Serangan Terhadap Kriptografi dengan Teknik *Power Analysis*

Deasy Trisnawati, Prescy Pangastuti S.A., dan Dicky Ekklesia

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if11050@students.if.itb.ac.id, if11051@students.if.itb.ac.id, if11070@students.if.itb.ac.id

Abstrak

Perancang sistem kriptografi seringkali mengasumsikan bahwa informasi rahasia dalam proses enkripsi dan dekripsi dimanipulasi dalam suatu lingkungan perhitungan yang aman dan dapat dipercaya. Pada kenyataannya, komputer-komputer dan *microchip* yang digunakan seringkali membocorkan informasi tentang operasi yang sedang diprosesnya, seperti informasi tentang *power consumption*, radiasi elektromagnetik, dan informasi lainnya. Paper ini mendefinisikan beberapa metode untuk menganalisa pengukuran *power consumption* sehingga dapat menemukan kunci rahasia dari sebuah sistem kriptografi, serta mendiskusikan beberapa pendekatan untuk membangun sistem kriptografi yang dapat beroperasi secara aman pada perangkat-perangkat keras yang dapat mengalami kebocoran informasi.

***Kata kunci**: Differential Power Analysis, Simple Power Analysis, DPA, SPA, serangan, DES, power consumption*

1. Pendahuluan

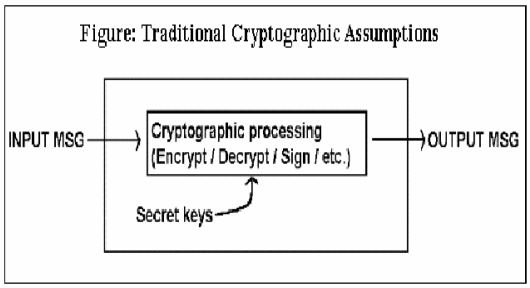
Serangan yang melibatkan beberapa bagian dari sistem keamanan akan sulit untuk diprediksi dan dimodelkan. Jika perancang *cipher*, pengembang perangkat lunak, dan pengembang perangkat keras tidak saling mengetahui pekerjaan masing-masing, asumsi-asumsi mengenai keamanan yang dibuat pada tiap level dari sebuah perancangan sistem mungkin akan menjadi tidak lengkap atau tidak realistis. Sebagai hasil, *security fault* seringkali disebabkan oleh interaksi yang tidak dapat diantisipasi antara komponen-komponen yang dirancang oleh orang-orang yang berbeda. [2]

Peneliti kriptografi telah banyak melakukan analisa tentang bagaimana meningkatkan keamanan dari perangkat kriptografi *portable*, seperti *smart card*. Seiring dengan itu, peneliti juga telah mengembangkan beberapa serangan yang dapat dilakukan terhadap perangkat itu, seperti *Simple Power analysis*, *Differential Power analysis*, *High-Order Differential Power analysis*, dan teknik-teknik lain yang berkaitan. Teknik-teknik ini dinilai sangat kuat, sehingga dapat digunakan oleh kriptanalis untuk mengekstraksi kunci-kunci rahasia dari perangkat-perangkat kriptografi. Penerapan dari teknik-teknik ini adalah dengan mengeksploitasi karakteristik yang sederhana dari *input* dan *output* dalam sebuah sistem kriptografi, kemudian menganalisa sebuah bagian dari arsitektur sistem, yaitu struktur matematis dari algoritma. [3]

2. Pengenalan *Power Analysis*

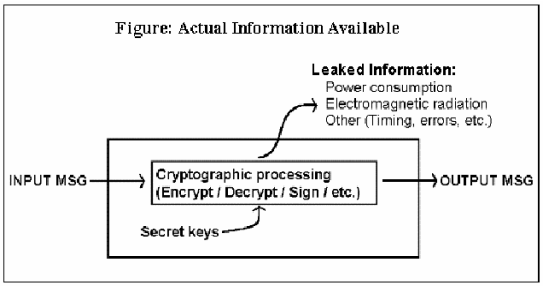
Sebuah perangkat kriptografi menggunakan sebuah kunci rahasia untuk

memproses informasi *input* dan/atau untuk memproduksi informasi *output*. Perancang protokol mengasumsikan bahwa penyerang sistem kriptografi hanya dapat mengetahui informasi *input* dan *output* tersebut, tetapi tidak dapat mengetahui informasi tentang kunci rahasia [3]. Gambar 1 menunjukkan tentang asumsi kriptografi tradisional, dimana penyerang hanya dapat mengetahui plainteks dan/atau cipherteks.



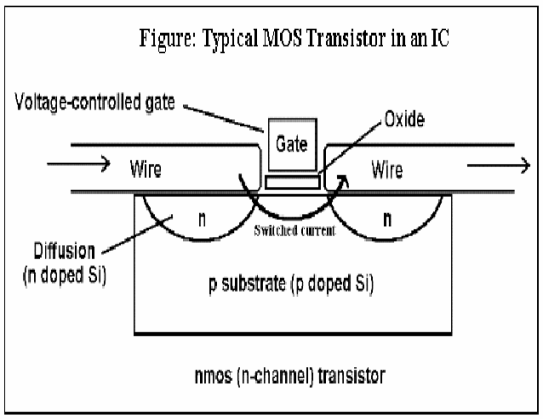
Gambar 1. ***Traditional Cryptographic Assumption***

Walaupun demikian, informasi-informasi lain pada pemrosesan kriptografi seperti informasi tentang *power consumption*, radiasi elektromagnetik, dan yang lainnya seperti *timing* dan error, dapat juga diketahui oleh penyerang sehingga dapat melakukan serangan berdasarkan informasi-informasi ini [3]. Serangan ini disebut serangan dengan menggunakan teknik *Power Analysis*. Gambar 2 menunjukkan informasi-informasi yang dapat diambil pada saat dilakukan pemrosesan kriptografi (proses enkripsi, dekripsi, penandatanganan, dan lain-lain).



Gambar 2. ***Actual Information Available***

Sebagian besar perangkat kriptografi modern dibuat dengan menggunakan gerbang logika semikonduktor, yang dirancang di luar transistor, dan bertindak sebagai *switch* kontrol tegangan, sehingga membentuk sebuah *Integrated Circuit* (IC). Elektron mengalir melalui lapisan bawah transistor ketika *charge* diaplikasikan (atau dihilangkan) dari gerbang transistor. Elektron ini kemudian mengirimkan *charge* pada gerbang transistor lainnya. Pergerakan dari *charge* ini akan mengkonsumsi banyak *power* (*power consumption*) dan memproduksi radiasi elektromagnetik, dimana keduanya dapat dideteksi dengan cukup mudah. Gambar 3 menunjukkan proses yang terjadi pada transistor yang terdapat dalam sebuah *Integrated Circuit* (IC). [2,3]



Gambar 3. ***Typical MOS Transistor in an IC***

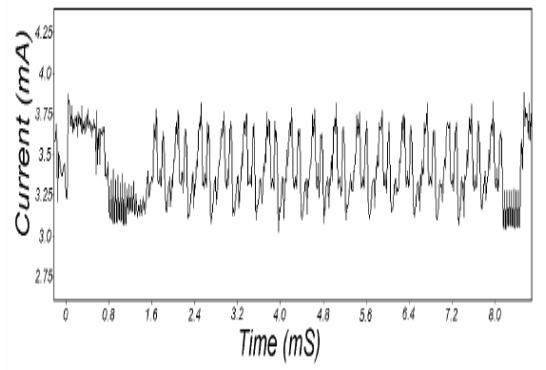
Untuk mengukur *power consumption* dari sirkuit, sebuah resistor kecil (50 ohm) dihubungkan seri dengan *input power* atau *input* dasar. Perbedaan tegangan yang melalui resistor dibagi dengan resistansi atau hambatan yang diukur pada saat itu. Beberapa laboratorium memiliki peralatan yang dapat mengukur perbedaan tegangan pada frekuensi yang tinggi (1 GHz) dengan

ketepatan yang sangat tinggi (kurang dari 1% error). [2,3]

3. *Simple Power Analysis* (SPA)

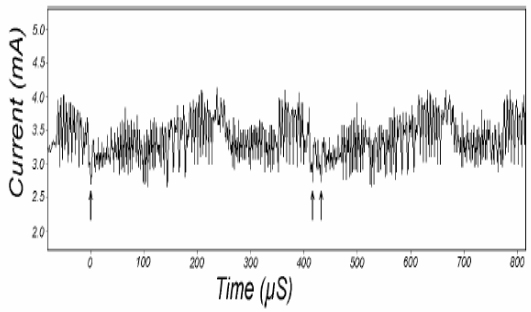
3.1 Teknik *Simple Power Analysis*

SPA merupakan sebuah teknik yang melibatkan pengukuran *power consumption* secara langsung selama operasi kriptografi berlangsung [2]. Jumlah dari *power* yang dikonsumsi berbeda-beda, tergantung pada instruksi mikroprosesor yang dijalankan. Fitur-fitur penting dari sebuah algoritma, seperti putaran DES, operasi RSA, dan fitur-fitur lainnya dapat diidentifikasi dengan cukup mudah, karena operasi-operasi yang dijalankan oleh mikroprosesor berbeda-beda secara signifikan, dan akhirnya menimbulkan perbedaan *power consumption* yang cukup signifikan pada fitur-fitur ini [3]. SPA dapat digunakan untuk memecahkan implementasi RSA dengan memeriksa perbedaan yang signifikan antara operasi perkalian dan pengkuadratan, serta memecahkan implementasi DES dengan memeriksa perbedaan yang signifikan antara operasi permutasi dan *shift* (seperti permutasi PC1 atau rotasi dari register C dan D) [3].



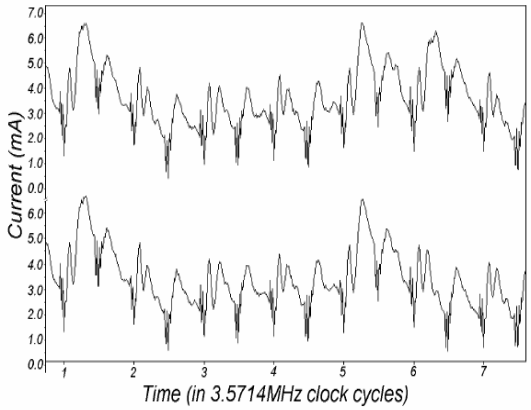
Gambar 4. Pelacakan SPA untuk sebuah operasi DES

Gambar 4 menunjukkan pelacakan SPA dari sebuah *smart card* yang menggunakan operasi DES. Tampak pada gambar bahwa 16 putaran DES dapat dideteksi dengan jelas.



Gambar 5. Pelacakan SPA untuk sebuah operasi DES putaran 2 dan 3

Gambar 5 menggambarkan pelacakan yang lebih detil dari gambar sebelumnya, untuk putaran kedua dan ketiga dari operasi enkripsi DES. Dapat dilihat dari gambar, 28-bit register C dan D dirotasikan satu kali pada putaran ke-2 (panah kiri), dan dua kali pada putaran ke-3 (dua panah kanan).



Gambar 6. Pelacakan SPA yang Menunjukkan *Clock Cycle* yang berbeda

Gambar 6 menunjukkan gambaran resolusi yang lebih tinggi dari pelacakan SPA yang melalui dua daerah, masing-masing

tujuh *clock cycle* pada 3.5714 MHz. Perbedaan yang terdapat di antara *clock cycle* disebabkan oleh adanya perbedaan *power consumption* dari instruksi mikroprosesor yang berbeda. Gambar pelacakan yang pertama pada Gambar 6 menunjukkan jalur eksekusi melalui fitur SPA dimana instruksi *jump* dijalankan. Sedangkan gambar pelacakan yang kedua menunjukkan kasus dimana instruksi *jump* tidak dijalankan. Titik perbedaan dapat dilihat dengan jelas, yaitu pada putaran ke-6.

SPA dapat menunjukkan urutan instruksi yang dieksekusi, sehingga SPA dapat digunakan untuk memecahkan implementasi kriptografi tertentu, bergantung pada operasi dan data yang sedang diproses. Sebagai contoh [2,4]:

Penjadwalan kunci DES
Proses komputasi penjadwalan kunci DES melibatkan pemutaran 28-bit register kunci. Di dalam algoritmanya, pencabangan kondisional tertentu biasanya digunakan untuk memeriksa bit yang digeser ke akhir sehingga salah satu bit dapat mengalami *wrapping***.** Hasil pelacakan *power consumption* untuk bit ‘1’ dan bit ‘0’ akan memberikan fitur SPA yang berbeda, jika jalur eksekusi menggunakan cabang yang berbeda untuk setiap bit.

Permutasi DES
Dalam DES, dilakukan beberapa permutasi bit. Pencabangan tertentu pada perangkat lunak atau *microcode* dapat menyebabkan perbedaan *power consumption* untuk bit ‘0’ dan bit ‘1’.

Perbandingan
Ketidaksesuaian pada operasi perbandingan string dan memori biasanya dijalankan dengan pencabangan kondisional tertentu. Pencabangan tersebut dapat menunjukkan karakteristik SPA.

Perkalian
Operasi perkalian cenderung lebih banyak memberikan atau membocorkan informasi mengenai data yang sedang diprosesnya.

Eksponensial
Fungsi eksponensial melakukan *scanning* terhadap exponen, kemudian melakukan proses pengkuadratan pada tiap iterasi dengan operasi perkalian tambahan untuk setiap bit exponen yang sama dengan ‘1’. Fungsi eksponensial ini dapat digunakan untuk pelacakan, jika operasi pengkuadratan dan operasi perkalian memiliki *power consumption* yang berbeda, membutuhkan waktu yang berbeda, dan dipisahkan oleh kode-kode yang berbeda.

3.2 Pencegahan *Simple Power Analysis*

Teknik untuk pencegahan SPA cukup sederhana untuk diimplementasikan. Diantaranya adalah dengan menghindari penggunaan prosedur yang dapat menunjukkan pencabangan kondisional tertentu, sehingga tidak menunjukkan karakteristik pada pelacakan SPA. Jika suatu algoritma mewariskan banyak pencabangan, maka algoritma tersebut harus dapat dimodifikasi secara kreatif. [2]

Penggunaan perangkat keras dan mode algoritma yang digunakan juga dapat berpengaruh dalam pencegahan SPA. Sebagian besar perangkat lunak *hard-wired* untuk algoritma kriptografi simetri menimbulkan variasi *power consumption* yang tidak terlalu signifikan, sehingga tidak dapat digunakan untuk menemukan kunci yang diinginkan.

4. *Differential Power Analysis* (DPA)

4.1 Teknik *Differential Power Analysis*

DPA merupakan serangan yang jauh lebih kuat dibandingkan dengan SPA, dan lebih sulit untuk dihindari. Jika SPA menggunakan inspeksi visual untuk mengidentifikasi fluktuasi *power*, maka DPA menggunakan teknik analisis statistik dan koreksi *error* untuk mengekstrak informasi yang berkaitan dengan kunci rahasia. [3]

Implementasi DSA terdiri dari 2 fase : pengumpulan data dan analisis data [3]. Pengumpulan data untuk DPA dilaksanakan seperti pada SPA, yaitu dengan pelacakan *power consumption* selama operasi kriptografi sebagai fungsi dari waktu. Untuk DPA, dilakukan observasi tentang jumlah operasi kriptografi yang menggunakan kunci target.

Langkah-langkah berikut ini menunjukkan contoh proses serangan DPA pada sistem kriptografi yang menerapkan algoritma DES [3,4] :

a. Melakukan pengukuran *power consumption* pada beberapa putaran terakhir dari 1000 operasi DES. Setiap sample terdiri dari 100000 item data. Data yang telah dikumpulkan (koleksi data) dapat direpresentasikan sebagai array 2 dimensi S[0..999][0..99999], dimana indeks pertama merupakan nomor operasi, dan indeks kedua merupakan sampel. Untuk contoh ini, diasumsikan bahwa penyerang memiliki cipherteks , C[0..999].

b. Selanjutnya, penyerang memilih fungsi seleksi (D) yang tergantung pada kunci. Dalam kasus ini, fungsi seleksi adalah D(Ki,C), dimana Ki merupakan informasi kunci dan C adalah cipherteks. Misalkan, tujuan dari penyerang adalah untuk menemukan 6 bit dari kunci DES yang merupakan *input* dari S-Box yang menghasilkan 4 bit sebagai keluaran, sehingga Ki adalah masukan 6 bit tersebut. Hasil D(Ki,C) diperoleh dengan melakukan *Initial Permutation* (IP) pada C, sehingga mendapatkan R dan L, melakukan ekspansi terhadap R, melakukan ekstraksi pada masukan 6 bit untuk S4, meng-XOR dengan Ki, dan menggunakan hasil XOR tersebut sebagai *input* untuk operasi *lookup* standar pada DES S4. Setelah itu dilakukan pemilihan sebuah bit target (sebagai contoh, bit yang paling signifikan) dari hasil S. Permutasi P diaplikasikan pada bit tersebut, dan hasil dari fungsi D(Ki,C) di set menjadi 0 jika hasil permutasi P pada bit yang dipilih sama dengan bit yang berkorespondensi pada L. Jika tidak, maka D(Ki,C) adalah 1.

c. Penghitungan T[0..63][0..99999], dari set data S dengan menggunakan hasil dari fungsi D.

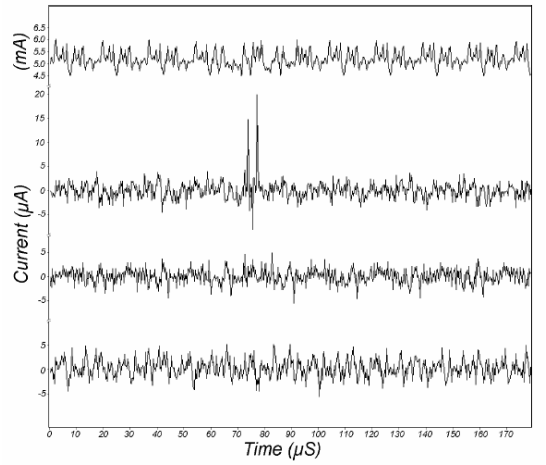
$$T[i][j] = \sum_{k=0}^{999} \left(D(i, C[k]) - \frac{1}{2} \right) (S[k][j]) \quad (1)$$

d. Penyerang mengetahui bahwa hanya terdapat sebuah nilai Ki yang benar, dan nilai-nilai lainnya salah. Pada T[i][0..99999] dimana i=Ki, D(i,C[k]) untuk tiap k akan sama dengan nilai bit target dalam L pada operasi DES, sebelum hasil fungsi F pada DES di-XOR-kan. Ketika perangkat target melakukan operasi DES, nilai bit ini disimpan pada register, dimanipulasi dalam unit logika, dan seterusnya. -- sehingga dapat mendeteksi perbedaan *power consumption*. Dengan demikian, untuk bagian dari T[i=Ki] dimana bit sedang dimanipulasi, T[i] akan

menunjukkan perkiraan *power consumption*. Sebaliknya, untuk T[i!=Ki], nilai D(i,C[k]) tidak akan berkorespondensi dengan operasi yang benar-benar dieksekusi oleh perangkat target. Sehingga, T[i] juga tidak akan berkorelasi dengan proses yang benar-benar dijalankan dan T[i] akan bernilai 0.

e. Langkah di atas diulang pada S-Box lainnya untuk menemukan 48 bit kunci untuk putaran terakhir. Serangan kemudian dapat diulang untuk menemukan kunci putaran sebelumnya.

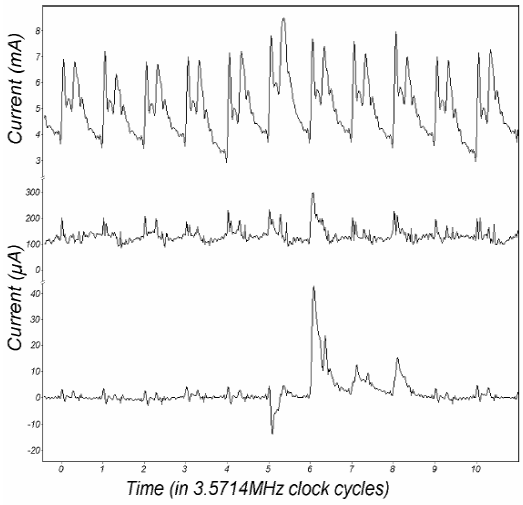
Gambar 7 menunjukkan empat pelacakan, pada sebuah operasi kriptografi *smart card*. Pelacakan paling atas merupakan referensi pelacakan *power* yang menunjukkan *power consumption* selama operasi DES. Untuk tiga pelacakan di bawahnya, pelacakan pertama dihasilkan dengan menggunakan kunci tebakan Ki yang benar, sedangkan dua pelacakan lainnya dihasilkan dengan menggunakan kunci tebakan Ki yang salah. Jumlah sampel yang digunakan adalah 1000.



Gambar 7. Pelacakan DPA, satu benar dan dua salah

Gambar 8 menunjukkan pengaruh rata-rata dari sebuah bit pada pengukuran *power consumption* secara detil. Pelacakan paling atas adalah referensi pelacakan *power consumption*. Pelacakan kedua menunjukkan deviasi standar dalam pengukuran *power consumption*. Pelacakan terakhir menunjukkan pelacakan *power consumption* dengan sampel 10000.

Ukuran karakteristik DPA adalah sekitar 40µA, jauh lebih rendah dibandingkan deviasi standar pada point yang berkoresponden. Kenaikan standar deviasi pada *clock cycle* ke-6 yang sesuai dengan karakteristik DPA mengindikasikan bahwa nilai operan memberikan pengaruh yang signifikan pada *power consumption* dan menunjukkan terdapatnya berbagai macam nilai operan yang sedang dimanipulasi. Instruksi level rendah seringkali melakukan manipulasi terhadap banyak bit, sehingga fungsi seleksi dapat secara simultan memilih nilai untuk bit-bit yang berbeda.



Gambar 8. Pengukuran DPA Kuantitatif

Beberapa sumber memperkenalkan *noise* pada pengukuran DPA, termasuk radiasi elektromagnetik dan *thermal noise*

[2]. Kesalahan kuantitatif yang disebabkan oleh perbedaan antara *device clocks* dan *sample clocks* dapat menimbulkan *error-error* tambahan. Selain itu, *temporal misalignment* yang salah dari pelacakan dapat menimbulkan banyak gangguan (*noise*) dalam perhitungan.

4.2 *Differential Power Analysis* dari Algoritma Lainnya

Algoritma kunci publik dapat dianalisa dengan menggunakan DPA, dengan menghubungkan nilai kandidat yang akan dihitung dengan pengukuran *power consumption* [2]. Untuk operasi eksponensial modular, dimungkinkan untuk menguji bit exponen yang diprediksi dengan memeriksa apakah nilai yang diprediksi tersebut sesuai dengan perhitungan yang sebenarnya. Algoritma *Chinese Remainder Theorem* RSA juga dapat dianalisa, sebagai contoh yaitu dengan memeriksa *power consumption* dari fungsi seleksi pada reduksi CRT atau pada proses rekombinasi.

DPA dapat digunakan untuk memecahkan implementasi dari hampir semua algoritma simetri dan asimetri [2]. Secara umum, kebocoran sinyal selama berlangsungnya operasi algoritma asimetri cenderung lebih sulit diperoleh daripada algoritma simetri, sebagai contoh adalah adanya kompleksitas komputasi yang relatif besar pada operasi perkalian, sehingga penerapan SPA dan DPA secara efektif sulit dilakukan dan pengukuran *power consumption* yang harus dilakukan juga menjadi lebih kompleks.

4.3 Pencegahan *Differential Power Analysis*

Teknik untuk pencegahan DPA dan serangan-serangan *power analysis* lainnya dibagi dalam 3 pendekatan. [2]

Pendekatan pertama, adalah dengan mengurangi ukuran sinyal (misalnya dengan menggunakan eksekusi *path code* yang konstan), memilih operasi yang dapat membocorkan informasi yang tidak terlalu banyak pada *power consumption*, menyeimbangkan Hamming Weights dan transisi status, dan dengan melindungi perangkat secara fisik. Sayangnya, pada umumnya pengurangan ukuran sinyal hingga menjadi 0 tidak dapat dilakukan, penyerang masih dapat menjalankan DPA dengan jumlah sampel yang cukup banyak. Perlindungan yang cukup baik pada perangkat dapat mencegah serangan, akan tetapi menyembabkab peningkatan ukuran dan *cost* dari perangkat.

Pendekatan kedua, adalah dengan melibatkan *noise* pada pengukuran *power consumption*. Seperti pada reduksi ukuran sinyal, penambahan *noise* dapat meningkatkan jumlah sampel yang dibutuhkan untuk sebuah serangan, bahkan dimungkinkan sampai menghasilkan jumlah sampel yang sangat besar. Pada pendekatan ini dapat ditambahkan pengacakan urutan dan waktu eksekusi.

Pendekatan ketiga, adalah dengan merancang sistem kriptografi dengan asumsi bahwa informasi dapat bocor. Prosedur *update* kunci *non linear* dapat digunakan untuk meyakinkan bahwa pelacakan *power* tidak dapat dihubungkan di antara operasi-operasi. Sebagai contoh, proses *hashing* 160-bit kunci dengan algoritma SHA dapat digunakan untuk menghancurkan informasi yang mungkin didapatkan oleh penyerang tentang kunci secara efektif. Penggunaan

proses modifikasi modulus dan exponen pada skema kunci publik juga dapat digunakan untuk mencegah penyerang untuk mengumpulkan informasi dari sejumlah operasi yang besar. Selain itu, penggunaan *counter* pada kunci dapat mencegah penyerang untuk mengumpulkan jumlah sampel yang besar. Perancang sistem kriptografi yang menggunakan metodologi perancangan yang memungkinkan adanya kebocoran, harus mendefinisikan rata-rata kebocoran serta fungsi-fungsi yang memungkinkan kebocoran. Dari pendefinisian tersebut, perancang melakukan teknik reduksi atau penyamaran kebocoran, sehingga sistem kriptografi aman dari serangan *power analysis*.

5. *High-Order Differential Power Analysis* (HO-DPA)

Teknik DPA yang dideskripsikan di atas menganalisa informasi yang berasal dari kejadian tunggal di antara sampel-sampel, sementara *high-order* DPA dapat digunakan untuk melakukan korelasi antara beberapa sub operasi kriptografi yang berbeda [3].

Pada *high-order* DPA, sinyal-sinyal didapat dari beberapa sumber yang berbeda, sinyal didapat dengan menggunakan teknik pengukuran yang berbeda-beda, dan sinyal dengan *temporal offset* yang berbeda dikombinasikan pada aplikasi dengan teknik DPA. Sebagai tambahan, fungsi diferensial yang lebih umum (D) dapat diterapkan. Fungsi pemrosesan sinyal yang lebih canggih juga dapat diterapkan. Oleh karena itu, fungsi pemrosesan dasar dari HO-DPA memiliki bentuk yang lebih umum dari standar yang digunakan pada fungsi DPA, sebagai contoh :

$$T[i][j] = F_0\left(\sum_{k=0}^{n} F_1(D(i, C[k], ..)F_2(S_0[i][j], S_1[i][j], S_2[i][j], ..)\right) \quad (2)$$

6. Serangan Lain yang berkaitan

Radiasi elektromagnetik dapat digunakan sebagai informasi dalam serangan *power analysis* dan merupakan tantangan yang cukup besar bagi perancang sistem kriptografi. Hal ini dikarenakan mudahnya pelacakan radiasi elektromagnetik. Bahkan radio AM sederhana dapat mendeteksi sinyal yang cukup kuat dari banyak perangkat kriptografi. Selain teknik pengukuran radiasi elektromagnetik, kini semakin banyak dikembangkan teknik-teknik pengukuran sinyal lainnya.

7. Kesimpulan

Teknik *Power Analysis* merupakan salah satu teknik serangan yang harus diperhitungkan. Serangan ini mudah untuk diimplementasikan, menghabiskan biaya yang rendah untuk perangkat, dan sulit untuk dideteksi. Serangan *Power Analysis* tidak hanya dapat diterapkan pada *smart card*, tetapi juga pada berbagai produk lainnya. Satu-satunya solusi yang paling baik untuk memecahkan masalah serangan ini adalah dengan merancang sistem kriptografi dengan asumsi bahwa informasi dapat bocor, sesuai dengan perangkat keras yang digunakan. Untuk itu, para perancang sistem kriptografi, baik perancang algoritma, perancang protokol, perancang perangkat lunak, maupun perancang perangkat keras, sebaiknya bekerja secara bersama-sama ketika mengembangkan sebuah sistem kriptografi yang aman.

Referensi

[1] R. Anderson, M.Kuhn, *Low Cost Attacks on Tamper Resistant Devices*, http://www.c1.cam.ac.uk/ftp/users/rja14/tamper2.ps.gz, diakses tanggal 1 Januari 2005 pukul 10:30.

[2] P. Kocher, J. Jaffe, and B. Jun, *Differential Power Analysis*, http://www.cryptography.com/resources/whitepapers/DPA.html, diakses tanggal 1 Januari 2005 pukul 10:00.

[3] P. Kocher, J. Jaffe, and B. Jun, *Introduction to Differential Power Analysis and Related Attacks*, http://www.cryptography.com/resources/whitepapers/DPATechInfo.html, diakses tanggal 1 Januari 2005 pukul 10:00.

[4] R. Munir, *Bahan Kuliah ke-12 : Data Encryption Standard (DES)*, Departemen Teknik Informatika, ITB, 2004.