content/Context;Ljava/lang/String;Ljava/lang/
    String;)Lcom/google/crypto/tink/integration/android/
    AndroidKeysetManager$Builder;
172_apks011_smali/16
    CFF2C83B4B4550D446C4BD60890BA6C43B047FC2D9D81120EFFF05CE69884D/mobi/
    zapzap/utils/AppUtil.smali:      invoke-virtual {p0}, Lcom/google/crypto/
    tink/integration/android/AndroidKeysetManager;->getKeysetHandle()Lcom/
    google/crypto/tink/KeysetHandle;
```

6　今後の課題

6.1　他のサードパーティ製 API の調査

4.3.1 で述べた通り、サードパーティ製 API は Tink 以外も存在するので、調査の幅を広げることが可能であると考える。また、他のサードパーティ製 API には 4.2 で述べた通り、公式 API とは違い、ドキュメントが公開されていないものもある。サードパーティ製の API の分析ではまず、その API についてのドキュメントが存在しているかの確認を行い、存在する場合はそのドキュメントから API のリストを作成する。存在しない場合はサードパーティ製の API のソースコードを解析し、API のドキュメントを作成してから API のリストの作成を行う。APK の解析の前に API の解析を行う必要があるという点が公式 API との違いである。作成したリストをもとに 4.5 と同様の調査を行うことが可能であると考える。

6.2　独自実装等の API の調査

4.2 で述べた通り、独自実装等の API は、ドキュメントが作成され、かつ公開されている可能性が低いため、4.4 の様に API のドキュメントから API のリストを作成することが不可能である。API のリストではなく開発者が独自実装等の際に利用する可能性の高いキーワード等を調査、整理し smali ファイル内で調査する。そしてその調査対象のキーワード群がどのメソッド名や引数として利用されているのかを調査しさらにそれらを利用しているメソッドやクラスを発見することで独自実装等の API を調査することが可能であると考える。

7　まとめ

近年開発者向けユーザブルセキュリティ、ユーザブルプライバシーの研究分野においてソフトウェア開発者の暗号技術の利用に関する研究が活発になっており、開発者による暗号技術の利用が適切にされていないことが判明している。そこで本研究ではソフトウェアの暗号技術の利用状況の網羅的な調査の一環として、Java で開発された Android アプリケーションを調査対象とし、Android アプリケーションの現状はどのような暗号技術が利用されているのかまた暗号技術の利用には何らかの傾向があるのかなどを明らかにすることを目的とし調査を行った。Google 社のサードパーティ製 API である Tink から暗号に関するメソッドを抽出し、705 個のメソッドリストを作成した。307,587 個の APK から展開された smali ファイルとこのメソッドリストをマッチングさせることで暗号技術利用の現状を明らかにした。Tink を利用している APK は AndroidKeysetManager クラスとそのメソッドが使用されている”mobi.zapzap” だけであった。このアプリケーション名は、”ZapZap - Mobile Wallet ”であり日本ではサービスしていない Android 版モバイルアプリケーションであった。使用されている API の分析から設定値を保存する SharedPreferences へのアクセスに Tink 上の AndroidKeysetManager クラスとそのメソッドを使用しているため、暗号技術そのものとして Tink は使用されていないことがわかった。今後、より詳しい API での暗号技術利用傾向を知るために他のサードパーティ製 API や、独自実装等の API に調査の幅を広げる必要があると考察した。

参考文献

[1] Stat counter. Mobile Operating System Market Share Worldwide,StatCounter Global Stats-December 2020. http://gs.statcounter.com/os-market-share/mobile/,(参照 2020-01-27)

[2] Google LLC, "Google Play", https://play.google.com/store, （参照 2021-01-21）

[3] Android Developers, "Android Developers", https://developer.android.com/index.html?hl=ja, （参照 2021-01-21）

[4] iBotPeaches, "Apktool", https://ibotpeaches.github.io/Apktool/, （参照 2021-01-21）

[5] JesusFreke, "Smali/baksmali", https://github.com/JesusFreke/smali, （参照 2021-01-21）

[6] INTERNET Watch, "Google 事例"https://internet.watch.impress.co.jp/docs/news/1046144.html, (参照　2021-01-21)

[7] Android Developers, "API reference", https://developer.android.com/reference?hl=ja, （参照 2021-01-21）

[8] Google LLC, "google/tink", https://github.com/google/tink, （参照 2021-01-28）

[9] Facebook, "Conceal", https://facebook.github.io/conceal/, （参照 2021-01-28）

[10] Tink Cryptography API for Android,"Tink Cryptography API for Android",https://google.github.io/tink/javadoc/tink-android/1.5.0/, （参照 2021-01-21）

[11] Université du Luxembourg, "AndroZoo", https://androzoo.uni.lu/, （参照 2021-01-25）

[12] Wonderwill Limited, "ZapZap - Mobile Wallet",https://www.zapzapwallet.com/,（参照 2021-01-25）

A　Android Developers の API リファレンスに記載されているメソッドを抽出して作成したリスト

クラス名	メソッド名 (引数)
ObjectName	MethodName
com/google/crypto/tink/Aead	decrypt
com/google/crypto/tink/Aead	encrypt
com/google/crypto/tink/aead/AeadConfig	init
com/google/crypto/tink/aead/AeadConfig	register
com/google/crypto/tink/aead/AeadConfig	registerStandardKeyTypes
com/google/crypto/tink/aead/subtle/AeadFactory	createAead
com/google/crypto/tink/aead/subtle/AeadFactory	getKeySizeInBytes
com/google/crypto/tink/aead/AeadKeyTemplates	createAesCtrHmacAeadKeyTemplate
com/google/crypto/tink/aead/AeadKeyTemplates	createAesEaxKeyTemplate
com/google/crypto/tink/aead/AeadKeyTemplates	createAesGcmKeyTemplate
com/google/crypto/tink/aead/AeadKeyTemplates	createKmsAeadKeyTemplate
com/google/crypto/tink/aead/AeadKeyTemplates	createKmsEnvelopeAeadKeyTemplate
com/google/crypto/tink/aead/AeadWrapper	getInputPrimitiveClass
com/google/crypto/tink/aead/AeadWrapper	getPrimitiveClass
com/google/crypto/tink/aead/AeadWrapper	register
com/google/crypto/tink/aead/AeadWrapper	wrap
com/google/crypto/tink/mac/AesCmacKeyManager	aes256CmacTemplate
com/google/crypto/tink/mac/AesCmacKeyManager	getKeyType
com/google/crypto/tink/mac/AesCmacKeyManager	getVersion
com/google/crypto/tink/mac/AesCmacKeyManager	keyFactory
com/google/crypto/tink/mac/AesCmacKeyManager	keyMaterialType
com/google/crypto/tink/mac/AesCmacKeyManager	parseKey
com/google/crypto/tink/mac/AesCmacKeyManager	rawAes256CmacTemplate
com/google/crypto/tink/mac/AesCmacKeyManager	register
com/google/crypto/tink/mac/AesCmacKeyManager	validateKey
com/google/crypto/tink/prf/AesCmacPrfKeyManager	aes256CmacTemplate
com/google/crypto/tink/prf/AesCmacPrfKeyManager	getKeyType
com/google/crypto/tink/prf/AesCmacPrfKeyManager	getVersion
com/google/crypto/tink/prf/AesCmacPrfKeyManager	keyFactory
com/google/crypto/tink/prf/AesCmacPrfKeyManager	keyMaterialType
com/google/crypto/tink/prf/AesCmacPrfKeyManager	parseKey
com/google/crypto/tink/prf/AesCmacPrfKeyManager	register
com/google/crypto/tink/prf/AesCmacPrfKeyManager	validateKey
com/google/crypto/tink/aead/AesCtrHmacAeadKeyManager	aes128CtrHmacSha256Template
com/google/crypto/tink/aead/AesCtrHmacAeadKeyManager	aes256CtrHmacSha256Template
com/google/crypto/tink/aead/AesCtrHmacAeadKeyManager	getKeyType
com/google/crypto/tink/aead/AesCtrHmacAeadKeyManager	getVersion
com/google/crypto/tink/aead/AesCtrHmacAeadKeyManager	keyFactory
com/google/crypto/tink/aead/AesCtrHmacAeadKeyManager	keyMaterialType
com/google/crypto/tink/aead/AesCtrHmacAeadKeyManager	parseKey
com/google/crypto/tink/aead/AesCtrHmacAeadKeyManager	register
com/google/crypto/tink/aead/AesCtrHmacAeadKeyManager	validateKey
com/google/crypto/tink/subtle/AesCtrHmacStreaming	expectedCiphertextSize
com/google/crypto/tink/subtle/AesCtrHmacStreaming	getCiphertextOffset
com/google/crypto/tink/subtle/AesCtrHmacStreaming	getCiphertextOverhead
com/google/crypto/tink/subtle/AesCtrHmacStreaming	getCiphertextSegmentSize
com/google/crypto/tink/subtle/AesCtrHmacStreaming	getFirstSegmentOffset
com/google/crypto/tink/subtle/AesCtrHmacStreaming	getHeaderLength
com/google/crypto/tink/subtle/AesCtrHmacStreaming	getPlaintextSegmentSize
com/google/crypto/tink/subtle/AesCtrHmacStreaming	newDecryptingChannel
com/google/crypto/tink/subtle/AesCtrHmacStreaming	newDecryptingStream

次ページに続く

前ページからの続き

クラス名	メソッド名 (引数)
com/google/crypto/tink/subtle/AesCtrHmacStreaming	newEncryptingChannel
com/google/crypto/tink/subtle/AesCtrHmacStreaming	newEncryptingStream
com/google/crypto/tink/subtle/AesCtrHmacStreaming	newSeekableDecryptingChannel
com/google/crypto/tink/subtle/AesCtrHmacStreaming	newStreamSegmentDecrypter
com/google/crypto/tink/subtle/AesCtrHmacStreaming	newStreamSegmentEncrypter
com/google/crypto/tink/streamingaead/AesCtrHmacStreamingKeyManager	aes128CtrHmacSha2561MBTemplate
com/google/crypto/tink/streamingaead/AesCtrHmacStreamingKeyManager	aes128CtrHmacSha2564KBTemplate
com/google/crypto/tink/streamingaead/AesCtrHmacStreamingKeyManager	aes256CtrHmacSha2561MBTemplate
com/google/crypto/tink/streamingaead/AesCtrHmacStreamingKeyManager	aes256CtrHmacSha2564KBTemplate
com/google/crypto/tink/streamingaead/AesCtrHmacStreamingKeyManager	getKeyType
com/google/crypto/tink/streamingaead/AesCtrHmacStreamingKeyManager	getVersion
com/google/crypto/tink/streamingaead/AesCtrHmacStreamingKeyManager	keyFactory
com/google/crypto/tink/streamingaead/AesCtrHmacStreamingKeyManager	keyMaterialType
com/google/crypto/tink/streamingaead/AesCtrHmacStreamingKeyManager	parseKey
com/google/crypto/tink/streamingaead/AesCtrHmacStreamingKeyManager	register
com/google/crypto/tink/streamingaead/AesCtrHmacStreamingKeyManager	validateKey
com/google/crypto/tink/subtle/AesCtrJceCipher	decrypt
com/google/crypto/tink/subtle/AesCtrJceCipher	encrypt
com/google/crypto/tink/aead/AesCtrKeyManager	getKeyType
com/google/crypto/tink/aead/AesCtrKeyManager	getVersion
com/google/crypto/tink/aead/AesCtrKeyManager	keyFactory
com/google/crypto/tink/aead/AesCtrKeyManager	keyMaterialType
com/google/crypto/tink/aead/AesCtrKeyManager	parseKey
com/google/crypto/tink/aead/AesCtrKeyManager	register
com/google/crypto/tink/aead/AesCtrKeyManager	validateKey
com/google/crypto/tink/subtle/AesEaxJce	decrypt
com/google/crypto/tink/subtle/AesEaxJce	encrypt
com/google/crypto/tink/aead/AesEaxKeyManager	aes128EaxTemplate
com/google/crypto/tink/aead/AesEaxKeyManager	aes256EaxTemplate
com/google/crypto/tink/aead/AesEaxKeyManager	getKeyType
com/google/crypto/tink/aead/AesEaxKeyManager	getVersion
com/google/crypto/tink/aead/AesEaxKeyManager	keyFactory
com/google/crypto/tink/aead/AesEaxKeyManager	keyMaterialType
com/google/crypto/tink/aead/AesEaxKeyManager	parseKey
com/google/crypto/tink/aead/AesEaxKeyManager	rawAes128EaxTemplate
com/google/crypto/tink/aead/AesEaxKeyManager	rawAes256EaxTemplate
com/google/crypto/tink/aead/AesEaxKeyManager	register
com/google/crypto/tink/aead/AesEaxKeyManager	validateKey
com/google/crypto/tink/aead/subtle/AesGcmFactory	createAead
com/google/crypto/tink/aead/subtle/AesGcmFactory	getKeySizeInBytes
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	expectedCiphertextSize
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	getCiphertextOffset
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	getCiphertextOverhead
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	getCiphertextSegmentSize
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	getFirstSegmentOffset
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	getHeaderLength
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	getPlaintextSegmentSize
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	newDecryptingChannel
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	newDecryptingStream
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	newEncryptingChannel
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	newEncryptingStream
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	newSeekableDecryptingChannel
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	newStreamSegmentDecrypter

次ページに続く

前ページからの続き

クラス名	メソッド名 (引数)
com/google/crypto/tink/subtle/AesGcmHkdfStreaming	newStreamSegmentEncrypter
com/google/crypto/tink/streamingaead/AesGcmHkdfStreamingKeyManager	aes128GcmHkdf1MBTemplate
com/google/crypto/tink/streamingaead/AesGcmHkdfStreamingKeyManager	aes128GcmHkdf4KBTemplate
com/google/crypto/tink/streamingaead/AesGcmHkdfStreamingKeyManager	aes256GcmHkdf1MBTemplate
com/google/crypto/tink/streamingaead/AesGcmHkdfStreamingKeyManager	aes256GcmHkdf4KBTemplate
com/google/crypto/tink/streamingaead/AesGcmHkdfStreamingKeyManager	getKeyType
com/google/crypto/tink/streamingaead/AesGcmHkdfStreamingKeyManager	getVersion
com/google/crypto/tink/streamingaead/AesGcmHkdfStreamingKeyManager	keyFactory
com/google/crypto/tink/streamingaead/AesGcmHkdfStreamingKeyManager	keyMaterialType
com/google/crypto/tink/streamingaead/AesGcmHkdfStreamingKeyManager	parseKey
com/google/crypto/tink/streamingaead/AesGcmHkdfStreamingKeyManager	register
com/google/crypto/tink/streamingaead/AesGcmHkdfStreamingKeyManager	validateKey
com/google/crypto/tink/subtle/AesGcmJce	decrypt
com/google/crypto/tink/subtle/AesGcmJce	encrypt
com/google/crypto/tink/aead/AesGcmKeyManager	aes128GcmTemplate
com/google/crypto/tink/aead/AesGcmKeyManager	aes256GcmTemplate
com/google/crypto/tink/aead/AesGcmKeyManager	getKeyType
com/google/crypto/tink/aead/AesGcmKeyManager	getVersion
com/google/crypto/tink/aead/AesGcmKeyManager	keyFactory
com/google/crypto/tink/aead/AesGcmKeyManager	keyMaterialType
com/google/crypto/tink/aead/AesGcmKeyManager	parseKey
com/google/crypto/tink/aead/AesGcmKeyManager	rawAes128GcmTemplate
com/google/crypto/tink/aead/AesGcmKeyManager	rawAes256GcmTemplate
com/google/crypto/tink/aead/AesGcmKeyManager	register
com/google/crypto/tink/aead/AesGcmKeyManager	validateKey
com/google/crypto/tink/aead/subtle/AesGcmSiv	decrypt
com/google/crypto/tink/aead/subtle/AesGcmSiv	encrypt
com/google/crypto/tink/aead/AesGcmSivKeyManager	aes128GcmSivTemplate
com/google/crypto/tink/aead/AesGcmSivKeyManager	aes256GcmSivTemplate
com/google/crypto/tink/aead/AesGcmSivKeyManager	getKeyType
com/google/crypto/tink/aead/AesGcmSivKeyManager	getVersion
com/google/crypto/tink/aead/AesGcmSivKeyManager	keyFactory
com/google/crypto/tink/aead/AesGcmSivKeyManager	keyMaterialType
com/google/crypto/tink/aead/AesGcmSivKeyManager	parseKey
com/google/crypto/tink/aead/AesGcmSivKeyManager	rawAes128GcmSivTemplate
com/google/crypto/tink/aead/AesGcmSivKeyManager	rawAes256GcmSivTemplate
com/google/crypto/tink/aead/AesGcmSivKeyManager	register
com/google/crypto/tink/aead/AesGcmSivKeyManager	validateKey
com/google/crypto/tink/subtle/AesSiv	decryptDeterministically
com/google/crypto/tink/subtle/AesSiv	encryptDeterministically
com/google/crypto/tink/daead/AesSivKeyManager	aes256SivTemplate
com/google/crypto/tink/daead/AesSivKeyManager	getKeyType
com/google/crypto/tink/daead/AesSivKeyManager	getVersion
com/google/crypto/tink/daead/AesSivKeyManager	keyFactory
com/google/crypto/tink/daead/AesSivKeyManager	keyMaterialType
com/google/crypto/tink/daead/AesSivKeyManager	parseKey
com/google/crypto/tink/daead/AesSivKeyManager	rawAes256SivTemplate
com/google/crypto/tink/daead/AesSivKeyManager	register
com/google/crypto/tink/daead/AesSivKeyManager	validateKey
com/google/crypto/tink/integration/android/AndroidKeysetManager.Builder	build
com/google/crypto/tink/integration/android/AndroidKeysetManager.Builder	doNotUseKeystore
com/google/crypto/tink/integration/android/AndroidKeysetManager.Builder	withKeyTemplate
com/google/crypto/tink/integration/android/AndroidKeysetManager.Builder	withKeyTemplate

次ページに続く

前ページからの続き

クラス名	メソッド名 (引数)
com/google/crypto/tink/integration/android/AndroidKeysetManager.Builder	withMasterKeyUri
com/google/crypto/tink/integration/android/AndroidKeysetManager.Builder	withSharedPref
com/google/crypto/tink/integration/android/AndroidKeysetManager	add
com/google/crypto/tink/integration/android/AndroidKeysetManager	add
com/google/crypto/tink/integration/android/AndroidKeysetManager	delete
com/google/crypto/tink/integration/android/AndroidKeysetManager	destroy
com/google/crypto/tink/integration/android/AndroidKeysetManager	disable
com/google/crypto/tink/integration/android/AndroidKeysetManager	enable
com/google/crypto/tink/integration/android/AndroidKeysetManager	getKeysetHandle
com/google/crypto/tink/integration/android/AndroidKeysetManager	isUsingKeystore
com/google/crypto/tink/integration/android/AndroidKeysetManager	promote
com/google/crypto/tink/integration/android/AndroidKeysetManager	rotate
com/google/crypto/tink/integration/android/AndroidKeysetManager	setPrimary
com/google/crypto/tink/integration/android/AndroidKeystoreAesGcm	decrypt
com/google/crypto/tink/integration/android/AndroidKeystoreAesGcm	encrypt
com/google/crypto/tink/integration/android/AndroidKeystoreKmsClient.Builder	build
com/google/crypto/tink/integration/android/AndroidKeystoreKmsClient.Builder	setKeyStore
com/google/crypto/tink/integration/android/AndroidKeystoreKmsClient.Builder	setKeyUri
com/google/crypto/tink/integration/android/AndroidKeystoreKmsClient	deleteKey
com/google/crypto/tink/integration/android/AndroidKeystoreKmsClient	doesSupport
com/google/crypto/tink/integration/android/AndroidKeystoreKmsClient	generateNewAeadKey
com/google/crypto/tink/integration/android/AndroidKeystoreKmsClient	getAead
com/google/crypto/tink/integration/android/AndroidKeystoreKmsClient	getOrGenerateNewAeadKey
com/google/crypto/tink/integration/android/AndroidKeystoreKmsClient	withCredentials
com/google/crypto/tink/integration/android/AndroidKeystoreKmsClient	withDefaultCredentials
com/google/crypto/tink/subtle/Base64	decode
com/google/crypto/tink/subtle/Base64	decode
com/google/crypto/tink/subtle/Base64	decode
com/google/crypto/tink/subtle/Base64	decode
com/google/crypto/tink/subtle/Base64	encode
com/google/crypto/tink/subtle/Base64	encode
com/google/crypto/tink/subtle/Base64	encode
com/google/crypto/tink/subtle/Base64	encodeToString
com/google/crypto/tink/subtle/Base64	encodeToString
com/google/crypto/tink/subtle/Base64	urlSafeDecode
com/google/crypto/tink/subtle/Base64	urlSafeEncode
com/google/crypto/tink/BinaryKeysetReader	read
com/google/crypto/tink/BinaryKeysetReader	readEncrypted
com/google/crypto/tink/BinaryKeysetReader	withBytes
com/google/crypto/tink/BinaryKeysetReader	withFile
com/google/crypto/tink/BinaryKeysetReader	withInputStream
com/google/crypto/tink/BinaryKeysetWriter	withFile
com/google/crypto/tink/BinaryKeysetWriter	withOutputStream
com/google/crypto/tink/BinaryKeysetWriter	write
com/google/crypto/tink/BinaryKeysetWriter	write
com/google/crypto/tink/subtle/Bytes	byteArrayToInt
com/google/crypto/tink/subtle/Bytes	byteArrayToInt
com/google/crypto/tink/subtle/Bytes	byteArrayToInt
com/google/crypto/tink/subtle/Bytes	concat
com/google/crypto/tink/subtle/Bytes	equal
com/google/crypto/tink/subtle/Bytes	intToByteArray
com/google/crypto/tink/subtle/Bytes	xor
com/google/crypto/tink/subtle/Bytes	xor

次ページに続く

前ページからの続き

クラス名	メソッド名 (引数)
com/google/crypto/tink/subtle/Bytes	xor
com/google/crypto/tink/subtle/Bytes	xorEnd
com/google/crypto/tink/Catalogue	getKeyManager
com/google/crypto/tink/Catalogue	getPrimitiveWrapper
com/google/crypto/tink/subtle/ChaCha20Poly1305	decrypt
com/google/crypto/tink/subtle/ChaCha20Poly1305	encrypt
com/google/crypto/tink/aead/ChaCha20Poly1305KeyManager	chaCha20Poly1305Template
com/google/crypto/tink/aead/ChaCha20Poly1305KeyManager	getKeyType
com/google/crypto/tink/aead/ChaCha20Poly1305KeyManager	getVersion
com/google/crypto/tink/aead/ChaCha20Poly1305KeyManager	keyFactory
com/google/crypto/tink/aead/ChaCha20Poly1305KeyManager	keyMaterialType
com/google/crypto/tink/aead/ChaCha20Poly1305KeyManager	parseKey
com/google/crypto/tink/aead/ChaCha20Poly1305KeyManager	rawChaCha20Poly1305Template
com/google/crypto/tink/aead/ChaCha20Poly1305KeyManager	register
com/google/crypto/tink/aead/ChaCha20Poly1305KeyManager	validateKey
com/google/crypto/tink/CleartextKeysetHandle	fromKeyset
com/google/crypto/tink/CleartextKeysetHandle	getKeyset
com/google/crypto/tink/CleartextKeysetHandle	parseFrom
com/google/crypto/tink/CleartextKeysetHandle	read
com/google/crypto/tink/CleartextKeysetHandle	write
com/google/crypto/tink/Config	getTinkKeyTypeEntry
com/google/crypto/tink/Config	register
com/google/crypto/tink/Config	registerKeyType
com/google/crypto/tink/CryptoFormat	getOutputPrefix
com/google/crypto/tink/DeterministicAead	decryptDeterministically
com/google/crypto/tink/DeterministicAead	encryptDeterministically
com/google/crypto/tink/daead/DeterministicAeadConfig	init
com/google/crypto/tink/daead/DeterministicAeadConfig	register
com/google/crypto/tink/daead/DeterministicAeadFactory	getPrimitive
com/google/crypto/tink/daead/DeterministicAeadFactory	getPrimitive
com/google/crypto/tink/daead/DeterministicAeadKeyTemplates	createAesSivKeyTemplate
com/google/crypto/tink/daead/DeterministicAeadWrapper	getInputPrimitiveClass
com/google/crypto/tink/daead/DeterministicAeadWrapper	getPrimitiveClass
com/google/crypto/tink/daead/DeterministicAeadWrapper	register
com/google/crypto/tink/daead/DeterministicAeadWrapper	wrap
com/google/crypto/tink/subtle/EcdsaSignJce	sign
com/google/crypto/tink/signature/EcdsaSignKeyManager	createKeyTemplate
com/google/crypto/tink/signature/EcdsaSignKeyManager	ecdsaP256Template
com/google/crypto/tink/signature/EcdsaSignKeyManager	getKeyType
com/google/crypto/tink/signature/EcdsaSignKeyManager	getPublicKey
com/google/crypto/tink/signature/EcdsaSignKeyManager	getVersion
com/google/crypto/tink/signature/EcdsaSignKeyManager	keyFactory
com/google/crypto/tink/signature/EcdsaSignKeyManager	keyMaterialType
com/google/crypto/tink/signature/EcdsaSignKeyManager	parseKey
com/google/crypto/tink/signature/EcdsaSignKeyManager	rawEcdsaP256Template
com/google/crypto/tink/signature/EcdsaSignKeyManager	registerPair
com/google/crypto/tink/signature/EcdsaSignKeyManager	validateKey
com/google/crypto/tink/subtle/EcdsaVerifyJce	verify
com/google/crypto/tink/subtle/EciesAeadHkdfDemHelper	getAead
com/google/crypto/tink/subtle/EciesAeadHkdfDemHelper	getSymmetricKeySizeInBytes
com/google/crypto/tink/subtle/EciesAeadHkdfHybridDecrypt	decrypt
com/google/crypto/tink/subtle/EciesAeadHkdfHybridEncrypt	encrypt
com/google/crypto/tink/hybrid/EciesAeadHkdfPrivateKeyManager	eciesP256HkdfHmacSha256Aes128CtrHmacSha256Template

次ページに続く

前ページからの続き

クラス名	メソッド名 (引数)
com/google/crypto/tink/hybrid/EciesAeadHkdfPrivateKeyManager	eciesP256HkdfHmacSha256Aes128GcmTemplate
com/google/crypto/tink/hybrid/EciesAeadHkdfPrivateKeyManager	getKeyType
com/google/crypto/tink/hybrid/EciesAeadHkdfPrivateKeyManager	getPublicKey
com/google/crypto/tink/hybrid/EciesAeadHkdfPrivateKeyManager	getVersion
com/google/crypto/tink/hybrid/EciesAeadHkdfPrivateKeyManager	keyFactory
com/google/crypto/tink/hybrid/EciesAeadHkdfPrivateKeyManager	keyMaterialType
com/google/crypto/tink/hybrid/EciesAeadHkdfPrivateKeyManager	parseKey
com/google/crypto/tink/hybrid/EciesAeadHkdfPrivateKeyManager	rawEciesP256HkdfHmacSha256Aes128CtrHmacSha256CompressedTemplate
com/google/crypto/tink/hybrid/EciesAeadHkdfPrivateKeyManager	rawEciesP256HkdfHmacSha256Aes128GcmCompressedTemplate
com/google/crypto/tink/hybrid/EciesAeadHkdfPrivateKeyManager	registerPair
com/google/crypto/tink/hybrid/EciesAeadHkdfPrivateKeyManager	validateKey
com/google/crypto/tink/subtle/EciesHkdfRecipientKem	generateKey
com/google/crypto/tink/subtle/EciesHkdfSenderKem.KemKey	getKemBytes
com/google/crypto/tink/subtle/EciesHkdfSenderKem.KemKey	getSymmetricKey
com/google/crypto/tink/subtle/EciesHkdfSenderKem	generateKey
com/google/crypto/tink/signature/Ed25519PrivateKeyManager	ed25519Template
com/google/crypto/tink/signature/Ed25519PrivateKeyManager	getKeyType
com/google/crypto/tink/signature/Ed25519PrivateKeyManager	getPublicKey
com/google/crypto/tink/signature/Ed25519PrivateKeyManager	getVersion
com/google/crypto/tink/signature/Ed25519PrivateKeyManager	keyFactory
com/google/crypto/tink/signature/Ed25519PrivateKeyManager	keyMaterialType
com/google/crypto/tink/signature/Ed25519PrivateKeyManager	parseKey
com/google/crypto/tink/signature/Ed25519PrivateKeyManager	rawEd25519Template
com/google/crypto/tink/signature/Ed25519PrivateKeyManager	registerPair
com/google/crypto/tink/signature/Ed25519PrivateKeyManager	validateKey
com/google/crypto/tink/subtle/Ed25519Sign.KeyPair	getPrivateKey
com/google/crypto/tink/subtle/Ed25519Sign.KeyPair	getPublicKey
com/google/crypto/tink/subtle/Ed25519Sign.KeyPair	newKeyPair
com/google/crypto/tink/subtle/Ed25519Sign	sign
com/google/crypto/tink/subtle/Ed25519Verify	verify
com/google/crypto/tink/subtle/EllipticCurves.CurveType	valueOf
com/google/crypto/tink/subtle/EllipticCurves.CurveType	values
com/google/crypto/tink/subtle/EllipticCurves.EcdsaEncoding	valueOf
com/google/crypto/tink/subtle/EllipticCurves.EcdsaEncoding	values
com/google/crypto/tink/subtle/EllipticCurves.PointFormatType	valueOf
com/google/crypto/tink/subtle/EllipticCurves.PointFormatType	values
com/google/crypto/tink/subtle/EllipticCurves	computeSharedSecret
com/google/crypto/tink/subtle/EllipticCurves	computeSharedSecret
com/google/crypto/tink/subtle/EllipticCurves	ecdsaDer2Ieee
com/google/crypto/tink/subtle/EllipticCurves	ecdsaIeee2Der
com/google/crypto/tink/subtle/EllipticCurves	ecPointDecode
com/google/crypto/tink/subtle/EllipticCurves	encodingSizeInBytes
com/google/crypto/tink/subtle/EllipticCurves	fieldSizeInBytes
com/google/crypto/tink/subtle/EllipticCurves	generateKeyPair
com/google/crypto/tink/subtle/EllipticCurves	generateKeyPair
com/google/crypto/tink/subtle/EllipticCurves	getCurveSpec
com/google/crypto/tink/subtle/EllipticCurves	getEcPrivateKey
com/google/crypto/tink/subtle/EllipticCurves	getEcPrivateKey
com/google/crypto/tink/subtle/EllipticCurves	getEcPublicKey
com/google/crypto/tink/subtle/EllipticCurves	getEcPublicKey
com/google/crypto/tink/subtle/EllipticCurves	getEcPublicKey
com/google/crypto/tink/subtle/EllipticCurves	getEcPublicKey
com/google/crypto/tink/subtle/EllipticCurves	getModulus

次ページに続く

前ページからの続き

クラス名	メソッド名 (引数)
com/google/crypto/tink/subtle/EllipticCurves	getNistP256Params
com/google/crypto/tink/subtle/EllipticCurves	getNistP384Params
com/google/crypto/tink/subtle/EllipticCurves	getNistP521Params
com/google/crypto/tink/subtle/EllipticCurves	getY
com/google/crypto/tink/subtle/EllipticCurves	isNistEcParameterSpec
com/google/crypto/tink/subtle/EllipticCurves	isSameEcParameterSpec
com/google/crypto/tink/subtle/EllipticCurves	isValidDerEncoding
com/google/crypto/tink/subtle/EllipticCurves	modSqrt
com/google/crypto/tink/subtle/EllipticCurves	pointDecode
com/google/crypto/tink/subtle/EllipticCurves	pointDecode
com/google/crypto/tink/subtle/EllipticCurves	pointEncode
com/google/crypto/tink/subtle/EllipticCurves	pointEncode
com/google/crypto/tink/subtle/EllipticCurves	validatePublicKey
com/google/crypto/tink/subtle/EncryptThenAuthenticate	decrypt
com/google/crypto/tink/subtle/EncryptThenAuthenticate	encrypt
com/google/crypto/tink/subtle/EncryptThenAuthenticate	newAesCtrHmac
com/google/crypto/tink/subtle/EngineFactory	getCustomCipherProvider
com/google/crypto/tink/subtle/EngineFactory	getCustomKeyAgreementProvider
com/google/crypto/tink/subtle/EngineFactory	getCustomKeyFactoryProvider
com/google/crypto/tink/subtle/EngineFactory	getCustomKeyPairGeneratorProvider
com/google/crypto/tink/subtle/EngineFactory	getCustomMacProvider
com/google/crypto/tink/subtle/EngineFactory	getCustomMessageDigestProvider
com/google/crypto/tink/subtle/EngineFactory	getCustomSignatureProvider
com/google/crypto/tink/subtle/EngineFactory	getInstance
com/google/crypto/tink/subtle/EngineFactory	toProviderList
com/google/crypto/tink/subtle/EngineWrapper.TCipher	getInstance
com/google/crypto/tink/subtle/EngineWrapper.TKeyAgreement	getInstance
com/google/crypto/tink/subtle/EngineWrapper.TKeyFactory	getInstance
com/google/crypto/tink/subtle/EngineWrapper.TKeyPairGenerator	getInstance
com/google/crypto/tink/subtle/EngineWrapper.TMac	getInstance
com/google/crypto/tink/subtle/EngineWrapper.TMessageDigest	getInstance
com/google/crypto/tink/subtle/EngineWrapper.TSignature	getInstance
com/google/crypto/tink/subtle/EngineWrapper	getInstance
com/google/crypto/tink/subtle/Enums.HashType	valueOf
com/google/crypto/tink/subtle/Enums.HashType	values
com/google/crypto/tink/subtle/Hex	decode
com/google/crypto/tink/subtle/Hex	encode
com/google/crypto/tink/subtle/Hkdf	computeEciesHkdfSymmetricKey
com/google/crypto/tink/subtle/Hkdf	computeHkdf
com/google/crypto/tink/prf/HkdfPrfKeyManager	getKeyType
com/google/crypto/tink/prf/HkdfPrfKeyManager	getVersion
com/google/crypto/tink/prf/HkdfPrfKeyManager	hkdfSha256Template
com/google/crypto/tink/prf/HkdfPrfKeyManager	keyFactory
com/google/crypto/tink/prf/HkdfPrfKeyManager	keyMaterialType
com/google/crypto/tink/prf/HkdfPrfKeyManager	parseKey
com/google/crypto/tink/prf/HkdfPrfKeyManager	register
com/google/crypto/tink/prf/HkdfPrfKeyManager	staticKeyType
com/google/crypto/tink/prf/HkdfPrfKeyManager	validateKey
com/google/crypto/tink/subtle/prf/HkdfStreamingPrf	computePrf
com/google/crypto/tink/mac/HmacKeyManager	getKeyType
com/google/crypto/tink/mac/HmacKeyManager	getVersion
com/google/crypto/tink/mac/HmacKeyManager	hmacSha256HalfDigestTemplate
com/google/crypto/tink/mac/HmacKeyManager	hmacSha256Template

次ページに続く

前ページからの続き

クラス名	メソッド名 (引数)
com/google/crypto/tink/mac/HmacKeyManager	hmacSha512HalfDigestTemplate
com/google/crypto/tink/mac/HmacKeyManager	hmacSha512Template
com/google/crypto/tink/mac/HmacKeyManager	keyFactory
com/google/crypto/tink/mac/HmacKeyManager	keyMaterialType
com/google/crypto/tink/mac/HmacKeyManager	parseKey
com/google/crypto/tink/mac/HmacKeyManager	register
com/google/crypto/tink/mac/HmacKeyManager	validateKey
com/google/crypto/tink/prf/HmacPrfKeyManager	getKeyType
com/google/crypto/tink/prf/HmacPrfKeyManager	getVersion
com/google/crypto/tink/prf/HmacPrfKeyManager	hmacSha256Template
com/google/crypto/tink/prf/HmacPrfKeyManager	hmacSha512Template
com/google/crypto/tink/prf/HmacPrfKeyManager	keyFactory
com/google/crypto/tink/prf/HmacPrfKeyManager	keyMaterialType
com/google/crypto/tink/prf/HmacPrfKeyManager	parseKey
com/google/crypto/tink/prf/HmacPrfKeyManager	register
com/google/crypto/tink/prf/HmacPrfKeyManager	validateKey
com/google/crypto/tink/hybrid/HybridConfig	init
com/google/crypto/tink/hybrid/HybridConfig	register
com/google/crypto/tink/HybridDecrypt	decrypt
com/google/crypto/tink/hybrid/HybridDecryptFactory	getPrimitive
com/google/crypto/tink/hybrid/HybridDecryptFactory	getPrimitive
com/google/crypto/tink/hybrid/HybridDecryptWrapper	getInputPrimitiveClass
com/google/crypto/tink/hybrid/HybridDecryptWrapper	getPrimitiveClass
com/google/crypto/tink/hybrid/HybridDecryptWrapper	register
com/google/crypto/tink/hybrid/HybridDecryptWrapper	wrap
com/google/crypto/tink/HybridEncrypt	encrypt
com/google/crypto/tink/hybrid/HybridEncryptFactory	getPrimitive
com/google/crypto/tink/hybrid/HybridEncryptFactory	getPrimitive
com/google/crypto/tink/hybrid/HybridKeyTemplates	createEciesAeadHkdfKeyTemplate
com/google/crypto/tink/hybrid/HybridKeyTemplates	createEciesAeadHkdfParams
com/google/crypto/tink/subtle/ImmutableByteArray	getBytes
com/google/crypto/tink/subtle/ImmutableByteArray	getLength
com/google/crypto/tink/subtle/ImmutableByteArray	of
com/google/crypto/tink/subtle/ImmutableByteArray	of
com/google/crypto/tink/subtle/IndCpaCipher	decrypt
com/google/crypto/tink/subtle/IndCpaCipher	encrypt
com/google/crypto/tink/JsonKeysetReader	read
com/google/crypto/tink/JsonKeysetReader	readEncrypted
com/google/crypto/tink/JsonKeysetReader	withBytes
com/google/crypto/tink/JsonKeysetReader	withFile
com/google/crypto/tink/JsonKeysetReader	withInputStream
com/google/crypto/tink/JsonKeysetReader	withJsonObject
com/google/crypto/tink/JsonKeysetReader	withPath
com/google/crypto/tink/JsonKeysetReader	withPath
com/google/crypto/tink/JsonKeysetReader	withString
com/google/crypto/tink/JsonKeysetReader	withUrlSafeBase64
com/google/crypto/tink/JsonKeysetWriter	withFile
com/google/crypto/tink/JsonKeysetWriter	withOutputStream
com/google/crypto/tink/JsonKeysetWriter	withPath
com/google/crypto/tink/JsonKeysetWriter	withPath
com/google/crypto/tink/JsonKeysetWriter	write
com/google/crypto/tink/JsonKeysetWriter	write
com/google/crypto/tink/KeyManager	doesSupport

次ページに続く

前ページからの続き

クラス名	メソッド名 (引数)
com/google/crypto/tink/KeyManager	getKeyType
com/google/crypto/tink/KeyManager	getPrimitive
com/google/crypto/tink/KeyManager	getPrimitive
com/google/crypto/tink/KeyManager	getPrimitiveClass
com/google/crypto/tink/KeyManager	getVersion
com/google/crypto/tink/KeyManager	newKey
com/google/crypto/tink/KeyManager	newKey
com/google/crypto/tink/KeyManager	newKeyData
com/google/crypto/tink/KeyManagerImpl	doesSupport
com/google/crypto/tink/KeyManagerImpl	getKeyType
com/google/crypto/tink/KeyManagerImpl	getPrimitive
com/google/crypto/tink/KeyManagerImpl	getPrimitive
com/google/crypto/tink/KeyManagerImpl	getPrimitiveClass
com/google/crypto/tink/KeyManagerImpl	getVersion
com/google/crypto/tink/KeyManagerImpl	newKey
com/google/crypto/tink/KeyManagerImpl	newKey
com/google/crypto/tink/KeyManagerImpl	newKeyData
com/google/crypto/tink/KeyTemplate.OutputPrefixType	valueOf
com/google/crypto/tink/KeyTemplate.OutputPrefixType	values
com/google/crypto/tink/KeyTemplate	create
com/google/crypto/tink/KeyTemplate	getOutputPrefixType
com/google/crypto/tink/KeyTemplate	getTypeUrl
com/google/crypto/tink/KeyTemplate	getValue
com/google/crypto/tink/KeyTypeManager.KeyFactory	createKey
com/google/crypto/tink/KeyTypeManager.KeyFactory	deriveKey
com/google/crypto/tink/KeyTypeManager.KeyFactory	getKeyFormatClass
com/google/crypto/tink/KeyTypeManager.KeyFactory	parseKeyFormat
com/google/crypto/tink/KeyTypeManager.KeyFactory	validateKeyFormat
com/google/crypto/tink/KeyTypeManager.PrimitiveFactory	getPrimitive
com/google/crypto/tink/KeyTypeManager	getKeyClass
com/google/crypto/tink/KeyTypeManager	getKeyType
com/google/crypto/tink/KeyTypeManager	getPrimitive
com/google/crypto/tink/KeyTypeManager	getVersion
com/google/crypto/tink/KeyTypeManager	keyFactory
com/google/crypto/tink/KeyTypeManager	keyMaterialType
com/google/crypto/tink/KeyTypeManager	parseKey
com/google/crypto/tink/KeyTypeManager	supportedPrimitives
com/google/crypto/tink/KeyTypeManager	validateKey
com/google/crypto/tink/KeysetHandle	assertEnoughEncryptedKeyMaterial
com/google/crypto/tink/KeysetHandle	assertEnoughKeyMaterial
com/google/crypto/tink/KeysetHandle	generateNew
com/google/crypto/tink/KeysetHandle	generateNew
com/google/crypto/tink/KeysetHandle	getKeysetInfo
com/google/crypto/tink/KeysetHandle	getPrimitive
com/google/crypto/tink/KeysetHandle	getPrimitive
com/google/crypto/tink/KeysetHandle	getPublicKeysetHandle
com/google/crypto/tink/KeysetHandle	read
com/google/crypto/tink/KeysetHandle	readNoSecret
com/google/crypto/tink/KeysetHandle	readNoSecret
com/google/crypto/tink/KeysetHandle	toString
com/google/crypto/tink/KeysetHandle	write
com/google/crypto/tink/KeysetHandle	writeNoSecret
com/google/crypto/tink/KeysetManager	add

次ページに続く

前ページからの続き

クラス名	メソッド名 (引数)
com/google/crypto/tink/KeysetManager	add
com/google/crypto/tink/KeysetManager	addNewKey
com/google/crypto/tink/KeysetManager	delete
com/google/crypto/tink/KeysetManager	destroy
com/google/crypto/tink/KeysetManager	disable
com/google/crypto/tink/KeysetManager	enable
com/google/crypto/tink/KeysetManager	getKeysetHandle
com/google/crypto/tink/KeysetManager	promote
com/google/crypto/tink/KeysetManager	rotate
com/google/crypto/tink/KeysetManager	setPrimary
com/google/crypto/tink/KeysetManager	withEmptyKeyset
com/google/crypto/tink/KeysetManager	withKeysetHandle
com/google/crypto/tink/KeysetReader	read
com/google/crypto/tink/KeysetReader	readEncrypted
com/google/crypto/tink/KeysetWriter	write
com/google/crypto/tink/KeysetWriter	write
com/google/crypto/tink/aead/KmsAeadKeyManager	getKeyType
com/google/crypto/tink/aead/KmsAeadKeyManager	getVersion
com/google/crypto/tink/aead/KmsAeadKeyManager	keyFactory
com/google/crypto/tink/aead/KmsAeadKeyManager	keyMaterialType
com/google/crypto/tink/aead/KmsAeadKeyManager	parseKey
com/google/crypto/tink/aead/KmsAeadKeyManager	register
com/google/crypto/tink/aead/KmsAeadKeyManager	validateKey
com/google/crypto/tink/KmsClient	doesSupport
com/google/crypto/tink/KmsClient	getAead
com/google/crypto/tink/KmsClient	withCredentials
com/google/crypto/tink/KmsClient	withDefaultCredentials
com/google/crypto/tink/KmsClients	add
com/google/crypto/tink/KmsClients	get
com/google/crypto/tink/KmsClients	getAutoLoaded
com/google/crypto/tink/aead/KmsEnvelopeAead	decrypt
com/google/crypto/tink/aead/KmsEnvelopeAead	encrypt
com/google/crypto/tink/aead/KmsEnvelopeAeadKeyManager	getKeyType
com/google/crypto/tink/aead/KmsEnvelopeAeadKeyManager	getVersion
com/google/crypto/tink/aead/KmsEnvelopeAeadKeyManager	keyFactory
com/google/crypto/tink/aead/KmsEnvelopeAeadKeyManager	keyMaterialType
com/google/crypto/tink/aead/KmsEnvelopeAeadKeyManager	parseKey
com/google/crypto/tink/aead/KmsEnvelopeAeadKeyManager	register
com/google/crypto/tink/aead/KmsEnvelopeAeadKeyManager	validateKey
com/google/crypto/tink/subtle/Kwp	unwrap
com/google/crypto/tink/subtle/Kwp	wrap
com/google/crypto/tink/Mac	computeMac
com/google/crypto/tink/Mac	verifyMac
com/google/crypto/tink/mac/MacConfig	init
com/google/crypto/tink/mac/MacConfig	register
com/google/crypto/tink/mac/MacConfig	registerStandardKeyTypes
com/google/crypto/tink/mac/MacFactory	getPrimitive
com/google/crypto/tink/mac/MacFactory	getPrimitive
com/google/crypto/tink/mac/MacKeyTemplates	createHmacKeyTemplate
com/google/crypto/tink/NoSecretKeysetHandle	parseFrom
com/google/crypto/tink/NoSecretKeysetHandle	read
com/google/crypto/tink/subtle/PemKeyType	readKey
com/google/crypto/tink/subtle/PemKeyType	valueOf

次ページに続く

前ページからの続き

クラス名	メソッド名 (引数)
com/google/crypto/tink/subtle/PemKeyType	values
com/google/crypto/tink/prf/Prf	compute
com/google/crypto/tink/subtle/PrfAesCmac	compute
com/google/crypto/tink/prf/PrfConfig	register
com/google/crypto/tink/subtle/PrfHmacJce	compute
com/google/crypto/tink/subtle/PrfHmacJce	getMaxOutputLength
com/google/crypto/tink/subtle/prf/PrfImpl	compute
com/google/crypto/tink/subtle/prf/PrfImpl	wrap
com/google/crypto/tink/subtle/PrfMac	computeMac
com/google/crypto/tink/subtle/PrfMac	verifyMac
com/google/crypto/tink/prf/PrfSet	computePrimary
com/google/crypto/tink/prf/PrfSet	getPrfs
com/google/crypto/tink/prf/PrfSet	getPrimaryId
com/google/crypto/tink/prf/PrfSetWrapper	getInputPrimitiveClass
com/google/crypto/tink/prf/PrfSetWrapper	getPrimitiveClass
com/google/crypto/tink/prf/PrfSetWrapper	register
com/google/crypto/tink/prf/PrfSetWrapper	wrap
com/google/crypto/tink/PrimitiveSet.Entry	getIdentifier
com/google/crypto/tink/PrimitiveSet.Entry	getKeyId
com/google/crypto/tink/PrimitiveSet.Entry	getOutputPrefixType
com/google/crypto/tink/PrimitiveSet.Entry	getPrimitive
com/google/crypto/tink/PrimitiveSet.Entry	getStatus
com/google/crypto/tink/PrimitiveWrapper	getInputPrimitiveClass
com/google/crypto/tink/PrimitiveWrapper	getPrimitiveClass
com/google/crypto/tink/PrimitiveWrapper	wrap
com/google/crypto/tink/PrivateKeyManager	getPublicKeyData
com/google/crypto/tink/PrivateKeyManagerImpl	getPublicKeyData
com/google/crypto/tink/PrivateKeyTypeManager	getPublicKey
com/google/crypto/tink/PrivateKeyTypeManager	getPublicKeyClass
com/google/crypto/tink/PublicKeySign	sign
com/google/crypto/tink/signature/PublicKeySignFactory	getPrimitive
com/google/crypto/tink/signature/PublicKeySignFactory	getPrimitive
com/google/crypto/tink/signature/PublicKeySignWrapper	getInputPrimitiveClass
com/google/crypto/tink/signature/PublicKeySignWrapper	getPrimitiveClass
com/google/crypto/tink/signature/PublicKeySignWrapper	register
com/google/crypto/tink/signature/PublicKeySignWrapper	wrap
com/google/crypto/tink/PublicKeyVerify	verify
com/google/crypto/tink/signature/PublicKeyVerifyFactory	getPrimitive
com/google/crypto/tink/signature/PublicKeyVerifyFactory	getPrimitive
com/google/crypto/tink/subtle/Random	randBytes
com/google/crypto/tink/subtle/Random	randInt
com/google/crypto/tink/subtle/Random	randInt
com/google/crypto/tink/Registry	addCatalogue
com/google/crypto/tink/Registry	getCatalogue
com/google/crypto/tink/Registry	getInputPrimitive
com/google/crypto/tink/Registry	getKeyManager
com/google/crypto/tink/Registry	getKeyManager
com/google/crypto/tink/Registry	getPrimitive
com/google/crypto/tink/Registry	getPrimitive
com/google/crypto/tink/Registry	getPrimitive
com/google/crypto/tink/Registry	getPrimitive
com/google/crypto/tink/Registry	getPrimitive
com/google/crypto/tink/Registry	getPrimitive

次ページに続く

前ページからの続き

クラス名	メソッド名 (引数)
com/google/crypto/tink/Registry	getPrimitive
com/google/crypto/tink/Registry	getPrimitive
com/google/crypto/tink/Registry	getPrimitives
com/google/crypto/tink/Registry	getPrimitives
com/google/crypto/tink/Registry	getPublicKeyData
com/google/crypto/tink/Registry	getUntypedKeyManager
com/google/crypto/tink/Registry	newKey
com/google/crypto/tink/Registry	newKey
com/google/crypto/tink/Registry	newKeyData
com/google/crypto/tink/Registry	newKeyData
com/google/crypto/tink/Registry	registerAsymmetricKeyManagers
com/google/crypto/tink/Registry	registerKeyManager
com/google/crypto/tink/Registry	registerKeyManager
com/google/crypto/tink/Registry	registerKeyManager
com/google/crypto/tink/Registry	registerKeyManager
com/google/crypto/tink/Registry	registerKeyManager
com/google/crypto/tink/Registry	registerPrimitiveWrapper
com/google/crypto/tink/Registry	wrap
com/google/crypto/tink/Registry	wrap
com/google/crypto/tink/subtle/RewindableReadableByteChannel	close
com/google/crypto/tink/subtle/RewindableReadableByteChannel	disableRewinding
com/google/crypto/tink/subtle/RewindableReadableByteChannel	isOpen
com/google/crypto/tink/subtle/RewindableReadableByteChannel	read
com/google/crypto/tink/subtle/RewindableReadableByteChannel	rewind
com/google/crypto/tink/hybrid/subtle/RsaKemHybridDecrypt	decrypt
com/google/crypto/tink/hybrid/subtle/RsaKemHybridEncrypt	encrypt
com/google/crypto/tink/subtle/RsaSsaPkcs1SignJce	sign
com/google/crypto/tink/signature/RsaSsaPkcs1SignKeyManager	getKeyType
com/google/crypto/tink/signature/RsaSsaPkcs1SignKeyManager	getPublicKey
com/google/crypto/tink/signature/RsaSsaPkcs1SignKeyManager	getVersion
com/google/crypto/tink/signature/RsaSsaPkcs1SignKeyManager	keyFactory
com/google/crypto/tink/signature/RsaSsaPkcs1SignKeyManager	keyMaterialType
com/google/crypto/tink/signature/RsaSsaPkcs1SignKeyManager	parseKey
com/google/crypto/tink/signature/RsaSsaPkcs1SignKeyManager	rawRsa3072SsaPkcs1Sha256F4Template
com/google/crypto/tink/signature/RsaSsaPkcs1SignKeyManager	rawRsa4096SsaPkcs1Sha512F4Template
com/google/crypto/tink/signature/RsaSsaPkcs1SignKeyManager	registerPair
com/google/crypto/tink/signature/RsaSsaPkcs1SignKeyManager	rsa3072SsaPkcs1Sha256F4Template
com/google/crypto/tink/signature/RsaSsaPkcs1SignKeyManager	rsa4096SsaPkcs1Sha512F4Template
com/google/crypto/tink/signature/RsaSsaPkcs1SignKeyManager	validateKey
com/google/crypto/tink/subtle/RsaSsaPkcs1VerifyJce	verify
com/google/crypto/tink/subtle/RsaSsaPssSignJce	sign
com/google/crypto/tink/signature/RsaSsaPssSignKeyManager	getKeyType
com/google/crypto/tink/signature/RsaSsaPssSignKeyManager	getPublicKey
com/google/crypto/tink/signature/RsaSsaPssSignKeyManager	getVersion
com/google/crypto/tink/signature/RsaSsaPssSignKeyManager	keyFactory
com/google/crypto/tink/signature/RsaSsaPssSignKeyManager	keyMaterialType
com/google/crypto/tink/signature/RsaSsaPssSignKeyManager	parseKey
com/google/crypto/tink/signature/RsaSsaPssSignKeyManager	rawRsa3072PssSha256F4Template
com/google/crypto/tink/signature/RsaSsaPssSignKeyManager	rawRsa4096PssSha512F4Template
com/google/crypto/tink/signature/RsaSsaPssSignKeyManager	registerPair
com/google/crypto/tink/signature/RsaSsaPssSignKeyManager	rsa3072PssSha256F4Template
com/google/crypto/tink/signature/RsaSsaPssSignKeyManager	rsa4096PssSha512F4Template
com/google/crypto/tink/signature/RsaSsaPssSignKeyManager	validateKey

次ページに続く

前ページからの続き

クラス名	メソッド名 (引数)
com/google/crypto/tink/subtle/RsaSsaPssVerifyJce	verify
com/google/crypto/tink/integration/android/SharedPrefKeysetReader	read
com/google/crypto/tink/integration/android/SharedPrefKeysetReader	readEncrypted
com/google/crypto/tink/integration/android/SharedPrefKeysetWriter	write
com/google/crypto/tink/integration/android/SharedPrefKeysetWriter	write
com/google/crypto/tink/signature/SignatureConfig	init
com/google/crypto/tink/signature/SignatureConfig	register
com/google/crypto/tink/signature/SignatureKeyTemplates	createEcdsaKeyTemplate
com/google/crypto/tink/signature/SignatureKeyTemplates	createRsaSsaPkcs1KeyTemplate
com/google/crypto/tink/signature/SignatureKeyTemplates	createRsaSsaPssKeyTemplate
com/google/crypto/tink/signature/SignaturePemKeysetReader.Builder	addPem
com/google/crypto/tink/signature/SignaturePemKeysetReader.Builder	build
com/google/crypto/tink/signature/SignaturePemKeysetReader	newBuilder
com/google/crypto/tink/signature/SignaturePemKeysetReader	read
com/google/crypto/tink/signature/SignaturePemKeysetReader	readEncrypted
com/google/crypto/tink/subtle/StreamSegmentDecrypter	decryptSegment
com/google/crypto/tink/subtle/StreamSegmentDecrypter	init
com/google/crypto/tink/subtle/StreamSegmentEncrypter	encryptSegment
com/google/crypto/tink/subtle/StreamSegmentEncrypter	encryptSegment
com/google/crypto/tink/subtle/StreamSegmentEncrypter	getHeader
com/google/crypto/tink/StreamingAead	newDecryptingChannel
com/google/crypto/tink/StreamingAead	newDecryptingStream
com/google/crypto/tink/StreamingAead	newEncryptingChannel
com/google/crypto/tink/StreamingAead	newEncryptingStream
com/google/crypto/tink/StreamingAead	newSeekableDecryptingChannel
com/google/crypto/tink/streamingaead/StreamingAeadConfig	init
com/google/crypto/tink/streamingaead/StreamingAeadConfig	register
com/google/crypto/tink/streamingaead/StreamingAeadFactory	getPrimitive
com/google/crypto/tink/streamingaead/StreamingAeadFactory	getPrimitive
com/google/crypto/tink/streamingaead/StreamingAeadKeyTemplates	createAesCtrHmacStreamingKeyTemplate
com/google/crypto/tink/streamingaead/StreamingAeadKeyTemplates	createAesGcmHkdfStreamingKeyTemplate
com/google/crypto/tink/streamingaead/StreamingAeadWrapper	getInputPrimitiveClass
com/google/crypto/tink/streamingaead/StreamingAeadWrapper	getPrimitiveClass
com/google/crypto/tink/streamingaead/StreamingAeadWrapper	register
com/google/crypto/tink/streamingaead/StreamingAeadWrapper	wrap
com/google/crypto/tink/subtle/prf/StreamingPrf	computePrf
com/google/crypto/tink/subtle/SubtleUtil	androidApiLevel
com/google/crypto/tink/subtle/SubtleUtil	bytes2Integer
com/google/crypto/tink/subtle/SubtleUtil	integer2Bytes
com/google/crypto/tink/subtle/SubtleUtil	isAndroid
com/google/crypto/tink/subtle/SubtleUtil	mgf1
com/google/crypto/tink/subtle/SubtleUtil	putAsUnsigedInt
com/google/crypto/tink/subtle/SubtleUtil	toDigestAlgo
com/google/crypto/tink/subtle/SubtleUtil	toEcdsaAlgo
com/google/crypto/tink/subtle/SubtleUtil	toRsaSsaPkcs1Algo
com/google/crypto/tink/config/TinkConfig	init
com/google/crypto/tink/config/TinkConfig	register
com/google/crypto/tink/subtle/Validators	validateAesKeySize
com/google/crypto/tink/subtle/Validators	validateCryptoKeyUri
com/google/crypto/tink/subtle/Validators	validateExists
com/google/crypto/tink/subtle/Validators	validateKmsKeyUriAndRemovePrefix
com/google/crypto/tink/subtle/Validators	validateNotExists
com/google/crypto/tink/subtle/Validators	validateRsaModulusSize

次ページに続く

前ページからの続き

クラス名	メソッド名 (引数)
com/google/crypto/tink/subtle/Validators	validateRsaPublicExponent
com/google/crypto/tink/subtle/Validators	validateSignatureHash
com/google/crypto/tink/subtle/Validators	validateTypeUrl
com/google/crypto/tink/subtle/Validators	validateVersion
com/google/crypto/tink/subtle/X25519	computeSharedSecret
com/google/crypto/tink/subtle/X25519	generatePrivateKey
com/google/crypto/tink/subtle/X25519	publicFromPrivate
com/google/crypto/tink/subtle/XChaCha20Poly1305	decrypt
com/google/crypto/tink/subtle/XChaCha20Poly1305	encrypt
com/google/crypto/tink/aead/XChaCha20Poly1305KeyManager	getKeyType
com/google/crypto/tink/aead/XChaCha20Poly1305KeyManager	getVersion
com/google/crypto/tink/aead/XChaCha20Poly1305KeyManager	keyFactory
com/google/crypto/tink/aead/XChaCha20Poly1305KeyManager	keyMaterialType
com/google/crypto/tink/aead/XChaCha20Poly1305KeyManager	parseKey
com/google/crypto/tink/aead/XChaCha20Poly1305KeyManager	rawXChaCha20Poly1305Template
com/google/crypto/tink/aead/XChaCha20Poly1305KeyManager	register
com/google/crypto/tink/aead/XChaCha20Poly1305KeyManager	validateKey
com/google/crypto/tink/aead/XChaCha20Poly1305KeyManager	xChaCha20Poly1305Template

以上