暗号プロトコル辞典：暗号技術のユーザビリティ向上に向けた暗号プロトコルデータベースの検討

前島 涼太[1]　金岡 晃[1]

概要：暗号の技術は近代暗号の始まり以降、たくさんの手法が提案されている。しかし、ほとんどの暗号プロトコルは実用化がいまだされていない。一般の利用者がこれらの高機能暗号の技術詳細を理解することはますます困難になっている。2014 年に金岡が暗号技術の提供を自動化するためのフレームワークを提案した。金岡の研究では、提供者側は開発時に安全性を検討することなく開発可能であることや、利用者側も自身で安全性の確認をしなくて良いなど双方に利点があるとされている。提案されたフレームワークは、「暗号プロトコルの記述言語」「提案言語で記述されたプロトコルのデータベース」「暗号プロトコル選択エンジン」の 3 つのコンポーネントから構成されている。暗号プロトコルのデータベース構築を行うためには、暗号プロトコルが提供しうる細分化した情報が必要となる。
そしてその暗号プロトコルの自動適用にあたっては、暗号の機能が整理された暗号機能データベースや暗号プロトコル情報が整理された暗号プロトコルデータベース、利用可能なアプリケーション情報が整理されたが利用可能アプリデータベースの 3 つのデータベースが必要になる。本研究では、それら 3 つのデータベースをまとめたものを「暗号プロトコル大辞典」と呼び、その実現を目的とする。暗号プロトコル大辞典の実現のために、書籍を中心にプロトコルを調査し、暗号プロトコルを分類し、分類に基づきプロトコルを整理し、暗号プロトコル大辞典の基礎を作り上げた。

Cryptographic Protocol Dictionary: A Study of Cryptographic Protocol Database for Improving Usability of Cryptographic Techniques

Ryota Maejima[1]　Akira Kanaoka[1]

1. はじめに

セキュリティやプライバシの機能を提供する暗号プロトコルは多くの提案がされている。その多くは実用化が本格的には進んでおらず、実用化が見込まれる技術もプロトコルの提案からは 10 年以上経ているものが多い。学術的にはさらに高機能な暗号プロトコルが日々提案されていき、暗号技術はますます高度化していく。

一方で、暗号技術を適切に利用することの困難性が存在する。暗号プロトコル自身は安全性評価などを経て安全性がある程度担保されているものの、そのプロトコルを実装したライブラリやソフトウェア、さらにはそれらを用いたシステムでの利用となった場合、問題が起きることも多い。たとえば、広くも利用されている RSA 暗号の鍵については、機器の初期設定のまま用いられることで同じ暗号鍵が複数の箇所で利用されていることが調査として判明している。暗号そのものが安全であっても、適切な利用がされなければシステムとしては安全ではなくなる。

さらに、暗号技術の利用は、アプリケーションやシステムの開発者にとってはアプリやシステムの本来目的ではなく、開発者が暗号技術の知識を十分に持っていないことが容易に発生しうる。暗号技術の高度化は、そういった知識の不十分性を促進してしまうことにもなる。

そういった中、金岡による暗号技術の自動適用のフレームワークの提案 [1] や、Acar らによる開発者をターゲットにしたセキュリティのユーザビリティ実現についての研究 [2]、など、開発者へのユーザビリティをテーマにした研究が始まっている。実現はさまざまな方法が考えられるが、

[1] 東邦大学
Toho University

Copyright (c) 2017 by the Information Processing Society of Japan

自動化や補助ツールなど、開発者が十分な知識がなくとも安全になるための技術開発が進むことが 1 つ考えられる。

自動化や補助ツール実現には、暗号技術の適用対象となるシステムやアプリケーションがどういった機能を持つかの情報があり、それに従い提供されるセキュリティ機能が抽出され、機能実現の技術が検索され、適用ないし推薦されていく、というフローを設け、それに従い周辺の技術やデータの整備がされることが考えられる。その場合、暗号の機能と機能実現の技術群、技術を実際に利用可能なライブラリ情報が整理される必要がある。本稿ではそれらをまとめて暗号プロトコル辞典と呼ぶこととする。

本稿では暗号プロトコル辞典の実現に向けて、現在世の中にどういった暗号機能があるか、どういった技術があるかを調査して、暗号プロトコル辞典の初期検討を行った。和文の学術書から暗号技術に関連する書籍を 24 冊選び、そこに掲載されている暗号プロトコルあるいは暗号プロトコルの分類情報を計 186 種類リストアップし、そこから暗号プロトコルの機能を抽出し、機能に従い分類を行った。

2. サービスへの高機能暗号の適用を容易にするフレームワークと暗号プロトコル記述言語

2014 年に金岡はサービス開発者あるいは利用者にとって高機能な暗号技術が容易に利用可能ができるようにすることを目的とし、フレームワークを提案した。また暗号プロトコル選択に利用される暗号プロトコル記述言語についての基礎的な提案も行い、フレームワークの実現性を評価するための試作を行った。フレームワークの構成により利用側が高機能暗号プロトコルの技術詳細を知ることなく適用することが可能になるが、実現にはまだ多くの課題が残されているという結論であった [1]。

フレームワークは、暗号技術利用者、暗号アプリ・サービス提供者、暗号プロトコル検索エンジンと、各種データベースという複数のエンティティから構成される。暗号技術利用者が暗号プロトコル検索エンジンに渡すユーザ要求とサービス情報に従い、検索エンジンが暗号機能データベース、暗号プロトコル情報データベース、利用可能アプリ情報データベースから適切な暗号プロトコルを選択し暗号技術利用者に検索結果を返す。検索結果には利用が勧められる暗号プロトコル情報とともに、利用可能なアプリやサービスの情報が与えられる。暗号技術利用者はそれに従い、暗号アプリ・サービス提供者にアプリやサービスの提供を要求し、暗号技術を利用する。

各エンティティはソフトウェアや開発環境、WebAPI として自動化されることが考えられている。

提案されたフレームワークでの各エンティティやエンティティ間の通信プロトコル、また通信に用いられる情報のフォーマットについてはいずれも詳細は未定義であり、実現に向けてはまだ多くの課題が残っている。

3. 暗号プロトコル辞典

金岡の提案したフレームワークでは、暗号プロトコル検索エンジンが利用するデータベースとして以下の 3 つのデータベースがあった。

- 暗号機能データベース
- 暗号プロトコルデータベース
- 利用可能アプリ情報データベース

本研究ではこれらのデータベース群をまとめたものを暗号プロトコル辞典と呼ぶことにする。そして暗号プロトコル辞典実現に向けて、暗号機能や暗号プロトコルの整理を行い、利用可能アプリ情報データベース作成に向けた作業項目の抽出を行う。

3.1 辞典実現に向けた調査作業

暗号機能や暗号プロトコルの整理のために、どういった暗号機能と暗号プロトコルが存在するかを、様々な情報源より収集し、網羅的な調査を実施する。

情報源として検討すべきは以下の情報が考えられる。

- 標準規格
- 学術論文
- 書籍（技術書・学術書）

それぞれの情報源について、どういった暗号プロトコルが存在し、そのプロトコルがどういった機能を持つかを抽出することがまず行われる。そして抽出された情報に基づき、暗号機能の整理を行い、整理された機能を用いて暗号プロトコルの分類が行われる。

本稿では、暗号機能の整理と暗号プロトコル分類の初期検討として、上記情報源のうち和文の書籍に焦点を当て、暗号プロトコルとその機能の抽出を行うこととした。

3.2 暗号プロトコルの収集・選定・分類

暗号プロトコル大辞典の実現のために、書籍を中心にプロトコルを調査し、また各プログラミング言語で書かれた暗号ライブラリで利用可能なプロトコルがあるか調査した。

暗号に関する書籍を和文の学術書を中心に 24 冊集めた [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26]。そして各書籍から暗号プロトコルをの名称をリストアップし、暗号プロトコル大辞典に掲載するかどうかの選定を行った。その結果、計 185 個の暗号プロトコル候補がリストアップされた。

その後、リスト化された暗号プロトコル候補の分類について暗号機能の面からの分類検討を行い、分類方法と分類名称である機能名を定めた。その際、リスト化された暗号プロトコル候補のうち、機能名にあたると判断されたものは暗号プロトコル候補からは除外をした。

Copyright (c) 2017 by the Information Processing Society of Japan

- 公開鍵暗号
- 共通鍵暗号
- ハッシュ関数
- 秘密分散
- 秘密計算
- メッセージ認証コード
- 認証
- ゼロ知識証明
- コミットメント
- ハイブリッド暗号
- 変換
- 紛失通信
- 詳細不明
- 放送暗号
- 不正者追跡暗号
- 同時交換

図 1　暗号プロトコルの機能分類（大分類）

- 公開鍵暗号
  - 秘匿
    - ID ベース
  - 署名
    - 単純署名
    - ブラインド署名
    - グループ署名
    - リング署名
    - 否認不可署名
    - 検証者指定署名
    - フォワード安全署名
    - 代理署名
    - 代理再署名
    - 多重署名
    - 集約署名
    - 付録型署名
    - メッセージ回復型署名

図 2　暗号プロトコルの機能分類（公開鍵暗号の下位分類）

- 共通鍵暗号
  - ブロック暗号
  - ストリーム暗号
  - 鍵配送

図 3　暗号プロトコルの機能分類（共通鍵暗号の下位分類）

3.3　暗号機能データベースとなる情報分類

暗号機能面からの分類を以下に示す。図 1 は機能の大分類を示す。さらに細かい分類を持つものを図 2、3、4 に示した。これらの分類を基に暗号機能データベースが作成される。

3.4　暗号プロトコルデータベースとなる情報分類

図 1、図 2、図 3、図 4、に従いリスト化した暗号プロトコルを分類したものを図 1、図 2、図 3、図 4、図 5、図 6、図 7、図 8、図 9、に示す。なお、機能一覧との整合性のために、分類に該当する暗号プロトコルがない場合であっても分類情報は記載し、プロトコル情報欄は空欄で示した。暗号プロトコルの総計は 166 である。

- 秘密分散
  - ランプ型秘密計算法
  - 視覚型秘密計算法
  - 検証可秘密計算

図 4　暗号プロトコルの機能分類（秘密分散の下位分類）

大分類	中分類	小分類	暗号プロトコル名
公開鍵暗号	秘匿	ID ベース	RSA 暗号
			Rabin 暗号
			ElGamal 暗号
			OAEP
			RSA-OAEP
			Cramer-Shoup 暗号
			Goldwasser-Micali 暗号
			Paillier 暗号
			逆数暗号
			楕円 ElGamal 暗号
			楕円 RSA 暗号
			高次乗除暗号
			Merkle-Hellman 暗号
			McEliece 暗号
			CDMF
			ACE Encrypt
			ECIES
			EPOC
			PSEC
			RSAP 暗号
			制限 Rabin 暗号
			ナップザック暗号
			Boneh-Franklin IBE 方式
			境-笠原 IBE 方式
			Boneh-Boyen IBE 方式
			Gentry
			Boneh-Boyen IBE 方式
			Waters IBE 方式 (2005)
			Waters IBE 方式 (2009)
			Intrusion-resilient 暗号

表 1　暗号プロトコルリスト（公開鍵暗号:秘匿）

4.　考察

4.1　暗号機能分類と暗号プロトコルリスト

できあがったもの自体への考察。和文の学術書を中心にした調査により得られた暗号機能分類は、大分類で 16 の種類に分割された。分類によってはさらに下位の分類を持つものもあり、大分類「公開鍵暗号」の下位分類は「秘匿」「署名」に分けられ、さらに下位の分類も存在している。「署名」の下位分類では 13 の小分類が存在し、この分野での利用可能用途の広さをうかがわせる。

Copyright (c) 2017 by the Information Processing Society of Japan

大分類	中分類	小分類	暗号プロトコル名
公開鍵暗号	署名	単純署名	RSA 署名
			ElGamal 署名
			RSA-FDH 署名
			Schnorr 署名
			Boneh-Boyen 署名
			ESIGN 署名
			Fiat-Shamir 署名
			DSA
			楕円 ElGamal 署名
			楕円 DSA 署名
			楕円 Schnorr 署名
			楕円 RSA 署名
			楕円 ESIGN 署名
			Nyberg-Rueppel 署名
			阿部・岡本署名
			RSA-PSS 署名
			RSA-PSS-R 署名
			ACE Sign
			QUARTZ
			SFLASH
			改良 Rabin 署名

表 2 暗号プロトコルリスト（公開鍵暗号：署名：単純署名）

大分類	中分類	小分類	暗号プロトコル名
公開鍵暗号	署名	ブラインド署名	
		グループ署名	
		リング署名	
		否認不可署名	
		検証者指定署名	
		フォワード安全署名	
		代理署名	
		代理再署名	
		多重署名	
		集約署名	
		付録型署名	
		メッセージ回復型署名	

表 3 暗号プロトコルリスト（公開鍵暗号：署名：その他）

暗号プロトコルのリストは 166 を数えた。これらがすべて現実に利用可能であることについては何の保証もない。後述する利用可能ライブラリの調査と合わせることで、現実的に利用可能性の高い暗号アルゴリズムなどが明確化されていくことが期待される。

4.2 利用可能ライブラリの調査

暗号プロトコルの調査だけであると、実際に適用が可能かは不明である。金岡によるフレームワークにおいても、暗号機能 DB と暗号ぷトロコツ情報 DB とともに利用可能アプリ情報 DB が示されており、自動適用に向けては欠かせない情報となる。暗号化・復号や電子署名、ハッシュ関数といった暗号プロトコルはオープンソースや無料利用など、広く利用可能なライブラリを使って行われることが

大分類	中分類	小分類	暗号プロトコル名
公開鍵暗号	認証		Feige-Fiat-Shamir 認証
			Fiat-Shamir 認証
			岡本認証
			GPS
			Guillou-Quisquate 認証方式
	鍵配送		楕円 Diffie-Hellman 鍵配送
			Diffie-Hellman 鍵配送
			ID-KDS
	鍵カプセル化		PSEC-KEM
	分散暗号		RSA 分散暗号

表 4 暗号プロトコルリスト（公開鍵暗号：認証、鍵配送、鍵カプセル化、分散暗号）

大分類	中分類	小分類	暗号プロトコル名
共通鍵暗号	ブロック暗号		SERPENT
			twofish
			LUC
			Skipjack
			RC2
			SXAL/MBAL
			MISTY1
			ENCRiP
			SPEAM1
			ELCURVE
			CIPHERUNICORN-E
			M8
			Triplo
			Hierocrypt-L1
			CS-Cipher
			IDEA
			Khazad
			Nimbus
			Anubis
			Camellia
			Grand Cru
			Hierocrypt-3
			Noekeon
			Q
			SC2000
			SHACAL
			NUSH
			SAFER++

表 5 暗号プロトコルリスト（共通鍵暗号：ブロック暗号）

多い。

同じプログラミング言語でもさまざまな暗号技術ライブラリがある。また、ライブラリによっては利用可能な暗号プロトコルの差や、提供する機能の差が大きいこともある。例えば、鍵や証明書の生成など幅広い暗号機能を実行することができるライブラリや、セキュリティ機能が必要なア

Copyright (c) 2017 by the Information Processing Society of Japan

大分類	中分類	小分類	暗号プロトコル名
共通鍵暗号	ストリーム暗号		バーナム暗号
			RC4
			OFB
			ECB
			CFB
			CBC
			GCC
			FSAngo
			BLIC
			BMGL
			Leviathan
			LILI-128
			SNOW
			SOBER-t16
			SOBER-t32
			PANAMA
	鍵配送		Kerberos
			Bellare-Rogaway 法

表 6 暗号プロトコルリスト（共通鍵暗号：ストリーム暗号、鍵配送）

大分類	中分類	小分類	暗号プロトコル名
ハッシュ関数			MD4
			MD5
			N-HASH
			RIPEMD
			SHA-1
			Whirlpool
			SHA-256
			SHA-384
			SHA-512
			KECCARK

表 7 暗号プロトコルリスト（ハッシュ関数）

プリケーションの開発などに利用できるライブラリがあるなどライブラリによって実装できる暗号プロトコルはさまざまである。Java、JavaScript、C、C++、C#、Ruby、Perl、Python、PHP、Visual Basic .NET といった代表的なプログラム言語に対して暗号ライブラリの有無を調査し、そこで用いられている暗号プロトコルを抽出することでそういった傾向が明らかになるであろう。

また、ライブラリを対象にした調査では、ライブラリが対応していると謳っているものを確認するだけでなく、実際に利用可能かを調査したうえで利用可能アプリ DB への採用を決定するべきであると考える。実際に利用可能な試作実装などを行う上で得られた適用のむずかしさや、他のライブラリとの互換性についても調査がされることが望ましいだろう。

4.3 調査対象

本論文では、和文の学術書を調査して暗号プロトコルを抽出した。その結果得られたものは、暗号機能 DB の基礎となる暗号機能分類においては有用であったと言える。一方で、得られた暗号プロトコルリストは、1 つの分類に対して 1 つのものや、分類に対して具体的プロトコルが記載されていないものなど、さらなる充実が必要である。

暗号プロトコルの充実さは、調査対象を標準規格に広げることで果たされると考えられる。標準規格としては、NIST の FIPS と SP 文書、IETF、IEEE、ITU-T、ISO、OASIS 等を対象とすることを検討している。また厳密には標準規格ではないが CRYPTREC の情報も参考とする予定である。

利用可能アプリ DB 作成において実施される予定の各言語でのライブラリ調査の結果、ライブラリがサポートしている暗号プロトコルで本リストに含まれていないものが現れることも十分考えられる。その際には本リストを更新し、網羅性を高める。

4.4 まとめ

本論文では、金岡らが提案した暗号技術の自動適用に向けたフレームワーク実現のための各種データベースの実現について、調査を行い基礎的な実現の検討をした。対象となったデータベースは「暗号機能データベース」「暗号プロトコルデータベース」「利用可能アプリデータベース」の 3 つであり、本論文ではそのうち「暗号機能データベース」と「暗号プロトコルデータベース」の構築に向けた初期段階として、和文の学術書に記載のある暗号プロトコルを抽出し、そのリストを基に暗号機能データベースの基となる暗号機能の分類を行い、その分類に従い暗号プロトコルのリストを整理した。整理されたリストは暗号プロトコルデータベースの基となるものである。今後は、各プログラム言語で提供されている暗号ライブラリの調査を行い、利用可能アプリデータベースの基となる情報の収集を行う予定である。また、暗号機能とプロトコルについても英文の学術書や標準規格を調査し、充実化を図る予定である。

参考文献

[1] 金岡晃, “サービスへの高機能暗号の適用を容易にするフレームワークと暗号プロトコル記述言語”, コンピュータセキュリティシンポジウム 2014 (CSS 2014), 2014

[2] Y. Acar, S. Fahl and M. L. Mazurek, ”You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users,” 2016 IEEE Cybersecurity Development (SecDev), 2016

[3] 守屋悦朗, ”情報・符号・暗号の理論入門”, サイエンス社, 2007

[4] 澤田秀樹, ”暗号理論と代数学”, 海文堂, 2005

[5] 今井秀樹, ”暗号の本”,BT ブックス日刊工業新聞社, 2010

[6] 日本応用数理学会, 森山大輔、西巻陵、岡本龍明”公開鍵暗号の数理”, 共立出版, 2011

[7] 黒澤馨, ”現代暗号への招待”, サイエンス社, 2010

[8] NRI セキュアテクノロジーズ, ”クラウド時代の情報セキュリティ”, 日経 BP 社, 2011

[9] 佐々木良一, 手塚悟, 吉浦裕, 三島久典, ”インターネット

Copyright (c) 2017 by the Information Processing Society of Japan

大分類	中分類	小分類	暗号プロトコル名
秘密分散			Shamir 秘密分散
			Blakley 秘密分散
	ランプ型秘密分散法		
	視覚型秘密分散法		
	検証可秘密分散		Chor-Goldwasser-Micali-Awerbuch 検証可能秘密分散
秘密計算			Yao 秘密計算
メッセージ認証コード			CBC-MAC 方式
			EMAC 方式
			Two-Track-MAC
			UMAC
			OMAC 方式

表 8 暗号プロトコルリスト（秘密分散、秘密計算、メッセージ認証コード）

大分類	中分類	小分類	暗号プロトコル名
認証			UNIX パスワード方式
			使い捨てパスワード方式
			CHAP
			PAP
			FFS 認証法
			CQ 認証法
ゼロ知識証明			
コミットメント			Pedersen コミットメント
ハイブリッド暗号			黒澤-Desmedt ハイブリッド暗号
変換			藤崎-岡本変換
			Canetti-Halevi-Katz 変換
紛失通信			Rabin 紛失通信
			Even-Goldreich-Lempel 紛失通信
＜詳細不明＞			B-CRYPT
			BARAS
			ACR
			FWZ1
放送暗号			
不正者追跡暗号			
同時交換			

表 9 暗号プロトコルリスト（その他）

時代の情報セキュリティ”, 共立出版, 2000
[10] 青木隆一, 稲田龍, 村井純, ”PKI と電子社会のセキュリティ”, 共立出版, 2001
[11] 岡本龍明, 山本博資, ”現代暗号”, 産業図書, 2011
[12] 藤原良, 神保雅一, ”符号と暗号の数理”, 共立出版, 2010
[13] N. コブリッツ著, 林彬訳, ”暗号の代数理論”, 丸善出版, 2012
[14] J.A. ブーフマン著, 林芳樹訳, ”暗号理論入門”, 丸善出版, 2012
[15] S.C. コウチーニョ著, 林彬訳, ”暗号の数学的基礎”, 丸善出版, 2016
[16] 一松信, ”暗号の数理”, 講談社, 2005
[17] 佐々木良一, 手塚悟, ”情報セキュリティの基礎”, 共立出版, 2016
[18] 黒澤馨, ”現代暗号の基礎数理”, コロナ社, 2014
[19] 今井秀樹, ”情報・符号・暗号の理論”, コロナ社, 2012
[20] 辻井重男, 岡本栄司, ”暗号のすべてユビキタス社会の暗号技術”, 電波新聞社, 2002
[21] 宮地充子, ”代数学から学ぶ暗号理論”, 日本評論社, 2012
[22] 岡本栄司, ”暗号理論入門”, 共立出版, 2015
[23] D.R.Stinson 著, 櫻井幸一訳, ”暗号理論の基礎”, 共立出版, 2003
[24] 岡本栄司, 西田隆志, ”暗号と情報セキュリティ”, コロナ社, 2016
[25] 宮地充子, 菊池浩明, ”情報セキュリティ”, オーム社, 2009
[26] 結城浩, ”暗号技術入門”,SB クリエイティブ, 2015

Copyright (c) 2017 by the Information Processing Society of Japan