高速道路における車々間通信システムへの ID ベース暗号の適用とその評価

レスアンヒウ† 井手口哲夫† 奥田隆史† 田学軍†

近年、自動車事故や渋滞を軽減するために、車々間・路車間通信システムの実用化検討が進んでいる。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。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。本稿では、ID ベース暗号を用いて、高速道路における車々間(路車間) 認証方式を提案し、その評価を行う。提案方式は三つのステップがある。まず、ステップ 1 は秘密鍵生成である。次に、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と暗号通信を行う。最後に、第 3 ステップはステップ 2 で利用した暗号鍵と復号鍵の鍵ペアを失効させる処理である。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できると考えられる。また、本提案の評価として各ステップの通信可能時間を算出し、プログラムの実行時間と通信方式のパケットフレームにより、処理・通信時間を測定し、その結果より、処理・通信時間は通信可能時間の 17%以下であることから、本提案方式の有効性を考察する。

Applying ID based Encryption to Inter-Vehicle Communication on Highway and its Evaluation

LE XUAN HIEU† TETSUO IDEGUCHI†
TAKASHI OKUDA† XUEJUN TIAN†

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。

暗号技術では主に共通鍵暗号と公開鍵暗号がある。前者は暗号化する時と復号する時に同じ鍵と同じアルゴリズムを使い、「対称アルゴリズム」とも呼ばれている。後者は暗号鍵と復号鍵がそれぞれ違う鍵を使う方式で、片方の鍵を相手に公開し、暗号化と復号が違う処理で行われることで「非対称アルゴリズム」とも呼ばれている。一方の鍵で暗号化した暗号文は、もう一方の鍵でしか復号できないと言う性質を利用して、デジタル署名などの本人確認に応用することができる。

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 IEEE16092.2 がある[1]。本方式では、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証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、送信元公開鍵証明証の検証で手間がかかると考えられる。現在、公開鍵証明証不要と言われ、公開鍵暗号の一種である ID ベース暗号の実用化研究が盛んである[2]。ID ベース暗号を用いれば、送信元公開鍵証明証検証の時間を節約できると考えられる。

そこで本稿では、ID ベース暗号を用いて、高速道路における車々間(路車間) 認証方式を提案し、評価を行う。

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ったり、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。

ID ベース暗号の特徴は先に公開鍵 P_K を決めてから秘密鍵 Sk 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 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) 復号可能であるので、信頼できる KGC は必ず必要となる。以下に ID ベース暗号による暗号化通信の利用手順を示す（図 2)[7][8]。

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

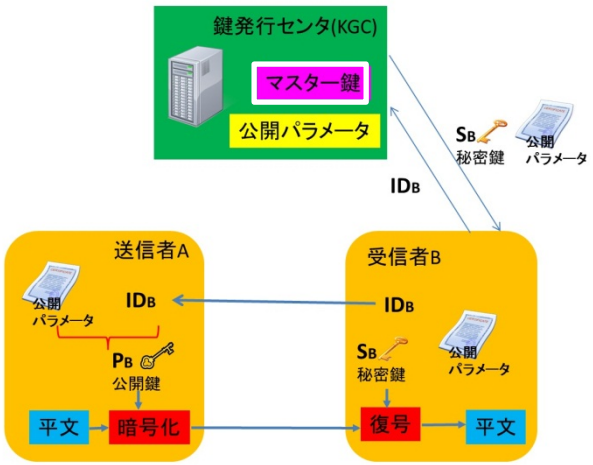

図 2:ID ベース暗号

1. 鍵発行センタ KGC は IBE の共有パラメータを生成し、公開する。
2. 利用者は自らを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 は自分のマスター鍵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暗号文を復号する。

3. 提案方式

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。しかし、一般道路では鍵発行センタ KGC の設置が困難であるため、まず高速道路環境で検討する。高速道路の料金所を鍵発行センタとする。提案方式は 3 つのステップから成り、処理内容について述べる。

3.1 *step1:*秘密鍵生成

高速道路の入口で料金支払い処理と共に行う。手順を以下に示す(図 3.1)。

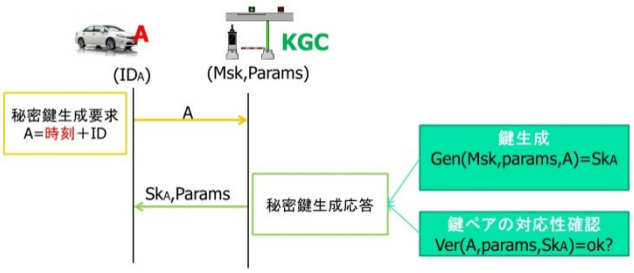

図 3.1: 秘密鍵生成

1. 秘密鍵生成要求
車 A は料金所に入るとき、自分の ID データ A を KGC に送り、秘密鍵生成を申請する。ID データ A は入る時刻と車 A の固有 ID からなったデータである。固有 ID が車 A 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、本稿で提案する鍵ペアが一回しか使えない鍵ペアである。つまり、高速道路に入る度に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。

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 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[9]。例えば、ID が 00003001968030026 20 である時、時刻情報を追加し、ID データ 20120906123216000030019680300262 0 となる。

2. 秘密鍵生成応答
KGC では、受信した ID データ A と自らのマスター鍵 Msk、公開パラメータ params から、A に対応する秘密鍵 SkA を生成する。鍵ペアの対応性を確認し、SkA と params を車 A に返信する。この通信が狭い範囲であり、安全性は確保されているものとする。

3.2 *step2:*車々間・路車間認証

高速道路に入ってから、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 3.2)。ただし、受信側 B は車または路側機である。

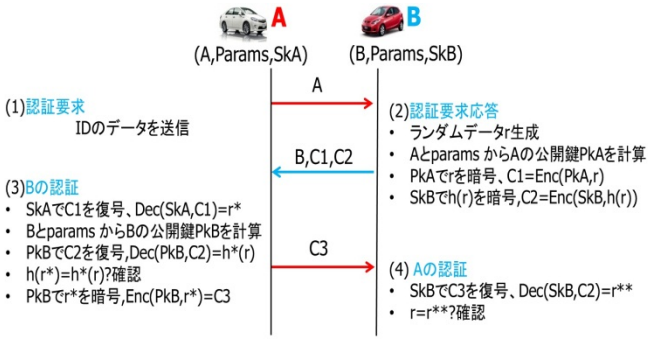

図 3.2: 認証方式

1. 認証要求
送信側は自分の ID データを受信側へ送る。
2. 認証要求応答
受信側では、ランダムにチャレンジデータ r を生成する。受信した ID データ A と KGC の公開情報 params から送信側の公開鍵 PkA を計算し、PkA で r を暗号化する。また、自らの秘密鍵 SkB で r のハッシュ値も暗号化し、自分の ID データ B と暗号文と共に送信側に返信する。
3. 受信側 B の認証
送信側では、まずチャレンジデータ r を暗号化した暗号文を自分の秘密鍵で復号する。次に、B と params から受信側の公開鍵 PkB を計算し、r のハッシュ値の暗号文を復号し h*(r)を得る。先の復号で得られた r*のハッシュ

値を計算し、h*(r)と一致すれば、受信側(B) の認証が成功する。その後、B の公開鍵 PkB で r*を暗号化し、B に送る。

4. 送信側 A の認証

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(A)の認証が成功する。

認証後の暗号通信は二つの方法がある。

【ケース 1】 チャレンジデータ r を共通鍵として、共通暗号で暗号通信を行う。

【ケース 2】 そのまま鍵ペアを利用して、公開鍵暗号で暗号通信を行う。

3.3 *step3:*鍵の失効

高速道路から出たとき、自分の ID データを送っても、受信した相手が KGC の params を使えず、公開鍵を計算できないため、認証が失敗し、秘密鍵も無効となる。つまり、鍵ペア(PkA, S kA) は一回しか使えない。但し、通信中の相手との通信は終了まで可能である。

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 3.2 により、B の認証で h(r*) = h*(r) 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、A 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。

つまり、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。

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[10] 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

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

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[11] であると前提する。文献[12] 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、本稿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

$$t_2 \geq \frac{2 \times 100m}{(100-50)Km/h} = \frac{200m \times 3600s}{50 \times 1000m} = 14.4s$$

となる。同様、路車間通信可能時間 t_3 は

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

となる。

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。プログラムについて以下に説明する。

(1) アルゴリズム

計算コストが小さい、簡単に理解できる Boneh-Franklin (BF) の手法を採用する。以下にアルゴリズムを示す。

【KGC のパラメータ生成[setup(k)]】 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。

$\mathrm{H1}: \{0,1\}^* \to G1$, $H2: \{0,1\}^* \to GT$, $H3: GT \to \{0,1\}^*$

ただし、M ∈ {0,1}*に対し、H3(H2(M)) = M が成立する。

3. 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、$P_{pub} = s * P$を計算し、params = $(\mathrm{H1}, \mathrm{H2}, \mathrm{H3}, \mathrm{P}, P_{pub})$とセットする。
4. s を KGC のマスターキー(主秘密鍵)、params を公開パラメータとする。

- 秘密鍵生成[Gen(Msk, params, ID)]

与えるID ∈ {0,1}*に対する秘密鍵Sk_{ID} を計算する。

$$Sk_{ID} = s * H1(ID) \in G1$$

- 暗号化[Enc(M, params, ID)]

平文M ∈ {0,1}* は以下の手順で暗号化する。

1. ランダムに$x \in Z_p^*$ を生成する
2. $\mathrm{U} = x * P$を計算する
3. $G_{ID} = e(H1(ID), P_{pub})$ 一回ペアリング
4. $\mathrm{V} = \mathrm{H2(M)} * {G_{ID}}^x$を計算する

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

- 復号[Dec(S kID, params,C)]

秘密鍵Sk_{ID}を利用し、以下の手順で復号する。

1. ペアリング$e(Sk_{ID}, U)$を計算する

2. $Y = V * e(Sk_{ID}, U)^{-1}$ を計算する

3. H3(Y) = M(平文) を得る

ここで、ペアリングの双線形性により、

$$e(Sk_{ID}, U) = e(s * H1(ID), x * P) = e(s * p, x * H1(ID))$$

$$= \left[e(P_{pub}, H1(ID)) \right]^{x} = G_{ID}{}^{x}$$

ゆえに、

$$Y = V * e(Sk_{ID}, U)^{-1} = H2(M) * G_{ID}{}^{x} * e(Sk_{ID}, U)^{-1}$$

$$= H2(M) * G_{ID}{}^{x} * G_{ID}{}^{-x} = H2(M)$$

よって、

H3(Y) = H3(H2(M)) = M

を得られ、復号アルゴリズムの完全性が明らかになる。

【補足】

秘密鍵で暗号化と公開鍵で復号のアルゴリズムは Boneh-Franklin(BF) の手法に定義しないが、ペアリングの双線形性により、以下のように定義できる。

- **秘密鍵で暗号化 Enc(S kID, params, M)**

1. ランダムに$x \in Z_p^*$ を生成する

2. $U = x * P_{pub}$を計算する

3. $G_{ID} = e(Sk_{ID}, P)$ 一回ペアリング

4. $V = H2(M) * G_{ID}{}^{x}$を計算する

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

- **公開鍵で復号 Dec(ID, params,C)**

1. ペアリング$e(H1(ID), U)$を計算する

2. $Y = V * e(H1(ID), U)^{-1}$ を計算する

3. H3(Y) = M(平文) を得る

(2) プログラムの言語

認証後、**共通鍵暗号で暗号通信**を行う場合、チャレンジデータ r を共通鍵として利用する。r はランダムに生成されるため、ハッシュ関数 H2 : {0, 1}∗ → GT が不要である。C 言語プログラムを利用し、実現する。しかし、**公開鍵暗号で暗号通信**を行う場合、認証後の通信メッセージを GT の元に変換する H2 関数が必要である。実際に、C 言語で H2 を実現するのはかなり困難であるため、Java 言語プログラムを採用する。

(3) 測定機器の性能

測定機器(コンピュータ)の性能を表 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 Pbc 0.5.12[13] ,Eclipse juno 4.2

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)

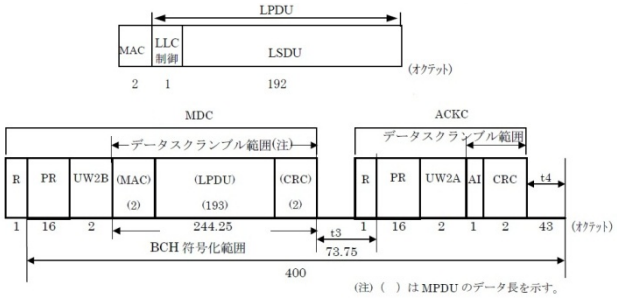

図 4.1: MDS フォーマット(文献[8],pp.67-69 より引用)

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。

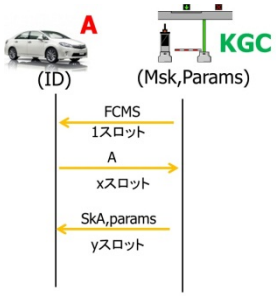

図 4.2 秘密鍵生成の通信

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。

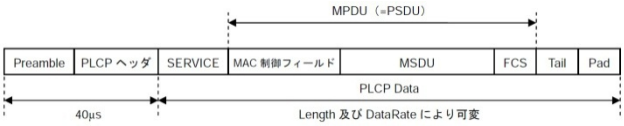

図 4.3 フレームフォーマット、(文献[9],p.115 より引用)

- 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 結果と考察

(1) ケース 1:認証後、共通鍵暗号で暗号通信を行う場合

各処理に C 言語プログラムを実行し、50 回測定の処理時間の結果は表 4.2 に示す。

表 4.2 ケース 1 の処理時間

ステップ	秘密鍵生成(ms)	認証時間(ms)			
		認証応答	B の認証	A の認証	合計
最大値	56.76	60.52	64.54	33.36	143.09
最小値	33.85	42.75	40.09	15.39	100.08
平均	**42.78**	50.09	49.78	23.39	**124.09**

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: ケース 1 の通信時間

ステップ	秘密鍵生成		車々間通信			路車間通信		
通信方式	DSRC		700MHz帯通信システム					
単位データサイズ	400bytes		100bytes 程度			最大7kbytes 程度		
送受信データ	A	SkA,params	A	B,C1,C2	C3	A	B,C1,C2	C3
サイズ(Bytes)	34	1297	34	1284	625	34	1284	625
時間(ms)	**5.87**		0.12	2.97	1.5	0.1	0.95	0.5
			4.57			**1.58**		

4.2.1 で導入した条件と表 4.2, 表 4.3 より表 4.4 に比較結果を示す。

表 4.4: ケース 1 の比較結果

ステップ		秘密鍵生成	車々間通信	路車間通信
通信可能 時間		3600	14400	3600
処理・通信時間	処理時間(ms)	42.78	124.09	
	通信時間(ms)	5.87	4.568	1.584
	結果(ms)	48.65	128.66	125.67
処理・通信時間／通信可能時間		**1.35%**	**0.89%**	**3.49%**

表 4.4 の結果により、秘密鍵生成のステップと車々間（路車間）認証のステップにおいて、提案方式の処理と通信時間は通信可能時間の 4%以下である。

(2) ケース 2:認証後、公開鍵暗号で暗号通信を行う場合

各処理に Java 言語プログラムを実行し、50 回測定の処理時間の結果は表 4.5 に示す。

表 4.5 ケース 2 の処理時間

ステップ	秘密鍵生成(ms)	認証時間(ms)			
		認証応答	B の認証	A の認証	総時間
最大値	176	239	267	145	628
最小値	141	197	216	108	541
平均	**155.3**	217.56	240.5	121.8	**579.9**

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 4.6 である。

表 4.6: ケース 2 の通信時間

ステップ	秘密鍵生成		車車間通信			路車間通信		
通信方式	DSRC		700MHz帯通信システム					
単位データサイズ	400bytes		100bytes 程度			最大7kbytes 程度		
送受信データ	A	SkA,params	A	B,C1,C2	C3	A	B,C1,C2	C3
サイズ(Bytes)	34	459	34	460	213	34	460	213
時間(ms)	3.26		0.12	1.088	0.6	0.1	0.4	0.2
			1.784			0.76		

4.2.1 で導入した条件と表 4.5, 表 4.6 より表 4.7 に比較結果を示す。

表 4.7: ケース 2 の比較結果

ステップ		秘密鍵生成	車々間通信	路車間通信
通信可能 時間		3600	14400	3600
処理・通信時間	処理時間(ms)	155.3	579.9	
	通信時間(ms)	3.26	1.79	0.76
	結果(ms)	158.56	581.69	580.66
処理・通信時間／通信可能時間		4.40%	4.04%	16.13%

表 4.4 の結果により、秘密鍵生成のステップと車々間（路車間）認証のステップにおいて、提案方式の処理と通信時間は通信可能時間の 17%以下である。

(3) 考察

表 4.4 と表 4.7 の結果により、以下のように考えられる。

1. 秘密鍵生成

処理時間と通信時間は通信可能時間に比べ、ケース 1 とケース 2 のそれぞれの結果は 1.35% と 4.4% である。また、その後、車と鍵発行センター(KGC) との通信を行わないため、この結果から提案方式を適用できる。

2. 車々間通信

認証時間は通信可能時間の約 1%(ケース 1）や 4.04%(ケース 2) である。残り 95%の時間に、十分に暗号通信を行うことができる。

3. 路車間通信

認証時間は通信可能時間に比べ、ケース 1 では 3.49%であり、残り 96% の時間に、十分に暗号通信を行うことができる。ケース 2 の結果は 16.13% であり、時間条件を満たすが、ケース 1 の結果の 5 倍になってしまう。しかし、路車間通信のデータサイズは 7KBytes 程度であるため、残り 80% の時間に、十分な通信量を暗号で転送できる。

以上の考察から、高速道路において ID ベース暗号を用いる車々間（路車間) 認証方式を適用することが可能である。

5. まとめ

本稿では、ID ベース暗号を用いて、高速道路における車々間(路車間) 通信システムの認証方式を提案し、評価を行った。

まず、この提案方式で、機器同士はお互いに正当性を確認でき、機能条件を満たす。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一回しか使えないことで、安全性が高まる。

次に、通信可能時間の理論値を算出し、プログラムの実行時間で処理時間を測定した。また、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（路車間) 認証のステップにおいて、提案方式の処理と通信時間は通信可能時間の 17%以下である。このことから、高速道路において ID ベース暗号を用いる車々間（路車間)認証方式を適用することが可能である。

謝辞

本研究の一部は、平成 25 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] 「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] 境・大岸・笠原：“ Cryptosystems Based on Pairing, ” 暗号と情報セキュリティシンポジウム予稿集, 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] 車載器管理番号確認方 http://www.orse.or.jp/use2/service04.html
[10] 「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
[11] 「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
[12] 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
[13] PBC Library http://crypto.stanford.edu/pbc/
[14] 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.
[15] 山口 英, 鈴木 裕信 (編), 『情報セキュリティ』, 共立出版, 2000.
[16] Java-pairing http://code.google.com/p/java-pairing/