رتبه دوم پژوهش‌های کاربردی

گروه تخصصی برق و کامپیوتر

عنوان طرح

ماجول امنیت سخت افزاری بومی صدف

مجری

مرکز پژوهشی پارسا شریف

نماینده

دکتر بهنام ستارزاده

همکاران

سید امین حبیبی، علی جهانیان، حسین همائی، سید محمد سبط، رضا کارکن ورنوسفادرانی، حامد حسین طلایی، جواد زندی و زینب ایرانمنش

شرکت همکار

شرکت ارتباطات سیار ایران، اداره کل ایمنی شبکه

چکیده‌ی طرح

در دنیای امروز، رمزنگاری به عنوان مهم‌ترین راهکار حفظ محرمانگی و کنترل دسترسی به اطلاعات شناخته می‌شود. در نیم‌قرن اخیر روش‌های رمزنگاری رشد چشم‌گیری داشته‌اند. اما نقطه‌ی آسیب‌پذیری این روش‌ها، حفظ محرمانگی کلید رمزنگاری است؛ به صورتی که سطح امنیتی اطلاعات، در گروی کارآمدی سامانه حفاظت از کلید است. در حال حاضر ایمن‌ترین راه برای حفاظت از کلید ذخیره‌ی آن، در یک سخت‌افزار حفاظت شده است. این سخت‌افزار حفاظت شده را ماجول امنیت سخت‌افزاری می‌نامند. در این ماجول از ایمن‌ترین مکانیسم‌های سخت‌افزاری و نرم‌افزاری شناخته شده در علم و مهندسی اطلاعات، برای حفاظت از کلیدهای داخل آن استفاده می‌شود. این ماجول در علم امنیت اطلاعات با اصطلاح «ریشه اطمینان» شناخته می‌شود؛ چرا که تمام سلسله مراتب امنیت سامانه، برای حفاظت کلید به این ماجول اطمینان می کند. در این طرح، ماجول امنیت سخت‌افزاری بومی صدف با پیشرفته‌ترین مکانیسم‌های رمزنگاری و حفاظت از کلید ارائه شده است. این ماجول که مطابق با استانداردهای صنعتی این فناوری طراحی و پیاده‌سازی شده است؛ می‌تواند افق‌های نوینی از امنیت اطلاعات و ارتباطات را برای سامانه‌های بزرگ در سطح ملی نظیر بانک‌ها، اپراتورهای تلفن همراه و سایر سازمان‌ها بگشاید.