Several algorithms for computing the multiplicative inverse in $\text{GF}(2^m)$ have been proposed in literature [1–8]. In [4], multiplicative inverse is computed using an improved modification of the extended Euclidean algorithm called almost inverse algorithm. That iterative algorithm can compute the multiplicative inverse in approximately $2^m$ clock cycles [4]. In [6] an architecture able to compute the Montgomery multiplicative inverse for both, $\text{GF}(p)$, for a prime $p$, and $\text{GF}(2^m)$ on a unified-field hardware platform was proposed.

1. Computing multiplicative inverses by using FLT-related techniques is inefficient as those methods require many field multiplication and squaring operations; 2. ITMIA is a competitive design option only when using normal basis representation and A new algorithm for performing fast inversion in $\text{GF}(2^m)$ is presented. The algorithm requires $O(m \log_2 m)$ computation time. Using serial-in-parallel-out multiplication, the design of the algorithm is highly regular, modular, and well suited for VLSI implementation. AUTHORS. G.-L. Feng, Charles C. Wang, T. K. Truong, Howard M. Shao, Leslie J. Deutsch, Jim K. Omura, Irving S. Reed, VLSI Architectures for Computing Multiplications and Inverses in $\text{GF}(2^m)$, IEEE Transactions on Computers, v.34 n.8, p.709-717, August 1985 [doi:10.1109/TC.1985.1676616].

12. J. L. Massey and J. K. Omura, "Computational method and apparatus for finite field arithmetic," U. S. Patent Application, to appear, and Inverses in $\text{GF}(2^m)$. C. C. Wang, T. K. Truong, H. M. Shao and L. J. Deutsch Communications Systems Research Section. J. K. Omura. There is a need for good multiplication and inversion algorithms that can be easily realized on VLSI chips. Massey and Omura recently developed a new multiplication algorithm for Galois fields based on a normal basis representation. In this paper, a pipeline structure is developed to realize the Massey-Omura multiplier in the finite field $\text{GF}(2^m)$. With the simple squaring property of the normal-basis representation used together with this multiplier, a pipeline architecture is also developed for computing inverse elements in $\text{GF}(2^m)$. The designs developed for the Massey-Omur