A Comment on "A New Public–Key Cipher System Based Upon the Diophantine Equations"

S.R. Blackburn*, S. Murphy† and K.G. Paterson‡

Information Security Group, Royal Holloway,

University of London, Surrey TW20 0EX, U.K.

March 17, 1995

Abstract — The public key system proposed by Lin, Chang and Lee [1] is insecure, even if used as a private key system.

Index Terms — Public key cryptography, knapsack cryptosystems.

---

*This author's research supported by EPSRC Research Grant No. GR/H23719.

†This author acknowledges the support of the Nuffield Foundation

‡This author's research supported by a Lloyd's of London Tercentenary Foundation Research Fellowship.

In [1], the authors present a public key system based on an integer knapsack problem. Following the notation of [1], let $\mathcal{D} = \{0, \ldots w\}$. The message block $(m_1, \ldots, m_n)$, where $m_i \in \mathcal{D}$, is encrypted to $C = \sum_{i=1}^{n} m_i s_i$, where $(s_1, \ldots, s_n)$ forms the public key. The method for choosing s_i to allow a form of trapdoor decryption is given in [1]. We show below that this method produces an insecure cryptosystem.

Lemma 1 *There is a unique $m'_j \in \mathcal{D}$ such that $C = m'_j s_j \bmod q_j$.*

Proof: Clearly a solution exists since, noting $q_j \mid s_i$ for $i \neq j$,

$$C = \sum_{i=1}^{n} m_i s_i = m_j s_j \bmod q_j.$$

For any $x \in \mathcal{D}$,

$$xR_jN_j \leq x\left(\frac{q_j}{k_jR_j} + 1\right) R_j < x(w+1)R_j \leq wk_jR_j < q_j.$$

If $m'_j s_j = C \bmod q_j$, then $m'_j R_j N_j = m_j R_j N_j \bmod q_j$. Since both sides of this equation are less than q_j, we have $m'_j = m_j$. □

By using this lemma, we show that is possible to decrypt using only the public key $(s_1, \ldots s_n)$. Let $G_j = \gcd\{s_i\}_{i \neq j}$, so q_j divides G_j. Consider the congruence $C = xs_j \bmod G_j$. Clearly $x = m_j$ is a solution. We show that this is, in fact, the only solution in $\mathcal{D}$. If $C = m'_j s_j \bmod G_j$ for $m'_j \in \mathcal{D}$, then $m'_j s_j = m_j s_j \bmod q_j$. By the lemma, m'_j and m_j differ by a multiple of q_j.

But $q_j > w$, so $m'_j = m_j$. To find m_j, it therefore suffices to find the unique solution $x \in \mathcal{D}$ to the congruence $C = xs_j \bmod G_j$. This is trivally solved using the extended Euclidean algorithm.

This cryptanalysis is related to that presented in Section IV C of [1]. The exhaustive search in Steps 2-4 of their attack merely finds solutions to linear congruences, which can be solved directly.

We finally note that this system is insecure even as a private key cipher, since $(s_1, \ldots, s_n)$ can be easily deduced from a small number of known plaintext–ciphertext pairs.

References

[1] C.H. Lin, C.C. Chang and R.C.T. Lee, "A New Public–Key Cipher System Based Upon the Diophantine Equations", *IEEE Trans. Comp.* Vol. 44, No. 1 January 1995, pp. 13–19.