1.	Record Nr.	UNINA9910141193903321
	Titolo	2011 Fourth International Symposium on Parallel Architectures, Algorithms and Programming
	Pubbl/distr/stampa	[Place of publication not identified], : IEEE, 2011
	Descrizione fisica	1 online resource (xvii, 359 pages)
	Disciplina	004.11
	Soggetti	High performance computing
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph

Sommario/riassunto

In the recent years, embedded systems began to be used in sensitive applications such as personal digital assistants and smart cards. Due to very strict cost and power constrains, the support for cryptography provided by these devices is often limited to either public or private key primitives. This limitation is much more evident in devices where the cryptographic algorithms are implemented using hardware resources. In this paper, we propose an extension of a public-key cryptosystem to support also private-key, and we evaluate our architecture on FPGA platforms. In particular, we propose a new arithmetic unit in which the polynomial modular multiplication of ECC is extended to compute also the polynomial arithmetic operations over binary extended field of AES. We compare our design with an architecture obtained by instantiating state of the art implementation of AES and ECC and we evaluate the trade-offs. The experimental results show that our proposed architecture takes up less hardware resources. Nevertheless, the achieved performances are better compared to the ECC reference core, while the ones compared to AES only implementation are comparable with the state of the art.