3rd. INTERNATIONAL CONFERENCE ON
SCIENCE AND ENGINEERING
2 June 2016 ISTANBUL - TURKEY
www.3icesconf.com

رای گیری الکترونیکی بااستفاده از رمز نگاری همریختی

محمد جنتی پور
سازمان آب و برق خوزستان
Jannatipour.m@kwpa.gov.ir

زینب السادات ملائکه زاده
سازمان آب و برق خوزستان
Malaekeh.z@kwpa.gov.ir

میترا مهمدی
سازمان آب و برق خوزستان
Mohmedi.m@Kwpa.gov.ir

چکیده

در این مقاله سیستم رای گیری الکترونیکی بر اساس رمزنگاری همریختی برای اطمینان ازمخفیانه بودن رای، حفظ حریم خصوصی و قابلیت اطمینان در رای گیری مورد بررسی قرار گرفته است. رمزنگاری همریختی یک زیر مجموعه از همریخت حریم خصوصی است که این قادر به محاسبه داده های رمزگذاری شده به طور مستقیم و همچنین رمزنگاری نتیجه عملیات به صورت خودکارمی باشد. به همین دلیل از آن برای طیف گسترده ای از برنامه های کاربردی از جمله محاسبات چندجانبه امن، پایگاه داده رمزگذاری، رای گیری الکترونیکی، و غیره استفاده میگردد. در این مقاله، با استفاده از مکانیسم رمزنگاری همریختی به طراحی و پیاده سازی یک سیستم رای گیری الکترونیکی پرداخته شده است که جدای از امتیازات در میان رای دهندگان، شمارش کننده گان آرا، و اعلام کننده های نتایج ، نشان می دهد که این سیستم رای گیری علاوه بر تضمین ناشناس ماندن در رای دادن ، ارائه تقلب در طول شمارش آرا را غیر ممکن می نماید.

کلمات کلیدی – سیستم رای گیری الکترونیکی، ناشناس ماندن، رمزنگاری همریختی ، همریخت جمعی،RSA