بخشی از ترجمه مقاله

عنوان فارسی مقاله :

پروتکل تایید دوگانه از طریق به اشتراک گذاری

رمز برای تگ های RFID کم هزینه

عنوان انگلیسی مقاله :

Double Verification Protocol via Secret Sharing

for Low-Cost RFID Tags

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

9. Conclusion

To overcome known security weaknesses and/or privacy omission in previous ultralightweight authentication protocols, we propose UMAPSS. It incorporates the $(2, n)$ Shamir's secret sharing and achieves significant security enhancement. It supplies a robust privacy protection through mechanisms for double verification and mutual authentication. It reduces the overtime security omission using a session control mechanism. It ensures unlinkability and randomization by applying a dynamic update mechanism. Based on typical security characteristics and the ability to resist malicious attacks, our protocol performs favourably.

It is ultralightweight, requiring only two simple bitwise operations on low-cost RFID tags without significantly increasing the burden at both the tag's and the server's ends. It removes triangular function operations, lessening exposure to security issues related to their biased outputs. UMAPSS balances superior security performance and practical competitiveness.

۹. نتیجه گیری

به منظور غلبه بر ضعف های شناخته شده امنیتی و یا نبود حریم خصوص در پروتکل های قبلی تایید هویت، پروتکل UMPASS پیشنهاد داده شده است. این پروتکل الگوریتم به اشتراک گذاری (2,n) مربوط به Shamir را به کار می گیرد و به بهبود امنیتی قابل توجهی دست می یابد. این پروتکل حفاظت قدرتمندی را از طریق مکانیزم های تایید هویت متقابل و دوگانه فراهم می کند. این پروتکل حذف امنیت اضافه کار را با استفاده از مکانیزم کنترل جلسه کاهش می دهد و قابلیت تفکیک و تصادفی سازی را با به کارگیری مکانیزم به روز رسانی پویا تضمین می کند. پروتکل UMPASS براساس مشخصات امنیتی و توانایی مقاومت در مقابل حملات مخرب عملکرد مطلوبی دارد.

این پروتکل بسیار سبک وزن است و تنها به دو عملیات بیتی ساده بر روی تگ های کم هزینه RIFD بدون افزایش قابل توجه بار در تگ و سرور نیاز دارد. این پروتکل عملیات توابع مثلثی را از بین می برد و کمتر در معرض مسائل امنیتی قرار می گیرد. پروتکل UMPASS توازنی میان عملکرد برتر امنیتی و رقابت عملیاتی ایجاد می کند.