


Sl No	Particulars		
1	Name of the Candidate	Dr. Anil Kumar M N	
2	Address of the parent institution	Federal Institute of Science and Technology Mookkannor, Angamaly, Kerala-683577	
3	PhD Thesis Title	Area Efficient Arithmetic Unit of Elliptic Curve Cryptography Processor with High Throughput	
4	Research guide Name	Dr. V Sridhar	
	Department and Designation	Principal, PESCE Mandya	
5	Date of Registration for PhD	10-08-2009	
	University /Branch	Mysore/Electronics	
6	Date of Award of PhD degree	20-03-2014	
7	<p><u>Brief synopsis</u></p> <p>The data security, authentication and integrity have become an important and urgent need for healthcare information, confidential communication, storage and financial services etc. Public key cryptosystem is the most effective way to secure data transaction and messaging. Elliptic Curve Cryptosystem (ECC) has been considered as an alternative to Rivest, Shamir and Adleman (RSA) because the same security level can be obtained with shorter keys in ECC.</p> <p>The focus of the most of the research in ECC is the implementation of the fundamental operation $Q=k.P$ (point operation) with the optimal hardware resources with an increase in the throughput of the point operation. The point operation $Q=k.P$ involves the addition, subtraction, multiplication, squaring and inversion over Galois field $GF(p)$ or over a Binary field. Inversion is the costliest operation in terms of area and speed among other field operations. Binary Inversion Algorithm (BIA) is the most suitable algorithm for the computation of inversion over $GF(p)$ of National Institute of Standards and Technology (NIST) recommended prime field $p-521$ which is a Mersenne prime number. The NIST recommend prime field $p-521$ has the highest key length and hence there is a need to implement this prime field with less hardware resources with throughput improvement. Considering the above all aspects specified, an area efficient inversion unit of elliptic curve cryptography processor with high throughput specifically for NIST recommended prime field $p-521$ has been focused and designed.</p> <p>Area efficiency in the architectural area of Binary Inversion Algorithm has been obtained by applying new property of Mersenne prime number in the architecture of BIA. This new property has replaced the computation of two operations by a single operation with less hardware resources. Another property has been used to increase the throughput but with extra hardware resources. The proposed architecture of the inversion implemented by integrating these two properties in the architecture of BIA offered less hardware resources with an increase in the throughput. The proposed architecture of inversion unit has 1042 number of two -input EXOR, 1042 number of two-input OR and 2084 number of two-input AND gates lesser than the earlier reported architecture with an increase in throughput of approximately .1% .</p>		