ADD for info

21

POSSIBLE AREAS OF DSTO R&D SUPPORT FOR DSD CRYPTANALYTIC COMPUTING REQUIREMENTS

NOTES BY

BACKGROUND:

The maintenance of a successful cryptanalytic capability demands large scale computing support, and with the observed continual improvement in the communications security technology and procedures used , the computational demands continue to grow. Although the rate of growth fluctuates considerably, especially with Australia's

In DSD's case due to the small number of infrequent but large upgrades; A 3400 in 1965, an increase 14 years later in 1978, to a CYBER 175, an increase in 1986, 8 years later to a CRAY XMP.

The critical factor, which determines whether cryptanalysis remains affordable, is how relates to the rate of change in price performance of available high speed computers, and in general the rate of growth of requirement has been matched by a similar growth in large computer price/performance.

Since the early 1980's, it has become evident that the efforts to continually develop faster "conventional" single processor supercomputers has reached the point of diminishing returns (for example a CRAY XMP processor, released in 1982 and still current, represents at most X2 the power of a 1S processor,

21 A

released in 1979. An individual CRAY "Y" processor, to be released in 1987 will be at most 2X the speed of an "X" CPU). In order to continue to achieve the required increase in performance at acceptable prices a different strategy is now being observed. Engineering developments are enabling high performance processing units to be produced at much lower cost, and manufacturers such as CRAY are combining them in multi CPU computers offering price performance capabilities in line with the traditional rate of improvement of perhaps 20-30% per annum.

Another class of approach is the development of computers variously described as "array processors", "massively parallel architectures" or "transputer arrays", by firms including Denelcor, Inmos, BB & N and INTEL. The starting point for most of these approaches is the use of VLSI technology such as standard micro-processors, which individually have low performance but very high performance per dollar. The presumption is that if effective hardware architectures can be designed to interconnect large numbers of these units, and effective software techniques can be devised to organise real world problems into segments which can be executed in parallel, then spectacular increases in computer power and reductions in cost will be achieved. Unfortunately, this problem has proved to be rather intractable as the financial failure of many projects and some whole companies (e.g. DENELCOR) illustrate.

21 B

Nevertheless it is now recognised that parallel processing probably represents the only way in which the required increases in supercomputing power can continue to be provided, leading to the high level of commitment to parallel processing made by organisations such as INTEL, ETA, CRAY, Fuj tsu, Hitachi and the Supercomputer Research Centre in Maryland.

What are the implications for Cryptanalysis, and in particular DSD?

Even though parallel processors in some form have been available for over 25 years, the Sigint community has continued to use large general purpose computers for most crypt work, however

They can involve many times the workload of conventional programming and can be rendered useless requiring new cryptanalytic algorithms no longer suitable to the particular special purpose machine. It has been found that timing is critical. With "conventional" supercomputers changing in price performance by 20-30% per annum, is late in delivering or takes too long , its initial clear cut advantage is negated.

Possible areas of DSD Sponsored R & D

The scale of commitment overseas in both government and industry to supercomputing and parallel processing is such that it is probably not feasible to expect Australia could make a broad based contribution.

However there are two specific areas of potential value to DSD:

1. General research into techniques for effective parallel hardware and software architectures. Whilst it is unlikely to produce an Australian parallel supercomputer it would provide a body of expertise which could assist planning and selection of systems for DSD crypt support.
2. Research into the development of

Some Special Considerations

The availability of sufficient skilled cryptanalysts (and systems support staff) is definitely one of the most important limiting factors on DSD's crypt capability, leading to the selection of FOLKLORE and a CRAY for MARSIK and will undoubtedly dictate a requirement for an NSA/GCHQ compatible machine next time. This would limit our ability to select other more cost effective approaches which may be available in the future,

Cryptanalytic computing requires more flexibility than most supercomputer applications. Processes such as weather or seismic analysis involve mathematical descriptions of known physical processes (and fortunately the physics do not change with time). Crypt mathematical techniques often change very rapidly and any crypt computer must be flexible enough to cope with this.

Secure in the knowledge that it was a variant of a long line of a particular manufacturers machines all exhibiting similar structure, DSD could, for example

If DSTO resources were used for some Crypt computing R & D, the only effective means of ensuring close enough association with cryptanalytic activity and specific orientation to cryptanalytic supercomputing requirements would be their integration into CH, and the maintenance of close ties with relevant NSA and GCHQ areas.

21F

PARALLEL PROCESSORS ETC. - NOTES BY

I think it is very good policy to pursue ideas of massively parallel processors as applied to cryptanalysis,

If using DSTO personnel would not encroach on DSD's budget, it would be appropriate that they undertake the study. But I stress the importance of close involvement in studies by the other agencies. If we do have to pay, we should do the study ourselves. Cryptanalysis is not something that can be learnt overnight, and I was unimpressed by a recent go-it-alone effort by DRCS.

Alternatives to supercomputers seem to be:

(a) Massively parallel processors, (very new, much development needed for each).

(b) Flexible (hybrid) processors -
Fairly expensive.

(c)

(d) Array Processors attached to mainframes (cheap, rarely very powerful).

The trend seems to be more and more in favour of super computers (like CRAY) because of the increase in variety and turnover of cryptologics. There are two factors in modern cryptographic developments which affect us:

(a) complexity, for which we need CPU power,

(b) variety,

It is the latter which is increasingly becoming a problem, and has led to developments such as:

. DSD gets MARSIK for compatibility as much as CPU power.

. was designed especially to allow high level coding.

.

It seems that CRAY's currently represent the best compromise between CPU power and ease of programming. I think to go at this stage towards more specialist devices could have serious problems:

(a) We couldn't develop in a timely manner.

(b) We could be left with a white elephant if the targets change.

To sum up:

. We should energetically pursue studies of radical development of computing hardware.

. DSTO could be used subject to the above reservations.

. We will need to increase CPU power, but

. We need to be able to adapt quickly to proliferating cryptologics