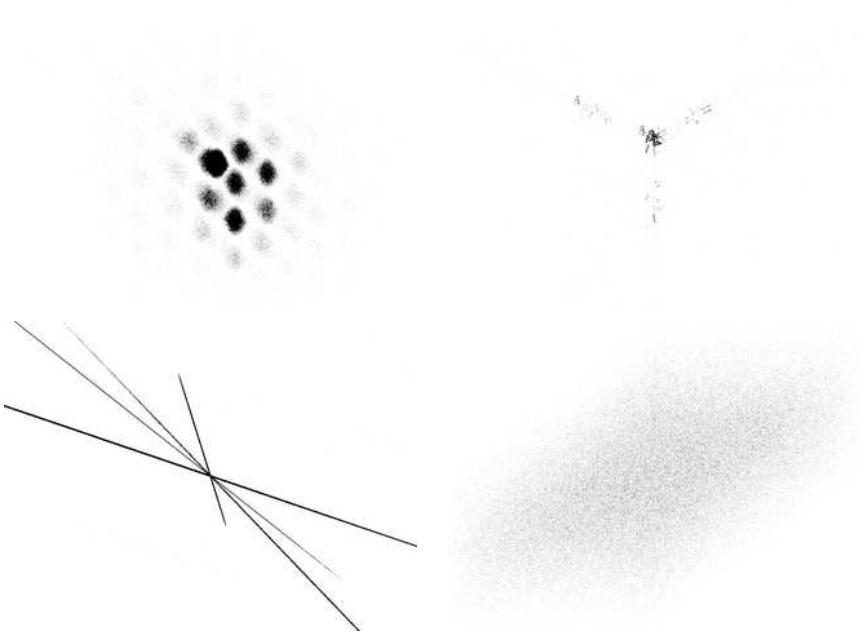

Figure 2.3: These are phase diagrams of the sequence number generators for four operating systems. The lower right shows a correct implementation of RFC 1948 sequence number generation (by FreeBSD 4.6.) The artistic patterns of the other three systems denote predictability that can be exploited by an attacker. The upper right shows IRIX 6.5.15m, the upper left Windows NT 4.0 SP3, and the lower left shows a few of the the many TCP/IP stacks for OpenVMS.

The TCP close sequence (see Figure 2.4) is asymmetric; each side must close its end of the connection independently.

2.1.4 SCTP

A new transport protocol, *Stream Control Transmission Protocol (SCTP)*, has recently been defined [Stewart *et al.*, 2000; Coene, 2002; Ong and Yoakum, 2002]. Like TCP, it provides reliable, sequenced delivery, but it has a number of other features.

The most notable new feature is the capability to multiplex several independent streams on a SCTP connection. Thus, a future FTP built on top of SCTP instead of TCP wouldn't need a PORT command to open a separate stream for the data channel. Other improvements include a four-way handshake at connection establishment time, to frustrate denial-of-service attacks, record-marking within each stream, optional unordered message delivery, and multi-homing of each connection. It's a promising protocol, though it isn't clear if it will catch on. Because it's new, not many firewalls support it yet. That is, not many firewalls provide the capability to filter SCTP traffic on a per-port basis, nor do they have any proxies for applications running on top of