Abstract

With the capabilities of computing increasing by leaps and bounds, the need for trusted communication also rises. The present state of ensuring secure communication between devices largely relies on the use of cryptographic keys. The primitive and advanced key generation strategies involve the use of password only, biometric, quantum, PRNG technologies. Recently, the use of contextual information to generate highly secure keys has proven to be a realistic and unobstructed method in the field of cryptography. Contextual information like temperature, luminance and ambient audio may be used for this purpose. This paper presents a detailed survey on the cryptographic techniques for key generation based on contextual information. A brief comparison on the current techniques is also presented in this survey.


Index Terms

Computer Science Security
Keywords

Contextual Information, Key Generation, Data Encryption, Ambient Audio, Audio Fingerprinting