要 旨

携帯電話に適した小額課金方式

上岡 隆

近年，携帯端末を対象として電子商取引であるモバイルコマース (MC) が急速な広がりを見せていている．特にブラウザフォンと呼ばれる，インターネットに接続可能な携帯電話を対象とした MC が注目を集めており，携帯電話での小口の決済を目的とした小額課金方式が提案されている．現在，提案されている小額課金方式の中で，もっとも高速かつ安全な方式として Five-units Coin を提案した．Five-units Coin では支払額の検証法として顧客-商店間の認証子でコインの単価を示し，セッション鍵でマスクしたコインの枚数を示すことによって金額の検証を行っていた．そのため，第三者によってコインの枚数を予測され，セッション鍵が盗まれる等の危険性があった．本研究では Five-units Coin における問題点を解決した，新しい携帯電話向け小額課金方式の提案を行っている．提案方式では認証子内に残高を含めることにより，第三者によるセッション鍵の推察を困難にすることに成功している．また顧客-商店間のセッション鍵に顧客-発行主体間のセッション鍵と支払総額を利用することにより，商店側による不正請求が検出可能となっている．

キーワード　SAS-Coin，Five-units Coin，小額課金，携帯電話

Abstract

A Micropayment System for Moblie Phones

Takashi Kamioka

In recent years, electronic commerce for a portable terminal called mobile commerce (MC) has spread quickly. MC for mobile phones starts to garner attention. Therefore, some micropayment systems for mobile phones are proposed. Five-units Coin was proposed as the most high-speed and secure system in a micropayment systems. In Five-units Coin, amount of pay was verified by authentication data showing unit of coin and number of sheets concealed with session key. Consequently, there was a danger that session key would be stolen by third person. This research have proposed new micropayment system for mobile phones which solved the problem in Five-units Coin. By proposal system, it succeeded in making difficult guess of session key by third person by including bank balance into authentication data. Moreover, by using session key between customer-broker and total amount of pay for creating session key between customer-stores, unjust claim by store side became detectable.

key words SAS-Coin, Five-units Coin, Mircopayment, Mobile phone