IN MEMORIAM

TORE HERLESTAM (1929-1986)

The cryptologic community was deeply saddened by the sudden death on 11 November 1986 from a cerebral stroke of one of its most prominent members, Tore Herlestam.

Tore, who received his doctorate in mathematics from the University of Göteborg, Sweden, in 1959 had joined the newly-formed Department of Information Theory at the University of Lund, Sweden, as a Research Professor just three months prior to his death. For more than twenty years previously, he served in the Department of Signal Security of the General Staff of Defense in Sweden. It is a measure of his stature in the field of cryptology that he was permitted to perform his defense work at home in his beloved Skåne (southern Sweden) rather than at the Department's Stockholm facility. Tore's untimely death not only shortened cruelly the academic career that he had anticipated with much pleasure, but it also prevented him entirely from taking up his planned duties on the Editorial Board of the IACR's forthcoming *Journal of Cryptology*.

Much of Tore's research was in the classified sector of cryptology where his influence extended well beyond the Swedish borders. He was a frequent and welcome guest at many cryptologic workshops sponsored by other west European signal security agencies. Tore's published research in cryptology spans a broad spectrum, but his greatest contributions were probably those he made to the theory of stream ciphers. I remember especially Tore's work to establish under what conditions the linear complexity of the output sequence from a boolean combining function, $f(x_1, x_2, \dots, x_n)$, fed by binary linear feedback shift registers with lengths $L_1, L_2, \dots, L_n$, would be given by $f(L_1, L_2, \dots, L_n)$, the formal evaluation of the algebraic normal form of the boolean function with the boolean variable x_i replaced by the integer L_i and with the boolean EXCLUSIVE-OR and AND operations replaced by integer addition and multiplication. Tore's lucid presentation on this problem at the 1982 International Symposium on Information Theory captured the imagination of my then doctoral student, Rainer Rueppel, and led eventually to the paper by Rueppel and Othmar Staffelbach in the January 1987 *IEEE Transactions on Information Theory*, which gives the most general formulation yet of "Herlestam's theorem".

Like many other members of the classified research community, Tore was deeply mistrustful of public-key cryptography. Unlike most, he gave some solid reasons for his mistrust. Together with his friend and colleague, Rolf Johannesson, Tore presented a paper ("On Computing Logarithms over $GF(2^n)$ ") at the 1981 International Symposium on Information Theory suggesting that taking logarithms in an extension field of $GF(2)$ was much easier than in a prime field $GF(p)$ of about the same size—many researchers (including this writer) were unconvinced. Ian Blake and his colleagues at the University of Waterloo, Canada, however, took the suggestion in earnest and made important contributions to the problem. The *coup de grace* was applied by Don Coppersmith in his July 1984 *IEEE Transactions on Information Theory* paper that fully vindicated Tore's intuition and prevented further work on what would have been an insecure public-key technique.

Tore's 1978 paper, "Critical Remarks on Some Public-Key Cryptosystems", which appeared in the Scandinavian journal *BIT*, suggested on the basis of small examples some weaknesses in the Merkle-Hellman trapdoor knapsack public-key cryptosystem and in the Rivest-Shamir-Adleman (RSA) public-

key cryptosystem. We all recall Adi Shamir's later brilliant demonstration of the insecurity of the trapdoor knapsack scheme. Ron Rivest, however, was able to show that the purported "weaknesses" in RSA were of no danger in a full-scale RSA cryptosystem. But Tore's intuition of a weakness in RSA continues to haunt some cryptographers and will probably continue to do so until either the RSA cryptosystem is broken or it is proved in entirety to be secure.

I remember Tore's technical writing with especial pleasure because of its clarity. His paper, "On Functions of Shift Register Sequences", which appears in *Advances in Cryptology EUROCRYPT 85*, is a beautiful exposition on the fundamental theory of stream ciphers. I know I will miss the useful mathematical advice that Tore was always generous in supplying from his encyclopedic store. And like many other cryptologists who were personal friends of Tore, I miss and will miss his quick and hearty laughter.

James L. Massey
President, IACR