**رساله‌ی دکتری: داود نوری، ۱۳۹۹**

# امنیت برای RFID با استفاده از رمزنگاری منحنی بیضوی برای سیستم‌های پزشکی مبتنی بر اینترنت اشیاء

چکیده

اینترنت اشیا از اجزای مختلفی تشکیل شده است که با استفاده از این اجزا، همه موجودات می‌توانند با استفاده از اینترنت داده‌های خود را ارسال کنند. همگام با رشد روز افزون اینترنت اشیا، بکارگیری روش‌های مناسب برای برقراری ارتباطات امن در سیستم‌های مراقبتی و بهداشتی امری بسیار حیاتی است. اتخاذ مکانیزم‌های بهینه با امنیت بالا برای این منظور بیش از پیش در کارآیی سیستم‌های اطلاعات پزشکی تاثیرگذار بوده و امروزه تحقیقات زیادی در این زمینه در حال انجام است. یکی از مهمترین اجزا در اینترنت اشیا، کارت‌های RIFD هستند که برای ارتباط بین موجودات در محیط استفاده شوند. از آنجایی که کارت‌های RFID کاربردهای مهم و بسیار زیادی در اینترنت اشیا دارند، حملات به این شبکه‌ها در حال توسعه است. اگرچه مطالعات زیادی برای امنیت کارت‌های RFID انجام شده است، ولی بدلیل توسعه روز افزون این شبکه‌ها، مسئله امنیت بیشتر از قبل باید مورد توجه قرار بگیرد. رمزنگاری منحنی بیضوی با توجه به کارایی بالا، هزینه محاسباتی کم و اندازه کوچک کلید، اخیرا مورد توجه محققان زیادی قرار گرفته است و می‌تواند در امنیت کارت‌های RFID بسیار موثر باشد.

در این رساله با هدف بهبود در امنیت کارت‌های RFID، مدل جدیدی مبتنی بر رمزنگاری منحنی بیضوی ارایه شده است که علاوه بر حفظ امنیت، زمان اجرای ضرب منحنی بیضوی کمتر، و هزینه محاسباتی پایین‌تری نسبت به کارهای تحقیقاتی مشابه دارد. همچنین یک راه حل مدیریت کلید برای مشکلات دسترسی پویا در کارت‌های RFID به‌منظور مقیاس‌پذیر کردن شبکه برای سیستم‌های مراقبتی و بهداشتی نیز ارائه شده است. با توجه به ارزیابی ما از امنیت این پروتکل مبتنی بر رمزنگاری منحنی بیضوی، این پروتکل برای برنامه‌های کاربردی که به امنیت بالایی نیاز دارند مناسب می‌باشد. در نهایت، ما مقایسه‌ای از امنیت، هزینه ارتباطات، محاسبات و کارایی برای پروتکل پیشنهاد شده را ارائه می‌دهیم که نشان می‌دهد پروتکل پیشنهادی از لحاظ این معیارها کارآمدی و کارایی بالاتری نسبت به کارهای مشابه قبلی دارد.

**کلیدواژه‌ها:** اینترنت اشیا، سیستم‌های پزشکی، احرازهویت، رمزنگاری منحنی بیضوی، RFID، مدیریت کلید

**شماره‌ی پایان‌نامه:** ۱۲۷۴۸۶۵۱۹۸۶۴۲۷۷۱۳۹۸۱۶۲۲۶۴۵۸۴
**تاریخ دفاع:** ۱۳۹۹/۰۷/۲۳
**رشته‌ی تحصیلی:** مهندسی فناوری اطلاعات
**دانشکده:** فنی و مهندسی

**استاد راهنما:** دکتر حسن شاکری
**استاد مشاور:** دکتر مسعود نیازی ترشیز

## *Ph.D. Dissertation:*

# Security for RFID using Elliptical Curve Cryptography for Internet of Things in Healthcare Environment

Abstract:
The rapid development of IoT technology has led to the usage of various devices in our daily life. Along with the ever-increasing rise of the Internet of Things, the use of appropriate methods for establishing secure communications in health care systems is vital. The adoption of high-security optimal mechanisms for this purpose has been more effective regarding the efficiency of medical information systems; hence, many studies are being conducted in this field today. One of the most important components is the RFID cards that can be used for communication between entities in the environment. In healthcare systems, patient information is critical and nobody should have access to this information. Thus, providing security for these networks is essential. Recently, good researches have been done in the area of authentication for medical information systems, using RFID technology, which has a low computational cost.
In this thesis, we propose a novel method based on Elliptic Curve Cryptography for vital and efficient and scalable authentication between RFID cards, card readers and servers. This proposed method maintains security and has less computational cost and low elliptic curve point multiplication running time compared to similar recent methods.