HYPER ELLIPTIC CURVE CRYPTOSYSTEMS PADA *EMBEDDED MICROPROCESSOR*

Iwan Kustiawan[1]

ABSTRAK : Dalam tulisan ini dipaparkan *Hyper Elliptic Curve Cryptosystems* (HECC) yang dianggap potensial paling aman dari sudut pandang kriptografi. Selain itu, akan ditunjukkan hasil implementasi formula yang diturunkan untuk HECC genus 4 pada Pentium4 dan mikroprosesor ARM. Kriptosistem ini dijalankan pada *embedded* processor ARM7TDMI. ARM mewakili *Advanced RISC Machine* dan menunjukkan arsitektur RISC tipikal dengan fitur-fitur tambahan seperti *flag-depending instruction execution.* ARM 7 didasarkan pada arsitektur von Neuman dan banyak ditemukan pada perangkat *hand held* seperti PDA. Hasil percobaan menunjukkan bahwa kurva-kurva genus 4 sangat sesuai diimplementasikan pada prosesor 32-bit. HECC sebagai alternatif yang setara dengan ECC dapat menjadi pilihan kriptosistem untuk aplikasi-aplikasi sekuriti *embedded* masa mendatang.

ABSTRACT : In this paper were presented HECC, which are considered potentially the most secure from the point of view of cryptography. In addition, the results will be shown explicitly that the implementation of the formula derived for the HECC genus 4 on Pentium 4 and microprocessor ARM. Cryptosystem is executed on the ARM7TDMI embedded processor. ARM represented Advanced RISC Machine, and showed typical RISC architecture with additional features such as the flag-depending instruction execution. ARM 7 based on the von Neuman architecture, and many found in the devices such as small hand held PDA. The experiment result shows that curves genus 4 is implemented according to the 32-bit processors. HECC as the alternative which is equivalent to the ECC can be cryptosystem choice for embedded security applications in the future.

Kata Kunci : *Cryptosystem*, HECC, ECC, *embedded processor*.

[1] *Iwan Kustiawan, S.Pd., M.T. adalah dosen Jurusan Pendidikan Teknik Elektro UPI*