情報処理学会
グループウェアとネットワークサービス研究会
2014年11月27日, 28日

# ID ベース暗号を用いた車々間・路車間認証方式の提案とその評価

レ・スアン・ヒウ[†1]　井手口　哲夫[†1]　奥田　隆史[†1]　田　学軍[†1]

車々間・路車間通信システムにおいてもセキュリティ面で様々な脅威が存在している。これらの脅威に対応するために、暗号技術を用いて発信元の真正性確認とメッセージの完全性や機密性を確保することは必要不可欠である。それを実現するために、車載器や路側機の機器間認証が必要となる。本論文では、従来の公開鍵暗号より利便性が高いとされる ID ベース暗号を用いて、車々間および路車間の認証方式を提案する。提案方式は二つのステップから構成される。まず、車両の ID に対する秘密鍵を生成する。次に、道路で走行している車両同士や車両と路側の間の機器認証を行う。認証ステップにおいて機器同士がお互いに正当性を確認できる。認証後、暗号通信で不正行為防止と機密性確保も可能となる。また、実現可能性を確認するために通信可能時間に対する処理・通信時間の割合についての評価を行い、提案方式の有効性を示す。

# A Proposal of inter-vehicle (road-vehicle) authentication method using ID-based encryption and its Evaluation

LE XUAN HIEU[†1]　TETSUO IDEGUCHI[†1]
TAKASHI OKUDA[†1]　XUEJUN TIAN[†1]

From a security side, various menaces exist in the IVC-RVC system. It is essential that using Cryptography to authenticity check of the source and to ensure message confidentiality and integrity. To realize it, The certification between the in-vehicle device and roadside device is necessary. In this paper, using the ID-based encryption which is more convenience than the conventional public key encryption, we propose an authentication method of IVC-RVC. There are two steps in the proposed scheme. The first is that generating a secret key for the ID of the vehicle. The next is device authentication between the roadside - the vehicle and among vehicles traveling on the road. In the authentication step, devices can confirm the authenticity each other. After authentication, confidentiality and ensuring fraud prevention can be achieved by using cryptographic communication. To confirm effectiveness of the proposed method, we carry out simulation to evaluate the processing and communication time.

## 1. はじめに

近年、自動車事故や渋滞を軽減するために、車々間・路車間通信を用いた衝突・追突防止などの安全運転支援サービスや渋滞などの交通情報を提供するサービスの普及を期待されている。しかし、セキュリティ面から、車々間・路車間通信システムにおいて様々な脅威が存在している [1]。

これらの脅威に対応するために、暗号技術を用いた発信元の真正性確認とメッセージの完全性や機密性を確保することは必要不可欠である。そのため、まず車載器や路側機の機器間認証が重要となる。

公開鍵アルゴリズムによるデジタル署名方式を用いて車々間・路車間通信セキュリティ規格として、米国で検討されている(IEEE1609.2)[1]。本方式は公開鍵暗号基盤(PKI:Public Key Infrastructure)を適用した方式である。車載器や路側機は鍵ペア（秘密鍵と公開鍵）を生成し、信頼できる第三者機関である認証局(CA:Certification Authority)に登録する。CA から秘密鍵に対となる公開鍵の所有者を証明する公開鍵証明書が発行される。認証や暗号通信の際、受信側において、メッセージに対する電子署名の検証と送信元公開鍵証明書の検証によって真正性と完全性の確認が実現される。しかし、毎回、送信元公開鍵証明書の検証で手間がかかり、通信オーバヘッドが大量で車々間通信には負荷となる。

現在、ID ベース暗号の実用化研究が盛んになされている。従来の公開鍵暗号に比べて ID ベース暗号は公開鍵認証センターが不要であり、受信側では送信者の公開鍵取得、公開鍵証明書作成、公開鍵証明書添付、公開鍵の検証などの処理も不要である利点を持っている [2]。しかし、限られた通信時間と利用可能な設備の環境である車々間通信システムにおいては ID ベース暗号を用いて車々間認証手法の研究は詳細に検証されてない。

そこで本論文では、ID ベース暗号を用いて、車々間および路車間の認証方式を提案する。実現可能性を評価するた

†1 愛知県立大学情報科学研究科
Graduate School of Information Science and Technology
Aichi Prefectural University

めに通信可能時間に対して処理・通信時間の割合について評価を行い、提案方式の有効性を示す。

## 2. ID ベース暗号

ID ベース暗号 (Identity-Based Encryption：IBE) とは、公開鍵暗号方式の一つで、ID 情報を公開鍵として利用できる方式である。IBE の概念は 1984 年に Shamir によって、提案された [3]。しかし、予備通信が必要であり、安全性上のしきい値があり、必ずしも満足のいくものではなかった。

これらの問題は 2000 年にペアリングの双線形性を利用し、境・大岸・笠原らによって解決された[4]。その後、ペアリングを利用した Boneh-Franklin(BF)の手法[5]、Boneh-Boyen (BB1) の手法[6] などがある。

### 2.1 暗号仕組み

ID ベース暗号の特徴は先に公開鍵 ($P_k$: Public key)を決めてから秘密鍵($S_k$: Secret key) を生成することである。秘密鍵 $S_k$ を生成できるのは鍵発行センターKGC（Key Generation Center）のみである。そのため，任意のユーザ宛の暗号文を不正に復号可能であるため、信頼できる KGC は必ず必要となる。図 2 に ID ベース暗号による暗号化通信の利用手順を示す[7][8]。

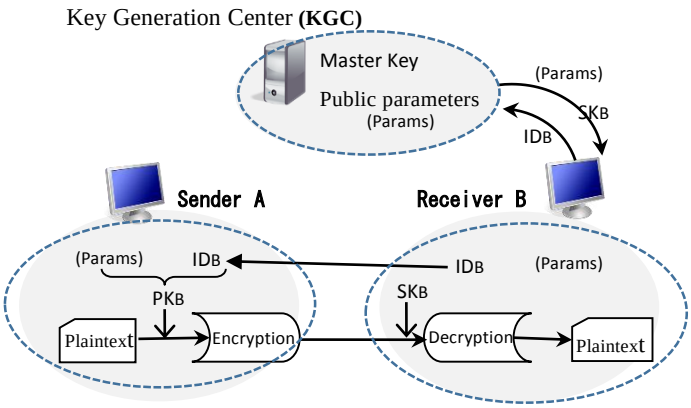


図 2.1 :ID ベース暗号

1. 鍵発行センターKGC は IBE の共有パラメータ(params)を生成し、公開する。
2. 利用者は自ら特定する一意の情報(ID) を KGC へ送り、秘密鍵生成を申請する。
3. KGC は自分のマスターキーを利用して申請者の秘密鍵を生成し、安全な方法により申請者へ送る。
4. 送信者は、受信者の ID と KGC の公開パラメータを用いて暗号化を行い、暗号文を送信する。
5. 受信者は自分の秘密鍵で復号

### 2.2 ID ベース暗号の利点

従来の公開鍵暗号に比べて ID ベース暗号(IBE)は次のような利点を持っている [7]。

**公開鍵認証センターが不要**

IBE においては暗号送信者は、受信者の ID と共通パラメータのみから暗号分を作成することが可能であり、この共通パラメータと ID の信頼性を確保できれば安全な通信が実現できる。したがって、送信者の公開鍵取得、公開鍵証明書作成、公開鍵証明書添付、公開鍵の検証などの処理が不要である。

**新規ユーザへの対応が容易**

新規ユーザを追加する際、公開鍵暗号では、そのユーザの公開鍵の入手と認証を行った上で公開鍵リストを更新必要があるが、IBE では、ID 以外に新たに必要な情報を追加する必要はない。

**未登録者への送信が可能**

受信者の ID 入手できれば暗号文の作成ができるため、未登録者への送信が可能である。

### 2.3 階層型 ID ベース暗号

運用面では、一つの KGC ですべての利用者の鍵生成を行う場合，KGC の負担が非常に大きくなるため、複数の KGC を階層的に用いて鍵生成を行う必要が生じる。

階層型 ID ベース暗号(HIDE :Hierarchical ID-Based Encryption）[9]は,ユーザを木構造の各ノードに対応させた ID ベース暗号で,各ノードは子ノードの秘密鍵を生成し，ノードの ID はルートノードまでのノード列となる.

## 3. 提案方式

階層型 ID ベース暗号を用いて、車々間・路車間の認証方式を提案する。

### 3.1 車両の ID のアプローチ

車両の ID は車両 を特定の一意の情報であり、更新が困難である。安全性を高めるため、本論文で提案する鍵ペアが使い捨て鍵ペアである。即ち、有効期限があり、その期限を消えたら秘密鍵を生成する必要がある。そのため、そのままの固有 ID を使えず、時刻情報を追加したデータを使い、秘密鍵生成する[5]。

また、固有 ID の信頼性を確認する必要があるので、現在普及している ETC(Electronic Toll Collection ) サービスの ETC 車載器管理番号を ID として使い、ID の確認を ETC の処理で行う。ETC 車載器管理番号は 19 桁の数字列である[17]。例えば、ID が 0000300196803002620 である時、時刻情報を追加し、ID データ yyyymmddhhmmss00003001968- 03002620 となる。

ID ベース暗号の ID は任意の文字列であるため、ETC 車

載器管理番号の他に免許証明書番号も考えられる。ただし、前提条件として、その ID は信頼性を確認済みものである。

### 3.2 鍵発行センターの設置場所

鍵ペアは使い捨て鍵ペアであるため、一定の期間中に更新する必要がある。利便性と現実性を考え、車両が走行中や休憩場所で秘密鍵を入手することができればよい。そのため、鍵発行センターは以下のような５つの場所に設置すると考えられる。

1. 高速道路の料金所(ETC ゲート)
2. 信号機
3. ガソリンスタンド
4. 充電スタンド
5. コンビニエンスストア

個々鍵発行センターの負荷を減らすために、階層型 ID ベース暗号を採用する。

### 3.3 車々間・路車間の認証方式

車々間・路車間の認証方式は２つのステップから成る。ステップ 1 は車両の ID に対する秘密鍵を生成することである。ステップ 2 は道路で走行している車両同士や車両と路側の間の機器認証を行う。

#### 3.3.1 秘密鍵生成

鍵発行センターは５つの所に設置すると考え、５つのサーバが必要である。それらのサーバから発行した鍵ペアで認証や暗号通信を行うために、各サーバのマスターキーを同じ鍵発行センター(root)で発行する必要である。

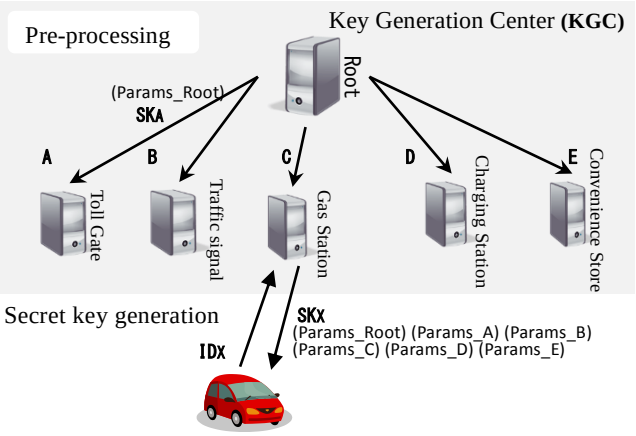


図 3.3.1:秘密鍵生成

図 3.3.1 に示すように、事前処理としてまず各サーバ（子鍵発行センター）はあるルート鍵発行センターに自分の ID を送信し、秘密鍵生成を申請する。ルート鍵発行センター（Root）では、その ID に対する秘密鍵を生成し、自分の公開パラメータを返信する。次に、各サーバ（子鍵発行センター）では、秘密鍵をマスターキーとする。また、自分の公開パラメータを他のサーバへ送信する。ここまで、各子鍵発行センターの設定を完了する。

その後、車両はいずれかのサーバへ自分の ID データを送信し、秘密鍵生成を申請する。車両の ID データを前述のように固有 ID に時刻情報を追加したデータである。子鍵発行センターではその ID データに対する秘密鍵を生成し、すべての鍵発行センターの公開パラメータと共に返信する。

#### 3.3.2 認証

走行している前後の車または路側機と通信する時、先に認証を行う必要がある。以下に認証の手順を説明する(図 3.3.2)。ただし、受信側 Y は車または路側機である。

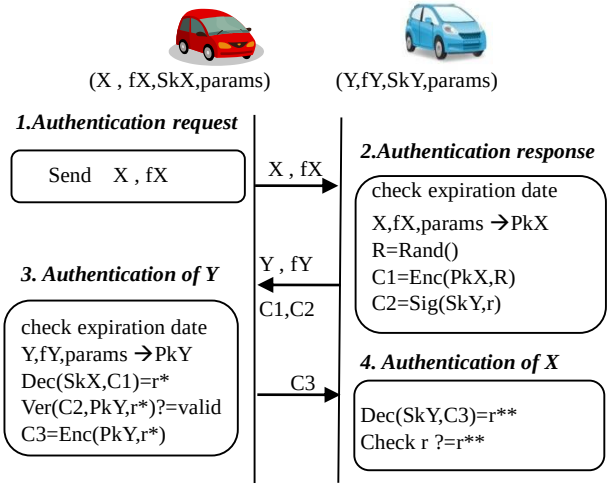


図 3.3.2:認証手順

1. 認証要求

送信側は自分の ID データ(X)と秘密鍵生成したサーバ ID (fX)を、認証を要求する。

2. 認証要求応答

受信側では、X と fX の有効期限を確認する。有効であれば、（X、fX）と params から送信側の公開鍵 PkX を計算する。次に、ランダムにチャレンジデータ r を生成する。PkX で r を暗号化し、自らの秘密鍵 SkY で r の署名を生成する。自分の ID データ（Y）、秘密鍵生成したサーバ ID (fY) と暗号文と共に送信側に返信する。時間を節約するために、チャレンジデータ r 生成、r の署名生成の処理を事前に計算する。

3. 受信側 Y の認証

送信側 X では、まず Y と fY の有効期限を確認してから受信側の公開鍵 PkY を計算する。次に、チャレンジデータ r を暗号化した暗号文を自分の秘密鍵で復号し、r*

を得る。公開鍵 PkY と r*で署名 C2 を検証する。署名の検証ができれば、受信側 Y の認証が成功する。その後、Y の公開鍵 PkY で r*を暗号化し、Y に送る。

4. 送信側 X の認証

受信側 Y では、秘密鍵で受信した暗号文を復号し、チャレンジデータ r と一致すれば、送信側 X の認証が成功する。

## 4. 評価

提案方式の機能条件を満たすことと処理時間についての評価を行う。

### 4.1 機能条件

図 3.3.2 により、Y の認証で署名 C2 検証を成り立つことから送信側は受信側の正当性を確認する。また、X の認証で r = r** を成り立つことで、受信側は送信側の正当性を確認する。即ち提案方式で、車載器同士または車載器と路側機はお互いに正当性が確認できる。その後、暗号通信で、なりすましやデータ改竄の不正行為も防止できる。また、暗号化された暗号文を盗聴されても、復号できないため、メッセージの機密性が確保できる。公開鍵と秘密鍵の鍵ペアが一回しか使えないことで、安全性が高い。

### 4.2 処理時間

車々間・路車間通信の特徴の一つは通信できる時間が短い。その通信可能な時間に認証処理を完了する条件を満たすかを確認する。まず、各ステップの通信可能時間を計算する。次に、プログラムで各ステップの処理時間を測定し、通信方式のパケットフレームなどによる通信時間を計算する。最後に、通信可能時間に対する処理・通信時間の割合についての評価を行い、提案方式の有効性を示す。

4.2.1 条件導入

提案方式の各ステップにおける通信可能時間を求める。

**(1) 秘密鍵生成の時間条件**

高速道路の入口で料金支払い処理と共に行うため、ETC が利用している狭域通信(DedicatedShort Range Communication:DSRC) 方式[11] を使う。DSRC の通信範囲は 30m で、車の速度は入口において約 30Km/h とすると、通信可能時間 $t_1$ は

$$t_1 = \frac{30m}{30Km/h} = \frac{30m \times 3600s}{30 \times 1000\,m} = 3.6\,s$$

である。

一方、一般道の場合、鍵発行センターはコンビニ、ガソリンスタンドや充電スタンドでは車両を停止するため、もっと時間がある。残りの信号機の場合では通信可能時間は

$$t_1 = \frac{30m}{60Km/h} = \frac{30m \times 3600s}{60 \times 1000\,m} = 1.8\,s$$

となるため、秘密鍵生成の時間条件は 1.8 秒以下である。

**(2) 車々間・路車間通信可能時間**

日本の高速道路には、法定の最高速度は 100Km/h であり、最低速度は 50Km/h である。通信方式は 700MHz 帯通信システム[12] であることを前提する。文献[13] から、車々間の最大通信距離は 300m であり、路車間の最大通信距離は 239m であるとしたが、本論文で利用する車々間と路車間の通信距離は 100m とする。

そこで、車々間通信可能時間 $t_2$ は

$$t_2 \geq \frac{100m \times 2}{(100-50)\,Km/h} = \frac{100 \times 2 \times 3600s}{50 \times 1000} = 14.4\,s$$

となる。

一般道路では、最高の速度は 60Km/h と規定されている。最低速度を規定されていないが、走行すると、20Km/h 以上と考えられる。計算すると、通信可能な時間$t_2$は

$$t_2 \geq \frac{100m \times 2}{(60-20)\,Km/h} = \frac{100 \times 2 \times 3600s}{40 \times 1000} = 18s$$

である。ゆえに、車車間通信の条件は 14.4 秒以下である。

高速道路において路車間通信可能時間 $t_3$ は

$$t_3 \geq \frac{100m}{100\,Km/h} = \frac{100 \times 3600s}{100 \times 1000} = 3.6\,s$$

となる。一方、一般道においての計算は

$$t_3 \geq \frac{100m}{60\,Km/h} = \frac{100 \times 3600s}{60 \times 1000} = 6\,s$$

となるため、路車間通信の条件は 3.6 秒以下である。

4.2.2 処理時間の測定方法

提案方式の各ステップに、処理ごとにプログラムを実行し、時間測定を行う。

**(1) アルゴリズム**

文献[9]の方式に基づいて次のアルゴリズムで HIDE を構成する。

**【ルートセットアップ】**

ルート KGC は以下の動作を行う。

1. セキュリティパラメータ k を入力とし，位数 p の群である$\mathrm{G1}, \mathrm{G2}$ と GT, ペアリング$\mathrm{e}: \mathrm{G1} \times \mathrm{G2} \to \mathrm{GT}$ を選ぶ。
2. ハッシュ関数を選ぶ。
   $\mathrm{H1}: \{0,1\}^* \to G1\,,\quad H3: \{0,1\}^* \to G1$
3. $\mathrm{G1}$の生成元P (楕円曲線の点)、$Z_p^*$から整数$s$ をランダムに選び、$Q_0 = s_0 * P$を計算し、
   $\mathrm{params} = (\mathrm{G1}, \mathrm{G2}, \mathrm{P}, Q_0, H1, H3)$とセットする。

4. $s_0$ をルート KGC のマスターキー(主秘密鍵)、params を公開パラメータとする。

**【下位レベルセットアップ】**

各子 KGC はランダムな値$s_i \in Z_p^* \ (i = A,B,C,D,E)$ を選び、秘密値として保持しておく。また、$Q_i = s_i * P$ も公開パラメータとして公開する。$(A,B,C,D,E$は図 3.3.1 に示す各子 KGC である)

子 KGC の公開鍵は$H1(i)(i = A,B,C,D,E)$である。秘密鍵$Sk_i$はルート KGC で生成する。

$$Sk_i = s_0 * H1(i)$$

**【秘密鍵生成】**

子 KGC で与えるID ∈ {0,1}*に対する秘密鍵$Sk_{ID}$ を計算する。

$$Sk_{ID} = Sk_i + s_i * H1(ID) \in G1 \qquad (i = A,B,C,D,E)$$

**【公開鍵で暗号化】**

平文M ∈ {0,1}* は以下の手順で暗号化する。

1. ランダムに$r \in Z_p^*$ を生成する
2. $U1 = r * P$ を計算する
3. $U2 = r * H1(ID)$
4. $G_{ID} = e(H1(i), Q_0) \quad (i = A,B,C,D,E)$
5. $V = M \oplus {G_{ID}}^r$ を計算する

生成された U1,U2, V の組み合わせである C = (U1,U2, V) が暗号文として利用する。

**【秘密鍵で復号】**

秘密鍵$Sk_{ID}$を利用し、復号する。

$$V \oplus \frac{e(Sk_{ID}, U1)}{e(Q_i, U2)} = M$$

ペアリングの写像の双線形性により、

$$e(H1(i), Q_0)^r = e(Sk_{ID}, U1)/e(Q_i, U2)$$

であるため、暗号文 C から平文 M を得られる。

**【秘密鍵で署名生成】**

平文M ∈ {0,1}* は以下の手順で暗号化する。

1.ランダムに$r \in Z_p^*$ を生成する

2.$U1' = r * P$を計算する

3.$V' = Sk_{ID} + r * H3(M)$ を計算する

U1', V の組み合わせである C = ($U1'$, $V'$) が M の署名として利用する。

**【公開鍵で署名検証】**

公開鍵H1(ID),メッセージ M と署名 C = (U1' , V') より以下の関係が成り立つか否かで署名を検証する

$$e(Q_0, H1(i)) * e(Q(i), H1(ID)) * e(U1', H3(M)) ?= e(P, V')$$

**(2) 測定機器の性能**

測定機器(コンピュータ)の性能を表 4. 1 に示す

表 4.1 測定機器の性能

| | |
|---|---|
| CPU | Intel Core i5 (2.40 GHz) |
| Memory | 4.00 GB |
| OS | Ubuntu 12.04 TLS |
| Software | Gcc 4.6.3 ,Gmp 5.0.2<br>Pbc 0.5.12 (type A) [18] |

**4.2.3 通信時間の計算方法**

各ステップにおいて通信方式のパケットフレームに基づいて通信時間を計算する。ここで、秘密鍵生成ステップの通信を DSRC とし、 車々間・路車間通信の通信方式を 700MHz 帯高度道路通信システム とする。

(1) 狭域通信 DSRC 通信方式

秘密鍵生成の通信方式は DSRC(π/4 シフト QPSK) と想定する。この方式の特徴を以下に示す。

- 通信速度が 4906 kbps であり、通信データサイズが 400Bytes である。

- 移動局は最初に基地局からフレームコントロールメッセージスロット(FCMS) を受信してから、通信を行う。

- メッセージデータスロット(Message Data Slot:MDS)

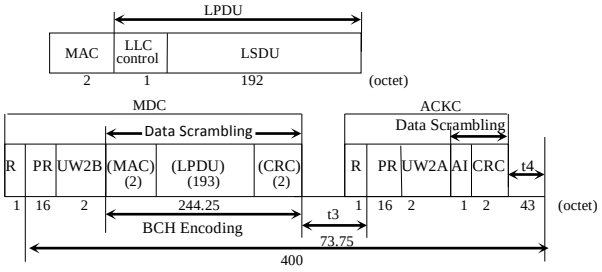


図 4.1: MDS format(文献[11],pp.67-69 より引用)

LPDU は、LLC(Logical Link Control:論理リンク制御) 制御フィールドと LSDU（LinkService Data Unit）からなる。LLC 副層から渡される LPDU がオクテットの単位で正規化したものでない場合は破棄する。 193 オクテット以上の長さを有する LPDU は，MAC 副層で 193 オクテットの単位で分割化し，複数のフレームを用いて伝送する。また、データ長が 193 オクテット未満の場合には、MAC 副層で 193 オクテットまで 0 を挿入し、193 オクテットとする。

」秘密鍵生成の通信を図 4.2 に示す。

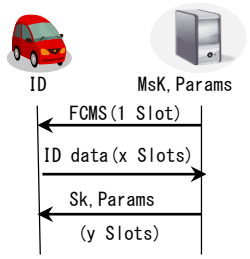


図 4.2 秘密鍵生成の通信

ここで、一つスロットの通信時間は

$$\frac{401 \times 8}{4906 \times 1000} = 0.00065(s)$$

である。従って、通信時間は

$$(1 + x + y) \times 0.65(ms)$$

となる。

(2) 700MHz 帯高度道路交通システム

車々間・路車間の通信方式は 700MHz 帯高度道路交通システムと想定する。本システムは、変調方式に OFDM（Orthogonal Frequency Division Multiplexing）方式を用いる伝送方式とする[11]。本節の目的は通信時間を計算することであり、文献[11] の「パケット 1 個の送信に要する時間の計算法」を利用し、計算を行う。

**【パケット 1 個の送信に要する時間の計算法】**

送信に要する時間は、パケットの長さとデータレートによって異なる。以下に、図 4.3 のフレームフォーマットを参照し、MSDU(MAC Service Data Unit:MAC サービスデータ単位) 長が xBytes、データレートが 12Mbps（16QAM R=1/2）の場合について計算法を例示する。

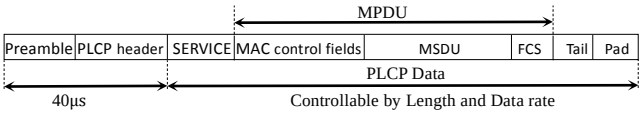


図 4.3 Frame format (文献[12],p.115 より引用)

● PLCP(Physical Layer Convergence Protocol) Data の長さを計算 MPDU (MAC Protocol Data Unit ,(x + 28)Bytes）に SERVICE（16bit)、Tail（6bit)、及び Pad を付加する。Pad は、PLCP Data が OFDM シンボル 1 個を含むデータビット数の整数倍になるように追加する。この例では、MPDU に SERVICE と Tail を付加した段階で、$(x + 28) \times 8 + 16 + 6 = y$(bits)となる。OFDM シンボル 1 個に含まれるデータビット数が 96 なので、Pad を z(bits)とすれば、(y + z)/96 シンボル分になる。

● パケット全体の送信に要する時間を計算
Preamble と PLCP ヘッダの送信時間（パケットによらず40μs）を含めて、$40 + [(y + z)/96] \times 8 = v(\mu s)$となる。なお、送信前の最短スペース時間（32μs）の待機分を含めると、(v + 32)μsとなる。

● 複数パケットの連続送信の場合
基地局は、路車間通信期間に複数のパケットを送信するとき、パケット間に最短スペース時間の待機を行うことを考慮して全体の送信に要する時間を計算する。

また、文献[12] による、車々間通信用のデータサイズは 100Bytes 程度であり、路車間通信用のデータサイズは最大 7k Bytes 程度であるとされる。そこで、車々間通信 MSDU 長(x) は最大 60 Bytes とする。

#### 4.2.4 結果

各処理に C 言語プログラムを実行し、1000 回測定の処理時間の結果は表 4.2 に示す。

表 4.2 処理時間

| ステップ | 秘密鍵生成 (ms) | 認証時間(ms) | | | |
|---|---|---|---|---|---|
| | | 認証応答 | X の認証 | Y の認証 | 合計 |
| 最大値 | 80.4 | 88.9 | 108.3 | 40.0 | 213.1 |
| 最小値 | 47.8 | 44.1 | 80.8 | 20.2 | 151.3 |
| 平均 | 56.5 | 53.7 | 90.7 | 29.2 | 173.6 |

4.2.3 で説明した計算方法に実際のデータサイズを適用し、計算した結果は表 4.3 である。

表 4.3 処理時間

| ステップ | 秘密鍵生成 | 車々間認証 | 路車間認証 |
|---|---|---|---|
| 通信方式 | DSRC | 700MHz 帯通信システム | |
| 単位データ | 400B | 100B 程度 | 最大 7KB 程度 |
| 通信時間(ms) | 9.8 | 6.6 | 2.1 |

表 4.2 の最悪場合の結果に通信時間を加え、4.2.1 で導入した条件と比較する。その結果を表 4.4 に表示する。

表 4.4 比較結果

| ステップ | 秘密鍵生成 | 車々間認証 | 路車間認証 |
|---|---|---|---|
| A= 条件 (ms) | 1800 | 14400 | 3600 |
| B=処理時間(ms) | 80.4 | 213.1 | |
| C=通信時間(ms) | 9.8 | 6.6 | 2.1 |
| D= B+C | 90.2 | 219.7 | 215.2 |
| D/A | 5.0% | 1.5% | 6.0% |

秘密鍵生成ステップにおいて、処理・通信時間は通信可能時間の 5.0%を占めている。秘密鍵と公開パラメータを受信した後、車両と鍵発行センターとの通信を行わないため、この結果で提案方式が適用できると考えられる。

認証ステップにおいて次のように考えられる。

車々間認証の場合、処理・通信時間は通信可能時間の 1.5%を占め,残りの 98%以上の時間に十分に暗号通信を行うことができる。

路車間認証の場合、処理・通信時間は通信可能時間の 6.0%を占め, 路車間通信のデータサイズは 7KBytes 程度であるため、残りの 94%の時間に十分に暗号通信を行うことができる。

以上の考察から、道路に ID ベース暗号を用いる車々間および路車間の認証方式が適用できると考えられる。

## 5. おわりに

本論文では、ID ベース暗号を用いて、車々間および路車間通信システムの認証方式を提案し、評価を行った。

本提案方式は機器同士がお互いに正当性を確認でき、機能条件を満たしている。認証後、暗号通信でなりすましやデータ改竄の不正行為も防止できる。暗号化された暗号文を盗聴されても、復号できないため、メッセージの機密性が確保できる。公開鍵と秘密鍵の鍵ペアが 1 回しか使えないことで、安全性が高まる。

また、高速度路と一般道において通信可能時間の理論値から条件を導入し、プログラムの実行時間で処理時間を測定した。通信方式の標準規格により通信時間を計算した。結果により、秘密鍵生成のステップと車々間および路車間の認証のステップにおいて、提案方式の処理・通信時間は通信可能時間の僅かな時間(6%以下)しか占めていない。故に、道路において ID ベース暗号を用いる車々間および路車間の認証方式を適用することができると確認した。

**謝辞**

本研究の一部は、平成 26 年度文部科学省科学研究費補助金基盤研究(C)(24500087, 24500088)の支援を受けて行った。

## 参考文献

[1] 運転支援通信システムに関するセキュリティガイドライン「ITS FORUM RC-009 1.0 版」, ITS 情報通信システム推進会議,2011.
[2] 小林鉄太郎, 山本剛, 鈴木幸太郎, 平田真一, ID ベース暗号の応用とキーワード検索暗号、NTT 技術ジャーナル 2010.2 ,pp.17-20 , 2010.
[3] A.shamir,"Identity-based cryptosystem and signature schemes".In Proc. CryPTO1984,volume 196 of Lecture Notes in Computer Science,pp47-53.Springer-verlag,1985.
[4] Ryuichi Sakai , Kiyoshi Ohgishi and Masao Kasahara, "Crypto-systems Based on Pairing",Proc. of SCIS2000, C20, Jan. 2000
[5] D. Boneh and M. Franklin, " Identity-Based Encryption from the Weil Pairing, " CRYPTO 2001, LNCS 2139, pp.213-229, 200136
[6] X. Boyen, "The BB1 Identity-Based Cryptosystem:A Standard for Encryption and KeyEncapsulation ",IEEE P1363.3 draft,2006.
[7] CRYPTREC ID ベース暗号調査 WG, 「ID ベース暗号に関する調査報告書」, http://www.cryptrec.go.jp/report/c08 idb2008.pdf 2009.
[8] 岡本 栄司, 岡本 健, 金山 直樹, 「ペアリングに関する最近の研究動向」, 電子情報通信学会基礎・境界ソサイエティ Fundamentals Review Vol.1 No.1 ,pp.51-60,2007.
[9] C. Gentry and A. Silverberg,"Hierarchical ID- Based Crypto-graphy," in Proceedings of Advances in Cryptology — Asiacrypt 2002, Lecture Notes in Computer Science 2501, pp.548–566, 2002.
[10] 高木 剛,「進化する公開鍵暗号(RSA 暗号,楕円曲線暗号,ID ベース暗号)」、電子情報通信学会技術研究報告. IT, 情報理論 108(472), pp.47-48, 2009
[11] 「狭域通信（DSRC）システム標準規格 ARIB STD-T75 1.5 版」,電波産業会,2008
[12] 「700MHz 帯高度道路交通システム標準規格 ARIB STD - T109 1.0 版」,電波産業会,2012
[13] 佐々木 邦彦, 「700MHz 帯高度道路交通システムの標準規格の概要について」, 第 94 回電波利用懇話会, 電波産業会,2012
[14] 中ノ森 賢朗,岐部 景子,太刀川 喜久男,「 ETC/ETC 応用 /ITS スポットと ITS 通信」、電子情報通信学会誌 Vol.95, No.8, pp.706-711, 2012
[15] 安藤英 里子, 佐藤 尚宜, 福澤 寧子, 「車車／路車間通信システムへの online/ offline 認証方式の適用」、 信学技報,ITS2011-22(2011-12),pp.13-18、2011
[16] 車載器管理番号確認方 http://www.orse.or.jp/use2/service04.html
[17] PBC Library http://crypto.stanford.edu/pbc/
[18] ITS ホームページ - 国土交通省 http://www.mlit.go.jp/road/ITS/j-html/
[19] IPA 独立行政法人 情報処理推進機構 情報セキュリティ http://www.ipa.go.jp/security/index.html