6-8　匿名認証通信技術

江村恵太　高橋健志

本稿では、筆者らが考案した暗号化通信と匿名認証とを同時に実現する“匿名認証通信技術”について紹介する。本機能の実現には、単純な暗号化通信技術と匿名認証技術との組み合わせではうまくいかない。例えば、いくら匿名でユーザを認証する機能を実現していたとしても、IP アドレス等の通信時の付加情報によりその匿名性が損なわれてしまう場合や、暗号化通信のために公開鍵暗号基盤を利用するとユーザの公開鍵（の証明書）からユーザを特定可能であるため、匿名性を担保できない場合などが考えられる。本研究では、暗号方式（グループ署名及び ID ベース暗号）及び匿名通信プロトコル（Onion Routing）を用いた提案匿名認証通信プロトコルを紹介し、その性能を評価する。本プロトコルの安全性は、暗号理論における標準的な証明可能安全性の枠組みで評価した。

1　はじめに

プライバシー保護の観点から、ユーザを特定することなく匿名のままサービスを提供するための技術が多く考案されている [1]。しかし匿名性によりプライバシーが保護される一方、悪意あるユーザかどうか、匿名ユーザがサービスを得る権限を有しているかどうかの確認が問題となり、例えば IP アドレスを秘匿するなどの単純な通信路の匿名化だけでは解決できない。そこで暗号技術、特に匿名認証技術が多く利用される。

匿名で署名者の権限を確認可能な暗号技術として、グループ署名が知られている [2]。グループ署名では、グループ管理者が署名者に署名鍵を発行、署名者はその鍵を用いて署名（グループ署名）を作成し、検証者はグループ共通の公開鍵でグループ署名を検証することで“署名者がグループメンバであること”のみを検証する。特にグループ署名ではリンク付け不可能性（Unlinkability）と呼ばれる強い匿名性を実現し、ある 2 つのグループ署名が同じ署名者によって作成されたか否かという情報を暗号理論的に隠している。また、グループ管理者のみが署名者の特定を行うことができ、悪意ある署名者の特定も可能である。なお、グループ署名はあくまで署名から個人を特定する情報が漏えいしないことを保証しているにすぎず、実際に使用する際には注意が必要である。例えば、グループ署名を送付する場合、パケットに含まれる送信元 IP アドレスを秘匿する必要がある。そこで、中継機器（プロキシ）を用いてユーザとプロバイダ（Service Provider: SP）の間の通信を仲介するツール（Simpleproxy [3] や Tor [4]）を利用して、グループ署名を送付することが考えられる。この場合、「グループ」＝「サービスを受ける権限を持つユーザの集合」とすることで、SP はユーザを特定することなく、検証することが可能となる。しかしながら、これはあくまでユーザのプライバシーを考慮したに過ぎず、安全な通信を達成するためには、通信の暗号化も考慮する必要がある。ここで“いかにして匿名性を維持したまま通信を暗号化するか？”が問題となる。ユーザが公開鍵を所持する場合、公開鍵証明書より匿名性が損なわれてしまう。共通鍵暗号を利用する場合においても、SP が鍵交換プロトコルの実施にユーザの公開鍵を必要とするため、同様の問題が発生する。

本研究では、暗号方式（グループ署名及び ID ベース暗号 [5]）及び匿名通信プロトコル（Onion Routing）を利用した暗号化匿名通信プロトコルを提案した [6]。また、そのプロトタイプを実装・評価し、そのフィージビリティを検証した。その結果、従来の SSL 通信（匿名認証機能を有さない）などに比べると非効率であるが、Tor ネットワーク利用時に必要な処理時間と比較して非常に効率的であることから、そのフィージビリティは十分高いと判断した。本稿では、提案匿名認証通信プロトコルの概要を紹介する。

2　提案匿名認証通信プロトコルの概要

提案匿名認証通信プロトコルでは、ID ベース暗号（Identity-based encryption: IBE）[5] と呼ばれる暗号方式を利用する。IBE とは、任意の値を公開鍵に設定可能な公開鍵暗号であり、鍵生成センタ（Key Generation Center: KGC）が公開鍵に対する秘密鍵を

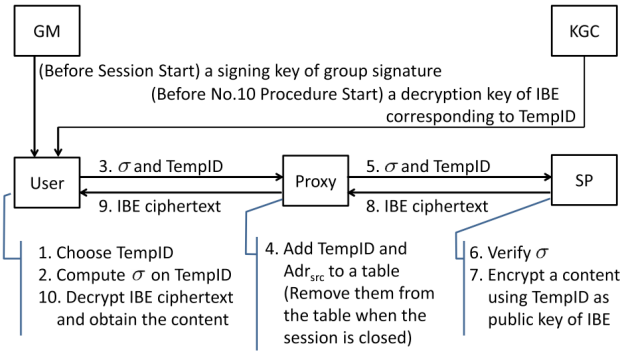

図 1　提案匿名認証通信プロトコルの枠組み [6][8]

生成、ユーザに発行する。

図 1 に提案匿名認証通信プロトコルの概要を述べる。本プロトコルでは、セッションごとにランダムな値（以下 TempID）を生成し、暗号化通信のための公開鍵とする。さらに TempID に対し、グループ署名 σ を作成する。この σ と TempID を、プロキシを介して SP に送付する。SP はグループ署名を検証したのち、TempID を公開鍵としてコンテンツ M を暗号化する。ユーザは TempID に対する秘密鍵を KGC から入手することにより、コンテンツ M を得ることができる。なお、IBE では秘密鍵生成前でも暗号化が可能であるため、ユーザは復号前の時点で TempID に対する復号鍵を KGC から入手すればよいことに注意されたい。

グループ署名 σ を検証することで、SP は匿名のままユーザがサービスを利用する権限を有することを確認できる。また、TempID に対する署名であるため、TempID を選択したのはこのユーザであることも同時に保証できる。さらに IBE の安全性（識別不可能性）により、コンテンツ M に関する情報は暗号文から漏えいしない。詳細な安全性証明は文献 [6] を参照されたい。

3　提案匿名認証通信プロトコルの効率

本章では、文献 [6][8] における提案匿名認証通信プロトコルの効率評価を紹介する。文献 [6][8] では、グループ署名の計算と送付（図 1 手順 2）を SendRequest アルゴリズム、グループ署名の検証（図 1 手順 6）を ValidityCheck アルゴリズム、IBE によるコンテンツの暗号化（図 1 手順 7）を SendContent アルゴリズム、ユーザによる暗号文の復号（図 1 手順 10）を GetContent アルゴリズムと定義している。グループ署名に古川 - 今井グループ署名方式 [7]、IBE に Boneh-Franklin 方式 [5]、暗号ライブラリとして TEPLA [11] を利用した場合の実行時間を表 1 に示す。なお古川 - 今井グループ署名方式の効率改善版を使用

表 1　実行時間（アルゴリズム）[6][8]

Algorithm	Entity	Time(msec)	Proxy Module
SendRequest	User	63.90	Simple Proxy
		62.50	Tor
ValidityCheck	SP	87.67	Simple Proxy
		89.40	Tor
SendContent	SP	87.36	Simple Proxy
		85.99	Tor
GetContent	User	52.17	Simple Proxy
		54.23	Tor

表 2　実行時間（1 セッション）[6][8]

Scheme	Cryptographic Operations	Time(msec)	Proxy Module
None	-	2.55	Simple Proxy
	-	8375.48	Tor
SSL	Enc &Auth	14.22	Simple Proxy
		7750.00	Tor
Ours	Enc &Anon. Auth	293.53	Simple Proxy
		9755.53	Tor

しているが、詳細は文献 [6][8] を参照いただきたい。実装環境としては Apple MacBookPro（processor: 2.6 GHz Intel Core i7, Memory: 16 GB, 1600 MHz DDR3, Darwin Kernel Version 13.1.0）を利用し、VMware（Fusion 6.0.2）にて 2 つの VM を立て、それぞれプロキシ、SP とした。

次にプロキシとして Simpleproxy と Tor を利用した場合それぞれの 1 セッションの実行時間を表 2 に示す。

提案匿名認証通信プロトコルでは、SSL の場合と比較すると匿名性の保証や ID ベース暗号で必要な双線型写像の計算などのため効率が悪い。ただし msec オーダーの効率は実現している。一方プロキシとして Tor を用いる場合、元々 Tor で必要な実行時間に対し、本プロトコルが占める割合は少ないことがわかる。また、IP アドレスを秘匿するため、Tor は実行ごとに異なるサーバを経由して通信を行うため効率が悪いとともに、毎回の実行時間にぶれが生じる結果となった。これらの結果から、提案匿名認証通信プロトコルは実用的な効率を有するといえる。

4　おわりに

本稿では、暗号化と匿名認証とを同時に実現可能な匿名認証通信技術を紹介した。本研究の改良版として、IBE を使用するより効率的な手法も提案した。その詳細は文献 [9] を参照されたい。

実際のシステムにおいて、鍵の紛失やユーザの離脱に備えるための鍵失効機能はなくてはならない。しかしながら通常の電子署名や公開鍵暗号と異なり、削除ユーザか否かの判定を匿名下で行うことは困難である。

削除可能グループ署名 [10] を利用することが考えられるが、いまだ実用上十分な効率を達成していない。そのため、効率的な削除可能グループ署名の提案が今後の課題である。

【参考文献】

1 Selected papers in anonymity. http://freehaven.net/
2 D. Chaum and E. van Heyst, “Group signatures,” In EUROCRYPT, pp.257–265, 1991.
3 Simpleproxy: Crocodile group software. http://www.crocodile.org/software.html.
4 Tor Project. Tor project: Anonymity online. https://www.torproject.org/.
5 D. Boneh and M. K. Franklin, “dentity-based encryption from the weil pairing,” SIAM J. Comput., 32(3), 586–615, 2003.
6 Keita Emura, Akira Kanaoka, Satoshi Ohta, Kazumasa Omote, and Takeshi Takahashi, “Secure and Anonymous Communication Technique,” Formal Model and Its Prototype Implementation, IEEE Trans. Emerging Topics Comput. 4(1), 88–101, 2016.（文献 [8] のフルバージョン）
7 Jun Furukawa and Hideki Imai, “An Efficient Group Signature Scheme from Bilinear Maps,” IEICE Transactions 89-A(5), 1328–1338, 2006.
8 Keita Emura, Akira Kanaoka, Satoshi Ohta, and Takeshi Takahashi, “Building secure and anonymous communication channel: formal model and its prototype implementation,” ACM SAC 2014, 1641–1648, 2014.
9 Keita Emura, Akira Kanaoka, Satoshi Ohta, and Takeshi Takahashi, “A KEM/DEM-Based Construction for Secure and Anonymous Communication,” COMPSAC Workshops 2015, 680–681, 2015.
10 Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, and Yusuke Sakai, “Revocable Group Signature with Constant-Size Revocation List,” Computer Journal. 58(10), 2698–2715, 2015.
11 TEPLA, “University of Tsukuba Elliptic Curve and Pairing Library,” [Online], Available, http://www.cipher.risk.tsukuba.ac.jp/tepla/index_e.html, accessed Feb. 20, 2015.

江村恵太　（えむら　けいた）

サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（情報科学）
暗号理論

高橋健志　（たかはし　たけし）

サイバーセキュリティ研究所
サイバーセキュリティ研究室
主任研究員
博士（国際情報通信学）
サイバーセキュリティ、通信プロトコル