www.rcii.ir

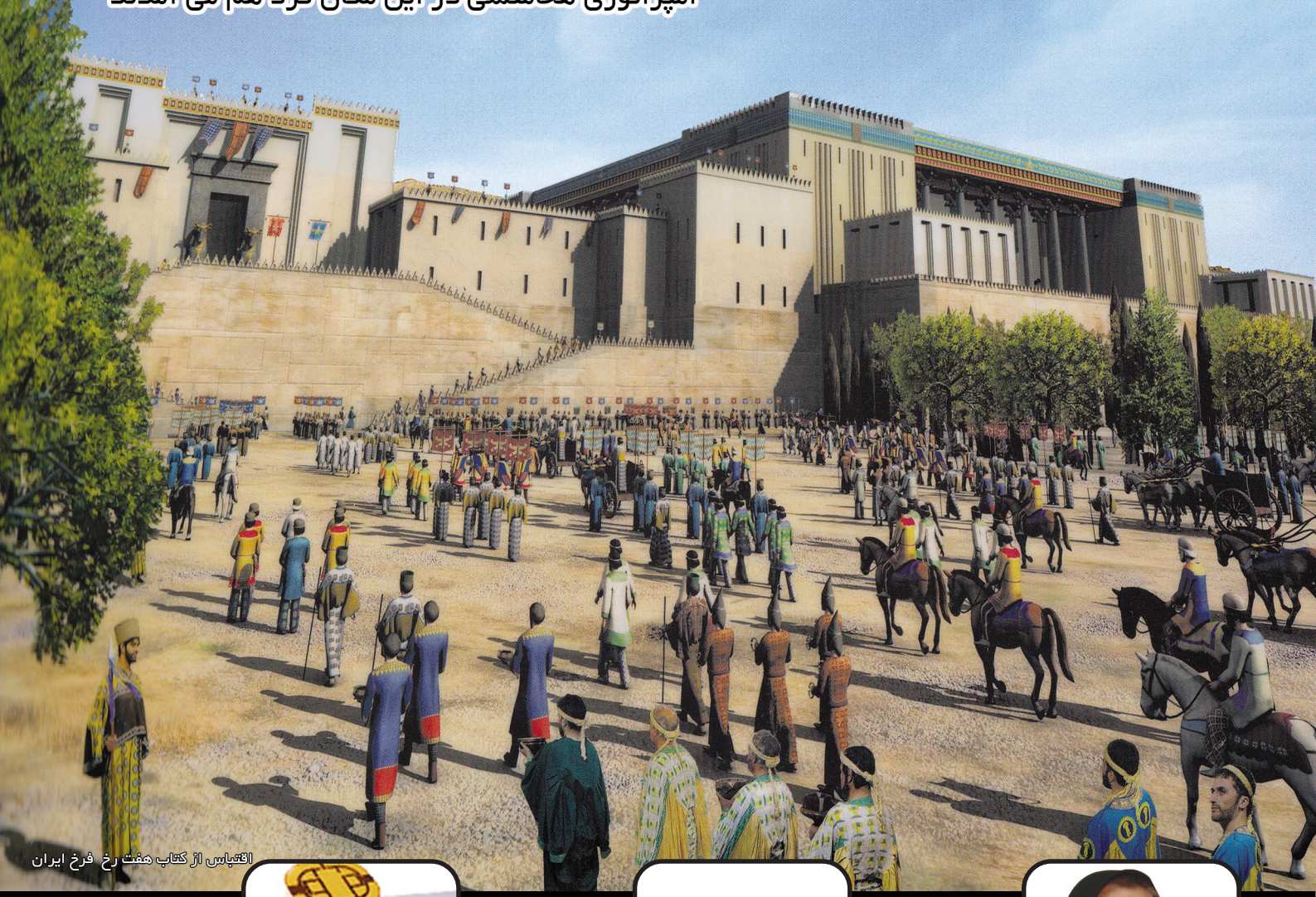
فصلنامه مرکز تحقیقات صنایع انفورماتیک / دوره جدید / شماره۱۷ / زمستان ۱۳۹۲

# گزارش صنایع انفورماتیک

RCII

عید مبارک

همه ساله در مراسم نوروز، نمایندگان ایالت های مختلف امپراتوری هخامنشی در این مکان گرد هم می آمدند



اقتباس از کتاب هفت رخ فرخ ایران

ترسیم نقشه راه برای تصمیم سازی های اثربخش

((سرمقاله))

مرکز تحقیقات صنایع انفورماتیک

RCII

مرکز تحقیقات صنایع انفورماتیک

در کنفراس های ملی


مروری بر کارت هوشمند

((مقاله))

به نام خداوند بخشنده مهربان

**یادداشت نخست**

به قلم مدیر مسئول

## ترسیم نقشه راه برای تصمیم گیری‌های اثر بخش

توسعه صنعتی پایدار وابسته به تصمیمات کارشناسانه و باثبات متولیان حاکمیتی، علی الخصوص مسئولان محترم وزارت صنعت، معدن و تجارت است. سیاست گذاری اصولی و مدبرانه این وزارتخانه می تواند صنایع کشور را در جهت صحیح هدایت کرده و از اتلاف سرمایه ملی جلوگیری کند.

بدون شک سرمایه گذارن انواع بنگاه های تولیدی و خدماتی اعم از دولتی، تعاونی یا خصوصی به دنبال ارائه کالا یا خدمتی موثر به مشتریان و کسب سود هستند. این بنگاه ها برای آغاز فعالیت خود باید از وزارت صنعت، معدن و تجارت مجوزهای لازم را اخذ کنند و پس از اخذ مجوز، نهادهای حاکمیتی نمی توانند به دلایل مختلف از جمله فناوری مورد استفاده در تولید محصول و فشار سایر تولیدکنندگان یا واردکنندگان آن کالا، مجوز اعطایی را لغو یا فقط از بعضی بنگاه ها به دلیل مقبولیت فناوری مورد استفاده، حمایت ویژه نمایند.

پیشنهاد می شود کلیه تشکل های تولیدی، صنعتی و بازرگانی با تشکیل کمیته های تخصصی، نقشه راه حوزه فعالیت خود را ترسیم و به مسئولان محترم وزارت صنعت، معدن و تجارت ارائه دهند تا با ایجاد بستری باکیفیت و سالم جهت تصمیم گیری اثربخش، کارشناسانه و باثبات در طراحی و تدوین برنامه های راهبردی صنعت و تجارت مشارکتی فعال داشته باشند. وزارت صنعت، معدن و تجارت نیز با اتکاء به نظرات کارشناسی و خبرگان صنایع مختلف اقدام به تهیه سند راهبردی توسعه صنعت کشور نموده و آن را منتشر و در اختیار سرمایه گذاران قرار دهد. به این ترتیب ضمن ممانعت از وابستگی سیاست های کلان و راهبردی صنعت کشور به تغییرات مدیریتی در سطوح حاکمیتی، چراغ راهی بلند مدت برای سرمایه گذاران فراهم خواهد شد که به اتکاء آن سرمایه گذاری ایشان در حاشیه امنیت بیشتری قرار می گیرد.


**گزارش صنایع انفورماتیک**

فصلنامه مرکز تحقیقات صنایع انفورماتیک

دوره جدید / شماره۱۷ / زمستان۱۳۹۲

**صاحب امتیاز:** مرکز تحقیقات صنایع انفورماتیک

**مدیر مسئول:** ویدا سینا

**مدیر اجرایی:** افسانه عبادی

**مدیرفنی:** رامین رضایی

**همکاران این شماره:** محمد امین صابریان، علی محمودی، مجتبی خانی هومن مرجانی، مهدی حولکیان

**نشانی:** تهران، خیابان کریم خان زند، خیابان شهید عضدی(آبان جنوبی)، خیابان رودسر،پلاک۳

**تلفن:** ۸۸۹۲۵۹۵۰ (۱۰خط)

**فکس:** ۸۸۹۳۷۶۵۸

**سایت :** www.rcii.ir

مجری طرح فصلنامه:گروه رسانه‌ای مهرتابان/۰۹۱۲۳۰۸۹۳۰۳

[akbarkarimi40@yahoo.com]

**نشانی آزمایشگاه‌ها:**

**آزمایشگاه مرکزی:** تهران، خیابان کریم خان زند، خیابان شهید عضدی(آبان جنوبی)، خیابان رودسر،پلاک۳

**تلفن:** ۸۸۹۲۵۹۵۰ (۱۰خط) **فکس:** ۸۸۹۳۷۶۵۸

**آزمایشگاه بندر عباس:** مجتمع آزمایشگاهی اداره کل استاندارد و تحقیقات صنعتی هرمزگان مستقر در اسکله شهید رجایی

تلفن: ۰۷۶۱۴۵۱۴۲۵۹ فکس:۰۷۶۱۴۵۱۴۲۵۸

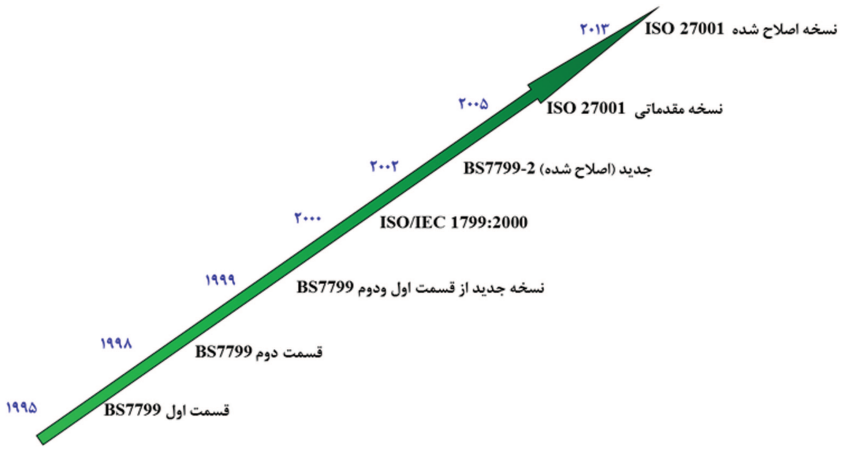
**آزمایشگاه پرند:** شهرک صنعتی پرند، بلوار فن آوری، خیابان گلزار، خیابان گلگشت قطعه D 44

تلفکس:۵۶۴۱۸۸۹۲-۵۶۴۱۸۸۶۴-۵۶۴۱۸۸۶۵

# راهکاری بهینه در پیاده سازی سیستم مدیریت امنیت اطلاعات مبتنی بر ISO 27001:2013

محمد امین صابریان

بررسی رویه بهبود استانداردهای مدیریتی و رویکرد چارچوب هایی نظیر COBIT و ITIL بیانگر این حقیقت است که جهت گیری به سمت افزایش ارتباط استانداردهای مدیریتی با کسب و کار هر سازمان و افزایش سوددهی اقتصادی در کنار تسهیل اجرای امور و افزایش کیفیت و کارایی و دقت به واسطه مکانیزه شدن زیرساخت های بهره گیری از استانداردها است؛ این موضوع در نسخه جدید استاندارد ISO 27001:2013 به وضوح مشهود بوده و مهمترین علامت آن افزودن الزاماتی نظیر استخراج اهداف امنیتی منطبق با کسب و کار سازمان و نیز الزاماتی نظیر پایش و اندازه گیری اهداف امنیتی و مخاطرات است. شکل مقابل نمایی از تاریخچه این استاندارد را نشان می دهد.




■◆■

یکی از بهترین مدل ها در جهت محقق نمودن الزامات استاندارد ISO 27001:2013 و بهبود مستمر امنیت اطلاعات سازمان، استخراج اهداف امنیتی بر اساس ماموریت ها و چشم انداز سازمان هدف و ارائه داشبورد مدیریتی جهت ردیابی وضعیت اهداف امنیتی به صورت لحظه ای است. در داشبورد امنیتی که به صورت نمودارهای گرافیکی برای مدیر سازمان نمایش داده می شود، باید شاخص های مرتبط با هر نمودار که منطبق با هر هدف امنیتی است، از قبل استخراج و وزن دهی شده باشد و ارتباط drilldown بین هر نمودار و مخاطراتی که منجر به تعیین مسیر نمودار شده اند وجود داشته باشد، به طوری که مدیر سازمان در هر لحظه قادر به شناسایی دلایل بالا یا پایین رفتن مخاطرات سازمان خود باشد.

می توان داشبورد مدیریتی را مشابه آخرین نسخه چارچوب COBIT منطبق با چارچوب کارت امتیازدهی متوازن (BSC) طراحی کرد و منظرهایی نظیر رشد و یادگیری، فرایندهای داخلی، مشتری و در نهایت مسایل مالی را مدنظر داشت و مخاطرات را با توجه به آن شناسایی و پایش و اندازه گیری نمود.

در ادامه مهمترین تغییرات نسخه ISO 27001:2013 با نسخه قبلی منتشر شده در سال ۲۰۰۵ ارائه شده است:

■ تغییر بندهای استاندارد و منطبق نمودن آن با سایر استانداردهای مدیریتی

■ درخواست استفاده از یک متدولوژی بهبود مستمر امنیت اطلاعات و حذف الزام استفاده از چرخه دمینگ جهت بهبود مستمر

■ الزام شناسایی زمینه های داخلی و خارجی فعالیت های سازمان شامل انواع استانداردها و روش های اجرای فعالیت ها، طرف های بیرونی مرتبط با سازمان و ... .

■ توسعه شناسایی نیازمندی های امنیتی ذی نفعان به شناسایی نیازمندی های امنیتی کلیه عامل های درونی و بیرونی (بخش های علاقه مند) سازمان که در فعالیت های سازمان نقش دارند.

■ الزام شناسایی شفاف نیازمندی های امنیتی مرتبط با ارتباطات درونی و بیرونی سازمان

■ الزام استخراج اهداف امنیتی منطبق با فعالیت های سازمان که در این راستا استخراج ماموریت، چشم انداز و فعالیت های سازمان در جهت تعیین سطح امن سازی و برنامه ریزی برخورد با مخاطرات بسیار موثر است.

■ هدایت و رهبری سیستم مدیریت امنیت اطلاعات به صورت الزامی بر عهده مدیر ارشد سازمان گذاشته شده است.

■ جایگزین شدن الزام تعیین مالک هر مخاطره به جای تعیین مالک هر دارایی، در این صورت مالک هر مخاطره مسئولیت برخورد با مخاطره را بر عهده خواهد داشت.

■ پیامدها، مخاطرات و فرصت ها جایگزین اقدامات پیشگیرانه شده و اقدامات پیشگیرانه حذف شده است.

■ بر خلاف نسخه قبلی استاندارد که کنترل ها از پیوست A استاندارد انتخاب و کاربردپذیری آنها بررسی می شد در نسخه جدید استاندارد کنترل ها در طی فرایند ترمیم مخاطرات تعیین می شوند.

■ قوی تر شدن الزامات مربوط به کارایی، پایش و اندازه گیری طرح ترمیم مخاطرات و سطح تحقق اهداف امنیتی

■ افزایش اختیارات مرتبط با روش شناسایی مخاطرات و عدم اشاره به الزامات مرتبط با شناسایی تهدیدات و آسیب پذیری ها در استخراج مخاطرات

■ افزایش تعداد حوزه های امنیتی مورد بررسی و کاهش مجموع تعداد کنترل های مربوط به هر حوزه

■ جایگزین شدن اسناد اطلاعاتی به جای مستندات و سوابق

اسناد اطلاعاتی که استاندارد ISO 27001:2013 در متن خود، تهیه آنها را الزام نموده است عبارتند از:

■ قلمرو سیستم مدیریت امنیت اطلاعات (بند ۴.۳)
■ خط مشی امنیت اطلاعات (بند ۵.۲)
■ فرایند ارزیابی مخاطرات امنیت اطلاعات (بند ۶.۱.۲)
■ فرایند ترمیم مخاطرات امنیت اطلاعات (بند ۶.۱.۳)
■ بیانیه قابلیت کاربرد (بند ۶.۱.۳ d)
■ اهداف امنیت اطلاعات (بند ۶.۲)
■ مدارک صلاحیت (بند ۷.۲ d)
■ اطلاعات مستند شده و تعریف شده توسط سازمان که لزوم اثربخشی ISMS را نشان می دهند. (بند ۷.۵.۱b)
■ کنترل ها و طرح ریزی عملیاتی (بند ۸.۱)
■ نتایج ارزیابی مخاطرات امنیت اطلاعات (بند ۸.۲)
■ نتایج ترمیم مخاطرات امنیت اطلاعات (بند ۸.۳)
■ مدارک مرتبط با نتایج پایش و اندازه گیری (بند ۹.۱)
■ مدارک مرتبط با برنامه های ممیزی و نتایج ممیزی (بند ۹.۲g)
■ مدارک مرتبط با نتایج بازنگری مدیریت (بند ۹.۳)
■ مدارک مرتبط با ماهیت عدم انطباق ها و فعالیت های مرتبط انجام شده (بند ۱۰.۱f)
■ مدارک مرتبط با نتایج اقدامات اصلاحی (بند ۱۰.۱g)

سری استانداردهای 27001 شامل تعداد زیادی

ادامه در صفحه بعد

ادامه از صفحه قبل

استاندارد و راهنما هستند که استاندارد اصلی آنها ISO 27001است و این استاندارد به همراه ISO 27002 که به توصیف کنترل های پیوست A استاندارد ISO 27001 می پردازد، در سال ۲۰۱۳ به روز شده اند. استاندارد ISO 27002 به معرفی بهترین نمونه ها برای هر یک از کنترل های استاندارد می پردازد و مشاورین پیاده سازی ISO 27001 با مطالعه و بررسی آن می توانند مصادیق استفاده از هر یک از کنترل های استاندارد در طرح های ترمیم هر مخاطره را بررسی و استفاده کنند، البته اجباری به استفاده از آنها نیست. بر اساس متن استاندارد ISO27001:2013 جهت آشنایی با اصلاحات و تعاریف به کار رفته در استاندارد، به آخرین نسخه از استاندارد ISO 27000 رجوع شود و به منظور آشنایی با زمینه فعالیت های درونی و بیرونی سازمان به بند ۵.۳ از استاندارد ISO 31000:2009 رجوع شود.

پیاده سازی سیستم مدیریت امنیت اطلاعات وابسته به زیرساخت های تکنولوژی، فرایندی، دانش پرسنلی و سطح هزینه ای است که سازمان حاضر به پذیرفتن آن است. مکانیزه کردن امور شناسایی، پایش، اندازه گیری مخاطرات و اهداف امنیتی و طرح های تداوم فعالیت های برخورد با حوادث، وابسته به زیرساخت های تکنولوژی سازمان هدف بوده و با توجه به آن هزینه های خاص خود را طلب می کند، با این وجود با توجه به رویکرد سازمان هدف می توان از نرم افزارهایی مشابه Excel در جهت مدیریت امور و کاهش هزینه ها استفاده نمود که این امر نیازمند بهره گیری از توان پرسنلی با توجه به خط مشی های سازمان هدف است.

مرکز تحقیقات صنایع انفورماتیک با تجربه ای بیش از ۲۰ سال در زمینه انواع استانداردهای مدیریتی و فنی و به عنوان اولین شرکت در ایران که موفق به پیاده سازی سیستم مدیریت امنیت اطلاعات بر مبنای ISO 27001:2005 و اخذ گواهینامه بین المللی آن برای یکی از سازمان های بزرگ تحت قرارداد خود شده است و با پشتوانه بیش از ۱۰۰ پرسنل متخصص و دارا بودن پروانه فعالیت از نظام ملی مدیریت امنیت اطلاعات (نما) به شماره ۱۲۴۱۶ آماده ارائه خدمات مشاوره در جهت پیاده سازی سیستم مدیریت امنیت اطلاعات در سطوح مختلف سازمانی بوده و با دانش کامل نسبت به استاندارد ISO 27001:2013 و سایر استانداردها و چارچوب های استانداردسازی فناوری اطلاعات و تخصص بالا در زمینه طراحی و پیاده سازی شبکه، اجرای آزمون نفوذپذیری و نیز تخصص ارزیابی امنیت محصولات فناوری اطلاعات، آمادگی خود را در جهت پیاده سازی سیستم مدیریت امنیت اطلاعات مبتنی بر ISO 27001:2013 در انواع سازمان‌ها با انواع زیرساخت ها و توانمندی ها اعلام می دارد.

# مروری بر کارت هوشمند

علی محمودی

**چکیده:**

کارت هوشمند[۱]، یکی از مهم ترین ابزارهای تصدیق کاربر و ذخیره اطلاعات محرمانه است و در طراحی آن از الگوریتم های رمزنگاری استفاده می شود. امروزه در بسیاری از کاربردهایی که نیاز به نگهداری و انتقال امن اطلاعات و داده ها، کنترل دسترسی به سیستم های رایانه ای و نیز کنترل دسترسی فیزیکی به محیط های خاص به عنوان کلید الکترونیکی وجود دارد، از کارت های هوشمند استفاده می شود. مهم ترین علل محبوبیت کارت های هوشمند اندازه کوچک، مقاوم بودن در برابر دست کاری[۲] و قابل حمل بودن آن ها است.


## مقدمه

تاریخچه استفاده از کارت های پلاستیکی برای شناسایی افراد به حدود سال ۱۹۵۰ بر می گردد. در آن زمان فقط از بدنه پلاستیکی کارت به سادگی برای نوشتن نام و مشخصات دارنده کارت به صورت حروف برجسته[۳] استفاده می شد و کارت نقشی شبیه به کارت های اعتباری امروزی ایفا می کرد. پیشرفت در زمینه استفاده از کارت ها، با ایجاد نوار مغناطیسی[۴] بر روی کارت که توسط ماشین مخصوصی قابل خواندن و نوشتن بود، سرعت گرفت و وارد مرحله جدیدی شد [۱]. با وجود محبوبیت این نوع کارت ها در صنعت بانکداری و امور مالی ـ اعتباری، سطح امنیتی ارائه شده توسط کارت های مغناطیسی پایین بود. در نتیجه با پیشرفت تکنولوژی نیمه هادی، نسل سوم کارت ها یعنی کارت های هوشمند پا به عرصه وجود نهاد.

## انواع کارت‌های هوشمند

بر اساس نوع تراشه به کار رفته در کارت و نحوه ارتباط بین کارت و کارتخوان[۵]، رده بندی های مختلفی برای کارت هوشمند وجود دارد [۱].

### الف) تقسیم بندی کارت ها بر حسب نوع تراشه

**۱- کارت‌های حافظه‌ای (Memory Cards)**: در کارت‌های حافظه‌ای، تراشه توانایی پردازش و مدیریت اطلاعات را ندارد و فقط داده ها، از طریق پروتکل های هم زمان با کارتخوان، انتقال داده می شوند. کارت تلفن، کارت پارک اتومبیل، کارت بلیط الکترونیکی مترو و اتوبوس و... نمونه ای از کارت های حافظه ای هوشمند هستند.

**۲- کارت های ریزپردازنده دار (Multifunction Cards Microprocessor)**: در این نوع از کارت های هوشمند، تراشه توانایی پردازش و مدیریت اطلاعات را دارد. برای این کار یک تابع یا نرم افزار خاص در تراشه ریزپردازنده، برای مدیریت داده ها از طریق سیستم عامل کارت[۶] قرار می گیرد. کارت های بانکی، کارت سوخت و سیم کارت، نمونه های بارز از این کارت ها هستند.

### ب) تقسیم بندی کارت ها بر حسب روش ارتباط بین کارت و کارتخوان:

**۱- کارت هوشمند تماسی (Contact Smart Card)**: در این نوع کارت ها، ارتباط کارت با کارتخوان از طریق اتصالات الکتریکی که روی بدنه کارت وجود دارد

برقـــرار می شود. استانداردهـــــای ISO/IEC 7816 و ISO/IEC 7810 استانداردهای تدوین شده برای این نوع کارت‌هاهستند. کارت سوخت، گواهی نامه‌های هوشمند و سیم کارت نمونه ای از کارت های تماسی هستند.

**۲-کارت هوشمند غیر تماسی (Contactless Smart Card):** در این نوع کارت‌ها، سیگنال لازم و تغذیه تراشه کارت به جای اینکه از اتصالات روی بدنه کارت تامین شود با القاء سیگنال ها از طریق امواج الکترومغناطیسی و رادیویی (Radio Frequency Identification :RFID) به کارت صورت می گیرد و بین کارت و کارتخوان اتصال فیزیکی برقرار نمی شود. کارت های غیر تماسی اغلب از دو نوع استاندارد ISO/14443 و ISO 693 استفاده می کنند و در کاربردهایی چون کنترل ترافیک در بزرگراه ها، پارکینگ ها و بلیط الکترونیکی اتوبوس و مترو به کار گرفته می شوند.

## استانداردهای کارت هوشمند

**۱- استانداردهای ISO /IEC:** مهم ترین استانداردها در زمینه کارت هوشمند توسط سازمان بین المللی استاندارد(ISO) با همکاری کمیسیون بین المللی صنایع الکترونیکی، IEC تدوین شده‌اند. استانداردهای ISO/IEC موجود در مورد کارت های تماسی به طور خلاصه شامل بندهای یکم الی شانزدهم استاندارد ISO/IEC 7816 بوده و در مورد کارت های غیر تماسی شامل سه استاندارد ISO/IEC 10536، ISO/IEC 14443 و ISO/IEC 15693 است.

**۲-استانداردهای CEN (کمیته اروپایی استاندارد)**

**۳-استانداردهای EMV**

**۴-استانداردهای ETSI**

**۵-استانداردهای GSM بیشتر مربوط به استانداردهای سیم کارت SIM**

**۶-استاندارد Global Platform**

## مباحث رمزنگاری

### الف- زیرساخت کلید عمومی PKI

یکی از موارد بهره گیری از کارت های هوشمند، استفاده از آن ها برای فعال سازی سازوکارهای مرتبط با ارائه اعتماد مبتنی بر زیرساخت کلید عمومی در سازمان و نیز نگهداری زوج کلیدهای کاربران است. از این رو، این دسته از کارت ها باید امکانات مورد نیاز برای تولید کلیدهای رمزنگاری، انجام فرایندهای رمزنگاری، تولید امضای دیجیتال و ارتباط با نرم افزارهای مجهز به زیرساخت کلید عمومی را در اختیار کاربران قرار دهند.

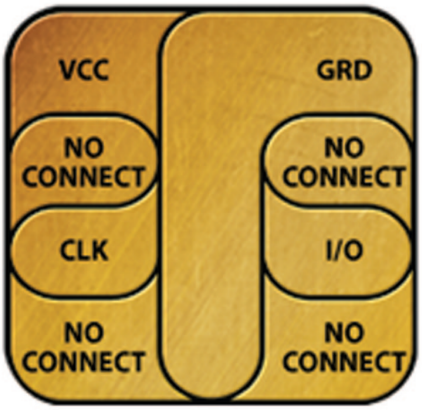
برای ارائه سطح مطلوب کارکردی و امنیتی در حوزه رمزنگاری مورد استفاده در زیر ساخت کلید عمومی، استانداردهای FIPS 140-2 و بخش پانزدهم ISO/IEC 7816 باید توسط کارت های هوشمند پشتیبانی شوند.

### ب- الگوریتم های رمزنگاری

از طرفی برای رمزنگاری اطلاعات در کارت های هوشمند از الگوریتم های رمزنگاری از قبیل RSA، DES، AES و ... که در آنها مولدهای اعداد تصادفی و توابع یک طرفه چکیده ساز به کار گرفته شده است، استفاده می شود. برای اطلاع بیشتر به [۲] رجوع شود.

### ج - حملات کانال جانبی

پیاده سازی الگوریتم های رمزنگاری در سامانه هایی مانند کارت هوشمند، منجر به نشت اطلاعات حساسی از مقادیر میانی الگوریتم می شود. این




اطلاعات حساس از طریق کمیت های فیزیکی موسوم به کانال جانبی نشت می کند و می تواند اطلاعات مخفی سامانه را آشکار سازد. کارت هوشمند و سایر سامانه های رمزنگاری باید به گونه‌ای طراحی شوند که در برابر این تحلیل ها مقاوم باشند. از انواع حملات کانال جانبی، می توان به موارد زیر اشاره کرد[۲]:

۱- حمله تحلیل خطا
۲- حمله تحلیل زمانی
۳- حمله تحلیل توان
۴- حمله تحلیل تشعشعات مغناطیسی و ...

چالش های استفاده از کارت هوشمند در کشور

با توجه به گسترش روز افزون استفاده از کارت های هوشمند در داخل کشور، تقریبا هر روز شاهد ارائه سرویس های جدید امنیتی مبتنی بر کارت هوشمند هستیم. اما آنچه که در حال حاضر، فرایند رشد و گسترش استفاده از کارت های هوشمند را مورد تهدید قرار می دهد، عدم وجود نظارت نظام مند و سازمان یافته بر فرایند تولید، توزیع و بهره گیری از این دسته محصولات است.

باید توجه داشت که برای اطمینان از ارائه سطح مطلوب امنیتی توسط کارت های هوشمند، علاوه بر انجام آزمون های فیزیکی و کارکردی، بایستی آزمون های امنیتی مختلفی نیز بر روی آن ها انجام شود. از جمله آزمون های مهمی که باید بر روی کارت های هوشمند انجام شوند و هم اکنون هیچ مرجعی در کشور، متولی انجام آن ها نیست، عبارتند از:

- آزمون های کارکرد کارت هوشمند مبتنی بر استانداردهای ISO /IEC
- آزمون‌های امنیت ماژول‌های رمزنگاری برای کارت هوشمند.
- آزمون ارزیابی امنیتی کارت های هوشمند
- ارزیابی مقاومت کارت های هوشمند در برابر حملات کانال جانبی

در حال حاضر، مرکز تحقیقات صنایع انفورماتیک، به‌عنوان متولی تدوین شاخص های ارزیابی کارت های هوشمند و انجام آزمون های مزبور، آمادگی ارائه مشاوره های لازم برای نیل به سطح مطلوب امنیتی و کارکردی در حوزه کارت های هوشمند را به سازمان ها و فعالان حوزه فناوری اطلاعات دارد.

## نتیجه گیری

کارت های هوشمند از جمله متداول ترین و در عین حال حساس ترین ابزارهای تصدیق کاربر و ذخیره سازی اطلاعات سری هستند. استفاده از کارت های هوشمند در حوزه های بسیاری افزایش چشمگیری داشته است. سیم کارت و کارت های بانکی، نمونه هایی هستند که نشان می دهند تا چه حد این فناوری زندگی امروزه مردم جهان را تحت تاثیر قرار داده است. در این مقاله، به اختصار به معرفی کارت های هوشمند، دسته بندی، استانداردها و مباحث رمزنگاری مربوط به آن پرداختیم.

## مراجع

[۱] م. ریحانی تبار، "حمله به کارتهای هوشمند با استفاده از اطلاعات نشتی"، کارشناسی ارشد: دانشگاه صنعتی شریف، ۱۳۸۱.
[۲] ج. باقر زاده، "تحلیل توانی کارت هوشمند"، کارشناسی ارشد: دانشگاه صنعتی شریف، ۱۳۹۱.

1. Smart Cards
2. Proof-Tamper
3. Embossed
4. Magnetic Stripe
5. Reader
6. Card OS

خبـــــــر
گزارش انفورماتیک

### حضور مرکز تحقیقات صنایع انفورماتیک در بیستمین کنفرانس اپتیک و فوتونیک ایران و ششمین کنفرانس مهندسی و فناوری فوتونیک ایران

مرکز تحقیقات صنایع انفورماتیک با ارائه دو مقاله در بیستمین کنفرانس اپتیک و فوتونیک ایران و ششمین کنفرانس مهندسی و فناوری فوتونیک ایران شرکت کرد. آقای علی پوراکبر صفار با ارائه دو مقاله با عناوین «بهبود خواص سطحی و آنالیز میکروسکوپی لنزهای تماسی چشم تحت پرتودهی با لیزر اگزایمر» و «بررسی مورفولوژی و خواص سطحی غشای پلی کربنات تحت پرتودهی با لیزر ArF» به‌عنوان نماینده مرکز تحقیقات صنایع انفورماتیک در این کنفرانس حضوری فعال داشت.

مجتبی خانی

# رمزنگاری کوانتومی


## چکیده

رمزنگاری کوانتومی روشی در مقابل رمزنگاری کلید عمومی است که برای تولید و توزیع کلید مورد استفاده قرار می گیرد. رمزنگـــاری کـــوانتومی، به علت پیچیدگی های ریاضی رمزنگاری کلید عمومی و کم اثر شدن این پیچیدگی ها در مقابل اقدامات هکرها مطرح شد. پروتکل های مختلف توزیع کلید بر اساس نوع تکنولوژی کوانتومی مورد استفاده به دو دسته پروتکل های مبتنی بر اصل عدم قطعیت Heisenberg و پروتکل های مبتنی بر همبستگی کوانتومی تقسیم می شوند که در این مقاله به بررسی کلی رمزنگاری کوانتومی و یکی از پروتکل های مبتنی بر اصل عدم قطعیت Heisenberg و یکی از پروتکل های مبتنی بر همبستگی کوانتومی[1] پرداخته خواهد شد.


## مقدمه

به عمل پنهان کردن اطلاعات، رمزنگاری گفته می شود که هدف از آن انتقال اطلاعات به صورت امن است. یکی از راه های ایجاد امنیت در انتقال پیام استفاده از کلید های مشترک است. اگر از رمزنگاری سنتی بگذریم، رمزنگاری کنونی را می توان به دو دسته ی کلاسیک و نوین تقسیم بندی کرد. منظور از رمزنگاری کلاسیک، رمزنگاری منسوخ شده نیست. از روش های رمزنگاری کلاسیک می توان به روش هایی که در آن از الگوریتم هایی مانند DES استفاده می شود، نام برد. استفاده از این الگوریتم ها به علت وابستگی ریاضی کلیدها به یکدیگر قابل رمزگشایی است. محققان IT با موفقیت نشان داده اند که اصول فیزیک کوانتومی و رمزنگاری کوانتومی در شبکه های نوری قادر به محافظت بهتر از ارتباطات است.

رمزنگاری کوانتمی اولین بار توسط Stephen Wiesner در دهه ۱۹۷۰ مطرح شد. در سال ۱۹۹۱ Artur Ekert دانشجوی دوره دکتری در دانشگاه Oxford، روش دیگری برای رمزنگاری کوانتومی ارائه کرد. این نکته قابل ذکر است که رمزنگاری کوانتومی فقط برای تولید و توزیع کلید استفاده می شود و این روش برای رمزنگاری اطلاعات و انتقال آنها کاربردی ندارد. برای بررسی دقیق رمزنگاری کوانتومی و اینکه با اصطلاحات و مفاهیم اولیه آشنا شوید ابتدا مختصری به بررسی امواج الکترومغناطیسی و کوانتوم می پردازیم؛ سپس در رمزنگاری کوانتومی و ایجاد و توزیع کلید در این رمزنگاری بررسی عمیق تری خواهیم داشت.

## امواج الکترومغناطیس

امواج الکترومغناطیسی، رده ای از امواج با مشخصات زیر است:

- امواج الکترومغناطیسی دارای ماهیت و سرعت یکسانی هستند؛
- در طیف امواج الکترومغناطیس شکافی وجود ندارد، یعنی هر فرکانس دلخواه را می توان تولید کرد.
- این امواج برای انتشار خود نیاز به محیط مادی ندارند.
- امواج الکترومغناطیسی جزو امواج عرضی هستند.

از جمله منابع زمینی امواج الکترومغناطیسی می توان به امواج دستگاه رله تلفن، چراغ های روشنایی و غیره اشاره کرد.

## فوتون

فوتون به عنوان ذره بنیادینی است که واحد کوانتومی نور یا هر نوع تابش الکترومغناطیسی محسوب می شود. هر فوتون مقدار معینی انرژی، اندازه حرکت و اندازه حرکت زاویه ای یا اسپین[2] دارد.

## قطبش[3] (پولاریزاسیون)

قطبش یکی از خاصیت های هر موج الکترومغناطیسی مثل نور است. قطبش نور نخستین بار توسط Huygens در سال ۱۹۶۰ میلادی کشف شد. از قطبش می توان استفاده های فراوانی مثلا در زمینه رمزنگاری کوانتومی نمود. در ادامه بیشتر به این موضوع پرداخته خواهد شد.

## اصول رمزنگاری کوانتومی

همانطور که گفته شد امواج الکترومغناطیسی می توانند قطبیده[4] شوند. قطبیدگی بنابر قرارداد با جهت میدان الکتریکی تعریف می شود که در آن یا جهت نوسانات میدان الکتریکی ثابت است یا به شکل معینی تغییر می کند. اگر در فرآیند قطبیدگی دقت کافی شود می توان فرآیند ایجاد فوتون ها را به گونه ای قرار داد که همیشه فوتون هایی با قطبش های عمودی و افقی ایجاد شوند.

یک قطبش گر یا پولارایزر[5] وسیله ای است که تنها اجازه عبور نور با جهت قطبیدگی خاص را می دهد. بنابراین اگر نور کاملاً قطبیده نشده باشد تنها نیمی از آن از قطبش گر عبور می کند.

همانطور که گفته شد هر فوتون اندازه حرکت زاویه ای یا اسپین دارد. در این نظریه فوتون مستقل از اینکه چه قطبش اولیه ای داشته یا از قطبش گر رد می شود یا خیر، اما اگر رد شد با محور قطبش گر هم خط می شود.

## اصل عدم قطعیت Heiseberg

نظریه کوانتومی بیشتر بر این موضوع استوار است که بعضی از کمیت هایی که در فیزیک کلاسیک پیوسته در نظر گرفته می شوند، در حقیقت کوانتیده یا گسسته هستند. به طور خلاصه تنها دو نوع توصیف در مورد یک ذره مادی یا یک فوتون وجود دارد: یکی توصیف موجی و دیگری توصیف ذره ای. بدین صورت که به یک ذره می توان هم خصوصیات مادی (مانند اندازه حرکت و مکان) هم خصوصیات موجی (مانند طول موج و بسامد) نسبت دهیم. تابش الکترومغناطیسی هم جنبه های موجی و هم جنبه های ذره ای را نشان می دهد. نظریه عدم قطعیت Heiseberg را می توان در دو حالت زیر بیان کرد:

۱) اگر تابش الکترومغناطیسی را به زبان ذرات بیان کرده و مکان فوتون را در هر لحظه با دقت کامل تعیین کنیم در آن صورت عدم قطعیت در مکان و زمان صفر

می شود اما از طرف دیگر عدم قطعیت در آنچه به موج فوتون نسبت داده می شود (مانند طول موج) بی نهایت بزرگ است.

۲)از طرفی دیگر اگر بتوانیم آنچه به موج فوتون منسوب است را دقیق مشخص کنیم در این صورت عدم قطعیت در موج فوتون صفر شده و مکان فوتون نامشخص خواهد بود.

## همبستگی کوانتومی

همبستگی کوانتومی یکی از پدیده های عجیب کوانتومی است که می تواند میان دو ذره که نسبت به هم فاصله دارند ارتباط ایجاد کند به شکلی که هر نوع تغییر در یکی از این ذره ها بلافاصله در ذره دیگر نیز تغییر به وجود می آورد، حتی اگر هر یک از این ذره ها در یک سوی جهان قرار داشته باشند.

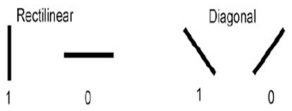
## رمزنگاری کوانتومی

در این بخش به قسمت اصلی بحث می رسیم. همانطور که قبلا هم گفته شد رمزنگاری کوانتومی تنها برای تولید و توزیع کلید استفاده می شود. این کلید در مرحله های بعدی می تواند همراه با هر الگوریتم رمزنگاری برای تبدیل پیام به رمز یا بالعکس استفاده شود. رمزنگاری کوانتومی به هر دو طرف ارتباط این امکان را می دهد که کلید رمز خود را از طریق کانال خصوصی کاملاً امنی انتقال دهند.

برای تولید و توزیع کلید های کوانتومی می توان از پروتکل های BB 84، B 92، SARG04، E91 و BBM 92 استفاده کرد. در ادامه به بررسی پروتکل BB84 که بر اساس اصل عدم قطعیت Heisenberg و پروتکل E91 که مبتنی بر همبستگی کوانتومی هستند، می پردازیم.

پروتکل BB84 مبتنی بر اصل عدم قطعیت Heisenberg این پروتکل توسط Bennet و Brassard در سال ۱۹۸۴ ارائه شد که مبتنی بر اصل عدم قطعیت Heisenberg است. بنابر این اصل که در بخش های قبلی هم به آن اشاره شد، وقتی در اندازه گیری قطبش فوتون جهت اندازه گیری خاصی را انتخاب می کنیم این انتخاب تمام اندازه گیری های بعدی را تحت تاثیر قرار می دهد. به عنوان مثال بدون اینکه بدانیم فوتون دارای چه حالت اولیه ای است، اگر جهت عمودی را برای اندازه گیری قطبش یک فوتون انتخاب کنیم فوتون با قطبش عمودی از قطبش گر رد می شود و قطبش افقی اصلا رد نمی شود. حال اگر اندازه گیری دیگری در زاویه ۴۵ درجه از اندازه گیری اول انجام دهیم احتمال عبور فوتون از قطبش گر دوم دقیقا $\frac{1}{2}$ است و اینگونه بیان می کنیم که قطبش گر اول اندازه گیری قطبش گر دوم را کاملا تصادفی می کند. بنابراین در صورتی می توان جهت این قطبش را تشخیص داد که یک قطبش گر با صفر تا ۹۰ درجه انتخاب گردد. زیرا یک قطبش گر ۴۵ یا ۱۳۵ درجه نیز یک خروجی با همین قطبش ها می دهد. به شکل زیر توجه کنید. همانطور که در شکل دیده می شود دو جفت پایه را می توان تعریف کرد:

-پایه قائم (⊞) با دو محور عمودی یا افقی (Rectilinear)
-پایه قطری (⊠) با دو محور ۴۵ درجه یا ۱۳۵ (یا ۴۵-) درجه (Diagonal)




## نحوه کد گذاری

به طور کلی با توجه به توضیحات داده شده، ارسال کننده با استفاده از منبع، یکی از چهار حالت قطبش بالا (صفر، ۴۵، ۹۰، ۱۳۵) را برای گیرنده ارسال می کند. در طرف دیگر از گیرنده برای اندازه گیری قطبش استفاده می شود.

## نمونه عبور فوتون ها از قطبش گر

گیرنده نتیجه اندازه گیری را ذخیره می کند. در ادامه گیرنده با استفاده از کانال عمومی، نوع فیلتر های اندازه گیری خود (Rectilinear و Diagonal) را بیان می کند. در تمام این مراحل نتیجه اندازه گیری توسط گیرنده پنهان نگه داشته می شود. سپس فرستنده نیز به گیرنده درباره اینکه کدام فیلتر گیرنده درست بوده اطلاع می دهد. تنها در حالتی که فرستنده و گیرنده از نوع یکسانی برای اندازه گیری استفاده کرده باشند، می توان مطمئن بود که اندازه گیری درستی انجام گرفته است. با استفاده از اندازه گیری های مشترک بین فرستنده و گیرنده و در نهایت به بیت تبدیل شدن آنها، کلید ساخته می شود.

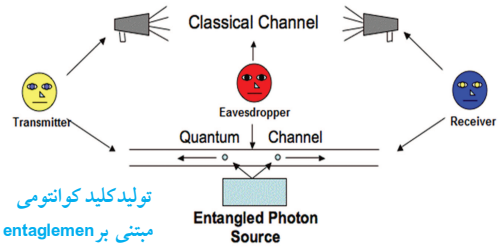
$$\begin{cases} \text{“1”} = |\nearrow\rangle \\ \text{“0”} = |\nwarrow\rangle \end{cases} \quad \begin{cases} \text{“1”} = |\updownarrow\rangle \\ \text{“0”} = |\leftrightarrow\rangle \end{cases}$$

| فرستنده | ⊞ | ⊠ | ⊠ | ⊠ | ⊞ | ⊠ | ⊞ | ⊠ | ⊞ | ⊠ |
|---|---|---|---|---|---|---|---|---|---|---|
| | ↕ | ↖ | ↖ | ↗ | ↕ | ↖ | ↔ | ↗ | ↔ | ↗ |
| | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| | | | * | * | | | | * | | * |
| گیرنده | ⊠ | ⊠ | ⊞ | ⊠ | ⊞ | ⊠ | ⊞ | ⊞ | ⊞ | ⊞ |
| | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| Raw Key⇒ | | 0 | | 1 | 1 | 0 | 0 | | 0 | |

## نحوه ایجاد و تبادل کلید در BB۸۴

### پروتکل E 91 مبتنی بر همبستگی کوانتومی

در سال ۱۹۹۱، Artur Ekert پروتکل جدیدی برای توزیع کلید ارائه کرد. این پروتکل از یک کانال کوانتومی و منبع تولید تک فوتون استفاده می کند. عملکرد این پروتکل به این صورت است که دو زوج همبستگی از یکدیگر تفکیک شده و هر یک از فرستنده و گیرنده یکی از آن دو زوج را دریافت می کنند. با توجه به شکل، هر یک فیلتری برای اندازه گیری جزئی دریافتی خود استفاده می کنند. این پروتکل نیز مانند پروتکل BB84 در قسمت دوم عملکردی خود تبادلاتی در کانال کلاسیک انجام می دهد تا فیلتر های اندازه گیری هر دو طرف مشخص گردد. در نهایت به ازای هر اندازه گیری که فرستنده و گیرنده از فیلتر یکسانی استفاده می کنند باید انتظار نتیجه ای متضاد بر اساس قوانین همبستگی کوانتومی داشته باشند. این موضوع به این معناست که هر دو طرف تبادل، اندازه گیری های خود را مثل قبل تفسیر می کنند با این تفاوت که رشته بیتی هر یک از آن دو، مکمل باینری دیگری است. در این صورت اگر یکی از طرفین کلید خود را معکوس کند، یک کلید مخفی بین آن دو به اشتراک گذاشته شده است.




## نتیجه گیری

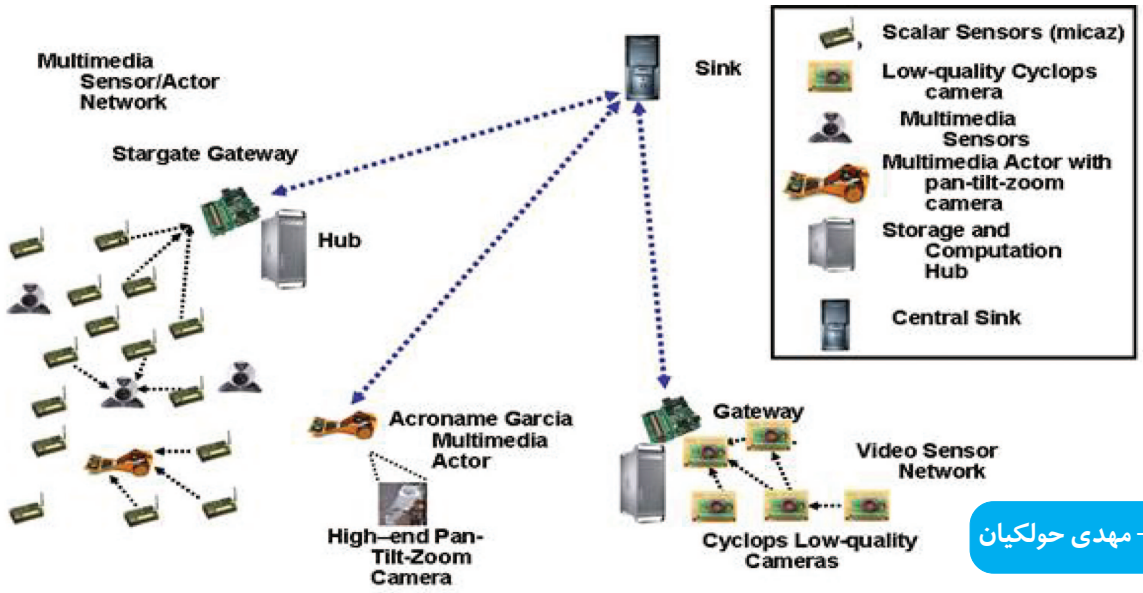
رمزنگاری کوانتومی مانند همتای کلاسیک خود نیاز به یک کلید مشترک برای رمزگذاری و رمزگشایی پیام ها دارد. در این مقاله دیدی از رمزنگاری کوانتومی و پروتکل های تولید و توزیع کلید کوانتومی ایجاد شد. فقط با بودن یک کانال کلاسیک و یک کانال کوانتومی ناامن، این امکان بوجود خواهد آمد تا کلیدی مخفی برای ارسال پیام های رمزشده بین فرستنده و گیرنده به اشتراک گذاشته شود.

## منابع

[1] Shon Harris, CISSP All in one, sixth edition, 2013
[2] C. H. Bennett, G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175-179, 1984
[3] Quantum Cryptography : On the Security of theBB84 Key-Exchange Protocol, Thomas Baign`eres
[4] Quantum Key Distribution Protocols and Applications, Sheila Cobourne, 8th March 2011
[5] GILLES VAN ASSCHE, QUANTUM CRYPTOGRAPHY ANDSECRET-KEY DISTILLATION, 2006
[6]http://daneshnameh.roshd.ir/
[7] http://www.iranjoman.com/
[8] http://www.quantiki.org/wiki/BB84_and_Ekert91_protocols
[9] http://www.atomki.hu/atomki/TheorPhys/quantumcor.htm
[10] http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/bb84coding.html

1 - Quantum correlation
2 - spin
3 - Polarization
4 - Polarized
5 -polarizer

# شبکه حس گر بی سیم




هومن مرجانی - مهدی حولکیان

## چکیده

شبکه حس گر بی سیم از تعدادی گره های حس گر تشکیل شده است که برای جمع آوری اطلاعات مفید از محیط مورد نظر به کار گرفته می شود. داده های حس شده باید جمع آوری شود و سپس به منظور پردازش و پاسخ به درخواست کاربر نهایی به گره اصلی شبکه فرستاده شوند. از آنجائی که این شبکه از گره هایی با انرژی محدود تشکیل شده است، باید روش هایی برای جمع آوری و اجماع داده با راندمان انرژی بالا به کار گرفته شود تا طول عمر شبکه بالا رود. به کاربردن تکنیک های اجماع داده در هر دور از برقراری ارتباط، باعث کاهش انرژی مصرفی کل سیستم و درنتیجه باعث افزایش طول عمر شبکه خواهد شد. برای این منظور تکنیک های زیادی با توجه معماری شبکه و الگوریتم های مسیریابی مورد استفاده در آن معماری در شبکه های تخت و سلسله مراتبی ارائه شده است.

**کلمات کلیدی:** شبکه حس گر بی سیم، گره حس گر، تکنیک اجماع داده، طول عمر شبکه، شبکه تخت، شبکه سلسله مراتبی.

## مقدمه:

با توسعه و تکامل اتوماسیون سیستم های نظامی، حمل و نقل، صنعت، بهداشت و درمان و غیره، این سیستم ها به محیط پیرامون خود مانند یک محیط جدید با قابلیت تغییرپذیری و هوشمندی نگاه می کنند و مکانیزم کارکرد این سیستم های جدید ابتدا دریافت مداوم داده های محیط اطراف خود و سپس اتخاذ تصمیم در مورد عملکرد خود نسبت به محیط است. مهمترین مسائل در این سیستم ها به طور کلی به صورت زیر دسته بندی می شوند:

۱- جمع آوری داده های مناسب و متناسب برای انجام عملکرد سیستم با توجه به درخواست کاربران از سیستم.

۲- ارزیابی داده های خام به دست آمده از محیط و ایجاد اطلاعات صحیحی از این داده ها.

۳- چگونگی فرموله کردن (معنی دارکردن) آنها برای نمایش به کاربران.

۴- ارزیابی عملکرد انجام شده با توجه به داده های جمع آوری شده و بهبود آن در هر مرحله.

اما از آنجائی که تمامی موارد گفته شده، به چگونگی و نحوه جمع آوری داده ها بستگی دارد، می توان گفت جمع آوری داده های مناسب و متناسب برای انجام عملکرد سیستم، اصلی ترین مسئله برای سیستم های جدید تلقی می شود که این اطلاعات و داده های مورد نیاز از محیط پیرامون توسط شبکه های حس گر بی سیم تهیه می شوند.

### ۱- شبکه حس گر بی سیم

شبکه حس گر بی سیم[۱] معمولاً[۲] از تعداد زیادی گره های حس گر[۲] تشکیل شده است که قادر به برقراری ارتباط با یکدیگر و همچنین با یک گره خارجی به نام سینک[۳] (چاهک) یا ایستگاه (گره) اصلی شبکه[۴] هستند. حس گرها می توانند به طور تصادفی در یک محیط غیرثابت و تغییرپذیر با شرایط سخت، مانند یک میدان جنگ یا در یک محیط ثابت و مشخص کارگذاشته شوند. حس گرها می توانند با یکدیگر ارتباط برقرار کنند و با همکاری هم، یک شبکه ارتباطی مانند یک شبکه تک یا چند مسیره یا یک ساختار سلسله مراتبی[۵] با چندین خوشه[۶] (کلاستر) و رهبر خوشه[۷] (کلاستر هد) تشکیل دهند. سنسورها به طور مرتب از محیط پیرامون خود داده حس می کنند، آنها را پردازش می کنند و به گره اصلی شبکه انتقال می دهند. تعداد تکرارهای ارسال داده و تعداد حس گرهای کارگذاشته شده در محیط معمولا به کاربرد شبکه بستگی دارد.

روی کارآمدن تکنولوژی های جدید در ساخت پردازش گر[۸] و حافظه های[۹] کوچک و کم هزینه و تکنولوژی های جدید رادیویی، محققین را قادر ساخت تا به ساختن گره های حس گر کوچک[۱۰] کم هزینه با قابلیت برقراری ارتباط بی سیم بپردازند. اگر چه این نودها در مقایسه با حس گرهای بزرگ[۱۱] و پرهزینه از نظر انرژی و میزان پایداری بسیار ضعیف تر هستند، اما با به کاربردن صدها یا هزاران گره از آنها می توان شبکه حس گر با کیفیت ساخت.

### ۲- کاربردها و چالش های شبکه حس گر بی سیم

شبکه های حس گر بی سیم برای کاربردهای مختلفی از جمله مسائل نظامی، مشاهده محیط، سیستم های حمل و نقل و غیره به کار می روند. برای هر کابر حس گرهای مخصوصی مانند حس گرهای حساس به درجه حرارت، گرما و غیره مناسب با عملکرد شبکه ساخته می شود.

مهمترین مسئله در گره های حس گر انرژی محدود و پایان پذیر باطری آنها است، این امر باعث ایجاد محدودیت در طور عمر[۱۲] و کیفیت عملکرد شبکه

می شود. به همین دلیل پروتکل هایی که بر روی این شبکه ها اجرا می شوند باید قادر باشند تا منابع (توان باطری) گره ها را به طور سودمند مصرف کنند تا طول عمر شبکه افزایش پیدا کند.

بنابر آنچه که گفته شد، تحقیقات بسیاری بر روی مسئله محدودیت انرژی و مدیریت منابع در شبکه های حس گر بی سیم صورت گرفت و در این راستا پروتکل هایی ارائه شد که تمامی این پروتکل ها (الگوریتم ها) در صدد افزایش طول عمر گره ها، کاهش پهنای باند مورد نیاز با برقراری ارتباطات محلی در بین گره ها و در نهایت افزایش طول عمر شبکه بودند. از آنجائی که داده های تولید شده (حس شده) توسط گره های موجود در شبکه حس گر بی سیم که در مجموع داده ها و اطلاعات شبکه حس گر را تشکیل می دهند، برای پردازش کاربر نهایی بسیار زیاد هستند، به روش هایی برای جمع آوری داده ها و تبدیل آنها به یک سری اطلاعات دارای مفهوم و معنی نیاز است. یک راه ساده برای انجام این عمل «اجماع داده» نام دارد که هدف آن ایجاد یک فیلترینگ مناسب برای حذف داده های اضافه، تکراری و حذف نویزها بر روی داده ها است. برای انجام عمل اجماع داده پروتکل های مختلفی با توجه به معماری و مسیریابی های مختلف در شبکه حس گر بی سیم ارائه شده است که در ادامه به تعریف و توصیف دقیق آنها می پردازیم.

## ۳- پروتکل های اجماع داده براساس معماری شبکه

### ۳-۱- پروتکل های اجماع داده در شبکه های تخت

#### ۳-۱-۱- push diffusion

در این پروتکل تمام حس گرها نقش فعال و یکسانی را دارند و هنگامی که گره سینگ به آنها درخواستی را می فرستد، آغاز کننده انتشار داده هستند. تکنیک اسپین[13] در این پروتکل به کار گرفته شده است. دو ویژگی مهم اسپین که در این پروتکل به کار گرفته شده است عبارت اند از data negotiation و resource adaptation. برای اجرای این پروتکل، گره های حس گر به منظور توصیف آنچه که مشاهده کرده اند، نیازمند یک توصیف کننده هستند.

#### ۳-۱-۲- Two phase pull diffusion

یک پروتکل مجتمع سازی داده energy efficient است که آن را direct diffusion نیز می نامند. این پروتکل در واقع شمایی از مسیریابی data centric است که پایه و اساس آن مبتنی بر به دست آوردن داده در حس گرها است. ویژگی ها و صفات داده ها، پیام های مورد استفاده در شبکه است.

### ۳-۲- پروتکل های اجماع داده براساس خوشه بندی در شبکه های سلسله مراتبی

#### ۳-۲-۱- پروتکل LEACH[14]

پروتکل غیر یکپارچه ای است که گره های حس گر خودشان را به خوشه هایی به منظور فیلتر کردن داده ها تقسیم می کنند و برای هر خوشه یک رهبر خوشه تعریف می شود. در هر خوشه داده ها از گره های حس گر آن خوشه به رهبر خوشه ارسال می شوند و سپس از رهبر خوشه به طور مستقیم یا غیر مستقیم به گره اصلی شبکه ارسال می شود. پیامد این الگوریتم کاهش اطلاعات ارسالی به گره اصلی شبکه است و این امر ناشی از این است که در گره رهبر هر خوشه ابتدا فیلترینگی روی داده های دریافتی از گره های خوشه انجام می شود و سپس ارسال به گره اصلی شبکه انجام می پذیرد.

اگر بخواهیم پروتکل LEACH را به طور جزئی تر مورد بحث قرار دهیم، می توانیم آن را شامل دو فاز بدانیم:

**Setup phase**: شامل سازماندهی شبکه به خوشه ها و تعیین یک رهبر برای هر خوشه است.

**Stead phase**: مجتمع سازی داده در گره های رهبر هر خوشه و سپس ارسال به گره اصلی شبکه است.

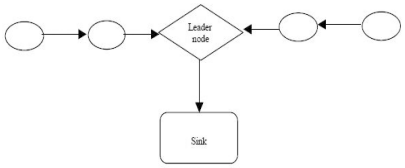
#### ۳-۲-۲- پروتکل HEED[15]

با توجه به محدودیت های پروتکل LEACH و عدم یکپارچگی آن، مکانیزم اجماع داده دیگری به نام HEED مطرح شد که هدف آن ایجاد خوشه هایی سودمند به منظور افزایش طول عمر شبکه است. اصلی ترین فرض به کار گرفته شده در این الگوریتم، توانایی در به کار بردن سطوح انرژی چندگانه در گره های حسگر است. انتخاب رهبر خوشه براساس ترکیبی از میزان انرژی باقی مانده هر گره و میزان مجاورت هر گره به گره های همسایه خود انجام می شود.

### ۳-۳- پروتکل اجماع داده براساس ساختار زنجیر در شبکه های سلسله مراتبی

#### ۳-۳-۱- پروتکل PEGASIS[16]

در این پروتکل گره ها به صورت یک ساختار خطی زنجیروار به منظور اجماع داده سازماندهی می شوند. گره ها ساختار زنجیروار را با به کار بردن یک الگوریتم زیاده خواهانه[17] ایجاد می کنند. این فرم زنجیروار فرض می کند که تمام گره ها از تمام وضعیت شبکه اطلاع دارند. در این ساختار، گره اصلی شبکه معمولاً در مرکز این زنجیر تعریف می شود.




### ۳-۴- پروتکل اجماع داده براساس ساختار درخت[18] در شبکه های سلسله مراتبی

#### ۳-۴-۱- پروتکل PEDAP[19]

در این پروتکل فرض بر آن است که گره ها به صورت غیر یکپارچه و تصادفی در محیط کارگذاشته شده اند. همچنین مکان استقرار آنها ثابت است و گره اصلی شبکه از مکان گره ها در آگاه است. حسگرها می توانند به طور مستقیم با یکدیگر ارتباط داشته باشند و داده های خود را به گره اصلی شبکه ارسال کنند. گره ها به طور مداوم داده هایی را از محیط دریافت می کنند و همیشه داده هایی را در هر دوره از ارتباط برای ارسال دارند. همچنین گره ها داده هایی که از همدیگر دریافت می کنند را با داده های خود مقایسه کرده و سپس به فیلترینگ یا مجتمع سازی آنها می پردازند.

## ۴- نتیجه گیری

در این مقاله ما ابتدا به مساله محدودیت انرژی در شبکه های حس گر بیسیم پرداختیم و سپس فاکتورهای را که راندمان انرژی بالایی را برای ما فراهم می آورند و در نهایت باعث افزایش طول عمر شبکه می شوند معرفی کردیم. در بین این فاکتورها تکنیک های اجماع داده نقش بسیار مهمی را در ایجاد راندمان انرژی بالا و سودمندی انرژی برای ما فراهم می کرد. در نتیجه با توجه به معماری شبکه و الگوریتم های مسیر یابی مورد استفاده در شبکه های بی سیم حس گر بر اساس ساختار شبکه به دسته بندی پروتکل های اجماع داده در سه معماری شبکه های تخت و سلسله مراتبی پرداختیم.

در شبکه های تخت به معرفی دو پروتکل Pull diffusion و Direct diffusion پرداخته و مزایا و معایب آنها را بیان کردیم. در شبکه های سلسله مراتبی اجماع داده را به سه بخش اجماع داده بر اساس خوشه بندی اجماع داده بر اساس ساختار زنجیر و اجماع داده بر اساس ساختار درخت تقسیم بندی کردیم. در دسته اول به معرفی دو پروتکل LEACH و HEED و در دسته دوم به معرفی پروتکل PEGASIS پرداختیم.

در ادامه با توجه به عیوب موجود در پروتکل های اجماع داده فوق به معرفی پروتکل اجماع داده بر اساس ساختار درخت (PEDAP) در شبکه های سلسله مراتبی پرداختیم که با توجه به نتایج شبیه سازی های انجام شده و مقایسه آن با سایر پروتکل ها و مزایای آن نسبت به دیگر روش ها، در حال حاضر به عنوان کارآمد ترین پروتکل اجماع داده محسوب می شود.

پروتکل تمام جنبه های یک شبکه حس گر بی سیم هنگامی که گره اصلی در مرکز شبکه یا دور از گره های شبکه قرار گرفته باشد را در نظر می گیرد و در هر دو مورد از سایر پروتکل ها مزیت دارد و باعث ایجاد طول عمر بیشتری برای شبکه می شود.

1. wireless sensor network
2. sensor nodes
3. sink
4. Base station
5. Hierarchical
6. cluster
7. Cluster head
8. processor
9. memory
10. micro sensor
11. macro sensor
12. life time
13. SPIN
14. low Energy Adaptive clustering Hierarchy
15. Energy Efficient Distributed Clustering Approach Hybrid
16. Gathering Protocol for Sensor Information System Power Efficient data
17. Greedy
18. Tree Based Data Aggregation
19. Power Efficient Data Gathering and Aggregation protocol

# سامانه ارتباط یکپارچه اتصال

## راهکار جامع، یکپارچه و ایمن مخابراتی در بستر فناوری اطلاعات

**اتصال، با یکپارچه سازی ابزارهای متعدد ارتباطی و حضورِ تنها یک رابط کاربری، به راحتی توانسته است کاربران را، از طریق تمامی دستگاهها و تقریباً از هرنقطه جغرافیایی، در دسترس نگاه داشته و پاسخگوی تمام نیازهای ارتباطی سازمان باشد.**


- دارای گواهی سطح بلوغ امنیتی محصول از مرکز تحقیقات صنایع انفورماتیک
- دارای گواهینامه بین‌المللی ISO 9001: 2008 و ISO 14001: 2004
- دارای تأییدیه فنی شورای عالی انفورماتیک کشور


**شرکت طرح و توسعه اتصال یکپارچه** (سهامی خاص)

دفتر مرکزی: تهران، میدان آرژانتین، خیابان احمد قصیر (بخارست)، کوچه ۱۱، شماره ۶ ، طبقه سوم،واحد ۳، کد پستی ۱۵۱۳۷۴۵۸۱۵

تلفن: ۸۸۷۲۱۹۰۰ (۱۰ خط) نمابر: ۸۸۷۲۳۶۷۳

www.ettesal.co info@ettesal.co

# مرکز تحقیقات صنایع انفورماتیک

## بازوی اجرایی سازمان حمایت از حقوق مصرف کنندگان در ارزیابی سازمان های ارائه کننده خدمات پس از فروش

### تاریخچه ارزیابی خدمات پس از فروش محصولات:

با تصویب قانون حمایت از حقوق مصرف کنندگان در سال ۱۳۸۸ و تصویب آیین نامه های اجرایی در سال ۱۳۹۰، ارزیابی خدمات پس از فروش محصولات در زمینه های زیر به صورت رسمی آغاز گردید:

۱- لوازم خانگی، مصنوعات الکتریکی و الکترونیکی، صوتی و تصویری و وسایل ارتباطی

۲- ماشین آلات صنعتی و معدنی

۳- ماشینهای راه سازی، کشاورزی و تجهیزات وابسته

شرکتهای واردکننده به هنگام ثبت نمایندگی شرکتهای خارجی یا در هنگام تمدید آن مورد ارزیابی قرار گرفته و در صورت برخورداری از زیرساختهای مورد تایید ارائه خدمات قادر به ادامه فعالیت می باشند.

### نحوه ارزیابی خدمات پس از فروش:

بعد از ارائه درخواست از سوی شرکت واردکننده یا عرضه کننده و تحویل مدارک مورد نیاز، قرار داد منعقد خواهد شد و سپس ارزیابی از شرکت درخواست کننده که شامل سه بخش بررسی مستندات، نظرسنجی و تحقیقات مشتریان و بازرسی از دفتر مرکزی و نمایندگیهای مجاز شرکت درخواست کننده می باشد انجام می گیرد. پس از انجام ارزیابی های ذکر شده گزارشی از کلیه مستندات و مشاهدات صورت گرفته تهیه شده و برای سازمان حمایت از حقوق مصرف کنندگان ارسال می گردد و سازمان براساس گزارش شرکت بازرسی گواهی تایید خدمات را به شرکت درخواست کننده ارزیابی، ارائه می نماید.

### مزایای ارزیابی خدمات پس از فروش:

- دریافت گواهینامه خدمات مورد قبول اصناف جهت واردات کالا
- اطلاع از نقاط ضعف شرکت و برطرف نمودن آن جهت بهبود عملکرد شرکت
- اطلاع از نظرات مشتریان و رفع نارضایتیهای موجود در نتیجه افزایش سهم بازار
- ارتقاء سطح دانش پرسنل از طریق ارزیابی انجام شده
- ایجاد رویه جدید برای فعالیتهای آتی شرکت

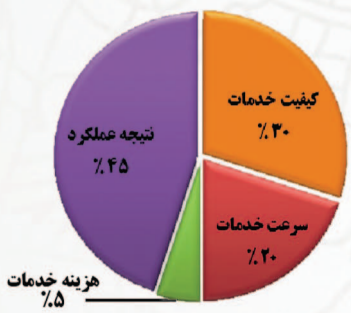
### شاخصهای مورد ارزیابی:

۱. کیفیت خدمات

۲. سرعت خدمات

۳. هزینه خدمات

۴. نتیجه عملکرد



# ایران هفت رخ فرخ

## گهوارهٔ تمدن

با مطالعه و درک جایگاه مهم خاور نزدیک است که ما دینی را که به این بنیانگذاران واقعی تمدن در امریکا و اروپا داریم و مدتهاست به تاخیر افتاده ادا می کنیم.

ویل‌دورانت

## چهارراه تمدن‌ها

فلات ایران، به دلیل موقعیت جغرافیایی طبیعی اش نقطه ای است که می بایست تمام نقل و انتقال‌های قاره عظیم آسیا در آن رخ داده و از آن عبور کرده باشد و همواره نیز عبور کرده است.

ارنست هرتسفلد

## هژمونیت امپراتوری جهانی

اگر بخواهیم دستاوردهای ایران هخامنشی را ارزیابی کنیم ، بی تردید مفهوم 'حکومت جهانی واحد' ، یعنی ادغام ملت ها و فرهنگ های گوناگون جهانی ، مهم ترین میراث آن قلمداد می‌شود.

ریچارد فرای

## دور از ظلمات فرهنگی

عموم دانشمندان مسلمان، چه در رشته‌های دینی چه در علوم عقلی، ایرانی بودند... فقط ایرانیان بودند که خود را وقف پاسداری از معرفت و نگارش آثار روشمند علمی کرده بودند. به این ترتیب، صحت گفته پیامبر اسلام (ص ) آشکار شد که دانش اگر در ثریا هم باشد ایرانیان بدان دست خواهند یافت.

ابن خلدون (فیلسوف عرب)

## منیگری کلمات

ناگهان خود را در رایجه بهشتی و نسیم روح بخش جاودانه ای یافتم که از دشت‌های بارور فارس و دیگر سرزمین‌های ایران زمین می وزید.

یوهان ولفگانگ گوته

## استوار چون سرو

بارزترین نمونه قدرت جذب فرهنگی ایرانیان ، در مورد مغول ها دیده می شود. این قوم وحشی ، که کشتار مردم و انهدام شهرها پی آمد ورودشان به فلات ایران بود، تنها پس از گذشت دو نسل ، آنچنان شیفته تمدن ایران شدند که خود به حامیان جدی و رواج دهندگان فرهنگ ایرانی ، تغییر ماهیت دادند.

دونالد ویلبر

## بازآفرینی تمدن

ایران عصر صفوی دنیایی دیگر بود. دنیایی میان تمدن غرب و چین از یکسو و جهان عرب و آسیای میانه از سوی دیر، ئنیای غرق نور که درخشش گنبدهای فیروزه ای رنگش در پس سایه سار درختان غوغا می‌کرد.

آنری استرلن

اقتباس از کتاب هفت رخ فرخ ایران با هماهنگی خانه فرهنگ گویا