REKABENTUK DAN SINTESIS SUATU CIP INKRIPSI MENGGUNAKAN ALGORITMA BLOWFISH

oleh

SITI ZARINA BT. MD. NAZIRI

Tesis yang diserahkan untuk memenuhi
keperluan bagi Ijazah Sarjana Sains

September 2001

PENGHARGAAN

Dengan nama Allah yang Maha Pemurah lagi Maha Mengasihani

Alhamdulillah, syukur ke hadrat Allah S.W.T. kerana dengan limpah kurnianya saya telah berjaya menyempurnakan tesis ini. Dalam kesempatan ini, saya ingin merakamkan ucapan terima kasih saya yang tidak terhingga kepada kedua-dua ibu-bapa saya yang telah memberikan dorongan dan kepercayaan untuk saya meneruskan kajian ini. Tidak lupa juga kepada insan tersayang yang telah banyak memberikan semangat dan sokongan dalam menempuh sebarang kesukaran sepanjang kajian ini dijalankan.

Sekalung terima kasih juga saya ucapkan kepada Prof. Madya Dr. Othman bin Sidek selaku Penyelia Utama yang telah benyak memberikan bantuan sama ada cadangan, nasihat dan keperluan-keperluan lain dalam merealisasikan kajian ini sehinggalah ke peringkat akhir penulisan tesis ini. Tidak ketinggalan ucapan terima kasih saya kepada saudara Rhett Whatcott, iaitu salah seorang daripada tenaga pengajar VHDL di Xilinx, Inc., yang telah banyak membantu saya dalam kajian ini.

Akhir sekali, ucapan terima kasih saya hulurkan kepada juruteknik-juruteknik di Pusat Pengajian Kejuruteraan Elektrik & Elektronik, Kampus Kejuruteraan USM, yang telah banyak memberikan bantuan teknikal dan tunjuk ajar dalam menyempurnakan kajian ini. Buat sahabat-sahabat di mana juga berada, terima kasih saya ucapkan kerana tanpa semangat, dorongan dan kesudian kalian berkongsi suka dan duka, tidak mungkin saya berada di tahap ini. Semoga kajian kali ini dapat memberi sumbangan kepada kajian-kajian berkaitan yang seterusnya.

Semoga Allah memberikan Rahmat kepada semua yang terlibat.

Segala yang baik datangnya dari Allah dan segala kekurangan datangnya dari saya sendiri.

Siti Zarina bt. Md. Naziri

September 2001

KANDUNGAN

SENARAI RAJAH

SENARAI JADUAL

SENARAI ISTILAH

atas-ke-bawah	*top-down*
bawah-ke-atas	*bottom-up*
celusan	*throughput*
cipher aliran	*stream cipher*
cipher blok	*block cipher*
daya-kasar	*brute-force*
jaringan	*network*
kekangan	*constraints*
keruntuhan	*avalanche*
kod-sumber	*source-code*
laluan paip	*pipeline*
logik boleh-aturcara	*programmable logic*
memboleh-tulis	*write-enable*
nyahpijat	*debug*
pengesahan	*verify*
penggantian	*substitution*
penimbal sejagat	*global buffer*
pindah-turun	*download*
selak	*latches*
teks-biasa	*plaintext*
teks-kod	*ciphertext*
tukar-ganti	*swapping*

SENARAI KEPENDEKAN

ASIC	*Application Specific Integrated Circuit*
CIB	Cip Inkripsi Blowfish
CLB	Tatarajah blok logik *(Configurable logic block)*
CPLD	*Complex Programmable Logic Device*
DES	*Data Encryption Standard*
FPGA	*Field Programmable Gate Array*
HD	*Hardware Debugger*
IDEA	*International Data Encryption Algorithm*
IOB	Blok masukan & keluaran *(Input & output block)*
RAM	Ingatan capaian rawak *(Random Access Memory)*
RSA	Riverst-Shamir-Adelman
UCF	*User constraints file*
VHDL	*Very-High-Speed-Integrated-Circuit Hardware Description Language*

REKABENTUK DAN SINTESIS SUATU CIP INKRIPSI MENGGUNAKAN ALGORITMA BLOWFISH

ABSTRAK

Penemuan kriptografi sebagai teknik pengabur maklumat telah membuka lembaran baru dalam keselamatan maklumat maya. Penciptaan pelbagai algoritma kriptografi telah menggalakkan implementasi algoritma-algoritma tersebut ke bentuk perisian dan perkakasan. Namun, bilangan kriptografi dalam bentuk perkakasan masih kurang, terutamanya yang menggunakan VHDL sebagai medium rekabentuknya. Dalam kajian ini, satu *cipher* blok simetrik iaitu Blowfish, yang dikatakan di antara algoritma yang paling selamat digunakan setakat ini, telah diimplementasikan ke dalam bentuk perkakasan menggunakan FPGA Xilinx, iaitu XC4052XLA HQ240. VHDL telah digunakan sebagai medium kemasukan rekabentuk dengan menggunakan pendekatan bawah-ke-atas. Keseluruhan peringkat rekabentuk dilakukan sepenuhnya menggunakan perisian Xilinx Foundation Series V2.1. Penggunaan kekangan telah membantu meningkatkan kelajuan rekabentuk. Rekabentuk ini telah menggunakan CLB sebanyak 1374 dan menghasilkan get berjumlah 151 537. Nilai celusan bagi rekabentuk ini ialah 20.83 Mbit/s pada frekuensi jam 11.4 MHz. Konfigurasi rekabentuk ini telah dilakukan ke atas papan pembangunan FPGA APS-X240 PC104. Dengan adanya kajian ini, adalah diharapkan agar ia dapat memberikan sumbangan dalam bidang kriptografi selain menaikkan peranan FPGA dan VHDL dalam rekabentuk digital, terutamanya rekabentuk inkripsi yang amat mengambil kira faktor kepantasan.

DESIGN AND SYNTHESIS OF AN ENCRYPTION CHIP USING BLOWFISH ALGORITHM

ABSTRACT

The founding of cryptography as an obscuring method in ensuring the security of any information, has opened a new era in cyberspace information security. The creation of many cryptographic algorithms stimulates the implementation of these algorithms into the form of software and hardware. However, the number of hardware cryptography is still few, especially the VHDL-created designs. As an initiative, many parties have done a number of researches in this approach. In this research, the symmetrical block cipher, Blowfish, which is among of the safest algorithm used nowadays, is selected to be implemented into a form of hardware, that is FPGA Xilinx XC4052XLA HQ240. Meanwhile, VHDL is used as the design entry in bottom-up approach. The whole design process uses Xilinx Foundation Series version 2.1 software. The design speed is increased by the use of constraints. For this design, 1374 of FPGA's CLBs have been used and 151 537 equivalent gates are generated. The estimated throughput for the design is 20.83 Mbit/s at 11.4 MHz of clock frequency. Configuration of the design has been done on APS-X240 PC104 FPGA development board. Finally, it is hoped that this research will give some contribution in the field of cryptography. At the same time, this research is also hoped to enhance the usage of FPGA and VHDL in any digital design, especially encryption design, which really concern in speed factor.

BAB 1

PENGENALAN

1.1 Kriptografi

Dunia kita kini semakin kecil dengan berkembangnya teknologi informasi. Sehubungan ini, komunikasi dalam era siber telah menjadi lumrah dan bilangan penggunanya semakin meningkat. Dalam alam siber sendiri, pelbagai maklumat bertukar tangan setiap hari, seperti tunai digital, nota, pesanan, malah maklumat-maklumat sulit yang lain termasuklah rahsia syarikat dan pertahanan sesebuah negara. Namun, adakah kita sebagai pengguna benar-benar pasti akan keselamatannya?

Kita mungkin tidak menyedari tentang hakikat semulajadi suatu kejadian; apabila suatu keadaan itu semakin baik, satu keadaan lain yang berkaitan akan berlaku sebaliknya. Begitulah yang berlaku ke atas teknologi siber. Perkembangannya yang kian pesat telah mengundang kepada jenayah siber; seperti pencerobohan ke atas sistem maklumat sulit, kecurian dan penipuan wang tunai dan kerosakan suatu jaringan sistem (Schneier, 1998). Masalah-masalah ini telah mencetuskan kesedaran pelbagai pihak untuk menggunakan teknik pengabur maklumat iaitu **kriptografi**, yang bertujuan untuk melindungi maklumat mereka. Perkataan kriptografi sebenarnya merupakan gabungan dua perkataan Greek, iaitu *kripte* dan *grafik*. *Kripte* bermaksud 'tersembunyi',

manakala *grafik* bermaksud 'tulisan' (Nichols, 1999). Oleh itu, gabungan dua perkataan tersebut telah menghasilkan definisi kriptografi sebagai suatu sains penulisan pesanan yang hanya membenarkan penerima tertentu sahaja untuk membaca pesanan tersebut (Nichols, 1999).

Buat masa ini, kriptografi telah menjadi sebahagian daripada sistem informasi. Pelbagai jenis elemen dalam sistem informasi telah menggunakan khidmat kriptografi, bermula dari surat-elektronik *(e-mail)* sehinggalah yang terkini, iaitu peralatan komunikasi selular, kesemua elemen ini memerlukan keselamatan maklumat seperti yang ditawarkan oleh kriptografi. Penggunaannya akan menjadi lebih meluas apabila lebih banyak syarikat-syarikat kewangan dan komunikasi mula beralih ke bidang penggunaan rangkaian komputer (Schneier, 1997).

Selaras dengan perkembangan dan kesedaran ke atas kepentingan aspek keselamatan ke atas sistem operasi, kerajaan Amerika Syarikat, iaitu negara yang memonopoli bidang kriptografi ini, telah melonggarkan syarat eksport, iaitu penghapusan lesen ke atas produk-produk inkripsi. Pengumuman yang telah dibuat oleh kerajaan Amerika Syarikat pada 12 Januari 2000 ini merangkumi produk-produk kriptografi seperti kod-sumber inkripsi, perkakasan dan komponen-komponen inkripsi (Johnston, 2000). Sebelum ini, produk-produk tersebut hanya boleh dipasarkan dan diedarkan di Amerika Syarikat dan negara-negara tertentu sahaja. Penghapusan lesen ini secara tidak langsung akan menguntungkan pelbagai pihak, termasuklah bidang penyelidikan kriptografi yang sedang dijalankan oleh banyak negara di dunia.

Walau bagaimanapun, perkembangan teknologi kriptografi yang pesat akan menjurus kepada perkembangan aktiviti pecah-masuk *(hacking)*. Pelbagai teknik penyelesaian dan teknik matematik untuk memecah-masuk elemen-elemen kriptografi semakin mudah untuk diperolehi, terutamanya melalui internet. Keadaan ini telah memudahkan pemecah-masuk *(hackers)* untuk melakukan kriptanalisis ke atas elemen-elemen kriptografi (Clark, 1999). Oleh itu, pelbagai usaha dan cara, terutamanya dalam bidang penyelidikan, telah dijalankan untuk memperbaiki taraf keselamatan elemen-elemen kriptografi ini.

1.2 Peranan kriptografi

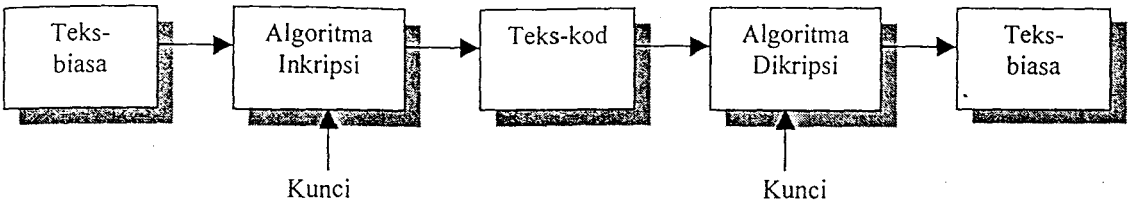
Kriptografi dicipta untuk menjalankan tugas-tugas penting berkaitan keselamatan maklumat. Di antara peranannya ialah untuk memastikan penerima mengetahui siapakah pengirim maklumat tersebut. Selain itu, dengan adanya kriptografi, penerima juga dapat memastikan maklumat yang diterimanya tidah berubah atau diubah semasa proses penghantaran maklumat.

Berdasarkan peranannya sebagai elemen keselamatan, penggunaan kriptografi akan menawarkan hak tanggungjawab, keadilan, ketepatan, dan hak persendirian kepada sistem atau perkakas yang diwakilinya (Schneier, 1997). Dalam penawaran hak tanggungjawab dan keadilan, kriptografi berperanan untuk mengelak sebarang bentuk pengkhianatan yang boleh berlaku ke atas kewangan elektronik. Penawaran ketepatan oleh kriptografi pula dapat dilihat pada sistem yang dapat menentukan identiti seseorang. Dalam pada itu, kriptografi dapat memberikan khidmat persendirian yang

amat diperlukan oleh syarikat, terutamanya yang terlibat dalam pemasaran secara elektronik. Kriptografi juga mampu menghalang penceroboh atau pesaing syarikat untuk membaca atau mengubah rahsia-rahsia syarikat.

1.3 Proses Inkripsi

Untuk menjelaskan suatu proses inkripsi, cuba kita ambil contoh berikut: katakan **pengirim**, Ina, hendak menghantar pesanan kepada rakannya, Han yang akan bertindak sebagai **penerima**. Dalam kriptografi, pesanan asal yang ditulis oleh Ina ini dipanggil **teks-biasa** *(plaintext)*. Ina akan mengubah pesanan tersebut menggunakan **kunci** tertentu kepada suatu bentuk teks yang tidak difahami, yang dikenali sebagai **teks-kod** *(ciphertext)*. Proses ini dipanggil proses **inkripsi**. Teks yang telah diubah itu dihantar kepada Han. Han yang berperanan sebagai penerima akan membuka teks yang telah diubahsuai tersebut menggunakan **kunci** tertentu yang membolehkan Han membaca pesanan Ina yang asal. Proses yang kedua ini dipanggil **dikripsi**. Kunci yang digunakan ketika inkripsi dan dikripsi mungkin merupakan kunci yang sama, atau mungkin kunci yang berlainan. Namun begitu, terdapat kemungkinan ada pihak lain yang cuba mengubah teks tersebut atau mendapatkan teks sebenar dengan pelbagai cara. Oleh itu, adalah amat penting untuk memilih jenis algoritma kriptografi yang sesuai. Perkara ini akan dibincangkan dalam Bab 3. Secara ringkasnya, proses inkripsi dan dikripsi ini boleh diterangkan oleh Rajah 1.1.



Rajah 1.1: Proses inkripsi dan dikripsi

1.4 Inkripsi perkakasan dan Inkripsi perisian

Inkripsi wujud dalam dua bentuk, iaitu inkripsi perkakasan dan inkripsi perisian. Buat masa ini, inkripsi perisian menjadi pilihan utama. Namun begitu, kajian yang giat sedang dijalankan untuk mengimplementasikan algoritma-algoritma inkripsi ini ke dalam bentuk perkakasan. Suatu algoritma yang baik sepatutnya boleh diimplemenkan ke dalam bentuk perkakasan dan sesuai untuk sebarang saiz pemproses *(processors)* (Schneier, 1994). Sebagai pengguna, pemilihan yang dibuat di antara kedua-duanya perlu mengambilkira pelbagai aspek keselamatan yang sesuai dengan penggunaannya.

Walaupun inkripsi perisian telah digunakan secara meluas, inkripsi dalam bentuk perkakasan masih menjadi pilihan pihak pertahanan dan aplikasi komersil terutamanya dalam bidang komunikasi. Menurut Schneier (1996), pemilihan ini disebabkan oleh beberapa faktor. Faktor yang pertama ialah faktor **kelajuan**. Perpindahan elemen inkripsi ke dalam suatu cip akan mempercepatkan perjalanan sistem yang diwakilinya, lebih-lebih lagi jika cip yang digunakan mempunyai kelajuan yang tinggi.

Faktor kedua pula ialah faktor **keselamatan**. Penggunaan algoritma inkripsi dalam bentuk peranti adalah lebih selamat berbanding penggunaan perisian kerana kaedah ini dapat mengelakkan pencerobohan yang tidak dijangka, terutamanya ke atas algoritma itu sendiri. Terdapat inisiatif oleh pihak-pihak tertentu untuk memaksimumkan ciri-ciri keselamatan peranti kriptografi ini. Antara langkah yang digunakan ialah dengan penciptaan peranti yang disadur dengan bahan kimia tertentu, yang mana bahan kimia ini akan memusnahkan logik cip tersebut jika terdapat sebarang cubaan pencerobohan dilakukan ke atas cip tersebut. Selain itu, keselamatan suatu cip inkripsi itu akan lebih terjamin apabila kesemua elemen kriptografi, bermula dari teks masukan sehinggalah ke peringkat penghasilan kunci, dimasukkan ke dalam cip yang sama.

Faktor yang ketiga ialah inkripsi perkakasan **mudah** untuk dimasukkan ke dalam suatu sistem, terutamanya dalam sistem komunikasi. Penghasilan peranti inkripsi yang boleh dimuatkan ke dalam telefon, faksimili dan mesin-mesin komunikasi lain, ternyata menjimatkan ruang dan lebih murah berbanding penggunaan perisian dan mikropemproses yang amat sukar untuk diaplikasikan ke atas mesin-mesin seumpama ini. Malah, pengguna-pengguna yang masih baru menggunakan komputer boleh menggunakan perkakas inkripsi ini, asalkan penyambungan perkakas tersebut dilakukan dengan betul.

Selain itu, faktor yang berikutnya tidak kurang pentingnya, iaitu penggunaan inkripsi perkakasan **tidak dapat dikesan** *(invisible)*. Dalam hal ini, adalah agak sukar bagi penceroboh untuk membolosi sistem inkripsi ini kerana ia tidak dipaparkan pada skrin komputer.

Terdapat tiga (3) jenis inkripsi perkakasan yang terdapat di pasaran. Jenis-jenis inkripsi perkakasan tersebut ialah pertama, modul-modul inkripsi yang *self-contained*, kedua ialah kotak-kotak inkripsi yang khusus untuk rangkaian komunikasi, dan ketiga ialah papan *(board)* yang dapat dimasukkan ke dalam komputer peribadi. Jenis perkakas inkripsi yang pertama banyak digunakan oleh institusi-institusi kewangan yang berfungsi untuk mengesahkan kata laluan pengguna dan pengurusan kunci. Kajian kali ini telah membolehkan penghasilan produk inkripsi dari jenis ketiga, iaitu dalam bentuk papan interaktif.

Menurut Preneel (1998), kepantasan suatu inkripsi perkakasan bergantung kepada penggunaan laluan paip *(pipeling)* dan keselarian *(parallelism)*. Kepantasan inkripsi perisian pula dilihat daripada segi keboleh-masukan *(access)* ke dalam ingatan *(memory)*.

Oleh itu, adalah penting bagi pengguna untuk mengetahui sejauh mana keperluan inkripsi perkakasan tersebut kepada mereka. Antara perkara-perkara yang perlu diambil kira ialah jenis perkakasan yang digunakan, sistem operasi, perisian aplikasi yang digunakan bersama-sama dengan peranti tersebut dan jaringan *(network)* yang terbabit.

Daripada perbincangan di atas, dapatlah disimpulkan di sini bahawa perkakas inkripsi mempunyai kelebihan daripada segi kelajuan, harga, dan keselamatan. Kekurangan inkripsi perisian pula adalah kerana tidak dapat menyediakan kelebihan seperti inkripsi perkakasan. Namun, daripada aspek lain, inkripsi perisian tetap mempunyai kelebihannya. Di antara kelebihan inkripsi perisian ialah ia boleh diadaptasi oleh mana-

mana komputer hanya dengan sedikit pengubahsuaian berdasarkan keperluan penggunanya. Selain itu, salinan ke atas kod-kod algoritma kriptografi dalam bentuk perisian, terutamanya dalam kod C, boleh dilakukan dengan mudah dan murah, terutamanya daripada internet. Kod-kod seumpama ini banyak diimplementasikan ke dalam bentuk program, yang digunakan secara meluas oleh sistem-sistem pengendalian yang utama di seluruh dunia.

1.5 Maklumat Berkenaan Kajian dan Tesis

Seperti negara-negara lain, negara kita juga telah mula mengorak langkah dalam meneroka bidang kriptografi yang ternyata dapat memberikan sumbangan yang besar dalam kemajuan negara, khususnya dalam bidang pengkomputeran dan multimedia. Terdapat beberapa universiti dan badan-badan tertentu di dalam dan luar negara yang menjalankan beberapa kajian ke atas implementasi algoritma kriptografi ke dalam bentuk perkakasan.

Antara kajian tersebut ialah implementasi algoritma DES ke atas CPLD Altera oleh Dr. Zulkarnain Mohd. Yusoff, Teo Pock Cheung, dan Ahmad Zuri Sha'ameri (Teo, *et al.*, 2000) di Universiti Teknologi Malaysia. Dalam kajian ini, algoritma DES telah dipecahkan kepada empat (4) segmen untuk tujuan dilaluan-paipkan. Teknik laluan paip telah digunakan untuk meningkatkan nilai celusan oleh DES. Selain itu, rekabentuk dalam kajian ini menggunakan AHDL, iaitu bahasa perihalan perkakasan (HDL) yang khusus untuk perisian Altera dalam memprogram CPLD Altera dengan lebih efisien.

Selain itu, dari universiti yang sama, satu kajian implementasi lain telah dijalankan menggunakan algoritma tidak simetrik, iaitu algoritma RSA. Kajian oleh Prof. Dr. Mohd. Khalil Hani, Tan Siang Lin, dan Nasir Shaikh-Husin telah mengimplementasikan algoritma ini ke dalam peranti FPGA. Menurut penyelidik-penyelidik tersebut, algoritma ini telah dipilih kerana algoritma tidak simetrik dapat memenuhi segala keperluan dalam menjamin keselamatan sistem komputer (Hani *et al.*, 2000). Bahasa HDL yang digunakan untuk mewakili rekabentuk tersebut ialah VHDL, dan implementasi dilakukan ke atas Altera FLEX10KE siri FPGA pada kad PCI untuk membolehkan interaksi antara komputer dan peranti yang mewakili rekabentuk RSA.

Davor Runje dan Mario Kovac daripada University of Zagreb pula telah mengimplementasi algoritma IDEA ke dalam FPGA Xilinx. Modul teras yang dinamakan sebagai *Round* telah digunakan untuk mengimplementasikan algoritma ini. Penggunaan modul teras dikatakan dapat menjimatkan kitar rekabentuk, mempercepatkan masa penghasilan produk untuk ke pasaran, dan menjimatkan kos kerana menggunakan peranti boleh-aturcara seperti FPGA (Runje & Mario, 1998).

Terdapat juga kajian implementasi yang menerapkan penggunaan algoritma berlainan untuk proses-proses tertentu di dalam kriptografi. Ahto Buldas dan Jüri Põldre (1997) telah menggunakan algoritma RSA untuk proses penukaran kunci, dan algoritma IDEA untuk proses inkripsi. Kajian selama lebih kurang empat (4) tahun ini telah menghasilkan satu cip 1.0 μm 104 mm^2 berekabentuk CMOS untuk mewakili rekabentuk peranti kriptografi ini. Penggunaan teknik-teknik tertentu telah meningkatkan nilai celusan bagi rekabentuk tersebut.

Semenjak algoritma Blowfish diperkenalkan pada tahun 1994, banyak produk kriptografi berasaskan perisian telah dihasilkan menggunakan algoritma ini. Salah satu daripada perisian tersebut ialah Counterpane Systems' Password Safe versi 1.70 oleh Counterpane Internet Security (Computimes, 1999). Ia adalah satu pengkalan data percuma yang dapat menjana kata laluan *(password)* dengan selamat. Namun, bilangan produk perkakasan yang menggunakan algoritma ini masih rendah, dan masih banyak kajian sedang dilakukan untuk mengimplementasikan algoritma ini ke dalam bentuk perkakasan.

Dalam kajian yang berkaitan, Basheer (1998) daripada University of Bradford telah merekabentuk algoritma Blowfish menggunakan pendekatan skematik dengan menggunakan beberapa pengubahsuaian ke atas rekabentuk algoritma Blowfish, terutamanya ke atas rangkaian Feistel yang menjadi teras kepada algoritma Blowfish. Dalam kajian yang lain pula, VHDL juga telah digunakan sebagai perwakilan rekabentuk bagi algoritma Blowfish. Di sini, perekabentuk-perekabentuk tersebut, Andreas Johansson dan Anders Fältros (1999) telah menggunakan andaian-andaian tertentu dalam beberapa bahagian algoritma tersebut kerana fungsi cip inkripsi yang sebenar tidak dapat dihasilkan.

Daripada kajian-kajian yang dinyatakan, dapatlah disimpulkan bahawa penggunaan laluan paip adalah nadi kepada kepantasan rekabentuk perkakasan kriptografi. Penggunaan bahasa perihalan perkakasan yang sesuai dengan peranti yang disasarkan dapat meningkatkan prestasi rekabentuk. Penggunaan peranti boleh-aturcara seperti FPGA dan CPLD dapat menjimatkan masa, tenaga dan kos dalam proses rekabentuk.

Pengubahsuaian dan andaian juga boleh dilakukan untuk merealisasikan keperluan suatu rekabentuk kriptografi perkakasan.

Sehubungan itu, untuk kajian ini, percubaan untuk membina satu bentuk inkripsi perkakasan telah dilakukan ke atas algoritma Blowfish, yang dikatakan di antara algoritma kriptografi yang paling selamat digunakan setakat ini. Implementasi algoritma ini telah dilakukan ke atas peranti boleh-aturcara FPGA Xilinx dari keluarga XC4000XLA yang boleh beroperasi pada voltan yang rendah, iaitu FPGA XC4052XLA HQ240, dengan menggunakan VHDL sebagai elemen kemasukan rekabentuk. Kajian ini akan menghasilkan satu rekabentuk cip inkripsi yang berkepantasan tinggi (mempunyai nilai celusan yang tinggi), di samping dapat merangkumkan kesemua elemen kriptografi ke dalam satu rekabentuk yang sama untuk menjamin keselamatannya.

1.5.1 Objektif Kajian

Objektif utama bagi kajian ini ialah untuk merekabentuk dan menghasilkan suatu cip inkripsi yang berasaskan algoritma Blowfish menggunakan VHDL sebagai kemasukan rekabentuk *(design-entry)*, manakala FPGA sebagai peranti sasarannya. Selain itu, kewujudan projek ini akan mengetengahkan penggunaan VHDL sebagai medium merekabentuk pelbagai rekaan digital selain dapat membuktikan kebolehan dan keberkesanannya dalam suatu rekabentuk. Objektif terakhir bagi kajian ini ialah untuk menaikkan peranan FPGA sebagai alternatif kepada penggunaan ASIC, selain sebagai tapak memindahkan rekaan yang efektif, berkesan, malah menjimatkan masa dan kos.

1.5.2 Kaedah Pelaksanaan Kajian

Terdapat dua (2) bahagian penting dalam rekabentuk cip inkripsi ini, iaitu bahagian penghasilan sub-kunci, dan bahagian inkripsi data.

Rekabentuk bahagian pertama, iaitu bahagian penghasilan sub-kunci, dilakukan terlebih dahulu. Ini adalah kerana sub-kunci ini akan digunakan untuk rekabentuk bahagian yang seterusnya. Terdapat dua pilihan pendekatan yang akan digunakan, iaitu penjanaan terus sub-kunci daripada kod sumber dalam bahasa C dan penulisan kod sendiri menggunakan VHDL. Sebagai nilai permulaan sub-kunci, cadangan asal oleh pencipta algoritma Blowfish, Bruce Schneier, telah digunakan iaitu nilai-nilai pi (π). Perkara-perkara ini akan dibincangkan dalam Bab 3.

Bahagian kedua rekabentuk iaitu bahagian inkripsi data menerapkan dua (2) elemen penting, iaitu pertama, penghasilan kod perwakilan rekabentuk menggunakan VHDL, dan kedua, implementasinya ke atas peranti FPGA. Bermula dengan kajian berkenaan algoritma dan sintaks VHDL, penulisan kod dibuat dan pengujian ke atas kod tersebut dilakukan beberapa kali untuk mencapai keputusan yang memuaskan. Akhir sekali, selepas peringkat sintesis, implementasi rekabentuk dilakukan dan pengoptimuman dibuat ke atas ruang dan kelajuan cip inkripsi. Nilai-nilai penting dalam kriptografi seperti kelajuan cip inkripsi, bilangan denyutan jam untuk menghasilkan keluaran inkripsi atau dikripsi dan nilai celusan akan dicatatkan dan dibuat perbandingan bagi kedua-dua jenis pengoptimuman.

1.5.3 Keperluan Peralatan

Dalam merealisasikan kajian ini, peralatan-peralatan berikut telah digunakan:

- **Perisian Xilinx Foundation Series V2.1 dan Active-HDL 3.6**

  Perisian Xilinx Foundation Series V2.1 oleh Xilinx, Inc. digunakan bagi perlaksanaan keseluruhan peringkat rekabentuk, bermula dari peringkat kemasukan rekabentuk sehinggalah ke peringkat implementasi. Perisian Active-HDL 3.6 oleh Aldec, Inc. pula digunakan untuk pengujian rekabentuk dalam bentuk simulasi pada peringkat kelakuan *(behavioural)*, iaitu tanpa melalui peringkat sintesis seperti dalam aliran rekabentuk menggunakan Xilinx.

- **Komputer peribadi (PC) yang mempunyai saiz RAM yang besar**

  Peringkat sintesis dan implementasi oleh Xilinx Foundation Series (yang menggunakan khidmat Synopsys untuk perkakas sintesis) bagi suatu litar yang agak kompleks memerlukan ingatan yang besar. Oleh itu, PC yang digunakan mempunyai ingatan bersaiz 128 MB untuk mempercepat proses sintesis dan implementasi ke atas rekabentuk. Keperluan ini telah dicadangkan oleh salah seorang tenaga pengajar VHDL di Xilinx, Inc. iaitu saudara Rhett Whatcott.

- **Peranti FPGA Xilinx XC4000X**

  Pemilihan peranti FPGA yang sesuai hanya dilakukan setelah melalui peringkat sintesis, yang mana maklumat-maklumat rekabentuk seperti bilangan get terjana, akan mempengaruhi pemilihan peranti tersebut. FPGA yang dipilih adalah daripada

keluarga XC4000X. Sebagai peranti sasaran permulaan, FPGA Xilinx model XC4052XLA HQ240 digunakan untuk sebarang pengujian implementasi. Setelah beberapa ujian implementasi dilakukan, peranti ini didapati paling sesuai untuk mewakili rekabentuk cip inkripsi ini. Pemilihan peranti ini akan dibincangkan secara terperinci dalam Bab 5.

1.5.4 Organisasi Tesis

Dalam bab pertama iaitu Bab Pengenalan, bidang kriptografi akan diterangkan secara terperinci. Bab ini akan membincangkan definisi dan peranan kriptografi, serta proses inkripsi yang dilalui oleh suatu maklumat. Perbandingan di antara kriptografi perisian dan kriptografi perkakasan juga turut dibincangkan. Bahagian terakhir dalam bab ini akan memaparkan topik berkenaan kajian dan tesis yang dijalankan, termasuklah objektif, kaedah pelaksanaan dan keperluan kajian.

Bab seterusnya akan mengupas topik-topik berkenaan medium rekabentuk dan peranti sasaran yang digunakan, iaitu VHDL dan FPGA. Antara topik-topik yang dibincangkan ialah perbandingan kedua-dua elemen ini dengan elemen-elemen lain serta kebaikan penggunaan kedua-dua elemen tersebut dalam rekabentuk yang dibuat. Bab ini juga akan membincangkan keberkesanan penggabungan penggunaan VHDL dan FPGA dalam suatu rekabentuk. Aliran rekabentuk menggunakan perisian Xilinx Foundation Series turut dibincangkan.

Algoritma Blowfish yang menjadi nadi kepada kajian ini akan dibincangkan dalam Bab 3. Sebagai pendahuluan, jenis-jenis algoritma kriptografi telah diperkenalkan berserta komponen utamanya, iaitu kunci algoritma. Penerangan berkenaan algoritma Blowfish pula merangkumi komponen-komponen utama Blowfish, iaitu sub-kunci, inkripsi, dikripsi dan penghasilan sub-kunci, serta penggunaan Kotak-S sebagai penyimpan sub-kunci. Selain itu, kupasan berkenaan rangkaian Feistel yang digunakan dalam algoritma ini juga dipaparkan.

Antara intipati kepada tesis ini ialah maklumat berkenaan rekabentuk yang dijalankan. Maklumat rekabentuk ini dipaparkan dalam Bab 4. Dua peringkat rekabentuk bagi algoritma Blowfish, iaitu peringkat penghasilan sub-kunci dan peringkat inkripsi data akan dibincangkan lebih lanjut dalam bab ini. Maklumat-maklumat lain yang berkaitan dengan rekabentuk cip inkripsi ini seperti perisian pilihan dan aliran rekabentuknya, teknik rekabentuk yang digunakan, komponen rekabentuk serta aliran data keseluruhan bagi cip inkripsi turut dipaparkan.

Bab 5 pula akan membincangkan keputusan yang diperolehi daripada rekabentuk cip inkripsi ini secara menyeluruh. Keputusan bagi setiap peringkat rekabentuk yang dilalui oleh rekabentuk tersebut dipaparkan dan ulasan dibuat untuk setiap keputusan yang diperolehi. Maklumat-maklumat penting bagi suatu cip inkripsi seperti penggunaan ruang FPGA, bilangan kitar jam yang diperlukan untuk suatu proses inkripsi dan dikripsi beroperasi, kelajuan cip inkripsi, dan celusan yang diperolehi juga akan dihuraikan berdasarkan analisa data tersebut.

Bahagian terakhir bagi tesis ini ialah kesimpulan kajian dan rancangan untuk memperbaiki rekabentuk cip inkripsi ini. Masalah-masalah yang dihadapi semasa menjalankan kajian ini dan cara menanganinya juga turut dibincangkan.

BAB 2

VHDL DAN FPGA

2.1 Pengenalan

Peningkatan struktur dan kebolehan FPGA *(Field Programmable Gate Array)* telah mendorong perekabentuk kriptografi untuk menerapkan rekabentuk mereka ke dalam FPGA. Pendekatan ini masih baru dan penggunaannya dalam bidang kriptografi tidak begitu meluas. Oleh itu, rekabentuk cip inkripsi Blowfish kali ini telah menggunakan pendekatan ini untuk membuktikan kebolehan VHDL dan FPGA ke atas rekabentuk algoritma kriptografi. Rekabentuk ini menggunakan VHDL sebagai elemen kemasukan rekabentuk. Selepas kod rekabentuk dalam bentuk VHDL ini disintesis, rekabentuk tersebut akan diimplemenkan ke dalam suatu peranti tersedia iaitu FPGA. Perisian Xilinx Foundation Series V2.1 telah digunakan untuk mewakili perkaitan kedua-dua elemen ini. Bab ini akan mengupas topik-topik yang berkaitan dengan VHDL dan FPGA serta keberkesanan penggunaan VHDL ke atas rekabentuk FPGA.

2.2 VHDL

Very-High-Speed-Integrated-Circuit (VHSIC) *Hardware Description Language* atau ringkasnya VHDL adalah satu pendekatan rekabentuk yang semakin popular di kalangan perekabentuk cip di seluruh dunia. VHDL adalah satu bahasa pengaturcaraan yang direkacipta khusus untuk memperihalkan litar dan sistem digital (Pellerin, 1999). Keberkesanannya dalam penciptaan litar-litar elektronik digital yang kompleks tidak dapat dinafikan lagi kerana ia memudahkan pengujian suatu rekabentuk menggunakan simulasi dan sintesis.

Sebenarnya, VHDL telah dicipta untuk memudahkan rekabentuk cip. VHDL yang lahir pada awal tahun 1980-an ini adalah produk yang dihasilkan semasa projek penyelidikan litar terkamil kelajuan tinggi yang dibiayai oleh Kementerian Pertahanan Amerika Syarikat yang ketika itu sedang dijalankan (Pellerin, 1999). Keperluan rekabentuk yang semakin kompleks dan bersaiz besar ketika itu menyebabkan sekumpulan jurutera daripada tiga (3) buah syarikat, iaitu IBM, Texas Instrument, dan Intermetrics, telah digabungkan oleh kementerian ini untuk menyempurnakan spesifikasi implementasi bahasa pemperihal rekabentuk ini. Namun, versi untuk kegunaan umum, iaitu versi 7.2 hanya digunakan pada tahun 1985 (Pellerin, 1999).

Secara umumnya, VHDL boleh digunakan sebagai bahasa rekabentuk yang universal, tetapi kebolehannya lebih menjurus kepada rekabentuk sistem digital. Untuk mencapai matlamat rekabentuk, pelbagai metodologi boleh dilakukan menggunakan VHDL, seperti teknik atas-ke-bawah *(top-down)* dan bawah-ke-atas *(bottom-up)*. Seperti yang

telah dinyatakan sebelum ini, perkakas utama yang berfungsi dalam VHDL ialah simulasi dan sintesis.

2.2.1 VHDL dan Kaedah Skematik

Sebelum penemuan VHDL, perekabentuk telah menggunakan kaedah skematik. Akibat perkembangan teknologi, kaedah tradisional ini tidak lagi menjadi pilihan kerana keupayaan peranti terkini menyebabkan kebolehan kaedah skematik menjadi terhad dan memakan masa. Oleh itu, ramai perekabentuk kini telah beralih kepada penggunaan VHDL kerana kaedah skematik didapati mempunyai banyak kelemahan walaupun ia adalah kaedah yang termudah. Kaedah tradisional ini menspesifikasikan sistem sebagai suatu rangkaian sambungan elemen-elemen, walhal dalam keadaan yang sebenarnya tidak begitu. Suatu spesifikasi sistem selalunya diberikan dalam bentuk kelakuan sistem jangkaan. Kaedah tradisional ini juga tidak berupaya untuk menampung rekabentuk litar yang kompleks dan tidak praktikal untuk peranti-peranti terkini yang terdiri daripada berjuta-juta get logik.

2.2.2 Kelebihan VHDL

Penggunaan VHDL kini kian berkembang. Sudah tentu perkembangan sebegini dikaitkan dengan keupayaan bahasa ini sendiri ke atas sebarang rekabentuk. Antara kelebihannya yang paling ketara ialah bahasa HDL ini boleh digunakan ke atas sebarang logik boleh-aturcara *(programmable logic)* dan ASIC *(Application Spesific*

Integrated Circuit). Ini bermakna ia bebas diimplemenkan ke atas sebarang PLD dan ASIC. Di samping itu, penggunaannya sebagai pintu bagi kemasukan rekabentuk banyak ditawarkan oleh perisian-perisian rekabentuk. Selain itu, VHDL juga membenarkan simulasi dilakukan ke atasnya sebagai medium pengujian rekabentuk.

Kebanyakan peralatan sintesis logik terkini membenarkan pembinaan rekabentuk peringkat get yang dioptimumkan terus daripada VHDL. Sintesis VHDL dipercayai telah dapat meningkatkan produktiviti sesuatu rekabentuk, terutamanya rekabentuk yang besar.

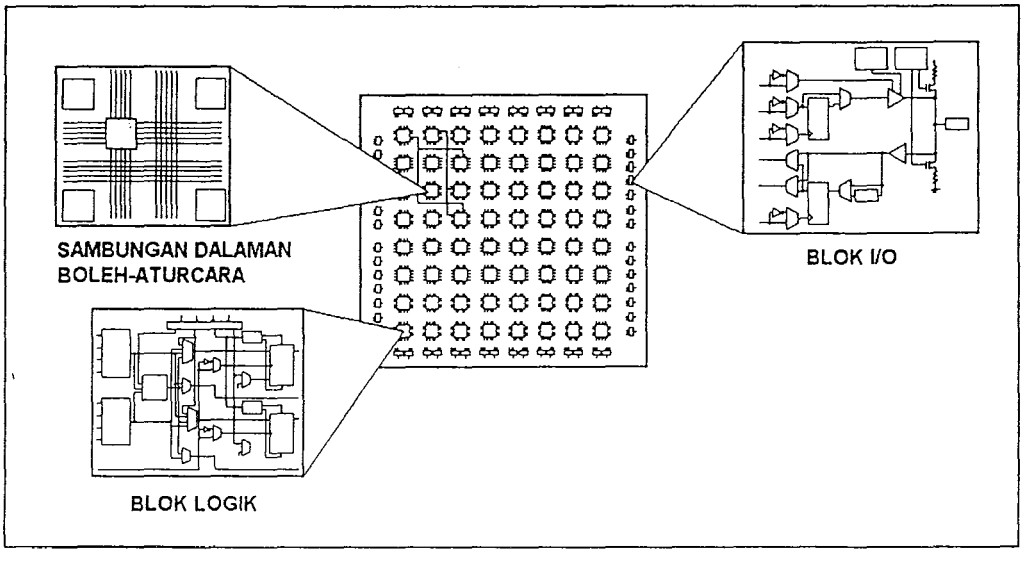
VHDL juga berkebolehan dalam penggunaan semula rekabentuk ke atas projek yang lain atau rekabentuk seterusnya. Ini adalah kerana VHDL ialah bahasa yang piawai, dan telah ditawarkan oleh kebanyakan perisian rekabentuk. Secara tidak langsung, penggunaan semula ini juga dapat meningkatkan produktiviti dan menjimatkan masa suatu proses rekabentuk.

2.3 FPGA

FPGA adalah ringkasan bagi *Field-Programmable Gate Array*, yang kini semakin luas penggunaannya sebagai peranti untuk memindah-turunkan *(downloading)* rekabentuk litar. FPGA sebenarnya lahir daripada perubahan teknologi yang dilakukan ke atas PLA *(programmble logic array)* yang wujud seawal tahun 1970-an. FPGA didefinisikan sebagai peranti logik boleh-aturcara yang terdiri daripada beribu-ribu blok bangunan semesta yang dikenali sebagai tatarajah blok logik (CLBs), yang mana

penyambungannya terdiri daripada susunan laluan dan suis boleh-ubah, yang bergantung kepada rekabentuk yang digunakan (XESS, 1999). Sebelum ini, litar-litar yang direkabentuk perlu melalui proses fabrikasi yang banyak memakan masa dan menelan belanja yang tinggi, lebih-lebih lagi di negara kita. Penemuan FPGA sebenarnya merupakan penyelamat bagi keadaan ini.

Gate array dalam FPGA ialah suatu komponen yang mengandungi sejumlah besar get yang mempunyai fungsi dan sambungan dalaman yang hanya akan ditentukan selepas suatu rekabentuk dimasukkan ke dalam FPGA tersebut. *Field-programmable* pula membolehkan perekabentuk menentukan atau memprogram sendiri fungsi dan sambungan dalaman *(interconnect)* pada peringkat keadaan tertentu (Katz, 1994). Peranti FPGA mempunyai binaan seperti tatasusunan-get *(gate-array-like architecture)* dengan sel logik yang disusun secara matriks yang dikelilingi oleh sel masukan/keluaran (I/O) (lihat Rajah 2.1). FPGA menggabungkan banyak get logik, daftar, dan I/O dengan kelajuan sistem yang pantas.

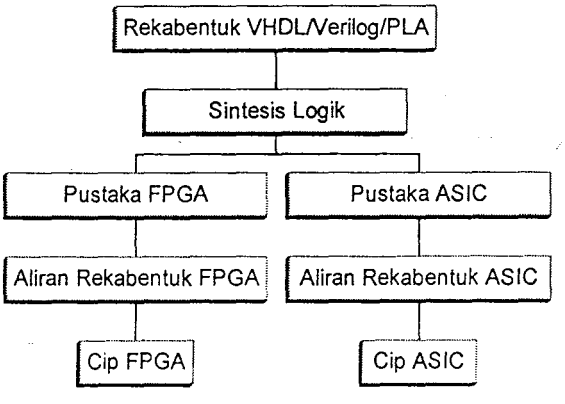


Rajah 2.1: Binaan FPGA (Xilinx, 1999b)

Sebagai sebuah syarikat yang terkenal dalam bidang mikroelektronik, Xilinx Inc., telah menghasilkan pelbagai jenis FPGA yang mempunyai kapasiti dan kebolehan berbeza. Xilinx menawarkan beberapa keluarga FPGA yang boleh-aturcara dan berasaskan ingatan statik *(SRAM based)*, termasuklah siri Virtex, Spartan, XC3000, XC4000, dan XC5000. Walau bagaimanapun, pemilihan jenis FPGA dalam suatu rekabentuk bergantung kepada jenis dan spesifikasi rekabentuk yang digunakan.

2.3.1 Perbezaan antara FPGA dan ASIC

Selain FPGA, terdapat satu lagi peranti yang seakan-akan sama dengan FPGA, yang juga bertindak sebagai peranti sasaran, iaitu ASIC. Jika dilihat sekali imbas, aliran rekabentuk bagi kedua-dua peranti ini adalah sama (Rajah 2.2).



Rajah 2.2: Aliran rekabentuk sintesis kelakuan bagi FPGA dan ASIC

Perbezaan yang paling ketara di antara kedua-dua peranti ini ialah ASIC memerlukan seseorang perekabentuk itu menetapkan dan memastikan rekabentuknya memenuhi apa

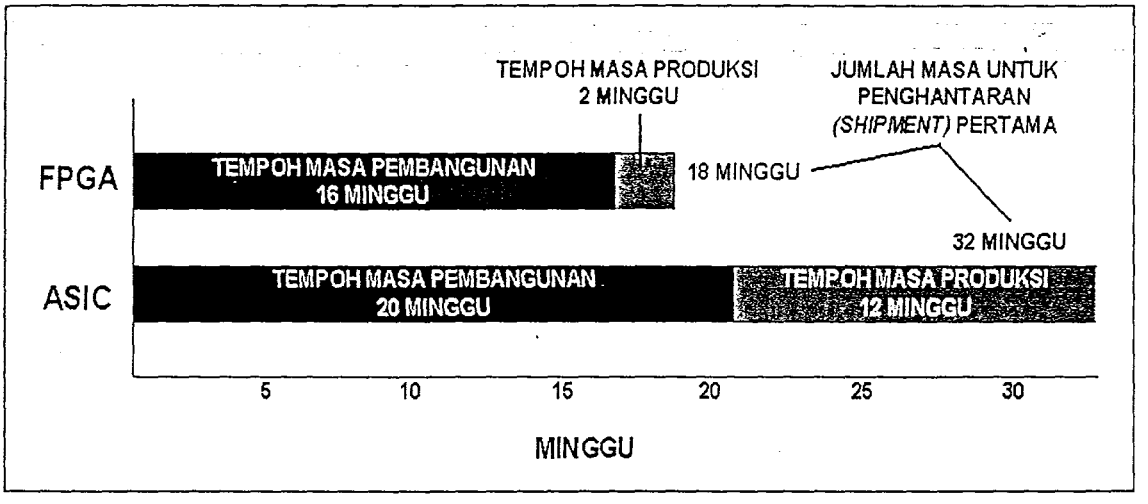
yang dikehendaki kerana selepas rekabentuk tersebut diimplemenkan, rekabentuk tersebut tidak boleh diubah lagi. Oleh itu, kita dapat menafsirkan ASIC sebagai peranti yang digunakan khusus untuk rekabentuk yang tetap. Walaupun kos produksinya adalah rendah, kos untuk memulakan suatu rekabentuk menggunakan ASIC adalah tinggi (Bouldin, 2000).

Ini berbeza dengan FPGA yang membenarkan seseorang perekabentuk itu mengubah rekabentuknya walaupun telah diimplementasi. FPGA juga tidak tertakluk kepada sebarang aplikasi. Oleh itu, FPGA boleh dijadikan sebagai peranti sasaran oleh kebanyakan perkakasan rekabentuk berasaskan komputer (CAD). Keadaan ini akan memudahkan proses merekabentuk dan amat sesuai diterapkan sebagai bahan pembelajaran.

Dengan merekabentuk fungsi ASIC ke dalam FPGA, seseorang perekabentuk itu dapat menjimatkan wang, usaha, dan luas papan. Dengan hanya satu rekaan, fungsi tersebut boleh dijadikan hak intelektual persendirian, dan boleh digunakan berulang kali. Misalnya, perubahan rekabentuk dari A ke B, hanya memerlukan perubahan ke atas program FPGA, sedangkan papan yang digunakan masih sama. Kadang-kala, rekabentuk A dan B tersebut boleh dimasukkan ke dalam papan yang sama dan disimpan di dalam bahagian ingatan, cuma penentuan aplikasi sahaja yang diperlukan (Lesea, 1998).

Terdapat kelebihan yang ketara dalam penggunaan logik boleh-aturcara berbanding ASIC dalam pembangunan dan produksi rekabentuk. Masa yang agak lama diambil oleh ASIC untuk proses pembangunan dan produksi suatu rekabentuk berbanding

penggunaan FPGA, iaitu perbezaan sebanyak 14 minggu (lihat Rajah 2.3). Selain itu, keupayaan FPGA yang menyokong aliran rekabentuk VHDL dan Verilog memudahkan perpindahan perekabentuk ASIC kepada penggunaan FPGA. Kemajuan teknologi pemprosesan telah banyak menyumbang kepada harga FPGA yang lebih sesuai berbanding ASIC. Maka, tidak hairanlah jika pengguna ASIC yang amat menitik-beratkan harga, masa produksi, dan kebolehan untuk boleh-aturcara, telah berpindah kepada penggunaan FPGA (Sharp, 1998).



Rajah 2.3: Perbezaan masa yang diambil oleh FPGA dan ASIC untuk proses pembangunan dan produksi (Sharp, 1998)

2.3.2 Kelebihan FPGA

Kebanyakan perekabentuk kini telah beralih kepada penggunaan FPGA kerana ia mempunyai beberapa kelebihan yang ketara berbanding peranti-peranti lain. Penggunaan FPGA dapat mengelakkan proses fabrikasi yang banyak memakan masa dan belanja. Kewujudan get-get yang tersedia di dalam FPGA didapati menjimatkan. Seseorang perekabentuk itu tidak perlu membuat pemasangan litar yang berselirat ke