PENERAPAN ALUR DESAIN ALLIANCE DALAM PERANCANGAN *CORE* PROSESOR KRIPTO IDEA

Sarwono Sutikno, Aditya Timur Baladika,
Marta Dinata A., dan Sigit Dewantoro
VLSI Research Group, Laboratorium Elektronika dan Komponen, Labtek VIII Lt. 3,
Departemen Teknik Elektro, Institut Teknologi Bandung, Indonesia
Jalan Ganesha 10 Bandung 40135, Telp. 022-2509172 ext. 3223
ssarwono@ieee.org, aditya@ic.vlsi.itb.ac.id, marta@ic.vlsi.itb.ac.id, sigit@ic.vlsi.itb.ac.id

Abstrak

Alliance merupakan sekumpulan tool CAD (Computer Aided Design) lengkap dan tersedia gratis dan digunakan untuk membantu proses perancangan core rangkaian terintegrasi digital mulai dari rangkaian sederhana sampai yang komplek dengan jutaan transistor. Alliance ini digunakan untuk merancang prosesor kripto IDEA (International Data Encryption Algorithm). Perancangan dengan menggunakan tool-tool ini meliputi beberapa tahap yaitu pendeskripsian rangkaian secara behavioral dan struktural dalam bentuk VHDL (Very High Speed Integrated Circuit Hardware Description Language), sintesis deskripsi behavioral ke sel standar, routing layout rangkaian, dan verifikasi setiap tahap. Layout rangkaian dibentuk oleh tool Alliance secara otomatis dengan masukan berupa deskripsi VHDL.

Prosesor kripto IDEA yang dirancang dengan menggunakan Alliance ini berfungsi untuk menyandikan data rahasia yang akan dikirim melalui jalur komunikasi untuk menjadi data random dengan menggunakan sebuah kunci sehingga data itu menjadi aman dari ancaman pihak lain. IDEA merupakan salah satu jenis algoritma penyandian kunci simetrik yang masih digunakan sebagai algoritma standar dalam penyandian data saat ini. Pengirim data dan penerima data meggunakan kunci rahasia yang sama yang masing-masing digunakan untuk menyadikan data yang akan dikirim dan menerjemahkan data yang diterima. Prosesor kripto ini dapat bekerja untuk mengenkripsi data rahasia dan mendekripsi data random dalam sistem bus data PCI yang menggunakan frekuensi kerja 33 MHz.

Kata Kunci : kripto, VHDL, layout, alliance

1. Pendahuluan

Dewasa ini produksi chip berkembang pesat seiring dengan kebutuhan konsumen. Sebelum proses produksi chip terdapat tahap perancangan rangkaian yang membentuk chip itu. Untuk perancangan diperlukan *tool* yang berfungsi untuk simulasi. Proses simulasi merupakan hal yang terpenting dilakukan pada tahap perancangan IC. Biasanya untuk proses simulasi dibutuhkan waktu sekitar 40-50 % dari total waktu tahap perancangan. Dengan demikian aspek simulasi menjadi suatu hal yang sangat penting dalam proses terciptanya sebuah chip yang siap pakai. *Alliance VLSI CAD tools* merupakan salah satu perangkat perancangan dan simulasi yang ditampilkan dalam perannya untuk membantu perancangan chip [1]. Pada kasus ini dirancang sebuah prosesor Kripto IDEA (*International Data Encryption Algorithm*) dengan menggunakan *tool* tersebut.

IDEA merupakan algoritma penyandian yang masih digunakan sebagai standar dalam penyandian yang menggunakan kunci simetris [6]. Algoritma penyandian IDEA, muncul pertama kali tahun 1990, dikembangkan oleh Xuejia Lai dan James L. Massey. Setelah itu di Depatemen Teknik Elektro, Institut Teknologi Bandung dilakukan penelitian dalam pengimplementasian algorima ini ke perangkat keras.

Spesifikasi prosesor kripto IDEA yang dirancang ini adalah kompatibelitas dengan bus data PCI dengan frekuensi *clock* 33 MHz [2], kemampuan melakukan proses enkripsi dan proses deskripsi, dan teknologi target 1 mikron.

Perancangan *core* prosesor ini telah dipublikasikan dalam komunitas *opencores* yang dapat dilihat di http://www.opencores.com/cores/idea.

2. Sekilas tentang *Alliance VLSI CAD tools*

Alliance berisikan sekumpulan *tool* CAD meliputi *tool* untuk simulator logika, sintesis logika, *place and route*, verifikasi layout. *Alliance* merupakan hasil perancangan dan pengembangan yang dilakukan di Laboratorium ASIM, Pierre et Merie Curie University, Paris, Perancis [1].

2.1. Kenapa Harus Memakai Alliance ?

Alasan digunakan *Alliance* dalam perancangan ini adalah sbb.:

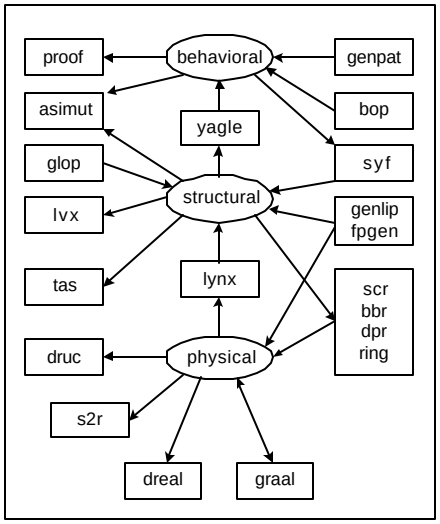
- **Bebas Teknologi Proses**
  Alliance memiliki sejumlah library layout yang mengandalkan pendekatan layout simbolik. Pendekatan ini memberikan kebebasan dalam pemilihan teknologi proses sehingga para desainer akan mudah dan cepat mentransfer desain mereka dari satu penyuplai silikon ke penyuplai lainnya yang masing-masing menggunakan teknologi yang berbeda. Dengan demikian *time to market* dapat menjadi lebih singkat dimana *time to market* sekarang ini menjadi aspek yang sangat penting dalam produksi peralatan elektronik.
- **Bersahabat dengan berbagai OS dan platform**
  Paket Alliance telah dirancang untuk bekerja pada berbagai platform dan jaringan komputer. Sampai sekarang Alliance dapat bekerja pada sistem Linux, FreeBSD, SunOS, Spartac, dan Windows. Untuk aplikasi grafik, library Xwindow dapat digunakan digunakan. Beberapa platform hardware, dari mikrokomputer berbasiskan Intel 386 sampai Sparc Stations dan DEC Stations didukung oleh Alliance.
- **Mandiri dan saling berhubungan**
  Dari sekian banyak tool Alliance masing-masingnya dapat bekerja sebagai program yang berdiri sendiri sebagai bagian dari kerangka besar desain Alliance yang lengkap. Karena itu setiap tool Alliance mendukung beberapa format deskripsi VLSI standar : SPICE, EDIF, VHDL, CIF, dan GDS2.
- **Kompak**
  Tidak seperti system CAD komersial yang ada, system CAD Alliance bisa bekerja pada workstation sederhana dengan resource sistem yang cukup kecil. Untuk proyek pendidikan yang kecil, misal 5000 gerbang, Alliance cukup menggunakan sebuah sistem Unix dengan kapasitas memori 8 sampai 20 Mbytes, penyimpanan data pada disk sebesar 30 Mbytes tiap user, dan kemampuan grafik.
- **Mudah dipahami**
  Semua tool dan flow desain bisa dipelajari dan diajarkan dengan mudah.. Pada tahap desain dapat digunakan satu tool atau lebih selama penggunaanya sesuai. Untuk pedoman penggunaan Alliance secara praktis tersedia dokumentasi dalam bentuk online (Unix man) dan paper.
- **Tersedia *Free***
  Alliance tersedia *free* untuk semua pengguna diseluruh dunia yang daatur oleh General Public License (GNU).

2.2. Alur Perancangan dengan Menggunakan Alliance

Dibawah ini diperkenalkan alur utama dari metoda desain *Alliance* untuk merealisasikan rangkaian VLSI. Alur itu terdiri dari 5 bagian, yaitu :

1. Pembentukan dan verifikasi deskripsi behavioral
2. Pembentukan dan verifikasi deskripsi struktural
3. Implementasi dalam bentuk fisik yaitu layout rangkaian
4. Verifikasi layout rangkaian
5. Tes dan evaluasi menyeluruh

2.3. Tool-tool Alliance



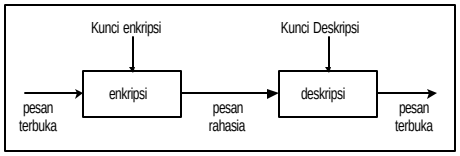
Gambar 1. Tool Alliance

Pada Gambar 1 dapat dilihat sejumlah tool Alliance yang berhubungan dengan tiga buah level deskripsi rangkaian, yaitu behavioral, struktural, dan fisik.

3. Kriptografi dan IDEA

Kriptografi merupakan suatu cabang ilmu yang mempelajari seluk beluk penyandian pesan sehingga suatu pesan menjadi aman. Dalam hal ini dikenal dua jenis pesan yaitu pesan terbuka dan pesan rahasia. Pesan terbuka merupakan pesan asli yang belum disandikan sedangkan pesan rahasia adalah pesan asli yang sudah disandikan. Proses pembentukan pesan rahasia dari pesan terbuka disebut enkripsi dan proses sebaliknya disebut deskripsi. Kedua proses enkripsi dan deskripsi itu masing-masing memerlukan sebuah kunci yaitu kunci enkripsi dan kunci deskripsi.

Proses enkripsi dan deskripsi dapat dipandang sebagai suatu sistem terintegrasi yang disebut dengan sistem kriptografi, yang ditunjukkan oleh Gambar 2, untuk membentuk fungsi penyandian yang diharapkan.



Gambar 2. Sistem Kriptografi

IDEA merupakan algoritma penyandian simetris yang beroperasi pada sebuah blok pesan terbuka 64-bit. Digunakan kunci yang sama, berukuran 128-bit, untuk proses enkripsi dan deskripsi. Pesan rahasia yang dihasilkan berupa sebuah blok 64-bit juga. Sebelum kunci enkripsi digunakan pada proses enkripsi, kunci itu dibagi menjadi 52 buah subkunci 16-bit dengan cara rotasi kiri. Proses deskripsi menggunakan algoritma yang sama dengan proses enkripsi namun 52 buah subkunci deskripsinya harus diturunkan dari 52 buah subkunci enkripsi.

Pesan terbuka yang akan dikirim ini dapat berupa aliran bit, file teks, aliran suara digital, atau citra video digital yang disimbolkan dengan *M*,. Pesan rahasia disimbolkan dengan *C* yang bisa berukuran sama atau tidak dengan *M* Fungsi enkripsi *e* dioperasikan pada pada *M* untuk menghasilkan *C* dengan menggunakan kunci enkripsi K_1, yang ditulis secara matematis sebagi berikut

$$e_{K_1}(M) = C$$

Dalam proses deskripsi, fungsi deskripsi *d* dioperasikan pada *C* dengan menggunakan kunci deskripsi K_2 , dimana $K_2 = K_1$ pada algoritma ini, untuk menghasilkan *M* sebagai berikut

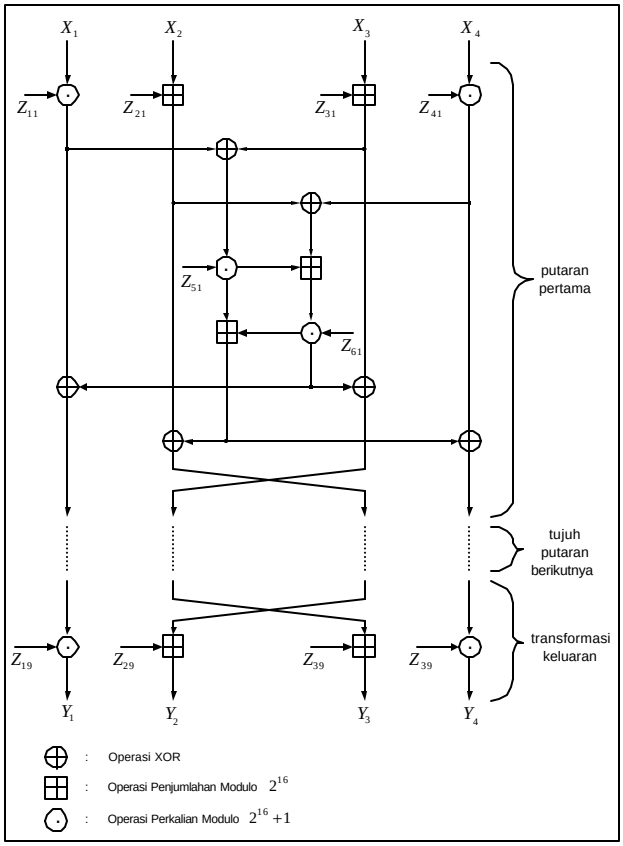
$$d_{K_2}(C) = M$$

Karena proses enkripsi dan deskripsi adalah untuk memperoleh pesan terbuka, seperti pada Gambar 2, maka beralaku identitas berikut

$$d_{K_2}(e_{K_1}(M)) = M$$

Algoritma ini menggunakan operasi campuran dari tiga operasi aljabar yang berbeda, yaitu operasi XOR, operasi penjumlahan modulo 2^{16} dan operasi perkalian modulo $2^{16} + 1$. Semua operasi ini digunakan dalam pengoperasian sub-blok 16-bit.

Algorima ini melakukan proses iterasi yang terdiri dari 8 putaran dan 1 transformasi keluaran, dimana gambaran komputasi untuk putaran pertama dan transformasi keluaran ditunjukkan pada Gambar 3.



Gambar 3. Algoritma IDEA

4. Penggunaan Alur Desain Alliance dalam Perancangan *Core* Prosesor Kripto IDEA

Sebelum lebih jauh melangkah dalam penggunaan alur desain alliance untuk merancang *core* prosesor kripto IDEA, perlu dijelaskan arsitektur umum prosesor IDEA itu. Seperti terlihat pada arsitektur umum prosesor IDEA yang ditunjukkan oleh Gambar 4,

prosesor IDEA dibentuk oleh sejumlah blok penyusun yaitu :

1. Blok penyandi IDEA
   Blok ini berfungsi untuk melakukan proses penyandian data. Jika subkunci yang diproses oleh blok ini berupa subkunci enkripsi maka pesan yang dihasilkannya adalah pesan rahasia dan jika yang di proses berupa subkunci deskripsi maka pesan yang dihasilkan adalah pesan sebenarnya.

2. Blok pembangkit subkunci
   Blok ini berfungsi untuk membentuk 52 buah subkunci enkripsi 16 bit dari kunci enkripsi 128 bit dan membentuk 52 buah subkunci deskripsi 16 bit dari kunci deskripsi 128 bit.

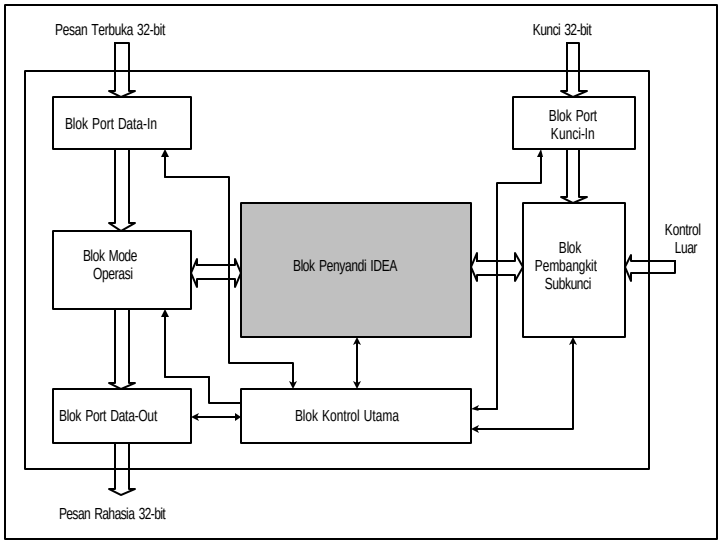
3. Blok port data-in
   Blok ini berfungsi untuk membaca 2 buah blok data masukan 32 bit dan menyimpannya sebagi blok data masukan 64 bit yang akan dienkripsi atau dideskripsi.

4. Blok port data-out
   Blok ini berfungsi untuk mengeluarkan blok data keluaran 64 bit yang merupakan hasil enkripsi atau deskripsi dengan cara membaginya menjadi 2 buah blok data keluaran 32 bit.

5. Blok port kunci-in
   Blok ini berfungsi untuk membaca 4 buah blok kunci 32 bit dan menyimpannya sebagai blok kunci 128 bit.

6. Blok mode operasi
   Blok ini berfungsi untuk menentukan mode operasi yang digunakan pada proses enkripsi dan deskripsi.

7. Blok kontrol
   Blok ini berfungsi untuk mengontrol operasi antara blok fungsional yang menyusun sebuah blok yang lebih besar seperti sinkronisa transfer data antara blok.



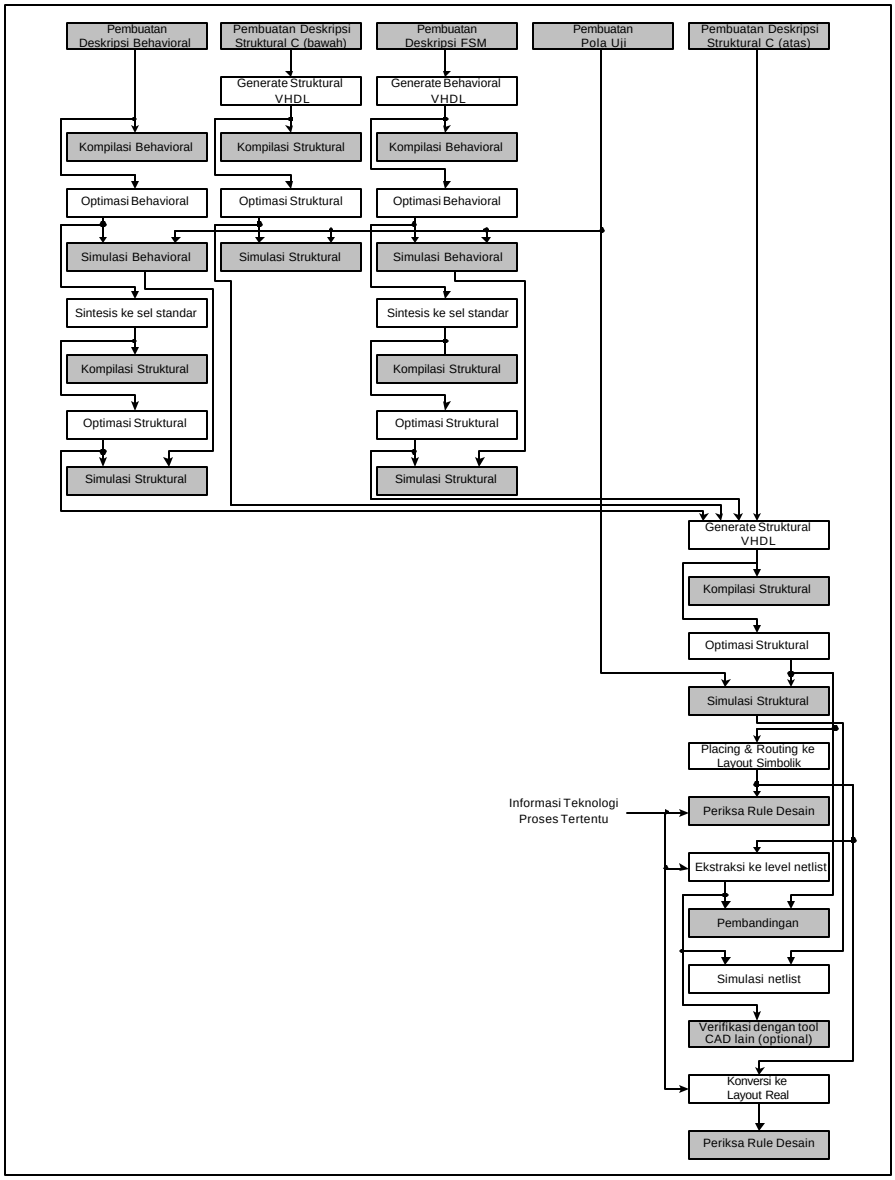
Gambar 4. Arsitektur Umum Prosesor IDEA

Pada Gambar 5 dapat dilihat alur desain dengan menggunakan tool Alliance untuk semua blok-blok penyusun blok prosesor kripto IDEA. Tahap perancang itu dimulai dengan pembentukan deskripsi blok-blok fungsional secara behavioral, struktural c, dan fsm dan pembentukan pola uji untuk masing-masing blok yang berhubungan. Akhir dari alur perancangan itu adalah layout *real* yang telah tervalidasi dan siap diproses di *silicon foundry*.

5. Kesimpulan

Perancangan dan simulasi *core* prosesor kripto IDEA telah berhasil dilakukan dengan meggunakan sejumlah tool Alliance dan mengikuti alur perancangan VLSI yang diberikan oleh Alliance untuk teknologi proses 1 mikron. Hasil simulasi fungsional, baik pada kondisi *delay* nol maupun tidak (kondisi *real*), terhadap semua blok penyusun yang dirancang telah menunjukkan hasil yang diinginkan untuk mencapai fungsi penyandian dengan algoritma IDEA.

Hasil rancangan *core* blok penyandi prosesor IDEA mempunyai 67 *clock cycle* untuk memproses data



Gambar 5. Alur Perancangan *Core* Blok Prosesor IDEA dengan Menggunakan Alliance

input 64 bit untuk menghasilkan data output 64 bit. Dengan demikian blok ini memiliki *throughput* sebesar **0,955 bit/*clock cycle*** . Blok penyandi ini bekerja sampai frekuensi clock **16,17** Mhz berdasarkan hasil simulasi yang diperoleh, yang berarti spesifikasi frekuensi *clock* 33 MHz belum tercapai. Jika prsosesor ini diintegrasikan pada system dengan frekuensi 16,17 MHz maka kecepatan transfer datanya adalah sebesar **16 Mbit/detik**. Sedangakan jumlah sel standar yang digunakan adalah sebanyak 25310 buah.

Rancangan ini memerlukan optimasi lebih lanjut terhadap berbagai hal seperti *delay*, *fanout*, dan lain-lain sehingga bisa didapatkan hasil yang lebih baik Untuk memperbesar *troughput* diperlukan perancangan dengan menggunakan teknik *pipeline*.

Referensi

[1] ASIM, *Alliance: A Complete CAD System for VLSI Design*, http://www-asim.lip6.fr/alliance.

[2] Dipert Brian, *The PCI Handbook*, Annabooks, San Diego, 1995

[3] Gajski D., *Principle of Digital Design*, Prentice-Hall, 1997.

[4] H. Bonnenberg, A. Curiger, R. Zimmermann, N. Felber, H. Kaeslin, W. Fichtner, "VINCI: VLSI Implementation of The New Block Chiper IDEA", *Proceeding of IEEE CICC*, 1993.

[5] Man Young Ree, *Cryptography and Secure Communications*, McGraw-Hill, Singapore, 1994.

[6] Menezes Alfred J., Oorschot Paul C. van, Vanstone Scott A., *Handbook of Applied Cryptography*, CRC Press, USA, 1997.

[7] Schneier B., *Applied Cryptography: Protocols, Algorithms, and Sources Code in C, second edition*, John Wiley & Sons, 1996.

[8] Sherwani Naveed, *Algorithms for VLSI Physical Design Automation*, Kluwer Academic Publishers, Boston, 1995.

[9] Smith Michael J. S., *Application-Spesific Integrated Circuit*, Addison Wesley, 1997.

[10] Smith Douglas J., *HDL Chip Design*, Doone Publications, Madison, 1996

[11] Tinder R., *Digital Engineering Design: A Modern Approach*, Prentice-Hall, 1991.

[12] Xuiejia L. and James L. Massey, "On The Design and Security of Block Chipers", *ETH Series in Information Processing*, v.1, Konstanz: Hartung-Gorre Verlag, 1995.