Nomination Statement

I would like to nominate the IEEE S&P 24 paper *Video-Based Cryptanalysis: Extracting Cryptographic Keys from Video Footage of a Device's Power LED Captured by Standard Video Cameras* (authored by Ben Nassi, Etay Iluz, Ofek Vayner, Or Cohen, Dudi Nassi, Boris Zadov, and Yuval Elovici) for the **Best Scientific Cybersecurity Paper of 2024**.

This interesting work introduces a novel threat model for recovering cryptographic keys by leveraging video footage of a device's power LED, captured using standard video cameras. Building on their prior research, the authors demonstrate that a device's power LED, designed to indicate binary on/off states, inadvertently leaks information strongly correlated with the device's power consumption. They previously exploited this phenomenon to recover cryptographic keys (Optical Cryptanalysis, CCS'23) and speech data (Glowworm_Attack, CCS'21) using professional photodiodes and expensive ADC.

This paper challenges longstanding assumptions in cryptanalysis and disputes several key misconceptions in cybersecurity (primarily regarding ways by which computing devices need to be constructed to achieve protection of keys against physical attacks):

Misconceptions About Cryptanalysis Risk

1. *"Professional equipment is required for cryptanalysis."*
   The authors show that widely available tools, such as IP video cameras and smartphone cameras, can be used for cryptanalysis. Namely, that cryptanalysis is not confined to those with access to professional-grade equipment and instead can be executed using low-cost, ubiquitous devices that anyone owns.
2. *"Advanced expertise in digital signal processing and cryptanalysis is required to extract keys."*
   The paper disproves this by showing that attackers with basic skills in analyzing 8-bit RGB video footage can successfully recover cryptographic keys. This redefines cryptanalysis as an accessible capability, even for less technically sophisticated adversaries.

Misconceptions About Device Exposure

3. *"Exposure of devices to cryptanalysis decreases over time."*
   The authors reveal that inexpensive IoT devices (e.g., smartphones and smartcards) with constrained CPU rates (500 MHz–1 GHz) are expected to remain vulnerable to video-based cryptanalysis over time. As the deployment of IoT devices with limited CPU rates continues to grow and video cameras

improve in sensitivity and resolution, the exposure of devices to video-based cryptanalysis attacks is expected to increase in time.

Misconceptions About Industry Progress

4. *"The industry has developed leakage-free devices."*
   Despite advances in cryptanalysis research, the paper highlights that developing completely leakage-free devices remains a formidable challenge for the industry. This emphasizes once again the complexity of building circuits that are resilient to side-channel attacks in practice.

By disputing the above mentioned misconceptions regarding cryptanalysis, the paper makes a profound contribution to the science of cybersecurity. The authors provide a scientific basis to the falsehood of a longstanding axiom in the field of cryptanalysis, and, in fact, **cryptanalysis has always been within reach of ordinary attackers** (by exploiting the power LED of devices to infer power consumption variations). Moreover, the findings of the paper establish a basis for the need to integrate LEDs into circuits in a trusted manner that does not endanger the confidentiality of the information processed by the CPU. Consequently, I nominate it for the NSA_award.