Remarks on the Security of the AES and the XSL Technique

S. Murphy and M.J.B. Robshaw
Information Security Group,
Royal Holloway, University of London,
Egham, Surrey, TW20 0EX, U.K.
s.murphy@rhul.ac.uk and m.robshaw@rhul.ac.uk

October 23, 2002

Abstract

This note gives some background information relevant to recent claims of key recovery attacks on the AES.

Introduction

There has been much recent speculation [3, 4, 8] about the potential for key recovery attacks on the AES [7]. This speculation arises from two recent developments.

- A proposal for a new method of block cipher analysis known as the XSL technique [3, 4].
- An analysis of the AES in terms of a new cipher (the BES) in order to clarify the mathematical structure of the AES [6].

The analysis of the AES in terms of the BES was given in our Crypto 2002 paper [6] and its applicability is independent of the XSL technique [3, 4]. Nevertheless, we briefly referred to the XSL technique in the following way.

> The AES **F**-system derived from the BES is far simpler [than the basic AES $GF(2)$-system], which would suggest that the XSL algorithm would solve this **F**-system far faster (2^{100} AES encryptions) than the $GF(2)$-system. However, the estimate given for the number of linearly independent equations generated by the XSL technique [3] appears to be inaccurate [1].

The first sentence is, in effect, the source of the AES speculation. However, this first sentence should not be used without reference to the second. The purpose of this note is to give further details about both these comments. In particular we stress that the point at issue is the conjectured effectiveness of the XSL technique. The arguments made for the XSL technique [3, 4] are heuristic and are certainly not universally accepted [2]. Thus any statements about the work effort of an AES key recovery using the XSL technique [3, 4, 5, 8] have not been substantiated.

Algebraic Structure of the AES and XSL

The AES has a very simple algebraic structure. By embedding the AES in a new 128-byte cipher, the BES, we showed that an AES round can be defined by two algebraically simple operations over $\mathbf{F} = GF\left(2^8\right)$ [6]. This provides a simplified framework for the analysis of the AES. As a byproduct, we showed how an AES encryption can be described by a very small and extremely sparse multivariate quadratic (MQ) system over $\mathbf{F}$.

In two papers, Courtois and Pieprzyk [3, 4] described an AES encryption using a highly complicated MQ system over $GF(2)$. Courtois and Pieprzyk proposed the XSL technique to solve such a $GF(2)$-system. The observation that the XSL technique, if correct, would be far more suited to the sparse AES MQ $\mathbf{F}$-system, instead of the complicated AES MQ $GF(2)$-system, was given in our Crypto paper [6].

We based our discussion of the XSL technique on the estimates given in the "second attack" of the original XSL paper [3] and we refer to this paper for a full description of the XSL technique. However, we give a simple overview of the XSL technique.

- Generate equations of higher degree from the original set of equations.
- Regard the system of equations as linear combinations of formal terms.
- Solve this linear system (if possible).

It is clear that a highly accurate estimate of the number of generated equations that are linearly independent is required in order to ascertain whether the resulting linear system is soluble.

We consider the application of the XSL technique to the simple $\mathbf{F}$-description of the AES. We use the notation of [6] and consider the version of the AES with 128-bit keys. We ignore the slight complications introduced by the possibility of a "0-inversion". In [6], we gave the following very simple multivariate quadratic equations for each round $i = 0, \ldots, 9$, and for $j = 0, \ldots, 15$ and $m = 0, \ldots, 7$ (where $m + 1$ is interpreted modulo 8):

$$0 = x_{i,(j,m)} w_{i,(j,m)} + 1; 0 = x_{i,(j,m)}^2 + x_{i,(j,m+1)}; \text{ and } 0 = w_{i,(j,m)}^2 + w_{i,(j,m+1)}.$$

Thus, for a given i and j, we obtain $8 \times 3 = 24$ such multivariate quadratic equations. This set of 24 equations covers an ensemble of eight **F**-inversions (since i and j are fixed) and involves 41 **F**-terms. It follows that the natural definition of an "XSL S-Box" over **F** is a function $S^*_{i,j} : \mathbf{F}^8 \to \mathbf{F}^8$ defined by

$$\begin{aligned} S^*_{i,j}\left((x_{i,(j,0)}, \ldots, x_{i,(j,7)})\right) &= \left(x_{i,(j,0)}, \ldots, x_{i,(j,7)}\right)^{(-1)} = \left(x^{(-1)}_{i,(j,0)}, \ldots, x^{(-1)}_{i,(j,7)}\right) \\ &= \left(w_{i,(j,0)}, \ldots, w_{i,(j,7)}\right). \end{aligned}$$

This S-Box over **F** provides a closed collection of quadratic relations and is an extension of the original concept of an XSL S-Box. In the original AES XSL S-Box over $GF(2)$, all $GF(2)$ relations are related to the S-Box transformation (**F**-inversion) [3, 4]. By contrast, in this new AES XSL S-Box over **F**, only 8 of the 24 equations are directly related to the S-Box transformation (**F**-inversions). Thus quadratic terms in the original AES XSL S-Box over $GF(2)$ are always the product of an input and an output variable, whereas the AES XSL S-Box over **F** involves quadratic terms solely in input variables and solely in output variables.

We have defined a very simple XSL S-Box over **F** which, in the notation of Courtois and Pieprzyk [3], has the following parameters. An XSL S-Box over **F** has size $s = 8$ with $B = 16$ S-Boxes in a round. There are $r = 24$ quadratic relations within an S-Box and $t = 41$ terms involved in these relations. These terms are given by

$$x_{i,(j,m)},\ w_{i,(j,m)},\ x^2_{i,(j,m)},\ w^2_{i,(l,m+1)},\ x_{i,(j,m)}w_{i,(,m+1)} \text{ and } 1.$$

Courtois and Pieprzyk define the complexity of an S-Box from an XSL perspective in terms of parameter Γ. They give two different definitions in the two papers [3, 4] and give a value of $2^{22.9}$ in the later paper [4]. However, the XSL S-Box over **F** is a far simpler entity and the equivalent complexity parameter is given by

$$\Gamma = \left(\frac{t-r}{s}\right)^{\lceil \frac{t-r}{s} \rceil} = \left(\frac{41-24}{8}\right)^{\lceil \frac{41-24}{8} \rceil} \approx 9.6.$$

In the proposed XSL technique, higher degree equations are manufactured by multiplying an equation from one particular S-box, the *active* S-Box, by terms from other *passive* S-boxes. The number of passive S-boxes that are used in the attack is denoted by $P - 1$, so the highest degree of equations and terms used by the XSL technique is $2P$. The XSL technique considers three classes of higher degree equations. The number of linearly independent equations in each of these three classes is estimated [3] by:

$$\begin{aligned} R &\approx \binom{S}{P}(t^P - (t-r)^P), \\ R' &\approx \binom{S}{P-1} sB(N_r+1)(t-r)^{P-1}, \text{ and} \end{aligned}$$

$$R'' \approx \binom{S}{P-1}(S_k - L_k)(t-r)^{P-1}.$$

The total number of terms is estimated [3] by $T \approx \binom{S}{P} t^P$ and the number of linearly independent equations (estimated by $R + R' + R''$) cannot exceed the number of terms (estimated by T). Courtois and Pieprzyk suggest possible methods of overcoming such a deficit, such as the "T' method", where the number of terms T is "reduced" by T' [3, 4]. However, Coppersmith has cast doubt on the general applicability of the T' method [2] anyway.

Courtois and Pieprzyk discussed the solution of the AES MQ $GF(2)$-system using the XSL technique [3]. Our comment [6] about the work effort of an AES key recovery was based on the application of these XSL estimates to the AES MQ **F**-system. When we apply these estimates we obtain the following values.

$P = 2$	R	$27,979,200$
	R'	$4,811,136$
	R''	$874,752$
	Equations $(R + R' + R'')$	$33,665,088$
	Terms T	$33,788,100$
$P = 3$	R	85.19×10^9
	R'	8.18×10^9
	R''	2.97×10^9
	Equations $(R + R' + R'')$	95.18×10^9
	Terms T	91.94×10^9

For $P = 3$, generating terms and equations of degree 6, routine use of the XSL estimates indicates that there would be more linearly independent equations than terms. This might suggest that the XSL technique generates a soluble linear **F**-system of size about $91.94 \times 10^9 \approx 2^{36}$. All of the recent discussions about the work effort of an AES key recovery [4, 5, 6, 8] are based on the complexity of solving such a linear system.

The work effort we gave in [6] was based on naive Gaussian elimination, the basic technique for solving such a linear system, and this has complexity $O(n^3)$ for an $(n \times n)$ matrix. If we use this technique on an **F**-matrix with 2^{36} rows and columns, then we would require about $(2^{36})^3 = 2^{108}$ **F**-operations. An AES encryption requires 160 **F**-inversions, so a (very) rough comparison suggests that an AES encryption and key setup might require about 2^8 **F**-operations. Thus *if XSL is a valid technique*, an AES key recovery might be possible with a work effort of about 2^{100} AES encryptions. This might be compared to the 2^{230} steps that were estimated by [3] when working over $GF(2)$.

We note that the linear system generated by applying the XSL technique to the AES MQ **F**-system would be extremely sparse. Thus matrix techniques with lower complexity than naive Gaussian elimination might be suitable. In general, if this resulting linear system can be solved with a technique with complexity

$O(n^\omega)$ (for an $n \times n$ matrix), then the XSL estimates would suggest an AES key can be recovered with a work effort of $2^{36\omega-8}$ AES encryptions ($2^{36\omega}$ **F**-operations). The work effort for an AES key recovery of 2^{87} **F**-operations (2^{79} AES encryptions) suggested by Courtois and Pieprzyk [4, 5] is based on a lower and probably unrealistic complexity exponent $\omega = 2.376$ for the complexity of solving this linear system of size 2^{36}.

Accuracy of the XSL Estimates

Clearly the important issue is the validity of the XSL technique and not the choice of complexity exponent. The justification of the XSL technique is heuristic [3, 4] and an analysis of the XSL technique requires a *particularly accurate* count of the terms and equations generated.

It appears that analysis of the XSL technique overestimates the number of linearly independent equations that are generated, as Coppersmith has stated [2]. As can be seen from our figures, the XSL estimates for the AES MQ **F** system with $P = 3$ suggest that there are significantly more linearly independent equations than terms. Yet this is clearly impossible since there cannot be more linearly independent equations than terms. Thus a routine application of the XSL technique to the AES MQ **F**-system provides estimates for the number of linearly independent equations that must have a significant error. Certainly they are not sufficiently accurate to ensure that the XSL technique can work as claimed [3, 4].

Conclusions

In this note we have provided some background to different claims for AES key recovery attacks based on the XSL technique. However we believe that the XSL estimates do not have the accuracy needed to substantiate claims of the existence of an AES key recovery attack based on the XSL technique [2, 6].

References

[1] D. Coppersmith. Personal Communication. 30 April 2002.

[2] D. Coppersmith. Impact of Courtois and Piepryzk Results. NIST AES Discussion Forum, available at `http://www.nist.gov/aes`. 19 September 2002.

[3] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. IACR eprint server, `http://www.iacr.org`. March 2002.

[4] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. To appear at AsiaCrypt 2002.

[5] N. Courtois. The XSL attack on AES. `http://www.minrank.org/aes/`. September 2002.

[6] S. Murphy and M.J.B. Robshaw. Essential Algebraic Structure within the AES. In, M. Yung, editor, *Advances in Cryptology — CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 1–16, Springer-Verlag. August 2002.

[7] National Institute of Standards and Technology. Advanced Encryption Standard. FIPS 197. 26 November 2001.

[8] B. Schneier. Crypto-Gram Newsletter, Counterpane Internet Security, available at `http://www.counterpane.com/crypto-gram.htm`. 15 September 2002.