ID ベース暗号の匿名通信への応用

田中 寛之 †　　齋藤 彰一 †　　松尾 啓志 †

† 名古屋工業大学 466-8555 愛知県名古屋市昭和区御器所町

あらまし

インターネットにおけるプライバシー保護の重要性が増しており，様々な匿名通信方式が提案されている．多くの既存方式では，多数の参加ノードの公開鍵を得るためにディレクトリサーバを用いている．しかし，クエリを監視することで参加ノードの行動を推測できるため，匿名性の低下につながる．我々は，既存の DHT に基づく匿名通信に ID ベース暗号を応用し，公開鍵取得による匿名性の低下を防ぐ方式を提案する．本論文では，提案方式の構成を示し，提案方式を既存の匿名通信方式に適用する方法について述べる．

Applying ID-Based Encryption to Anonymous Communication

Hiroyuki Tanaka †　　Shoichi Saito †　　Hiroshi Matsuo †

†Nagoya Institute of Technology Gokiso-cho Showa-ku Nagoya-shi Aichi 466-8555 Japan

Abstract Severity of disclosing personal information is increased. Many anonymous communication systems have been studied. The systems usually use a directory server to manage public keys of participating nodes. However, this way breaks anonymity because query messages for the directory server can give an attacker route information of an anonymous communication path.

We propose applying ID-based encryption (IBE) to anonymous communication. The proposal prevents routing information from leaking by query messages. This paper describes structure of the proposal system and a method of applying IBE to existing anonymous communication systems.

1　はじめに

インターネットの普及により，多種多様なサービスが利用可能である．その中には，医療相談や人権相談など相談者の匿名性が重要なサービスもある．また，モバイル環境において第三者に通信相手を特定されたくない状況もある．そのため，通信における匿名性を実現するための研究が行われている．匿名通信は，送信ノードを特定できないこと，受信ノードを特定できないこと，送受信ノード間を追跡できないことの 3 つの要件を満たす必要がある [1]．以下，これらをまとめて**匿名性**と言い，これら匿名性を備えた通信を**匿名通信**，匿名通信が使用する通信路を**匿名通信路**と言う．

匿名通信を実現する代表的な方式は，Onion Routing[2, 3] 等が採用している多重暗号を用いた多段中継方式である．この方式は，通信メッセージを複数の中継ノードを介して宛先ノードまで送る方式である．その時，各中継ノードに宛先ノードが分からないようにするために，送信ノードはメッセージを各中継ノードと受信ノードの公開鍵で暗号化する．各中継ノードは，自身の秘密鍵でメッセージを復号することで，次に送るノードのみを知ることができる．

この方式では，中継ノードの公開鍵を取得する必要がある．そのため，Cashmere[4] や Bifrost[5] では，ディレクトリサーバによる公開鍵管理を

行っている．しかし，送信ノードが公開鍵を入手するための，ディレクトリサーバへのクエリを監視することで，参加ノードの行動を推測できる．このため，匿名性が低下する．これは，DNS による名前解決からクライアントの動作を推測している研究 [6, 7] からも明らかである．

この課題を解決するには，通信をせずに公開鍵を入手できる必要がある．我々は匿名通信システムに ID ベース暗号 [8] (ID-Based Encryption:IBE) を取り入れる方法を提案する．IBE を多重暗号に適用することで，公開鍵を入手する通信をなくすことができる．しかし，IBE を使用するには，事前に中継ノードの ID を取得しなければならない．そのため，参加ノードへの ID 割り当て方式を工夫することで，通信無しで参加ノードの ID 割り当て状況を把握可能にする方法を提案する．これら 2 つの提案により，公開鍵の取得の際に匿名性が低下しない，多重暗号を用いた多段中継による匿名通信が可能となる．

本稿では，2 章で匿名通信の概要と問題点について述べ，3 章で提案方式について述べる．4 章で提案方式を既存の匿名通信に適用する方法について述べ，5 章で実装と評価を示し，6 章でまとめる．

2　匿名通信の概要と問題点

本章では匿名通信方式の概要と，既存方式の問題点について述べる．

2.1　多重暗号を用いた多段中継方式

IP 通信において双方向通信を行う場合，必ず両ノードがお互いの IP アドレスを知る必要がある．このため，IP 通信による匿名通信では，多数のノードでメッセージを中継し，その中に送信ノードと受信ノードを紛れ込ませることで隠蔽する必要がある．

多段に中継をしながら匿名性を保つには，各中継ノードが送信ノードと受信ノードを特定できてはいけない．しかし，受信ノードに確実に届かなければならない．これらのためには，各中継ノードは，自身が直接通信する前後の 2 ノードのみを知ることができるようにして，通信路全体を知ることができないようにすればよい．このために，公開鍵暗号を用いる．中継ノード毎の通信路情報を当該中継ノードの公開鍵で暗号化することで，各中継ノードが知り得る通信路情報を制限する．さらに，各通信路情報を中継順の逆順で多重暗号化することで，通信路情報を復号する各中継ノードは，通信路情報を中継順に取得することができる．以上により，多重暗号を用いた多段中継方式による匿名通信が可能となる．本方式は多数の匿名通信方式 [2, 3, 4, 5, 9] で使用されている．

2.2　ノード管理と公開鍵の取得

多重暗号による匿名通信路を構築するためには，参加ノード群から通信路を決定 (つまり，中継ノードを選択) し，選択した中継ノードの公開鍵を入手する必要がある．参加ノードの管理方法と公開鍵の入手方法として，事前に多数の参加ノード情報を取得する方式 (Tor[9]) と，分散ハッシュテーブル (Distributed Hash Table:DHT) によるノード管理とディレクトリサーバ[1]による公開鍵取得を組み合わせる方式 (Bifrost,Cashmere) がある．

参加ノード情報をあらかじめ多数取得する方式では，送信ノードは取得した参加ノード群から任意のノードを中継ノードとして選ぶ．この方式では，参加ノード情報を多数取得するため，参加ノード情報取得の通信状況から中継ノードを推測されることがない．さらに，公開鍵を別途取得する必要が無い．

一方，DHT を用いる方式では，任意の ID を指定して，その ID を管理するノードを中継ノードとする．この方法では，各中継ノードが ID を利用して次ノードを検索して中継するため，送信ノードが中継ノードの IP アドレスを調べる必要が無い．よって，この方法でも中継ノード選択に通信は不要である．しかし，公開鍵の入手にはディレクトリサーバを検索する必要があるため，この検索を監視することで他ノードが中継ノードを推測することができる．

[1] Cashmere では off-line central authority(CA) が相当する．

2.3 既存方式の問題点

既存方式 [4, 5] ではディレクトリサーバを用いて参加ノードの公開鍵を取得する．しかし，ディレクトリサーバへのクエリを監視することで，中継ノードの推測が可能となり匿名性が低下するという課題がある．この課題を解決するために，Tor では閾値以上の数のノード情報を集めてから通信を開始する方法を採用している．しかし，多数のノード情報をサーバから取得する方法はスケーラビリティがないといえる．

3 提案方式

DHT を用いた既存の匿名通信方式に IBE を導入することで，公開鍵配布に必要な処理を省き，既存方式の問題であったサーバによる匿名性が低下する問題を解決する方式を提案する．本章では，IBE の概要を述べ，次に IBE の匿名通信への応用方法と応用するための課題を述べる．

3.1 ID ベース暗号

ID ベース暗号とは，認証，署名，暗号化などを ID に基づいて行う暗号方式である．IBE の利用法の一つに，公開鍵暗号として利用するものがある．受信者の ID(任意の文字列，以下ノード ID と区別するために IBE-ID という) と共通パラメータを用いて受信者の公開鍵を計算し，暗号化を行う．共通パラメータとは，すべてのユーザが共有するハッシュ関数や素数などの鍵生成のための基本情報である．IBE では，信頼できる第三者が運用する秘密鍵生成局 (**PKG**) と呼ばれる機関が存在する．この PKG がマスター秘密鍵と共通パラメータの生成を行い，共通パラメータを周知させる．また，PKG がマスター秘密鍵と各利用者の IBE-ID を用いてそれぞれの秘密鍵を生成する．IBE では IBE-ID と共通パラメータの信頼性に基づいて安全性を確保するため，受信者の公開鍵とその証明書を検証する必要が無い．

3.2 IBE の導入と課題

IBE を導入することで，ディレクトリサーバへのクエリ監視による匿名性の低下を防ぐことができ，既存方式の課題を解決できる．つまり，通信先のノード ID を取得し，それを IBE における公開鍵の基になる IBE-ID とすることで別途公開鍵を入手する必要がなくなる．これにより，高い匿名性を保つ匿名通信方式が実現できる．

しかし，IBE を匿名通信方式に取り入れるために以下の解決すべき課題がある．次節以降において，これらの課題の解決する提案方式の詳細を述べる．

重複の無いノード ID 割り当て　提案手法では，PKG がノード ID を IBE-ID と見なして，その ID に対応する秘密鍵を発行するため，各ノード ID が重複して割り当てられてはならない．そのため，衝突しないようにノード ID を割り当てる仕組みが必要である．

割り当て済み ID の判断　IBE では，復号できる者がいない IBE-ID を用いても暗号化が可能である．しかし，未割り当てのノード ID を IBE-ID として匿名通信に用いた場合，復号できるノードが存在しないため，メッセージは受信者に届かない．そのため，割り当て済みのノード ID のみで暗号化を行う必要がある．このとき，公開鍵入手の通信と同様に，あるノード ID が割り当て済みか調べるために通信を用いると匿名性が低下する．したがって，通信を用いないで割り当て状況を確認する方法が必要である．

受信者のノード ID の検索　匿名通信において，ノード ID が長期間変化しないことは，ノード配置の固定化により匿名性の低下を招く．よって，Bifrost と Cashmere ではランダムにノード ID を割り当てている．この場合，メッセージを送るために，受信者の変化するノード ID を調べる方法が必要である．やはり，公開鍵入手と同様に通信は使用できない．

3.3 重複の無いノード ID 割り当て

IBE では，ノード ID を IBE-ID と見なして公開鍵を計算するためノード ID が重複してはならない．そのため，ノード ID 割り当て局 (Node-ID Allocation Server:**NIA**) を用意して，ノードの匿名通信システム参加時にノード ID の割り当てを行う．NIA は信頼できる第三者が運用する機関である．PKG がこの役割を担っても良い．

3.4 割り当て済みノード ID の判断

匿名性を低下させずに，割り当て済み ID のみで暗号化するには，通信なしで割り当て済みノード ID を取得できる必要がある．そこで，ノード ID の割り当てを規則的に行うことで，ノード ID から割り当て状況を推測可能にする．

単にノード ID を 0,1,…と順番につけた場合，DHT における ID 管理では割り当て済み ID が一部分に偏るため，効率的な検索ができない．そこで，この ID を 2 進数表記し上位と下位のビットを入れ替える (4 ビットの例:0001 → 1000, 0010 → 0100)．この入れ替えた値をノード ID とする．このノード ID は，ID 空間全体に均等に分散するため，DHT による検索効率を下げることはない．これにより，DHT の経路情報として保持しているノード ID から，少なくともどの ID までが割り当て済みか容易に判断できる．

3.5 受信ノード ID の検索

メッセージを送信するためには受信者のノード ID が分からなければならない．匿名性を低下させずに，受信者の変化するノード ID が検索可能である必要がある．本節では受信者のノード ID を検索する方法について考察し，IBE を用いた検索方法を提案する．

容易な検索方法は，フラッディングにより全参加ノードにサービス提供者の固有名 (以下，サービス名という) とそのノード ID を配布することである．しかし，ノード ID の変化の度にフラッディングする必要がある．さらに，スケーラビリティの確保は困難である．

フラッディングを用いずに受信者のノード ID の変化に追随する方法として，ランデブーポイント (Rendezvous Point:RP) 方式がある．RP 方式は Tor でも用いられており，受信者のノード ID が変化した場合でも通信路を構築可能である．

図 1 に提案方式における RP を用いた通信の例を示す．まず通信路構築の準備として，1) サービス提供ノード (受信ノード) は，サービス提供開始時にサービス名を PKG に登録して，サービス名を IBE における公開鍵の基とした場合に対応する秘密鍵を取得する．さらに，2) サービス提供ノードは，自身のサービス名のハッシュ値と同じ値の ID を管理するノードに対して匿名通信路を構築する（以下, このようなノードを RP ノードという）．次に，送信ノードがサービス提供ノードに接続する場合は，まず 3) サービス提供ノードにノード ID を要求するメッセージを作成する．このメッセージは，サービス名を IBE-ID とした公開鍵と中継ノードの公開鍵によって多重暗号化されており，送信ノードへの復路を構築するメッセージを含んでいる．しかし，サービス提供ノードのノード ID が不明であるため，4) サービス名のハッシュ値と同じ値の ID を管理する RP ノードに向けて当該メッセージを送信する．5) RP ノードは，受信したメッセージを，自身を RP として構築された全匿名通信路に転送する．6) サービス提供ノードは当該メッセージを受信し，サービス名に対応する秘密鍵で復号する．7) 復号に成功したサービス提供ノードは，送信ノードが作成した復路構築メッセージを用いて自身のノード ID を送信ノードに通知する．8) その後，送受信ノード間で匿名通信路を開設し通信を行う．

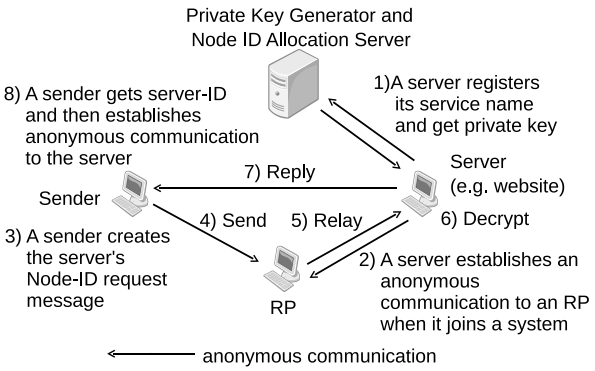

図 1: ランデブーポイントを用いた通信

送信ノードと RP ノードとサービス提供ノードの 3 点を結ぶ通信路は，すべて匿名通信路であるので，送信ノードを RP ノードとサービス提供ノードが特定することはできない．また，RP ノードは複数のサービス提供ノードへの RP として機能しており，メッセージがどのサービス提供ノードに向けられたものか知ることはできない．以上から，匿名性の低下させることなく，送信ノードはサービス提供ノードのノード ID を調べることが出来る．

for $i = 1$ to 160 **do**
  for j = 2^{i-1} to $2^i - 1$ **do**
    repeat
      t = ($random$ mod 2^{i-1}) + 2^{i-1}
    until t is not already assigned
    $NodeID = bit\_order\_reverse(t)$//assign ID
  end for
end for

図 2: ノード ID 割り当て方法

4 既存匿名通信方式への適用

本章では提案方式を既存の匿名通信方式に適用した場合について述べる．

4.1 提案方式の参加プロトコル

提案方式を適用するには，システムに NIA と PKG を追加する必要がある．両サーバは，全参加ノードが信用するものとする．参加プロトコルは次の 4 ステップからなる．1) 参加ノードが NIA にノード ID 割り当て要求を送る．2) NIA がノード ID を通知する．3) 参加ノードが，割り当てられたノード ID を PKG に通知する．4) PKG がノード ID に対応する秘密鍵を生成し，共通パラメータと共に返信する．なお，この間の通信は SSL を用いて行う．

4.2 ノード ID 割り当て方法

本節ではノード管理用の DHT として Chord[10] と Pastry[11] を用いる場合のノード ID 割り当て方法について述べる．提案方式では，割り当て済みノード ID を既に持っている情報から推測出来るようにノード ID を割り当てている．Chord と Pastry ではノード ID 空間の大きさは 2^{160} である．初期状態として 1 ノード (ノード ID:0) が参加している状態を考える．ノード ID 割り当て方法を図 2 に示す．$2^{i-1} \leq Node - ID \leq 2^i - 1$ ($i \geq 1$) に含まれるノード ID の集合を第 i 群と呼び，第 1 群から順番に割り当てる．なお，各群内でのノード ID の割り当て順は, ランダムとする．

この様にノード ID を割り当てることで, Chord の Finger table や Successor list，Pastry の Leaf set，Routing table や Neighborhood set を用い，既知のノード ID から，最新のノード ID の割り当て群が第 x 群であることが分かる．その結果, 少なくとも第 $x - 1$ 群のノード ID まで割り当てが完了していると判断することが出来る．これにより，匿名性の低下を防ぎつつ各ノードは使用可能なノード ID，つまり公開鍵が分かる．その他の DHT の実装に対するノード ID 割り当て方法は別途考える必要がある．

4.3 Bifrost と Cashmere への適用

Bifrost と Cashmere は DHT によるノード管理を行うため，PKG と NIA の追加と RP の機能を追加することで容易に適用できる．ノードの参加時は，まず，4.1 節に沿った参加処理を行う．そして当該ノードがサービス提供ノードの場合は，3.5 節の手順 1) と 2) を行う．次に，通信時には，3.5 節の手順 3) 以降により RP を使用してサービス提供ノードのノード ID，つまり公開鍵を取得する．以降の通信は RP は用いず，Bifrost，Cashmere それぞれの処理に従う．

4.4 Tor への適用

Tor に提案方式を適用する場合について述べる．Tor ではノードを ID で管理していないため，まずノード ID を割り当てる様に拡張する必要がある．ノード ID 割り当てと IBE によって，ディレクトリサーバから公開鍵を入手する必要はなくなり，中継ノードもノード ID による指定が可能になる．このため，IP アドレスの検索は，各中継ノードが行うことになるため，送信ノードがディレクトリサーバを検索することによる匿名性の低下は防ぐことができる．

しかし，Tor では DHT の経路情報に相当するもの，つまり他のシステム参加ノードの情報を自ノード内に有していない．そのため，送信ノードが割り当て済みのノード ID を調べるためには，ディレクトリサーバが定期的にノード ID の割り当て状況を通知する必要がある．また，各ノードが稼働中か否かを確かめるためにもディレクトリサーバが必要である．このように，公開鍵取得以外にディレクトリサーバが必要であるため，Tor では IBE 導入によるディレクトリサーバ不要となるメリットを享受できない．

提案方式を活かすには，対象の匿名通信方式がノードを ID 管理しており，既知の情報で割り

当て済みのノード ID を推測できる仕組みが必要がある．その仕組みとして DHT を Tor に加えた方式は，Bifrost の受信エリア [5] 内ノードが 1 台の場合と同じである．よって，単に Tor に提案方式を適用してもメリットは無いと言える．

5 実装と評価

提案システムを実装し，IBE 導入による課題である RP を介した受信ノード ID 取得に要する時間を計測した．実装は，Bifrost に IBE ライブラリ[2]を適用した．

評価環境は，CPU Core2Duo 3GHz, OS CentOS 5.4, ネットワーク 1000Base-T の LAN 接続の PC を 32 台を使用した．提案手法において RP を経由した受信ノード ID 取得には,「送信ノード→ RP」と「RP →受信ノード」と「受信ノード→送信ノード」の 3 つの匿名通進路を経由する．評価には，これら 3 つの匿名通信路に各 6 ノード (合計 18 ノード) を使用した．

測定の結果，ノード ID 取得時間は約 900ms である．この結果は LAN 環境かつ比較的高速な CPU を使用した場合であるため許容できる時間であるが，インターネット環境において様々な CPU が混在する実環境では，この数倍の時間が必要と考える．特に,「送信ノード→ RP」と「受信ノード→送信ノード」の 2 本はノード ID 取得のためのみに開設する通信路であり，大きなコストが必要である．このため，RP を介したノード ID 取得方法のコスト軽減が重要な課題と言える．

6 まとめ

既存の匿名通信方式に対して ID ベース暗号を導入し，公開鍵取得のための通信をなくすことで匿名性の低下を防ぐ手法を提案した．そして，提案方式を既存の匿名通信方式に適用した場合の動作について述べた．提案方式は Bifrost や Cashmere 以外にも DHT と多重暗号化を用いた匿名通信方式に適用可能である．ただし，高い匿名性を実現する代わりに，受信ノードのノード ID 取得コストが高く，特にインターネット環境では通信に時間を要すると考えられる．また，ノード離脱への対策も今後の課題である．

[2]BAO Yiyang “ibe-javapairing” : http://en.sourceforge.jp/projects/sfnet_ibe-javapairing/

謝辞

本研究の一部は文部科学省科学技術研究補助金基盤研究 C(課題番号:20500064) によるものである．

参考文献

[1] Pfitzmann, A. and Waidner, M.: Networks without user observability, *Computers & Security*, Vol. 6, No. 2, pp. 158–166 (1987).

[2] Goldschang, D., Reed, M. and Syverson, P.: Onion routing for anonymous and private internet connections, *ACM SIGCOMM Computer Communication Review*, Vol. 42, No. 2, pp. 39–41 (1999).

[3] Syverson, P. F., Goldschlag, D. M. and Reed, M. G.: Anonymous connections and Onion routing, *IEEE Journal on Specific Areas in Communications*, Vol. 16, No. 4, pp. 482–494 (1998).

[4] Zhuang, L., Zhou, F., Zhao, B. Y. and Rowstron, A.: Cashmere: Resilient anonymous routing, *Proceedings of the 2nd conference on Symposium on Networked Systems Design and Implementation*, pp. 301–314 (2005).

[5] Kondo, M., Saito, S., Ishiguro, K., Tanaka, H. and Matsuo, H.: Bifrost: A Novel Anonymous Communication System with DHT, *Second International Workshop on Reliability, Availability, and Security* (2009).

[6] Whyte, D., Kranakis, E. and van Oorschot, P.: DNS-based Detection of Scanning Worms in an Enterprise Network, *Proceedings of the 12th Annual Network and Distributed System Security Symposium* (2005).

[7] Ishibashi, K., Toyono, T. and Toyama, K.: Detecting Mass-Mailing Worm Infected Hosts by Mining DNS Traffic Data, *ACM SIGCOMM workshop on Mining network data* (2005).

[8] Boneh, D. and Franklin, M.: Identity-Based Encryption from the Weil Pairing, *SIAM Journal on Computing*, Vol. 32, No. 3, pp. 586–615 (2003).

[9] Dingledine, R., Mathewson, N. and Syverson, P.: Tor: The Second-Generation Onion Router, *Proceedings of 13th USENIX Security Symposium*, pp. 303–320 (2004).

[10] Stoica, I., Morris, R., Karger, D., Kaashoek, M. F. and Balakrishnan, H.: Chord : A Scalable Peer–To–Peer Lookup Service for Internet Applications, *Proceedings of the 2001 SIGCOMM conference*, pp. 149–160 (2001).

[11] Rowstron, A. and Druschel., P.: Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems, *Proceedings of the Middleware 2001 : IFIP/ACM International Conference on Distributed Systems Platforms*, pp. 329–350 (2001).