様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 ２１ 日現在

機関番号：３２６６１
研究種目：基盤研究(C)（一般）
研究期間：2019～2021
課題番号：１９Ｋ１１９７２

研究課題名（和文）開発者の暗号知識を不要にする先覚的な高機能暗号適用技術

研究課題名（英文）Anticipatory advanced cryptographic applicative techniques that eliminate the need for developers' cryptographic knowledge.

研究代表者

金岡　晃（KANAOKA, Akira）

東邦大学・理学部・准教授

研究者番号：００４５５９２４

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：代表的な高機能暗号プロトコルを機能とエンティティごとに分類しモデル化を行い、提案モデルを利用し要求を満たす組み合わせをリスト化して提供するなど簡便な方法で暗号技術の組み合わせ選択手法を実現した。また、Androidアプリケーションを対象に適用対象要素の抽出に向けて大規模な分析を行い、その結果Androidの公式APIだけでなくサードパーティ製APIの存在を確認し、それのサードパーティ製APIも解析可能なように分析手法を改良しより高精度かつ広範囲の分析方法とした。暗号適用支援技術としては基本的な暗号技術を対象に実際の開発環境上の拡張機能として実現し、実用性を確認し評価することに成功した。

研究成果の学術的意義や社会的意義
暗号技術利用によるデータの保護を分離・独立化のうえ自動化させるソフトウェア/システム開発環境を実現し、暗号技術の適切利用に係る負担を開発者から取り除くことでユーザブルセキュリティを達成する技術の創出することは、今後さらにIoT/ビッグデータ/AIの活用等で複雑化するソフトウェアやシステムに対し、安全かつ安心なソフトウェアやシステムを開発者の知識に依存することなく実現できる端緒となり、コンピュータサイエンスやセキュリティの学術研究や実システム開発・運用に大きな影響を与えることが期待でき、学術的と社会的の双方に意義を持つ研究となった。

研究成果の概要（英文）：We have realized a combination selection method for cryptographic techniques simply by classifying and modeling typical advanced cryptographic protocols by function and entity and providing a list of combinations that satisfy the requirements using the proposed model. In addition, we conducted a large-scale analysis of Android applications to identify elements to be applied. As a result, we confirmed the existence of official Android APIs and third-party APIs. We improved the analysis method to enable an analysis of these third-party APIs, resulting in a highly accurate and wide-ranging analysis method. The method has been improved to enable an analysis of official Android APIs and third-party APIs. As for cryptographic application support technology, we have successfully implemented support technology for basic cryptographic techniques as an extension to the actual development environment and confirmed and evaluated the practicality of the technology.

研究分野：情報セキュリティ

キーワード：ユーザブルセキュリティ　高機能暗号　ソフトウェア開発支援

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

セキュリティの担保とプライバシーの保護の実現には、OS やソフトウェアの脆弱性管理やネットワーク技術による境界防御などがあるが、データ自体に対しては暗号技術による保護と利活用が根本的な解決手法となる。共通鍵暗号や公開鍵暗号、ハッシュ関数を組み合わせることで、通信の秘匿化、相互認証、データの保証など、現在ではさまざまな暗号技術が提供され広範に利用されている。一方で、暗号利用の不適切さによるソフトウェアの脆弱性指摘や情報漏えい事件の発覚など、それら暗号技術を適切に利用することの困難性が指摘されている。

２．研究の目的

開発者はソフトウェア/システムを充実化させる先端技術の獲得に注力すべきであり、セキュリティの担保とプライバシー保護のための暗号技術の知識獲得をそれらと並行して行うことはもはや不可能であり不要であるのではと考えた。そこで「開発者の意図やシステムの目的を先覚的に認知し、自動的に高機能暗号をソフトウェア/システムに適用できる技術を確立できないか？」と研究の問いを置き、暗号技術利用によるデータの保護は分離・独立化のうえ自動化させるソフトウェア・システム開発環境を提供するための基盤技術を創出することを目的とした。

３．研究の方法

基盤技術の創出実現として以下の 4 つの研究アイテムを挙げた。

[研究アイテム 1] 暗号技術の機能分類とモデル化
[研究アイテム 2] 暗号技術の組み合わせの最適選択手法の確立
[研究アイテム 3] プログラム中の適用対象要素の抽出方法の確立
[研究アイテム 4] 暗号自動適用/適用支援技術の確立

それぞれのアイテムは次の研究アイテムの基盤となっているため、研究アイテムの番号順に研究を遂行していった。

４．研究成果

3 年間の研究により、研究アイテム 1 では代表的な高機能暗号プロトコルを機能とエンティティごとに分類しモデル化を行った（図 1、図 2）。研究アイテム 2 では研究アイテム 1 で果たされたモデル化を用いて、要求を満たす組み合わせをリスト化して提供するなど簡便な方法で実現を果たした。

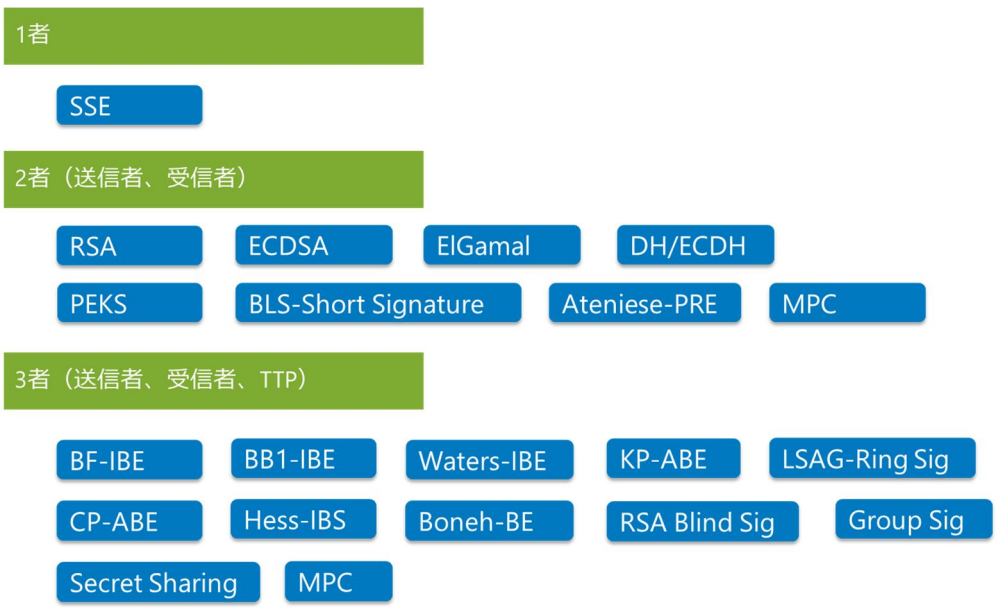

図 1：関わるエンティティ数による高機能暗号プロトコル分類

研究アイテム 3 においては、Android アプリケーションを対象に適用対象要素の抽出に向けて大規模な分析を行った。分析にあたり、高精度の分析を行うための技術の確立とともに、大規模データ分析を可能にする分析環境の構築を行い、100 万アプリでも十分に現実的な時間で解析を可能にした。

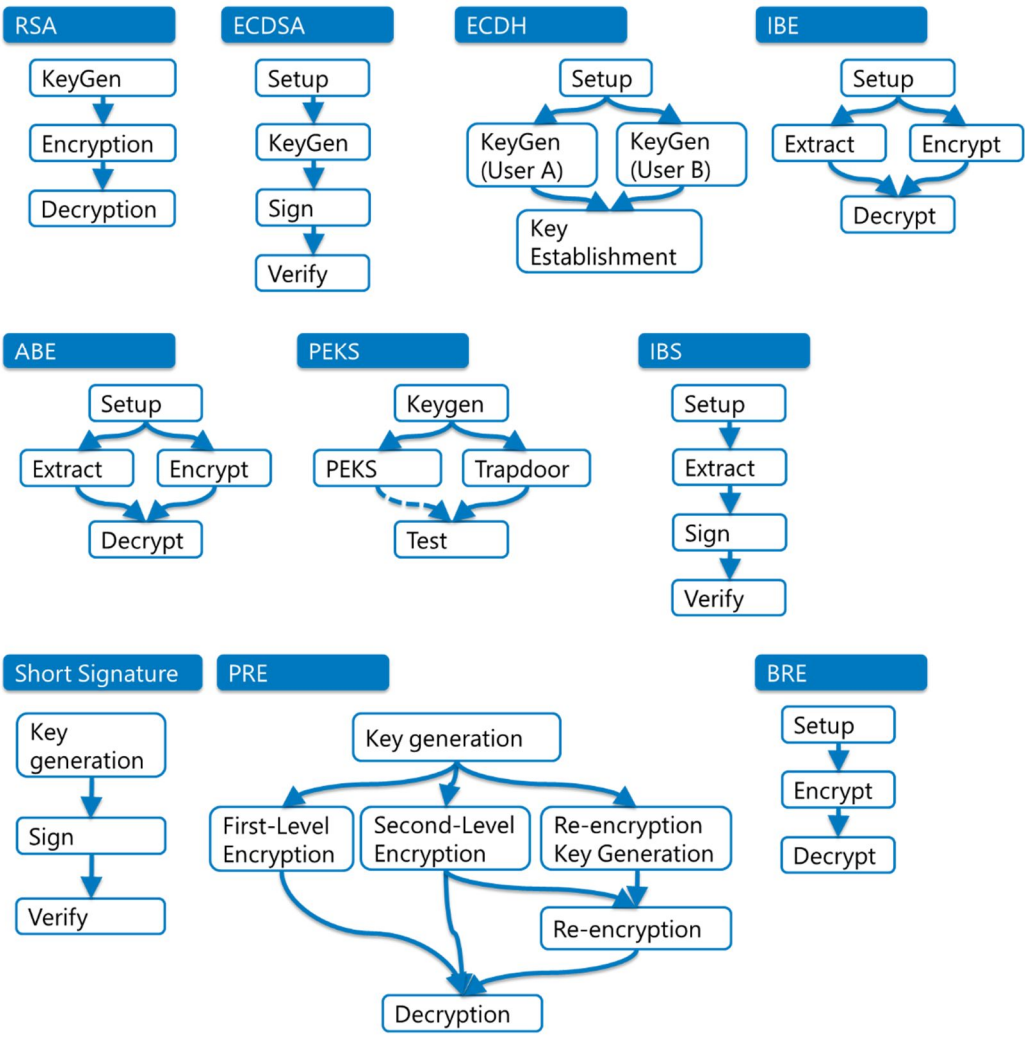

図 2：機能とフローによる高機能暗号プロトコル分類

解析の結果、Android の公式 API だけでなくサードパーティ製 API の存在を確認し、それのサードパーティ製 API も解析可能なように分析手法を改良しより高精度かつ広範囲の分析方法となった（表 1、表 2）。さらに分析結果を活用した抽出技術の提案と試作実装を実現した。
また研究アイテム 4 については、基本的な暗号技術についての暗号適用支援技術を実際の開発環境上（Android Studio、Visual Studio Code）の拡張機能やプラグインとして実現し、実用性を確認し評価することに成功した。一方で、高機能暗号の充実した支援技術にはさらなる研究が必要である点が明らかになり、それらの課題の整理と今後の発展に向けた指針を検討した。

表 1　抽出された暗号ライブラリ、サードパーティ製ライブラリの暗号利用クラス（抜粋）

ライブラリ名称	パッケージ名	分類
Spongy Castle	org.spongycastle	暗号ライブラリ
Bouncy Castle	org.bouncycastle	暗号ライブラリ
SQL Cipher	net.sqlcipher	暗号ライブラリ
JOSE: Javascript Object Signing and Encryption	com.nimbusds.jose	暗号ライブラリ
Conceal	com.facebook.crypto.cipher	暗号ライブラリ
Conscrypt	org.conscrypt	暗号ライブラリ
Amazon AWS S3 Client	com.amazonaws.services	暗号機能提供ライブラリ
okhttp	okhttp	暗号機能提供ライブラリ
AWS Key Management Service	com.amazonaws.services.kms.model	暗号機能提供ライブラリ
ExoPlayer	com.google.android.exoplayer2	暗号機能提供ライブラリ
Apache HTTP Client	org.apache.http.impl.auth	暗号機能提供ライブラリ
Visual Studio App Center	com.microsoft.appcenter.utils.crypto	暗号機能提供ライブラリ
Realm	io.realm	暗号機能提供ライブラリ
Zip4j	net.lingala.zip4j.crypto	暗号機能提供ライブラリ
Apache Common Codes	org.apache.commons.codec.digest	暗号機能提供ライブラリ
iText	com.itextpdf.text.pdf.crypto	暗号機能提供ライブラリ
Tencent Open Platform	com.tencent.utils	独自ライブラリ
Alipay wireless SDK	com.alipay.sdk.encrypt	独自ライブラリ

表 2 暗号ライブラリ、サードパーティ製ライブラリの暗号利用クラスの利用状況

ライブラリ名称	利用アプリ数	
java.security	1224474	80.29%
javax.crypto	966326	63.37%
javax.net.ssl	667743	43.79%
android.security	3003	0.20%
androidx.security.crypto	2257	0.15%
Spongy Castle	62098	4.07%
Bouncy Castle	86128	5.65%
SQL Cipher	20798	1.36%
JOSE	25463	1.67%
Conceal	8402	0.55%
Conscrypt	27487	1.80%
AWS S3 Client3	32148	2.11%
okhttp	1291362	84.68%
Apache HTTP Client	241681	15.85%
AWS KMS	8342	0.55%
ExoPlayer	580507	38.07%
Visual Studio App Center	10861	0.71%
Realm	26605	1.74%
Zip4j	6439	0.42%
Apache Common Codes	62578	4.10%
iText	12268	0.80%
Tencent Open Platform	12453	0.82%
Alipay wireless SDK	13507	0.89%

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計9件（うち招待講演　0件／うち国際学会　0件）

１．発表者名
山下 雄大、金岡 晃

２．発表標題
等価的物理モデリングを用いた暗号技術のユーザ理解度評価

３．学会等名
研究報告セキュリティ心理学とトラスト（SPT）

４．発表年
2022年

１．発表者名
金岡 晃、小山 裕輝、岡田 雅之

２．発表標題
IPアドレスをサブジェクトに含んだWebサーバ証明書の調査と分析

３．学会等名
2022年暗号と情報セキュリティシンポジウム

４．発表年
2022年

１．発表者名
金岡 晃、阿部 衛

２．発表標題
Androidアプリケーションにおける暗号ライブラリ利用状況の大規模調査

３．学会等名
コンピュータセキュリティシンポジウム2021

４．発表年
2021年

１．発表者名
金岡 晃

２．発表標題
ユーザブルセキュリティ研究における満足度評価の実態調査

３．学会等名
情報処理学会 研究報告セキュリティ心理学とトラスト（SPT）

４．発表年
2021年

１．発表者名
河合 惇丞、金岡 晃

２．発表標題
Androidアプリケーションにおける暗号API利用動向の基礎調査

３．学会等名
情報処理学会 研究報告セキュリティ心理学とトラスト（SPT）

４．発表年
2020年

１．発表者名
石島 慧、金岡 晃

２．発表標題
暗号技術の等価的な物理的モデル化検討

３．学会等名
情報処理学会 研究報告セキュリティ心理学とトラスト（SPT）

４．発表年
2021年

１．発表者名
金岡 晃

２．発表標題
高機能暗号の自動適用に向けた暗号プロトコルのステークホルダーと処理フローの整理

３．学会等名
コンピュータセキュリティシンポジウム2019

４．発表年
2019年

１．発表者名
坂間 潤一郎、金岡 晃

２．発表標題
ビットコインにおけるデジタル署名の乱数分析

３．学会等名
研究報告コンピュータセキュリティ（CSEC）

４．発表年
2019年

１．発表者名
中山 道裕、金岡 晃

２．発表標題
オストリッチZIPの総合的リスクアセスメント

３．学会等名
研究報告セキュリティ心理学とトラスト（SPT）

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

Survey of cryptographic APIs in Android
https://github.com/kanaoka-laboratory/CryptAPISurvey_inAndroidApps
Web IP Certificate Survey
https://github.com/kanaoka-laboratory/WebIPCertSurvey
研究成果に関わる詳細な情報をGithubで公開した

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関