情報処理学会論文誌 Vol.55 No.1 470–483 (Jan. 2014)

online/offline相互認証方式を用いた路車間通信システム

安藤 英里子[1,a)] 佐藤 尚宜[1] 福澤 寧子[1]

受付日 2013年3月30日, 採録日 2013年10月9日

概要：路車間通信を用いたサービスは今後ますます広がっていくと期待される．路側機がユーザのリクエストに応じた情報を高速移動する車両に提供するサービスでは，相互認証および通信路の保護が不可欠となる．しかしながら，車両は高速に走行するため路車間の通信時間は短いうえ，低リソースの車載器では処理が遅いため認証処理時間がかかり，路側機との通信時間内に相互認証およびサービスが完了しない可能性がある．そこで，車載器の認証処理の高速化を図るために，認証処理の大部分を事前計算することでonline時の処理時間の軽減を図るonline/offline相互認証方式を提案し，路側機と通信可能な時間内に認証およびサービスが完了することを確認し，提案方式の有効性を評価した．

キーワード：路車間通信，相互認証，online/offline，セキュリティ

Car-to-Infrastructure Communication Systems by Using Online/offline Authentication Protocol

Eriko Ando[1,a)] Hisayoshi Sato[1] Yasuko Fukuzawa[1]

Received: March 30, 2013, Accepted: October 9, 2013

Abstract: It is expected that the service using car-to-infrastructure communication will be more common in the future. Mutual authentication and secure communication is necessary to use service which provides information appropriate to user's request. Communication time between car and road-side unit (RSU) is short because speed of cars is high. Moreover, authentication takes time because on-board unit (OBU) on car is low-performance. There is a possibility that mutual authentication and service are not completed within communication time between RSU and OBU. Therefore, we propose online/offline authentication protocol to improve authentication time on OBU. Authentication processing time on OBU when OBU can communicate with RSU is short because most part of authentication processing on OBU is completed in advance. We apply online/offline authentication protocol to car-to-infrastructure communication systems and evaluate it.

Keywords: car-to-infrastructure communication, authentication, online/offline, security

1. はじめに

ETC[*1]（Electronic Toll Collection System）による高速道路での自動料金収受やVICS[*2]（Vehicle Information and Communication System）による道路交通情報の配信など路車間通信を用いたシステムは，我々の生活に欠かせない社会基盤となっている．ITS（Intelligent Transport Systems）スポットサービスでは，ETCで用いる狭域無線通信DSRC（Dedicated Short Range Communication）を活用して低速移動する車両だけでなく，高速移動する車両への情報提供などの応用サービスが期待されている[1]．

応用サービスの提供には，セキュリティが重要である．たとえば，ユーザのリクエストに応じて近隣情報を配信する場合，プライバシ保護のために，ユーザのリクエスト内容や近隣情報の暗号化などの通信路の保護が必要である．また，正規ユーザ（サービス加入申込を正当に行ったユー

[1] 株式会社日立製作所横浜研究所
Hitachi Ltd., Yokohama Research Laboratory, Yokohama, Kanagawa 244–0817, Japan
[a)] eriko.ando.yf@hitachi.com

[*1] ETCは，一般財団法人道路システム高度化推進機構の登録商標です．
[*2] VICSは，一般財団法人道路交通情報通信システムセンターの登録商標です．

ザ）だけがサービスを利用できるように，サービス提供者はユーザを認証する必要がある．同様に，正規ユーザもフィッシングによるクレジットカード情報流出などの被害に合わないために，サービス提供者を認証する必要がある．したがって，サービス提供者（路側機）とユーザ（車載器）間での相互認証と通信路の保護は必要不可欠となる．

路車間通信のセキュリティ規格の 1 つに IEEE 1609.2 があり [2]，署名によるメッセージの認証と共通鍵によるメッセージの暗号化が規定しているが，相互認証の仕組みは規定されていない．共通鍵暗号技術を用いた路車間認証方式もあるが [3]，MAC（Message Authentication Code）によるメッセージ認証であり，相互認証の仕組みではない．

無線通信向けには共通鍵暗号技術を用いた相互認証方式がある [4]．共通鍵暗号は公開鍵暗号よりも処理が高速であるが，秘密情報である共通鍵を各サービス提供者と車載器間で共有しなければならないため，ユーザが利用するサービス数が多くなるほど秘密情報が増加し，安全に管理するためのコストが増加する．

一方，公開鍵暗号技術を用いた認証方式としては，無線 LAN（Local Area Network）における機器認証や通信路の保護の仕組みを規定している IEEE 802.11i [5] がある．機器認証の方式は複数存在し，片方または相互に公開鍵暗号技術を用いる認証が広く利用されているが，公開鍵暗号技術を用いた認証処理は時間がかかり，高速に移動する車載器の認証には適さない．

そこで本論文では，共通鍵暗号技術と比較して鍵管理が容易な公開鍵暗号技術を用いて高速に移動する車載器と路側機との間の相互認証方式を提案する [6]．具体的には，車載器の相互認証にかかる全処理量は変わらないが，路側機と通信する前（offline 時）に可能な限り事前処理しておくことで，路側機との通信が発生したとき（online 時）の車載器の処理量軽減を図る online/offline 相互認証方式を提案する．

本論文では，認証に使う鍵などのセキュリティ情報の発行/設定，更新，破棄までのライフサイクルに従って，online/offline 相互認証方式を適用した路車間通信システムを提案し，online/offline 相互認証方式の安全性および実測値に基づく処理時間を評価し，車載機の online 時の処理時間を 99%以上削減し，性能要件である認証と暗号化のための通信鍵の共有が 18.28 ms 以下で完了することを示す．

以下，2 章で研究対象とする路車間通信システムおよびセキュリティの必要性，3 章でセキュリティ要件および性能要件，4 章で online/offline 相互認証方式を述べ，5 章で本方式を適用した場合の路車間通信システムを述べる．6 章で本方式の有効性を評価し，7 章で本論文をまとめる．

2. 路車間通信システム

2.1 概要

本論文で対象とする路車間通信システムを**図 1** に示す．路車間通信システムは車載器，路側機，サービスサーバで構成される．路車間は無線通信，路側機とサービスサーバ間は無線または有線で通信する．路側機は，路側機単体で設置される，もしくは信号機や電光掲示板などと一体化された形で設置される．

一般的な路車間通信システムでは，**表 1** に示すように，安全運転支援，交通の効率化のためのサービス提供やその他応用サービスが想定されている [7], [8]．安全運転支援や交通の効率化のためのサービスでは，サービスサーバや路側機が保有する情報を車載器にブロードキャストする 1 方向通信である．一方，その他応用サービスは，サービスサーバまたは路側機が車載器と双方向に通信し，車載器のリクエストに応じた情報を提供する．本論文では，その他応用サービスの中でも，車載器が高速に移動しながら路側機またはサービスサーバと双方向に通信するサービスを対象とする．

2.2 相互認証の必要性

2.1 節で述べた本論文で対象とするサービスを実現する場合に，路車間通信で発生しうる攻撃とその影響を，脅威ごとに洗い出した結果を**表 2**，**表 3**，**表 4** に示す．ただし，機器（車載器，路側機，サービスサーバ）への物理的攻撃や電波妨害などの物理層への攻撃は対象外とする．

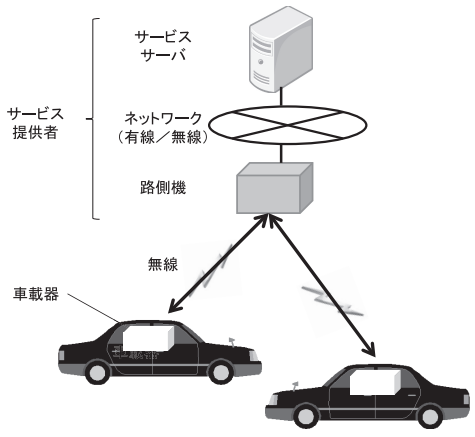

図 1 路車間通信システム
Fig. 1 Car to infrastructure communication system.

表 1 サービス例
Table 1 Examples of services.

カテゴリ	通信タイプ	サービス例
安全運転支援	1 方向通信	制限速度，信号情報などの通知
交通の効率化	1 方向通信	交通渋滞，工事箇所などの通知
その他 応用サービス	双方向通信	有料道路の課金，近隣情報の通知， 駐車場へのアクセス管理， 保険サービス，推薦経路の通知

表 2 機密性の侵害
Table 2 Attacks on confidentiality.

攻撃対象サービス	攻撃方法	影響
推薦経路の通知	車載器の推薦経路を盗聴し，追跡する	プライバシの侵害につながる
有料道路の課金	料金所通過時に流れるクレジットカード情報を盗聴する	クレジットカード情報が漏洩し，悪用される

表 3 完全性の侵害
Table 3 Attacks on integrity.

攻撃対象サービス	攻撃方法	影響
有料道路の課金，駐車場へのアクセス管理	車載器になりすまし，有料道路や関係者以外利用禁止の駐車場を利用する	正しい課金ができない
		関係者以外の車が駐車され，関係者車両のスペースがなくなる

表 4 可用性の侵害
Table 4 Attacks on availability.

攻撃対象サービス	攻撃方法	影響
全てのサービス	同じ情報を繰返し送り，帯域を圧迫させる	サービス品質が低下し，利用者が減る
	ウィルスを送り，機器を壊す	機器を再び購入しなければならない

安全運転支援や交通の効率化のためのサービスで通知する情報は公共的な情報であり，ブロードキャストされるため，完全性と可用性が必要であるが，機密性は必ずしも必要でない．特に完全性が侵害された場合は，偽情報に従って，車載器がドライバに注意喚起するため，影響が大きい．一方，その他応用サービスでは，ユーザの走行場所などプライバシに関わる情報やクレジットカード情報などを通信するため，機密性も必要となる．

機密性の確保にはメッセージの暗号化が有効である．完全性の確保にはメッセージ認証や機器認証が有効である．安全運転支援や交通の効率化のためのサービスでは，サービス提供者が一方的にメッセージを送るため，サービス提供者の認証が必要となる一方，その他応用サービスでは，サービス提供者と車載器との間で双方向に通信するため，相互認証が必要となる．可用性の確保にはメッセージへのシーケンス付与やウィルス検知ソフトの導入などがある．

路車/車車間通信のセキュリティ規格に IEEE 1609.2 があり [2]，署名を用いたメッセージ認証と共通鍵暗号技術を用いた暗号化が規定されているが，相互認証は規定されていない．そこで，本論文は路車間通信向けの相互認証の仕組みについて考察し，online/offline 相互認証方式を適用した路車間通信システムを提案する．

2.3 路車間通信における相互認証の課題

無線通信における機器の相互認証プロトコルの 1 つに，無線 LAN で用いられている IEEE 802.11i がある [5]．端末が無線 LAN で通信する際には，初めにアクセスポイント経由で Radius（Remote Authentication Dial In User Service）サーバなどの認証サーバと認証する．認証は複

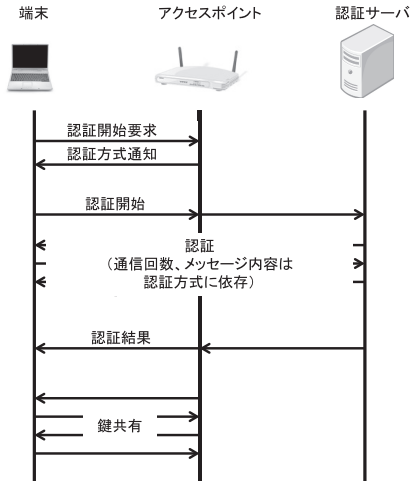

図 2 無線 LAN の認証
Fig. 2 Wireless LAN authentication.

数の方式が利用可能であり，通信回数およびメッセージ内容は認証方式に依存する．認証に成功した後に，アクセスポイントと端末との間で暗号化通信に用いる鍵を共有する（**図 2**）．この方式ではアクセスポイント/認証サーバと車載器間で多数の通信が発生し，認証および鍵共有に時間がかかる．たとえば，EAP（Extensible Authentication Protocol)-TLS（Transport Layer Security）方式による認証方式の場合，端末とアクセスポイント/認証サーバ間で，認証と鍵共有で合計 14 回の通信が発生する．

また，IEEE 802.11i での認証には複数の方式があり，端末が検証済みの公開鍵を用いてサーバを認証する，公開鍵を用いる一般的な認証方式は処理に時間がかかるため，高速に処理するためには，高性能なリソースが必要となる．しかし，端末（路車間認証の場合は車載器）は，低価格で提供することが望まれるため，高性能なリソースを利用できず，処理に時間がかかる．

相互認証に共通鍵暗号技術を用いる方法もある．共通鍵暗号技術を用いた相互認証プロトコル MISP [9], [10] は車載器への適用も検討されている [11]．共通鍵の処理は公開鍵よりも高速であるが，認証する機器間で事前に共通鍵を共有する必要がある．路側機と車載器間で相互認証を行う場合，車載器はユーザが利用するすべてのサービスの共通鍵を保有しなければならない．共通鍵は車載器とサービス提供者以外に漏洩してはならない秘密情報であるため，ユーザが利用するサービスの数に応じて秘密情報を安全に管理するためのコストが増加する．公開鍵暗号技術の場合，車載器が管理すべき秘密情報は車載器の公開鍵ペアの秘密鍵のみであり，加入サービスの数に依存しない．

そこで本論文では，車載器が管理すべき秘密情報の数の観点から公開鍵暗号技術を用いた相互認証の仕組みを対象とし，車載器の処理負荷軽減を図る方式を提案する．

表 5 性能要件算出のための前提条件
Table 5 Preconditions for computing the requirement.

項目		前提条件
通信	走行速度	100km/h
	通信領域	20m
	同時接続台数	4 台
	伝送速度	4096kbps
	1 スロット データ容量	400byte [内訳] サービス：183byte，制御：217byte
	1 フレーム 利用可能 スロット数	最大 9 スロット [内訳] ブロードキャスト：1 スロット(必須) 制御 ：1 スロット(必須) ユニキャスト ：7 スロット以下
サービス	リクエストデータ	3.7kbyte
	サービスデータ	25kbyte

3. セキュリティ要件および性能要件

本論文で対象とする路車間通信システムの前提条件，セキュリティに関する機能要件および性能要件を述べる．

(1) 前提条件

車載器は一般ユーザが購入する安価な低リソース機器である．一方，路側機はサービス提供者が購入するため，高リソース機器である．また，路車間通信以外の通信路は保護されているものとする．

(2) セキュリティ要件

- 路側機と車載器が互いの真正性を確認できること
- 認証や通信路の保護のために新たに発生する鍵などのセキュリティ情報の安全性を確保すること

(3) 性能要件

路車間通信に用いられる DSRC では 1 台の路側機と車載器が通信可能な領域が数十 m と短い．車載器と路側機がつねに通信するには多数の路側機が必要だが，コストがかかるため，路側機が車載器とつねに通信可能な状態になるのは難しい．したがって，車載器は 1 台の路側機と通信可能な時間内に，相互認証とサービスが完了させなければならない．文献 [8], [12], [13], [14] で規定されている数値を参考に，**表 5** に示す値から性能要件を算出する．時速 100 km/h の車載器が 20 m 進むのにかかる時間は 720 ms であり，1 台の路側機は最大 4 台の車載器と同時に通信するため，1 台の車載器が路側機と通信するのに割り当てられる時間は 180 ms になる．サービスは車載器が路側機経由でサービスサーバにリクエストを送り，リクエストに対応するデータ（サービスデータ）を受信する．1 フレームのうち，特定の相手へデータを送るユニキャストに利用できるスロットは 7 スロット以下であり，1 スロットがサービスに利用できるデータ量は 183 byte とする．本論文では，国土交通省国土技術政策総合研究所が次世代道路サービス提供システムに関する検討 [8] で想定しているサービスデータ量を用いて相互認証に割り当てられる時間を算出する．リクエストデータが 3.7 kbyte，サービスデータが 25 kbyte の場合，データ送信に必要なフレームはそれぞれ 3 フレーム，20 フレームである．伝送速度は 4096 kbps なので，データ送受信時間の合計は 161.72 ms（リクエスト 21.09 ms，サービスデータ 140.63 ms）である．したがって，18.28 ms 以下で相互認証，リクエストおよびサービスデータの暗号化に使う通信鍵の共有を完了する必要がある．

4. 路車間通信向け online/offline 相互認証方式の提案

4.1 高速化の基本方針

署名生成の高速化を図る方式として，online/offline 署名方式 [15] がある．この方式では，署名生成に必要な処理のうち，事前計算可能な処理を offline 時（通信が発生する前）に処理しておくことで，署名生成全体の処理量は変わらないが，online（通信発生）時の処理時間を短縮できる．本論文では，online/offline 署名方式の考え方をもとに，相互認証の高速化，すなわち，online 時の認証処理の軽減を図る．以下に高速化の基本方針を述べる．

(1) 車載器の相互認証処理の効率化

公開鍵を用いた相互認証を行う場合，車載器は低リソース，路側機は高リソースという前提条件より，車載器の処理時間が特に課題になり，路側機がある程度の処理を負担しても認証時間への影響は少ない．そこで，車載器の認証処理の効率化を図る．

(2) 署名方式と暗号方式の組合せ

機能要件より相互認証が必要である．公開鍵暗号技術を用いた相互認証には，署名を用いる方式と暗号化を用いる方式がある．署名方式では，認証者は被認証者から受信した署名の検証に成功した場合，被認証者を認証したことになる．署名は，認証者が送った乱数の署名である．暗号化方式では，認証者が乱数と暗号化した乱数を被認証者に送り，被認証者からの復号結果と乱数が一致した場合，被認証者を認証したことになる．相互認証の場合，相互に上記処理を行うため，相互認証する二者は，署名方式の場合は署名生成処理と検証処理，暗号化方式の場合は暗号化処理と復号処理がそれぞれ 1 回ずつ発生する．

署名を用いた相互認証に online/offline 署名方式を適用する場合，online/offline 署名方式は署名生成処理の一部は事前計算できるが，署名検証処理は事前計算できないため，車載器における署名生成処理時間は短縮できるが，署名検証処理時間は短縮できない．

そこで，online/offline 署名方式の考え方を ElGamal 型暗号方式の暗号化処理に適用する．車載器においては，被認証のための署名生成処理と暗号化処理を行い，路側機においては車載器認証のための署名検証処理と被認証のための復号処理が発生するように online/offline 署名方式と

表 6 略号
Table 6 Abbrevations.

略号	定義
data1 | data2	*data1* と *data2* を連結する
Enc (key, data)	鍵 *key* でデータ *data* を暗号化する
Dec (key, data)	鍵 *key* でデータ *data* を復号する
Sig (key, data)	鍵 *key* でデータ *data* の署名を生成する
Ver (key, sign, data)	鍵 *key* でデータ *data* の署名 *sign* を検証する
Mac(key, data)	鍵 *key* でデータ *data* の MAC(Message Authentication Code)を生成する

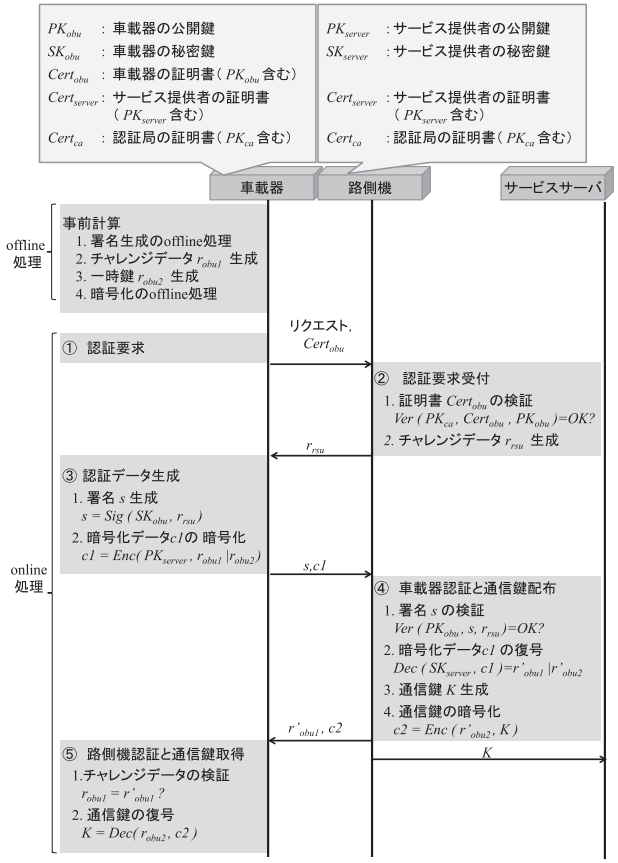

図 3 online/offline 相互認証方式
Fig. 3 Online/offline authentication.

online/offline 暗号方式を組合せ，車載器の認証処理の効率化を図る．

(3) 通信回数および通信時間の削減

通信回数が増加すると，通信による遅延時間も増える．その結果，認証や暗号化通信するための通信鍵の共有にかかる時間が長くなる．そこで，通信回数を少なくするために，認証と通信鍵の共有を同じフェーズで行う．

4.2 online/offline 相互認証処理

以降，本論文で利用する略号を**表 6** に，提案する online/offline 相互認証方式を**図 3** に示す．本方式では，車載器の認証に online/offline 署名方式，路側機の認証に online/offline 暗号方式を用いる．

路側機にはサービス提供者の公開鍵ペア（秘密鍵 SK_{server} と公開鍵 PK_{server}），公開鍵証明書（以下，証明書 $Cert_{server}$）および認証局の証明書（$Cert_{ca}$）が設定される．車載器には車載器の公開鍵ペア（秘密鍵 SK_{obu} と公開鍵 PK_{obu}）と証明書（$Cert_{obu}$），サービス提供者の証明書（$Cert_{server}$）が設定される．各証明書には有効期間，証明書の発行者，署名アルゴリズム，シリアル番号などの情報および公開鍵の情報が含まれる．

車載器は，offline 処理として，車載器の秘密鍵（SK_{obu}）とサービス提供者の公開鍵（PK_{server}）を用いて，署名生成と暗号化の中で事前計算が可能な処理を実施する．また，車載器が路側機を認証するためのチャレンジデータ（乱数 r_{obu1}）と通信鍵（K）を配布してもらうための一時鍵（乱数 r_{obu2}）も生成し，メモリに保持しておく．通信鍵（K）と一時鍵（r_{obu2}）は共通鍵であり，本論文では共通鍵暗号は国際標準である AES（Advanced Encryption Standard）を用いる．

事前計算が可能な offline 処理の詳細は 4.3 節で述べる．以下，online 処理を述べる．

① 認証要求

車載器は，車載器の証明書（$Cert_{obu}$）とともに認証要求を路側機に送る．

② 認証要求の受付

路側機は，車載器の証明書（$Cert_{obu}$）を認証局の公開鍵（PK_{ca}）で検証したのち，車載器を認証するためのチャレンジデータとして乱数（r_{rsu}）を生成し，車載器に送信する．

③ 認証データ生成

車載器は，車載器の秘密鍵（SK_{obu}）を用いてチャレンジデータ（r_{rsu}）の署名（s）を生成する．このとき，offline 処理結果を用いるため，処理時間を短縮できる．詳細は 4.3.1 項で述べる．

次に，車載器は offline 処理で生成したチャレンジデータ（r_{obu1}）と一時鍵（r_{obu2}）を結合し，サービス提供者の公開鍵（PK_{server}）で暗号化する．暗号化は offline 処理結果を用いるため，処理時間を短縮できる．詳細は 4.3.2 項で述べる．車載器は，チャレンジデータ（r_{rsu}）の署名（s），チャレンジデータ（r_{obu1}）と一時鍵（r_{obu2}）の暗号化データ（$c1$）を路側機に送る．

④ 車載器認証と通信鍵配布

路側機は，認証要求時に受信した証明書（$Cert_{obu}$）から取り出した公開鍵（PK_{obu}）と乱数（r_{rsu}）を用いて署名（s）を検証する．検証成功の場合は，正しい公開鍵ペアを保持する車載器であることを認証したことになる．検証失敗の場合は，路側機は車載機に認証失敗のメッセージを送り，認証処理を終了する．

次に，路側機はサービス提供者の秘密鍵（SK_{server}）を用いて暗号文（$c1$）を復号し，r'_{obu1} を得る．また，通信路を保護するための通信鍵（K）を生成し，復号した一時鍵（r'_{obu2}）で暗号化する．そして，暗号化した通信鍵（$c2$）と復号した乱数（r'_{obu1}）を車載器に送るとともに，通信鍵（K）は必要に応じてサービスサーバにも送る．

⑤　路側機認証と通信鍵取得

車載器は，路側機が復号した値（r'_{obu1}）と車載器が生成したチャレンジデータ（r_{obu1}）が等しいことを確認する．等しい場合は，正しい公開鍵ペアを保持する路側機，すなわちサーバ提供者を確認したことになる．等しくない場合は，車載器は路側機に認証失敗のメッセージを送り，認証処理を終了する．

次に，車載器は暗号化された通信鍵を一時鍵（r_{obu2}）で復号する．路側機と車載器との相互認証が完了するとともに通信鍵（K）の共有も完了する．

① から ⑤ で示す認証処理の中で，以下に示す状況が発生する場合は，認証に失敗したとして，認証処理を終了する．

- 車載器が ① または ③ の処理の後，路側機にデータを送信したが，一定時間内に路側機から応答がない場合
- 路側機が ② の処理の後，車載器にデータを送信したが，一定時間内に車載器から応答がない場合

また，車載器または路側機が送信したデータに対応しないデータを受信した場合は認証失敗のメッセージを送り，処理を終了する．

4.3 online/offline 処理

4.3.1 online/offline 署名方式

4.2 節で述べた online/offline 相互認証処理において，車載機の認証に利用した online/offline 署名方式を詳述する．

online/offline 署名方式に米国標準である ECDSA（Elliptic Curve Digital Signature Algorithm）[16] を用いる．ECDSA を用いた場合の署名生成処理を**図 4**，検証処理を**図 5**，図中の記号を**表 7** に示す．

署名生成は図 3 の ③-1 のチャレンジデータ（r_{rsu}）の署名（s）生成に用いる．このとき，入力に関係なく計算可能な処理（図 4 の (1)〜(4)）は offline で処理する．したがって，乱数生成 1 回，スカラー倍算 1 回，剰余算 1 回，剰余逆元演算 1 回の処理時間を短縮でき，online 時の処理（図 4 の (5)，(6)）はハッシュ処理 1 回，剰余加算 1 回と剰余乗算 2 回となる．スカラー倍算（バイナリ法）1 回の処理コストは 4,096 回の剰余乗算コストと同等であるため [6]，online 時の処理時間の短縮効果は大きい．

署名検証は図 3 の ②-1 の証明書（$Cert_{obu}$）検証と ④-1 の署名（s）検証に用いる．署名検証処理は入力に関係なく計算できる処理がないため，すべて online 処理になる．図 5 は署名（s）検証を示し，チャレンジデータ（r_{rsu}）の署名（s）を車載機の公開鍵（PK_{obu}）で検証する．車載機の証明書（$Cert_{obu}$）検証の場合，証明書に含まれる車載機の公開鍵（PK_{obu}）の署名を認証局の公開鍵（PK_{ca}）で検証する．署名値は証明書（$Cert_{obu}$）に含まれている．

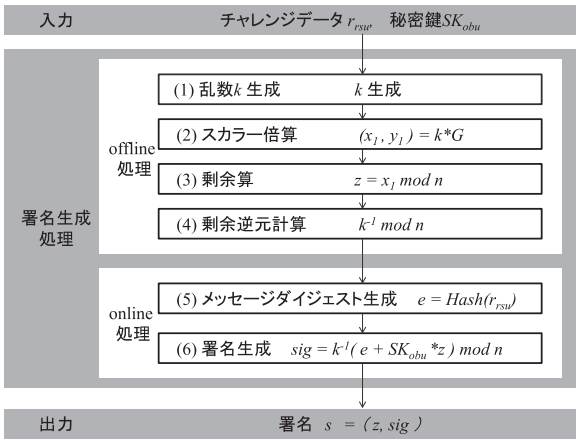

図 4　ECDSA による署名生成処理
Fig. 4　Signing on ECDSA.

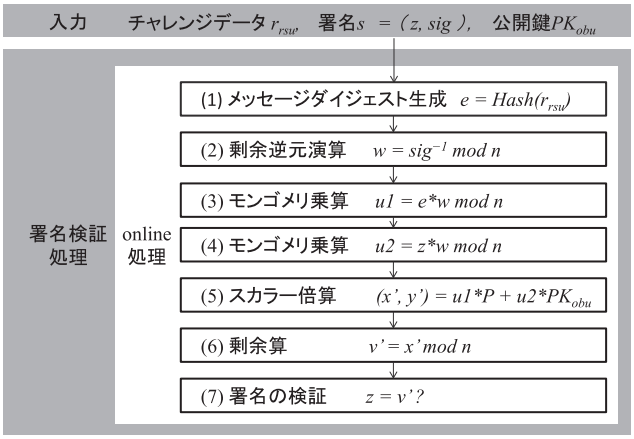

図 5　ECDSA による署名検証処理
Fig. 5　Verification on ECDSA.

表 7　記号
Table 7　Open parameters and keys.

項目	記号	説明
公開パラメータ	P	素数
	a,b	F_p 上の楕円曲線 $E: Y^2 = X^3 + aX + b$
	G	E 上の点（ベースポイント）
	N	P の位数
秘密鍵	SK_{obu}, SK_{server}	n-1 以下の自然数
公開鍵	PK_{obu}, PK_{server}	$d_A P$（E 上の点）
ハッシュ関数	$Hash(data)$	$data$ のハッシュ値を生成する
乗算	$data1*data2$	$data1$ と $data2$ を乗算する

4.3.2 online/offline 暗号方式

4.2 節で述べた online/offline 相互認証処理において，路側機の認証に利用した online/offline 暗号方式を詳述する．

online/offline 暗号方式に国際標準である ECIES-KEM [17] を用いる．ECIES-KEM を用いた場合の暗号

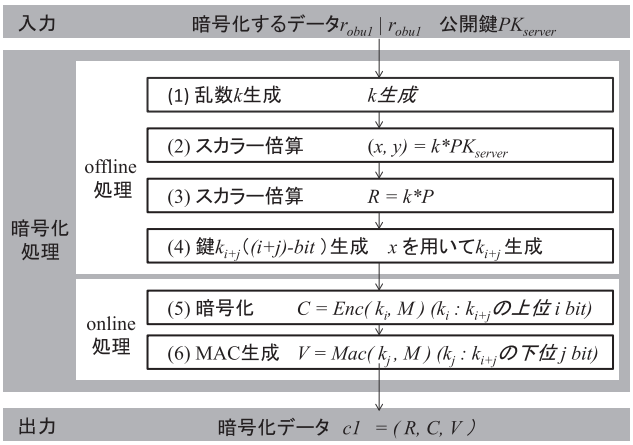

図 6 ECIES-KEM による暗号化処理
Fig. 6 Encryption on ECIES-KEM.

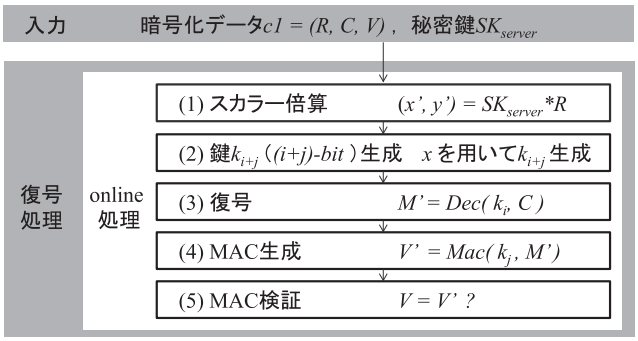

図 7 ECIES-KEM による復号処理
Fig. 7 Decription on ECIES-KEM.

化処理を**図 6**，復号処理を**図 7** に示す．図中の記号は表 7 と同じである．

暗号化は図 3 の ③-2 のチャレンジデータ（r_{obu1}）と一時鍵（r_{obu2}）の暗号化に用いる．このとき，入力に関係なく計算可能な処理（図 6 の (1)〜(4)）は offline 処理する．したがって，乱数生成 1 回，スカラー倍算 2 回，鍵生成処理 1 回の処理時間を短縮できる．online 処理は暗号化と MAC 生成処理（図 6 の (5)，(6)）であり，これらは共通鍵暗号を用いることで高速に処理できる．

復号処理は，図 3 の ④-2 の認証データ（$c1$）の復号で用いる．復号処理は入力に関係なく計算できる処理がないため，すべて online 処理になる（図 7）．

5. online/offline 相互認証方式適用の路車間通信システム

4 章で述べた online/offline 相互認証方式を路車間通信システムに適用するためには，公開鍵ペアなどのセキュリティ情報の管理が必要となる．そこで，5.1 節で管理すべきセキュリティ情報の定義，5.2 節でセキュリティ情報を管理するに際し，登場するエンティティ，5.3 節で認証のアーキテクチャを述べ，5.4 節でセキュリティ情報のライフサイクルに従ってセキュリティ情報の管理を提案する．

表 8 セキュリティ情報
Table 8 Security information.

格納場所		セキュリティ情報
車載器	1	車載器の公開鍵ペア（秘密鍵と公開鍵）
	2	車載器の証明書
	3	サービス提供者の証明書
	4	認証局の証明書
路側機	5	サービス提供者の公開鍵ペア（秘密鍵と公開鍵）
	6	サービス提供者の証明書
	7	認証局の公開鍵

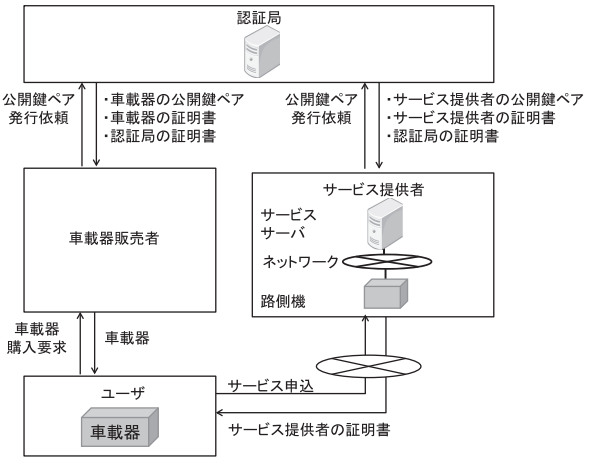

図 8 エンティティ関係モデル
Fig. 8 Entity relationship model.

5.1 セキュリティ情報

online/offline 相互認証に必要なセキュリティ情報を**表 8** に示す．これらのセキュリティ情報は認証局が発行し，online/offline 相互認証が行われる前に各機器に設定する．

5.2 構成

online/offline 相互認証方式を路車間通信システムに適用した場合のエンティティを**図 8** に示す．

(1) 認証局

認証局は，以下の生成/発行を行う．証明書は公開鍵の真正性を証明するものであり，有効期間，証明書の発行者，署名アルゴリズム，シリアル番号などの情報および公開鍵の情報が含まれる．

- 認証局の証明書

認証局自身の証明書であり，認証局が発行した路側機と車載器の証明書検証に用いる．証明書は，路側機および車載器に格納される．

- サービス提供者の公開鍵ペアと証明書

公開鍵ペアと証明書はサービスごとに発行され，車載器にサービス提供者を確認してもらうために用いる．これらはサービスサーバと各路側機に格納される．また，証明書はサービス加入ユーザの車載器にも格納される．

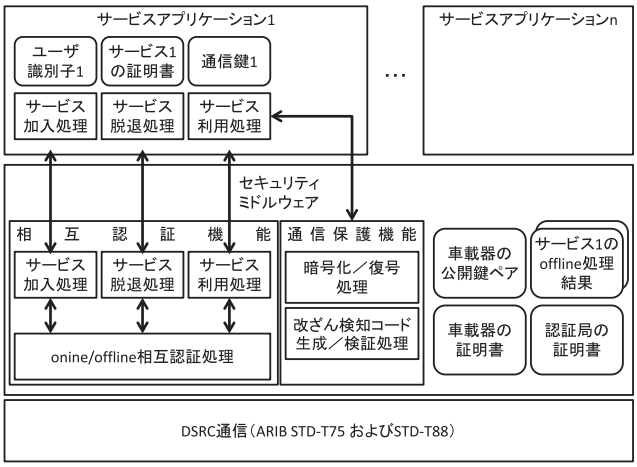

図 9 認証のアーキテクチャ（車載器）
Fig. 9 Authentication architecture (OBU).

● 車載器の公開鍵ペアと証明書

公開鍵ペアと証明書は車載器ごとに発行され，サービス提供者に車載器を確認してもらうために用いられる．これらは車載器に格納される．

(2) 車載器販売者

車載器販売者は車載器を製造/販売する．車載器販売時には，認証局から取得した車載器ごとの公開鍵ペアと証明書を対象の車載器に設定してユーザに渡す．

(3) サービス提供者

サービス提供者は車載器に向けてサービスを提供する．サービスを開始する際には，認証局にサービス提供者の公開鍵ペアを発行してもらい，認証局の公開鍵ペアと証明書を路側機に格納する．公開鍵ペアと証明書はサービス提供者ごとに発行される．つまり，サービス提供者の各路側機には同じ公開鍵ペアと証明書が格納される．

(4) ユーザ

ユーザは車載器の公開鍵ペアと証明書が格納された車載器を購入し，サービスを受ける．サービスはユーザが申し込み，サービス提供者の証明書を取得する．

5.3 認証のアーキテクチャ

本論文で提案するセキュリティ機能は，通信プロトコルとサービスアプリケーションの間のセキュリティミドルウェアとして存在する（**図 9**）．本ミドルウェアは各サービスの加入，利用，脱退のときに，サービスアプリケーションから呼び出される．加入時は，サービス加入処理が online/offline 相互認証処理と連携してサービス提供者と相互認証を行い，ユーザ識別子とサービスの証明書をサービス提供者から取得し，利用時の online/offline 相互認証のための offline 処理を行う．利用時は，サービス利用処理が online/offline 相互認証処理と連携してサービス提供者と online/offline 相互認証を行い，サービス提供者から通信鍵を取得する．そして，通信保護機能が通信鍵を用いてサービス提供者と安全に通信する．脱退時は，サービス脱退処理が online/offline 相互認証処理と連携してサービス提供者と相互認証した後，車載器に保存されているユーザ識別子やサービスの証明書を破棄する．

図 9 は車載器のアーキテクチャを示すが，路側機も同様である．ただし，本論文ではサービス提供者が路側機を管理する前提のため，路側機に搭載されるサービスアプリケーションは 1 つになる．

5.4 セキュリティ情報の管理

(1) 発行/設定

認証局は自身の自己証明書を発行し，保存する．

サービス提供者は，サービス立ち上げ時に公開鍵ペアと証明書の発行を認証局に要求し，認証局の証明書とともに取得する．取得したセキュリティ情報は路側機に設定する．

車載器販売者は，車載器販売時に当該車載器の公開鍵ペアと証明書の発行を認証局に要求し，認証局の証明書とともに取得する．取得したセキュリティ情報は車載器に設定する．車載器に公開鍵ペアが設定されると，署名生成処理の offline 処理が実行され，処理結果をメモリに保存する．

ここで，認証局からサービス提供者や車載器販売者にセキュリティ情報を配布する際や，路側機や車載器にセキュリティ情報を設定する際の機密性や完全性の確保は，本論文の検討対象外とする．また，路側機や車載器に設定されるセキュリティ情報，特に秘密鍵は漏洩防止のため，耐タンパ性のあるメモリに格納するものとする．

ユーザは車載器を購入すると，ネットワークを介してサービスの加入を申し込む．サービスの加入申し込みは車両停止時に行われることを前提とし，処理時間の高速化は本論文の検討対象外とする．車載器のなりすましやフィッシング防止のため，サービスの加入申し込み時も車載器とサービス提供者は互いの真正性を確認する必要がある．認証プログラムの開発コストの観点から 4 章で述べた online/offline 相互認証方式と同様の相互認証を行う．**図 10** に車載器がサービスに加入する際の処理を示し，以下に，図 10 の ①～⑥ の処理内容を述べる．

① サービス加入要求

車載器が路側機にサービス加入リクエストと車載器の証明書（$Cert_{obu}$）を送る．

② サービス加入要求受付

路側機は車載器の証明書（$Cert_{obu}$）が失効していないことを確認し，図 3 の ② と同様に，車載器の証明書検証とチャレンジデータ（乱数：r_{rsu}）の生成を行い，サービス提供者の証明書（$Cert_{server}$）とチャレンジデータ（r_{rsu}）

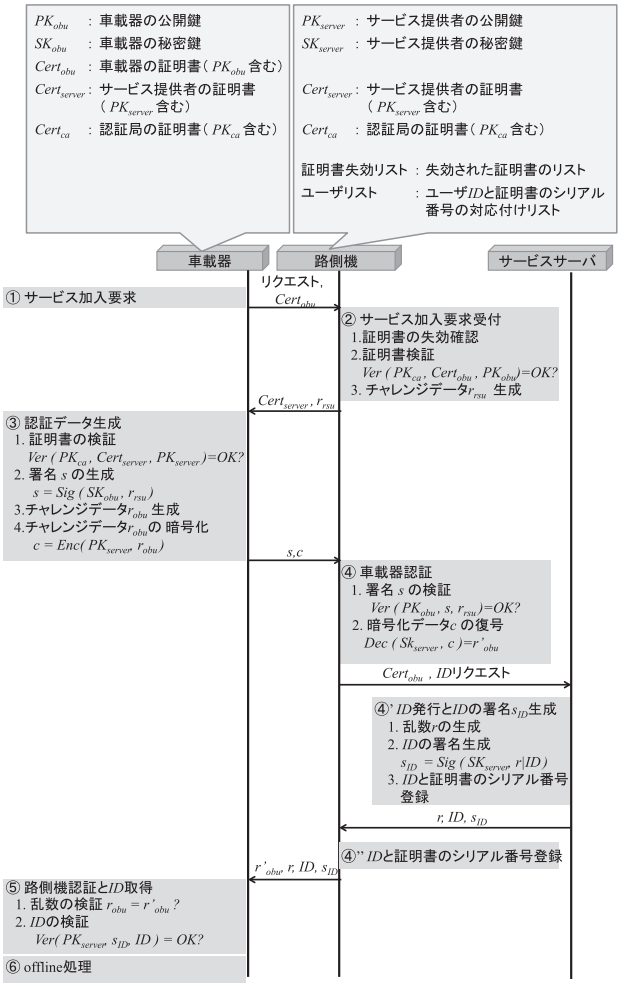

図 10 サービス加入処理
Fig. 10 Service application.

を車載器に送る．車載器の証明書（$Cert_{obu}$）が失効している場合は，路側機はチャレンジデータ（r_{rsu}）を生成せず，車載器に認証失敗のメッセージを送り，認証処理を終了する．

③ 認証データの生成

車載器は認証局の公開鍵（PK_{ca}）でサービス提供者の証明書（$Cert_{server}$）を検証し，署名（s）と，チャレンジデータ（r_{obu}）をサービス提供者の公開鍵で暗号化したデータ（c）生成する．ただし，サービス提供者の公開鍵は事前に入手できていないので，ここでは offline による事前計算ではなく，online で処理する．車載器は署名（s）とチャレンジデータ（r_{obu}）の暗号化データ（c）を路側機に送る．サービス提供者の証明書（$Cert_{server}$）を検証に失敗した場合は，車載器は署名（s）および暗号化データ（c）は生成せず，路側機に認証失敗のメッセージを送り，認証処理を終了する．

④ 車載器認証（④' および ④" 含む）

路側機が署名（s）検証により車載器を確認し，サービスサーバに路側機の証明書（$Cert_{obu}$）とユーザ識別子（ID）の発行リクエストを送るとともに，暗号化データ（c）を復号する．署名（s）検証に失敗した場合は，路側機はただちに車載器に認証失敗のメッセージを送り，認証処理を終了する．

路側機からユーザ識別子（ID）の発行を要求されたサービスサーバは乱数（r），ユーザ識別子（ID）およびユーザ識別子の署名（s_{ID}）を生成し，ユーザ識別子（ID）と車載器の証明書のシリアル番号と紐付けて登録する．そして，路側機に乱数（r），ユーザ識別子（ID）およびユーザ識別子の署名（s_{ID}）を送り，路側機もユーザ識別子（ID）と車載器の証明書のシリアル番号と紐付けて登録する．路側機は，暗号化データ（c）の復号結果（r'_{obu}），ユーザ識別子（ID），乱数（r）および署名（s_{ID}）を車載器に送る．

⑤ 路側機認証と ID 取得

車載器は生成したチャレンジデータ（r_{obu}）と受信した乱数（r'_{obu}）を比較し，路側機を確認する．そして，ユーザ識別子の署名（s_{ID}）を検証した後，ユーザ識別子（ID）を保存する．チャレンジデータ（r_{obu}）と受信した乱数（r'_{obu}）が一致しない場合やユーザ識別子の署名（s_{ID}）検証に失敗した場合，車載器は路側機に認証失敗のメッセージを送り，認証処理を終了する．

⑥ offline 処理

車載器は図 3 に示した offline 処理を実施し，結果を保存する．

また，4.2 節と同様に，一定時間内に応答がない，または送ったデータに対応する応答がない場合は，認証失敗のメッセージを通信相手に送り，認証処理を終了する．

(2) 運用

走行中の車載器が路側機と通信可能になると，(1) で発行/設定されたセキュリティ情報を用いて 4 章で述べた online/offline 相互認証を行い，サービスを受ける（**図 11**）．図 3 の処理との違いを下記に示す．

- 車載器の証明書確認（図 11 ②'）

路側機が車載器の証明書の失効確認およびシリアル番号とユーザ識別子の対応確認を行う．この確認によりサービス脱退後のサービス享受を防ぐ．

- 路側機の証明書の値確認（図 11 ③-0）

車載器は，車載器にあるサービス提供者の証明書と受信した証明書の値を確認する．確認失敗の場合は，車載器は認証失敗のメッセージを路側機に送り，認証処理を終了する．この確認処理と ⑤-1 でのチャレンジデータの確認により，なりすまし路側機でないことを確認する．

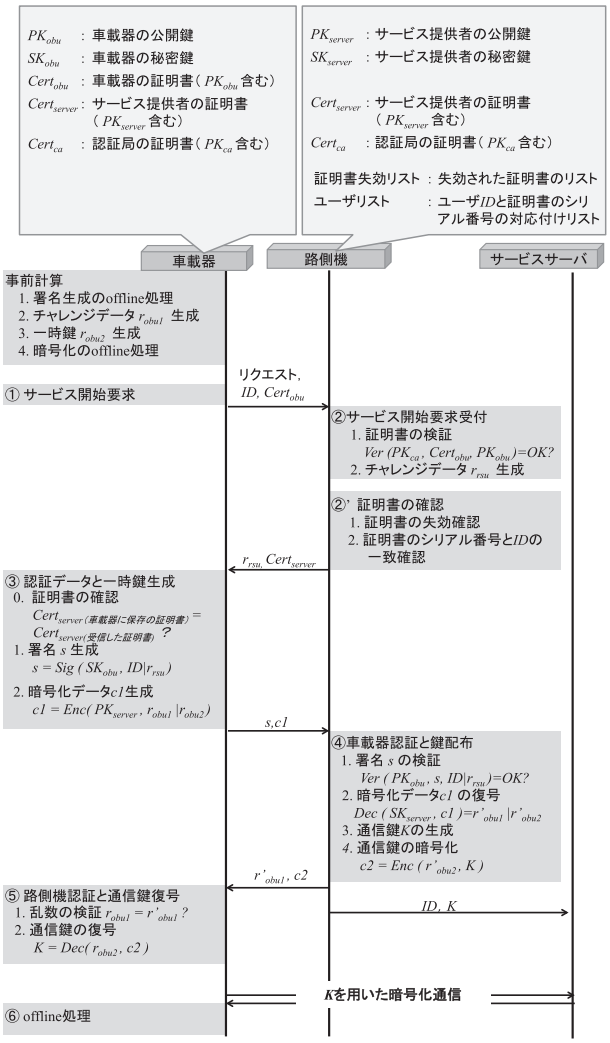

図 11 online/offline 相互認証によるサービス利用時の認証
Fig. 11 Authentication by using online/offline authentication protocol at the time of service use.

● offline 処理（図 11 ⑥）

サービス終了時に，車載器は次のサービス利用のために，図 11 の事前計算を実施し，結果を更新する．

(3) 破棄

ユーザがサービスを脱退する際は，サービス加入時と同様にサービス提供者に脱退要求を送り，相互認証を行う．脱退申し込みも走行停止時に行われることを前提とし，処理時間の高速化は本論文の検討対象外とする．以下にサービス加入時と異なる処理を記す．

● サービス脱退要求受付

サービス利用時と同様に処理（図 11 ② と ②’）する．

● 認証データの生成

サービス利用時と同様に処理（図 11 ③）する．

● 車載器認証

図 10 の ④ を実施し，④’ は実施しない．

● 路側機認証

車載器は生成したチャレンジデータ（r_{obu}）と受信した乱数（r'_{obu}）を確認後，ユーザ識別子（ID）と署名（s_{ID}）を路側機に送り，サービス提供者の証明書（$Cert_{server}$）を削除する．図 10 の ⑥ は実施しない．チャレンジデータ（r_{obu}）と受信した乱数（r'_{obu}）が一致しない場合，車載器は路側機に認証失敗のメッセージを送り，サービス脱退処理を終了する．

● 脱退 ID の検証

路側機が署名（s_{ID}）検証に成功すると，サービスサーバと路側機はユーザ識別子（ID）を削除し，処理が終了する．署名（s_{ID}）検証に失敗した場合，路側機は車載器に認証失敗のメッセージを送り，サービス脱退処理を終了する．

(4) 車載器破棄

車載器を破棄した場合は，ユーザは認証局または車載器販売者などを経由して車載器の公開鍵ペアと証明書を失効し，認証局がサービス提供者に証明書失効リストを配布する．したがって，第 3 者が車載器を盗んでもサービスは受けられない．

6. 評価

6.1 安全性評価

本節では online/offline 相互認証方式の認証プロセスの安全性評価を NIST 800-63-1 [18] にある 7 項目で評価する．ただし，暗号アルゴリズム自体の安全性は保証されているとする．

(1) オンライン上の推測

オンライン上の推測とは，第 3 者が認証に必要な秘密情報の値を推測することである．online/offline 相互認証方式の秘密情報は車載器とサービス提供者の秘密鍵，一時鍵，通信鍵である．

● 秘密鍵

車載器およびサービス提供者の秘密鍵は通信路に現れない．暗号アルゴリズムは安全との仮定から秘密鍵を使って生成された値（署名（s_{obu}）と暗号化データ（$c1$））から秘密鍵が推測されることは困難である（図 11）．

● 一時鍵

一時鍵（r_{obu2}）は路側機の公開鍵（PK_{obu}）で暗号化されて送られる．暗号アルゴリズムは安全との仮定から一時鍵が推測されることは困難である．

● 通信鍵

通信鍵（K）は，一時鍵（r_{obu2}）で暗号化されて送信される．暗号アルゴリズムは安全との仮定から通信鍵が推測されることは困難である．

(2) フィッシング

フィッシングとは第3者が検証者になりすまし，認証要求者をだまして認証要求者の秘密情報を開示させることである．online/offline相互認証方式において，第3者がサービス提供者になりすまし，認証要求受付として，図11のチャレンジデータ（r_{rsu}）を車載器に送ったとしても，図11の④-2で正しく復号することができず，⑤-1の路側機認証に失敗する．

(3) ファーミング攻撃

ファーミング攻撃とは，事前にルータなどの設定が変更され，偽サイトに誘導されてしまう攻撃である．路車間通信システムの場合，路側機の設定が書き換えられ，偽のサービスサーバにつながってしまうことになる．本論文では路側機はサービス提供者によって正しく管理されているものとし，今回の評価対象外とする．

(4) 盗聴

通信路の盗聴は可能であるが，秘密情報である秘密鍵，一時鍵および通信鍵は通信路上に現れない，もしくは暗号化されて通信路を流れるので，盗聴されても秘密情報が漏洩することはない．

(5) リプレイ攻撃

リプレイ攻撃とは，盗聴した情報を用いて第3者が認証してもらうことである．online/offline相互認証方式において，路側機に車載器を認証してもらうための署名（s）は認証時に路側機から送信される乱数をもとに生成されるため，リプレイ攻撃はできない．一方，車載器に路側機を認証してもらうためには，路側機は認証データ（$c1$）を復号してチャレンジデータ（r_{obu1}）を取得し，車載器に送る必要があるが，チャレンジデータ（r_{obu1}）は認証のたびに異なる値を用いるので，リプレイ攻撃できない．

(6) セッションハイジャック

セッションハイジャックとはセッションを管理するセッションIDを盗み，第3者が路側機や車載器になりすますことをいう．通信鍵（K）を取得以降は，通信鍵によるメッセージの暗号化とMAC付与が行われるため，セッションハイジャックはできない．また，中間者攻撃も行えないため（(7)で詳述），相互認証処理中のセッションハイジャックもできない．

(7) 中間者攻撃

中間者攻撃とは路側機と車載器の通信に第3者が割り込み，両者が交換する情報を第3者の情報にすり替えて，秘密情報の盗聴などを行うことである．

第3者が車載器になりすまし，車載器の証明書（$Cert_{obu}$），署名（s），暗号化データ（$c1$）をすり替えても路側機の処理で失敗する．具体的には，第3者が車載器の証明書（$Cert_{obu}$）の代わりに第3者の証明書を路側機に送付した場合，路側機での証明書のシリアル番号とユーザ識別子（ID）の対応がとれず（図11 ②'），認証に失敗する．第3者が署名（s）の代わりに第3者の秘密鍵で生成した署名を路側機に送付した場合，路側機は車載器の公開鍵（PK_{obu}）で署名検証するため（図11 ④），署名検証に失敗する．第3者が暗号化データ（$c1$）をすり替えた場合，路側機は暗号化データ（$c1$）を復号したr'_{rsu2}で通信鍵（K）を暗号化するため，第3者は通信鍵（K）を取得できないため認証に失敗したことと同等になる．

また，第3者がサービス提供者になりすまし，チャレンジデータ（r_{rsu}）または暗号化された通信鍵（$c2$）をすり替えても，第3者は車載器が生成した一時鍵（r_{obu2}）を取得できず，車載器と同じ通信鍵を共有することができないため，認証に失敗したことと同等になる．したがって，中間者攻撃はできない．

上記のように各項目を満たすため，online/offline相互認証方式は安全であるといえる．

次に，車載器/路側機からの情報漏洩について述べる．秘密情報のうち，一時鍵と通信鍵は，車載器/路側機が保持する時間が短いため，車載器/路側機から情報が漏洩する可能性は非常に低い．また，有効期間も短いため，情報が漏洩した場合でも影響は非常に小さい．

一方，秘密鍵は車載器/路側機に長期間保存される．5.4節(1)で述べたとおり，秘密鍵は耐タンパ性のあるメモリに保存するため，車載器/路側機から漏洩する可能性は低い．

仮に，車載器から秘密鍵が漏洩した場合は，認証局が該当車載器の公開鍵証明書を失効し，サービス提供者に証明書失効リストを配布することで漏洩した秘密鍵の悪用を防止する．路側機から秘密鍵が漏洩した場合は，該当サービスを受けるすべての車載器にサービスを利用しないよう通知し，新しい公開鍵を配布する必要がある．しかしながら，本論文では路側機はサービス提供者が適切に管理することを前提としており，発生可能性は低いとする．

6.2 性能要件

online/offline相互認証方式が3章で述べた性能要件である相互認証と暗号化のための通信鍵の共有が18.28 ms以下で完了することを確認するために処理時間を評価する．

6.2.1 前提条件

処理時間は路側機および車載器の性能，利用するアルゴリズムなどに依存する．本論文では，**表9**に示す条件で処理時間を評価する．車載のCPUは，車車間/路車間通信の情報セキュリティ基盤機能を検討する欧州の研究プロジェクトEVITA（E-Safety Vehicle Intrusion Protected Applications）で検討している値を参考とする[19]．路側機

表 9 性能評価の前提条件
Table 9 Preconditions for performance evaluations.

項目		前提条件
機器性能	車載器 CPU	50～250MHz
	路側機 CPU	2.4GHz
アルゴリズム	online/offline 署名	ECDSA
	online/offline 暗号	ECIES-KEM 暗号化：AES MAC：HMAC
	ハッシュ関数	SHA-256
	通信鍵の暗号化	AES
データ長	証明書	129byte
	チャレンジデータ	128bit
	ECDSA 鍵長	256bit
	一時鍵	128bit
	通信鍵	128bit

表 10 基本処理性能
Table 10 Basic performance.

処理		性能	
		192bit（実測値）	256bit（推定値）
ECDSA(*1)	スカラー倍算	2226.881 μs	5278.533 μs
	モンゴメリ乗算	1.674 μs	2.976 μs
	モンゴメリ還元	1.951 μs	1.951 μs
	剰余加算	0.179 μs	0. 239 μs
	剰余逆元演算	70.513 μs	94.017 μs
SHA-256 (*1)		1.163 μs（ブロック数 1）	
AES[21](*2)		426Mbit/s（スループット）	

(*1)測定環境：Texas Instruments DSP C6416 600MHz
(*2)測定環境：Pentium*3 Ⅲ 800MHz

は車載器より高性能であり，本論文では一般的なパソコンと同等の性能と仮定する．証明書のデータ長は IEEE1609.2 のフォーマットを参考にしたものである．

乱数生成はハッシュ関数 1 回の処理コスト，HMAC (Keyed-Hashing for Message Authentication code) [20] はハッシュ関数 2 回の処理コストとして評価する．また，剰余算および剰余乗算はモンゴメリ乗算と同じ処理コストとして評価する．

表 10 に示すように，Texas Instruments 社の DSP (Digital Signal Processor) C6416 600 MHz の環境下で ECDSA（モンゴメリ法による実装）と SHA-256 を測定した結果を用いて，online/offline 相互認証方式の処理時間の評価を行う．AES の処理時間は文献 [21] の数値を用いる．

6.2.2 online/offline 相互認証方式の評価

(1) 車載器の online 処理時時間

online/offline 相互認証方式での車載器の online 処理は図 3 の ① ③ ⑤ である．前提条件（表 9）より車載器の CPU は 50～250 MHz なので，ECDSA と SHA-256 は表 10 に示す処理時間を 2.4 倍（250 MHz の場合）または 12 倍（50 MHz の場合），AES は 3.2 倍（250 MHz の場合）または 16 倍（50 MHz の場合）し，処理時間を見積もる（**表 11**）．認証要求とチャレンジデータ検証時の値の比較時間は非常に短いため有意な処理時間としない．

*3 Pentium は，インテル・コーポレーションの登録商標です．

表 11 車載器の online 処理時間
Table 11 Online processing time of OBU (On-Board Unit).

No.	処理		処理時間の推定値 (μs)	
			250MHz	50MHz
①	認証要求		—	—
③-1	署名生成	図 4(5)：メッセージダイジェスト生成	2.791	13.956
		図 4(6)：署名生成	14.858	74.292
③-2	暗号化データ生成	図 6(5)：暗号化	5.582	27.912
		図 6(6)：MAC 生成	1.923	9.615
⑤-1	チャレンジデータ検証		—	—
⑤-2	通信鍵の復号		0. 962	4.810
合計			26.116	130.585

*No.は図 3 に対応

表 12 車載機の offline 処理時間
Table 12 Offline processing time of OBU.

No.	処理		処理時間の推定値 (*ms*)	
			250MHz	50MHz
1	署名生成の offline 処理	図 4(1)：乱数生成	0.003	0.014
		図 4(2)：スカラー倍算	12.668	63.342
		図 4(3)：剰余算	0.007	0.036
		図 4(4)：剰余逆元演算	0.226	1.128
2	チャレンジデータ生成		0.003	0.014
3	一時鍵生成		0.003	0.014
4	暗号化の offline 処理	図 6(1)：乱数生成	0.003	0.014
		図 6(2)：スカラー倍算	12.668	63.342
		図 6(3)：スカラー倍算	12.668	63.342
		図 6(4)：鍵生成	0.003	0.014
合計			25.577	127.882

認証データ生成は，図 4 に示す online 処理部分を見積もる．すなわち，認証データ生成にはメッセージダイジェストの生成でハッシュ関数 1 回，署名生成で剰余加算 1 回と剰余乗算 2 回の処理が発生する．また，暗号化は図 6 に示す online 処理部分を見積もる．すなわち，AES による暗号化 1 回と HMAC による MAC 生成 1 回の処理が発生する．

(2) 車載器の offline 処理時時間

図 3 に示した車載器の offline 処理時間を見積もった結果，合計 25.577～127.882 ms となる（**表 12**）．

(3) 路側機の online 処理時時間

online/offline 相互認証方式での路側機の online 処理は図 3 の ② ④ である．前提条件（表 9）より路側機の CPU は 2.4 GHz なので，ECDSA と SHA-256 は表 10 に示す処理時間を 0.25 倍，AES は 0.33 倍し，処理時間を見積もった（**表 13**）．

証明書と署名検証処理（図 3 ②-1，④-1）は，図 5 に示すとおり，ハッシュ関数 1 回，剰余逆元演算 1 回，モンゴメリ乗算 2 回，スカラー倍算 2 回，剰余算 1 回である．署名値の比較時間は非常に短いので有意な処理時間としない．

一時鍵の復号処理（図 3 ④-2）は図 7 に示すとおり，スカラー倍算 1 回，ハッシュ関数 3 回（鍵生成：1 回，MAC 生成：2 回）と AES 暗号化 1 回が発生する．

路車間通信システムに online/offline 相互認証方式を適

表 13 路側機の処理時間
Table 13 Processing time of RSU (Road-Side Unit).

No.	処理		処理時間の推定値（μs）
②-1	証明書（$Cert_{obu}$）の検証	図 5(1)：メッセージダイジェスト生成	0.291
		図 5(2)：剰余逆元演算	23.504
		図 5(3)：モンゴメリ乗算	0.744
		図 5(4)：モンゴメリ乗算	0.744
		図 5(5)：スカラー倍算（2 回）	2639.267
		図 5(6)：剰余算	0.744
		図 5(7)：署名の検証	—
②-2	チャレンジデータ生成		0.291
④-1	署名（s）の検証（処理時間の内訳は②-1 と同じ）		2668.294
④-2	暗号化データ（c*1*）の復号	図 5(1)：スカラー倍算	1319.633
		図 5(2)：鍵生成	0.291
		図 5(3)：復号	0.2
		図 5(4)：MAC 生成	0.582
		図 5(5)：MAC 検証	—
④-3	通信鍵（K）生成		0.291
④-4	通信鍵の暗号化		0.100
合計			6660.976

*No.は図 3 の番号に対応

表 14 通信路を流れるデータ量の見積り
Table 14 Data size on network.

No	処理	データ量(byte)	合計(byte)
① - ②	証明書	129	145
	ユーザ識別子	16	
② - ③	乱数	16	145
	証明書	129	
③ - ④	署名	64	128
	暗号化された一時鍵	64	
④ - ⑤	乱数	16	32
	暗号化された通信鍵	16	

*No.は図 3 の番号に対応

用すると，図 11 の ②’ に示すように路側機が証明書を確認するが，これは車載器の処理（図 11 の ③）と並行処理が可能なため，今回の評価の検討対象外とする．

(4) データ送信時間

online/offline 相互認証方式で発生する通信にかかる時間をデータ量から見積もる．データ量は**表 14** に示す．3 章の前提条件に記載のとおり，個別通信で利用できる 1 スロットあたりのデータ量は 183 byte である．したがって，各通信で個別通信に 1 スロット，制御用に 1 スロット，同報通信用に 1 スロットの合計 3 スロット利用するため，データ送信時間の合計は 9.375 ms となる．

(5) online/offline 相互認証時間の評価

車載器の online 処理時間が 0.026～0.130 ms，offline 処理時間が 25.577～127.882 ms なので，車載機の online 時の処理を約 99.9%削減できることになる．また，路側機の online 処理時間が 6.66 ms，通信にかかる時間が 9.375 ms なので，online/offline 相互認証にかかる時間は 16.061～16.165 ms である．したがって，3 章に記載の性能要件 18.28 ms 以下を満たす．

本論文では最大伝送速度 4,096 kbps で 1 台の路側機と同時に通信可能な車載器は 4 台との前提のもと評価を行ったが，実際の環境下では伝送速度が下がる可能性がある．**図 12** に伝送速度が下がった場合の相互認証にかかる時間およびサービスデータ送受信時間の関係を示す．路側機/車載器の認証処理時間は伝送速度には依存しないため，一定である．伝送速度が下がった場合は相互認証時に発生するデータの送受信時間とサービスデータの送受信時間が増加し，サービスデータの送受信が完了しないうちに路側機との通信が切れてしまう．したがって，路側機と同時に通信可能な車載器の接続台数を制限する必要が発生する．

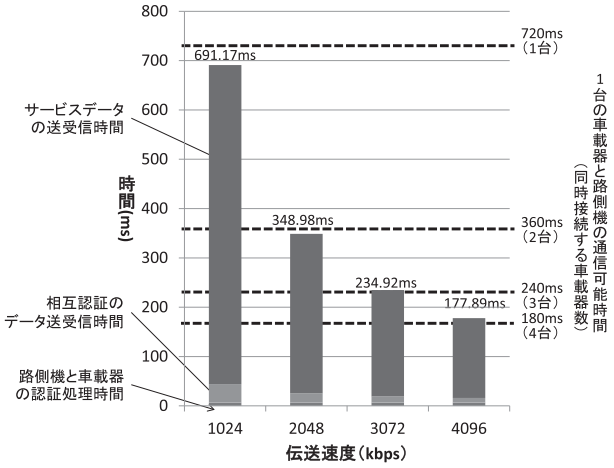

図 12 伝送速度と各処理時間
Fig. 12 Transmission rate and processing time.

7. おわりに

本論文では，路車間通信システムにおいて，車載器が路側機を介してサービス提供者と双方向に通信する場合に，互いの真正性を確認するための認証と暗号化通信のための通信鍵を高速に共有する方式を提案した．

路車間通信では車載器は高速に移動するため認証と通信鍵の共有を高速に行う必要があるうえ，低リソースの車載器の処理負荷を軽減する必要がある．そこで，相互認証および通信鍵の共有にかかる処理量は変わらないが，車載器が路側機との通信が発生していないとき（offline 時）に可能な限り事前処理しておくことで，路側機との通信が発生したとき（online 時）の車載器の処理を減らす online/offline 相互認証方式を適用する路車間通信システムを提案した．そして，online/offline 相互認証方式の安全性と性能を評価した．安全性評価は，NIST SP800-63-1 に記載されている認証プロセスで発生する 7 つの脅威 [18] が提案方式には存在しないことを確認した．性能評価では，実測値に基づいて，online 時の認証処理時間を算出した結果，相互認証と暗号化通信のための通信鍵の共有が性能要件の 18.28 ms 以下を満たすことを確認した．

今後の課題は，実機での性能評価，効率的な車載器の失効管理，サービス提供者と路側機管理者が異なる場合のセキュリティ情報の安全性確保の実現である．

参考文献

[1] ITS スポットサービス，入手先 ⟨http://www.mlit.go.jp/road/ITS/j-html/spot_dsrc/index.html⟩.
[2] IEEE Standards 1609.2, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages (July 2006).
[3] 畑　正人ほか：即時応答性に優れた路車間認証方式，*Symposium on Cryptography and Information Security* (*SCIS*) (2012).
[4] 藤川賢治ほか：無線インターネットサービスに必要なセキュリティを提供する高速認証システム，情報処理学会研究報告，2002-DPS-107 (Mar. 2002).
[5] IEEE Standard 802.11i, Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment6: Medium Access Control (MAC) Security Enhancements (June 2004).
[6] 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，電子情報通信学会 ITS 研究会 (2011).
[7] ETSI TR 102 638 v1.1.1, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definition (June 2009).
[8] 国土技術政策総合研究所：次世代道路サービス提供システムに関する共同研究報告書 (2006).
[9] 堀　良彰ほか：無線 LAN における MIS プロトコルに対するセキュリティ評価，*Symposium on Cryptography and Information Security* (*SCIS*), pp.247–252 (Jan. 2005).
[10] 森岡仁志ほか：MIS プロトコルと PDMA による高速ハンドオーバー，電子情報通信学会技術研究報告 (2005).
[11] 真野　浩：高速シームレスモバイル通信，情報処理学会研究報告，高度交通システム（ITS）(2007).
[12] 服部有里子：路車間通信における同報・個別通信混在時の安定したサービス提供のための制御方式，情報処理学会論文誌，Vol.53, No.1, pp.175–183 (2012).
[13] 社団法人電波産業会：ARIB STD-T75 境域通信（DSRC）システム標準規格 (2008).
[14] 社団法人電波産業会：ARIB STD-T88 境域通信（DSRC）アプリケーションサブレイヤ標準規格 (2007).
[15] Even, S., Goldreich, O. and Micali, S.: On-line/off-line Digital Signatures, *Advances in Cryptology – CRYPTO 1989*, LNCS2332, pp.263–275, Springer-Verlag (1990).
[16] ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).
[17] ISO/IEC 18033-2, Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers (2006).
[18] NIST (National Institute of Standards and Technology): SP800-63-1 Electronic Authentication Guideline (2011).
[19] EVITA, Deliverable D3.2: Secure On-board Architecture Specification (2011).
[20] IETF, RFC 2104 HMAC: Keyed-Hashing for Message Authentication (1997).
[21] Daemen, J. and Rijmen, V.: *The Design of Rijndael*, Springer (2002).

安藤 英里子 （正会員）

2002 年 3 月九州大学大学院数理学府修士課程修了．同年 4 月（株）日立製作所システム開発研究所に入所．以来，情報セキュリティに関する研究開発に従事．現在，（株）日立製作所横浜研究所にて主に ITS における情報セキュリティ技術の研究開発に従事．

佐藤 尚宜

1992 年 3 月九州大学理学部数学科卒業．1994 年同大学大学院数理学研究科修士課程修了．1996 年同大学院数理学研究科博士課程修了（数理学博士）．同年 4 月から学術振興会特別研究員．1999 年（株）日立製作所システム開発研究所へ入所．以来，暗号と情報セキュリティに関する研究と開発に従事．現在，（株）日立製作所横浜研究所主任研究員．

福澤 寧子 （正会員）

1985 年日本女子大学家政学部家政理学科物理学系卒業．同年（株）日立製作所システム開発研究所（現，横浜研究所）入所．以来，ソフトウェアの生産性管理技術，暗号技術，移動体システムや社会情報システムにおけるセキュリティ技術の研究開発に従事．横浜研究所主管研究員，博士（工学）．