匿名性確保と不正者追跡の両立が可能な通信方式

千田浩司[†] 小宮輝之[†] 林 徹[†]

本論文では，インターネット上における，利用者の不正防止およびプライバシ保護の両立を目的として，通常の通信では利用者の十分な匿名性を提供するが，匿名の利用者による不正が発覚した場合は，その匿名性を失効することが可能な技術を提案する．提案方式は，利用者が誰と通信しているかのプライバシ情報を知ることはどの機関であっても困難とでき，一方で利用者の匿名性悪用による不正を防止するために，事前に承認された複数の第三者機関のうちの一定数以上が正しく協力した場合は，その不正利用者を特定できる．逆に第三者機関どうしが結託した場合でも，その結託した機関が一定数に満たなければ利用者のプライバシは侵害されずに済む．さらに提案方式は，各機関の処理正当性が検証可能であることを特徴とし，これにより信頼できる機関を仮定する必要がなくなる．すなわち，正当な利用者の匿名性，および不正者追跡処理に関する頑健性が保証される．したがって本提案技術により，インターネット利用者の匿名性および不正者追跡可能性の両立というトレードオフ問題が解決される．

Anonymous Networks with a Robust Anonymity Revocation Scheme

Koji Chida,[†] Teruyuki Komiya[†] and Toru Hayashi[†]

For protecting both privacy and illegal act on the Internet, we present a scheme that ordinarily provides user anonymity but enables us to revoke the anonymity only if a corruption has been detected. A remarkable feature of the proposed scheme is the ability to revoke anonymity if more than threshold third parties, who are recognized by users in advance, perform the procedure of anonymity revocation correctly. In other words, users' communication privacy is guaranteed unless more than threshold third parties collude. Another feature is that the correctness of the procedure of every related organization is verifiable, and thereby provides anonymity and preserves the robustness of the anonymity revocation scheme. Therefore, using the proposed scheme, we can solve the trade-off between communication privacy and the traceability of malicious users.

1. はじめに

1.1 背景

近年のインターネット社会では，その匿名性の高さから，不正取引や個人の名誉毀損にあたるような情報公開等の事件が後を絶たない．これらの問題を防ぐために，インターネット接続のゲートの役割を持つISPやその他各種サービスプロバイダが通信ログを保管しておき，問題が発生した場合には不正な情報の発信元を開示可能とする対策がとられているが，これは十分な対策であるとはいい難い．たとえば，通信路に匿名プロキシ[1)]を中継させることで，受信端末に発信元の個人情報やIPアドレス等の端末情報をいっさい与えないことが可能となり，匿名プロキシが外国で管理されていれば，発信元の開示処理はさらに難航する．加えて匿名プロキシが多段に中継されている場合は，その中継数に応じて問題がさらに深刻化し，少なくとも1台の匿名プロキシの通信ログが削除されてしまえば，発信元に関する情報の取得は困難を極める．しかし冒頭であげた匿名性悪用の問題に対して，情報の発信元と受信先あるいは受信メッセージの関係を集中管理することで解決を図る場合は，特に発信元である利用者のプライバシの観点からみて望ましくない．すなわち，つねに通信が管理されているという利用者の心理的な抑圧があることに加え，管理機関に保管された通信ログが，内部犯行，人的ミス，システムのセキュリティホール等によって漏洩した場合の被害が甚大になるという問題が生じる．

一方，通信路における匿名性を効果的に高める実用的な手段として，Mix-net[3)]やOnion Routing[10)]と呼ばれる技術がそれぞれ知られている．これらはともに，通信路にプロキシを多段に中継させ，各プロキシは前段のプロキシあるいは送信端末から受信した情

† NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories

報に対して特定の暗号処理を施し，その変換された情報を後段のプロキシあるいは受信端末に送信することで，情報の発信元と受信端末あるいはそれに送信されたメッセージとの対応関係をすべての機関に対して秘匿する技術であり，これにより受信端末に送信されたメッセージの発信元を特定することは，受信者はもとより，各々の中継プロキシ管理者でさえ非常に困難となる．Mix-net および Onion Routing の特徴や技術的差異については 2.1，2.2 節で述べるが，Mix-net は電子投票への適用が代表的であり，Onion Routing は e-mail，Web ブラウズ等，即時性が求められる通信に適していることで知られる．

1.2 課　　題

Mix-net や Onion Routing に代表される，各プロキシが暗号処理を施すことで実現される多段プロキシ中継型の匿名通信路技術を用いた場合，情報の発信元となる利用者は，自分自身と，通信相手あるいは送信メッセージという関係を任意の機関に対して秘匿することが可能となり，受信者に送信されたメッセージの発信元を特定するためには，基本的には通信経路を遡り経路中にある全プロキシの管理者に逐次情報開示を求めなければならない☆．

それでは前記にあげた匿名通信路技術は，利用者の匿名性悪用に対してはどの程度耐性があるだろうか．一般には，匿名性と追跡可能性はトレードオフの関係であることから，プロキシを多段に中継すればする程，匿名性は向上するが不正者追跡は困難になる．逆に中継させるプロキシが少なければ，管理者の不正結託等による匿名性侵害の危険性が高まる．また不正者追跡を重視した場合，プロキシ側で通信ログを保管する必要が生じ，一般にいつそのログが必要となるか分からないために運用面での負担が大きいと考えられ，さらにログの真正性も考慮する必要がある．この場合少なくとも，プロキシ管理者によるログ改ざんを防ぐ手段が求められる．また不正情報発信元の端末情報（IP アドレス等）を得たとしても，実際に不正をはたらいた利用者が特定できなければ問題解決とならない場合が多い．しかし利用者側と管理者側の双方の立場をふまえて考えれば，十分信頼できる匿名性，および頑健な不正者追跡処理は，両立されるべき条件であるといえよう．

1.3 解決手段の特徴と効果

本論文では，1.2 節で与えた匿名性と不正者追跡可能性のトレードオフ問題に着目し，解決手段として，匿名性と不正者追跡可能性を閾値制御可能な方式を提案する．提案方式の基盤技術は，各プロキシの暗号処理により実現される多段プロキシ中継型の匿名通信路技術に加え，処理正当性が検証可能な秘密分散技術[7]（VSS: Verifiable Secret Sharing scheme）を応用した閾値暗号技術[4),6),8)] となり，これらの技術の組合せにより提案方式が実現される．提案方式では複数の第三者機関を必要とし，不正利用者を追跡するための処理は，閾値数以上の第三者機関が合意することで実行可能となる．逆に，この不正利用者追跡処理が実行可能な特徴により，閾値数以上の第三者機関が不正結託した場合は正当な利用者であっても匿名性を侵害されてしまう．また送受信端末間を中継する全プロキシの管理者が結託した場合も同様に利用者の匿名性が侵害される．ただし第三者機関の閾値数は，可変だがシステムにおいて単一である一方，中継プロキシ数は，各々の利用者が通信ごとに任意に選ぶことができる．そのため第三者機関の閾値数は，事前に選ばれた第三者機関の信頼性を加味してシステム管理者が慎重に選ぶ必要がある．

一方，プロキシ管理者は不正者追跡処理に立ち会う必要がなく，さらにプロキシ側で通信ログを保管する必要もないため，運用面での負担が少なく済む．そして閾値数を満たす任意の第三者機関の協力により実行される不正者追跡処理は，その処理正当性が公開検証可能であるため，高い頑健性を有するとともにすべての第三者機関を信頼する必要はない．不正者追跡処理全体における頑健性は，プロキシ管理者が不正者追跡処理を妨害しない限り不正利用者を確実に特定でき，プロキシ管理者の処理妨害があった場合は，その事実が発覚する．またもちろん，無実の利用者またはプロキシ管理者を不正者に仕立てる不正行為も技術的に困難となる．

2. 関 連 技 術

提案方式を説明する前に，本章では提案方式の基盤をなす主な既存技術について概要紹介する．

2.1 Mix-net [3)]

Mix-net は，ネットワーク上に複数配置されたプロキシから構成され，各プロキシは複数の入力暗号文各々に対し暗号処理を施したうえで，ランダムな順序

☆ 実際の Onion Routing システム[11)] では，送信端末からの情報を受信するエージェントが存在し，送受信端末の対応関係を切り離す処理を行う．したがって，不正利用者の操作する端末情報をエージェントが特定できる反面，そのエージェントに対しては利用者の匿名性が十分保護されない．本論文では利用者の匿名性向上の目的で，前記エージェントの処理は送信端末自体が行う構成とし，単一機関による利用者の匿名性侵害をより困難にしている．

でそれらを出力することで入出力の対応関係を撹乱するような匿名通信路技術である．そしてこの操作により，すべてのプロキシの内部情報を知ることなく，複数からなる情報発信元と，受信端末に送信された複数のメッセージとの対応付けを任意の攻撃者に対して困難にする．

次に Mix-net のプロトコルについて説明する．今，情報発信元の利用者あるいはその操作端末を U_j $(j = 1,\ldots,n)$，プロキシを M_i $(i = 1,\ldots,m)$，受信端末を R とする．このとき，まず U_j は R に送信するメッセージ msg_j に対して，暗号文 $C_i^{(j)} \stackrel{\text{def}}{=} \mathcal{E}_{i+1}(C_{i+1}^{(j)})$ $(i = m-1,\ldots,0)$ を生成する．ここで $C_m^{(j)} = msg_j$ とし，$\mathcal{E}_i$ は M_i のみ復号可能な暗号関数とする．そして通信時には，M_i は n 個の暗号文の組 $\{C_{i-1}^{(j)}\}$ を M_{i-1}（$i = 1$ であれば U_j）から受信し，すべての暗号文に対し復号処理を施し，その復号結果の順序をランダムに並べ替えた組 $\{C_i^{(j)}\}$ を M_{i+1}（$i = m$ であれば R）へ送信する．これにより，利用者の匿名性を侵害することを目的とする攻撃者 $\mathcal{A}$ が，M_a $(1 \le a \le m)$ の内部情報の取得が不可能であるとき，$\{C_{a-1}^{(j)}\}$，$\{C_a^{(j)}\}$ の対応付けの困難性は，暗号関数 $\mathcal{E}_i$ の秘匿性に帰着する．すなわち，$\mathcal{A}$ が少なくとも 1 台のプロキシの内部情報を取得することが不可能であれば，$\mathcal{E}_i$ として強秘匿（semantically secure）暗号を用いることで，利用者が R に送信するメッセージを $\mathcal{A}$ が特定することは困難となる．

しかしながら Mix-net は，一定数以上の入力がない限り R へメッセージが送信されないため，即時性が強く要求される通信には向いていない．このことから，メッセージ送信の即時性よりも，より強い匿名性が重視される，電子投票への適用について数多く検討されている．

2.2 Onion Routing [10)]

Onion Routing は，Mix-net よりも匿名性に対する仮定が強くなるが，即時通信が可能なことから，e-mail や Web ブラウズ等の匿名通信に適しているといえる．Onion Routing の構成は，Mix-net 同様，ネットワーク上に複数配置されたプロキシからなり，各プロキシが入力暗号文に対して暗号処理を施すが，Mix-net のように入出力の対応関係を撹乱するのではなく，通信経路の特定を困難にすることで匿名性を高める．すなわち Onion Routing は，送受信端末間の全体の通信経路を暗号技術により秘匿する技術であり，通信路全体の傍受は困難という仮定の下，受信端末に送信されたメッセージの発信元を知ることを任意の攻撃者に対して困難にする．

次に Onion Routing のプロトコルについて説明する．利用者あるいはその操作端末 U_j は，受信端末 R_ℓ $(1 \le \ell \le N)$ および中継プロキシ M_{j_i} $(i = 1,\ldots,m_j\,;\, 1 \le j_i \le m)$ を決定した後，メッセージ msg_j に対して R_ℓ，M_{j_i} のアドレスを各層に埋め込んだ多重暗号文 $C_0^{(j)}$ を作成する．今，説明を簡単にするため，$j_i = i$，$m_j = m$ とすると，$C_0^{(j)}$ は以下で与える再帰的計算により得られる．

$$C_i^{(j)} \stackrel{\text{def}}{=} \mathcal{E}_{i+1}(\mathsf{Addr}_{i+2} \,\|\, C_{i+1}^{(j)}) \quad (i = m-1,\ldots,0).$$

ここで $\|$ はデータの連結，Addr_i $(i = 1,\ldots,m)$，Addr_{m+1} で便宜上それぞれ M_i，R_ℓ のアドレス，また 2.1 節同様，$C_m^{(j)} = msg_j$ とし，$\mathcal{E}_i$ は M_i のみ復号可能な暗号関数とする．そして通信時には，M_i は $C_{i-1}^{(j)}$ を M_{i-1}（$i = 1$ であれば U_j）から受信し，これを復号して $\{\mathsf{Addr}_{i+1}, C_i^{(j)}\}$ を得た後，Addr_{i+1} に従い，$C_i^{(j)}$ を M_{i+1}（$i = m$ であれば R_ℓ）へ送信する．すなわち，通信路の傍受が不可能であれば，U_j から発信された情報 $C_0^{(j)}$ がどのプロキシを経由し，最終的にどのようなメッセージがどの受信端末に送信されたのか特定することは，$C_0^{(j)}$ を復号することに帰着される．しかし利用者の匿名性を侵害することを目的とする攻撃者 $\mathcal{A}$ が，少なくとも局所的には通信路の傍受が可能であり，実際にある程度 U_j の通信相手または最終段の中継プロキシが予測可能な状況においては，プロキシの中継数や，最終段の中継プロキシに至る通信経路とはほとんど無関係に，$\mathcal{A}$ が最終段の中継プロキシの出力情報，または受信端末の入力情報を傍受することで，U_j からの送信情報と受信端末の受信情報との相関関係（時刻やデータサイズ）を比較する攻撃が有効となりうるため，その点で Mix-net に比べ匿名性は劣るといえる．しかし利用者が中継プロキシを多数の中から選ぶことができ，かつ通信相手も不特定多数であるとき，Onion Routing は通常の通信に比べ十分高い匿名性を有するといえる．

2.3 検証可閾値暗号 [4),6),8)]

閾値暗号とは，秘密鍵を複数に分散させ，その分散鍵を保持する機関のうちの一定数以上が協力した場合に限り復号可能な暗号系を指し，現在まで，閾値 ElGamal 暗号[6)]，閾値 RSA 暗号[8)]，閾値 Paillier 暗号[4)] 等が知られている．以降，閾値暗号関数を $\mathcal{P}$ とし，分散鍵を保持する機関の数を k，復号に必要な閾値を t で表す．

現在まで知られている閾値暗号は，秘密分散法[9)] を基に構成されている．そして秘密分散法における処理

正当性を検証可能とした，VSS[7] を応用すれば，やはり処理正当性が検証可能な，検証可閾値暗号が構成できることが知られている．

検証可閾値暗号の特徴として，分散鍵を保持する任意の機関が，秘密鍵を明かすことなく，秘密鍵を用いた自身の処理の正当性を証明することが可能な点があげられる．すなわち，秘密鍵を明かさないことにより，一定数以上の機関が正しければ，その正しい機関群によって特定の暗号文のみ復号するといった制御が可能となる．また，VSS や検証可閾値暗号では，秘密鍵を知るディーラを仮定することなく，任意の機関が分散鍵を取得可能な方法も知られている[2),5),7)]．

3. 提 案 方 式

本章では，既存の匿名通信路技術[3),10)] および検証可閾値暗号[4),6),8)] を組み合わせることで実現可能な，通常は既存の匿名通信路技術同様の匿名性が提供されるが，誹謗中傷文の公開等，匿名利用者の不正が発覚した場合は，事前に指定された第三者機関のうちの一定数以上が利用者の匿名性失効を必要と判断したときのみ，その不正利用者を特定可能な技術を提案する．また以降では，2.3 節で説明した検証可閾値暗号の分散鍵を保持する機関を T_j $(j = 1, \ldots, k)$ で表し，既存技術[2),5),7)] を用いる等して，検証可閾値暗号の秘密鍵を知る機関は存在しないことを前提とする．

3.1 プロトコル

提案方式におけるシステム構成は，自身のプライバシを保護するために匿名通信を利用する利用者群あるいは利用者各々の操作端末群 $\{\mathsf{U}\}$，利用者の匿名性を提供するプロキシ群 M_i $(i = 1, \ldots, m)$，匿名の利用者からのメッセージを受信する受信端末群 $\{\mathsf{R}\}$，そして匿名利用者の不正が発覚した場合に不正者追跡処理を実行する第三者機関群あるいは第三者機関各々の操作端末群 T_j $(j = 1, \ldots, k)$ からなる．また 2.1，2.2 節の説明に用いた暗号関数 $\mathcal{E}_i$ は，ここでは検証可閾値暗号とし，M_i，T_j はそれぞれ暗号関数 $\mathcal{E}_i$ の秘密鍵，検証可閾値暗号関数 $\mathcal{E}_i$，$\mathcal{P}$ の分散鍵を保持し，$\mathcal{E}_i$，$\mathcal{P}$ は公開とする．ここで $\mathcal{E}_i$，$\mathcal{P}$ により生成される暗号文は，T_j のうちの任意の t 人が協力することで復号可能とする．また U，M_i はそれぞれ署名生成関数 $\mathcal{S}_0$，$\mathcal{S}_i$ を保持し☆，対応する署名検証関数 $\mathcal{V}_0$，$\mathcal{V}_i$ は公開とする．一方，匿名通信を実現するプロトコルは 2.1，2.2 節で述べたいずれの既存技術であってもよい．ただし本節では，できるだけ提案方式の本質を明確にする目的で，2.2 節で述べた Onion Routing プロトコルに対して経路を固定することで暗号文へのアドレス埋め込みを不要とした，簡易なプロトコルを例に提案方式を説明する．

まず匿名通信処理について説明する．

送信端末 U の匿名通信処理

(1) メッセージ $C_m \stackrel{\text{def}}{=} msg$ に対し，$i = m - 1, \ldots, 0$ について $C_i \stackrel{\text{def}}{=} \mathcal{E}_{i+1}(C_{i+1})$ を計算する．
(2) 乱数 Γ_0 を生成し，$S_0 \stackrel{\text{def}}{=} \mathcal{S}_0(C_0 \| \Gamma_0)$ を計算する．
(3) (C_0, Γ_0, S_0) を M_1 に送信する．

プロキシ M_i の匿名通信処理

(1) $\mathcal{V}_{i-1}(C_{i-1} \| \Gamma_{i-1}, S_{i-1}) = 1$ が成り立つことを確認する☆☆．もし成り立たない場合は，M_{i-1}（$i = 1$ であれば U）の不正事実を公表し，処理を終了する．
(2) C_{i-1} を復号し，C_i を得る．
(3) $\Gamma_i \stackrel{\text{def}}{=} \mathcal{P}(C_{i-1} \| \Gamma_{i-1} \| S_{i-1})$ を計算する．
(4) $S_i \stackrel{\text{def}}{=} \mathcal{S}_i(C_i \| \Gamma_i)$ を計算する．
(5) (C_i, Γ_i, S_i) を M_{i+1}（$i = m$ であれば R）に送信する．

受信端末 R の匿名通信処理

(1) $\mathcal{V}_m(C_m \| \Gamma_m, S_m) = 1$ が成り立つことを確認する．もし成り立たない場合は，M_m の不正事実を公表し，処理を終了する．
(2) 入力の組 (C_m, Γ_m, S_m) を保管する．
(3) メッセージ $C_m (= msg)$ に従った処理を実行する．

次に不正者追跡処理について説明する．なおここでは，第三者機関 T_j $(j = 1, \ldots, t)$ がメッセージ $C_m (= msg)$ の発信元となる利用者の追跡処理に正しく協力するものとして説明する．また任意の検証者を V で表す．

不正者追跡処理

[入力：(C_m, Γ_m, S_m)]

(1) V は $\mathcal{V}_m(C_m \| \Gamma_m, S_m) = 1$ が成り立つことを確認する．成り立たない場合は，R の不正と判断し，処理を終了する．
(2) $i = m, \ldots, 1$ について以下を行う．
  (a) T_j $(j = 1, \ldots, t)$ が協力し，Γ_i を復号

☆ 本論文では，記述を簡略化するため，$\mathcal{S}_i$ $(i = 0, 1, \ldots, m)$ により生成された署名を含む情報から，署名生成者が特定可能であるとする．したがって，実際には署名とともに署名生成者を特定する電子証明書等が付加されているものとする．

☆☆ ここで $\mathcal{V}_i$ は，$S_i = \mathcal{S}_i(C_i \| \Gamma_i)$ が成り立つ場合に限り 1 を返すような関数とする．

する（復号結果を $(\tilde{C}_{i-1}, \tilde{\Gamma}_{i-1}, \tilde{S}_{i-1})$ とする）．

(b) T_j $(j = 1, \ldots, t)$ が協力し，$\mathcal{E}_i$ に対応する分散鍵を用いて $\tilde{C}_{i-1}$ を復号する☆（復号結果を $\tilde{C}_i$ とする．すなわち $\tilde{C}_{i-1} = \mathcal{E}_i(\tilde{C}_i)$ が成り立つ）．

(c) V は $\tilde{C}_i = C_i$ および $\mathcal{V}_{i-1}(\tilde{C}_{i-1} \| \tilde{\Gamma}_{i-1}, \tilde{S}_{i-1}) = 1$ が成り立つことを確認する．もしいずれかが成り立たない場合は，M_i の不正と判断し，処理を終了する．

(d) $(C_{i-1}, \Gamma_{i-1}, S_{i-1}) \leftarrow (\tilde{C}_{i-1}, \tilde{\Gamma}_{i-1}, \tilde{S}_{i-1})$ とする．

(3) V は (C_0, Γ_0, S_0) から不正利用者 U を特定する☆☆．

ここで Γ_i は M_i により生成された暗号文であることが署名 S_i によって保証されるため，Γ_i の復号結果 $(\tilde{C}_{i-1}, \tilde{\Gamma}_{i-1}, \tilde{S}_{i-1})$ について $\mathcal{V}_{i-1}(\tilde{C}_{i-1} \| \tilde{\Gamma}_{i-1}, \tilde{S}_{i-1}) = 1$ を満たさない場合は，明らかに M_i の不正ということになる．また $\tilde{C}_i = C_i$ が成り立つかどうか，すなわち受信端末の保管する暗号文 Γ_m の中に埋め込まれた M_i の入出力情報が正しく対応しているかどうかは，$\mathcal{E}_i$ を検証可閾値暗号としているため検証可能である．一方，上記不正者追跡処理から，利用者情報またはプロキシ情報のいずれかが特定されることは明らかである．すなわち，本提案における不正者追跡処理手続きでは，任意の検証者が必ず不正者情報を得ることができる．ただし，このままでは検証者の取得した不正者情報が，真に不正者であるかどうかは自明でない．これについては 3.2.2 項で評価を行う．

3.2 評　　価

本節では，提案方式の匿名性および不正者追跡可能性について評価を行う．なお，匿名性に対する要件が一意でないことは 2.1，2.2 節からも明らかであるため，ここでは Mix-net を提案方式に適用した場合の匿名性要件，および Onion Routing を提案方式に適用した場合の匿名性要件を分け，個別に考察する．

3.2.1 匿　名　性

まず Mix-net を提案方式に適用した場合の匿名性要件の定義を以下に与える．

定義 1：Mix-net を適用した場合の匿名性要件

今，3.1 節で与えた提案方式について，匿名通信路技術として 2.1 節で与えた Mix-net を適用するとし，また不正者追跡処理は実行されないものと仮定する．このとき，利用者の匿名性を侵害することを目的とする攻撃者 $\mathcal{A}$ が，t 人以上の第三者機関，またはすべてのプロキシ管理者と結託しない限り，M_1 の入力情報 $\{(C_0^{(j)}, \Gamma_0^{(j)}, S_0^{(j)})\}$，および M_m の出力情報 $\{(C_m^{(j)}, \Gamma_m^{(j)}, S_m^{(j)})\}$ $(j = 1, \ldots, n)$ の対応付けが困難ならば，提案方式は $\mathcal{A}$ に対して匿名性を満たすという．ただしここで $C_{i-1}^{(j)} = \mathcal{E}_i(C_i^{(j)})$，$\Gamma_i^{(j)} = \mathcal{P}(C_{i-1}^{(j)} \| \Gamma_{i-1}^{(j)} \| S_{i-1}^{(j)})$，$S_i^{(j)} = \mathcal{S}_i(C_i^{(j)} \| \Gamma_i^{(j)})$ とし $(i = 1, \ldots, m)$，$\{C_i^{(j)}\}$，$\{\Gamma_i^{(j)}\}$ 内の要素のデータサイズはそれぞれ一定とする．

定義 1 から，$\mathcal{A}$ と結託しないプロキシ管理者の操作するプロキシを M_a $(1 \le a \le m)$ としたとき，$\mathcal{A}$ が少なくとも M_a の入出力情報 $\{(C_{a-1}^{(j)}, \Gamma_{a-1}^{(j)}, S_{a-1}^{(j)})\}$，$\{(C_a^{(j)}, \Gamma_a^{(j)}, S_a^{(j)})\}$ $(j = 1, \ldots, n)$ の対応付けが困難ならば，提案方式は $\mathcal{A}$ に対して匿名性を満たすことがいえる．すると今，M_a の入出力情報が $\Gamma_{a-1}^{(j)}$，$S_{a-1}^{(j)}$，$\Gamma_a^{(j)}$，$S_a^{(j)}$ を含まない $\{C_{a-1}^{(j)}\}$，$\{C_a^{(j)}\}$ のみであれば，これは Mix-net の匿名性の議論にほかならないことから，$S_{a-1}^{(j)}$，$S_a^{(j)}$ はそれぞれ単に $(C_{a-1}^{(j)}, \Gamma_{a-1}^{(j)})$，$(C_a^{(j)}, \Gamma_a^{(j)})$ に対する M_{a-1}，M_a の署名であることを考えれば，$\{(C_{a-1}^{(j)}, \Gamma_{a-1}^{(j)})\}$，$\{(C_a^{(j)}, \Gamma_a^{(j)})\}$ の対応付けに関して $\{\Gamma_{a-1}^{(j)}\}$，$\{\Gamma_a^{(j)}\}$ が $\mathcal{A}$ に対して有意な情報となりえないことを示せば，$\{C_{a-1}^{(j)}\}$，$\{C_a^{(j)}\}$ の対応付けが困難ならば提案方式は匿名性を満たすことが分かる．すると結局，$\mathcal{P}$ が強秘匿暗号であれば（たとえば閾値 Paillier 暗号は強秘匿であることが示されている[4]），$\Gamma_{a-1}^{(j)}$，$\Gamma_a^{(j)}$ からは，$C_{a-1}^{(j)}$，$C_a^{(j)}$ に関する情報はもとより $\Gamma_{a-1}^{(j)}$，$\Gamma_a^{(j)}$ の対応情報もまったく得られないことから，定義 1 より，$\mathcal{A}$ が Mix-net の匿名性，すなわち $\{C_{a-1}^{(j)}\}$，$\{C_a^{(j)}\}$ の対応付けが困難ならば，提案方式は $\mathcal{A}$ に対して匿名性を満たす．いい換えれば，提案方式の匿名性は Mix-net の持つ匿名性に帰着される．

次に Onion Routing を提案方式に適用した場合の匿名性要件の定義を以下に与える．

定義 2：Onion Routing を適用した場合の匿名性要件

☆ 本手続きは，M_i の署名が付与された C_i が $\tilde{C}_{i-1}$ の復号した結果かどうか検証するために必要となる．ここで $\mathcal{E}_i$ が強秘匿暗号であれば，C_i が C_{i-1} を復号した結果かどうかは，一般に C_{i-1}，C_i を生成した U，そしてそれらを復号可能な M_i のみとなる．しかしその場合，少なくとも U および M_i の結託により $\tilde{C}_{i-1}$ の偽造が可能となり，これを防ぐために提案方式では $\mathcal{E}_i$ を閾値数以上の第三者機関の協力により復号可能な検証可閾値暗号関数としている．

☆☆ 不正者追跡処理において，実際はプロキシ中継数 m が不明な場合であっても，$i = 0$ について手順 (2) を継続して行えば，V は不正利用者 U を特定できる．これについては 3.2.2 項で詳しく述べる．

今，3.1 節で与えた提案方式について，匿名通信路技術として 2.2 節で与えた Onion Routing を適用するとし，また不正者追跡処理の実行，閾値数以上の第三者機関の結託，および通信経路中の全プロキシの管理者の結託はないものと仮定する．このとき，任意のプロキシまたは受信端末の入力情報 (C_i, Γ_i, S_i) $(0 \leq i \leq m)$ から，情報の発信元 U および受信端末 R 双方を特定することが困難ならば，提案方式は匿名性を満たすという．ただしここで $C_m = msg$，$C_i = \mathcal{E}_{i+1}(\mathsf{Addr}_{i+2} \| C_{i+1})$，$\Gamma_i = \mathcal{P}(C_{i-1} \| \Gamma_{i-1} \| S_{i-1})$，$S_i = \mathcal{S}_i(\mathsf{Addr}_{i+1} \| C_i \| \Gamma_i)$ とし，U，R を知ることは，(C_i, Γ_i, S_i) からそれぞれ (C_0, Γ_0, S_0)，Addr_{m+1} を求めることと等しいとする．

定義 2 について，S_i に Addr_{i+1} を含めるのは，(C_i, Γ_i) は Addr_{i+1}（すなわち M_{i+1}）に送信した情報であることを M_i が示すためであり，これは，3.2.2 項で述べるが，不正者追跡を頑健にするために必要となる．しかし Addr_{i+1} の有無とは無関係に，提案方式が匿名性を満たすことを示すのは易しい．すなわち，プロキシが複数中継され，それらの全管理者が結託しなければ，$\mathcal{E}_i$，$\mathcal{P}$ を強秘匿暗号とすることで (C_0, S_0)，Addr_{m+1} の双方を求めることが困難なのは明らかである．したがって，通信路中にプロキシが複数中継されることを前提に提案方式は匿名性を満たすことが分かる．

一方 Onion Routing においては，2.2 節で述べたとおり，利用者の匿名性を侵害することを目的とする攻撃者が局所的な通信路しか傍受できない場合であっても，U からの送信情報および R への受信情報が傍受可能であれば，これらの時刻やデータサイズ等の相関関係を比較する攻撃が有効となりうる．しかし利用者が中継プロキシを多数の中から選ぶことができ，かつ通信相手も不特定多数であるとき，定義 2 で与えた匿名性要件の妥当性は十分であると考える．

3.2.2 不正者追跡可能性

次に提案方式における不正者追跡の頑健性について評価する．本論文では，提案方式の満たすべき不正者追跡の頑健性に対する要件を次のように定義する．

定義 3：不正者追跡の頑健性要件

今，3.1 節で与えた提案方式について，R の受信した情報 (C_m, Γ_m, S_m) の発信元特定手続きに t 人の第三者機関が正しく協力したと仮定する．このとき，検証者 V が正しく U の情報，あるいは匿名通信処理を不正実行した M_i の情報のいずれかを得ることができるならば，提案方式は不正者追跡に対して頑健であるという．

以降，提案方式で用いる署名の偽造は困難と仮定する．このとき，3.1 節の不正者追跡処理より，すべてのプロキシが処理を正しく実行したならば，不正利用者 U を示す情報 (C_0, Γ_0, S_0) が得られることは明らかである．また R が受信情報 (C_m, Γ_m, S_m) を偽れば，署名検証の時点でその事実が発覚する．したがって以降考慮すべき不正は，プロキシ管理者による不正者追跡の妨害処理に限られる．そこでまず (C_m, Γ_m, S_m) を R に送信した M_m の不正について考える．提案方式における不正者追跡処理では，M_m によって生成された暗号文 Γ_m が t 人の第三者機関によって正しく復号されたとき，その復号結果 $(\tilde{C}_{m-1}, \tilde{\Gamma}_{m-1}, \tilde{S}_{m-1})$ が，

(1) $\mathcal{V}_{m-1}(\mathsf{Addr}_m \| \tilde{C}_{m-1} \| \tilde{\Gamma}_{m-1}, \tilde{S}_{m-1}) = 1$ ☆

(2) $\tilde{C}_{m-1} = \mathcal{E}_m(\mathsf{Addr}_{m+1} \| C_m)$,

を満たす場合に限り，検証者 V は M_m の処理が正当であったと見なす（ただし (1)，(2) について，匿名通信路技術として Mix-net を用いた場合は Addr_m，Addr_{m+1} は不要）．すなわち定義 3 より，M_m が提案方式における不正者追跡の頑健性を破るためには，$\Gamma_m = \mathcal{P}(\tilde{C}_{m-1} \| \tilde{\Gamma}_{m-1} \| \tilde{S}_{m-1})$ に対して少なくとも (1)，(2) を満たす $(\tilde{C}_{m-1}, \tilde{\Gamma}_{m-1}, \tilde{S}_{m-1})$ を生成する必要がある．ところがその場合，(1) が成り立つならば，M_{m-1} が M_m に $(\tilde{C}_{m-1}, \tilde{\Gamma}_{m-1}, \tilde{S}_{m-1})$ を送信したことが保証され，(2) が成り立つならば，復号の一意性より $\tilde{C}_{m-1}$ は確かに R へ C_m を送信するための情報であることが分かり，これはすなわち M_m の処理が正当であったことを意味する．したがって，t 人の第三者機関が不正者追跡処理を正しく実行し，かつ検証者 V がその不正者追跡処理において M_m の不正を検出しない場合は，M_m の匿名通信処理が正当であったことが保証される．

以降 t 人の第三者機関が不正者追跡処理を正しく実行すると仮定し☆☆，M_i $(i = m-1, \ldots, 1)$ の不正について順次考えれば，上述と同様の議論により，結局 V が不正者追跡処理において M_i の不正を検出しなければ M_i は正しく匿名通信処理を行ったことが保証される．そして最終的に V が M_i $(i = m, \ldots, 1)$ の不正を検出しなければ，不正者追跡処理によって M_1 が生成した暗号文 Γ_1 の復号結果 (C_0, Γ_0, S_0) を得ることができる．ここで特に，署名 S_0 の生成者 U がプロキシ管理者を兼任している場合，U はメッセー

☆ これは仮定より $\tilde{S}_{m-1} = \mathcal{S}_{m-1}(\mathsf{Addr}_m \| \tilde{C}_{m-1} \| \tilde{\Gamma}_{m-1})$ が成り立つことと同値である．

☆☆ 提案方式では暗号関数 $\mathcal{E}_i$，$\mathcal{P}$ として検証可閾値暗号を仮定しているため，協力はするが不正な結果を返すような第三者機関がいた場合は，その不正が検証者 V に対して明らかとなる．

ジ C_m の発信元である利用者なのか，それとも C_m の暗号文を処理したプロキシの管理者なのか判定できないことが起こりうるが，いずれの場合であっても U が不正者であれば，(C_0, Γ_0, S_0) について不正者追跡処理を継続することで☆，Γ_0 の復号結果 $(\tilde{C}_b, \tilde{\Gamma}_b, \tilde{S}_b)$ $(1 \leq b \leq m)$ について $\mathcal{V}_b(\mathsf{Addr}_0 \| \tilde{C}_b \| \tilde{\Gamma}_b, \tilde{S}_b) = 1$, $\tilde{C}_b = \mathcal{E}_0(\mathsf{Addr}_1 \| C_0)$ を満たさない限り，V が U の不正を検出することになり，これを U が回避することは署名の偽造困難性に帰着される．したがって提案方式における不正者追跡処理が頑健であることが保証された．

以上，提案方式における不正者追跡では，t 人の第三者機関の協力によって不正利用者または不正プロキシ管理者を特定するための情報が得られることを示したが，プロキシ管理者の不正の有無にかかわらず t 人の第三者機関の協力によって不正利用者が特定可能であれば，より頑健な不正者追跡処理といえる．この頑健性向上アプローチに対する実現可能性を今後の検討課題としたい．

4. ま と め

本論文では，利用者の通信に対する匿名性，および不正利用者の追跡可能性の両立というトレードオフ問題を解決する技術を提案した．提案方式の基盤となる技術は，Mix-net や Onion Routing に代表される，各プロキシの暗号処理により実現される多段プロキシ中継型の匿名通信路技術，そして閾値 ElGamal 暗号等の検証可閾値暗号技術であり，前者により十分信頼できる匿名性を利用者に提供し，後者と署名技術の組合せにより頑健な不正者追跡が可能となる．すなわち本提案技術は，利用者の匿名性に関するプライバシ保護，そして匿名性悪用による利用者の不正防止の両立が求められるアプリケーションに有効であるといえる．

謝辞 論文全体の構成や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感謝いたします．

参 考 文 献

1) http://www.cybersyndrome.net/
2) Boneh, D. and Franklin, M.: Efficient generation of shared RSA keys, *Advances in Cryptology—CRYPTO '97*, LNCS 1294, Kaliski, B.S. (Ed.), pp.425–439, Springer-Verlag (1997).
3) Chaum, D.L.: Untraceable electronic mail, return address, and digital pseudonyms, *Comm. ACM*, Vol.24, No.2, pp.84–88, ACM Press (1981).
4) Cramer, R., Damgård, I. and Nielsen, J.B.: Multiparty computation from threshold homomorphic encryption, *Advances in Cryptology—EUROCRYPT '01*, LNCS 2045, Pfitzmann, B. (Ed.), pp.280–300, Springer-Verlag (2001).
5) Damgård, I. and Koprowski, M.: Practical threshold RSA signatures without a trusted dealer, *Advances in Cryptology—EUROCRYPT '01*, LNCS 2045, Pfitzmann, B. (Ed.), pp.152–165, Springer-Verlag (2001).
6) Desmedt, Y. and Frankel, Y.: Threshold cryptosystems, *Advances in Cryptology—CRYPTO '89*, LNCS 435, Brassard, G. (Ed.), pp.307–315, Springer-Verlag (1990).
7) Feldman, P.: A practical scheme for non-interactive verifiable secret sharing, *Proc. 28th IEEE Symposium on the Foundations of Computer Science* (*FOCS*), pp.427–437, IEEE Press (Oct. 1987).
8) Gennaro, R., Jarecki, S., Krawczyk, H. and Rabin, T.: Robust and efficient sharing of RSA functions, *Advances in Cryptology—CRYPTO '96*, LNCS 1109, Koblitz, N. (Ed.), pp.157–172, Springer-Verlag (1996).
9) Shamir, A.: How to share a secret, *Comm. ACM*, Vol.22, No.11, pp.612–613, ACM Press (1979).
10) 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, IEEE Press (1997).
11) http://www.onion-router.net/

(平成 15 年 11 月 28 日受付)
(平成 16 年 6 月 8 日採録)

千田 浩司（正会員）

昭和 50 年生．平成 12 年早稲田大学大学院理工学研究科数理科学専攻修士課程修了．同年日本電信電話（株）入社．現在，暗号応用技術の研究開発に従事．平成 13 年 SCIS 論文賞受賞．電子情報通信学会会員．

☆ ここでは便宜上添え字に 0 を用いているが，U をプロキシ管理者とすれば，整合性のため，この添え字は 1 以上 m 以下の整数とする必要がある．

小宮　輝之（正会員）

平成 8 年慶應義塾大学環境情報学部卒業．平成 10 年同大学大学院政策・メディア研究科修士課程修了．同年日本電信電話（株）入社．現在，同社情報流通プラットフォーム研究所研究員．ネットワークセキュリティの研究開発に従事．

林　　徹（正会員）

昭和 37 年生．昭和 60 年東京大学工学部計数工学科卒業．同年日本電信電話（株）入社．現在，セキュリティ技術の応用に関する研究開発に従事．