Table 1: Representative results of experiments

Sequence name	Frame numbers (prediction frame: frame to be coded)	PSNR [dB] between motion-compensated prediction and frame to be coded			
		Full search matching	Matching by separable convolution with E_1 only	Matching by separable convolution with E_1 and E_2	Matching by separable convolution with E_1, E_2 and E_3
Flower garden	40:42	22:87	17:57	22:19	22:75
	40:41	24:95	18:10	24:12	24.73
Salesman	30:35	31:58	28:01	31:25	31:52
	30:32	36:58	29:08	36:15	36:44
Jack-in-a-box	70:80	37:98	30:41	37:48	37:96
	70:72	41:51	30:73	40:23	41:40

Although using only the first eigenimage (E_1) is clearly inadequate, in every case as few as two eigenimages are sufficient for approximation within 1dB. When the prediction error is low (the most frequent situation), the difference between the full search result and the two-eigenimage SVD result is < 0.5dB. In these cases, the motion vector estimate is the same for the SVD approximation and for full search about 98% of the time. Even for high prediction errors, a maximum of three eigenimages is sufficient to come within 0.25dB of the full-search case. For two eigenimages, $P = 2$, and with $N = 16$, $K = 21$, the SVD method is about three times faster than full search. For three eigenimages, SVD is twice as fast as full search.

Conclusion: When SVD is used to convert a 2-D block-matching problem into a truncated sum of scalar products, its computational benefit depends on the block size and the number of eigenimages required to achieve an adequate approximation. For block-based motion estimation, only two or three eigenimages need be retained, providing at least a factor of 2 speed increase.

The method proposed here may be applied to other problems of 2-D block classification, and provides increasing benefit as the block size increases.

© IEE 1995
12 October 1995
Electronics Letters Online No: 19951481

J.A. Robinson (*Department of Systems Design Engineering, University of Waterloo, Ontario, N2L 3G1, Canada*)

References

1 GOLUB, G.H., and REINSCH, C.: 'Singular value decomposition and least squares solutions', *Numer. Math.*, 1970, **14**, pp. 403–420
2 ANDREWS, H.C., and PATTERSON, C.L.: 'Singular value decompositions and digital image processing', *IEEE Trans.*, 1976, **ASSP-24**, (1), pp. 26–53
3 ANDREWS, H.C., and PATTERSON, C.L.: 'Singular value decomposition (SVD) image coding', *IEEE Trans.*, 1976, **COM-24**, (4), pp. 425–432

Linear approximation of injective s-boxes

A. Youssef, S. Tavares, S. Mister and C. Adams

Indexing terms: Cryptography, Security of data

Nonlinearity is a crucial requirement for the substitution boxes in secure block ciphers. The authors derive an estimate for the expected nonlinearity of a randomly selected injective substitution box.

Introduction: Differential cryptanalysis [1] and linear cryptanalysis [2] are powerful cryptanalytic attacks on private-key block ciphers. The complexity of differential cryptanalysis depends on the size of the largest entry in the XOR table, the total number of zeros in the XOR table, and the number of nonzero entries in the first column in that table [1, 3]. The complexity of linear cryptanalysis depends on the size of the largest entry in the linear approximation table (LAT) [2].

One way to reduce the size of the largest entry in the XOR table is to use injective substitution boxes (s-boxes) such that the number of output bits of the s-box is sufficiently larger than the number of input bits. In this way, it is very likely that the entries in the XOR distribution table of a randomly chosen injective s-box will have only small values, making the block cipher resistant to differential cryptanalysis. Some proposed block ciphers, such as CAST [4] and Blowfish [5], take advantage of this property.

Conversely, Biham [6] proved that if $m \geq 2^n - n$ for an $n \times m$ s-box described by $f: Z_2^n \rightarrow Z_2^m$, then at least one linear combination of the output bits must be an affine combination of the input bits, and the block cipher can be trivially broken by linear cryptanalysis. In this Letter, we estimate the size of the largest entry in the LAT of a randomly selected injective s-box.

Definitions: The function $f: X \rightarrow Y$ is injective (or one-to-one) if for x, $\dot{x}$ in X the equality $f(x) = f(\dot{x})$ implies $x = \dot{x}$, i.e. distinct elements of X cannot have the same image in Y [7].

For a given s-box constructed from a mapping $f: Z_2^n \rightarrow Z_2^m$, the linear approximation table entry $LAT(\alpha, \beta)$ is defined as [2]:

$$LAT(\alpha, \beta) = \#\{X \in Z_2^n | \alpha \cdot X = \beta \cdot f(X)\} - 2^{n-1}$$

where $\alpha \in Z_2^n$, $\beta \in Z_2^m \{\underline{0}\}$, $\alpha \cdot X$ denotes the inner product of the vectors α and X evaluated over Z_2, and $\#\{\cdot\}$ denotes the cardinality of the enclosed set.

It is noticeable that $LAT(\alpha, \beta) = 2^{n-1} - d(\alpha \cdot X, \beta \cdot f(X))$, where

$$d(\alpha \cdot X, \beta \cdot f(X)) = \#\{X \in Z_2^n | \alpha \cdot X \oplus \beta \cdot f(X) = 1\}$$

It is also clear that the nonlinearity of the function f is given by

$$NL_f = 2^{n-1} - \max_{\alpha, \beta \neq \underline{0}} |LAT(\alpha, \beta)|$$

Throughout the rest of this Letter, the $\beta = \underline{0}$ case is not taken into consideration as it does not have any cryptographic significance.

The number of injective $n \times m$ s-boxes is given by

$$I(n, m) = \prod_{i=0}^{(2^n - 1)} (2^m - i)$$

Notation: Throughout this Letter, let $f: Z_2^n \rightarrow Z_2^m$ describe a random injective mapping, $wt(\alpha)$ denote the hamming weight of the binary vector α,

$$\binom{i}{j} = \begin{cases} \frac{i!}{j!(i-j)!} & i, j \text{ integers}, i \geq j \\ 0 & \text{otherwise} \end{cases}$$

$$wt(\beta \cdot f) = \#\{X \in Z_2^n | \beta \cdot f(X) = 1\}$$

$$P_w(k) \stackrel{def}{=} P\{wt(\beta \cdot f(X)) = k\}$$

$$P_d^{(\alpha, \beta)}(l) \stackrel{def}{=} P(d(\alpha \cdot X, \beta \cdot f(X)) = l) \quad \beta \neq \underline{0}$$

and

$$P_{d|w}(l, k) \stackrel{def}{=} P\{d(\alpha \cdot X, \beta \cdot f(X)) = l | wt(\beta \cdot f(X)) = k\}$$

Linear approximation table of injective mappings: We first determine the probability distribution of the weight of $\beta \cdot f(X)$:

Lemma 1:

$$P_w(k) = \frac{\binom{2^{m-1}}{k}\binom{2^{m-1}}{2^n - k}}{\binom{2^m}{2^n}}$$

Proof of lemma 1: For $\beta \neq \underline{0}$, $wt(\beta \cdot f)$ follows the hypergeometric distribution [8]. This follows by noting that the weight of $\beta \cdot f(X)$, $X \in Z2^n$ has the same distribution as that of the function constructed by randomly choosing 2^n bits from the function $\beta \cdot \pi$ where $\pi: Z_2^m \rightarrow Z_2^m$ is an arbitrary bijective mapping.

Given the weight of $\beta \cdot f$, the distribution of the distance between $\alpha \cdot X$ and $\beta \cdot f$ can be determined.

Lemma 2: For $\alpha \neq \underline{0}$, we have

$$P_{d|w}(l, k) = \frac{1}{\binom{2^n}{k}} \binom{2^{n-1}}{\frac{2^{n-1} + k - l}{2}} \binom{2^{n-1}}{\frac{k - 2^{n-1} + l}{2}}$$

Proof of lemma 2: Let $M_{ab} = \#\{X \in Z_2^n \mid \alpha \cdot X = a, \beta \cdot f(X) = b\}$, $a,b \in Z_2$. Then we have $d(\alpha \cdot X, \beta \cdot f(X)) = M_{10} + M_{01}$. Since $wt(\beta \cdot f(X)) = k$, this leads to $M_{01} + M_{11} = k$. We also have $M_{10} + M_{11} = 2^{n-1}$ as $\alpha \cdot X$ is a balanced function. Using these equations, we get

$$P_{d|w}(l,k) = P_{M_{11}|w}\left(\frac{2^{n-1}+k-l}{2}, k\right)$$

where

$$P_{M_{11}|w}(j,k) = \frac{\binom{2^{n-1}}{j}\binom{2^{n-1}}{k-j}}{\binom{2^n}{k}}$$

we obtain lemma 2.

Combining the two results above, the following theorem gives the probability distribution of the distance between $\alpha \cdot X$ and $\beta \cdot f(X)$ for fixed α and β. This can be used for finding the probability that a given entry in the LAT has a particular value, $2^{n-1} - l$.

Theorem 1:

$$P_d^{(\alpha,\beta)}(l) = \begin{cases} P_w(l) & \alpha = \underline{0} \\ \sum_{k=0}^{2^n} \frac{P_w(k)}{\binom{2^n}{k}} \binom{2^{n-1}}{\frac{2^{n-1}+k-l}{2}} \binom{2^{n-1}}{\frac{k-2^{n-1}+l}{2}} & \alpha \neq \underline{0} \end{cases}$$

Proof of theorem 1: The $\alpha = \underline{0}$ case follows because the distance between any function f and the zero function is the weight of f. For $\alpha \neq \underline{0}$, the result holds because

$$P_d^{(\alpha,\beta)}(l) = \sum_{k=0}^{2^n} P_{d|w}(l,k) * P_w(k)$$

For any integer value M_{LAT}, $0 < M_{LAT} \leq 2^{n-1}$, and by denoting the number of LATs with any entry having absolute value $\geq M_{LAT}$ by N^*_{LAT}, we have the following upper bound:

Corollary 1:

$$N^*_{LAT} \leq 2\left\{(2^m - 1)\sum_{l=M_{LAT}}^{2^{n-1}} P_d^{(\underline{0},\beta)}(2^{n-1} - l) + (2^m - 1)(2^n - 1)\sum_{l=M_{LAT}}^{2^{n-1}} P_d^{(\alpha,\beta)}(2^{n-1} - l)\right\}$$

Proof of corollary 1: We have

$$LAT(\alpha,\beta) = 2^{n-1} - d(\alpha \cdot X, \beta \cdot f(X))$$

From theorem 1, and noting that

$$\frac{N^*_{LAT}}{I(n,m)} = P\left\{\left(\max_{\alpha,\beta\neq\underline{0}} |LAT(\alpha,\beta)|\right) \geq M_{LAT}\right\} \leq \sum_{\alpha,\beta\neq\underline{0}} P\{|LAT(\alpha,\beta)| \geq M_{LAT}\}$$

we obtain the corollary above.

Take the minimum value of M_{LAT} for which $N^*_{LAT}/I(n,m) \leq 0.5$ as an estimate for the expected value of the maximum LAT entry. Table 1 shows the simulation results for $\overline{Max_{LAT}}$, the average value of the maximum entry in the LAT of a randomly selected $8 \times m$ injective s-box (m = 10, 12, ..., 32) together with our theoretical estimate, denoted by $\overline{Max^*_{LAT}}$. For all the results given in Table 1, the sample variance is upper bounded by two. The fast Walsh transform [9] and other speed-up techniques were used in the calculation of the maximum LAT entries throughout our simulation. It is worth noting that for m = 32, four of the s-boxes out of the 10 tested achieved a nonlinearity of 73, while the nonlinearity of the remaining six s-boxes was 72.

Table 1: Simulation results for $8 \times m$ injective s-boxes

m	10	12	14	16	18	20	22	24	26	28	30	32
Sample size	100	100	100	100	100	100	100	100	100	10	10	10
$\overline{Max^*_{LAT}}$	39	41	43	45	47	48	50	52	53	55	56	58
$\overline{Max_{LAT}}$	38	40	42	44	46	47	49	50	52	53	55	56

Conclusion: We have derived an upper bound for the fraction of injective s-boxes having the maximum absolute value entry in the linear approximation table greater than or equal to a specified value. Using this result. we derived an estimate for the expected value of this maximum LAT entry for a randomly selected injective s-box.

© IEE 1995
13 October 1995
Electronics Letters Online No: 19951466

A. Youssef and S. Tavares (*Department of Electrical and Computer Engineering, Queen's University, Kingston, Ontario, K7L 3N6, Canada*)

S. Mister and C. Adams (*Bell-Northern Research, PO Box 3511, Station C, Ottawa, Ontario, K1Y 4H7, Canada*)

References

1 BIHAM, E., and SHAMIR, A.: 'Differential cryptanalysis of DES-like cryptosystems'. Advances in Cryptology: Proc. Crypto '90, (Springer-Verlag, 1990), pp. 1–21
2 MATSUI, M.: 'Linear cryptanalysis method for DES cipher'. Advances in Cryptology: Proc. Eurocrypt '93, (Springer-Verlag, 1993), pp. 386–397
3 SEBERRY, J., ZHANG, X., and ZHENG, Y.: 'Systematic generation of cryptographically robust s-boxes'. 1st ACM Conf. on Computer and Communications Security, Fairfax, Virginia, November 1993, pp. 172–182
4 ADAMS, C.M., and TAVARES, S.E.: 'Designing s-boxes resistant to differential cryptanalysis'. Proc. 3rd Symp. State and Progress of Research in Cryptography, Rome, Italy, 1994, pp. 386–397
5 SCHNEIER, B.: 'Description of a new variable-length key, 64-bit block cipher (Blowfish)'. Proc. Fast Software Encryption Workshop, (Springer-Verlag, 1994), Paper LNCS 809, pp. 191–204
6 BIHAM, E.: 'On Matsui's linear cryptanalysis'. Advances in Cryptology: Proc. Eurocrypt '94, (Springer-Verlag, 1994), pp. 341–355
7 HUMPHREYS, J.F., and PREST, M.Y.: 'Numbers, groups and codes' (Cambridge University Press, Cambridge, 1989)
8 BLAKE, I.F.: 'An introduction to applied probability' (John Wiley and Sons, Inc., 1979)
9 AHMED, N., and RAO, K.R.: 'Orthogonal transforms for digital signal processing (Springer-Verlag, New York, 1975)

Probabilistic encryption key exchange

T. Moreau

Indexing terms: Cryptography, Information theory, Public key cryptography

A novel secret key exchange algorithm is proposed. It is based on the properties of the Blum Blum and Shum pseudo-random number generator (the 'x^2 mod N' generator), and on partial disclosure of the secret seed for this generator. The security and other features of the proposed cryptosystem are discussed.

Introduction: The need for secret key exchange algorithms has been addressed by early public key cryptosystems [1] as well as recent ones [2]. A secret key exchange is defined as a protocol interaction between unrelated parties that gives them a shared secret bit string from the uniform distribution [3]. As in [1], we limit the protocol to two messages, one initiating message and one response message, from the initiator party and the responder party, respectively. Unrelatedness is defined as the absence of both an alternate secret key distribution channel and on-line access to a third party. It is also necessary to get assurances from both parties get assurance that the bit string is unique to a particular key exchange session. This is achieved if the bit string is jointly determined from random numbers.

We propose a novel secret key exchange algorithm in which security is partially based on the Blum-Goldwasser probabilistic encryption cryptosystem [4] and the mathematical properties of the BBS pseudo-random number generator [5–7]. For a tutorial presentation, see [8]. Our proposal exhibits interesting properties for actual use in cryptographic applications: (i) a low processing