様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ５ 月 ２７ 日現在

機関番号：１４４０１
研究種目：挑戦的研究（萌芽）
研究期間：2019～2021
課題番号：１９Ｋ２２８４３

研究課題名（和文）インターネットにおける名前プライバシー保護技術のモデル化

研究課題名（英文）Protection method of name privacy in the Intrnet

研究代表者
長谷川　亨（Hasegawa, Toru）

大阪大学・情報科学研究科・教授

研究者番号：７０５７６２６４

交付決定額（研究期間全体）：（直接経費）　　5,000,000円

研究成果の概要（和文）：次世代インターネットアーキテクチャの情報指向ネットワーキングに対して，ネットワーク内の盗聴者などの攻撃者から，要求者が要求したコンテンツの名前の漏洩を防ぐ名前暗号方式を開発した．第一に，名前の暗号化は，暗号化した名前の盗聴頻度や暗号鍵を取得する頻度攻撃や名前攻撃に脆弱であるため，同一の名前を複数の暗号鍵を用いて暗号化することで脆弱性を解消した．具体的には，連続して暗号鍵を割り当てることで，脆弱性解消と通信性能の向上を両立させた．第二に，本方式のプロトタイプをプログラムスイッチ上に実装することで，本方式がインターネット規模のネットワークに展開可能なスケーラビリティを持つことを実証した．

研究成果の学術的意義や社会的意義
情報指向ネットワーキングは，キャッシュに，マルチキャストや移動通信のサポートなど，IPでは提供できない機能を有しており，次世代インターネットアーキテクチャとして期待されている．一方，宛先に名前を用いることによるプライバシー漏洩が，普及の課題となっている．これに対して，複数の鍵を用いて名前を暗号化することで，漏洩を防ぐ手法を発明し，さらに1テラビット/秒の速度で動作させた．本研究結果は，情報指向ネットワーキングの普及に貢献することが期待される．

研究成果の概要（英文）：The study designs a name encryption framework for ICN (Information Centric Networking) as a future Internet architecture, which is a promising future Internet architecture. This framework prevents adversaries, i.e., eavesdroppers on links, from knowing plaintext content names. That is, leakage of privacy to such adversaries is protected. The contributions are twofold: First, we design an encryption scheme with multiple secret keys to enhance resiliency against frequency and name guessing attacks, which leverage the information about the content popularity distribution. The scheme makes such attacks difficult by increasing the number of encrypted names, which preserves the communication performance. Second, we implement the prototype of the encryption scheme on a programmable switch. The implementation achieves 1 T bps forwarding speed and supports tens of thousands content providers. As a result, the study validates that the encryption scheme can be deployed at the Internet scale.

研究分野：情報ネットワーキング

キーワード：情報指向ネットワーキング　インターネット　プライバシー

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

情報指向ネットワーキング(ICN)は次世代インターネットアーキテクチャの有力な候補であり，日欧の共同研究プロジェクト GreenICN および ICN2020 による研究開発が進められるとともに，I.R.T.F.の icnrg ワーキンググループにおいて標準化文書が作成されつつあった．ICN は，キャッシュ，マルチキャスト，移動などの IP が持たない機能を具備しているが，一方，パケットの宛先の名前からプライバシーが漏洩することが課題であると認識され，この懸念が普及を阻害する要因の一つであった．名前は Universal Resource Identifier (URI)のように可読で，意味を持つため，名前を知った盗聴者(攻撃者)に要求者の趣味，嗜好などのプライバシー情報が漏洩する．これに対して，名前を暗号化する方式が提案されたが，これらは決定的な暗号方式，すなわち同じ平文を同じ暗号文に暗号化する方式であるため，多数のパケットを盗聴して，暗号化された名前の頻度を解析することで，平文の名前を推定する頻度攻撃に対する脆弱性が問題となっていた．

２．研究の目的

ネットワークの消費電力増が課題となっているインターネットでは，キャッシュによるトラフィック削減を可能とする ICN は，この点で IP と比較して優れている．一方，IP ではエンド―エンドで**確率的な**暗号方式でコンテンツの名前を暗号化することで，**強い**データプライバシーを提供しているのに対して，ICN では決定的な暗号方式を用いて名前を暗号化するため，**弱い**データプライバシーしか提供できない．ここで，「弱い」は，名前を暗号化しても，頻度攻撃や名前推定攻撃を用いて，攻撃者が平文の名前を推定できることを意味する．これに対して，本研究では，頻度攻撃や名前推定攻撃への耐性とキャッシュを両立する名前暗号方式を開発する．さらに，開発した方式がインターネットスケールの ICN ネットワークに展開可能であることを検証する．

３．研究の方法

従来の研究では、コンテンツが 1 パケットから構成される，単一の鍵を用いて暗号する最も単純なケースに対して，名前の暗号化方式が脆弱であることが示されていたが，どのような条件でどの程度，脆弱であるかが明確でなかった．本研究では，複数の鍵を用いて，ICN ネットワークのデータプライバシーを強化する方式を設計する．攻撃者モデルとして，その強度に応じて，2 段階のモデルを対象として，設計を進める．第 1 段階は，ネットワーク内のルータだけが攻撃者であるモデルである．このモデルで攻撃者は盗聴した暗号名の頻度から，平文の名前を推測する頻度攻撃が可能である．第 2 段階は，ルータと要求者(ユーザ)が結託するモデルである．このモデルでは，悪意ある要求者がコンテンツを暗号化する鍵を取得し，一方，結託するルータはパケットを盗聴し続ける．この名前推測攻撃では，要求者が取得した鍵とルータが盗聴した暗号名が一致すると，平文の名前を知ることができる．それぞれに対して，鍵の要求者への配布法を設計し，シミュレーションを用いて，頻度攻撃，名前推測攻撃への耐性を評価する．

４．研究成果

４．１　ルータが攻撃者のモデル

（１）単一鍵による暗号化

頻度攻撃への耐性のベースラインを知るため，まず，単一鍵を用いて名前を暗号化した場合に, 攻撃者が平文の名前の推測に成功する確率を評価した．従来の研究では，名前を持つ 1 つのデータが 1 パケットから構成される場合しか, 評価していなかったため, 複数パケット，具体的には 1～100 パケットから構成される場合の推測成功率を評価した．1000 個のデータを準備し, 要求者がインターネットのデータの人気度を近似する Zip-f 分布に従ってデータを要求する条件でパケットを生成し, 要求者を収容するルータで盗聴した. ここで, 攻撃者は全データの人気の順番を知っていることを仮定し，盗聴した暗号名の頻度とデータの人気順を比較して一致するデータの名前を推測する．図 1 では，データの人気順毎に推測成功率を示す．図 1 からも明らかなように，人気順が低い，すなわち人気度の高いデータの平文の名前は推測され易い．この結果については，電子情報通信学会研究報告(参考文献①)に発表している．

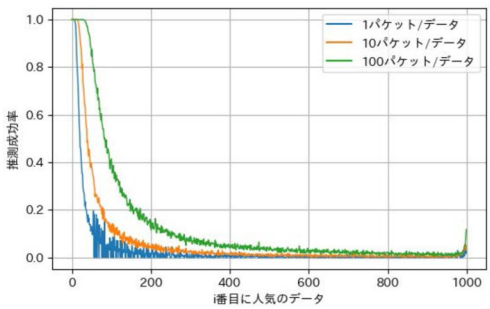

図1 推測成功率

（２）複数鍵による暗号化

単一鍵では頻度攻撃に対して脆弱であるため，複数鍵を用いた暗号化方式を検討した．まず，同一データのパケット名を、コンシューマ毎に複数の暗号鍵から一つ選択して暗号化しても、頻

度攻撃に対して脆弱であることを明らかにした．データ毎に準備する鍵数を 1～2 個，および 1～5 個の中から選択した場合の，推測成功率を図 2 に示す．図 2 が示すように，鍵数を増加させることで，全体の推測成功率を減少させるが，人気度の高いデータの推測成功率を減少させられない．これは，人気度の高いデータの要求頻度は複数鍵で暗号化しても，高いままであることが原因の一つとなっている．

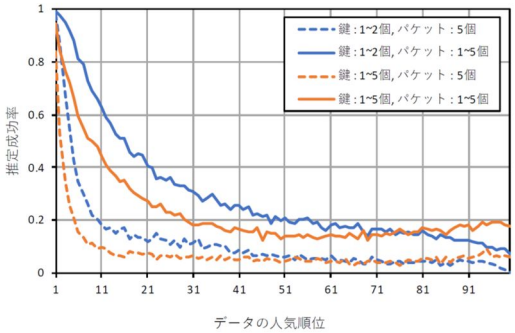

図 2 推測成功率　（複数の鍵）

これに対して，データを構成するパケットへの要求頻度がほぼ同一である暗号化したパケット列が複数存在するように，各データの名前を暗号化するのに使用する鍵数と，各鍵の使用割合を決定する匿名化アルゴリズムを設計した．具体的には，任意の暗号化したパケット名の列に対して，以下に示す k-ε匿名を満たすように，決定する．

1．構成するパケットの個数が等しい
2．平文のデータ名が異なる
3．盗聴頻度(要求頻度)の差がε(>0)以下

を満たす暗号化パケット名の列が k-1 個以上存在するように暗号鍵を割り当てる．

図 3 に k=3，ε=0.001 に設定して，左の図に示すデータ毎の要求頻度を右の図に示す盗聴頻度になるように，鍵を割り当てる．

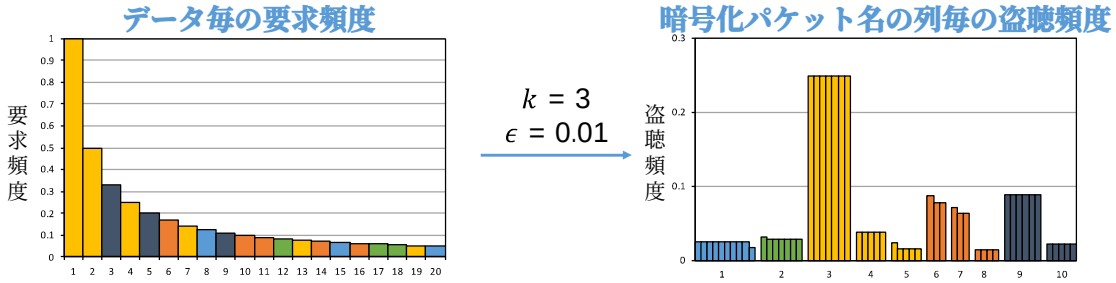

図 3　匿名化アルゴリズムを用いた盗聴頻度

表 1　k の値を変えたときのキャッシュヒット率の変化

$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
0.290	0.139	0.0867	0.0626	0.0486	0.0406

図 4 に鍵数 k を 1～5 に変化させた場合の推測成功率を示す．鍵数を増加させることにより，人気度の高いデータに対しても，推測成功率を削減している．一方，同一のデータのパケットが複数の鍵で暗号化されるため，個々の暗号化されたデータのパケットの要求頻度が減少するため，キャッシュにおけるパケットのキャッシュヒット率が減少する．表 1 に，鍵数 k を変化させた場合のキャッシュヒット率を示す．置き換えアルゴリズムは，LRU であり，キャッシュには全コンテンツの 1%のパケットが蓄積可能な容量としている．

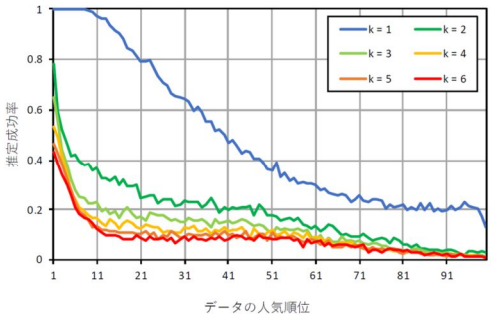

図4 推測成功率(匿名化アルゴリズム)

これらの結果，複数の鍵と匿名化アルゴリズムを用いることで，頻度攻撃への耐性を高めることができるが，キャッシュヒット率の減少が課題となる．この結果については，国際会議(参考文献②)に発表している．

4．2　ルータおよび要求者が攻撃者のモデル

（1）暗号化フレームワーク

攻撃者のルータが要求者の一部を乗っ取って結託すると，4．1 節の頻度攻撃より強力な名前推測攻撃が可能となる．名前推測攻撃では，攻撃者は全てのデータの平文の名前と人気度を知っていることを仮定している．攻撃者の要求者は，データの提供者に対して，知っている名前の鍵を要求し続ける．一方，攻撃者のルータはパケットを盗聴し続け，暗号化した名前を収集する．収集した暗号化名を暗号化した鍵と，取得した鍵が一致すると，そのデータを暗号化した鍵と平

文のデータ名を，攻撃者が知ることになる．頻度攻撃ならびに名前推測攻撃から平文の名前を防御するため，図 5 に示す暗号化フレームワークを設計した．要求者(Consumer)と提供者（Producer）の間にアノニマイザ(Anonymizer)を導入して，データの名前のプレフィクスとサフィクスを暗号化する．プレフィクスは提供者へのルーティングにルータが使用し，サフィクスは提供者の提供するデータを識別する．プレフィクスとサフィクスを複数の鍵を用いて暗号化することで，頻度攻撃の場合のように，名前推測攻撃への耐性を強化する．

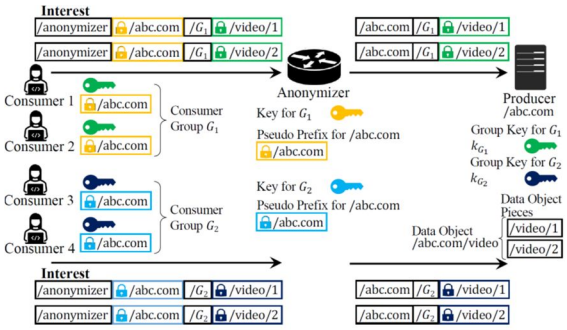

図5 暗号化フレームワーク

（２）リーセンシベースの鍵割当アルゴリズム

４．１では暗号化された名前の要求頻度を均等にすることを目的にしていたのに対して，同一のデータを連続して要求した要求者のグループに，同一の鍵を割り当てるアルゴリズムを設計した．具体的には，s 個の連続する要求に対して，同一の鍵を割り当て，s+1 個への要求があると新しい鍵に変更する．複数の鍵を用いる利点に加えて，データが要求される局所性を維持することにより，高いキャッシュヒット率を維持できることが期待できる．図 6，7 に 10^5 個のデータに対して，本鍵割当アルゴリズムを用いて名前を暗号化した場合の，名前推測攻撃への耐性と，キャッシュヒット率を示している．

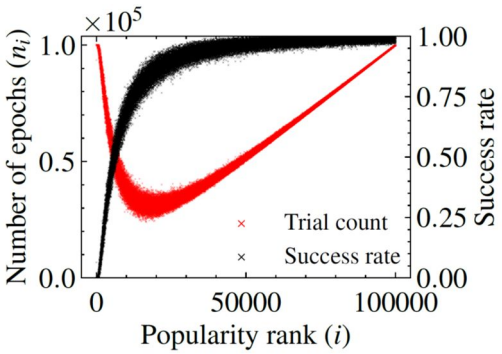

図6 名前推測攻撃の成功率と成功までの時間

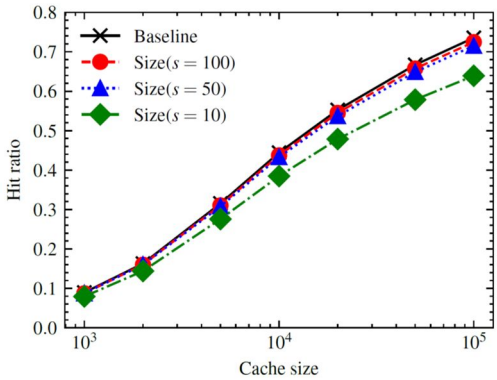

図7 キャッシュヒット率

図 6 では各人気順位のデータの平文の名前を最終的に攻撃者が知る確率(攻撃の成功率)と，それまでに必要な鍵の取得回数(Trial Count)を示している．人気度の低いデータの名前は知られる確率が高くなるが，どのような人気度においても，攻撃成功までに必要な取得回数は多く，名前推測攻撃に対して，高い耐性を示してる．図 6 では，鍵を一つだけ使用した場合(Baseline)と比較して，s が 10～100 個の場合，キャッシュヒット率の減少は少ない．この結果，リーセンシベースの鍵割当アルゴリズムは，名前推測攻撃への高い耐性と，高いキャッシュヒット率を両立させている．

最後に，設計したアノニマイザのプロトタイプをプログラマブルスイッチ上に実装し，提案した方式で暗号化した名前を持つ ICN のパケットを 1T ビット/秒で転送できることを実証した．この結果，提案した方式のスケーラビリティを検証した．この結果は，現在，国際会議で査読中である(参考文献③)．

＜引用文献＞

① 江夏 永広，小泉 佑揮，長谷川 亨，“ 頻度攻撃に対する ICN におけるデータ名暗号化の脆弱性に関する一考察，” 電子情報通信学会技術研究報告 (IN2019-109)，Mar. 2020.

② Toru Hasegawa, Shota Yamada, Yuki Koizumi, “A Study on Privacy Protection in ICN Networks using Multiple Encryption Keys,” in Proceedings of 2021 International Conference on Emerging Technologies for Communications (ICETC 2021), Dec. 2021.

③ Yutaro Yoshinaka, Kentaro Kita, Junji Takemasa, Yuki Koizumi and Toru Hasegawa, “Name Obfuscation Framework for Controlling Privacy and Performance on CCN,” under review.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計6件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 長谷川 亨，山田 翔太，小泉 佑揮
２．発表標題 ICN網における複数暗号鍵を用いた名前暗号化によるプライバシー保護に関する一考察
３．学会等名 電子情報通信学会技術研究報告
４．発表年 2021年

１．発表者名 山田 翔太，小泉 佑揮，長谷川 亨
２．発表標題 ICN網における複数暗号鍵を用いた名前暗号化の頻度攻撃に対する脆弱性に関する一考察
３．学会等名 電子情報通信学会総合大会講演論文集
４．発表年 2021年

１．発表者名 江夏 永広，小泉 佑揮，長谷川 亨
２．発表標題 頻度攻撃に対するICNにおけるデータ名暗号化の脆弱性に関する一考察
３．学会等名 電子情報通信学会技術研究報告（IN2019-109）
４．発表年 2020年

１．発表者名 江夏 永広，小泉 佑揮，長谷川 亨
２．発表標題 複数パケット名を活用した頻度攻撃に対するICNにおけるーデータ名暗号化の脆弱性に関する一考察
３．学会等名 電子情報通信学会総合大会講演論文集（B-7-3）
４．発表年 2020年

１．発表者名 Toru Hasegawa, Shota Yamada and Yuki Koizumi
２．発表標題 A Study on Privacy Protection in ICN Networks using Multiple Encryption Keys
３．学会等名 Proceedings of 2021 International Conference on Emerging Technologies for Communications (ICETC 2021)（国際学会）
４．発表年 2021年

１．発表者名 北 健太朗，武政 淳二，小泉 佑揮，長谷川 亨
２．発表標題 ミドルボックスを経由する通信の安全性を保証するための要件の定義とプロトコルの設計に関する一考察
３．学会等名 コンピュータセキュリティシンポジウム2021
４．発表年 2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	小泉　佑揮 (Koizumi Yuki) (50552072)	大阪大学・情報科学研究科・准教授 (14401)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関