Fluctuation and Noise Letters
Vol. 0, No. 0 (2001) 000–000

Remark on a "Non-Breakable Data Encryption" Scheme by Kish and Sethuraman

Andreas Klappenecker
Department of Computer Science, Texas A&M University
College Station, TX 77843-3112, USA
klappi@cs.tamu.edu

Received (received date)
Revised (revised date)
Accepted (accepted date)

We break a cryptosystem by Kish and Sethuraman and show that the authentication problem of their protocol can be fixed. We prove that finding an instance of this cryptosystem, which meets the design criteria, would show that P ≠ NP.

Keywords: Classical information; encryption; public key cryptography; Kish/Sethuraman cipher

1. Introduction

In [2], Kish and Sethuraman introduced a data encryption scheme that allows two parties to exchange information over a public channel without prior key exchange. The scheme assumes that Alice and Bob, respectively, have a set of invertible operators $\mathcal{A} = \{A(x)\,|\,x \in I_A\}$ and $\mathcal{B} = \{B(y)\,|\,y \in I_B\}$ such that $A(x)B(y) = B(y)A(x)$ holds for all x in I_A and all y in I_B. We assume that there exist efficient polynomial time algorithms to compute $A(x)$, $B(y)$ and their inverses; otherwise, the system is not of practical interest.

The scheme proposed in [2] works as follows: If Alice wants to communicate a message m to Bob, then she selects uniformly at random some operator $A(x)$ from $\mathcal{A}$ and sends $A(x)m$ over the public channel to Bob. Then Bob selects uniformly at random an operator $B(y)$ from $\mathcal{B}$ and replies by communicating $B(y)A(x)m$ to Alice. She communicates $A(x)^{-1}B(y)A(x)m = B(y)m$ back to Bob. It is possible for Bob to recover the message m by applying $B(y)^{-1}$ to the received cryptogram $B(y)m$.

The authors claim that the system is unconditionally secure for a proper choice of operator sets $\mathcal{A}$ and $\mathcal{B}$, but the current version of the protocol is easily broken with a man-in-the-middle attack. Indeed, suppose that Eve intercepts the messages from Alice and pretends to be Bob; this allows her to learn the message. Eve can relay the message to Bob by pretending to be Alice, so that the interception will go unnoticed.

It is possible to fix the problem of the protocol by augmenting it with standard authentication methods, see [3, Chapter 11]. For example, if Alice and Bob share a public key infrastructure, then they can use digital signatures to sign the messages. The problem in the original protocol illustrates that the system is certainly not more secure than methods of quantum cryptography, as was suggested in [2].

2. Complexity

Kish and Sethuraman impose a natural constraint on the operators $A(x)$ and $B(y)$:

($\star$) It should be infeasible to determine the message $B(y)^{-1}B(y)m = m$ by observing the publicly transmitted messages $A(x)m$, $B(y)A(x)m$, and $B(y)m$.

In the usual terminology of cryptography, this means that $A(x)$ and $B(y)$ are supposed to be *trapdoor one-way permutations*.

The last remark puts the open question from [2] regarding the existence of suitable systems $\mathcal{A}$ and $\mathcal{B}$ into perspective. Systems $\mathcal{A}$ and $\mathcal{B}$ of polynomial time computable operators satisfying ($\star$) exist if and only if the class P of all languages that are acceptable by a polynomial time deterministic Turing machine can be separated from UP $\cap$ coUP, where UP is the class of all languages that are accepted by a nondeterministic Turing machine that runs in polynomial time and has on any input at most one accepting path [1]. In particular, if one can show that systems $\mathcal{A}$ and $\mathcal{B}$ of efficiently computable operators exist which satisfy ($\star$), then P $\neq$ NP.

Therefore, we might have to settle for systems that might not satisfy ($\star$). A natural example is given by the RSA public key cryptosystem [4], which can be used in the Kish and Sethuraman encryption scheme as follows: Choose two distinct large primes p and q. Let $n = pq$ and let $I_A = I_B = \{k \,|\, 1 < k < n, \gcd(k, \phi(n)) = 1\}$. Then $A(x)m = m^x \bmod n$ and $B(y)m = m^y \bmod n$. Clearly, the two operators commute and their inverses are given by operators of the same type. Other public key cryptosystems can be used in a similar way. However, one usually avoids such usage of a public key cryptosystem because this is too inefficient.

Acknowledgements

The research by A.K. was supported by NSF CAREER award CCF 0347310, NSF grant CCR 0218582, a TEES Select Young Faculty award, and a Texas A&M TITF initiative.

References

[1] C.M. Homan and M. Thakur. One-way permutations and self-witnessing languages. *J. Comput. Syst. Sci.*, 67(3):608–622, 2003.

[2] L.B. Kish and S. Sethuraman. Non-breakable data encryption with classical information. *Fluctuation and Noise Letters*, 4(2):C1–C5, 2004.

[3] W. Mao. *Modern Cryptography – Theory and Practice*. Prentice Hall, 2004.

[4] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.