九州大学学術情報リポジトリ
Kyushu University Institutional Repository

端末フィンガープリント情報を用いた鍵乱用を防止可能なハイブリッド暗号化方式

陳, 春璐
九州大学大学院システム情報科学府 | 九州先端科学技術研究所

穴田, 啓晃
九州先端科学技術研究所

川本, 淳平
九州大学大学院システム情報科学研究院 | 九州先端科学技術研究所

櫻井, 幸一
九州大学大学院システム情報科学研究院 | 九州先端科学技術研究所

https://hdl.handle.net/2324/1662063

出版情報：コンピュータセキュリティシンポジウム. 2015, pp.2C2-3-, 2015-10-21
バージョン：
権利関係：

KYUSHU UNIVERSITY

端末フィンガープリント情報を用いた

鍵乱用を防止可能なハイブリッド暗号化方式

陳 春ろ*,*** 穴田 啓晃*** 川本 淳平**,*** 櫻井 幸一**,***

*九州大学大学院システム情報科学府 **九州大学大学院システム情報科学研究院
819-0395 福岡市西区元岡 744 ウェスト 2-712
chenchunlu@itslab.inf.kyushu-u.ac.jp { kawamoto, sakurai } @inf.kyushu-u.ac.jp
***九州先端科学技術研究所
814-0001 福岡市早良区百道浜 2-1-22
anada@isit.or.jp

あらまし インターネットにおいて，デジタルコンテンツの違法な利用の問題が多発している．この問題を解決するため，多くの暗号化方式が提案された．しかし，秘密鍵のコピーや転送などの漏洩を防ぐことが困難であるため，解決には至っていない．すなわち，秘密鍵の不正利用（鍵乱用）の問題が依然としてある．本論文では，端末フィンガープリント情報を用いた鍵乱用を防止できるハイブリッド暗号方式を提案する．この方式は，入手や変更ができないと仮定した端末のフィンガープリント情報を利用して再暗号化鍵を生成することから，たとえ利用者が秘密鍵を漏洩させた場合であっても，その秘密鍵は再暗号化鍵を生成した端末以外では動作しないことを保証できる．

キーワード：秘密鍵，不正利用，ハイブリッド暗号， 再暗号化

A Key-Misuse-Resistant Hybrid Encryption Scheme

using Terminal Fingerprint

Chunlu CHEN†‡ Hiroaki ANADA ‡ Junpei KAWAMOTO†‡ Kouichi SAKURAI†‡

†Kyushu University
744, Nishi-ku, Fukuoka Motooka, 819-0395, JAPAN
chenchunlu@itslab.inf.kyushu-u.ac.jp { kawamoto, sakurai } @inf.kyushu-u.ac.jp
‡Institute of Systems, Information Technologies and Nanotechnologies
2-1-22 , Sawara-ku, Fukuoka Momochihama, 814-0001, JAPAN
anada@isit.or.jp

Abstract Internet services raise an issue of illegal copying and distribution of digital contents. A lot of public key encryption schemes solve this issue. However, the secret key is not completely protected i. e. these kinds of encryption methods do not prevent illegal copying and distribution of secret keys. In this paper, we propose a key-misuse-resistant hybrid encryption scheme using terminal fingerprint. Since the terminal fingerprint is assumed to be unchangeable and unknowable, we ensure that our secret keys are valid in the terminal where such secret keys were created.

Keyword: Key-misuse-resistant, Terminal fingerprint, Hybrid encryption

1　はじめに

インターネットの高速化にともない，ストレージコストの削減並びにデータ共有のため第三者が管理するクラウドサーバへデータを保存することが増えている．しかし，第三者が管理するクラウドサーバは，一般的に完全に信頼することは難しく運用の問題により情報が漏洩する危険性がある．そのため，クラウドサーバへ保存するデータの機密性を保証する必要がある．通常，この目的のためには，クラウドサーバへ保存するデータをクライアント上で予め暗号化しておく方法が取られることが多い．しかしながら，伝統的な公開鍵暗号方式では，秘密鍵(SK)と公開鍵(PK)がペアとして利用されている．公開鍵暗号方式は安全性が高くなるが，鍵ペアの数が多い場合は管理の複雑性も高くなる．

公開鍵暗号方式は，メッセージを暗号化してコピーや転送など行動を無意味にする，メッセージの安全性を保証することができる．しかし，秘密鍵のコピーや転送による不正利用を防ぐことは依然に困難である．すなわち，不正ユーザから秘密鍵をコピーすることが可能である．そして，秘密鍵が漏洩した場合は責任者を判断することも困難である．鍵乱用を防止するために，近年様々な暗号方式が提案されている． 例えば，秘密鍵を生成するとき，ユーザの固有情報を利用して正当ユーザを判断する暗号方式が提案された．近い将来に暗号方式の発展として秘密鍵の漏洩問題が解決されることを期待している．現在ではユーザの固有情報は次の三つの関連技術が導入されている．

ハードウェア認定

物理的にクローニングできない機能はチップの製造プロセスと物理装置によって差分を抽出して使用する．そして，この差分は必ずチップ毎に異なる．同時に，この差分はチップの固有情報として測不可能となる．これを利用して秘密鍵を生成する[1]．ハードウェア認証システムは，ランダムコードを受信し，応答として固有のランダムコードを生成する．製造工程の違いによって生成されたチップは，コピーすることができない．

Kumar らは特定の入力を提供してチップの出力が異なる特性を用いて，出力の定義を設計して物理的クローニングできない機能を持つシステムを提案した[2]．チップの出力の唯一性によれば，現代社会で広く利用することが可能である．例えば，スマートカード，銀行カードに利用することができる．このように，我々の提案では，秘密鍵の唯一性を用いることで，コピーや他の違法行為からメッセージやキャッシュなどを保護することができる．

生体認証

生体認証技術は，コンピュータや光学，音響，バイオセンサーおよびその他のハイテクツールを利用して人の身体の自然な生理的特徴を取得すること（例えば，指紋，静脈，顔，虹彩など）と人の行動特徴を取得すること（例えば，手書き，音声，歩き方など）である．生体認証技術は個人の身元の特徴を利用しるので，優れたセキュリティ性能を持っており，どこでも使用することが簡単にできる[3]．また，生体認証は，ユニークな不変の秘密鍵として使用することができるが，更新ができないといった問題も深刻になっている．

Jain，Anil らはさまざまな生体認証システムを分析して評価を行った[4]．また，Uludag らは生体認証を利用してデジタル著作権管理システムを構築した[5]．生体認証は様々な分野で利用することが可能である．

実際，生活の中で，生体認証は非常に広く応用されている．たとえば，銀行カードの指紋認証，顔認証など便利な利用があるが，生体情報のプライバシー保護は重要な研究課題となっている．

端末フィンガープリント

一般に，端末情報（例えばコンピュータメモリ量，CPU 情報，アカウント情報，ブラウザフィンガープリントなど）というのは，端末の様々な固有情報である(以降，端末フィンガープリントと呼ぶ)．端末フィンガープリントは端末のメモリ量，アカウント情報，インストールされたソフト情報な

どを用いており，ユーザの習慣や興味によって決定される.従って，端末毎に異なる．ここでブラウザフィンガープリントを端末フィンガープリントの一部として説明する．ブラウザフィンガープリント情報はブラウザが有する機能(**ブラウザ情報**, **インストールされたソフトなど**)の様々なセットであり[6,7,8]，端末を識別するための特徴として用いることができる．そして，いろいろな場所で**応用されることも可能である**．本論文では，端末フィンガープリントが不変かつ抽出不可能であると仮定した上で提案する．

ハードウェア認証と生体認証方法は，キーの唯一性を保証することができるが，まだ鍵の安全性を保証することはできない．ハードウェア認証の更新は可能であるが，ハードウェア自体の更新を必要とするためシステムのコストも増大させる．生体認証は，変更することは不可能であるが，生体情報の保護は考えなければならない．

上記問題を考慮し，本論文は端末フィンガープリント情報を利用する．端末フィンガープリント情報はユーザ毎に異なるので，この情報を利用すれば，不正ユーザの結託攻撃を受けでも，正しい情報を手に入れない場合は復号できない．そして，本提案方式では，ユーザの端末フィンガープリント情報は秘密鍵として利用するので，外部に公開されることはない．従って，ユーザ自身から転送しない限りは秘密鍵の安全性も保証できる．

本論文では，共通鍵暗号化と二つの公開鍵暗号方式で構成された，鍵乱用を防止できるハイブリッド暗号化方式を提案する．端末フィンガープリント情報のハッシュ値は，第2の公開鍵方式における秘密鍵として利用する．そして，ウォーターズの CP-ABE 暗号方式[9]は最初の暗号化方式として，任意の公開鍵暗号方式と組み合わせて利用する．提案方式のスキームは，唯一な秘密鍵を生成するため，端末フィンガープリント情報を利用するだけではなく，システムの低コストを維持するため，ユーザ自分自身で端末フィンガープリント情報のハッシュ値を更新することもできる．

本論文は以下のように構成されている．第 2 節では，背景情報，正式な定義と CP-ABE 方式を導入する．第3節では，本提案方式の暗号化方式を説明する．第4節では提案方式のセキュリティと利点について説明する．最後に，結論とセクションとを検討する．

2 背景

提案した方式で利用している準備知識を紹介する．

2.1 双線形写像

G_1, G_2を素数位数 p の有限巡回群とする．G_1 の生成元$g \in G_1$, 任意の$\mathrm{a}, b \in Z_p$ に対し，双線形写像e: $G_1 \times G_1 \rightarrow G_2$ は以下の 二つの性質を満たす．

1. 双線形性:すべての$u, v \in G_1$と$\mathrm{a}, b \in Z_p$に $e(u^a, v^b) = e(u, v)^{ab}$を満たす
2. 非退化性:$e(g, g) \neq 1$

2.2 アクセス構造と線形秘密分散法

ここではアクセス構造と線形秘密分散法(LSSS)[10]の定義を説明する．

定義 1(アクセス構造)．$P = \{P_1, P_2, \ldots, P_n\}$は属性の集合として，もし$\Gamma$は下で閉じているスーパーセットの場合， $\Gamma \subset 2^P$が単調になる．すなわち，$\forall B, C$の場合，もし$B \in \Gamma$と$B \subset C$なると，$C \in \Gamma$となる．アクセス構造(それぞれ，単調構造を評価する)は，P の空でない部分集合のコレクションΓ(それぞれ，単調コレクション)である．すなわち $\Gamma \subset 2^P / \{\emptyset\}$ である．Γのメンバーは権限セットと呼ばれ，Γでいないメンバーのセットは権限外セットと呼ばれる．

定義 2(線形秘密分散方式(LSSS)[10])秘密分散法 $\prod$に対して権限セット $\boldsymbol{P}$ は(Z_pオーバー)線形と呼ばれる．

1. 権限セットの各参加者はZ_pから秘密を貰える．
2. 秘密分散法 $\prod$のため$\ell \times n$ の行列 M を生成して．すべて $i = 1, \ldots, \ell$, は M の i 番目の行である．関数 ρ を利用して， $\rho(i)$と参

加者マークを定義する．列ベクトル $\boldsymbol{v} = (s, r_2, \ldots, r_n)$の中で，$s \in Z_p$は共有する秘密である．ランダムに$r_2, \cdots, r_n \in Z_p$を選択して，秘密分散法 $\prod$において秘密 s を分散する $M\boldsymbol{v}$ は ℓ のベクトルで表示する．シェア $M\boldsymbol{v}$ は参加者 $\rho(i)$ に属している．

ここで$\prod$はΓで構成される線形秘密分散方式(LSSS)である．S は権限が持つユーザの属性とする．そして，定義 $I \subset \{1,2,\ldots,\ell\}$は$\{i;\ \rho(i) \in S\}$となる．$\prod$に対して，構造$\{\omega_i \in Z_p\}$が存在する．そして，$\{\lambda_i\}$は任意の秘密 s の有効なシェアなら，式$\sum_{i \in I} \omega_i \lambda_i = s$が成立する．

2.3 暗号文ポリシー属性ベース暗号

暗号文ポリシー属性ベース暗号[9]はある1つの暗号文に対して復号可能なユーザが複数存在できる，アクセス制御の柔軟性も高くなる暗号方式である．ここでは，暗号文ポリシー属性ベース暗号に関する関連研究を紹介する．Cheung と Newport[11]は DBDH 問題に基づく最初の CPA 安全の CP-ABE 方式を構築した．そして，システム属性とユーザの属性を計算・関連してユーザ秘密鍵を生成するという CHK 技術[12]を利用して CCA 安全も実現した．Naruse ら [13]は再暗号化を利用して新しい CP-ABE メカニズムを提案した．その提案方式は，暗号文を作成するために CP-ABE スキームに基づいて，メッセージを保護するため再暗号化の段階を増加した．Li ら[14]が提案した暗号化方式は，信頼可能な第三者から認証書を発行して，ユーザの秘密鍵の中に認証情報を含めて，復号するとき認証を行うという提案方式で，CP-ABE 方式より安全性が高くなる．しかし，第三者の計算量が大きいという欠点があり，実装することが難しい．2009 年に Li ら[15]が提案した暗号化方式は，ユーザの ID を‘属性’に含み込んで，復号するとき認証を行うという提案方式で，暗号方式の安全性が高くなる．しかし，鍵発行センタは鍵の管理作業量が高くなる．Hinek ら[16]は第三者サーバで発行されたトークンを利用して，鍵のコピーを無効化する手法を提案している．

本提案方式では，信頼できる第三者サーバを用いずとも安全性を保証できる暗号方式を目指している．秘密鍵に関連付けられている属性集合が，暗号文に関連付けられているアクセス構造を満たす場合のみ，その秘密鍵によって暗号文を復号することができる．

暗号文ポリシー属性ベース暗号では Setup, Encrypt, KeyGen, と Decrypt 四つのアルゴリズムで構成されている．

$\mathrm{Setup}(\lambda, U) \rightarrow (PK, MK)$：セキュリティパラメータλと属性集合 U を入力する．公開鍵 PK とシステムのマスター秘密鍵 MK を出力する．

$\mathrm{Encrypt}(PK, M, W) \rightarrow CT$：公開鍵 PK とメッセージ M とアクセス構造を入力する．暗号文 CT 出力する．

$\mathrm{KeyGen}(MK, S) \rightarrow SK$：システムのマスター秘密鍵 MK とユーザの属性集合 S を入力する．秘密鍵 SK を出力する．

$\mathrm{Decrypt}(CT, SK) \rightarrow M$：暗号文 CT とユーザの秘密鍵 SK を入力する．もし秘密鍵に関連付けられている属性集合が，暗号文に関連付けられているアクセス構造を満たすなら，メッセージ M を出力する．

3 システムのモデル

本節では，端末フィンガープリント情報を用いて鍵乱用を防止するハイブリッド暗号方式を提案する．そこで，鍵乱用を防ぐ属性ベースの暗号方式を提案する．最後に，端末フィンガープリント情報を用いて鍵乱用を防止するハイブリッド暗号方式の具体的な実現を提供する．

提案方式は「ユーザ」，「情報管理センタ」，「コンテンツ所有者」で構成される．

「ユーザ」：自分の情報を提供することとコンテンツを正当的に利用する．そして，自分がもっているブラウザフィンガープリント情報を管理する．

「情報管理センタ」：システム内の属性情報とブラウザフィンガープリント情報を管理し，暗号化に必要な鍵を公開している，ユーザの属性情報が含まれている秘密鍵を発行する．

「コンテンツ所有者」：コンテンツを暗号化する．

3.1　提案方式

提案の HybENC は，共通鍵暗号方式(CKE)，二つの公開鍵暗号方式(PKE1，PKE2)とハッシュ関数 H から成り $\mathrm{HybENC} = (\mathrm{CKE}, \mathrm{PKE1}, \mathrm{PKE2}, H)$と書ける．通常の適用方法と同じく CKE は写真やビデオのような大きなサイズのコンテンツデータを効率的に暗号化するため使用する．PKE1 は CKE の共通鍵を暗号化する．PKE1 としては任意の公開鍵暗号方式を利用できる．最後に PKE2 を利用して CKE の共通鍵の再暗号化を行う．ここで，端末フィンガープリント情報のハッシュ値を PKE2 の秘密鍵とし対応する公開鍵を計算する．構成を示す．

HybENC. $\mathbf{Key}(\boldsymbol{\lambda}) \rightarrow \mathbf{FK}, (\mathbf{PK1}, \mathbf{SK1}), (\mathbf{PK2}, \mathbf{SK2})$: この鍵生成アルゴリズムは，セキュリティパラメータ λ と端末フィンガープリント情報 fp を入力とし，次の計算を行う．$\mathrm{CKE.Key}(\lambda) \rightarrow \mathrm{FK}$，$\mathrm{PKE1.Key}(\lambda) \rightarrow (\mathrm{PK1}, \mathrm{SK1})$，$H_\lambda(\mathrm{fp}) \rightarrow \mathrm{SK2}$，$\mathrm{PKE2.Key}(\mathrm{SK2}) \rightarrow \mathrm{PK2}$．ここで，CKE. Key, PKE1. Key, PKE2. Key はそれぞれの暗号方式における鍵生成アルゴリズムを表す．出力は共通鍵 FK，鍵ペア $(\mathrm{PK1}, \mathrm{SK1})$，鍵ペア $(\mathrm{PK2}, \mathrm{SK2})$である．

HybENC. $\mathbf{Enc}(\mathbf{FK}, \mathbf{PK1}, \mathbf{PK2}, \boldsymbol{m}) \rightarrow \mathbf{CT}, \mathbf{CT2}$: この暗号化アルゴリズムは鍵$\mathrm{FK}, \mathrm{PK1}, \mathrm{PK2}$と平文 m を入力とし，次の暗号化を実行する．$\mathrm{CKE.Enc}(\mathrm{FK}, m) \rightarrow \mathrm{CT}$，$\mathrm{m1}=\mathrm{FK}$ としておいて $\mathrm{PKE1.Enc}(\mathrm{PK1}, \mathrm{m1}) \rightarrow \mathrm{CT1}$，$\mathrm{m2} = \mathrm{CT1}$とおいて$\mathrm{PKE2.Enc}(\mathrm{PK2}, \mathrm{m2}) \rightarrow \mathrm{CT2}$．ここで，CKE. Enc, PKE1. Enc, PKE2. Enc はそれぞれの暗号方式における暗号化アルゴリズムを表す．出力は暗号文$\mathrm{CT}, \mathrm{CT2}$である．

HybENC. $\mathbf{Dec}(\mathbf{FK}, \mathbf{SK1}, \mathbf{fp}, \mathbf{CT}, \mathbf{CT2}) \rightarrow \boldsymbol{m}$: この復号アルゴリズムは鍵$\mathrm{FK}, \mathrm{SK1}$，端末フィンガープリント情報 fp及び暗号文 $\mathrm{CT}, \mathrm{CT2}$を入力とし，次の復号を実行する．$H_\lambda(\mathrm{fp}) \rightarrow \mathrm{SK2}$ ，$\mathrm{PKE2.Dec}(\mathrm{SK2}, \mathrm{CT2}) \rightarrow \mathrm{m2}, \mathrm{CT1} = \mathrm{m2}$ としておいて$\mathrm{PKE1.Dec}(\mathrm{SK1}, \mathrm{CT1}) \rightarrow \mathrm{m1}, \mathrm{FK} = \mathrm{m1}$とおいて$\mathrm{CKE.Dec}(\mathrm{FK}, \mathrm{CT}) \rightarrow m$．ここで，CKE. Dec, PKE1. Dec, PKE2. Dec はそれぞれの暗号方式における復号アルゴリズムを表す．出力は平文mである．

上記のように，提案方式は端末フィンガープリント情報fpのハッシュ値を，再暗号化のための公開鍵暗号PKE2の秘密鍵SK2として利用している．ただし，復号アルゴリズムでは，その実行の度に，端末フィンガープリント情報fpから秘密鍵SK2が計算されるものとする．

3.2　提案方式

本提案では，暗号文ポリシー属性ベース暗号方式のうえで再暗号化を行うハイブリッド暗号方式を構築する．平文は属性情報と端末フィンガープリント情報を用いて暗号化される．この方式のメリットは，端末フィンガープリント情報の確認が許可されたユーザ以外で利用することが困難な点である．

3. 1 節のようにハイブリッド暗号で PKE1 として暗号文ポリシー属性ベース暗号方式を利用することによって，本提案方式を説明する．

提案では，ユーザ集合は$\mathrm{U} = \{1,2,\cdots,n\}$とする，すべての属性集合は$\mathrm{A} = \{1,2,\cdots,\ell\}$とする．ランダムに$s \in Z_p$を選択して，暗号化過程で利用する．

– $\mathrm{DO.\ Setup}(\boldsymbol{v}, \boldsymbol{w}) \rightarrow \mathbf{FK}$:セキュリティパラメータv と w を入力する．素数 p，(Z/Z_p)の生成元は$q\ mod\ p$として，共通鍵 FK

$$\mathrm{FK} = (q^v)^w\ mod\ p = (q^w)^v\ mod\ p$$

を出力する．

– $\mathrm{C.\ Enc}(\mathbf{FK}, \boldsymbol{m}) \rightarrow \mathbf{CT}$:共通鍵 FK と平文を入力する．暗号文 CT

$$\mathrm{CT} = (\mathrm{M}, \mathrm{FK})$$

を出力する．暗号文 CT と共通鍵 FK を情報管理センタに送信する．

–$\mathrm{Auth.\ Setup}\ (\boldsymbol{\lambda}) \rightarrow \mathbf{PK}, \mathbf{MK}$:セキュリティパラメータ λ を入力とする．システム全体の属性を$\mathrm{U} = \{1, \ldots n\}$とする．素数$p$，素数位数$p$の群 G_1, G_2，生成元$p \in G_1$，双線形写像 $e: G_1 \times G_1 \rightarrow G_2$を選ぶ．乱数 $a, b \in Z_p$ とハッシュ関数$\mathrm{H}: \{0,1\}^* \rightarrow G_2$ を利用して，公開鍵

$$\mathrm{PK}=g, g^b, e(g,g)^a$$

とシステムのマスター秘密鍵

$$\mathrm{MK}=g^{a}$$

を出力する.

–Auth. Ext($\mathbf{MK}, \boldsymbol{S}$) → $\mathbf{SK}$:マスター鍵 MK とユーザの属性集合 S を入力する. まず, 各ユーザに$t \in Z_p$ をランダムに選び, 秘密鍵 SK

$$SK = \left(g^{a+bt}, g^{t}, (K_X)_{X\in S}\right),$$

$$\forall_{X\in S}\ K_X = H(X)^{t}$$

を出力する.

–U. Setup($\mathbf{SK}, \boldsymbol{f}$) → $\mathbf{F}, \mathbf{D}$:ユーザは端末フィンガープリント情報 fのハッシュ値$H(f) = D$(本論文では RSA 暗号方式を利用する)を計算して, 二つの大きな素数p, qを選んで, $N = pq$を計算する. $DE \equiv 1 \bmod (p-1)(q-1)$を成り立つため e を計算する. ユーザの端末フィンガープリント公開鍵は$F = (N, E)$として, 秘密鍵 Dは自分自身で保存する.

–Auth. Enc($\mathbf{PK}, \mathbf{FK}, \boldsymbol{W}$) → $\mathbf{FT}$:システム公開鍵 PK, 共通鍵 FK, すべての属性を用いてアクセス構造(W, ρ)とメッセージ Mを入力する.

ここで, W は$\ell \times n$行列である. まず, アルゴリズムはランダムにベクトル$\boldsymbol{\gamma} = (s, y_2, \cdots, y_n) \in Z_p^n$と$r_1, r_2, \cdots, r_\ell \in Z_p$を生成する. ベクトルは共有する秘密の暗号指数 s として利用する. その中でW_iは W の i 行目に対応するベクトルであり, $\lambda_i = \boldsymbol{\gamma} \cdot W_i$に 1 から$\ell$まで計算される. 暗号文 FT

$$\mathrm{FT} = (FKe(g,g)^{as}, g^{s}, \widehat{Cs})$$

$$\widehat{Cs} = \left(g^{b\lambda_1} H(X_{\rho_1})^{r_1}, g^{r_1}\right), , \left(g^{b\lambda_\ell} H(X_{\rho_\ell})^{r_\ell}, g^{r_\ell}\right)$$

を出力する.

–Auth. ReEnc($\mathbf{FT}, \mathbf{F}$) → $\mathbf{FT}'$:暗号文 FT と端末フィンガープリント情報公開鍵 F を入力として, 再暗号文 FT′

$$\mathrm{FT}' = (\mathrm{FT})^{\mathrm{E}} \bmod N,$$

$$(\mathrm{FT})^{\mathrm{E}} = (FKe(g,g)^{as\mathrm{E}}, g^{s\mathrm{E}}, (\widehat{Cs})^{\mathrm{E}})$$

を出力する.

–U. Dec($\mathbf{FT}', \boldsymbol{D}$) → $\mathbf{FT}$:再暗号文 FT′ と端末フィンガープリント情報秘密鍵 D を入力として, 復号計算は次のように計算する.

$$(\mathrm{FT}')^{D} = (\mathrm{FT}^{\mathrm{E}})^{D} = \mathrm{FT} \bmod N.$$

–U. ReDec($\mathbf{FT}, \mathbf{SK}$) → $\mathbf{FK}$:暗号文 FT と秘密鍵 SKを入力として, 各正当ユーザの秘密鍵はアクセス構造ツリー(W, ρ)を満たす. 定義 $I \subset \{1,2,\ldots,\ell\}$は$\{i;\ \rho(i) \in S\}$となる. Πに対して, 構造$\{\omega_i \in Z_p\}$が存在する. そして, $\{\lambda_i\}$は任意の秘密 s の有効なシェアなら, 式$\sum_{i\in I} \omega_i \lambda_i = s$が成立する. 再復号計算は次のように計算する.

$$\frac{\mathrm{e}\left(g^{s}, g^{a+bt}\right)}{\prod_{i\in I}\left(e\left(g^{b\lambda_i} H(X_{\rho_i})^{r_i}, g^{t}\right) e\left(H(X_{\rho_i})^{t}, g^{r_i}\right)\right)^{\omega_i}}$$

$$= \frac{\mathrm{e(g,g)}^{as}\mathrm{e(g,g)}^{bts}}{\prod_{i\in I} e(g,g)^{bt\omega_i\lambda_i}} = e(g,g)^{as}$$

$$\frac{FKe(g,g)^{as}}{e(g,g)^{as}} = FK$$

–C. Dec($\mathbf{FK}, \mathbf{CT}$) → $\boldsymbol{m}$: 共通鍵 FK と暗号文 C を入力して, 平文を復号する.

4 安全性の検討

本論文では,暗号化された共有データの機密性が保護されていることと, 提案方式において秘密鍵が明らかにできないことを示した. 提案手法は暗号文ポリシー属性ベース暗号方式と同じ選択平文攻撃に対して安全である. 提案方式も選択平文攻撃に対して安全である. 暗号化したデータが公開されている場合は, 本提案方式も, ユーザからの結託攻撃に抵抗できる. 攻撃者は正当ユーザの端末フィンガープリント情報を知らないうえ, 秘密鍵を取得することができない.

本研究では, セキュリティを向上させるために再暗号システムを提案した. 従来の暗号方式ではサーバに暗号文と秘密鍵の両方を送信する必要がある. それに対し, 本提案では, ユーザは個人情報を使用して秘密鍵と再暗号鍵を生成する. また, サーバに再暗号鍵を送信する. そして, ユーザは秘密鍵を保持し, サーバは再暗号鍵を利用して暗号文の再暗号化をおこなう. 最後に,サーバは再暗号文をユーザに送信する.

ユーザは自分がもっている秘密鍵を利用して復号を行う.

提案した暗号方式はユーザの属性とユーザの端末フィンガープリント情報を利用する. ユーザは自身の属性情報を自由に変更できるが, 端末フィンガープリントは変更もできず直接その値を知ることもできないと仮定する. また, 鍵生成や暗号, 復号を行うプログラムのみフィンガープリントの値を取得でき, かつこのプログラムは信頼できるものとする端末. 今回の提案方式は前述条件に基づく構築する. ここで, 端末フィンガープリント情報はユーザ毎に異なる. ユーザ ID として利用でき, ユーザ自身情報の匿名性を保障できる. 端末フィンガープリント情報の利用は秘密鍵の転送などの不正行動を無意味となる. 正当ユーザが持っている秘密鍵には, 自分の端末フィンガープリント情報が含まれているので, 他の端末でフィンガープリント情報が異なると, 秘密鍵は失効する. このように秘密鍵の安全性が高くなる.

今回は, 端末フィンガープリント情報を用いた鍵乱用を防止可能なハイブリッド暗号化方式を提案した. また, 提案方式は秘密鍵の更新,削除することは簡単に実現できる. そして, 暗号方式の安全性を保証できる. また, ユーザを認証するための信頼できる第三者は必要ない. この方式では, 秘密鍵の生成と保存はユーザ自身で完結する.

本提案方式では, 各ユーザが鍵管理センタに暗号化された端末フィンガープリント情報を提供する必要がある. 同時にユーザのアクセス数が多い場合には, 管理センタの負荷も非常に重くなる. 将来的には, 再暗号化と再復号化の計算の複雑性を減らすことが研究の課題の一つである.

最後に, 提案システムはユーザが秘密鍵を譲渡あるいは漏洩させた場合であっても, その秘密鍵は鍵ペアを生成した端末以外では動作しないことを保証する.

5 まとめ

本研究では, ユーザ端末フィンガープリント情報を公開鍵と秘密鍵ペアを生成して利用する. さらに,端末フィンガープリント情報を用いて秘密鍵の更新をできる暗号方式を提案した. その結果として, 秘密鍵を漏洩させた場合であっても, 鍵ペアを生成した端末以外では不正利用が困難となる.

本提案は暗号化と復号化に要する計算量は増加している. この点は今後の課題として研究を続ける. また, 提案方式のセキュリティ問題では, ユーザがインターネットに接続している場合, 端末フィンガープリント情報が攻撃者によって盗聴される可能性がある. したがって, この問題を軽減する適切な解決策も検討するべきである.

謝辞

第 2 著者は日本学術振興会科学研究費補助金に部分的に支援されている(研究課題番号 15K00029). 第 4 著者は日本学術振興会科学研究費補助金に部分的に支援されている(研究課題番号 15H02711).

参考文献

[1] Suh, G. Edward, and Srinivas Devadas. "Physical unclonable functions for device authentication and secret key generation." *Proceedings of the 44th annual Design Automation Conference*. ACM, 2007.

[2] Kumar, Sandeep S. , et al. "The butterfly PUF protecting IP on every FPGA." *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*. IEEE, 2008.

[3] Jain, Anil, Lin Hong, and Sharath Pankanti. "Biometric identification." *Communications of the ACM* 43. 2 (2000): 90-98.

[4] Jain, Anil K. , Karthik Nandakumar, and Abhishek Nagar. "Biometric template security." *EURASIP Journal on Advances in Signal Processing* 2008 (2008): 113.

[5] Uludag, Umut, et al. "Biometric cryptosystems: issues and challenges." *Proceedings of the IEEE* 92. 6 (2004):

948-960.

[6] W. C. Nick Doty. (24 Feb 2015). *Fingerprinting Guidance for Web Specification Authors (Unofficial Draft)*. Available: http://w3c. github. io/fingerprinting-guidance/

[7] Aggarwal, Gaurav, et al. "An Analysis of Private Browsing Modes in Modern Browsers." *USENIX Security Symposium*. 2010.

[8] Eckersley, Peter. "How unique is your web browser?." *Privacy Enhancing Technologies*. Springer Berlin Heidelberg, 2010.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Security and Privacy, 2007. SP'07. IEEE Symposium on*, 2007, pp. 321-334.

[10] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography-PKC 2011*, ed: Springer, 2011, pp. 53-70.

[11] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proceedings of the 14th ACM conference on Computer and communications security*, 2007, pp. 456-465.

[12] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *Advances in Cryptology-Eurocrypt 2004*, 2004, pp. 207-222.

[13] T. Naruse, M. Mohri, and Y. Shiraishi, "Attribute Revocable Attribute-Based Encryption with Forward Secrecy," presented at the Proc. of the 2014 information processing society of Japan, Japan, 2014.

[14] J. Li, K. Ren, and K. Kim, "A2BE: Accountable Attribute-Based Encryption for Abuse Free Access Control," *IACR Cryptology ePrint Archive,* vol. 2009, p. 118, 2009.

[15] J. Li, K. Ren, B. Zhu, and Z. Wan, "Privacy-aware attribute-based encryption with user accountability," in *Information Security*, ed: Springer, 2009, pp. 347-362.

[16] Hinek, M. Jason, et al. "Attribute-Based Encryption with Key Cloning Protection." *IACR Cryptology ePrint Archive* 2008 (2008): 478.