

بررسی روش های رای گیری الکترونیکی

امین برازنده شیروان

www.ketab.ir

سرشناسه	برازنده شیروان، امین، ۱۳۶۵ -
عنوان و نام پدیدآور	بررسی روش های رای گیری الکترونیکی / امین برازنده شیروان.
مشخصات نشر	مشهد: انتشارات رزیتا، ۱۳۹۷.
مشخصات ظاهری	۱۱۶ ص: مصور (بخشی رنگی)، جدول: ۱۴/۵×۲۱/۵ س.م.
شابک	۱۵۰۰۰۰ ریال ۰-۸-۹۸۵۲۲-۰-۹۷۸:۹۷۸
وضعیت فهرست نویسی	فیا
داشت	پشت جلد به انگلیسی: Amin Brazandeh, Electronic voting.
موضوع	رای گیری الکترونیکی
موضوع	Electronic voting
موضوع	انتخابات
موضوع	Elections
موضوع	تکنولوژی و دولت
موضوع	Technology and state
رده بندی کنگره	JF۱۰۰۱/ب۴ ۱۳۹۷
رده بندی دیویی	۶/۳
شماره کتابشناسی ملی	۵۱۰۰۹۲

عنوان کتاب:	بررسی روش های رای گیری الکترونیکی
مؤلف:	امین برازنده شیروان
ناظر فنی چاپ و تولید:	رزیتا میرشاهی
ناشر:	انتشارات رزیتا
ویراستار:	امین برازنده شیروان
صفحه آرای و طراحی جلد:	رزیتا میرشاهی
نوبت چاپ:	چاپ اول
شمارگان:	۱۰۰۰ نسخه
شابک:	۹۷۸-۰-۹۸۵۲۲-۰-۹۷۸
قیمت:	۱۵۰۰۰ تومان
پایگاه اینترنتی:	www.rozitapub.ir
پست الکترونیکی:	info@rozitapub.ir

انتشارات رزیتا: مشهد، رضا شهر، شهرک طالقانی، ارغوان ۵ پلاک ۴۳

کل فرآیند انتخابات شامل ۲۵ مرحله اصلی می باشد که در حال حاضر تمامی این مراحل در جمهوری اسلامی ایران به جز مرحله رای گیری و شمارش آرا به صورت تمام الکترونیکی انجام می شود. این کتاب حاصل یک سال تحقیق در حوزه رای گیری الکترونیکی و الگوریتم های آن می باشد.

این کتاب شامل سه فصل می باشد که در فصل اول به بررسی روش های رای گیری الکترونیکی می پردازیم. در این فصل فرآیند های رای گیری را بررسی کرده و ویژگی های آن را به سه بخش رای گیری الکترونیکی را مشخص می کنیم. در پایان این فصل به بررسی فواید انتخابات در جمهوری اسلامی ایران می پردازیم.

در فصل دوم به مبانی تئوریک سیستم های رای گیری الکترونیکی پرداخته ، در مورد رمزنگاری بحث خواهیم کرد و روش هایی مانند نسیم محرمانه ، توابع درهم ساز و .. را مورد بررسی قرار خواهیم داد.

آخرین فصل کتاب در مورد الگوریتم ها و روش های رای گیری الکترونیکی صحبت خواهیم کرد و این فصل مهمترین فصل کتاب بوده که روش های مختلف رای گیری الکترونیکی به همراه مزایا و معایب هر روش را مشخص و کنیم و تعیین خواهیم کرد هر روش کدامیک از ویژگی های الگوریتم های رای گیری الکترونیکی را دارد و کدام روش را ندارد.

فهرست مطالب

۱۰	بررسی روش های رای گیری الکترونیکی
۱۰	فصل اول
۱۰	بررسی روش های رای گیری الکترونیکی
۱۰	مقدمه
۱۱	رای گیری الکترونیکی
۱۶	۱-۲- رایزبند رای گیری الکترونیکی
۱۷	۳-۱- رایزبند رای گیری الکترونیکی
۲۱	۴-۱- انواع رای گیری الکترونیکی
۲۱	۴-۱-۱ رای گیری الکترونیکی مبتنی بر کاغذ
۲۳	۴-۱-۲ رای گیری الکترونیکی
۲۵	۵-۱- ویژگی های سیستم های رای گیری الکترونیکی
۲۶	۵-۱-۱ صحت
۲۷	۵-۱-۲ مشخص نشدن هویت شخص رای دهنده
۲۷	۵-۱-۳ عدم وجود رسید
۲۸	۵-۱-۴ استحکام
۲۸	۵-۱-۵ قابلیت بازرسی
۲۹	۵-۱-۶ دموکراسی
۳۰	۵-۱-۷ عدالت

۳۰ ۶-۱- بررسی قوانین انتخابات در ایران

۳۱ ۱-۶-۱- انتخابات مجلس شورای اسلامی

۳۳ ۲-۶-۱- انتخابات ریاست جمهوری

۳۵ ۱-۷- خلاصه

۳۷ فصل دوم

۳۷ مبانی تئوری سیستم های رای گیری الکترونیکی

۳۸ ۱- مبانی رمزنگاری

۴۱ ۱-۱-۲- رمزنگاری متقارن

۴۵ ۲-۱-۲- رمزنگاری نامتقارن

۴۹ ۲-۱-۳- توابع درهم ساز

۵۲ ۲-۱-۴- اثبات تعاملی بدون دانش

۵۶ ۲-۱-۵- تسهیم محرمانه

۵۸ ۲-۱-۶- رمزنگاری هم ریخت

۵۹ ۲-۱-۷- رمزنگاری مجدد

۵۹ ۲-۱-۸- رمزنگاری کور کورانه

۶۱ ۲-۱-۹- رمزنگاری قابل انکار

۶۱ ۲-۲- احراز هویت کاربران

۶۲ ۲-۲-۱- رمز عبور ساده

۲-۲-۲- رمز عبور یک بار مصرف ۶۳

فصل سوم ۶۶

سیستم های رای گیری الکترونیکی ۶۶

۴-۱- روش های رای گیری الکترونیکی ۶۸

۴-۱-۱- روش ویر ۶۸

۴-۱-۲- روش هیرت و ساکو ۷۲

۴-۱-۳- روش جاسکوا ۷۴

۴-۱-۴- روش بنالو و توینز ترا (نسخه اول) ۷۵

۴-۱-۵- روش بنالو و توینز ترا (نسخه دوم) ۷۶

۴-۱-۶- روش کریر و مارتین ۷۷

۴-۱-۷- روش کوهن و فیسچر ۷۹

۴-۱-۸- روش بنالو و یانگ ۷۹

رمزنگاری خم بیضوی در عمل ۸۰

آرایش ۸۴

کلیدهای ضعیف ۸۴

امضاهای آسیب پذیر ۸۴

۲ مقدمات ۸۵

۲,۱ خمهای بیضوی کاربردی ۸۵

۸۹	۲,۲ جفت‌های کلید عمومی خم بیضوی
۹۰	۲,۴ امضاهاى دیجیتال خمیضوی
۹۱	۳ کاربرد خمهای بیضوی
۹۱	بینکوبین
۹۵	امنیت لایه انتقال (TLS)
۹۹	۴ آزمون سلامت رمزنگاری
۱۰۰	۴,۱ تولید کلید
۱۰۱	۴,۲ رمزهای امضاى برابر پیغام تکراری
۱۰۴	۴,۴ بینکوبین
۱۱۱	۴,۵ برنامه خروج موقت امن SSH
۱۱۳	۴,۶ امنیت لایه ی انتقال (TLS)