IDベースグループ検索可能暗号の安全性について

吉田岳史[1,a)]　江村恵太[1,2,b)]

概要：公開鍵検索可能認証暗号 (PAEKS: Public Key Authenticated Encryption with Keyword Search (Huang, Li (Information Sciences 2017)) では, 受信者がキーワードを検索する際, 送信者の公開鍵を指定してトラップドアを作成する. そのため, 検索効率が送信者数に比例するという問題がある. そこで Wang ら (IEEE Transactions on Information Forensics and Security 2024) は, ID ベースグループ検索可能暗号 (IBGEKS: Identity-Based Group Encryption With Keyword Search) を提案した. 送信者グループを定義, グループの誰が作成した暗号文かに依存せず検索が可能なトラップドアを生成することで, 検索の効率化を図っている. 本論文では, Wang らの IBGEKS 方式に対する攻撃を 2 つ提案する. 提案攻撃ではトラップドアが BLS 署名 (Boneh, Lynn, Shacham (ASIACRYPT 2001)) であることに着目した. 提案攻撃 1 では送信者をグループに登録するための登録オラクルを通じて, 提案攻撃 2 ではトラップドアオラクルを通じて BLS 署名の検証鍵相当を取得することで, トラップドアからキーワードに関する情報が漏れていることを示す. さらに提案攻撃 1 の一般化として, IBGEKS 方式が正当性を満たす場合, 攻撃者が登録オラクルにアクセス可能なモデルで安全な IBGEKS 方式は実現不可能であることも示す.

キーワード：ID ベースグループ検索可能暗号, 公開鍵検索可能認証暗号

On the Security of Identity-Based Group Encryption With Keyword Search

Takeshi Yoshida[1,a)]　Keita Emura[1,2,b)]

Abstract: In public key authenticated encryption with keyword search (PAEKS) (Huang and Li, Information Sciences 2017), each trapdoor is designated to a sender. Thus, a receiver needs to generate trapdoors for all senders even the receiver searches a keyword, and the search complexity depends on the number of senders. To solve the issue, Identity-Based Group Encryption With Keyword Search (IBGEKS) has been proposed (Wang et al., IEEE Transaction on Information Forensics and Security 2024). IBGEKS defines a sender group, and each trapdoor is designated to the group and works for searching against ciphertexts generated by a group member. In this paper, we give two keyword guessing attacks against their IBGEKS scheme where information of keyword is revealed from a trapdoor. We focus on the fact that a trapdoor is a Boneh-Lynn-Shacham (BLS) signature (ASIACRYPT 2001) where a keyword is a message to be signed. In both attacks, we construct an adversary that obtains a quasi-verification key of the BLS signature scheme via either the register oracle (that returns a sender's secret key) or the trapdoor oracle (that returns a trapdoor). We also generalize the first attack: if IBGEKS provides correctness, then no secure IBGEKS exists when an adversary is allowed to access the register oracle.

Keywords: Identity-Based Group Encryption With Keyword Search. Public Key Authenticated Encryption with Keyword Search

[1] 金沢大学
Kanazawa University
[2] 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology (AIST)
[a)] y0xxss1@stu.kanazawa-u.ac.jp
[b)] k-emura@se.kanazawa-u.ac.jp

1. はじめに

PEKS とキーワード推測攻撃. 暗号化されたキーワードを検索可能な公開鍵検索可能暗号 (PEKS: Public Key Encryption with Keyword Search) が Boneh ら [4] により提案されている. PEKS において, 送信者は受信者の公開鍵を用いてキーワードを暗号化する. 受信者は検索時, 自身の秘密鍵と検索キーワードを用いてトラップドアを作成する. サーバーは受け取った暗号文とトラップドアを入力とするテストアルゴリズムを実行する. 暗号化されたキーワードとトラップドアに紐づいたキーワードが一致する場合, テストアルゴリズムは 1 を出力する.

ここで受信者の公開鍵を用いれば, 誰でも自身が選んだキーワードの暗号文を作成可能であることに注意されたい. そのため, トラップドアを持つ攻撃者がそのトラップドアに紐づいたキーワードを推測可能となる. 具体的に, 任意のキーワードの暗号文を作成し, 攻撃対象のトラップドアを用いてテストアルゴリズムを実行することで, このキーワードがトラップドアに紐ついているかどうかを判定することが可能となる. この攻撃をキーワード推測攻撃 (KGA: Keyword Guessing Attacks) と呼ぶ. トラップドアからキーワードの情報が漏洩するということは, 受信者がどんなキーワードで検索を行っているかという情報が漏洩することとなる. さらに検索可能暗号の文脈では, キーワードのエントロピーは低く, かつその数は比較的少ない場合を想定することが一般的である. そのため, 上記識別にとどまらず, 検索キーワードの復元も可能であると想定される. 例えば Oxford English Dictionary (the second edition of the 20-volume) には 171,476 語 (in current use) が収録されている.[*1] $2^{18} = 262,144$ 程度でこの語数をカバーする. 英語キーワードを用いる前提ではあるが, 攻撃者はトラップドアに紐付いたキーワードを 2^{18} 回程度の施行で復元可能となる. これは通常の 128 ビット安全性と比較して非常に少ない計算量で攻撃が可能であることを示している.[*2] さらに検索に用いるキーワードはランダムに選ばれるわけではなく, 偏りがあると考えるのが妥当と言える. そのため, 実際は 2^{18} より少ない計算量で攻撃が可能であると想定される. これらの状況を鑑み, 検索可能暗号として KGA 耐性を持つことが望ましい.

PAEKS と検索効率. KGA 対策として, 公開鍵検索可能認証暗号 (PAEKS: Public Key Authenticated Encryption with Keyword Search) が Huang ら [13] により提案されている. PAEKS では暗号化に送信者の秘密鍵を使用する. 送信者秘密鍵を持たない攻撃者に対し, 任意のキーワードに対する暗号文の作成を防ぐことで, KGA 耐性を持たせることが可能となる.

PAEKS ではトラップドア作成時に受信者の秘密鍵に加え, 送信者の公開鍵を指定する. すなわち, PAEKS ではトラップドアが送信者に依存するため, 各送信者用にトラップドアを作成する必要がある. 例えば受信者があるキーワードが含まれるドキュメントを検索しようとした場合, 全ての送信者ごとにトラップドアを作成, 検索を行うことになる. よって検索効率は送信者の数に線型依存する. 一方, PEKS ではトラップドアが送信者に依存しない. そのため, 誰が作成した暗号文なのかを意識せず検索を行うことが可能である. すなわち, PEKS と比較した場合, PAEKS は KGA 耐性と引き換えに検索効率が悪化する. よって KGA 耐性を維持しつつ, 検索を効率化することが望まれる.

IBGEKS. KGA 耐性と検索効率性を両立する目的で, Wang ら [24] は ID ベースグループ検索可能暗号 (IBGEKS: Identity-Based Group Encryption With Keyword Search) を提案した. 受信者は送信者グループを定義, グループマスター鍵 $\mathsf{SK}_{\mathsf{gm}}$ を用いてグループ秘密鍵 gsk を作成する. 送信者は gsk を用いてキーワードを暗号化する. 受信者は $\mathsf{SK}_{\mathsf{gm}}$ を用いてキーワードに対するトラップドアを作成する. つまり, IBGEKS ではトラップドアは送信者ではなく送信者グループに依存する. そのため, グループの誰が作成した暗号文なのかを意識せず検索を行うことが可能であり, PAEKS と比較して検索が効率化されているといえる.

本論文の貢献. 本論文では, Wang らの IBGEKS 方式に対する攻撃を 2 つ提案, トラップドアからキーワードの情報が漏洩することを示す. 提案攻撃では, トラップドアがキーワードをメッセージとする Boneh-Lynn-Shacham (BLS) 署名 [6] であることに着目した. 提案攻撃 1 では送信者をグループに登録するための登録オラクルを通じて, 提案攻撃 2 ではトラップドアオラクルを通じて BLS 署名の検証鍵相当を取得する. BLS 署名検証を通し, トラップドアがキーワードに紐付いているかどうかを判定する. さらに提案攻撃 1 の一般化として, IBGEKS 方式が正当性を満たす場合, 攻撃者が登録オラクルにアクセス可能なモデルで安全な IBGEKS 方式は実現不可能であることも示す. 最後に修正可能性に関して議論する.

関連研究. IBGEKS と同様に PAEKS の検索効率を改善する目的で, Cheng ら [9] によりサーバ補助型公開鍵検索可能認証暗号 (SA-PAEKS: Server-Aided Public Key Authenticated Encryption with Keyword Search) が提案されている. テストサーバに加え, 送信者サーバと受信者サーバが定義される. 複数送信者を送信者サーバに, 複数受信者を受信者サーバとみなしてサーバ間で PAEKS 方式を実行することで, 暗号文サイズとトラップドアサイズが送受信

[*1] https://wordcounter.io/blog/how-many-words-are-in-the-english-language

[*2] なお 262,144 秒は 3 日程度である. 1 回のテストアルゴリズム実行に 1 秒とかなり悲観的に見積もった場合でも, 3 日程度でキーワードが復元可能となる.

者の数に依存しないという特徴を持つ. Zhang ら [27] も送信者サーバと受信者サーバを導入することで, 検索効率が送受信者数に依存しない方式を提案している. Xu ら [25] も同様の目的で受信者サーバを導入している. これらの方式において, 追加のサーバを定義している点が IBGKES と異なる.

2 つの暗号文が同じ平文の暗号化かどうかを判定可能な平文一致確認可能公開鍵暗号 (PKEET: Public Key Encryption with Equality Test) [26] の拡張として, グループベース PKEET (G-PKEET) [19] が提案されている. さらに PKEET の ID ベース版である平文一致確認可能 ID ベース暗号 (IBEET: Identity-Based Encryption with Equality Test) [21] の拡張として, グループベース IBEET (G-IBEET) [20] も提案されている. G-PKEET/G-IBEET では, PKEET/IBEET における平文回復攻撃, すなわちテストアルゴリズム実行者が任意の平文を暗号化, テストを通して暗号文の復号を試みる攻撃の対策をその主目的としている. グループに属する送信者のみが暗号化可能な枠組みを導入することで, 平文復元攻撃耐性を持たせている. 検索効率の向上は主目的として掲げられているわけではないが, テストアルゴリズム実行時にどの送信者が作成した暗号文かを意識する必要がないという点が, IBGKES との類似点として挙げられる.

グループ署名 [8] の暗号方式版としてグループ暗号 (GE: Group Encryption) が提案されている [3, 7, 15, 17, 23]. 受信者 (復号者) が誰なのかを秘匿するとともに, 開示者のみが受信者を特定可能な公開鍵暗号である. IBGEKS も “Group Encryption” という語が方式名に含まれているが, GE とは異なる暗号技術であることに注意されたい.

2. IBGEKS

本章では IBGEKS を定義する. なお Wang らは送信者と受信者に証明書を発行する認証局 (CA: Certificate Authority) を定義している. 本論文における攻撃とは無関係のため, CA に関する記述は割愛する. 以下 IBGEKS 方式 $\mathsf{IBGEKS} = (\mathsf{Setup}, \mathsf{KeyGen}_g, \mathsf{Register}, \mathsf{Enc}_P, \mathsf{Trapdoor}, \mathsf{Test})$ を定義する. $\mathcal{ID}_g$ を送信者グループ識別子とし, グループに含まれる送信者は識別子 $\mathsf{ID} \in \mathcal{ID}_g$ を持つと仮定する.

Definition1 (IBGEKS のシンタックス)

$\mathsf{Setup}(1^\lambda)$: セットアップアルゴリズムでは, セキュリティパラメータ λ を入力とし, 公開パラメータ pp を出力する.

$\mathsf{KeyGen}_g(\mathsf{pp}, \mathcal{ID}_g)$: グループ鍵生成アルゴリズムでは, pp, 送信者グループ識別子 $\mathcal{ID}_g$ を入力とし, グループマスター秘密鍵 $\mathsf{SK}_{\mathsf{gm}}$ を出力する.

$\mathsf{Register}(\mathsf{pp}, \mathsf{SK}_{\mathsf{gm}}, \mathsf{ID}_i)$: 登録アルゴリズムでは, $\mathsf{pp}, \mathsf{SK}_{\mathsf{gm}}$, 送信者の識別子 $\mathsf{ID}_i \in \mathcal{ID}_g$ を入力とし, グループ秘密鍵 gsk_i を出力する.

$\mathsf{Enc}_P(\mathsf{pp}, \mathsf{gsk}_i, \mathsf{ID}_i, w)$: 暗号化アルゴリズムでは, $\mathsf{pp}, \mathsf{gsk}_i, \mathsf{ID}_i$, キーワード w を入力とし, 暗号文 C_w を出力する.

$\mathsf{Trapdoor}(\mathsf{pp}, \mathsf{SK}_{\mathsf{gm}}, w')$: トラップドア生成アルゴリズムでは, $\mathsf{pp}, \mathsf{SK}_{\mathsf{gm}}$, 検索キーワード w' を入力とし, トラップドア $\mathsf{T}_{w'}$ を出力する.

$\mathsf{Test}(\mathsf{pp}, \mathsf{T}_{w'}, \mathsf{C}_w)$: テストアルゴリズムでは, $\mathsf{pp}, \mathsf{T}_{w'}, \mathsf{C}$ を入力とし, 0 または 1 を出力する.

次に正当性を定義する.

Definition2 (正当性) 全ての λ, $\mathsf{pp} \leftarrow \mathsf{Setup}(\lambda)$, $\mathcal{ID}_g$, $\mathsf{SK}_{\mathsf{gm}} \leftarrow \mathsf{KeyGen}_g(\mathsf{pp}, \mathcal{ID}_g)$, $\mathsf{gsk}_i \leftarrow \mathsf{Register}(\mathsf{pp}, \mathsf{SK}_{\mathsf{gm}}, \mathsf{ID}_i)$, w, w', $\mathsf{C} \leftarrow \mathsf{Enc}_P(\mathsf{pp}, \mathsf{gsk}_i, \mathsf{ID}_i, w)$, $\mathsf{T}_{w'} \leftarrow \mathsf{Trapdoor}(\mathsf{pp}, \mathsf{SK}_{\mathsf{gm}}, w')$ に対し, $w = w'$ の場合, $\Pr[\mathsf{Test}(\mathsf{pp}, \mathsf{T}_{w'}, \mathsf{C}_w) = 1]=1$ が, 不一致の場合, $\Pr[\mathsf{Test}(\mathsf{pp}, \mathsf{T}_{w'}, \mathsf{C}_w) = 0]=1-\mathsf{negl}(\lambda)$ が成り立つならば, IBGEKS 方式は正当であると定義する.

トラップドアからキーワードに関する情報が漏れない安全性として, Trapdoor Privacy[*3]を定義する. $\mathcal{C}$ をチャレンジャー, $\mathcal{A}$ を攻撃者とする.

Definition3 (Trapdoor Privacy) $\mathcal{C}$ は $\mathsf{pp} \leftarrow \mathsf{Setup}(\lambda)$, $\mathsf{SK}_{\mathsf{gm}} \leftarrow \mathsf{KeyGen}_g(\mathsf{pp}, \mathcal{ID}_g)$ を実行し, pp を $\mathcal{A}$ に送付する. ゲームを通して $\mathcal{A}$ は以下のオラクルを利用可能である.

登録オラクル : $\mathcal{A}$ は送信者の識別子として ID を $\mathcal{C}$ に送付する. $\mathcal{C}$ は $\mathsf{gsk} \leftarrow \mathsf{Register}(\mathsf{pp}, \mathsf{SK}_{\mathsf{gm}}, \mathsf{ID})$ を実行し, gsk を $\mathcal{A}$ に返す.

トラップドアオラクル : $\mathcal{A}$ は w を $\mathcal{C}$ に送付する. $\mathcal{C}$ は $\mathsf{T}_w \leftarrow \mathsf{Trapdoor}(\mathsf{pp}, \mathsf{SK}_{\mathsf{gm}}, w)$ を実行し, T_w を $\mathcal{A}$ に返す.

暗号化オラクル : $\mathcal{A}$ は ID, w を $\mathcal{C}$ に送付する. $\mathcal{C}$ は $\mathsf{C}_w \leftarrow \mathsf{Enc}_P(\mathsf{pp}, \mathsf{gsk}, \mathsf{ID}, w)$ を実行し, C_w を $\mathcal{A}$ に返す.

$\mathcal{A}$ は, 2 つのキーワード w_0^*, w_1^* を宣言し, $\mathcal{C}$ に送付する. ただし, w_0^*, w_1^* はトラップドアオラクル, 暗号化オラクルへ送付されていないキーワードとする. $\mathcal{C}$ は $b \xleftarrow{\$} \{0,1\}$ を選び, $\mathsf{T}_{w_b^*} \leftarrow \mathsf{Trapdoor}(\mathsf{pp}, \mathsf{SK}_{\mathsf{gm}}, w_b^*)$ を実行し, チャレンジトラップドア $\mathsf{T}_{w_b^*}$ を $\mathcal{A}$ に送付する. 以降, $\mathcal{A}$ は上記オラクルに引き続きアクセス可能である. ただし w_0^*, w_1^* のトラップドアオラクル, 暗号化オラクルへの送付は禁止する. $\mathcal{A}$ は $b' \in \{0,1\}$ を出力する. $b = b'$ の場合, 攻撃者は勝利すると定義する. もし全ての確率的多項式時間攻撃者 $\mathcal{A}$ に対し, 利得

$$\mathsf{Adv}_{\mathcal{A}}^{TP}(\lambda) = |\Pr[b = b'] - 1/2|$$

が λ に対して無視できる場合, IBGEKS は Trapdoor Pri-

[*3] Wang らの論文では IND-TP-CCA と呼称されている. なお検索可能暗号において, CCA 安全性とは攻撃者がテストオラクルにアクセス可能な場合と定義されている [2]. しかし IND-TP-CCA ではテストオラクルを定義していない. そのため本論文では IND-TP-CCA を Trapdoor Privacy と呼称する.

vacy を満たすと定義する.

3. IBGEKS 方式

Wang らの IBGEKS 方式を示すにあたり, 先に直感的な構成方針を記述する.

IBGEKS 方式は Boneh-Franklin (BF) ID ベース暗号 (IBE: Identity-Based Encryption) [5] を拡張して構成されている. Abdalla ら [1] により PEKS の匿名 IBE からの一般的構成が提案されており, BF-IBE は匿名 IBE であることから, 自然な選択であると考えられる. BF-IBE 方式の暗号文は

$$(\mathsf{C}_1, \mathsf{C}_2) = (g^r, M \oplus \mathsf{H}_3(e(S, \mathsf{H}_2(\mathsf{ID})^r))$$

と表される. ここで $S = g^\alpha$ がマスター公開鍵, $r \in \mathbb{Z}_p$ は乱数である. 復号鍵 $\mathsf{dk}_{\mathsf{ID}} = \mathsf{H}_2(\mathsf{ID})^\alpha$ を用いることで $e(\mathsf{C}_1, \mathsf{dk}_{\mathsf{ID}}) = e(g^r, \mathsf{H}_2(\mathsf{ID})^\alpha) = e(g^\alpha, \mathsf{H}_2(\mathsf{ID})^r) = e(S, \mathsf{H}_2(\mathsf{ID})^r)$ が計算できることを利用し,

$$M = \mathsf{C}_2 \oplus \mathsf{H}_3(e(\mathsf{C}_1, \mathsf{dk}_{\mathsf{ID}}))$$

と復号を行う. Abdalla らの一般的構成では, キーワード w を ID とみなした IBE の秘密鍵 $\mathsf{H}_2(w)^\alpha$ をトラップドア T_w とする. w を ID としてランダムな平文 R を暗号化, PEKS 暗号文を R と IBE 方式の暗号文とする. トラップドアで IBE 方式の暗号文が復号可能 (R が得られるか) かどうかで検索を行う. ここで平文をマスクしている $\mathsf{H}_3(e(\mathsf{C}_1, \mathsf{H}_2(\mathsf{ID})^\alpha))$ が計算可能かどうかで復号可能性を判定, 平文 R 部分を削除する. すなわち $\mathsf{C}_2 = \mathsf{H}_3(e(S, \mathsf{H}_2(w)^r))$ と設定,

$$\mathsf{C}_2 = \mathsf{H}_3(e(\mathsf{C}_1, \mathsf{T}_w))$$

が成り立つ場合, テストアルゴリズムは 1 を返す. これが Boneh らの PEKS 方式 [4] に相当する. ここで Naor 変換 [5] により, IBE の秘密鍵は署名とみなすことができることに注意されたい. BF-IBE 方式の場合, 秘密鍵は BLS 署名 [6] に相当する. すなわち, Boneh らの PEKS 方式におけるトラップドア $\mathsf{T}_w = \mathsf{H}_2(w)^\alpha$ もメッセージ w に対する BLS 署名となっている.

Wang らの IBGEKS 方式においても, トラップドア $\mathsf{T}_w = \mathsf{H}_2(w)^\alpha$ はキーワード w をメッセージとした BLS 署名である. グループマスター秘密鍵 $\mathsf{SK}_{\mathsf{gm}} = \alpha$ が BLS 署名の署名鍵に相当, 送信者 $\mathsf{ID}_i \in \mathcal{ID}_g$ に対し, 登録アルゴリズムにてグループ秘密鍵 $\mathsf{gsk}_i = \mathsf{H}_1(\mathsf{ID}_i)^\alpha$ を計算している. 暗号化アルゴリズムでは, Boneh らの PEKS 方式における $\mathsf{C}_1 = g^r$ の代わりに $\mathsf{C}_1 = \mathsf{H}_1(\mathsf{ID}_i)^r$ と設定する. BF-IBE 方式のマスター公開鍵 $S = g^\alpha$ の代わりに $\mathsf{gsk}_i = \mathsf{H}_1(\mathsf{ID}_i)^\alpha$ を用いることで

$$(\mathsf{C}_1, \mathsf{C}_2) = (\mathsf{H}_1(\mathsf{ID}_i)^r, \mathsf{H}_3(e(\mathsf{gsk}_i, \mathsf{H}_2(w)^r))$$

を計算, IBGEKS 方式の暗号文とする. テストアルゴリズムでは (Boneh らの PEKS 方式同様) T_w を用いて $(\mathsf{C}_1, \mathsf{C}_2)$ が復号可能かどうかを確認することで, 検索を行う.

Wang らの IBGEKS 方式

$\mathsf{Setup}(\lambda)$: $\mathbb{G}$, $\mathbb{G}_\mathsf{T}$ を素数位数 p の巡回群とする. $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_\mathsf{T}$ を双線形写像とし, $\mathsf{H}_1, \mathsf{H}_2 : \{0,1\}^* \to \mathbb{G}$, ハッシュ関数を $\mathsf{H}_3 : \mathbb{G}_\mathsf{T} \to \{0,1\}^*$ とする. 公開システムパラメータ $\mathsf{pp} = \{e, \mathbb{G}, \mathbb{G}_\mathsf{T}, \mathsf{p}, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3\}$ を出力する.

$\mathsf{KeyGen}_g(\mathsf{pp}, \mathcal{ID}_g)$: $\alpha \xleftarrow{\$} \mathbb{Z}_p^*$ を選択し, グループマスター秘密鍵 $\mathsf{SK}_{\mathsf{gm}} = \alpha$ を出力する.

$\mathsf{Register}(\mathsf{pp}, \mathsf{SK}_{\mathsf{gm}}, \mathsf{ID}_i)$: $\mathsf{ID}_i \in \mathcal{ID}$ として, グループ秘密鍵 $\mathsf{gsk}_i = \mathsf{H}_1(\mathsf{ID}_i)^\alpha$ を出力する.

$\mathsf{Enc}_P(\mathsf{pp}, \mathsf{gsk}_i, \mathsf{ID}_i, w)$: $r \xleftarrow{\$} \mathbb{Z}_p^*$ を選択し, $t = e(\mathsf{gsk}_i, \mathsf{H}_2(w)^r)$ を計算し, 暗号文 $\mathsf{C} = (\mathsf{H}_1(\mathsf{ID}_i)^r, \mathsf{H}_3(t))$ を出力する.

$\mathsf{Trapdoor}(\mathsf{pp}, \mathsf{SK}_{\mathsf{gm}}, w')$: $\mathsf{T}_w = \mathsf{H}_2(w)^\alpha$ を出力する.

$\mathsf{Test}(\mathsf{pp}, \mathsf{T}_{w'}, \mathsf{C}_w)$: $(\mathsf{C}_1, \mathsf{C}_2) = \mathsf{C}$ として, $\mathsf{H}_3(e(\mathsf{C}_1, \mathsf{T}_w)) = \mathsf{C}_2$ であれば 1 を, 不一致時に 0 を出力する.

ここで

$$\begin{aligned}\mathsf{H}_3(e(\mathsf{C}_1, \mathsf{T}_{w'})) &= \mathsf{H}_3(e(\mathsf{H}_1(\mathsf{ID}_i)^r, \mathsf{H}_2(w')^\alpha)) \\ &= \mathsf{H}_3(e(\mathsf{H}_1(\mathsf{ID}_i)^\alpha), \mathsf{H}_2(w')^r)\end{aligned}$$

かつ

$$\mathsf{C}_2 = \mathsf{H}_3(t) = \mathsf{H}_3(e(\mathsf{H}_1(\mathsf{ID}_i)^\alpha, \mathsf{H}_2(w)^r))$$

が成り立つ. よって $w = w'$ の場合, $\mathsf{H}_3(e(\mathsf{C}_1, \mathsf{T}_{w'})) = \mathsf{C}_2$ が成り立つ. $w \neq w'$ の場合, H_2 と H_3 の衝突困難性により, $\mathsf{H}_3(e(\mathsf{C}_1, \mathsf{T}_{w'})) \neq \mathsf{C}_2$ が成り立つ.

ここで BLS 署名の検証鍵 g^α が得られた場合, BLS 署名の検証式: $e(g^\alpha, \mathsf{H}_2(w)) = e(g, \mathsf{T}_w)$ を確認することで, トラップドアが w に紐ついているかどうか判定可能, すなわちキーワードの情報がトラップドアから漏洩することがわかる. しかし g^α は公開情報に含まれていないことに注意されたい. 次章で与える提案攻撃では, この g^α に相当する値をオラクルアクセスにより取得する. トラップドアがキーワードに対する BLS 署名であるかどうかを検証することで, Trapdoor Privacy を破る.

4. 提案攻撃

本章では, Wang らの IBGEKS 方式に対する攻撃を 2 つ提案する. 提案攻撃 1 では登録オラクルを通じて得られるグループ秘密鍵 $\mathsf{gsk}_i = \mathsf{H}_1(\mathsf{ID}_i)^\alpha$ を, 提案攻撃 2 ではトラップドアオラクルを通じて得られるトラップドア $\mathsf{T}_w = \mathsf{H}_2(w)^\alpha$ を BLS 署名の検証鍵とみなすことで, トラップドアからキーワードに関する情報が漏れていることを示す.

4.1 提案攻撃 1: 登録オラクルを用いる場合

提案攻撃 1 では, 登録オラクルを用いて Trapdoor Privacy を破る. トラップドア $\mathsf{T}_w = \mathsf{H}_2(w)^\alpha$ はキーワード w をメッセージとした BLS 署名であることは前述した通りである. ここでグループ秘密鍵 $\mathsf{gsk} = \mathsf{H}_1(\mathsf{ID})^\alpha$ が BLS 検証鍵 g^α の形式であることに着目する.

ここで以下の等式が成り立つ.

$$\begin{aligned} e(\mathsf{H}_1(\mathsf{ID}), \mathsf{T}_{w_b^*}) &= e(\mathsf{H}_1(\mathsf{ID}), \mathsf{H}_2(w_b^*)^\alpha) \\ &= e(\mathsf{H}_1(\mathsf{ID})^\alpha, \mathsf{H}_2(w_b^*)) \\ &= e(\mathsf{gsk}, \mathsf{H}_2(w_b^*)) \end{aligned}$$

攻撃者は任意の ID を登録オラクルに送付, $\mathsf{gsk} = \mathsf{H}_1(\mathsf{ID})^\alpha$ を得る. $e(\mathsf{H}_1(\mathsf{ID}), \mathsf{T}_{w_b^*}) = e(\mathsf{H}_1(\mathsf{ID})^\alpha, \mathsf{H}_2(w_0^*))$ の場合 $b = 0$, 成り立たない場合 $b = 1$ を出力する.

提案攻撃 1 の一般化. 提案攻撃 1 は IBGEKS 方式の代数的な性質を利用していた. ここで攻撃者は登録オラクルを通してグループ署名鍵を取得可能であること, (IBGEKS のシンタックス上) グループ署名鍵を用いて任意のキーワードに対する暗号文を作成できることに着目, 提案攻撃 1 を一般化する. この攻撃は IBGEKS 方式の代数的性質に依存しないことに注意されたい. 以下, IBGEKS 方式が正当性を満たすと仮定する.

$\mathcal{C}$ は $\mathsf{pp} \leftarrow \mathsf{Setup}(\lambda)$, $\mathsf{SK}_{\mathsf{gm}} \leftarrow \mathsf{KeyGen}_g(\mathsf{pp}, \mathcal{ID}_g)$ を実行し, pp を $\mathcal{A}$ に送付する. $\mathcal{A}$ は w_0^*, w_1^* を宣言し, $\mathcal{C}$ に送付する. $\mathcal{C}$ は $b \xleftarrow{\$} \{0,1\}$ を選び, $\mathsf{T}_{w_b^*} \leftarrow \mathsf{Trapdoor}(\mathsf{pp}, \mathsf{SK}_{\mathsf{gm}}, w_b^*)$ を実行し, $\mathsf{T}_{w_b^*}$ を $\mathcal{C}$ に送付する. $\mathcal{A}$ は任意の $\mathsf{ID} \in \mathcal{ID}_g$ を登録オラクルに送付する. $\mathcal{C}$ は $\mathsf{gsk} \leftarrow \mathsf{Register}(\mathsf{pp}, \mathsf{SK}_{\mathsf{gm}}, \mathsf{ID})$ を計算し, gsk を $\mathcal{A}$ に返す. $\mathcal{A}$ は $\mathsf{C}_{w_0^*} \leftarrow \mathsf{Enc}_P(\mathsf{pp}, \mathsf{gsk}, \mathsf{ID}, w_0^*)$, $\mathsf{C}_{w_1^*} \leftarrow \mathsf{Enc}_P(\mathsf{pp}, \mathsf{gsk}, \mathsf{ID}, w_1^*)$ を計算する. IGBEKS 方式が正当性を満たすことから, $\mathsf{Test}(\mathsf{pp}, T_{w_b^*}, \mathsf{C}_{w_0^*}) = 1$ の場合 $b = 0$, $\mathsf{Test}(\mathsf{pp}, T_{w_b^*}, \mathsf{C}_{w_1^*}) = 1$ の場合 $b = 1$ と判定することで Trapdoor Privacy を破る.

4.2 提案攻撃 2: トラップドアオラクルを用いる場合

提案攻撃 1 (およびその一般化) では攻撃者は登録オラクルにアクセスしていた. これは Wang らの Trapdoor Privacy の定義に沿ったものであることを強調しておく. 一方, Wang らは Trapdoor Privacy に関して,

> "*The Trapdoor Privacy game assumes the server to be the adversary. This game aims to prevent the adversary learning keywords from trapdoors if it does not know which IDs are in the group.*"

と記述している. 攻撃者が登録オラクルに ID を送付するということは, 攻撃者に対しグループに登録されている識別子が既知であるということになり, 上記記述に矛盾する. そこで登録オラクルを用いず, 攻撃者がグループに登録されている識別子を知らない状況においても, Wang らの IBGEKS 方式は Trapdoor Privacy を満たさないことを示す. この提案攻撃 2 では, トラップドア $\mathsf{T}_w = \mathsf{H}_2(w)^\alpha$ 自体が BLS 検証鍵に相当する (g^α の形式である) ことに着目した. ここで以下の等式が成り立つ.

$$\begin{aligned} e(\mathsf{H}_2(w), \mathsf{T}_{w_b^*}) &= e(\mathsf{H}_2(w), \mathsf{H}_2(w_b^*)^\alpha) \\ &= e(\mathsf{H}_2(w)^\alpha, \mathsf{H}_2(w_b^*)) \\ &= e(\mathsf{T}_w, \mathsf{H}_2(w_b^*)) \end{aligned}$$

$\mathcal{A}$ は w_0^*, w_1^* を宣言する. さらに任意の $w \notin \{w_0^*, w_1^*\}$ をトラップドアオラクルに送付, T_w を得る. $\mathcal{A}$ は $e(\mathsf{H}_2(w), \mathsf{T}_{w_b^*}) = e(\mathsf{T}_w, \mathsf{H}_2(w_0^*))$ が成り立つ場合, $b = 0$ を, $e(\mathsf{H}_2(w), \mathsf{T}_{w_b^*}) = e(\mathsf{T}_w, \mathsf{H}_2(w_1^*))$ が成り立つ場合 $b = 1$ を出力, Trapdoor Privacy を破る.

修正可能性について. 提案攻撃 2 は対称ペアリングの性質を用いていることから, 非対称ペアリングを用いることで回避可能であると考えられる. しかし攻撃 1 の一般化で述べた通り, Trapdoor Privecy の攻撃者が登録オラクルにアクセス可能である場合, キーワードに関する情報がトラップドアより漏洩する. IBGEKS のシンタックス上, グループ秘密鍵を 1 つでも入手すれば, 暗号化アルゴリズムが実行可能である. PEKS におけるキーワード推測攻撃と同様に, 攻撃者が任意のキーワードに対する暗号文を取得可能となることから, Trapdoor Privacy の実現は原理的に不可能である. そのため, 安全性モデルから登録オラクルを削除せざるを得ない. この場合, 攻撃者はグループ秘密鍵を一切持たない設定となる. これは (グループ秘密鍵を持つ) グループに所属するユーザであれば, そのグループに対して作成されたトラップドアから, キーワードに関する情報を得ることが可能となる余地を残す, 弱い安全性しか保証できないこととなる.

次に, グループに所属するユーザ以外に対する Trapdoor Privacy (以下, Outsider Trapdoor Privacy) について議論する. まず放送暗号における匿名性の文脈では, 受信者グループであっても暗号文から受信者の情報が得られない強い匿名性 (Full Anonymity) を保証する場合 [18], 受信者グループ以外に対して匿名性 (Outsider Anonymity) を保証する場合 [12] の 2 つの安全性が知られている. 検索可能放送暗号の文脈においても, 同様に Full/Outsider Anonymity が考慮されている [10, 11, 22]. あくまで受信者匿名性に関するものであり, Trapdoor Privacy を考慮したものではないことに注意されたい. ここで安全性の観点からは Full Anonymity が望ましいものの, 実現可能な暗号文長に関する制限が知られていることに注意されたい [14, 16]. 一方, Outsider Anonymity においては短い暗号文長が実現可能となる. さらに Fazio と Perera [12] は Outsider Anonymity に関し, "*This seems a natural relaxation, since often the*

contents of the communication already reveals something about the recipient set.” と主張している．これらの観点より, 適切なシナリオの元においては IBGEKS における Outsider Trapdoor Privacy に意義がある可能性は否定できず, 一概に適切な安全性モデルではないとは言い難い．

以上より, 方式の修正に先んじて IBGKES の適切な安全性モデルの定義及びその妥当性の議論が必要であることから, 本論文では Wang らの方式に対する修正については考慮しない．

5. 結論

本論文では, Wang らの IBGEKS 方式に対して, トラップドアからキーワードに関する情報が漏洩していることを示した。提案攻撃 1 では, 登録オラクルから入手したグループ秘密鍵を, 提案攻撃 2 ではトラップドアオラクルから入手したトラップドアを検証鍵として用いた．さらに提案攻撃 1 を一般化, Trapdoor Privacy の達成には登録オラクルを削除せざるを得ないことを示した．またこの弱い Trapdoor Privacy の妥当性に関し, 既存研究を鑑みて一概に適切な安全性モデルではないとは言い難いと結論付けた．適切な IBGEKS の安全性モデルの定義と方式の提案を今後の課題とする．

謝辞 本研究は JSPS 科研費 JP21K11897 の助成を受けたものです．

参考文献

[1] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. *Journal of cryptology*, 21:350–391, 2008.

[2] Michel Abdalla, Mihir Bellare, and Gregory Neven. Robust encryption. *Journal of Cryptology*, 31(2):307–350, 2018.

[3] Laila El Aimani and Marc Joye. Toward practical group encryption. In *Applied Cryptography and Network Security*, pages 237–252, 2013.

[4] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In *EUROCRYPT*, pages 506–522, 2004.

[5] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In *CRYPTO*, pages 213–229, 2001.

[6] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In *ASIACRYPT*, pages 514–532, 2001.

[7] Julien Cathalo, Benoît Libert, and Moti Yung. Group encryption: Non-interactive realization in the standard model. In *ASIACRYPT*, pages 179–196, 2009.

[8] David Chaum and Eugène van Heyst. Group signatures. In *EUROCRYPT*, pages 257–265, 1991.

[9] Leixiao Cheng and Fei Meng. Server-aided public key authenticated searchable encryption with constant ciphertext and constant trapdoor. *IEEE Transactions on Information Forensics and Security*, 19:1388–1400, 2024.

[10] Keita Emura. Generic construction of fully anonymous broadcast authenticated encryption with keyword search with adaptive corruptions. *IET Inf. Secur.*, 2023:1–12, 2023.

[11] Keita Emura, Kaisei Kajita, and Go Ohtake. Outsider-anonymous broadcast encryption with keyword search: Generic construction, CCA security, and with sublinear ciphertexts. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 107(9):1465–1477, 2024.

[12] Nelly Fazio and Irippuge Milinda Perera. Outsider-anonymous broadcast encryption with sublinear ciphertexts. In *Public Key Cryptography*, pages 225–242, 2012.

[13] Qiong Huang and Hongbo Li. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks. *Information Sciences*, 403:1–14, 2017.

[14] Aggelos Kiayias and Katerina Samari. Lower bounds for private broadcast encryption. In *Information Hiding*, pages 176–190, 2012.

[15] Aggelos Kiayias, Yiannis Tsiounis, and Moti Yung. Group encryption. In *ASIACRYPT*, pages 181–199, 2007.

[16] Hirokazu Kobayashi, Yohei Watanabe, Kazuhiko Minematsu, and Junji Shikata. Tight lower bounds and optimal constructions of anonymous broadcast encryption and authentication. *Des. Codes Cryptogr.*, 91(7):2523–2562, 2023.

[17] Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge arguments for matrix-vector relations and lattice-based group encryption. *Theoretical Computer Science*, 759:72–97, 2019.

[18] Benoît Libert, Kenneth G. Paterson, and Elizabeth A. Quaglia. Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In *Public Key Cryptography*, pages 206–224, 2012.

[19] Yunhao Ling, Sha Ma, Qiong Huang, Ximing Li, and Yunzhi Ling. Group public key encryption with equality test against offline message recovery attack. *Information Sciences*, 510:16–32, 2020.

[20] Yunhao Ling, Sha Ma, Qiong Huang, Ximing Li, Yijian Zhong, and Yunzhi Ling. Efficient group ID-based encryption with equality test against insider attack. *The Computer Journal*, 64(4):661–674, 2021.

[21] Sha Ma. Identity-based encryption with outsourced equality test in cloud computing. *Information Sciences*, 328:389–402, 2016.

[22] Sayantan Mukherjee. Statistically consistent broadcast authenticated encryption with keyword search - adaptive security from standard assumptions. In *ACISP*, pages 523–552, 2023.

[23] Khoa Nguyen, Reihaneh Safavi-Naini, Willy Susilo, Huaxiong Wang, Yanhong Xu, and Neng Zeng. Group encryption: Full dynamicity, message filtering and code-based instantiation. In *Public-Key Cryptography*, pages 678–708, 2021.

[24] Wei Wang, Dongli Liu, Zilin Zheng, Peng Xu, and Laurence Tianruo Yang. Identity-based group encryption with keyword search against keyword guessing attack. *IEEE Transactions on Information Forensics and Security*, 19:8023–8036, 2024.

[25] Yongliang Xu, Hang Cheng, Jiguo Li, Ximeng Liu, Xinpeng Zhang, and Meiqing Wang. Lightweight multi-user public-key authenticated encryption with keyword

search. *IEEE Transactions on Information Forensics and Security*, 20:3234–3246, 2025.

[26] Guomin Yang, Chik How Tan, Qiong Huang, and Duncan S. Wong. Probabilistic public key encryption with equality test. In *CT-RSA*, pages 119–131, 2010.

[27] Shengjie Zhang, Jianchang Lai, Liquan Chen, Jinguang Han, and Ge Wu. Keyword-field-free conjunctive searchable encryption for multi-user in emr system. *IEEE Internet of Things Journal*, pages 1–1, 2025 (Early Access). DOI: 10.1109/JIOT.2025.3572314.