Known Plaintext Cryptanalysis of Tree-Structured Block Ciphers

H.M. Heys[*] S.E. Tavares[†]

March 15, 1995

[*] Electrical Engineering, Memorial University of Newfoundland, St. John's, Newfoundland A1B 3X5, Canada

[†] Department of Electrical and Computer Engineering, Queen's University at Kingston, Kingston, Ontario K7L 3N6, Canada

Indexing Terms: Cryptography

Abstract: In this Letter we examine the cryptanalysis of a class of block ciphers referred to as substitution-permutation networks or SPNs. Specifically, we present a novel attack applicable to tree-structured SPNs. Because it uses a known plaintext approach, the attack is preferable to previously outlined chosen plaintext attacks. As well, it is shown that the attack is applicable to networks which are simple extensions of tree-structured SPNs.

Introduction: The concepts of "confusion" and "diffusion" introduced by Shannon [1] form the basis for a class of private key block ciphers referred to as substitution-permutation networks or SPNs. These networks, first suggested by Feistel [2], encrypt by passing an N-bit data block through R rounds of substitutions followed by permutations of the bit positions. The substitutions are accomplished by dividing the block into small n-bit sub-blocks and using N/n n-bit mappings referred to as S-boxes. The s-th S-box in round r is defined as a bijective mapping $S_{rs} : \mathbf{X}_{rs} \rightarrow \mathbf{Y}_{rs}$ where $\mathbf{X}_{rs} = [X_1^{(rs)} X_2^{(rs)} ... X_n^{(rs)}]$, $X_i^{(rs)} \in \{0,1\}$, and $\mathbf{Y}_{rs} = [Y_1^{(rs)} Y_2^{(rs)} ... Y_n^{(rs)}]$, $Y_i^{(rs)} \in \{0,1\}$. The cipher is keyed by applying τ_S bits of the key to select each S-box mapping from a set of mappings. A simple example of an SPN is illustrated in Figure 1.

Tree-structured SPNs or TS-SPNs are a fundamental class of SPNs that were initially introduced by Kam and Davida [3] and subsequently investigated by Ayoub [4]. These networks have the property that, assuming that each S-box output bit is a non-degenerate mapping of the S-box input bits, each ciphertext bit may be represented as a tree function of all plaintext bits. TS-SPNs are of interest because they are the only SPN structure known to provably satisfy the important cryptographic property of completeness. The network of Figure 1 with the last round removed so that there are 3 rounds of substitutions would be an example of a TS-SPN.

In [5], Heys and Tavares, extending the work of Anderson [6] on the cryptanalysis of bit-based tree ciphers, demonstrated the susceptibility of TS-SPNs to a chosen plaintext attack. Subsequently, Millan, Dawson, and O'Connor [7] outlined an improvement in the efficiency of the attack and O'Connor [8] showed that these networks are susceptible to differential cryptanalysis, also a chosen plaintext attack. The cryptanalysis presented in this Letter is preferable to these attacks because it is a known plaintext attack and is applicable to networks that are constructed by extending TS-SPNs to more rounds.

Cryptanalysis of TS-SPNs: Consider a TS-SPN. Let $\mathbf{Y}_{Rs}$ represent an n-bit sub-block of ciphertext bits associated with the output of a particular last round S-box S_{Rs} and let $\mathbf{X}_{Rs}$ represent the input to S-box S_{Rs}. From the definition of tree-structured networks, $Y_1^{(Rs)} = f_t(\mathbf{P})$ where f_t represents an R-level tree function of the N-bit plaintext input, $\mathbf{P}$, and $X_1^{(Rs)} = f_t'(\mathbf{P}')$ where $\mathbf{P}'$ is a vector of N/n plaintext bits which form the input to an $(R-1)$-level tree function, f_t'.

The cryptanalyst will attack the cipher by first determining a subset of the key bits called the target sub-key. For example, define the target sub-key to consist of key bits associated with the S-boxes which compose the tree function f_t' plus the key bit(s) from the last round S-box S_{Rs}. The attack proceeds by obtaining several known plaintext-ciphertext pairs and executing trial encryptions of the known plaintexts for all possible values of the target sub-key. The remaining key bits should be arbitrarily selected in each encryption. When the correct target sub-key is used, the value of bit $X_1^{(Rs)}$ will be correct in the trial encryption of all plaintexts. Each of the remaining $n-1$ input bits to S_{Rs} will be correct with a probability of $1/2$. As a result, the trial ciphertext sub-block $\mathbf{Y}_{Rs}$ will be the same as the actual ciphertext sub-block with a probability of $1/2^{n-1}$. If the wrong sub-key is used, we expect that $X_1^{(Rs)}$ will be correct only about $1/2$ the time. As a result the trial ciphertext sub-block will be the same as the actual ciphertext sub-block with a probability of $1/2^n$.

Once the target sub-key is determined, the remaining key bits may be revealed by targeting other tree functions or by exhaustive search. The complexity of the attack (defined as the number of encryption operations required) is given approximately by

$N_K \cdot N_P$ where N_P represents the number of known plaintexts needed to distinguish the correct sub-key from incorrect sub-keys and N_K represents the number of sub-key trials required.

To determine N_P consider a hypothesis test with hypothesis H_0 being that the trial target sub-key is incorrect and hypothesis H_1 being that the trial target sub-key is correct. The probability that the trial ciphertext sub-block is the same as the actual ciphertext sub-block is $p_0 = 1/2^n$ under H_0 and $p_1 = 1/2^{n-1}$ under H_1. Given a trial of N_P encryptions, the number of times that the trial and actual ciphertext sub-blocks are the same follows the binomial distribution but may be approximated by a Gaussian distribution with mean $\mu_i = N_P \cdot p_i$ and variance $\sigma_i^2 = N_P \cdot p_i \cdot (1 - p_i) \approx N_P \cdot p_i$ for hypothesis H_i, $i \in \{0,1\}$, where, for practical values of n, $(1/2^n)$, $(1/2^{n-1}) \ll 1$.

For convenience, we shall assume that the acceptable probability of error in selecting a hypothesis is the same for both H_0 and H_1. Hence, designing the hypothesis test so that the probability that a hypothesis is incorrectly chosen is given by $erfc(\alpha)$ leads to $\mu_0 + \alpha\sigma_0 = \mu_1 - \alpha\sigma_1$ where small values for α are sufficient to provide a suitably small probability of error in the hypothesis test. Consequently, N_P is given by

$$N_P \approx \alpha^2 (1 + \sqrt{2})^2 \cdot 2^n. \qquad (1)$$

Hence, assuming the S-box size to be fixed, the number of known plaintexts required in the attack is a constant, regardless of the block size.

Assuming that each S-box in the network is keyed independently of the other S-boxes, the number of sub-key trials required is given by $N_K \approx 2^{\tau_S \cdot \eta_S}$ where τ_S is the number of key bits used per S-box and η_S is the number of S-boxes that are targeted and is given by

$$\eta_S = (N/n) \sum_{r=1}^{R-1} (1/n)^r + 1 = (N/n) \left[\frac{1/n - 1/n^R}{1 - 1/n} \right] + 1. \qquad (2)$$

Hence, assuming S-boxes of fixed sized, the number of key trials required in the attack is $O(2^{cN})$ where c is a constant. Since the number of required known plaintexts is a constant, the complexity of the attack increases exponentially in the block size if the network size is increased without changing the size of the S-boxes.

Example 1: Consider a 64-bit TS-SPN which uses 4-bit S-boxes with each S-box requiring one unique key bit (i.e., $\tau_S = 1$). Such a TS-SPN consists of 3 rounds and requires a total of 48 key bits. Letting $\alpha = 4$, $N_P = 1.5 \times 2^{10}$ and $N_K = 2^6$. Hence, the complexity of the attack is 1.5×2^{16} encryption operations which is significantly less than the 2^{48} encryptions required in an exhaustive key search.

Cryptanalysis of Extended TS-SPNs: Consider extending a TS-SPN of R_T rounds to R rounds such that $R = R_T + (R_T - 2)$. Assume that the network uses the same permutation for each round selected from Ayoub's class of cryptographically equivalent permutations (CEP) [4]. It can be shown that this construction ensures that any R_T consecutive rounds are a TS-SPN. The network of Figure 1 is an example of an extended TS-SPN with $R_T = 3$.

Using a meet-in-the-middle approach, the attack outlined in the previous section can also be applied to such extended TS-SPNs. In this case, N_P and N_K may be determined as before with η_S now given by

$$\eta_S = 2(N/n)\left[\frac{1/n - 1/n^{R/2+1}}{1 - 1/n}\right]. \tag{3}$$

Example 2: Consider a 4-round SPN derived by extending the TS-SPN of Example 1 by one round. Using one key bit per S-box results in a total of 64 key bits. Letting $\alpha = 4$, $N_P = 1.5 \times 2^{10}$ and $N_K = 2^{10}$. Hence, the complexity of the attack is 1.5×2^{20} encryption operations which is significantly less than 2^{64} as in an exhaustive key search.

Conclusion: We have presented a novel cryptanalysis of tree-structured SPNs and noted that the attack can be extended to other related networks. The analysis clearly demonstrates the vulnerability of such ciphers to attacks requiring only a small number of known plaintext-ciphertext pairs.

References

[1] C.E. Shannon, "Communication theory of secrecy systems", *Bell System Technical Journal*, vol. 28, pp. 656-715, 1949.

[2] H. Feistel, "Cryptography and computer privacy", *Scientific American*, vol. 228, no. 5, pp. 15-23, 1973.

[3] J.B. Kam and G.I. Davida, "A structured design of substitution-permutation encryption networks", *IEEE Transactions on Computers*, vol. 28, no. 10, pp. 747-753, 1979.

[4] F. Ayoub, "The design of complete encryption networks using cryptographically equivalent permutations", *Computers and Security*, vol. 2, pp. 261-267, 1982.

[5] H.M. Heys and S.E. Tavares, "Cryptanalysis of tree-structured substitution-permutation networks", *IEE Electronics Letters*, vol. 29, no. 1, pp. 40-41, 1993.

[6] R.J. Anderson, "Tree functions and cipher systems", *Cryptologia*, vol. XV, no. 3, pp. 194-202, 1991.

[7] W. Millan, E.P. Dawson, and L.J. O'Connor, "Cryptanalysis of tree-structured ciphers", *IEE Electronics Letters*, vol. 30, no. 12, pp. 941-942, 1994.

[8] L.J. O'Connor, "A Differential Cryptanalysis of Tree-Structured Substitution-Permutation Networks", to appear in *IEEE Transactions on Computers.*

Figure 1. SPN with $N = 27$, $n = 3$, and $R = 4$