



دانشگاه سوادکوه

پردیس بین الملل

## پایان نامه کارشناسی ارشد

### طراحی پروتکل امن برای کیف پول همراه

از

الهام قره شیخ لو

استاد راهنما:

دکتر رضا ابراهیمی آتانی

اسفند ماه ۱۳۹۱

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

دانشکده پردیس بین الملل  
گروه مهندسی فناوری اطلاعات گرایش تجارت الکترونیکی

## طراحی پروتکل امن برای کیف پول همراه

از  
الهام قره شیخ لو

استاد راهنما:  
دکتر رضا ابراهیمی آتانی

اسفند ماه ۱۳۹۱

تقدیم به:

پدر و مادر عزیزم

## تشکر و قدردانی:

در طول کار بر روی این پایان نامه دوستان بسیاری به طرق مختلف مرا مورد حمایت قرار دادند. در اینجا باید از استاد راهنما جناب آقای دکتر رضا ابراهیمی آتانی بخاطر تمامی کمک هایشان تقدیر و تشکر کنم. از جناب آقای مهندس فرزاد توکلی به دلیل کمک های بی دریغشان تشکر می نمایم. اما تقدیر ویژه ام از خانواده عزیزم خواهد بود بخاطر حمایت مداوم و دلگرمی هایشان. در پایان از جناب آقای مهندس حجت شعبانپور به دلیل حمایت های پدرانۀ ایشان کمال تشکر را دارم.

## فهرست مطالب

۱	فصل ۱: مقدمه
۲	۱-۱- مقدمه
۴	۲-۱- تعریف مسئله
۴	۳-۱- هدف
۵	۴-۱- ساختار کلی پایان نامه
۶	فصل ۲: مفاهیم پیش زمینه
۷	۱-۲- مقدمه
۷	۲-۲- تجارت همراه
۹	۳-۲- پرداخت همراه
۱۰	۱-۳-۲- روند رشد پرداخت همراه در جهان و ایران
۱۲	۲-۳-۲- موارد استفاده پرداخت همراه
۱۲	۱-۲-۳-۲- فروش بلیط همراه
۱۳	۲-۲-۳-۲- کوپن همراه
۱۳	۳-۲-۳-۲- خرید و تحویل محتوا
۱۴	۴-۲-۳-۲- خدمات مبتنی بر مکان
۱۴	۵-۲-۳-۲- خدمات اطلاعاتی
۱۴	۶-۲-۳-۲- بانکداری همراه
۱۴	۷-۲-۳-۲- حراج همراه
۱۵	۸-۲-۳-۲- خرید همراه
۱۵	۹-۲-۳-۲- بازاریابی و تبلیغات همراه
۱۵	۱۰-۲-۳-۲- کارگزاری همراه
۱۶	۳-۳-۲- انواع پرداخت همراه
۱۶	۱-۳-۳-۲- دسته بندی بر اساس موقعیت مکانی
۱۷	۲-۳-۳-۲- دسته بندی بر اساس ارزش جا به جا شده
۱۷	۳-۳-۳-۲- دسته بندی بر اساس زمان پرداخت
۱۸	۴-۳-۳-۲- دسته بندی بر اساس مبنای پرداخت
۱۹	۵-۳-۳-۲- دسته بندی بر اساس اعتبار سنجی نشانه‌های استفاه شده در پرداخت
۱۹	۴-۲- کیف پول همراه
۲۱	۲-۴-۲- نقش‌ها و بازیگران جامعه کیف پول

۲۳	۵-۲- فناوری‌های شبکه و زیرساخت‌های پرداخت همراه
۲۴	۲-۵-۱- شبکه سلولی GSM
۲۵	۲-۵-۲- شبکه سلولی GPRS
۲۵	۲-۵-۳- شبکه سلولی نسل سوم (3G)
۲۷	۲-۵-۴- فناوری بلوتوث
۲۷	۲-۵-۵- فناوری RFID
۲۹	۲-۵-۶- فناوری NFC
۳۰	۲-۶- نقش تواناسازی فناوری‌های همراه در پرداخت همراه
۳۱	۲-۶-۱- استفاده از پیامک در پرداخت همراه
۳۲	۲-۶-۲- استفاده از USSD در پرداخت همراه
۳۲	۲-۶-۳- استفاده از WAP در پرداخت همراه
۳۴	۲-۶-۴- استفاده از NSDT در پرداخت همراه
۳۴	۲-۶-۵- استفاده از بلوتوث در پرداخت همراه
۳۵	۲-۶-۶- استفاده از RFID در پرداخت همراه
۳۶	۲-۶-۷- استفاده از NFC در پرداخت همراه
۳۸	۲-۷- امنیت
۳۹	۲-۷-۱- رمزنگاری متقارن و نامتقارن
۴۰	۲-۷-۲- توابع چکیده ساز
۴۱	۲-۷-۳- الگوریتم‌های رمزنگاری سبک وزن
۴۳	۲-۸- نتیجه گیری

### فصل ۳: کارهای مرتبط گذشته

۴۴	
۴۵	۳-۱- مقدمه
۴۵	۳-۲- پرداخت‌های خرد
۴۵	۳-۲-۱- معیار انتخاب پرداخت‌های خرد
۴۶	۳-۲-۲- معیارهای بررسی
۴۹	۳-۲-۳- میلی سنت
۴۹	۳-۲-۳-۱- ساز و کار و روش انجام
۵۱	۳-۲-۳-۲- ارزیابی میلی سنت
۵۴	۳-۲-۴- پرداخت واژه
۵۴	۳-۲-۴-۱- ساز و کار و روش انجام
۵۶	۳-۲-۴-۲- ارزیابی پرداخت واژه

۵۸	..... NetPay-۵-۲-۳
۵۹	..... ۱-۵-۲-۳- ساز و کار و روش انجام
۶۱	..... NetPay-۲-۵-۲-۳- ارزیابی
۶۴	..... PPay-۶-۲-۳
۶۴	..... ۱-۶-۲-۳- ساز و کار و روش انجام
۶۷	..... PPay-۲-۶-۲-۳- ارزیابی
۶۹	..... P2P-NetPay-۷-۲-۳
۶۹	..... ۱-۷-۲-۳- ساز و کار و روش انجام
۷۲	..... P2P-NetPay-۲-۷-۲-۳- ارزیابی
۷۴	..... WhoPay-۸-۲-۳
۷۴	..... ۱-۸-۲-۳- ساز و کار و روش انجام
۷۷	..... WhoPay-۲-۸-۲-۳- ارزیابی
۷۹	..... ۹-۲-۳- پرداخت خرد با نشانه (توکن) بدهی
۷۹	..... ۱-۹-۲-۳- ساز و کار و روش انجام
۸۱	..... ۲-۹-۲-۳- ارزیابی نشانه بدهی
۸۲	..... ۳-۳- کیف پول همراه
۸۳	..... ۱-۳-۳- کیف پول گوگل
۸۳	..... mFeiro-۲-۳-۳
۸۴	..... ۳-۳-۳- جیرینگ
۸۴	..... ۴-۳- نتیجه گیری

#### ۸۵ فصل ۴: پروتکل امن پیشنهادی برای کیف پول همراه

۸۶	..... ۱-۴- مقدمه
۸۶	..... ۲-۴- طراحی پروتکل پیشنهادی
۸۶	..... ۱-۲-۴- نیازمندی‌های طراحی
۸۷	..... ۲-۲-۴- علائم اختصاری مورد استفاده
۸۸	..... ۳-۲-۴- فرضیات پروتکل
۸۸	..... ۴-۲-۴- شمای کلی پروتکل
۸۹	..... ۵-۲-۴- جزئیات پروتکل
۸۹	..... ۱-۵-۲-۴- مرحله ثبت نام
۹۰	..... ۲-۵-۲-۴- مرحله عملیات
۹۵	..... ۳-۴- جایگاه پروتکل پیشنهادی



- ۹۶-۴-۴- الگوریتم‌های مناسب جهت استفاده در پروتکل پیشنهادی.....
- ۹۷-۴-۴-۱- رمزهای جریانی واجد شرایط.....
- ۱۰۰-۴-۴-۲- توابع چکیده ساز واجد شرایط.....
- ۱۰۲-۴-۴-۳- پیاده سازی توابع رمزنگاری و چکیده ساز.....
- ۱۰۲-۴-۴-۱- زیرساخت پیاده سازی.....
- ۱۰۵-۴-۴-۲- نتایج پیاده سازی.....
- ۱۱۳-۴-۴-۳- انتخاب الگوریتم.....
- ۱۱۳-۴-۵- بسترها و فناوری‌های ارتباطی پروتکل پیشنهادی.....
- ۱۱۶-۴-۶- ارزیابی پروتکل پیشنهادی.....
- ۱۱۹-۴-۷- مقایسه پروتکل پیشنهادی با طرح‌های گذشته.....
- ۱۲۴-۴-۸- تحلیل امنیتی پروتکل پیشنهادی.....
- ۱۲۷-۴-۹- نتیجه گیری.....

۱۲۸ **فصل ۵: جمع‌بندی و پیشنهادها**

- ۱۲۹-۵-۱- مقدمه.....
- ۱۲۹-۵-۲- جمع بندی.....
- ۱۳۰-۵-۳- نوآوری.....
- ۱۳۰-۵-۴- پیشنهادها.....

۱۳۲

مراجع

## فهرست شکل‌ها

- شکل (۱-۲) روند رشد کلی تراکنش پرداخت همراه با تنوع خدمات [9] ..... ۱۱
- شکل (۲-۲) روند رشد کلی تراکنش پرداخت همراه به تفکیک مناطق [9] ..... ۱۱
- شکل (۳-۲) میزان پذیرش کیف پول همراه بین مردم آمریکا در چهار ماه ابتدای سال ۲۰۱۲ [21] .. ۲۱
- شکل (۴-۲) بازیگران و نقش‌ها در جامعه کیف پول ..... ۲۳
- شکل (۵-۲) اصول رمزنگاری b بیت، با رمز بلوکی و رمز جریانی [35] ..... ۴۰
- شکل (۶-۲) ویژگی‌های توابع چکیده ساز [35] ..... ۴۱
- شکل (۷-۲) تعادل بین کارایی، امنیت، و هزینه در رمزنگاری سبک وزن [37] ..... ۴۲
- شکل (۱-۳) شمای کلی میلی سنت [39] ..... ۵۰
- شکل (۲-۳) شمای کلی پرداخت واژه [39] ..... ۵۵
- شکل (۳-۳) شمای کلی NetPay ..... ۶۰
- شکل (۴-۳) شمای کلی PPay [45] ..... ۶۵
- شکل (۵-۳) شمای کلی P2P-NetPay [45] ..... ۷۰
- شکل (۶-۳) شمای کلی WhoPay [45] ..... ۷۵
- شکل (۷-۳) شمای کلی نشانه بدهی ..... ۸۰
- شکل (۱-۴) شمای کلی پروتکل پرداخت خرد پیشنهادی ..... ۸۹
- شکل (۲-۴) ساختار نشانه اصلی ..... ۹۱
- شکل (۳-۴) ساختار زیر نشانه ..... ۹۲
- شکل (۴-۴) محیط برنامه نویسی NetBeans ..... ۱۰۴
- شکل (۵-۴) اجرای برنامه بر روی گوشی ..... ۱۰۶
- شکل (۶-۴) نمودار خطی زمان-طول پیام رمزهای جریانی ..... ۱۱۲
- شکل (۷-۴) نمودار خطی زمان-طول پیام توابع چکیده ساز ..... ۱۱۲
- شکل (۸-۴) بستر ارتباطی بین اعضاء مشمول در پروتکل پیشنهادی ..... ۱۱۶

## فهرست جدول‌ها

- جدول (۱-۲) آمار استفاده از تلفن همراه طی سال‌های ۸۴ تا ۹۰ در ایران [۱]..... ۸
- جدول (۲-۲) مهمترین فناوری‌های موجود مورد استفاده در پرداخت‌های همراه ..... ۳۰
- جدول (۳-۲) مقایسه فناوری‌های تواناساز پرداخت همراه ..... ۳۷
- جدول (۱-۳) فرآیند پرداخت در میلی سنت ..... ۵۰
- جدول (۲-۳) فرآیند پرداخت با در نظر گرفتن هزینه محاسباتی اعضاء در میلی سنت ..... ۵۱
- جدول (۳-۳) خلاصه هزینه محاسباتی هر عضو در میلی سنت ..... ۵۲
- جدول (۴-۳) فرآیند پرداخت در پرداخت واژه ..... ۵۵
- جدول (۵-۳) فرآیند پرداخت با در نظر گرفتن هزینه محاسباتی اعضاء در پرداخت واژه ..... ۵۶
- جدول (۶-۳) خلاصه هزینه محاسباتی هر عضو در پرداخت واژه ..... ۵۷
- جدول (۷-۳) فرآیند پرداخت در NetPay ..... ۶۰
- جدول (۸-۳) فرآیند پرداخت با در نظر گرفتن هزینه محاسباتی اعضاء در NetPay ..... ۶۱
- جدول (۹-۳) خلاصه هزینه محاسباتی هر عضو در NetPay ..... ۶۲
- جدول (۱۰-۳) فرآیند پرداخت در PPay ..... ۶۶
- جدول (۱۱-۳) فرآیند پرداخت با در نظر گرفتن هزینه محاسباتی اعضاء در PPay ..... ۶۶
- جدول (۱۲-۳) خلاصه هزینه محاسباتی هر عضو در PPay ..... ۶۷
- جدول (۱۳-۳) فرآیند پرداخت در P2P-NetPay ..... ۷۱
- جدول (۱۴-۳) فرآیند پرداخت با در نظر گرفتن هزینه محاسباتی اعضاء در P2P-NetPay ..... ۷۱
- جدول (۱۵-۳) خلاصه هزینه محاسباتی هر عضو در P2P-NetPay ..... ۷۲
- جدول (۱۶-۳) فرآیند پرداخت در WhoPay ..... ۷۶
- جدول (۱۷-۳) فرآیند پرداخت با در نظر گرفتن هزینه محاسباتی اعضاء در WhoPay ..... ۷۶
- جدول (۱۸-۳) خلاصه هزینه محاسباتی هر عضو در WhoPay ..... ۷۷
- جدول (۱۹-۳) فرآیند پرداخت در نشانه بدهی ..... ۸۰
- جدول (۲۰-۳) فرآیند پرداخت با در نظر گرفتن هزینه محاسباتی اعضاء در نشانه بدهی ..... ۸۰
- جدول (۲۱-۳) خلاصه هزینه محاسباتی هر عضو در نشانه بدهی ..... ۸۱
- جدول (۱-۴) فرآیند پرداخت در پروتکل پیشنهادی ..... ۹۴
- جدول (۲-۴) فرآیند پرداخت با در نظر گرفتن هزینه محاسباتی اعضاء در پروتکل پیشنهادی ..... ۹۵
- جدول (۳-۴) جایگاه پروتکل پیشنهادی در دسته بندی‌های مختلف پرداخت همراه ..... ۹۶

- جدول (۴-۴) ویژگی تلفن‌های همراه مورد آزمون ..... ۱۰۷
- جدول (۵-۴) زمان اجرای الگوریتم‌های رمز جریانی با ورودی بین ۱۶ تا ۱۲۸ بایت ..... ۱۰۸
- جدول (۶-۴) زمان اجرای الگوریتم‌های رمز جریانی با ورودی بین ۲۵۶ تا ۲۰۴۸ بایت ..... ۱۰۹
- جدول (۷-۴) زمان اجرای توابع چکیده ساز با ورودی بین ۱۶ تا ۱۲۸ بایت ..... ۱۱۰
- جدول (۸-۴) زمان اجرای توابع چکیده ساز با ورودی بین ۲۵۶ تا ۲۰۴۸ بایت ..... ۱۱۱
- جدول (۹-۴) ورودی‌های تابع چکیده ساز و رمزنگار در پیام‌های ارسالی پروتکل پیشنهادی ..... ۱۱۳
- جدول (۱۰-۴) خلاصه هزینه محاسباتی هر عضو در پروتکل پیشنهادی ..... ۱۱۷
- جدول (۱۱-۴) مقایسه کلی پرداخت‌های خرد منتخب با پروتکل پیشنهادی ..... ۱۲۰
- جدول (۱۲-۴) مقایسه پرداخت‌های خرد منتخب با پروتکل پیشنهادی از بُعد مشخصات ذاتی ..... ۱۲۱
- جدول (۱۳-۴) مقایسه پرداخت‌های خرد منتخب با پروتکل پیشنهادی از بُعد امنیت و حریم خصوصی (بخش اول) ..... ۱۲۲
- جدول (۱۴-۴) مقایسه پرداخت‌های خرد منتخب با پروتکل پیشنهادی از بُعد امنیت و حریم خصوصی (بخش دوم) ..... ۱۲۳
- جدول (۱۵-۴) مقایسه پرداخت‌های خرد منتخب با پروتکل پیشنهادی از بُعد توسعه و سیستمی ..... ۱۲۴

### طراحی پروتکل امن برای کیف پول همراه الهام قره شیخ لو

پرداخت همراه روش جدیدی جهت انجام عملیات و تراکنش‌های مالی به منظور انجام امور تجاری بر روی ابزارهای همراه بوده که از لحاظ ماهیتی با پرداخت‌های سنتی همانند چک و یا وجه نقد تفاوت اساسی دارد. پرداخت‌های همراه دارای مزایای غیر قابل انکاری چون راحتی، دسترسی و قابلیت تحرک و همچنین چالش‌های جدی نظیر امنیت و هزینه می‌باشند. تمامی روش‌های ارائه شده تاکنون سعی بر این دارند تا این چالش‌ها را تا حد قابل قبولی برطرف نمایند. پرداخت‌های همراه دارای کاربردهای فراوانی هستند. یکی از کاربردهای جدید پرداخت همراه استفاده از کیف پول همراه می‌باشد.

کیف پول همراه برنامه‌ای کاربردی است که بر روی ابزار همراه مثل تلفن همراه ذخیره شده و برای مشترکین امکان انجام تراکنش‌های مالی را فراهم می‌آورد. کیف پول همراه بر روی فناوری‌های ارتباطی مختلفی نظیر WAP، بلوتوث و یا پیامک قابل طراحی و پیاده‌سازی بوده که هر کدام مزایا و چالش‌های خاص خود را دارند. اکثر راه‌حل‌های ارائه شده در این زمینه نیازمند ارتباط همیشگی کیف پول همراه با شبکه مخابراتی و اینترنتی بوده که این ارتباط بر مشتری هزینه تحمیل می‌نماید. در حالی که پرداخت هزینه اتصال به شبکه برای هر تراکنش با ارزش مالی ناچیز، مقرون به صرفه نیست. حال اگر ارتباط با شبکه به هر دلیل مقدور نباشد و یا اینکه مشتری به دنبال دریافت خدمات اقتصادی تر برای این قبیل پرداخت‌ها باشد؛ باید از ساز و کارهای دیگری برای پرداخت استفاده نمود.

در این پایان نامه سعی بر آن است که پروتکل پرداخت خرد برون از خط جدیدی برای استفاده در کیف پول همراه ارائه و با استفاده از رمزنگاری متقارن و تابع چکیده ساز، امنیت آن تأمین گردد. روش تحقیق این پایان نامه مبتنی بر مدل سازی بوده و برای اثبات کارایی و امنیت پروتکل پیشنهادی از معیارهای موجود بهره گرفته و این پروتکل با نمونه‌های قبلی ارائه شده مقایسه می‌شود.

**واژه‌های کلیدی:** پرداخت همراه، کیف پول همراه، پرداخت خرد، امنیت، رمزنگاری متقارن، توابع چکیده ساز.

## Abstract

# Designing of a secure protocol for mobile wallet

Elham Gharehsheikhlou

Mobile Payments is a new method for operations and financial transactions in order to conduct commercial activities on mobile devices, which in terms of the nature has a major difference with traditional payment such as cheque or cash. Mobile payments have undeniable advantages like convenience, accessibility and mobility and also serious challenges such as security and cost. All methods have been proposed so far, is try to overcome these challenges to an acceptable level. Mobile payments have numerous applications. One of the new applications of mobile payment is the use of mobile wallet.

Mobile wallet is an application which store on the mobile devices like cell phone and gives subscribers the ability to perform financial transactions. Mobile wallet can be designed and implemented on different communication technologies such as WAP, Bluetooth or SMS, which each one has its own advantages and challenges. Most of the proposed solutions in this field require wallet continuous communication with network and internet which would impose a cost to the customer. While the network connection fee for each micro payment is not cost effective, if the network connection is not possible for any reason or customer is looking to receive more economical service for these payments, other mechanisms should be used for payment.

This thesis has tried to propose a new Off-line micro payment protocol to use in mobile wallet, and by using the symmetric encryption and hash function its security will be provided. The methodology used in this thesis is based on modeling and the existing criteria are used to prove the efficiency of the proposed protocol and the protocol has been compared with the previous proposed samples.

**Keywords:** Mobile payment, Mobile wallet, Micro payment, Security, Symmetric encryption, Hash functions.

# فصل ١:

## مقدمه

## ۱-۱- مقدمه

در گذشته نه چندان دور، پرداخت‌ها به شکل سنتی انجام می‌گرفت. فروشندگان، بازرگانان و در کل مردم برای پرداخت، پول را به صورت نقد جا به جا نموده و یا از روش‌هایی مانند چک و حواله استفاده می‌کردند. دیری نپایید که با نفوذ فناوری به همهٔ زوایای زندگی بشر و ایجاد تغییرات بنیادین در خواست‌ها و نیازمندی‌های او این بُعد از زندگی دستخوش تغییراتی شگرف گردید. در راستای همین دگرگونی‌ها بود که مکملی نوین برای پرداخت سنتی معرفی گردید و آن چیزی نبود جز پرداخت الکترونیکی<sup>۱</sup>. پرداخت الکترونیکی عبارت است از تراکنش جا به جایی ارزش بین فروشنده، مشتری، بانک و یا به طور کلی بین تمام اعضاء مشمول در یک معامله بر روی بسترها و شبکه‌های الکترونیکی مانند اینترنت، از طریق ابزار و ادوات الکترونیکی همانند کامپیوتر. پرداخت الکترونیکی بدون محدودیت زمانی انجام می‌شود، اما عموماً از نظر مکانی محدود است.

تغییرات به همین جا ختم نگردید. با فراهم آمدن بسترهای جدید ارتباطی مانند شبکه‌های بی سیم و یا شبکه‌های تلفن همراه و همچنین ظهور و گسترش ابزار و ادوات همراه، پرداخت الکترونیکی حصار محدودیت مکانی را شکست و جای خود را به پرداخت همراه<sup>۲</sup> داد. پرداخت همراه، سیستمی است که در آن تراکنش‌های ارزشمند پولی از طریق شبکه‌های بی سیم و با استفاده از ابزار همراه انجام می‌گیرد. پرداخت همراه دارای مزایایی چون عدم وابستگی به مکان کاربر و زمان، در دسترس بودن، و صرفه جوئی در منابع است. هر چند محدودیت‌هایی چون پهنای باند ارتباطی محدود، عمر کوتاه باتری و محدودیت‌های فنی موجود بر روی ابزار همراه جزء لاینفک این نوع پرداخت می‌باشد.

کیف پول همراه<sup>۳</sup> یکی از کاربردهای جدید پرداخت همراه می‌باشد که قابلیت جایگزینی کیف پول معمولی و بسیاری از کاربردهای دیگر را دارد. کیف پول همراه کاربردی است پیشرفته شامل تراکنش‌های همراه، و سایر موارد موجود در کیف پول معمولی. در واقع کیف پول همراه برنامه‌ای است که بر روی تلفن همراه ذخیره شده و به کاربران امکان انجام انواع تراکنش‌های مالی را می‌دهد. کیف پول همراه بر روی فناوری‌ها و خدمات ارتباطی مختلفی نظیر ارتباط حوزهٔ نزدیک (NFC)<sup>۴</sup>، بلوتوث، پیامک (SMS)<sup>۵</sup> و یا WAP<sup>۶</sup> قابل طراحی و پیاده سازی است که هر کدام مزایا و چالش‌های خاص خود را دارند. معمولاً انجام این تراکنش‌ها نیازمند اتصال به شبکهٔ مخابراتی و اینترنتی حین عملیات پرداخت است که همواره مورد تأیید و پسند کاربر نیست. به علاوه، پرداخت هزینهٔ اتصال به شبکه برای هر تراکنش مقرون به صرفه نمی‌باشد. بسیار اتفاق می‌افتد که کاربران در هنگام

<sup>۱</sup> electronic payment(e-payment)

<sup>۲</sup> mobile payment(m-payment)

<sup>۳</sup> mobile wallet

<sup>۴</sup> Near Field Communication (NFC)

<sup>۵</sup> Short Message Service (SMS)

<sup>۶</sup> Wireless Application Protocol (WAP)



استفاده از کیف پول همراه خود به شبکه‌هایی نظیر اینترنت دسترسی نداشته و یا به دنبال دریافت خدمات اقتصادی تر برای این قبیل پرداخت‌ها باشند. بنابراین باید این امکان فراهم آید تا کاربران در لحظه پرداخت نیازمند اتصال به شبکه نباشند.

از آن گذشته، برای طراحی یک سیستم پرداخت موفق (در قالب کیف پول همراه و یا سایر اشکال پرداخت) لازم است تا مواردی چون ترجیحات و علاقه مندی‌های کاربران، فرهنگ اجتماعی، توانایی‌های فنی و نیازمندی‌های قانونی در نظر گرفته شود که همه این موارد و سایر چالش‌های موجود مانند سادگی، قابلیت استفاده، سرعت و هزینه، طراحی یک سیستم پرداخت همراه موفق را به موضوعی حساس و چالشی تبدیل نموده است. یکی از مهمترین چالش‌های موجود در طراحی یک سیستم پرداخت، تأمین امنیت پرداخت است. از آنجا که در عملیات پرداخت، ارزش و یا اعتبار منتقل می‌شود، کاربران تا زمانی که به سیستم اعتماد کامل نداشته باشند؛ حاضر به استفاده از آن در سطح وسیع نخواهند بود. برای ایجاد امنیت در سیستم‌های پرداخت همراه، روش‌ها و راهکارهای زیادی همچون استفاده از امضاء رقمی<sup>۱</sup>، ساز و کارهای رمزنگاری<sup>۲</sup> و یا توابع چکیده ساز<sup>۳</sup> ارائه گردیده است که از آنها برای تضمین خدمات امنیتی چون محرمانگی داده<sup>۴</sup>، تمامیت داده<sup>۵</sup>، احراز اصالت<sup>۶</sup>، کنترل دسترسی<sup>۷</sup> و انکارناپذیری<sup>۸</sup> استفاده می‌شود. هر پرداختی که بتواند خدمات امنیتی فوق را پیاده‌سازی نماید در زمره پرداخت‌های امن قرار می‌گیرد. مقوله دیگر حائز اهمیت، این است که ایجاد امنیت نباید لطمه ای به کارایی سیستم وارد نماید. سیستم زمانی کاربردی می‌شود که امنیت و کارایی در کنار هم پیاده سازی شوند.

اکثر طرح‌های پیشنهادی در زمینه پرداخت همراه از رمزنگاری نامتقارن<sup>۹</sup> یا کلید عمومی<sup>۱۰</sup> برای تأمین امنیت استفاده می‌نمایند. گرچه کلید عمومی امنیت را در سطح قابل قبولی تضمین می‌نماید؛ اما برای پیاده سازی آن بر روی ابزار همراه با محدودیت‌های فنی ذاتی، کمی احتیاط لازم است. البته الگوریتم‌های سبکی در این زمینه ارائه شده که بر روی ابزار همراه قابل پیاده سازی و استفاده می‌باشند. با این حال انتخاب این نوع رمزنگاری برای تأمین امنیت بر روی ابزار و ادوات همراه موضوعی است که نیاز به بررسی بیشتر دارد.

در نقطه مقابل، رمزنگاری متقارن<sup>۱۱</sup> است که از نظر هزینه محاسباتی بسیار ساده تر از رمزنگاری نامتقارن بوده و می‌تواند گزینه مناسبی برای تأمین امنیت در سیستم‌های پرداخت همراه باشد. نکته حائز اهمیت در استفاده از این نوع رمزنگاری وابستگی امنیت طرح به امنیت کلید است که باید بخوبی تأمین شود.

<sup>1</sup> digital signature

<sup>2</sup> cryptography mechanism

<sup>3</sup> hash functions

<sup>4</sup> data confidentiality

<sup>5</sup> data integrity

<sup>6</sup> authentication

<sup>7</sup> access control

<sup>8</sup> non repudiation

<sup>9</sup> asymmetric cryptology

<sup>10</sup> public key

<sup>11</sup> symmetric cryptography

## ۱-۲- تعریف مسئله

در این بخش به تعریف مسئله پرداخته تا ضرورت و کاربرد تحقیق، مشخص شده و خط مشیء طراحی پروتکل برای کیف پول همراه که هدف نهایی این تحقیق می باشد ترسیم گردد.

در کشور ایران، پرداخت همراه همگام با بانکداری همراه رشد ننموده و اکثر بانکها و مؤسسات مالی کشور بانکداری همراه را به عنوان خط مشیء خود قرار داده و به ارائه طرحهایی پرداخته اند که صرفاً ارتباط کاربر با بانک را تحت پوشش قرار می دهد؛ در حالی که پرداخت همراه تراکنش های بین فروشنده با مشتری و یا بین مشتری با مشتری را نیز شامل می گردد.

اکثر طرح های موجود نیز نیازمند ارتباط بر خط با سرور بانک یا عضو سوم مورد اعتماد در حین پرداخت هستند. این بدان معنی است که در لحظه پرداخت باید هم دو عضو مشمول به شبکه متصل باشند؛ حال آنکه همه جا و در همه زمان این امکان فراهم نیست. مسافری را در نظر بگیرید که بعد از رسیدن به مقصد می خواهد با استفاده از کیف پول همراه خود کرایه تاکسی را پرداخت نماید. در مکانی که مسافر پیاده شده است (مثلاً پارکینگ یک هتل)؛ هیچ کدام از تجهیزات همراه او سیگنالی را از شبکه دریافت نمی نمایند. از طرفی این ارتباط بر کاربر هزینه تحمیل می نماید. به همین دلیل، انجام تراکنش های خرد برای کاربر به صرفه نبوده و عملاً برای پرداخت های کلان از این طرح ها استفاده می شود. مسئله امنیتی این طرح ها نیز جای بحث دارد.

## ۱-۳- هدف

هدف از ارائه این پایان نامه، طراحی پروتکلی امن برای کیف پول همراه با بهره گیری از فناوری پیامک و اینترنت در قسمت بر خط<sup>۱</sup> و استفاده از فناوری بلوتوث در بخش برون از خط<sup>۲</sup> می باشد. کاربر می تواند با استفاده از این کیف پول و از طریق گوشی تلفن همراه پرداخت را انجام دهد. به همین دلیل این کیف پول به صورت نظیر به نظیر (P2P)<sup>۳</sup> طراحی شده است؛ به طوری که کاربر برای پرداخت، نیازمند اتصال به عضو سوم مورد اعتماد نیست. نوع پرداخت همراه مورد استفاده، پرداخت خرد<sup>۴</sup> و مبتنی بر انتقال نشانه (توکن<sup>۵</sup>) است. در این طراحی خدمات امنیتی محرمانگی داده، تمامیت داده، احراز اصالت، کنترل دسترسی، انکارناپذیری و سایر ویژگی های افزون امنیتی در نظر گرفته شده است.

<sup>1</sup> on line

<sup>2</sup> off line

<sup>3</sup> Pree to Pree (P2P)

<sup>4</sup> micro payment

<sup>5</sup> token

## ۱-۴- ساختار کلی پایان نامه

پایان نامه پیش رو حاوی ۵ فصل است. فصل اول شامل مقدمه، تعریف مسئله و هدف پایان نامه می‌باشد. در فصل دوم، تعاریف پایه ای نظیر تجارت همراه<sup>۱</sup>، پرداخت همراه، مزایا، محدودیت‌ها، روند رشد آن، معرفی کیف پول و امنیت پرداخت بیان می‌گردد. در این فصل سعی شده که کلیه مفاهیم بکارگرفته شده در تشریح پایان نامه، مورد بررسی قرار گیرد.

از آنجا که تمرکز پایان نامه بر روی پرداخت‌های خرد است؛ فصل سوم به معرفی، تشریح پرداخت‌های خرد و مطالعه موردی بر روی تعدادی از این پرداخت‌ها اختصاص می‌یابد. به منظور مقایسه بهتر، معیارهایی جهت ارزیابی بیان گردیده و پرداخت‌ها در قالب این مجموعه از معیارها بررسی و تحلیل می‌شوند.

فصل چهارم حاوی تشریح پروتکل پیشنهادی اعم از ساختار کلی، جزئیات سیستم، بررسی، پیاده سازی و انتخاب الگوریتم‌های واجد شرایط برای استفاده در پروتکل، انتخاب بسترها و فناوری‌های ارتباطی مناسب می‌باشد. در این فصل پروتکل پیشنهادی با استفاده از معیارهای عنوان شده در فصل سوم مورد ارزیابی قرار گرفته و با سایر پرداخت‌های فصل پیشین مقایسه می‌گردد.

فصل پنجم یا فصل پایانی شامل خلاصه ای از اهداف پایان نامه و یافته‌های آن می‌باشد. جمع بندی، نوآوری و پیشنهادات آتی در حیطه موضوع این پایان نامه در این فصل گنجانده شده است.

---

<sup>۱</sup> mobile commerce(m-commerce)

## فصل ۲:

### مفاهیم پیش زمینه