従量制課金サービスにおける偽証防止方式の提案†

6G−8

飯田　恭弘　上野　正巳　阿川　雄資
NTT情報流通プラットフォーム研究所

1　はじめに

近年ネットワークの広帯域化に伴い，ライブ配信，映画配信，音楽配信，VoIP(Voice over IP) などのサービスが活発化し，ストリームコンテンツの販売も行われるようになってきた．このようなコンテンツを販売する場合，利用者が利用したい分だけを購入できることが望ましい．したがって，このようなコンテンツの販売には，従来のような定額課金だけでなく，利用者へ提供した量（時間，パケット量，データ量など）に応じた従量制の課金も考えられる．

ところが，従量制の課金においては，販売者が実際に利用者へ提供したコンテンツの量を決済機関へ偽って申告することで，不当に利益を得ることが可能である．本稿では，従量制の課金におけるこのような販売者の偽証を防止する方法について述べる．

2　関連技術

一般に，販売者による決済機関への偽証を防止するためには，利用者の公開鍵署名を決済機関が検証することが有効である [1]．そこで，この公開鍵署名の検証を繰り返し行うことで従量制の課金における販売者の偽証を防止できる可能性がある．具体的には販売者，利用者，決済機関の3者ともが公開鍵証明書を持つことを前提とするSET方式 [2] を，従量制の課金に適用することが考えられる．実際，SET方式を従量制の課金に適用する検討もすでになされている [3]．ところが，このような方法では下記の課題が生じる．

- 単位量のサービスの提供ごとに利用者，販売者，決済機関とも公開鍵署名を行うため，計算負荷が非常に高くなる可能性がある
- 単位量のサービスの提供ごとに販売者と利用者間で購入注文要求 (PReq)，購入注文応答 (PRes) を，また，販売者と決済機関間で承認要求 (AuthReq)，承認応答 (AuthRes) を行うため [2]，通信負荷が非常に高くなる可能性がある

3　提案方式

本節では，前節で述べた課題を解決しながら，販売者の偽証を防止する方法を述べる．本方法では，従量制のサービスを販売する販売者，このサービスを購入する利用者，および販売者と利用者の決済を行う決済機関の3者を考える．以下では，サービスの販売においてこの3者間が行う一連の手順を"準備段階"，"利用者認証段階"，"サービス授受段階"，"決済要求段階"に分けて説明する．

準備段階：

まず，利用者はあらかじめ自身を一意に特定できる利用者IDを取得する．この利用者IDは決済機関や他の機関が発行しても良い．なお，この利用者IDは他の利用者や販売者に公開する必要はない．次に，利用者は二つの素数 p，q を生成し，合成数 $N = p \times q$ を計算する．また，$S \in_U \mathbf{Z}_N{}^{\ddagger}$ を選び，下記の T を計算し，この T を利用者IDとともに決済機関へ送る (図中の①)．

$$T = S^2 \bmod N \tag{1}$$

ここでは，p や q を知らずに N を素因数分解することの困難さを利用してなりすましを防止する [4]．

利用者認証段階：

販売者は利用者からサービス提供の依頼を受けると，まず利用者の正当性 (正当な S を保持すること) を検証する (図中の②)．この検証方法は例えばFeige，Fiat，Shamirらの提案する認証方法 (Feige-Fiat-Shamir認証)[4] などの既存の認証方法を適用できるため，本稿では説明を省略する．なお，このとき販売者は決済機関または他の機関から N，T を取得するものとする．

サービス授受段階：

販売者は，利用者の正当性を確認すると，利用者へのサービスの提供を開始する．この手順を **Step.1** から **Step.4** に述べる．なお，本手順は提供したサービス量の正当性を，販売者が第3者へ主張できることを目的として設計している．

Step.1 利用者は以下のように X_1，X_2 を定め，販売者に送る (図中の③)．

$$X_1 = R_1^2 \bmod N \qquad (R_1 \in_U \mathbf{Z}_N^*) \tag{2}$$

$$X_2 = R_2^2 \bmod N \qquad (R_2 \in_U \mathbf{Z}_N^*) \tag{3}$$

Step.2 販売者は利用者に以下の a を送る (図中の④)．

$$a \in_U \{0, 1\} \tag{4}$$

Step.3 利用者は以下のように Y_1，Y_2 を定め，販売者に送る (図中の⑤)．

†A non-falsification method in a usage-based billing
Yasuhiro IIDA, Masami UENO, Yuji AGAWA
NTT Information Sharing Platform Labolatories

$if\ a=0\ then\ Y_1 = R_1 S \bmod N \quad Y_2 = R_2 \bmod N$ (5)

$if\ a=1\ then\ Y_1 = R_1 \bmod N \quad Y_2 = R_2 S \bmod N$ (6)

Step.4 販売者は以下を検証する．

$if\ a=0\ then\ Y_1^2 \stackrel{?}{=} TX_1 \bmod N \quad Y_2^2 \stackrel{?}{=} X_2 \bmod N$ (7)

$if\ a=1\ then\ Y_1^2 \stackrel{?}{=} X_1 \bmod N \quad Y_2^2 \stackrel{?}{=} TX_2 \bmod N$ (8)

ここで，$\stackrel{?}{=}$は，この両辺が等しいことを検証することを表す．これに成功すると，販売者は単位量だけサービスを提供する (図中の⑥)．また，販売者は X_1，X_2，Y_1，Y_2 の 4 つのパラメータを，サービスを提供した証としてセットで保存する．以降，販売者と利用者は上記の **Step.1** から **Step.4** を繰り返すことで次々とサービスの授受を続行する．販売者は利用者から受け取る 4 つのパラメータのセットの数を，利用者へ提供したサービスの分量の証とする．

決済要求段階：

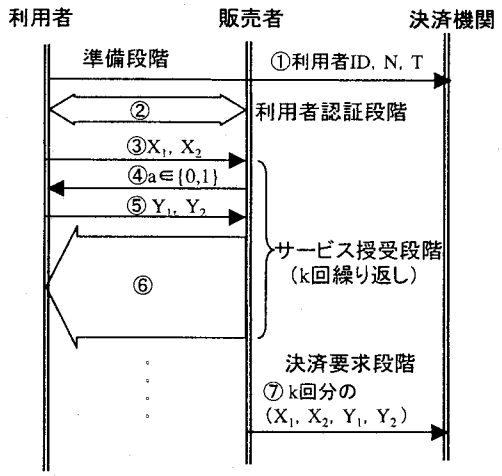
サービスの提供が完了すると，販売者はそれまでに取得した X_1，X_2，Y_1，Y_2 の 4 つのセットを全て決済機関へ送る (図中の⑦)．

決済機関はこれらを受信し，以下を検証する．

$$Y_1^2 = TX_1 \bmod N \quad Y_2^2 = X_2 \bmod N \quad (9)$$

または $Y_1^2 = X_1 \bmod N \quad Y_2^2 = TX_2 \bmod N$ (10)

これに成功すると，決済機関は利用者と販売者の間の決済を行う．



図： 提案方式に基づいたサービスの販売手順

4 不正対策に関する考察

本節では，提案方式の有効性を，利用者が行い得る不正，販売者が行い得る不正，および事故等による通信回線の切断時における，利用者と販売者の公平性の 3 つの観点から考察する．

利用者が行い得る不正：

利用者は他の利用者になりすます可能性がある．しかし，正当な S を持たない限り X_1，X_2，Y_1，Y_2 を正しく生成できず，なりすましは困難である．この根拠は Feige-Fiat-Shamir 認証と同様である．また，これらのパラメータを正しく生成できるのは，正当な S を保持する利用者に限られる．したがって，利用者が S を秘匿している限り，利用したサービスに対する請求を不当だとして支払いを免れることはできない．さらに，利用者は上記の 4 つのパラメータのセットと引き換えに単位量のサービスを受け取るため，少ない支払いで多くのサービスを受け取ることはできない．

販売者が行い得る不正：

販売者は既得した 4 つのパラメータのセットを再利用して利用者に不当に課金を行う可能性がある．この可能性に対しては，一度使用されたパラメータのセットを決済機関が管理し，これを 2 重に受信することを拒否するなどの運用で回避できる．

回線切断時の公平性：

サービスの授受中に事故等で回線が切断された場合にも，販売者は少なくとも回線の切断時までに受け取った 4 つのパラメータのセットをもとに課金ができる．したがって，このような場合でも利用者と販売者の公平性は保たれる．

5 まとめ

本稿では，従量制の課金における販売者の偽証防止を，公開鍵署名を利用せずに行う方法を提案した．本方法では，数百ビット以上のべき乗演算を行う公開鍵署名に対し，1 回の乗算を行うだけでよく，計算負荷を下げることが可能である．また，単位量のサービス授受には利用者と販売者間の通信だけでよく，通信負荷を下げることが可能である．今後は実装によって性能評価を行う予定である．

参考文献

[1] Information technology, Security techniques, Non-repudiation ISO/IEC 13888-1-4, 1997.12.1

[2] VISA International and MasterCard International, Secure Electronic Transaction(SET)SpecificationBook 1-3 Version 1.0, 1997, 5.31

[3] 可児島 健，"与信，課金管理への SET 決済方式の適用性と，運用方法の検討"，情報処理学会第 56 回全国大会講演論文集，2G-4，(1998)

[4] Feige, Fiat, and Shamir, Zero-Knowledge Proofs of Identity, Journal of Cryptology, 1, 2, pp.77-94, (1988)

‡ $\mathbf{Z}_N$ は 0 以上 N 未満の整数の集合，$\mathbf{Z}_N^*$ は $\mathbf{Z}_N$ かつ N と互いに素な整数の集合を表す．また，$x \in_U A$ は集合 A から一様にランダムに x を選ぶことを表す．