

**7th International Conference on
Electrical , Electronic Engineering and Smart Grids**



ارائه روشی برای رمزنگاری بوسیله شبکه عصبی

*امید پاکدل آذر

دکترای مهندسی برق مخابرات سیستم

چکیده:

هدف از هر سیستم رمزنگاری تبادل اطلاعات میان دو کاربر موردنظر بدون هرگونه نشتی اطلاعات به اشخاص دیگر که به صورت غیر مجاز می توانند به اطلاعات دسترسی پیدا نمایند می باشد. کلیدهای عمومی فراوانی مبتنی بر تئوری ها ارائه شده اند که این امر مستلزم توان محاسباتی می باشند. علاوه بر این فرآیند تولید کلیدهای عمومی بسیار پیچیده و زمان بر می باشند. برای غلبه بر این معایب، شبکه های عصبی برای تولید کلیدهای عمومی در این مقاله به کار برده شده است. این موضوع به عنوان محرکی برای بیان اثر متقابل شبکه های عصبی و رمزنگاری می باشد. در این نمونه رمزنگاری عصبی ، هر دو شبکه با دریافت یک بردار ورودی یکسان یک بیت خروجی تولید می کنند و بر اساس بیت خروجی آموزش داده می شوند. آموزش دو شبکه عصبی بر اساس بیت خروجی مشترک بیانگر یک پدیده طبیعی می باشد. سنکرون شدن به وسیله آموزش دوجانبه را می توان به سیستم های رمزنگاری به منظور تولید کلید اعمال نمود.

کلمات کلیدی:

رمزنگاری عصبی، آموزش دوجانبه، شبکه های عصبی مصنوعی، ماشین یادگیری