Valkyrie：非静的ネットワークに適応可能な匿名通信方式

山中晋爾[†] 古原和邦[††] 今井秀樹[††]

ネットワークにおいて匿名通信を実現する手法は，これまでに数多く提案されている．しかしながら，ネットワーク構造が変化してしまうような非静的なネットワークを持つ通信基盤において匿名通信を実現する手法は，Peer to Peer（P2P）の基盤技術を用いた方法しか提案されていない．本論文では P2P 基盤技術を用いず，既存のオニオン・ルーティングをベースとした，新しい匿名通信方式 Valkyrie を提案する．Valkyrie では，オニオン・ルーティングに対して新しいオニオン：代替オニオンおよびバックトラックオニオン，を導入した．これらの新しいオニオンを利用すれば，メッセージ送信途中に分断された経路を迂回することが可能となる．この結果，Valkyrie を用いることで非静的ネットワークにおいて匿名通信を実現できる．

Valkyrie: An Anonymous Routing Scheme on Unstable Network

Shinji Yamanaka,[†] Kazukuni Kobara[††] and Hideki Imai[††]

This paper proposes new anonymous routing scheme Valkyrie. Although, previous works in the literature already addresses the question of anonymity in packet networks, these solutions usually cannot apply to unstable networks, where the network topology changes dynamically. Valkyrie is based multiple encryption scheme and routing technique that is adopted by Onion Routing scheme. Because of that, Valkyrie can transmit messages on (stable) network anonymously. In addition, Valkyrie has two new onions: Alternate Onion and Back Track Onion. These two onions can bypass disconnection on unstable network. Consequently, Valkyrie is anonymous routing scheme which can run on unstable network.

1. はじめに

現在，インターネット上での匿名通信技術が注目を集めている．ネットワーク上での通信内容の秘匿は，SSL のようなセキュリティ要素技術を用いることで解決できる．しかしながら，たとえ SSL を利用したとしても，通信を行っている送信者や受信者がだれであるかを隠すことはできない．すなわち，通信の送信元 IP アドレスや宛先 IP アドレスは，パケットアナライザなどを用いてネットワーク上を流れるパケットのヘッダを読み取ることで確認することができる．このような送受信者の秘匿は，既存の標準化された技術では解決されていない．このことは，インターネットのような公的なネットワーク上で真の意味での匿名通信路を構築することが容易でないことを意味する．

これまでに，インターネット上で匿名通信路を構築する手法はいくつか提案されている[20]．これらの手法は大きく分けて 2 種類に分類される．1 つは，無条件安全性（Unconditionally Secure）を達成する方法で，もう 1 つは多重暗号化を利用して送信者と受信者を隠す方法である．しかし，これらの手法は，ネットワーク構造が動的に変化するネットワークにおいては利用できない．また，最近では P2P ベースの手法も提案されているが，これらの手法では通信路構成ノードが，自身の状態を保存するいわゆる stateful な方式となっており，ノードの負荷が高い．

本論文において提案する手法を Valkyrie と呼ぶことにする．Valkyrie は，オニオン・ルーティング[10),11),14),16),21)] の技術を，非静的ネットワークに対応させた方式である．ただし非静的とは，ネットワークを構成するノードの一部が匿名通信中に追加・離脱する可能性があり，それによりネットワーク構造が変化してしまう状態を指す．また，オニオンとはメッセージとメッセージの送信経路情報を多重暗号化したものである．そしてオニオン・ルーティングは，上記オニオンを利用してメッセージを複数のノードを経由させることにより送信者と受信者のつながりを絶つこ

† 東芝研究開発センター
Corporate Research & Development Center, TOSHIBA CORPORATION
†† 東京大学生産技術研究所
Institute of Industrial Science, The University of Tokyo

とができる技術である．

オニオン・ルーティングの問題点の 1 つに，1 回の通信においてオニオンを 1 個しか持たない点がある．この場合，ネットワーク構造の非静的な変化に対応できない可能性が高い．もう 1 つの問題点として，戻りオニオン（メッセージ受信者がメッセージ送信者に返信する際に用いられるオニオン）をメッセージ送信前に作成してしまう点があげられる．この場合，メッセージを送信した後（あるいは受信者がメッセージを受信した後）でネットワーク構造が変化した場合に，戻りオニオンを利用した返信メッセージが送信者に届かなくなる可能性が高い．

Valkyrie の特徴は，既存のオニオン・ルーティング方式を改良するために「代替オニオン」と「バックトラックオニオン」を導入した点にある．代替オニオンは予備のオニオンである．代替オニオンを利用することにより，たとえば正規の経路（主経路）上において経路途中のノードがネットワークから離脱してしまい，ネットワーク構造が変化した場合でも，遮断された経路を迂回することが可能となる．また，バックトラックオニオンとは，メッセージ送信中に動的に生成される戻りオニオンである．バックトラックオニオンを用いると，メッセージ返信時の経路はメッセージ送信時にアクティブ，すなわち経路が実在していたものになるので，返信メッセージを送信者に届けることができる可能性が高い．これら 2 つのオニオンは，提案方式をネットワーク構造の非静的な変化に対してロバストな方式にしている．

以降の本論文の構成は以下のとおりである．2 章では関連研究について述べる．また 3 章では，本論文における仮定と Valkyrie の目標を示す．4 章では提案方式について説明し，5 章において Valkyrie の安全性および有効性について議論する．そして最後に 6 章でまとめる．

2. 匿名通信路の関連研究

ネットワーク上で匿名通信路を構成する方法については，様々な手法が提案されている[20]．本章では，はじめに提案方式に関連の深い 2 つの手法を紹介した後，その他の匿名通信路ついて簡単に述べる．

MIX ネット[1),2),5),8)] は，複数の MIX サーバで構成された匿名通信の一手法である．**図 1** に，その概観を示す．MIX ネットでは，まずはじめに MIX サーバ 1 が複数の多重暗号化されたメッセージを受け取り，内部に蓄える．そして，サーバ 1 はそれらのメッセージを復号した後にシャッフルして，次の MIX サーバ 2 に送信する．MIX サーバ 2 も同様に受け取ったメッセージを復号・シャッフルして，次の MIX サーバ 3 に送信する．これを繰り返し，メッセージ群を複数の MIX サーバを経由させることにより，最終的に受信者はどのメッセージがだれから届いたのかを見分けることができなくなる．また，すべての MIX サーバが結託をしない限り，送信者とメッセージを結び付けることは不可能となり，匿名性が保たれる．しかしながら，MIX ネットは MIX サーバがつねにオンラインでいることが前提であるため，非静的なネットワークでの利用は難しい．Golle らは，最近「再利用可能な MIX ネット[12)]」を提案しているが，この方法も同様の問題をかかえている．

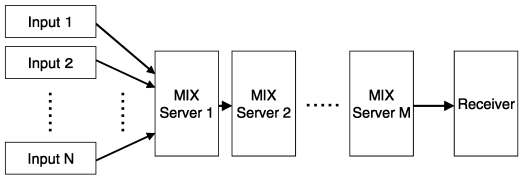


図 1 MIX ネットの概観
Fig. 1 Overview of Mix-net.

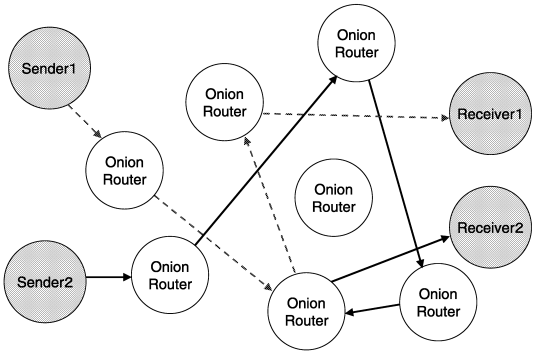


図 2 オニオン・ルーティングの概観
Fig. 2 Overview of Onion Routing.

図 2 にオニオン・ルーティングの概観を示す．図中において破線は Sender1 から Receiver1 へのメッセージの伝達経路を，実線は Sender2 から Receiver2 へのメッセージの伝達経路を表している．オニオン・ルーティングでは MIX ネットのようなシャッフルは行われないが，メッセージと経路情報の多重暗号方式を用いている．MIX ネットとの違いは，送信者が任意の送信・返信経路をあらかじめ選択できることと，ソケット接続をベースにした通信も行えるため，より早いメッセージの送信を行えることにある．しかし，オニオン・ルーティングもまた，ネットワーク構造が非静的に変化することは前提としておらず，メッセージ送信途中の経路において問題が発生したときに対処

できない．

Dining Cryptographer ネットワーク（DC ネット）[3),4),6),9),22),23)] とクリークネット[19)] は，強力な匿名機能（無条件安全性）を有する通信方式である．しかし，これらの方式は匿名通信の参加者同士が膨大な通信をやりとりする必要があり，実際のアプリケーションに利用するのは現実的ではない．

クラウズ[17),18)] は，ルーティングを利用して匿名通信を維持する手法である．オニオン・ルーティングと異なり，クラウズではデータの暗号化を行わないため，通信処理が軽いという特徴がある．そして，データをメンバ間でランダムに転送することで受信者の匿名性を保つ．ただし，送信先はメンバに知られてしまうのでオニオン・ルーティングと比較して匿名性が低いという欠点がある．

オニオン・ルーティングの実現方法として，近年 Universal Re-Encryption（URE）を利用する方式も提案されている．最近では，Klonowski らが，ユーザが経路情報を知らない状態でも匿名通信を可能とすることを目的として，メッセージのルーティング情報と，メッセージ本体とを分離して作成する手法を提案している[13)]．Klonowski らは主に 2 つの手法を提示しており，1 つはルーティング情報を信頼のおける第三者機関に作成してもらい，複数の機関から得られたルートを組み合わせて新しいルートを作成する merge onion の手法である．また，1 つは常時オンラインとなっている特別なサーバを仮定して，これを経路に組み込む online merge onion の手法である．しかしながら，前者の手法はルート情報作成・配布に対するサーバの負荷が大きく，また後者は，常時オンラインのサーバを仮定できるのであれば，このサーバのみを利用して匿名通信を行えばよいため利点が少ない．

また，Dingledine らは文献 7) において，オニオン・ルーティングの改良を行っている．Dingledine らの方式では，過去のトラフィックを再復号できない機構（forward secrecy），protocol cleaning の分離による匿名性維持，ネットワーク負荷制御，ディレクトリサーバの導入などを導入して，より利便性を高めるアプローチをしている．しかしながら，Dingledine らの手法も，ネットワーク構造が非静的に変化することを前提としていない点はオニオン・ルーティングと同様である．

3. 仮定と目標

本章では，本論文で前提とする仮定と，提案方式 Valkyrie の目標を示す．

3.1 提案方式の仮定

本節では，本論文で前提とする仮定を示す．

(1) **初期状態**：提案方式では，ネットワークは複数のノードとノード間を結ぶリンクで構成されているものとする．そしてネットワーク上のすべてのユーザは，Valkyrie のノードになることができる．また，すべてのノードはオニオン・データパケットを処理することが可能なオニオンルータになることができる．さらに，すべてのノードは，公開鍵暗号で用いる公開鍵/秘密鍵対とユニーク ID（IP アドレスや衝突の起きない乱数のようなもの）を持っている．たとえば，ノード X は ID：X と公開鍵：PK_X を持っている．そして，メッセージ送信者はメッセージ受信者の ID を知っているものとする．

(2) **定常的なネットワークトラフィックの存在**：ネットワーク上において通信をしている 2 者以外にだれも通信を行っていない場合を考える．このとき，どのような通信方式を利用しても，ダミーパケットなどを流さない限りその 2 者が通信をしていることは，次にあげるネットワーク盗聴者に知られてしまう．したがって，ネットワーク上においては一定のトラフィックが存在していることを仮定する．

(3) **ネットワーク盗聴者**：本論文では 2 種類の攻撃者を想定する．その 1 つはネットワーク盗聴者である．ネットワーク盗聴者は，ネットワーク上を流れるすべてのデータパケットの盗聴が可能である．すなわち，パケットヘッダの読み取り・パケット長やパケット数の計測を行うことができる．

(4) **悪意のノード**：もう 1 つの攻撃者は，経路上の悪意を持ったノードである．悪意を持ったノードは，だれが自分にメッセージを送ったのか（直前のノード）と，だれにメッセージを送るべきか（直後のノード）を知ることができる．

(5) **結託ノード数の限界**：送信者が送信経路を確定したときに，経路上のすべてのノードが悪意の結託をした場合は，匿名性を維持することができない．そのため，経路上の少なくとも 1 つのノードは結託に参加しないものとする．

(6) **計算量的な限界**：すべての攻撃者は，計算量的な限界を持つ．そのため，適切な暗号方式（アルゴリズム）・鍵の長さを採用することで，攻撃者は現実的な時間内には暗号文を解読することができない．

3.2 提案方式の目標

本節では，Valkyrie の目標を示す．匿名通信方式において，その匿名性としては次の 3 つが考えられる．すなわち，(1) 送信者の匿名性，(2) 受信者の匿名性，(3) 送信者と受信者のつながりの匿名性，である．

「送信者の匿名性がある」とは，ネットワーク上を流れるデータを攻撃者が見たときに，そのデータを送信した者がだれであるかが秘匿されていることを意味する．また，「受信者の匿名性がある」とは，ネットワーク上を流れるデータを攻撃者が見たときに，そのデータを受信する者がだれであるかが秘匿されていることを意味する．そして，「送信者と受信者のつながりの匿名性がある」とは，ネットワーク上を流れるデータを攻撃者が見た結果，ネットワーク上のだれとだれが通信しているかが秘匿されていることを意味する．

たとえば，MIX ネットでは最初の MIX サーバはデータ送信者がだれであるかを確認できるので，最初の MIX サーバに対しては送信者の匿名性が維持されていない．また，クラウズでは，送信先の情報は隠蔽されていないので，受信者の匿名性は維持されていない．Valkyrie の目標は，前節の条件において上記 (1) ～ (3) すべての匿名性を維持することにある．

4. 提 案 方 式

本章では，提案方式の概要および詳細を説明する．

1 章においても述べたが，提案方式 Valkyrie は送信者が受信者に対してメッセージを送信する際に，オニオンと呼ばれる「メッセージとメッセージをルーティングする経路情報を多重暗号化したもの」を利用する．提案方式では，メイン・オニオン，代替オニオン，バックトラックオニオンの 3 つのオニオンを利用する．メイン・オニオンは，既存のオニオン・ルーティングで用いられる ‘オニオン’ と同等の性質を持ち，はじめに優先的に利用される経路情報である．代替オニオンは，メイン・オニオンによって指定された主経路においてなんらかの問題が発生したときに，それを迂回するための予備の経路情報である．主経路において問題が発生しなかった場合には，代替オニオンは使用されない．ここで主経路における問題とは，ノード間の経路の切断や経路上のノードがネットワークから離脱する場合を想定している．

バックトラックオニオンは，メッセージ受信者がメッセージ送信者に対して返信する際に用いられる経路情報である．既存のオニオン・ルーティング方式における戻りオニオンは，メッセージ送信者があらかじめ作成しておき，メッセージに付加して受信者に対して送る．この場合，メッセージ返信時にあらかじめ作成された経路が利用不能となっている可能性がある．これに対し，バックトラックオニオンはメッセージを送信している間に，自分が通過してきた経路を記憶することで，動的に戻りオニオンを作成する．このような仕組みにすることで，メッセージ返信時においてバックトラックオニオンが指定する経路が利用できる可能性が高くなる．

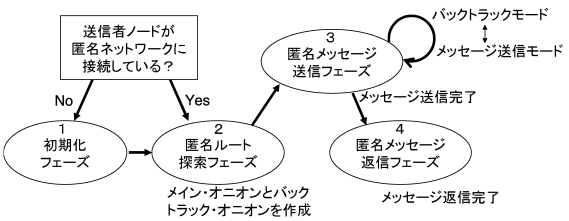


図 3 Valkyrie におけるフェーズのフロー
Fig. 3 The flow of the phase in Valkyrie.

4.1 提案方式の概要

本節では，提案方式の概要を示す．Valkyrie は，**図 3** に示すように，初期化フェーズ，匿名ルート探索フェーズ，匿名メッセージ送信フェーズ，そして匿名メッセージ返信フェーズの 4 つのフェーズから成り立っている．

ここで，メッセージ送信者をノード S，メッセージ送信先（メッセージ受信者）をノード R と呼ぶことにする．初期化フェーズにおいて，まだ匿名通信ネットワークに接続していないノード S は，すでに匿名通信ネットワークに接続済みのノード（ここではノード A と呼ぶことにする）に対して接続を試みる．ノード S とノード A が相互に認証して接続を完了すると次のフェーズに移行する．

匿名ルート探索フェーズでは，ノード S はノード R へとつながる経路を探索する．経路探索をする方法はひととおりではないが，ここでは一例をあげる．ノード S は，まず経路検索メッセージをブロードキャストする．このブロードキャストメッセージは，自分の通過する経路を記録しながらノード R へと転送されていく．その結果，ノード R において複数の経路情報が生成され，これがノード S に戻される．ノード S は，得られた経路のなかから，1 つを主経路として選択し他のいくつかの経路を予備のバックアップ経路として選ぶ．そして，経路情報の多重暗号化を行い，主経路からメイン・オニオンを作成しバックアップ経路から代替オニオンを作成する．それぞれのオニオンはメッセージを内包しており，メイン・オニオンと代替オニオンを適切につなげたものが，最終的なオニオン・データパケットとなる．

メッセージ送信者ノード S がオニオン・データパケットをすぐ隣のノード A に送ると，匿名メッセージ送信フェーズが始まる．このフェーズでは，それぞれのオニオン・ルータは受け取ったオニオン・データパケットに対して復号処理を行い，データパケットを転送する先を調べ，内部のオニオン・データパケットを入手する．そして，必要に応じてバックトラックオニオンを作成・更新し，データパケットを更新する．その後，オニオン・データパケットは次のノードに送信される．この「復号と転送」の繰返しは，オニオン・データパケットがノード R に届くまで続けられる．ここで，ノード R までの送信中に問題が発生しなければ，匿名メッセージ送信フェーズは終了する．しかしながら，途中のノードで問題が発生した場合は，メイン・オニオンの利用を中止し，代替オニオンの利用を試みる．代替オニオンを用いることで，オニオン・データパケットは，メイン・オニオンで通過できなかった経路を迂回することができる．

バックトラックオニオンは，匿名メッセージ返信フェーズにおいて，メッセージ受信者ノード R からメッセージ送信者ノード S に，匿名でメッセージを返信するときに利用される．

4.2 提案方式の詳細

本節では，Valkyrie の動作の詳細を述べる．

4.2.1 初期化フェーズ

初期化フェーズにおいて，メッセージ送信者ノード S とすでにネットワークに接続済みのノード A は相互に認証を行う．この認証方法の一例を**図 4** に示す．図 4 において，$PK_X(a)$ は，データ a を X の公開鍵で暗号化したものである．また，$SK_X(b)$ は，データ b を X の秘密鍵で復号したものである．そして，$Hash(c)$ は，データ c を一方向性関数に入力した出力値である．

ノード S はノード A と相互認証を行うと同時に，別のノード A' とも相互認証を行う．このようにすることで，メッセージがノード S から送られてきたときに，ノード A はそのメッセージがノード A' からノード S に送られて，それが転送されたものか，そもそもノード S が送信したものなのか区別がつかなくなる．すなわち，真のメッセージ送信者がノード S なのかどうかをノード A に対して隠蔽することができる．ノード S が 2 つ以上のノードと相互認証できた時点で，初期化フェーズは終了する．

4.2.2 匿名ルート探索フェーズ

匿名ルート探索フェーズでは，送信者ノード S は受信者ノード R までの経路情報を自分の匿名性を維持したまま知ることができる．匿名経路探索プロトコルは以下のように動作する．まず，ノード S は経路探索パケットをブロードキャストする．そのペイロードは次のように構成される，

$$[R \parallel SF \parallel PK_S^t \parallel DUMMY].$$

ここで，PK_S^t は，探索メッセージ返信時に用いられるノード S の一時公開鍵（使い捨ての公開鍵）である．一時公開鍵を繰り返し使用せずに使い捨てることにより，異なる時期におけるルート探索フェーズどうしのリンクがとれないようになる．また，'$\parallel$' は結合を意味している．そして，$DUMMY$ は適当な長さのダミーデータである．また，パケットのヘッダは，受信者 ID である R およびフラッグ SF を含んでいる．さらに，フラッグ SF は，パケット動作モードが匿名経路探索送信モードであることを意味している．

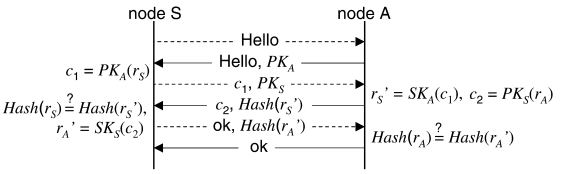


図 4 初期化プロトコルの例：初期化フェーズにおいて 2 つのノードは互いに公開鍵のチェックを行う．これに成功したとき認証成功と見なす
Fig. 4 The example of initialization phase.

図 5 は，匿名ルート探索フェーズの概観を示している．この図において，S は送信者ノードを，R は受信者ノードを意味している．他のノードは中間ノードであり，これらのノード群が匿名通信路を形成している．送信モードにおいて，メッセージ $\{m_i : 1 \leq i \leq 4\}$ は送信者から受信者へとメッセージが流れる様子を示している．また，返信モードにおいては，メッセージ $\{c_i : 1 \leq i \leq 4\}$ が受信者から送信者へと流れることを意味している．

送信モードにおいて，あるノードがパケットを受信したときには，まずパケットの送信先（宛先）がだれであるかを確認する．パケットを受け取ったノード自身が送信先ノードではなかった場合は，直前の（自分にメッセージを送信した）ノードのアドレスと送信者ノードの一時公開鍵とを，自分自身の共通鍵で暗号化する．そして，その暗号化されたデータを受け取ったパケットにつなげ，それを他のノードにブロードキャストする．

パケットを受け取ったノードが受信者ノード R だった場合（すなわち，ヘッダの送信先 ID が自分自身の ID と一致したとき）を考える．このときノード R は返信メッセージを作成し，メッセージが通ってきた経路

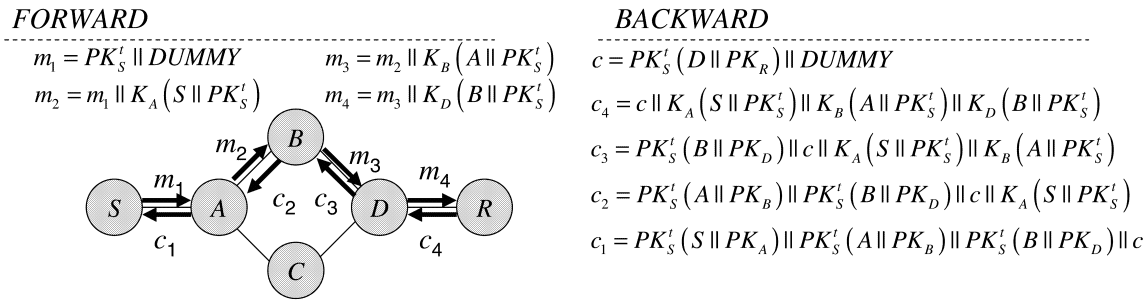


図 5 経路探索プロトコル
Fig. 5 The route seeking phase.

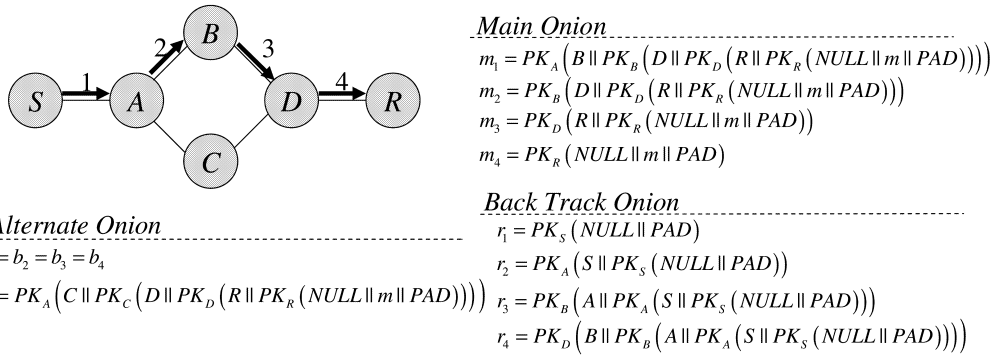


図 6 匿名送信フェーズにおける 3 つのオニオンの変遷：主経路でトラブルが発生しなかった場合
Fig. 6 The anonymous forwarding phase.

を逆方向に向かって転送させる．そのためにまずノード R は，フラッグ SF を，匿名経路探索返信モードを意味する SB に変更する．

そして，1 つ前のノード D の ID と自身の公開鍵 PK_R を，送信者の一時公開鍵 PK_S^t を用いて暗号化して，$PK_S^t(D \| PK_R)$ を作成する．このペイロードに対して，受信したデータを結合し，これを返信パケットとして返信する．図 5 における $BACKWARD$ は，返信データの例である．

中間ノードが返信パケットを受け取った場合は，まずパケットの最後尾部分を自身の共通鍵で復号する．その結果，次に送るべきノード（匿名経路探索送信モードにおいて自分に直接パケットを送信したノード）の ID と，送信者の一時公開鍵 PK_S^t を入手する．そして，中間ノードはその ID と自分自身の公開鍵を一時公開鍵を用いて暗号化する．最後に，暗号化したデータを受け取ったパケットの最前部に結合し，送信者側の次のノードに転送する．

これにより，送信者ノードは複数の経路情報を入手する．そして，得られた経路情報から主経路とバックアップ経路を選択し，メイン・オニオンおよび代替オニオンを作成する．

4.2.3 匿名メッセージ送信フェーズ

既存のオニオン・ルーティングに対する提案方式の利点は，代替オニオンとバックトラックオニオンにある．これらのオニオンを用いれば，非静的なネットワークに対して動的に適応することが可能である．本項では，匿名メッセージ送信フェーズの動作を示す．

はじめに，送信者はメイン・オニオン，代替オニオン，そしてバックトラックオニオンを作成する．たとえば，ネットワークトポロジが図 5 のようになっていた場合，3 種類のオニオンを**図 6** の m_1，b_1，r_1 のように作成する．

この図において $PK_X(Y \| z)$ は，2 つの情報 Y と z が結合されて，ノード X の公開鍵で暗号化されることを意味する．また，1 番目の引数 Y は，次に送信すべきノードの名前（宛先）であり，2 番目の引数 z はデータパケットペイロードである．そして，“m” は，送信者から受信者に送られるメッセージである．“$NULL$” は，次に送るべきノードが存在しないことを意味している．“PAD” はパディングで，真の受信者がだれであるのかを，中間ノードから隠蔽するために用いられている．送信者は，これらのオニオンを 1 つのデータパケットとして送信する．

匿名メッセージ送信フェーズでは 2 つの動作モード

が存在する．1つはメッセージ送信モードであり，もう1つはバックトラックモードである．メッセージ送信モードは平常の状態であり，主経路伝送中において経路の断線などのトラブルが発生していない場合のモードである．一方，主経路においてトラブルが発生した場合には，動作モードはバックトラックモードに切り替わる．そして，代替オニオンが利用可能となる分岐ノードまでの復帰（バックトラック）を試みる．無事に分岐ノードにたどり着いて，代替オニオンが利用可能となった場合には，動作モードは再びメッセージ送信モードに移行する．

まず，メッセージ送信モードにおける中間ノードの動作について説明する．ある中間ノードがメッセージ送信モードのデータパケットを受信した場合，メイン・オニオンおよびバックトラックオニオンの更新を行う．具体的には，まず，次に送るべきノードを知るためにメイン・オニオンを復号し，同時に次のノードに転送するデータパケット（新しいメイン・オニオン）を入手する．次に，受信データのバックトラックオニオン r と，自分にデータを転送した（1つ前の）ノード名 Y を自身の公開鍵 PK_X を使って暗号化して，新しいバックトラックオニオンを作成する．すなわち，$PK_X(Y \parallel r)$ が，更新されたバックトラックオニオンになる．

図6は匿名メッセージ送信フェーズの様子を示している．S は送信者ノード，R は受信者ノードを意味している．他の A，B，C，D は中間ノードである．ここで，ノード A の動作を説明する．ノード A はデータパケットを受け取ると，まずメイン・オニオンを復号する．その結果，次に送るべきノードはノード B であることを知る．次にバックトラックオニオン r_1=$PK_S(NULL \| PAD)$ と1つ前のノード S のノード名を自身の公開鍵 PK_A で暗号化する．すなわち，新しいバックトラックオニオンは $r_2 = PK_A(S \parallel r_1)$ となる．代替オニオンはバックトラックが行われていないので，更新されない．最後にこれらのオニオンを1つのオニオン・データパケットとして，ノード B に転送する．$1 \leq i \leq 4$ におけるメイン・オニオン (m_i)，代替オニオン (b_i)，バックトラックオニオン (r_i) の中身は図6に示すとおりである．データ送信がタイムアウトとならなかったときに，ノード A の動作は終了する．

次に，バックトラックモードにおける中間ノードの動作について説明する．メッセージの転送経路上において，ネットワークからの離脱などにより次ノードが消失したとする．すると，その手前の中間ノード X が，メッセージ送信モードのデータパケットを送信したときにタイムアウトとなる．このときノード X は，そのデータパケットをメッセージ送信モードからバックトラックモードへ移行させる．

ただし，代替オニオンは，送信者があらかじめ決めた主経路上のあるノードから，別の経路への分岐情報であるため，その分岐ノード以外のノードは代替オニオンを復号できない．ノード X は，まずデータパケットの代替オニオンの復号を試みて，自身が代替オニオンを利用可能か否かを確認する．ここで代替オニオンを復号できた場合は，その代替オニオンを新しい主経路情報と見なし，データパケットのモードをメッセージ送信モードに戻したうえで，データパケットの転送を再開する．一方，代替オニオンを復号できなかった場合は，バックトラックオニオンを復号し，その情報をもとにデータパケットが送られてきた方向に転送することで，バックトラック（後戻り）を行う．

バックトラックモードのデータパケットを受信した中間ノードは，ノード X と同様の確認・処理を行う．そして，分岐ノードがデータパケットを受信するまでバックトラック動作が繰り返される．

図7 は，匿名メッセージ送信フェーズのもう1つの例である．この図では，匿名ルート探索フェーズが終了した後に，主経路上のノード B とノード D の間で経路の切断が発生した場合を想定している．ノード B がメッセージ送信パケットを受け取った瞬間において，3つのオニオンの中身はそれぞれ $m_2 = PK_B(D \parallel PK_D(R \parallel PK_R(NULL \parallel m \parallel PAD)))$，$b_2 = PK_A(C \parallel PK_C(D \parallel PK_D(R \parallel PK_R(NULL \parallel m \parallel PAD))))$，$r_2 = PK_A(S \parallel PK_S(NULL \parallel PAD))$ のようになっている．

そして，ノード B はプロトコルに従って新しいオニオンを以下のように作成して，ノード D に転送する．

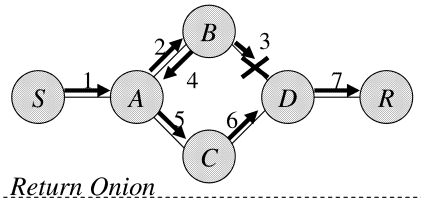
$m_3 = PK_D(R \parallel PK_R(NULL \parallel m \parallel PAD))$,

$b_3 = b_2$,

$r_3 = PK_B(A \parallel PK_A(S \parallel PK_S(NULL \parallel PAD)))$.

ノード D から受信確認が返らずタイムアウトになった場合には，ノード B はメイン・オニオンを使用を中止し，代わりに代替オニオンの使用を試みる．前述のとおり，Valkyrieでは代替オニオンの迂回分岐ノードに戻るまでは，今まで作成したバックトラックオニオンを復号しながら送信者側へと戻っていく．そして，代替オニオンを使用可能なノードに到着すると，その代替オニオンを新しいメイン・オニオンと見なして，受信者側への転送を再開する．

図7では，メイン・オニオン m_3 の使用を中止し



Main Onion

$$m_1 = PK_A\left(B \| PK_B\left(D \| PK_D\left(R \| PK_R\left(NULL \| m \| PAD\right)\right)\right)\right)$$
$$m_2 = PK_B\left(D \| PK_D\left(R \| PK_R\left(NULL \| m \| PAD\right)\right)\right)$$
$$m_3 = PK_D\left(R \| PK_R\left(NULL \| m \| PAD\right)\right)$$
$$m_4 = b_2 = PK_A\left(C \| PK_C\left(D \| PK_D\left(R \| PK_R\left(NULL \| m \| PAD\right)\right)\right)\right)$$
$$m_5 = PK_C\left(D \| PK_D\left(R \| PK_R\left(NULL \| m \| PAD\right)\right)\right)$$
$$m_6 = PK_D\left(R \| PK_R\left(NULL \| m \| PAD\right)\right)$$
$$m_7 = PK_R\left(NULL \| m \| PAD\right)$$

Alternate Onion

$$b_1 = b_2 = b_3 = PK_A\left(C \| PK_C\left(D \| PK_D\left(R \| PK_R\left(NULL \| m \| PAD\right)\right)\right)\right)$$

Return Onion

$$r_1 = PK_S\left(NULL \| PAD\right)$$
$$r_2 = PK_A\left(S \| PK_S\left(NULL \| PAD\right)\right)$$
$$r_3 = PK_B\left(A \| PK_A\left(S \| PK_S\left(NULL \| PAD\right)\right)\right)$$
$$r_4 = PK_A\left(S \| PK_S\left(NULL \| PAD\right)\right)$$
$$r_5 = PK_A\left(S \| PK_S\left(NULL \| PAD\right)\right)$$
$$r_6 = PK_C\left(A \| PK_A\left(S \| PK_S\left(NULL \| PAD\right)\right)\right)$$
$$r_7 = PK_D\left(C \| PK_C\left(A \| PK_A\left(S \| PK_S\left(NULL \| PAD\right)\right)\right)\right)$$

図 7 匿名送信フェーズにおける 3 つのオニオンの変遷：主経路上のノード B とノード D の間でトラブルが発生した場合
Fig. 7 The anonymous forwarding phase.

て，代替オニオン b_2 を新しいメイン・オニオン m_4 として利用する様子を示している．すなわち，ノード B は，代替オニオンの復号を試みるが，復号に失敗することで自身が分岐ノードでないことを確認する．そしてバックトラックオニオンを復号し，バックトラックすべきノードがノード A であることを知る．ノード B は，パケットの動作モードをバックトラックモードに変更したうえで，ノード A にデータパケットを転送する．

ノード A は，データパケットを受信すると，まず代替オニオンの復号を試みる．代替オニオンの最外層はノード A の公開鍵で暗号化されているので，ノード A はその復号に成功する．自分が分岐ノードであることを確認したノード A は，代替オニオンを新しいメイン・オニオンとして使用し，古いメイン・オニオンの使用を中止する．また，バックトラックオニオンには変更を加えず，データパケットの動作モードをメッセージ送信モードに戻す．さきほどの復号の結果から，次に転送すべきノードはノード C であることが分かるので，データパケットをノード C に送る．最終的に，この新しいメイン・オニオンを利用することで，トラブルの箇所を迂回して受信者までメッセージを送ることができる．

4.2.4 匿名メッセージ返信フェーズ

匿名メッセージ送信が終了したとき，受信者はメッセージと同時にバックトラックオニオンを入手している．このバックトラックオニオンを用いることにより，受信者は自身の匿名性を維持しつつ，送信者に対して返信を行うことができる．バックトラックオニオンは，ある種のオニオンであるが，メイン・オニオンや代替オニオンと異なり，返信メッセージを含んではいない．そのため，バックトラックオニオンは返信メッセージに結合される形で利用される．

中間ノードがバックトラックオニオンを受け取ったときには，メイン・オニオンの場合と同様にそれを復号し次の転送先を取り出して，転送を行う．そして，最終的には送信者のもとへ返信メッセージが到着し，匿名メッセージ返信フェーズは完了する．

5. 安全性と有効性

5.1 匿 名 性

送信者の匿名性：4.2.1 項で述べたように，初期化フェーズにおいてすべてのノードは他の 2 つ以上のノードと接続を行う．そして，メッセージ送信者 S は初期化フェーズ直後にはオニオン・データパケットの送信を行わずに，ある適当な時間が経過するのを待つ．その後，データパケットの送信を開始することにより，このデータを受け取った転送ノード A は，そのデータが S からのものであるか，S が他のノードから受け取ったデータを転送したものであるかを区別できない．これにより送信者の匿名性は保たれる．

ただし，S が初期化フェーズに 2 個のノードと接続を行ったときに，その 2 ノードが結託していた場合には送信者の匿名性は維持できない．この場合は，S は初期化フェーズに多数のノードと接続を行うことにより結託攻撃の回避を試みることが可能である．

受信者の匿名性：オニオン・データパケットは，メイン・オニオン，代替オニオン，バックトラックオニオンにより構成されている．そして，4.2.3 項で述べたように，パディングによりオニオン・データパケット全体の長さは隠蔽されている．さらに，多重暗号化により各オニオンどうしの境界部分は，送信者および受

信者以外のノードには特定することができない．この結果，中継ノードは，受け取ったオニオン・データパケットを分析しても，多重暗号を解読しない限りは，自分から何ホップ先に受信者が存在するかを有意な確率で推定することはできない．よって，受信者の匿名性も確保される．

この結果，Valkyrie では，送信者の匿名性と，受信者の匿名性がともに確保されているため，データ送信系路上のすべてのノードが結託しない限りにおいては，送信者と受信者のつながりの匿名性も確保される．

5.2 タイムアウト・MAC の利用

提案方式は，経路途中のノードが転送不能となっていて転送に失敗した場合や，攻撃者がデータパケットの削除をした場合に，タイムアウトを利用してバックトラックモードに移行することができる．また，攻撃者がデータパケットを改ざんすることも考えられるが，この攻撃に対してはメッセージ認証子（MAC）を導入することで対処可能である．MAC の利用の詳細については文献 15) を参照されたい．

5.3 動作モードの漏洩

匿名メッセージ送信フェーズにおいて，メッセージ送信モードとバックトラックモードの切替えが発生する．そして中継ノードは，オニオン・データパケットを受け取った際に，パケットに対して適切な処理をするために，そのデータパケットがどちらのモードになっているかを知る必要がある．つまりデータパケットのモードの情報は，暗号化されずにヘッダ情報として格納されることになる．この情報は，攻撃者も知ることが可能であるため，ここでは，どちらのモードになっているかを攻撃者が知ることにより匿名性が低くなるかどうかを議論する．

ネットワーク盗聴者は，経路途中で盗聴したオニオン・データパケットの動作モードを盗み見ることが可能である．しかしながら，動作モードがどちらであるにせよ，「データパケットが受信者側に転送されている」ということ以上の情報は得られないため，ネットワーク盗聴者に対する匿名性が低くなることはない．

悪意のノードが，オニオン・データパケットの動作モード情報を，攻撃に利用する場合を考える．単純な転送，すなわち送られてきたデータを次のノードに転送するだけの場合には，「データパケットが受信者側に転送されている」ということ以上の情報は得られない．一方，分岐ノードが悪意のノードであった場合には，バックトラックモードからメッセージ送信モードに切り替える際に，代替オニオンのサイズを知ることができる．しかしながら，代替オニオンはダミーデータを含んでいるので，受信者までのノード数は隠蔽されている．さらに受信者 R は，データを受信した後にダミーデータを別のノードに送信することにする．この結果，たとえ悪意の分岐ノードから受信者 R の直前のノードまでが結託したとしても，R が真の受信者であることを特定することは困難であり，匿名性が低くなることはない．

5.4 メッセージ量・通信回数の比較

Valkyrie のメッセージ量は，実装方法に依存する．たとえば，RSA を公開鍵暗号として，RC4 を共通鍵暗号として用いた場合を考える．そして 1 ホップ，すなわち中継ノードを 1 つ追加するために必要なデータサイズを u とする．また，オニオン・ルーティングの中継ノードの個数（ホップ数）および Valkyrie のメイン・オニオンの中継ノードの個数を k，代替オニオンの中継ノードの個数を $k/2$ であるとし，パディングやダミーデータのサイズを無視する．そして，代替オニオン，つまり予備のルート情報の数は m 個であるとする．オニオン・ルーティングの場合は，メッセージ全体のサイズが，ku であるのに対し，Valkyrie の場合は $ku(1 + m/2)$ となり，そのメッセージ量は予備の経路情報代替オニオンをいくつ保持するかに比例する．

次に，バックトラックが発生した場合のノード間の通信回数を考察する．メイン・オニオンの中継ノードの個数が k_1 であるとする．そして，代替オニオンが 1 つ含まれており，その中継ノードの個数を k_2 とする．するとメイン・オニオンと代替オニオンの構造，および，どの中継ノードが通信不能となったかにより通信回数は変化する．メイン・オニオンの中間の中継ノードに分岐があり，また $k_2 = k_1/2$ であると仮定する．そして，通信不能ノードがメイン・オニオンの分岐後に存在するものとする．すると，通信回数は平均的には，(メイン・オニオンによる通信回数)+(バックトラックオニオンによる通信回数)+(代替オニオンによる通信回数)，すなわち

$$\frac{3}{4}k_1 + \frac{1}{4}k_1 + k_2 = \left(\frac{3}{4} + \frac{1}{4} + \frac{1}{2}\right)k_1 = \frac{3}{2}k_1$$

となる．

一方，オニオン・ルーティングにおいてメッセージの転送に失敗して経路の再構成を行い，メッセージの再送信を行った場合を考える．Valkyrie の場合と同様に，転送経路上の中間以降のノードに通信不能ノードが存在するものとする．すると，通信回数は平均的には，(転送不能ノードまでの通信回数)+(再送信時の通信回数)，すなわち

$$\frac{3}{4}k_1 + k_1 = \frac{7}{4}k_1$$

となる．

すなわち，Valkyrie とオニオン・ルーティングを比較した場合，Valkyrie のほうがメッセージ量が多い（代替オニオンの個数に比例する）のに対して，経路上に通信不能ノードが存在した場合には，平均的には Valkyrie の通信回数のほうが少なくなる．

5.5 送受信失敗の可能性

代替オニオンおよびバックトラックオニオンを導入することにより，非静的なネットワークにおいてメッセージ送受信が成功する確率は，既存のオニオン・ルーティングと比較すれば高くなる．しかし，たとえばメイン・オニオンとすべての代替オニオンにおいて経路の切断などの問題が発生した場合には，提案方式においてもメッセージの送受信に失敗してしまう．すなわち，提案手法を用いても，非静的なネットワークにおいて送受信を 100%成功させることはできない．

6. ま と め

本論文では，新しい匿名通信方式 Valkyrie を提案した．既存の匿名通信方式とは異なり，Valkyrie ではネットワーク構造が非静的に変化した場合にも対応可能な方式として構成しているため，非静的なネットワークに適した強力な匿名通信の手法となっている．ただし，本論文では Valkyrie の概念説明に紙面の大部分を割いたため，データパケットの細部構造は割愛した．今後の課題は，今回提案したプロトコルをより簡潔なものとするとともに，攻撃者による盗聴・改ざんなどに対応できる方式としていくことである．また複数の予備経路を持たせることによりデータパケットが肥大化するため，通信量の削減も今後の目標となる．

謝辞 論文全体の構成および提案方式に関して数多くの貴重なコメントをいただいた査読者の方々に深く感謝いたします．

参 考 文 献

1) Abe, M.: Universally verifiable mix-net with verification work independent of the number of MIX servers, *Proc. EUROCRYPT'98*, Lecture Notes in Computer Science, Vol.1403, pp.437–447 (1998).
2) Berthold, O., Federrath, H. and Kopsell, S.: Web MIXes: A system for anonymous and unobservable internet access, *Anonymity 2000*, Lecture Notes in Computer Science, Vol.2009, pp.115–129 (2000).
3) Bleumer, G.: DC network (2004). http://www.francotyp.com/research/bleumer/EncInfSec/GBI.DCNetwork.pdf
4) Bos, J. and Boer, B.D.: Detection of disrupters in the DC protocol, *Proc. EUROCRYPT'89*, Lecture Notes in Computer Science, Vol.434, pp.320–327 (1990).
5) Chaum, D.: Untraceable electronic mail, return addresses and digital pseudonyms, *Comm. ACM*, Vol.24, No.2, pp.84–88 (1981).
6) Chaum, D.: The dining cryptographers problem: Unconditional Sender and Recipient Untraceability, *Journal of Cryptology*, Vol.1, pp.65–75 (1988).
7) Dingledine, R., Mathewson, N. and Syverson, P.: Tor: The Second-Generation Onion Router, *Proc. 13th USENIX Security Symposium* (2005).
8) Dingledine, R. and Syverson, P.: Reliable MIX cascade networks through reputation, *Proc. Financial Cryptography*, Lecture Notes in Computer Science, Vol.2357, pp.253–268 (2002).
9) Dolev, S. and Ostrovsky, R.: Efficient anonymous multicast and reception, *Proc. CRYPTO'97*, Lecture Notes in Computer Science, Vol.1294, pp.395–409 (1997).
10) Goldschlag, D., Reed, M. and Syverson, P.: Onion routing for anonymous and private internet connections, *Comm. ACM*, Vol.42, No.2, pp.39–41 (1999).
11) Goldschlag, D.M., Reed, M.G. and Syverson, P.F.: Hiding routing information, Lecture Notes in Computer Science, Vol.1174, pp.137–150 (1996).
12) Golle, P. and Jakobsson, M.: Reusable Anonymous Return Channels, *Proc. Workshop on Privacy in the Electronic Society* (*WPES*) (2003).
13) Klonowski, M., Kutyowski, M. and Zagórski, F.: Anonymous Communication with On-line and Off-line Onion Encoding, Lecture Notes in Computer Science, Vol.3381 (2005).
14) Korba, L., Song, R. and Yee, G.: Anonymous communications for mobile agents, *Proc. 4th International Workshop on Mobile Agents for Telecommnunication Applications*, Vol.44948 (2002).
15) Moller, B.: Provably Secure Public-Key Encryption for Length-Preserving Chaumian Mixes, *Topics in Cryptology* (*CT-RSA2003*), Lecture Notes in Computer Science, Vol.2612, pp.244–262 (2003).
16) Reed, M.G., Syverson, P.F. and Goldschlag, D.M.: Anonymous connections and onion routing, *IEEE Journal on Specific Areas in Communications*, Vol.16, No.4, pp.482–494 (1998).

17) Reiter, M.K. and Rubin, A.D.: Crowds: Anonymity for web transactions, *ACM Trans. Information and System Seurity*, pp.66–92 (1998).
18) Reiter, M.K. and Rubin, A.D.: Anonymous Web Transactions with Crowds, *Comm. ACM*, Vol.42, No.2, pp.32–38 (1999).
19) Sirer, E.G., Polte, M. and Robson, M.: CliqueNet: A Self-Organizing, Scalable, Peer-to-Peer Anonymous Communication Substrate. http://www.cs.cornell.edu/People/egs/papers/cliquenet-iptp.pdf
20) Song, R. and Korba, L.: Review of network-based approaches for privacy, *Proc. 14th Annual Canadian Information Technology Security Symposium*, Vol.44905 (2002).
21) Syverson, P.F., Goldschlag, D.M. and Reed, M.G.: Anonymous connections and onion routing, *Proc. 1997 IEEE Symposium on Security and Privacy*, pp.44–54 (1997).
22) Waidner, M.: Unconditional sender and recipient untraceability in spite of active attacks, *Proc. EUROCRYPT'89*, Lecture Notes in Computer Science, Vol.434, pp.302–319 (1990).
23) Waidner, M. and Pfitzmann, B.: The dining cryptographers in the disco: Unconditional Sender and Recipient untraceability with computationally secure serviceavility, *Proc. EUROCRYPT'89*, Lecture Notes in Computer Science, Vol.434, p.690 (1990).

(平成 16 年 11 月 30 日受付)
(平成 17 年 6 月 9 日採録)

山中　晋爾

昭和 50 年生．平成 13 年東京理科大学大学院工学系研究科電気工学専攻修士課程修了．平成 16 年東京大学大学院情報理工学系研究科電子情報学専攻博士課程を単位取得のうえ退学．同年株式会社東芝入社．現在，暗号および情報セキュリティの研究開発に従事．平成 12 年 SCIS 論文賞受賞．電子情報通信学会会員．

古原　和邦

昭和 45 年生．平成 6 年山口大学大学院工学研究科博士前期課程知能情報システム工学専攻修了．同年東京大学生産技術研究所入所．暗号と情報セキュリティの研究に従事．平成 15 年東京大学より博士号（工学）取得．著書に『電子透かし技術—ディジタルコンテンツのセキュリティー』（画像電子学会編，共著，東京電機大学出版局），『情報セキュリティハンドブック』（電子情報通信学会編，共著，電子情報通信学会），『Mobile Communications Secruity』（H. Imai Ed.，共著，Artech House Publishers）．平成 8 年 SCIS 論文賞，平成 13 年 WISA 論文賞，平成 14 年 ISITA 論文賞，平成 15 年 SCIS20 周年記念賞，電子情報通信学会論文賞および猪瀬賞受賞．電子情報通信学会，国際暗号研究学会（IACR）会員．

今井　秀樹（正会員）

昭和 41 年東京大学工学部電子工学科卒業．昭和 46 年同大学院博士課程修了．工学博士．昭和 47 年横浜国立大学助教授．昭和 59 年同教授．平成 4 年東京大学教授（生産技術研究所）．平成 17 年産総研セキュリティセンター長兼務．現在に至る．この間，符号理論，情報セキュリティ，通信方式等の研究に従事．電子情報通信学会著述賞，論文賞，米澤メダル，猪瀬賞，業績賞，功績賞，IEEE シャノン記念論文賞，総務大臣表彰，経済産業大臣表彰等受賞．著書『情報理論』『符号理論』『暗号のおはなし』等．信学会理事，監事，IEEE 情報理論ソサイエティ会長，国際暗号研究学会理事，情報理論とその応用学会会長，CRYPTREC 委員長等を歴任．IEEE，信学会フェロー．名誉博士（韓国，仏国）．