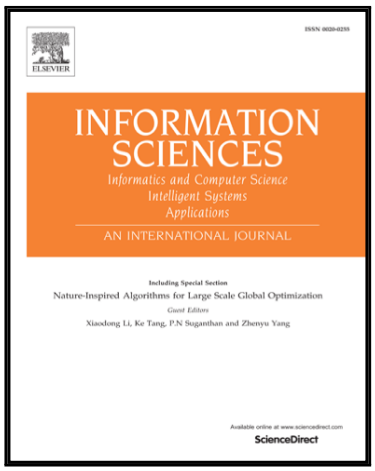
Accepted Manuscript



Attainable Unconditional Security for Shared-Key Cryptosystems

Fabrizio Biondi, Thomas Given-Wilson, Axel Legay

PII: S0020-0255(16)30441-8
DOI: 10.1016/j.ins.2016.06.019
Reference: INS 12293

To appear in: *Information Sciences*

Received date: 26 October 2015
Revised date: 22 April 2016
Accepted date: 15 June 2016

Please cite this article as: Fabrizio Biondi, Thomas Given-Wilson, Axel Legay, Attainable Unconditional Security for Shared-Key Cryptosystems, *Information Sciences* (2016), doi: 10.1016/j.ins.2016.06.019

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

Attainable Unconditional Security for Shared-Key Cryptosystems[☆]

Fabrizio Biondi[a,*], Thomas Given-Wilson[a,*], Axel Legay[a]

[a] *Inria, Campus de Beaulieu, 263 Avenue du Général Leclerc, 35042 Rennes, France*

Abstract

Preserving the privacy of private communication is a fundamental concern of computing addressed by encryption. Information-theoretic reasoning models unconditional security where the strength of the results does not depend on computational hardness or unproven results. Usually the information leaked about the message by the ciphertext is used to measure the privacy of a communication, with *perfect secrecy* when the leakage is 0. However this is hard to achieve in practice. An alternative measure is the equivocation, intuitively the average number of message/key pairs that could have produced a given ciphertext. We show a theoretical bound on equivocation called *max-equivocation* and show that this generalizes perfect secrecy when achievable, and provides an alternative measure when perfect secrecy is not achievable. We derive bounds for max-equivocation for *symmetric* encoder functions and show that max-equivocation is achievable when the entropy of the ciphertext is minimized. We show that max-equivocation easily accounts for key re-use scenarios, and that large keys relative to the message perform very poorly under equivocation. We study encoders under this new perspective, deriving results on their achievable maximal equivocation and showing that some popular approaches such as Latin squares are not optimal. We show how unicity attacks can be naturally modeled, and how relaxing encoder symmetry improves equivocation. We present some algorithms for generating encryption functions that are practical and achieve $90 - 95\%$ of the theoretical best, improving with larger message spaces.

Keywords: unconditional security, perfect secrecy, entropy, max-equivocation, private-key cryptography, symmetric encryption

[☆] An earlier version of this paper appeared in the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (2015)

[*] Corresponding author

Email addresses: `fabrizio.biondi@inria.fr` (Fabrizio Biondi), `thomas.given-wilson@inria.fr` (Thomas Given-Wilson), `axel.legay@inria.fr` (Axel Legay)

ACCEPTED MANUSCRIPT

Download English Version:

https://daneshyari.com/en/article/4944978

Download Persian Version:

https://daneshyari.com/article/4944978

Daneshyari.com