

?????, ?????, ?????? ??????????????, ?????????????? ?????????? (???????, 17. I 1956). ??
????????????????? ?????????? ? ?????????? ?????????? 1979, ?????????????? 1981. ? ?????????????? 1985. ??
1979. ?? 1993. ?????? ? ?????????? ?? ?????????? ?????????????? ? ?????????????? ? ??????????, ??? ?? ??????
????? ?????????? ?????????? (1986) ? ?????? ?????????? ?????????? (1990). ? ?????? ?????????? ?? ??????????
????????? ?????????? ?????????? 1986. ?? ?????????? ?????????? ?????? ? ?????? ??? ? 1988. ?? ??? ? ??????????
?? 1993. ?? 1997. ?????? ?? ?????????? ?????????????? ?? ?????????? ?????????????????? ?? ??????????????
(?????????????). ?????? 1997. ?????????? ?? ?? ?????????? ?????????????? ?? ?????????? ?? ?????????? ??????????????
??? ? ??????????, ??? ?? ?????? ?? 2001. ?? 2001. ?? 2003. ??? ?? ?????? ?????????????? ? Rome CryptoDesign
Center, Gemplus (????????), ? ?? 2003. ?????? ?? ? Telecom Italia Lab (????????). ?????? ?? ?????????? ??
????????????????, ?????????? ??????????, ?????????? ??????????????, ?????????? ?????????????, ?????????? ? ??????????
?????????. ?????? ?????????????????? ?????????????????? ?????????? ?????????? ?????????????????????? ? ?????
????????????? ?????????, ?????????? ?????????? ??????????????????, ?????????????? ?????????, ?????????? ??????????
????????????????, ?????????????? ?????????????????, ?????????? ?????????????????, ?????????????????? ?????????, ?????????? ?????????,
???????????????? ? ?????????????????? ?????????????? ??????????????. ?????????? ?? ?????? ?????????? ?????????????? ?? ??????????????????
????????????????????? ????????? (?? 1989). ?????????? ?? ?????????? ?????? ?????????? ?? ?????????????? ?? (1979) ? ??
????????????? ????????????????? (1986), ?? ?????????? „?????. ?????????? ??????????“ ?? ?????????????? ?????????-?????????????????
??? (1988).

?????: „Iterative optimum symbol-by-symbol decoding and fast correlation attacks“, *IEEE Transaction on Information Theory*, 2001, 47; ? R. Menicocci, „Statistical distinguishers for irregularly decimated linear recurring sequences“, *IEEE Transaction on Information Theory*, 2006, 52; „Exact Probabilistic Analysis of Memoryless Combiners“, *IEEE Transaction on Information Theory*, 2007, 53.

?????????????: ?. ??????, ?. ?????? (??.), ?????? 50 ?????? (1948–1998), ???, ?? 2003.

?????? ???????

*?????? ?? ?????????? ? 1. ?????? III ?????? ?????????? ?????????????????? (2018)

????????? #2
????????? 19 januar 2024 09:06:45 o? Admin
????????? 3 april 2025 07:55:22 ?? ?????????????? ??????????