عنوان مقاله:
پیادهسازی الگوریتم رمزنگاری A5/1 بر روی FPGA

محل انتشار:
کنفرانس بین المللی پژوهش در علوم و مهندسی (سال: 1395)

تعداد صفحات اصل مقاله: 6

نویسندگان:
صالح دلیریان - *دانشجوی کارشناسی ارشد مهندسی کامپیوتر دانشگاه محقق اردبیلی، گرایش معماری کامپیوتر،*

رضا اسودی - *استادیار دانشگاه محقق اردبیلی، گروه مهندسی برق و کامپیوتر،*

خلاصه مقاله:
الگوریتم رمزنگاری A5/1 یک نسخه بسیار قوی از الگوریتمهای رمزنگاری شبکههای تلفن همراه) GSM (است. اساس رمزنگاری A5/1 بر پایه سیستم رمز دنبالهای) stream cipher (است که مکالمات تلفنهای همراه را رمزنگاری میکند.این الگوریتم برای بیش از 130 میلیون مشترک تلفن همراه در قاره اروپا استفاده میشود. ما در این مقاله عملکرد این الگوریتم رمزنگاری و قسمتهای مختلف آن را شرح میدهیم و شبهکد نظیر آن را بیان نموده، سپس آن را با زبان توصیف سختافزار VHDL شبیهسازی میکنیم و نتایج حاصل را نشان میدهیم، در آخر این سیستم رمزنگاری را بر روی FPGAمدل Xilinx_Spartan-6 پیادهسازی خواهیم کرد و بعضی از پارامترهای خروجی را مورد بررسی قرار میدهیم و عملکردخوب و سریع این الگوریتم را نشان میدهیم.

کلمات کلیدی:
الگوریتم رمزنگاری GSM ، stream cipher ، A5/1
(Global System for Mobile) ، FPGA ، Xilinx_Spartan-6