4-2　プロキシ暗号と準同型暗号に関する研究

4-2 Research Activities on Proxy Cryptosystems and Homomorphic Encryption Schemes

王　立華
WANG Lihua

要旨

本稿では、2006年度から2010年度までセキュリティ基盤グループで行われた実用的な暗号プロトコルの研究開発に関する活動及びプロキシ暗号や準同型暗号に関する研究成果を紹介する。プロキシ再暗号と加法準同型暗号はそれぞれセキュアな広域分散ファイルシステムとワイヤレスセンサーネットワークにおける安全データ集計に応用される。

In this paper, we introduce our research activities during the past five years and then give a survey about our contributions on designing and developing practical cryptographic protocols including proxy (re)-cryptosystems and homomorphic encryption schemes. Among them, proxy re-encryption and additively homomorphic encryption are significant cryptographic primitives for secure cloud storage and secure data aggregation in wireless sensor networks.

[キーワード]
ペアリング，プロキシ暗号，結託攻撃，準同型暗号，位置情報認証
Pairing, Proxy cryptosystem, Collusion attack, Homomorphic encryption, Position information authentication

1　はじめに

公開鍵暗号系では、ペアとなる2つの鍵を使ってデータの暗号化と復号を行う。暗号化用の鍵は公開され、公開鍵と呼ばれる。復号用の鍵は公開鍵のペア鍵であり、秘密で所有者に保管され、秘密鍵と呼ばれる。例えば、ユーザAliceに送信するとき、Aliceの公開鍵を使って平文のメッセージを暗号化して、暗号文を送る。Alice以外の人間は公開鍵などの公開情報だけで暗号文を平文に解読することは困難であるが、Aliceは秘密鍵を使って簡単に暗号文を復号し、平文を得ることができる。

そこで、問題になるのはAliceに送信する前にデータを暗号化する際に、確実にAliceの公開鍵を使わなければならない。そうでないと情報漏えいや復号できなくなる恐れがある。それを解決するアプローチはインフラによって違う。

Public Key Infrastructure（PKI）

伝統的な公開鍵暗号（PKC）では、公開鍵はただ無作為の文字列である。そして、それだけで鍵の所有者Aliceを認証することはできない。Certificate Authority（CA）という信頼された機構によって提供される証明書を使って、この問題を解決できる。CAが偽装困難な署名、及び公開鍵とアイデンティティAliceの間の信頼されたリンクを提供する。公開鍵認証基盤（PKI）は、証明書（チェーン）を発行し、管理する。PKI方式の場合、Aliceに暗号文送信する前に、あらかじめ、Aliceの証明書を入手して、彼女の証明書の正当性について確かめる必要がある。特にユーザの数が非常に大きいときに、効率的でなく実用的ではない。

Identity-Based Cryptography（IBC）

1984年にShamir[1]が考案したIDベース暗号（IBC）が前述の問題を解決した。方法としては、任意の文字列であるAliceのアイデンティティID（または電子メールアドレス）を公開鍵とし、“秘密鍵生成局（PKG）”と呼ばれる信頼された機関から得たマスター秘密鍵、並びにAliceのIDを使ってAliceの秘密鍵を計算する。この方法では、証明

書が暗黙的に提供され、公開鍵の明示的な認証が不要となる。IDベース暗号（IBE）の主な欠点は、PKGに無条件の信頼である。結果としてPKGは、任意のユーザを偽装する、任意の暗号文を復号することが可能になってしまう。したがって、IBC方式はPKGが完全にグループ内のすべてのユーザによって信頼されている閉鎖的な組織に適している。

Certificate-Based Cryptography（CBC）

IBCの長所をPKIに統合するために、Gentry[2]が証明書ベースの暗号化（CBE）の概念を提案した。CBEスキームは認証者とユーザの間の公開鍵暗号化スキームとIDベースの暗号化スキームを結合する。各ユーザが自分の公開鍵と秘密鍵を生成して、CAに証明書を要求する。そしてCAがIDベース暗号方式の鍵生成アルゴリズムを使って証明書を作る。証明書はユーザ復号鍵の一部として暗黙的に使用される（復号鍵はユーザ作成の秘密鍵と証明書で構成される）。CAは証明書を知っているが、ユーザ秘密鍵を持っていないため、どんな暗号文も解読できない。CBCはIBCから暗黙の証明、そしてPKCから鍵保管不要（key-escrow-free）の特徴を引き継ぐより先進的な公開鍵認証フレームワークである。

2006年度から2010年度のセキュリティ基盤グループの活動では、上記のそれぞれの暗号インフラのフレームワークの中で、ユーザの利便性と安全性向上を目標として、情報社会の発展に伴い実社会の要請に応える暗号プロトコルの設計と評価を行った。本稿ではそれに関する研究活動の概要を述べる。**2**では効率的なペアリングに基づく暗号に関して国内外連携活動とプロキシ暗号の関連成果を紹介する。**3**では準同型暗号に関する成果と情報通信研究機構（NICT）内部連携活動による位置情報認証実証試験を紹介する。**4**では今までの貢献と今後の課題をまとめる。

2 ペアリングに基づく暗号について研究活動

2.1 効率的なペアリング暗号ワークショップ

2001年にBoneh、Franklin[3]によるペアリング（pairing）を用いてIDベース暗号系が発表されて以来、ペアリングの双線形性に基づいて様々な暗号プロトコルが提案され、注目が集まった。当時、暗号に使われたWeil pairingとTate pairingの計算コストはそれぞれ指数演算の約10倍と5倍とみられ、このようにPairingの計算量は大きいため、暗号プロトコルは多数に渡ってpairingを利用すると効率性が低くなる。本研究では、実社会に適用する性質を確保するとともに適切な回数で最低限にPairingを利用する効率よい暗号プロトコルについて、筑波大学、上海交通大学と共同研究の形で効率的な鍵共有[4]、プロキシ（Proxy）暗号方式の設計を行った。

2008年度に、国際交流プログラム海外研究者招へいファンドを獲得し、上海交通大学の曹珍富教授のTDT実験室とセキュリティ基盤グループの間に長期的な連携研究関係を結ぶためのワークショップを企画した。ワークショップでは、当該分野専門家の岡本栄司教授（筑波大学）、曹珍富教授（上海交通大学）、満保雅浩准教授（筑波大学）、高木剛教授（はこだて未来大学）、ミャオイン准教授（筑波大学）、山村明弘（NICT）による、ペアリング技術の現状、暗号研究の最新動向、センサーネットワーク応用における暗号と実装技術、認証技術等について、講演があった。曹珍富教授が主張している「暗号技術は市場により創出され発展する」という観点はワークショップのテーマになった。ワークショップでGF（3^n）上の楕円曲線上のEtaペアリングが効率よく、暗号システムの実装に採用されることがはこだて未来大学の高木教授の講演によって紹介された。一方でGF（3^n）上の楕円曲線上の離散対数問題の解決困難性が検証されていないことが問題であった。これは2009–2010年度に行った安全性が離散対数問題に帰着する暗号プロトコルの強度評価に関して共同研究[5]に繋ぐ。

（http://nictinfo.nict.go.jp/Announce/event/20081024.html後記：上海交通大学にて2010年10月にもワークショップを開催した。http://tdt.sjtu.edu.cn/workshop2010/）

ここで、代理権回収できるプロキシ暗号システム及び結託攻撃を防ぐプロキシ再暗号システムなど、実社会の要請に応える視点からより実用的な暗号に関する成果を紹介する。

2.2 プロキシ暗号に関する研究

1997年に満保と岡本[6]がプロキシ暗号システムという概念を紹介した（図1）。これは代理復号とも呼ばれる。代理復号というのは、ユーザAliceの公開鍵によって暗号化された暗号文をプロキシ（代理復号者Proxy decryptor）経由することで、Aliceに代わって暗号文を復号する暗号手法である。プロキシは事前にAliceから復号権利をもらう必要がある。

1998年にBlazeら[7]が代理復号と密接に関連している概念であるプロキシ再暗号（proxy re-encryption）即ちPREシステムを提案した。PREシステムでは、プロキシ（代理再暗号者proxy re-encryptor）が平文の情報を得ずにユーザAliceの暗号文をユーザBobの暗号文に変換できる。よって、プロキシの役割はクラウドの中の信頼されてないサーバとの関連性が非常に強い。

この2つのプリミティブは様々な発展がなされ、特にペアリングを用いてIBE[3]が提案されて以来、実用性に向け様々な特徴を持つ代理復号システムとPREシステムが提案されてきた。ここで私たちが提案したCBEに基づく代理復号システムとIDベースPREシステムを紹介する。両方ともペアリングの双線形性を利用した。

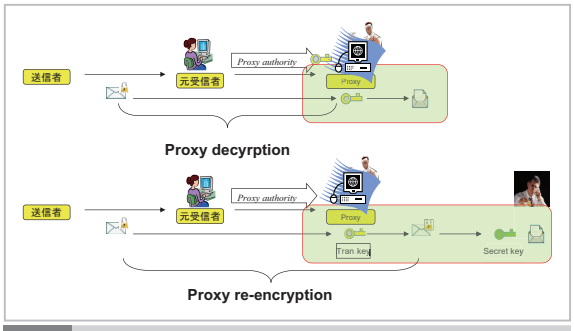

図1 プロキシ概念

2.3 ペアリングベース提案方式

定義G_1、G_2は乗法群、order pは素数、gはG_1の基底である。下記の条件を満たせば、$\hat{e}: G_1 \times G_1 \to G_2$はadmissible bilinear mapとなる：

(1) Bilinear. $\hat{e}(g^a, g^b) = \hat{e}(g,g)^{ab}$, for all $a, b \in Z_p^*$.

(2) Non-degenerate. $\hat{e}(g,g) \neq 1_{G_2}$.

(3) Computable. There is an efficient algorithm to compute $\hat{e}(f,h)$ for any $f, h \in G_1$.

双線形性の$\hat{e}(g^a, g^b) = \hat{e}(g,g)^{ab}$のお陰で提案した暗号プロトコルは望ましい特徴を満たす。そして、提案方式の安全性は下記の計算上問題が困難である仮定に基づく。

Discrete Logarithm Problem:
Given $g, g^a \in G_1$, or $\mu, \mu^a \in G_2$, find $a \in Z_p^*$.

Computational Diffie-Hellman (CDH) Problem:
Given $g, g^a, g^b \in G_1$, find $g^{ab} \in G_1$.

Bilinear Diffie-Hellman (BDH) Problem:
Given $g, g^a, g^b, g^c \in G_1$, find $\hat{e}(g,g)^{abc} \in G_2$.

Decisional Bilinear Diffie-Hellman Assumption (dBDH Assumption):
Given $g, g^a, g^b, g^c \in G_1$ and $\eta \in_R G_2$,
dBDH仮定は$\hat{e}(g,g)^{abc}$とηを分別することが困難であるという仮定である。

CBE-based proxy decryption schemes with revocability

本研究で初めて先進的なインフラであるCBEのフレームワークの中で、代理復号システム（CBPd）を構築した[8]。提案方式は**1**で紹介したように伝統的なPKCとIBEの長所を結合という利点を持つ。そして、プロキシ（代理復号者達proxy decryptors）用の共通パラメータを発行するというアプローチによって、一旦譲ったプロキシ復号権利を回収できるRevocabilityという特徴を持つ。

【Revocability】とは代理人の権限が有効である期間であっても代理権を解除し、代理人を交代することができる機能を有する、という意味である

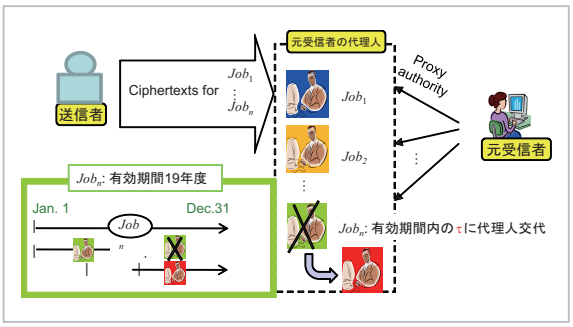

図2 Revocability

(図2)。例えば、プロキシCharlieは上司のAliceから2007年度のjobというプロジェクトの担当者として委任され、2007年度末まで、jobに関する暗号文をAliceに代わって復号できる。しかし、途中でCharlieが転職する場合や、なんらかの問題で信用されなくなる場合は、AliceはCharlieに委任した復号権利を回収する必要がある。

提案方式はCBEインフラの利点が持ち、受信者各自秘密鍵を生成し、秘密鍵を検証センターに預託しないため、受信側のプライバシーを保護するとともに、メールを受信者のIDとPKで暗号化して送信するが、PKの認証が不要なので、送信側に利便性がある。

ID-based proxy re-encryption constructions to prevent collusion attack

PREシステム[7]では、プロキシ(proxy re-encryptor)は平文の情報を得ずにユーザAliceの暗号文をユーザBobの暗号文に変換できる。よって、プロキシの役割はクラウドの中の信頼されていないサーバと非常に関連性がある。即ち、代理復号権利を代理再暗号権利へ転換すると、復号処理は再暗号処理と指定されたユーザの自分の秘密鍵による復号処理2ステップに分けられる。再暗号処理を担当するプロキシは再暗号しかできず、暗号文を解読することができない。そのお陰で代理再暗号は電子メールの転送や広域分散セキュアデータストレージなどに応用できる、非常に重要な研究テーマである。そのため、PREの研究が注目されてきた。その中で、IDベースPRE(IB-PRE)の研究もたくさんされた[9]–[12]。しかし、従来のIB-PREスキームはプロキシが他のユーザ及び他のプロキシと結託しないという仮定が必要である。この仮定はプロキシがローカルで管理されなくクラウドのような分散的なシステム環境では現実的ではないため、結託攻撃に対しても安全なIB-PREプロトコルの設計は重要な課題だと考えられる。

2005年Atenieseら[13]が伝統なPKIのフレームワークで初めて結託攻撃を提出し、collusion“safeness”、non-transferabilityなど耐結託攻撃な安全性要求を定義した(図3)。

1. *Collusion “safeness”*. Aliceが指定した復号者BobがAliceのプロキシと結託しても、Aliceの秘密鍵が漏洩されない。即ち $rk_{A\to B} + sk_B \nrightarrow sk_A$, ここの記号 $rk_{A\to B}$ はAliceの暗号文からBobの暗号文へ変換用の再暗号鍵、sk_A, sk_B はそれぞれAliceとBobの秘密鍵を示す。
2. Non-transferability. Aliceが指定した復号者BobがAliceのプロキシと結託しても、Aliceの暗号文からBob以外のユーザの暗号文へ変換用の鍵を偽造できない。即ち $rk_{A\to B} + sk_B \nrightarrow rk_{A\to C}$.

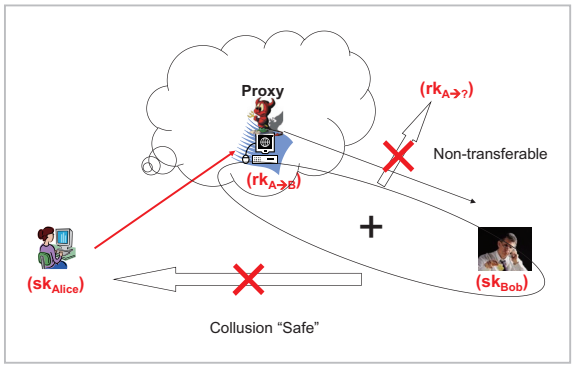

図3 耐結託攻撃

本研究はIBEのフレームワークの中で、Matsuo[11]の方式と似たように鍵生成センターPKGを再暗号鍵 seed $\left(\frac{H(id_A)}{H(id_B)}\right)^{u_B}$ の生成を担うことで、collusion“safeness”、non-transferabilityなど耐結託攻撃な安全性を満たしたIB-PRE方式を初めて実現した[14]。

そして、Single-hopなIB-PRE方式の場合はcollusion“safeness”、non-transferabilityなど安全性性質はIND-CPA(Indistinguishability under Chosen Plaintext Attack)安全性に含まれるという結論を得た。提案方式はランダムオラクル仮定でIND-CPA/CCAセキュアであり、dBDH仮定に帰着することを証明した。

3 加法準同型暗号及び位置情報認証への応用に関する考察

3.1 離散対数ベース加法準同型暗号

準同型暗号は2つの暗号文 $Enc(m_1)$、$Enc(m_2)$ が与えられた時に、平文や秘密鍵なしで

$Enc(m_1 \circ m_2)$が計算できる方式であり、プライバシー保護の用途において特に注目されている。ここで記号“∘”が表す計算の種類によって、加法準同型暗号[15]、乗法準同型暗号[16]、代数準同型暗号や完全準同型暗号など様々な方式がある。

1999年Paillier[15]が素因数分解に基づいて提案した加法準同型暗号方式は代表的な加法準同型暗号方式として知られている。方式は3つのアルゴリズムで構成する。

1. **鍵生成**　$n=pq$とし、$\gcd(L(g^{\lambda} \bmod n^2), n)=1$成立する基底$g \in B$をランダムに選ぶ。よって、(n, g)を公開パラメータとし、(p, q)（または等価な$\lambda=lcm(p-1, q-1)$）を秘密パラメータとする。
2. **暗号化処理**　平文を$m<n$とし、乱数$r<n$とする。暗号文$c=g^m \cdot r^n \bmod n^2$で計算する。
3. **復号処理**　暗号文$c<n^2$に対し、

$$\text{平文 } m=\frac{L(c^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n,$$

$$\text{ここで関数 } L(u)=\frac{u-1}{n}.$$

Paillierの準同型暗号方式は$Enc(m_1+m_2)=Enc(m_1) \cdot Enc(m_2)$を満たすので、加法準同型方式である。

一方、離散対数問題に基づく加法準同型暗号はまだない。そこで国際会議PKC 2006で、Chevallier-Mames、PaillierとPointcheval[17]が「離散対数問題に基づく加法或いは乗法fully準同型を実現できる暗号システムを見つける」という課題をアナウンスした。我々は問題の1つを解決し、ElGamal暗号システムを利用して離散対数に基づく加法準同型暗号を提案した[18][19]。オリジナル版のElGamal暗号システムは乗法準同型性を持つ。ElGamal方式の平文空間をMからg^{M_0}へ上げるというアプローチによって加法準同型を満たす目標を達成した。

1. **鍵生成**　まず、下記の条件を満たす素数p、p_0を選ぶ。
   (1)$p=2q+1$、qは大きい素数、(2)$p_0=2t^{\kappa}+1<p$、tは小さい素数、κは正の整数。
   そして、Z_p^*のorder qのsubgroupの生成元gと$Z_{p_0}^*$の生成元g_0を選ぶ。従って、system publicパラメータ$params=(p, q, g, p_0, g_0)$となり、平文空間と暗号文空間はそれぞれ$M=\{0,1,\ldots,p_0-2\}$と$C=Z_p^* \times Z_p^*$となる。
2. **暗号化処理**　公開鍵yと平文$m \in M$を入力し、乱数$r \in Z_q$を選び、暗号文$(c_1, c_2)=(g^r \bmod p, y^r \cdot (g_0^m \bmod p_0) \bmod p)$を出力する。
3. **復号処理**　秘密鍵xと暗号文(c_1, c_2)を入力し、平文$m=L_{g_0}(D_{\times}(x,(c_1,c_2)))$を計算する。
   ここで$D_{\times}(x,(c_1,c_2))=c_2/c_1^x \bmod p$,
   $L_{g_0}(g_0^m \bmod p_0)=m \bmod (p_0-1)$.

上記に述べたBasic版方式を比較すると、暗号化ステップでは提案方式がPaillier加法準同型方式より効率がよく、復号ステップではPaillier方式の方が効率がよい。双方のFast版[15][19]を比較すると、提案方式は効率がよいことが分かる（表1、[19]）。

表1　計算量比較

Schemes	Enc	Dec
Paillier-Basic	$[2]exp_{n^2}+[1]mul_{n^2}$ $\approx[128\log p_0]mul_{p_0}$	$[1]exp_{n^2}+[1]mul_n+L_n$ $\approx[64\log p_0]mul_{p_0}$
Paillier-Fast	$[1]exp_{n^2}+[1]mul_{n^2}$ $\approx[64\log p_0]mul_{p_0}$	$[\log \alpha]mul_{n^2}+[1]mul_n+L_n$ $\approx[16\log \alpha]mul_{p_0}$
Our-Basic	$[2]exp_p+[1]exp_{p_0}+[1]mul_p$ $\approx[17\log p_0]mul_{p_0}$	$[1]exp_p+[1]mul_p+L_{g_0}$ $\approx[(8+\log\log p_0)\log p_0]mul_{p_0}$
Our-Fast	$[2]exp_p+[1]exp_{q_0^2}+[1]mul_p$ $\approx[17\log p_0]mul_{p_0}$	$[\log x]mul_p+[1]mul_p$ $\approx[4\log \alpha]mul_{p_0}$

加法準同型を用いて内積準同型計算

加法準同型性を利用し、平文が一定条件を満たす場合は内積準同型性も実現できる。

■基本ルール　$Enc_{pk}(a) \hat{+} Enc_{pk}(b)=Enc_{pk}(a+b)$.
■倍数　$Enc_{pk}(a) \hat{\cdot} b=Enc_{pk}(a \cdot b)$.
■平文のVectorと暗号文のVectorの「内積」
$Enc_{pk}(\vec{a}) \hat{\cdot} \vec{b}=Enc_{pk}(\vec{a} \cdot \vec{b})$.

従って、

Given　$Enc_{pk}(s_i(0)), Enc_{pk}(s_i(1)), Enc_{pk}(s_i(2)), \ldots$
and $s_u(0), s_u(1), s_u(2), \ldots$

Compute　$\tilde{\rho}_{i-u}(\tau)=\sum_t Enc_{pk}(s_i(t)) \hat{\cdot} s_u(t+\tau)$
$=\sum_t Enc_{pk}(s_i(t) \cdot s_u(t+\tau))$

$$= Enc_{pk}(\sum_{t} s_i(t) \cdot s_u(t+\tau))$$
$$= Enc_{pk}(\rho_{i-u}(\tau))$$

Then $\rho_{i-u}(\tau) = \mathrm{Dec}_{sk}(\tilde{\rho}_{i-u}(\tau)),\ \text{for } \tau = 1,2,3,...$

それは位置情報認証実証試験に役に立った。

3.2 加法準同型暗号に基づいて位置情報認証実証試験

NICTの基盤技術の強みを生かすことを意識した2010年度プリプロジェクト「時刻・位置情報認証によるセキュリティ高度化技術の実証」という課題について、光・時空標準グループと連携して、位置情報の詐称を防ぐとともにプライバシー保護を配慮した位置情報認証システムの研究開発を行った[20]。

背景：情報の発信源の特定や物流の経由地点など、位置情報を利用したアプリケーションやサービスは多々見られる。しかしながら位置情報は不変的な性格を有するため、発信者を信用するしか手段はなく信頼性は非常に乏しい。また一度得た位置情報は繰り返し利用することができるため、複数の情報を利用して位置を詐称（結託攻撃）することをネットワーク上のやり取りで見破ることは難しい。そこで位置情報を認証する手段が必要である。

単純な解決策としては、GPS衛星との通信など位置情報を取得する際に認証を行うことである。しかしながら、現行のシステムでは相手にも自分の位置情報を伝えることとなり、プライバシー保護の問題もある。また、位置情報取得システムとユーザが同じ場所にいることを検知できなければならない。さらに、不正に位置情報取得システムを利用し位置情報を不正に入手する、既に得た位置情報から別の位置情報を計算し改ざんすることを防ぐ必要もある。

このような問題を解決するには、単に物理的に取得した情報だけでなく、その時だけ生成される即時的な情報の利用も必要である。さらにユーザとサーバ以外にも信頼できる第三者（Trusted Third Party：TTP）の設置や装置の耐タンパ性も要求される。従って、位置情報の認証の実現にはインフラとしての解決が必要になる。これによって以下の安全性要件が達成されることが目的となる。

- 位置情報のなりすましの検知
- 位置情報の不正利用、改ざんの検知
- 位置情報のプライバシーの保護

そこで、本論文では準同型暗号を応用し、その場に居ないと生成できない情報を利用することで位置情報を認証するプロトコルをActive TypeとPassive Typeの2種類を提案する。

準天頂衛星とLEX信号—Active Type

準天頂衛星（quasi-zenith satellites：QZS）[21]は日本国内のほぼ真上に位置する衛星であり、建物や地形の影響を受けずに信号受信を可能にするものである。例えば現在の静止衛星の場合、東京では48度以上の仰角を得ることができないため、静止衛星からの信号を受信できる場所が限定される。一方で準天頂衛星の場合は仰角を60度以上に設定できるのでどこからでも信号の受信が可能である。準天頂衛星は常に動いているため、24時間の利用を可能にするためには3機以上で構成する必要がある。準天頂衛星が常に動いている状態にあるので、地上で静止している受信者から見ると準天頂衛星と受信者の距離は常に変化する関係にある。準天頂衛星が発するLEX信号は42［MHz］の占有帯域幅であるため、距離換算すると約7.1［m］の分解能を持つ。また準天頂衛星の地表に対する移動速度は約2850［m/s］であるので、受信者–準天頂衛星間の距離の差が7［m］生じるのに約2.5［ms］要することとなる。

ここで受信者、認証局、準天頂衛星の3者の位置が分かっているとする。また、これら全ての時刻が同期していると仮定する。準天頂衛星から時刻Tに放送されたLEX信号はユーザに到達

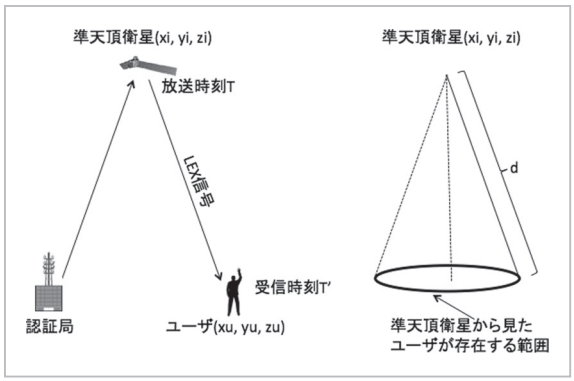

図4 Active Typeによるユーザ位置の特定手法の概略

するまで時間差がある（ユーザの受信時刻 T_0）。時刻差 $|T_0 - T|$ から準天頂衛星とユーザの距離 $d = c \cdot |T_0 - T|$ が算出できる。一方で準天頂衛星を管理している認証局は、時刻 T における準天頂衛星の位置 (x_i, y_i, z_i) が分かるので、(x_i, y_i, z_i) と $d = c \cdot |T_0 - T|$ から準天頂衛星から見た地表におけるユーザが存在する範囲を特定できる。ただし c は光の速度である。従って、認証局はユーザの受信時刻 T_0 が分かれば受信者が存在する範囲が決定できる（図5）。異なる3組の T、T_0、(x_i, y_i, z_i) が得られれば、互いに交わる3つの円の部分空間として受信者の位置が決定できる。この事実を利用した位置情報の認証手法を Active Type と呼ぶ。現実で Active Type 手法を実現する環境はまだ揃ってないのが、放送局などから受信した電波を利用する位置情報認証実証も試みた。

放送局と複数波同時受信装置—Passive Type

基本的な考え方は前述の準天頂衛星の場合と同様であり、ある放送局から放送された電磁波を異なる2点で受信した場合、お互いの放送局からの距離が異なれば受信波形にずれが生じることを利用する方法である。受信者 A、受信者 B を仮定し、それぞれ放送局からの距離を d_A、d_B とする。受信者 A が受信した信号波形を Wa、受信者 B が受信した信号波形を Wb とし、それらを相互相関関数へ入力することで位置の度合いを測る。この時、Wa と Wb は受信者 A、受信者 B の放送局への距離差 $|d_A - d_B|$ に応じた時間差が生じている。電磁波は光の速さと同じであるから、$|d_A - d_B|$ から Wa と Wb の相互相関が最大となる時間差が計算できる。逆に Wa と Wb の相互相関が最大となる時間差が得られれば、受信者 A から見て受信者 B が存在する範囲が決定できる。異なる3組の時間差を得られれば、互いに交わる3つの円の部分空間として受信者の位置が決定できる（図6）[22]。この事実を利用した位置情報の認証手法を Passive Type と呼ぶ。

この手法は複数の地上波を同時に受信するものである。地上波の発信源の集合を V とする。各発信源 $(v_i \in V)$ は常に信号系列 $\{s_{i1}, s_{i2}, ...\}$ を生成している。本手法の各エンティティは受動的にこれらの信号系列を受信している。このシステムの前提として3つのエンティティ、認証局（AC）、信頼できる第三者（TTP）、ユーザの時刻が正確に同期

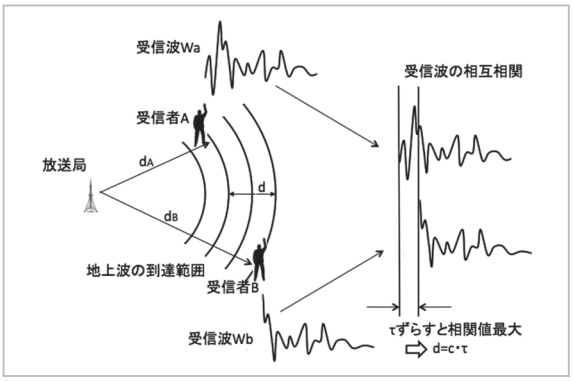

図5 Passive Type によるユーザ位置の特定手法の概略

していることが挙げられる。受信するときの時間差は相関法によって求める。

$$s_i(t) = 0,1,-1,2,0,...$$
$$s_u(t) = 1,-1,2,0,1,...$$
$$\text{相互相関法：} \rho(\tau) = \int s_i(t) s_u(t-\tau) dt$$
$$\rho(0) = \int s_i(t) s_u(t) dt$$
$$= 0 \times 1 + 1 \times (-1) + (-1) \times 2 + 2 \times 0 + 0 \times 1 ...$$
$$\rho(1) = \int s_i(t) s_u(t-1) dt$$
$$= 1 \times 1 + (-1) \times (-1) + 2 \times 2 + 0 \times 0 + ...$$
$$\vdots$$

時間差は τ_0：$\rho(\tau_0) = \max\{\rho(1), \rho(2), ...\}$ である。TTP のプライバシー保護しながら時間差を求める場合は、TTP 受信した信号を暗号化してからユーザに送信するべきである。ユーザは TTP からもらった暗号化された sequence と自分の受け取った平文の sequence の内積を計算して、**3.1** で述べた内積準同型暗号文になっているため、CA はそのまま復号して、$\rho(\tau)$ それから、τ_0 を得る。

TTP は複数存在し、それらの位置情報は認証局のみが知り、ユーザに対しては秘密であるにも関わらず、TTP の位置情報を参照してユーザの位置情報を認証する。

上記の実証試験は Paillier 方式だけで行ったが、提案した離散代数問題に基づく方式での実証試験、効率評価そしてそれに関わる平文空間と暗号文空間が等しい加法準同型暗号技術の研究開発などは残りの課題である。

4 むすび

2006年度から2010年度までにセキュリティ基盤グループで行われた実用的な暗号プロトコルの研究活動と成果の概要を述べた。上記の研究活動はNICT特別ファンドにおけるインセンティブ調査・研究、及び国際交流プログラム個別研究者招へい制度によりサポートされた。研究交流を深めるために当分野の専門家を招へいした。セミナー及びワークショップ（図6）を開催し、研究成果は国際会議、国際論文誌で発表した。成果は特許出願[23]を行った上、実証試験した結果を学会発表により社会へ発信した。審査委員会における事後評価より「十分な達成」と「計画を大幅に上回る」との評価を得た。

2010年度プリプロジェクトに資され「時刻・位置情報認証によるセキュリティ高度化技術の実証」に関して光・時空標準グループ及び鹿島宇宙技術センターのメンバーと連携して行った。

図6 ワークショップ風景

参考文献

1 Shamir, A., “Identity-based cryptosystems and signature schemes,” Blakely, G.R., Chaum, D. (eds.), CRYPTO 1984, LNCS, Vol. 196, pp. 47–53, Springer, Heidelberg, 1985.

2 Gentry, C., “Certificate-based encryption and the certificate revocation problem,” Biham, E. (ed.), EUROCRPYT 2003, LNCS, Vol. 2656, pp. 272–293, Springer, Heidelberg , 2003.

3 Boneh, D. and Franklin, M., “Identity-based encryption from the Weil pairing,” Kilian, J. (ed.), CRYPTO 2001, LNCS, Vol. 2139, pp. 213–229, Springer, Heidelberg, 2001.

4 S. Wang, Z. Cao, K.R. Choo, and L. Wang, “An improved identity-based key agreement protocol and its security proof,” Journal of Information Sciences, Vol. 179, pp. 307–318, 2009.

5 T. Hayashi, N. Shinohara, L. Wang, S. Matsuo, M. Shirase, and T. Takagi, “Solving a 676-bit Discrete Logarithm Problem in GF(3^{6n}),” PKC2010, LNCS, 6056, Springer-Verlag, Berlin, pp. 351–367, 2010.

6 Mambo, M. and Okamoto, E., “Proxy cryptosystem: delegation of the power to decrypt ciphertexts,” IEICE Trans. Fundamentals E80-A(1), pp. 54–63, 1997.

7 Blaze, M., Bleumer, G., and Strauss, M., “Divertible protocols and atomic proxy cryptography,” Nyberg, K.

(ed.), EUROCRYPT 1998, LNCS, Vol. 1403, pp. 127–144, Springer, Heidelberg, 1998.

8 L. Wang, J. Shao, Z. Cao, M. Mambo, and A. Yamamura, "A certificate-based proxy cryptosystem with revocable proxy decryption power," INDOCRYPT 2007, LNCS 4859, Springer-Verlag, Berlin, pp. 297–311, 2007.

9 Chu, C. and Tzeng, W., "Identity-based proxy re-encryption without random oracles," Garay, J.A., Lenstra, A.K., Mambo, M., Peralta, R. (eds.), ISC 2007, LNCS, Vol. 4779, pp. 189–202, Springer, Heidelberg, 2007.

10 Green, M. and Ateniese, G., "Identity-based proxy re-encryption," Katz, J., Yung, M. (eds.), ACNS 2007, LNCS, Vol. 4521, pp. 288–306. Springer, Heidelberg, 2007.

11 Matsuo, T., "Proxy re-encryption systems for identity-based encryption," Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds.), Pairing 2007, LNCS, Vol. 4575, pp. 247–267, Springer, Heidelberg, 2007.

12 Tang, Q., Hartel, P.H., and Jonker, W., "Inter-domain identity-based proxy reencryption," Yung, M., Liu, P., Lin, D. (eds.) INSCRYPT 2008, LNCS, Vol. 5487, pp. 332–347, Springer, Heidelberg , 2008.

13 Ateniese, G., Fu, K., Green, M., and Hohenberger, S., "Improved proxy re-encryption schemes with applications to secure distributed storage," Internet Society (ISOC): NDSS 2005, pp. 29–43, 2005.

14 L. Wang, L. Wang, M. Mambo, and E. Okamoto, "New Identity-Based Proxy Re-Encryption Schemes to Prevent Collusion Attacks," Pairing 2010, Springer-Verlag, Berlin, LNCS 6487, pp. 327–346, 2010.

15 Paillier, P., "Public-key cryptosystems based on composite degree residuosity classes," Stern, J. (ed.), EUROCRYPT 1999, LNCS, Vol. 1592, pp. 223–238, Springer, Heidelberg, 1999.

16 ElGamal, T., "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory (TIT), 31(4), pp. 469–472, 1985.

17 Chevallier-Mames, B., Paillier, P., and Pointcheval, D., "Encoding-free elgamal encryption without random oracles," Yung, M., Dodis, Y., Kiayias, A., Malkin, T.G. (eds.), PKC 2006, LNCS, Vol. 3958, pp. 91–104, Springer, Heidelberg, 2006.

18 L. Wang, L. Wang, Y. Pan, Z. Zhang, and Y. Yang, "Discrete-log-based additively homomorphic encryption and secure WSN data aggregation," ICICS 2009, Springer-Verlag, Berlin, LNCS 5927, pp. 493– 502, 2009.

19 L. Wang, L. Wang, Y. Pan, Z. Zhang, and Y. Yang, "Discrete-log-based additively homomorphic encryption and secure WSN data aggregation," Information Science, to appear, 2011.

20 王立華，田中秀磨，市川隆一，岩間司，小山泰弘，"準同型暗号技術を用いた位置情報認証に関する一考察," SCIS2011, 1F1-2, 2011.

21 宇宙航空研究開発機構，"準天頂衛星システムユーザインタフェース仕様書,"
http://qzss.jaxa.jp/is-qzss/IS-QZSS_12Draft_J.pdf

22 高島和宏，市川隆一，高橋冨士信，大坪俊通，小山泰弘，関戸衛，瀧口博士，ホビガートーマス，"VLBI 相関処理技術を利用した時空情報正当性検証に関する基礎研究," 第 112 回日本測地学会講演会，Nov. 4, 2009.

23 王立華，"代理復号と代理再暗号二つの機能付き ID ベースプロキシ暗号システムの構築方法," 特許出願番号：PCT/IB2009/006721.

（平成 23 年 6 月 15 日 採録）

王　立華（Lihua Wang）
ネットワークセキュリティ研究所
セキュリティ基盤研究室専攻研究員
博士（工学）
暗号プロトコル