بخشی از ترجمه مقاله

عنوان فارسی مقاله :

طرحی عملی بر مبنای باقیمانده درجه دوم برای تشخیص هویت و حریم خصوصی در سیستم های RFID موبایل

عنوان انگلیسی مقاله :

A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems

توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

بخشی از ترجمه مقاله

5. Conclusion and future work

In this paper we have a proposed a novel approach toauthentication and privacy in RFID systems based on un-ique quadratic residues. The proposed approach addresses the 3 main drawbacks of current schemes – robust secu-rity, EPC Class-1 Gen-2 compliance and suitability for mo-bile/wireless environments. The proposed approach can successfully validate the tag, reader and back-end server in a RFID system as legitimate parties and is cheaper than other quadratic residues based methods. Our collaborative authentication scheme is suitable for mobile/wireless reader environments where secure channel assumptions are invalid. Importantly, our proposed scheme is suited

to the computational constraints of EPC Class-1 Gen-2 pas-sive RFID tags as it only uses the modular squaring, CRC and PRNG functions that passive RFID tags are capable of and does not require the implementation of hash functions on RFID tags. This differentiates the proposed approach from the schemes proposed by Chen et al. [10] and Yeh et al. [11].

5. نتیجه گیری و کارهای آینده

در این مقاله، ما یک روش جدید برای تشخیص هویت و محرمانگی در سیستم های RFID بر مبنای باقیمانده های درجه دوم یکتا پیشنهاد داده ایم. روش پیشنهادی سه نقص مهم طرح های فعلی را بررسی می کند-امنیت قوی، سازگاری با EPC Class-1 Gen-2 و مناسب بودن برای محیط های موبایلی/بی سیم. روش پیشنهادی می تواند با موفقیت برچسب، بازخوان و سرور را به عنوان قسمت های مورد تایید در یک سیستم RFID اعتبار بخشی کند و از روش های دیگر بر مبنای باقیمانده های درجه دوم ارزان تر است. طرح تشخیص هویت اشتراکی ما برای محیط های بازخوان موبایلی/بی سیم که در آن ها فرض کانال ایمن درست نیست، مناسب است. نکته مهم دیگر آن که، طرح پیشنهادی ما برای محدودیت های محاسباتی برچسب های RFID غیر فعالی EPC Class-1 Gen-2، مناسب است، زیرا تنها از مربع کردن پایه ای، توابع CRC و PRNG استفاده می کند که برچسب های RFID غیرفعال می توانند انجام دهند و نیازی به توابع هش روی برچسب‌های RFID نیست. این مسائل روش پیشنهادی را از طرح های پیشنهادی چن و همکارانش[10] و یه و همکارانش[11] متفاوت می کند.