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

金岡 晃 †

† 東邦大学
274-8510 千葉県船橋市三山 2-2-1
akira.kanaoka@is.sci.toho-u.ac.jp

あらまし 広く利用されている RSA 暗号や AES 等よりも高機能な暗号プロトコルが数多く提案されているが、ほとんどが実用化されていない。高機能実現のための数学的背景理解に深い知識が求められ、サービス開発者やエンドユーザが理解困難であることが主因と考え、本論文では高機能暗号の適用を容易にするためのフレームワークを提案する。フレームワークでは、ユーザ側の要求事項とサービス情報のプロファイルから適用のためのエンジンが適切な暗号プロトコルを選択し、自動的に適用する。本論文では、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う。

A Framework for Facilitating to Apply Advanced Functional Cryptographic Protocols to Services, and Cryptographic Protocol Description Language

Akira Kanaoka†

†Toho University
2-2-1, Miyama, Funabashi, Chiba 274-8510 Japan
akira.kanaoka@is.sci.toho-u.ac.jp

Abstract Lots of cryptographic protocols are proposed day by day. However, almost all protocols are not yet used in real world. Based on hypothesis that difficulty of understanding mathematical background for achieving such advanced function is the primary factor, a framework for facilitating to apply advanced functional cryptographic protocols to services is proposed in this paper. The framework includes user-side requirements, service profiles, and selection engine. The selection engine selects appropriate cryptographic protocols for a service based on requirements and profiles. Furthermore, cryptographic protocol description language for selection is also proposed. Thus, prototype system is implemented for evaluation of proposed framework.

1 はじめに

暗号の技術は近代暗号の始まり以降、非常に多くの手法が提案されてきている。特に近年では、データの暗号化といった従来の単純な機能にとどまらず暗号化したまま検索が可能な手法や、より柔軟な演算を可能にする手法、また平文に戻すことなく代理再暗号化する機能や、利用

者情報を漏らさずに権利を持つものによる行為がされていることの保証など、高機能な暗号プロトコルがさまざまなアプローチで多く提案されている。それらは多くの利用者がネットワークを利用し、利用者が持つ情報資産を外部に預けることや、利用者の所有権を示すもの、利用者の匿名化などが多く求められるようになったネットワーク社会の発展に従い研究開発がされてきた。

これら高機能な暗号の実現には、さまざまな数学の技術を駆使して実現されるものが主であり、一般の利用者がこれら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。一般の利用者のみならず、方式を実装しシステム化する開発者にとっても理解は容易ではない。この状況は今後も簡単に変わるものではないと予想される。また、暗号技術それ自身は開発者や利用者が利用するサービスそのものではなく、サービス利用に対して安心と安全を提供するものであり、サービス開発者やユーザにとって暗号技術が実現される技術的背景の理解は必ずしも必須とは言えない。

本論文では、そういった背景を鑑み、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となるような暗号技術の自動適用が可能なフレームワークを提案する。フレームワークは、暗号プロトコルの記述言語と記述されたプロトコルのデータベースを中心に、ユーザ要求とサービス情報から適用すべき暗号プロトコルを選択するエンジンから構成される。これら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。

2　暗号技術提供自動化フレームワーク

2.1　フレームワーク全体像

本章では暗号化技術の提供を自動化するためのフレームワークを提案する。本フレームワークは、提供される暗号化技術の検索と検索のための情報記述方式、そして情報を格納するデータベースにより構成される。それらに対し暗号技術の提供を受ける利用者（暗号技術利用者）がユーザの要求と利用するサービスの情報を提示することで、適切な暗号化技術が選択され、それらの技術を提供する提供者により技術が提供される。全体像を図 1 に示す。暗号技術の利用者は、本フレームワークでは 2 種類に分別される。1 つはサービスあるいはアプリケーションの提供者側であり、もう 1 つはサービスあるいはアプリケーションのエンドユーザである。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保作業をしなくて良いなど、双方に利点がある。フレームワークはこれらの一連の流れを自動化することを前提として提案する。

以下の小節で、図 1 に示された書く要素について説明する。

2.2　ユーザ要求

暗号技術の利用者は、サービスあるいはアプリケーションを享受するにあたり、利用者自身のどういった情報が守られるべきか、またどういったレベルで守られるべきかといった情報を提示することが求められる。それらを明確にし、エンジンに渡すことで他の情報と合わせて適切な暗号化技術の提供を受けることができる。ユーザ要求には守られるべき情報とそのレベルに加え、利用者が許容することのできるコストの情報も合わせて記載される。ここでのコストは、支払うことができる金銭に加え、暗号化技術適用により動作が重くなるなどパフォーマンス低下の許容レベルについても含む。

2.3　サービス情報

ユーザからエンジンに送られるサービス情報には、サービスに関連する情報種類と特性、またサービスを実施するにあたり必要なエンティティ情報が送られる。情報種類では、そのサービス利用によりに利用者が入力する情報、サービス自身があらかじめ持っている情報、サービスにより生成される情報が含まれる。たとえばルー

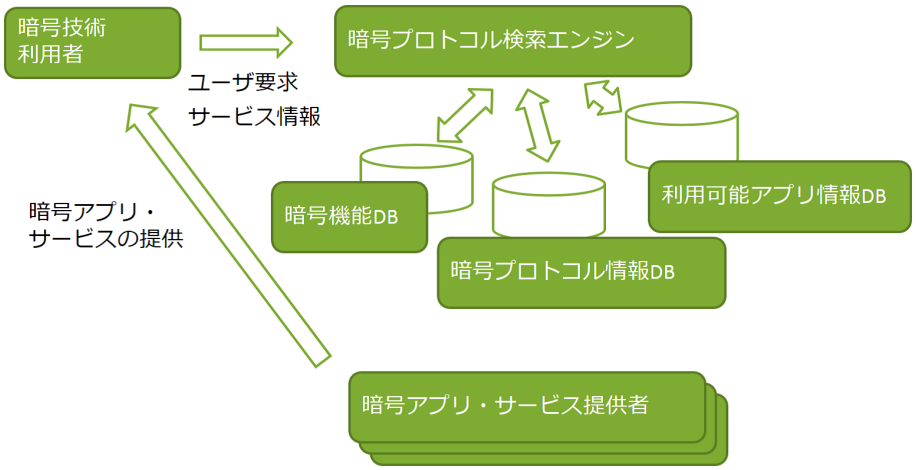

図 1: 提案フレームワークの全体像

ト検索が可能なオンライン地図では、利用者が入力する情報は現在地や目的地の情報であり、サービス自身があらかじめ持っている情報は地形情報や路線情報、時刻表情報などの情報、そしてサービスにより生成される情報は現在地から目的地までの現時点での最短ルート、となる。

エンティティ情報には、たとえばファイルをリモート保管するサービスでは、クライアントとサーバの 2 者がエンティティとして記載される。中継等が必要なサービスではクライアントとサーバに加え、中継するエンティティが必要であることが記載される。

2.4 暗号プロトコル検索エンジン

暗号プロトコル検索エンジンは、ユーザから要求されたユーザ要求とサービス情報に加え、さまざまな暗号プロトコルの情報が格納された暗号プロトコル情報 DB、プロトコル記載に用いられるさまざまな機能が記載された暗号機能 DB、そして暗号プロトコルを実際にどういう形で利用可能になっているかが格納された利用可能アプリ情報 DB の情報を用いて、ユーザ要求に従いサービスに関連する情報資産のうち保護される対象を選択し、サービス特性と関連エンティティ情報から必要とされる暗号機能群を挙げる。そして必要とされる暗号機能群から、暗号プロトコルの組み合わせを検索する。暗号プロトコルの組み合わせ検索では、機能群を満たす組み合わせだけではなく、ユーザ要求に含まれるコスト情報も考慮して検索が行われる。

2.5 暗号プロトコル記述言語

暗号プロトコル検索エンジンによる検索を可能にするためには、暗号プロトコルがどういった機能を持つか、どういったエンティティにより構成されるかの構成情報、利用するためのコスト情報、他の暗号プロトコルとの組み合わせ可能性などの情報が整理され記述されている情報が必要となる。暗号プロトコル記述言語に必要となる情報やその実現案については次章で詳細に述べる。

2.6 暗号プロトコル情報 DB

研究者により提案されてきた暗号プロトコルや、標準化がすんでいる暗号プロトコルなどが網羅的に含まれる DB である。各暗号プロトコルは DB 内で 1 つのエントリとして表現され、暗号プロトコルの詳細は暗号プロトコル記述言語により表現される。暗号プロトコル記述言語では、利用するためのコスト情報などが含まれるが、プロトコルの機能やエンティティ構成情報と比較して時間変化が大きい情報であるため、暗号プロトコル情報 DB に格納されるプロトコル情報ではこれら時間変化が大きい情報は載せ

ず、それらは別途利用可能アプリ情報 DB に格納される。

2.7 暗号機能 DB

暗号プロトコルには、データの暗号化といった単一の機能の実現だけではなく、データの認証や利用者の認証、署名、匿名化など複数の機能を同時に実現するものもある。暗号プロトコルはそれらの集合としてあらわされるものとし、プロトコルの表現のために暗号プロトコルが提供しうる機能を細分化した情報が提供される。暗号機能情報は、どういった脅威を解消あるいは軽減するかといった情報も合わせて持つ。複数機能により脅威が解消できる場合は、対応する暗号機能情報も合わせて記載されている。暗号機能 DB はそれら暗号機能情報が整理され載っている DB である。

2.8 暗号アプリ・サービス提供者

利用可能アプリ情報 DB に記載されている暗号アプリケーションあるいはサービスの提供者である。検索エンジンの検索結果を受けて、暗号技術利用者あるいは暗号プロトコル検索エンジンよりアプリケーション・サービスの提供依頼を受け、暗号技術利用者にアプリケーション・サービスを提供する。

3 暗号プロトコル記述言語

3.1 記述される項目

- プロトコル ID（重複なし）
- 概要情報（自然言語）
- 参照情報（論文や標準技術等。複数記載可能）
- 提供機能（前章の暗号機能に対応。機能 ID として記載。複数記載可能）
- エンティティ構成（プロトコルに関係するエンティティとその信頼性情報）
- 解析動向（攻撃や安全性解析などの研究動向。段階表示）

3.2 実現方式

検索が可能であることが求められるために、データとして検索が可能であり広範に利用可能な方式、さらに他のデータとの親和性が高いことが望ましい。実績や利用可能な実装などを考慮すると、XML や JSON などが適切であると考えられる。

4 サンプル実装案

4.1 サービス構成

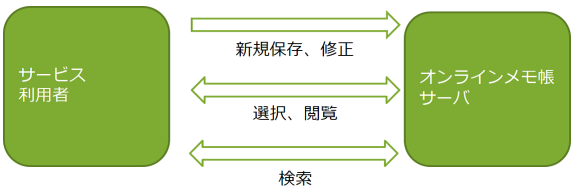

図 2: 暗号技術適用前のサービス構成

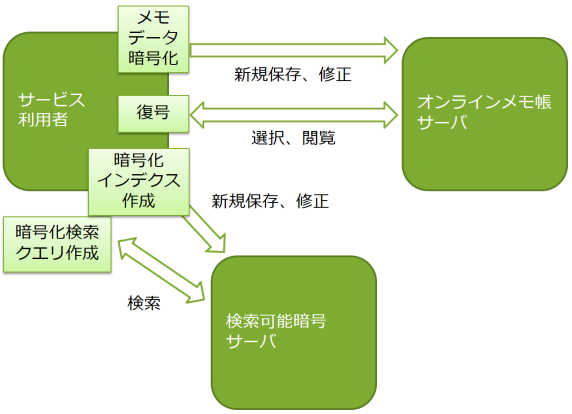

図 3: 暗号技術適用後のサービス構成

本章では、提案するフレームワークを実現するサンプル実装の案を示す。サービスの対象は利用者が作成したテキストデータ（メモ）をリモートで保存するオンラインメモ帳サービスとした。当該オンラインメモ帳サービスは Web ア

プリケーションとして実現され、利用者はブラウザを介して利用する。スマートフォンや PC では Web アプリケーションだけでなく、ローカルで稼働するアプリケーションも数多く存在するが、Microsoft が Windows8 より採用しているプログラミングモデルの Windows Runtime（WinRT）では、アプリケーションの実現に従来の C/C++と C#、VB に加え、HTML/CSS と JavaScript が含まれており、デスクトップアプリケーションも HTML と JavaScript で稼働することが拡大することも十分考えられる。

本サンプル実装では、サービス開発者が本提案エンジンを利用するのではなく、サービス利用者が利用するものとした。サービス利用者は、本提案エンジンに対応したブラウザ拡張機能をあらかじめインストールし、オンラインメモ帳サーバにアクセスした際にそのサービスに対して暗号プロトコルの自動適用を要求する。

オンラインメモ帳サーバのサービス情報については、オンラインメモ帳サーバがすでにサービス情報提供に対応しており、サービス情報はサーバより取得する。ユーザ要求はブラウザ拡張機能のインストール時の初期設定でユーザが設定済みであるとする。

サービス情報に記載された情報は

- サービスに入力される情報：テキスト情報（タイトルと本文）
- サービスがあらかじめ持っている情報:ユーザに関する情報はなし
- サービスにより生成される情報：検索用のインデクス
- サービスのプレイヤー:クライアント、サーバ

となっている。

ユーザ要求は

- サーバにテキスト情報を平文のまま渡さない
- メモ情報の検索機能を利用する
- 利用可能な上限金額 x 円

となっている。

図 4 は利用するサービスのイメージ画面である。

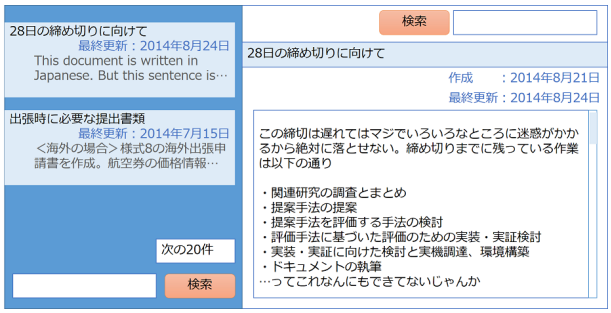

図 4: 暗号技術適用前のサービス画面

4.2　暗号技術の適用

サービス情報とユーザ要求の 2 つを受け取った暗号プロトコル検索エンジンは、暗号プロトコル DB より「データの暗号化」「検索可能暗号」の 2 つのプロトコルを候補として挙げる。次にこれら 2 つのプロトコルについて、利用可能アプリ情報 DB より利用可能なアプリを検索し、「データの暗号化」として JavaScript で利用可能な AES、「検索可能暗号」として尾形らの検索可能対称暗号（Simple-SSE）[1] を得る。JavaScript で利用可能な AES は無償利用が可能であり、Simple-SSE が利用可能な外部サービスは利用可能な上限金額を満たしている。

暗号プロトコル検索エンジンからの回答を受け取ったブラウザ拡張機能は、ユーザ要求に沿っているかを確認し、それぞれのサービス提供者からサービスの提供を受ける。また暗号サービス利用開始に先立ち、Simple-SSE サービスを提供しているサーバと通信を行いサービス開始手続きを行う。手続き終了後、すでにオンラインメモ帳サービスを利用していたのであればこれまでのメモ帳データの暗号化と暗号化インデクスの作成を行い、従来データの破棄と暗号化データの新規登録、暗号化インデクスの送信を行う。Simple-SSE サービスでは手続き依頼に従い、ユーザ用の暗号化インデックスを受領し、暗号化検索クエリの待機状態となる。

続いてサービス情報にしたがい、入力される情報の位置の特定とその情報入力をフックし暗号化し暗号化インデクスも同時に作成するスクリプトの追加を行う。同時に検索が行われる位置を特定しその情報入力をフックし、暗号化検索クエリ作成のスクリプト追加と、検索クエリの送信先をサーバから Simple-SSE サービス提供者に変更する。メモ帳の登録アクションの位置も特定し、登録アクション時にはオンラインメモ帳サーバに暗号化データを送ると同時い、Simple-SSE サービス提供者に対して暗号化インデクスの追加依頼を行う。

さらに、ブラウザ拡張機能は利用者の安心感を高めるために、サービスの利用画面に改良を加える。メモやメモタイトルの表示ゾーンに安心感を増すために緑色の装飾を施す（図 5）。図 6 は拡張機能を利用しなかった場合表示される画面である。

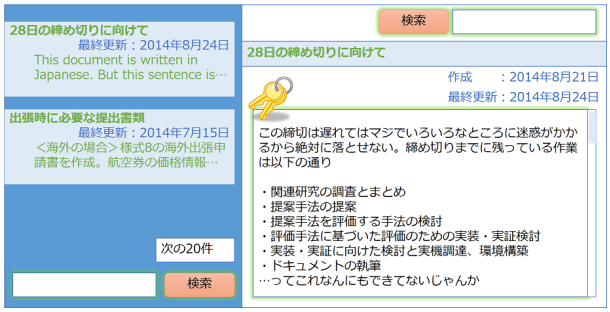

図 5: 暗号技術適用後のサービス画面

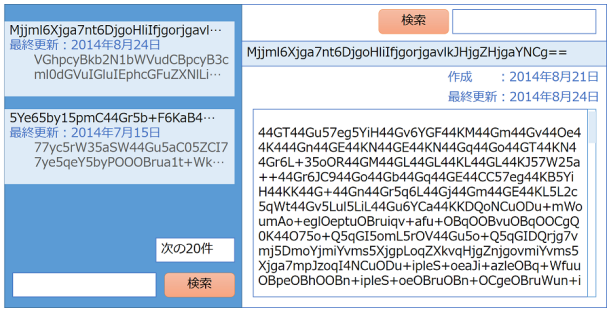

図 6: 暗号技術適用後のサービス画面（拡張機能抜き）

4.3　サービス実装案における前提

本サービス実装案では、多くの前提が置かれている。それらの整理を行い、次章での検討に繋げる。

- オンラインメモ帳サービスは本フレームワークに対応したサービス情報をすでに作成、保持し提供可能な状態となっている
- サービス情報の作成にあたり虚偽の記載や記載漏れがない
- ユーザ要求の記載内容が荒い粒度でもエンジンが検索可能となっている
- Simple-SSE 方式を提供する事業者が存在する
- HTML における情報入力位置の確実な特定が可能になっている

自動適用するためには、サービスの作りがそうなっていないと容易ではない。提案フレームワークが適切に稼働するためには、OS とアプリケーションの間において新たな階層（レイヤ）を用意し、

5　検討点と関連研究

前章でサービス実装案におけるいくつかの前提を示した。これらは提案するフレームワークの実現にあたりより深く検討しなければいけない点が多く含まれている。本章では、提案フレームワークの現実化と実用化に向けて必要な検討点を考察し、それら検討点の解消につながる可能性のある関連研究を紹介する。

5.1　ユーザ要求とサービス要求

ユーザ要求をサービス利用者あるいはサービス開発者が手動で作成をするとすると、暗号技術や脅威に対する知識の違いから記載粒度の違いが起きることが容易に想像される。本方式はそういったユーザに対して容易に適用できるフレームワークとして提案するものであるため、手動でのユーザ要求は避けられるべきである。

ユーザ要求の抽出には、完全な自動化あるいは抽出を補助する機構が考えられよう。自動化や補助機構についても、抽出されたユーザ要求が本当にユーザが要求するものかの保証や責任も考慮しなければならない。

サービス情報についても同様のことが言える。高機能な暗号技術の適用を容易にするためには、保護対象となるサービス情報は詳細に提供されるべきであるが、これらの抽出は暗号技術に対する知識が重要となる。こちらも自動化や補助機構について考慮する必要がある。

高橋らによるセキュリティにおけるサービス品質保証の提案はユーザ要求とサービス情報の抽出の良いヒントとなると考えられる [2]。サービス情報の抽出に対しては、マルウェアや Android アプリケーションを対象に行われているソフトウェアの静的解析や動的解析の手法が適用できる可能性もある。

5.2 暗号プロトコル記述言語と暗号機能一覧

暗号プロトコル記述言語は、プロトコルが持つ特徴と解消あるいは軽減される脅威の双方が過不足なく記載される必要がある。言語の記述能力の議論は、対象となる暗号プロトコルの多くにおいて適用が可能であるかなどの確認が必要となる。さまざまな研究者により提案されている暗号プロトコルは、今後機能がより詳細化されていくことや、新たな機能を提供可能にすることが十分に考えられる。記述言語の策定にあたっては改良することを前提にし、すでに標準化されている暗号プロトコルや広く利用されている暗号プロトコルを当初は対象とするなど代表的なプロトコルを網羅的に表現可能な仕様とするところから始めていくことが妥当であろう。

プロトコル記述に関しては、暗号の基本的機能を細分化した暗号機能一覧よりプロトコルの構成を記載する方法を取っているが、基本的機能の細分化も度合いが生じる。どの程度までの細分化が必要で十分かについては暗号プロトコル表現の過不足性と関係してくると考えられるため、記述言語と同様に機能一覧も改良を前提にした仕様策定をすることが望ましい。暗号プロトコルの記述については、機械処理が可能な方式については著者の調査では見つけることができなかったが、抽象的な表現として暗号プロトコルの表現に挑んだ研究もある [3, 4] がいずれも 10 年以上前の研究であり、表現能力についてはあらためて精査が必要であることに加え機械処理の可能性についてもさらなる検討が必要であると考えられる。

5.3 暗号プロトコルデータベース

暗号プロトコル記述言語により記載された暗号プロトコルのデータベースは、運用面での課題が残る。データベースの管理・運用はどの組織が行い、データベースの入力の判断は誰がどのように行うかは、データベースの質を保つために重要である。データベースの入力候補としてデータが外部より与えられた場合、その情報の正しさはどう判定されるのか、また正確性の担保や新鮮さの保証など、考えるべき事項は多い。また、世の中のすべての暗号プロトコルを随時導入していくことは運用負荷が非常に高く容易ではない。さらに暗号プロトコルは新規の提案だけでなく、攻撃や解析の状況も把握しなければならない。

情報通信研究機構による暗号プロトコル評価技術コンソーシアム（CELLOS）は、データベースとはいかないものの暗号プロトコルの評価についての分析と情報の公開を行っており、注目すべき活動と言える [5].

5.4 実世界との接点

利用者に容易に利用できることを考慮した場合、実世界との接点における自動化の対応を検討する必要が生じる。たとえば電子署名や電子認証に PKI の証明書を利用する場合、証明書取得において本人確認（法人格含む）が必要である。技術的には自動化することも可能であるが、高い保証レベルを求める場合には本人確認の厳格さを保つために対面での確認が求められているため、自動化が困難な場合も生じる。PKI の

証明書だけでなく、本人認証の登録においても同様のことが起きえる。これらについては米国NISTのSP 800-63が詳しい [6]

5.5 暗号技術適用後のインターフェース

本フレームワークにより暗号技術が適用された後のユーザインターフェースについても検討が必要となる。完全な自動化が行われ、ユーザやサービス提供者が本フレームワークに信頼を置いている場合には適用前のインターフェースを変えずに提供することで自然な利用が可能となる。一方で、本フレームワークを全世界のすべてが余すところなく利用するという状況は非現実的であり、信頼できるアプリケーションと信頼確認ができないアプリケーション、本フレームワーク対応アプリケーション、非対応アプリケーションとさまざまなケースに分かれる。その場合、ユーザが持つ不安を解消するために、適用後にサービスの本来目的を妨げることのない範囲で安心感を与えるためのインターフェース変更をする可能性もある。こういったインターフェースについては、電子メールをはじめとするメッセージの暗号化において研究されている分野でもある [7]。

5.6 自動適用の方法

暗号化する箇所や、複数サービスを利用する場合、参加エンティティが増える場合など、ユーザ要求やサービスに応じて柔軟に設定される必要がある。この場合、サービスやアプリ提供者がクライアント側の自動提供を行うことは容易でないと考えられるため、クライアント側の機構が自動適用のための調整作業を行う必要があると考えられる。

6 まとめ

技術的な理解に高い知識が求められる現代の高機能暗号プロトコルに対し、利用側が容易に適用可能なフレームワークを提案した。フレームワークは、暗号プロトコルの記述言語と記述されたプロトコルのデータベースを中心に、ユーザ要求とサービス情報から適用すべき暗号プロトコルを選択するエンジンから構成される。これら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。しかし実現にはまだ多くの課題が残されており、本論文ではフレームワークの提案に加えサンプル実装を行う案を示し、その案をもとに残る課題について考察を行った。

参考文献

[1] W. Ogata, K. Koiwa, A. Kanaoka, S. Matsuo. Toward Practical Searchable Symmetric Encryption. The 8th International Workshop on Security (IWSEC2013), 2013

[2] T. Takahashi, et. al. , Accountable Security Mechanism Based on Security Service Level Agreement. IEEE Symposium on Computers and Communications , 2013

[3] D. Monniaux. Abstracting Cryptographic Protocols with Tree Automata. In Proc. 6th SAS, 1999

[4] I. Cervesato. A Specification Language for Crypto-Protocols based on Multiset Rewriting, Dependent Types and Subsorting. Workshop on Specification, Analysis and Validation for Emerging Technologies - SAVE'01, 2001

[5] 情報通信研究機構. 暗号プロトコル評価技術コンソーシアム CELLOS. https://www.cellos-consortium.org/jp/

[6] W. Burr, et. al. Electronic Authentication Guideline, NIST Special Publication 800-63-2, 2013

[7] S. Ruoti, N. Kim, B. Burgon, T. Horst, K. Seamons. Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes. The ninth Symposium on Usable Privacy and Security (SOUPS2013), 2013