Unusual processor architecture for elliptic curve encryption is proposed in this paper. The architecture exploits projective coordinates \((x=X/Z, y=Y/Z)\) to convert \(GF(2^k)\) division needed in elliptic point operations into several multiplication steps. The processor has three \(GF(2^k)\) multipliers implemented using bit-level pipelined digit serial computation. It is shown that this results in a faster operation than using fully parallel multipliers with the added advantage of requiring less area. The proposed architecture is a serious contender for implementing data security systems based on elliptic curve cryptography.

For pre-prints please write to: abstracts@kfupm.edu.sa