# Article information:

On the adoption of scramble keypad for unlocking PIN-protected smartphones | International Journal of Information and Computer Security
<https://www.inderscienceonline.com/doi/pdf/10.1504/IJICS.2021.115345>

# Article summary:

1. The adoption of scramble keypad for unlocking PIN-protected smartphones is a promising solution to prevent shoulder surfing attacks.

2. Scramble keypad involves rearranging the position of digits on the keypad every time the phone is unlocked, making it difficult for an observer to memorize the PIN.

3. A user study showed that participants found scramble keypad easy to use and preferred it over traditional PIN entry methods.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article titled "On the adoption of scramble keypad for unlocking PIN-protected smartphones" published in the International Journal of Information and Computer Security discusses the use of a scramble keypad as an alternative method for unlocking PIN-protected smartphones. The authors, Geetika Kovelamudi, Bryan Watson, Jun Zheng, and Srinivas Mukkamala, are affiliated with the Department of Computer Science and Engineering at New Mexico Institute of Mining and Technology and The Institute of Complex Additive Systems Analysis.

The article presents a detailed analysis of the current methods used for unlocking PIN-protected smartphones and highlights their limitations. It then proposes the use of a scramble keypad as an alternative method that can improve security while also being user-friendly. The authors provide a thorough explanation of how the scramble keypad works and its potential benefits.

However, there are some potential biases in this article that need to be considered. Firstly, the authors do not provide any evidence to support their claim that current methods for unlocking PIN-protected smartphones are inadequate. While they do mention some limitations such as shoulder surfing attacks and smudge attacks, they do not provide any data or statistics to show how prevalent these attacks are or how effective they are in compromising smartphone security.

Secondly, the article seems to be promoting the use of a scramble keypad without fully exploring its potential drawbacks or considering other alternatives. For example, while the authors mention that users may find it easier to remember patterns on a scramble keypad than traditional PINs, they do not consider whether this could lead to users choosing weaker passwords or patterns that are easier to guess.

Additionally, there is no discussion about how easy it would be for attackers to crack a scramble keypad using brute force methods or other techniques. This is an important consideration since any new method for unlocking smartphones should be resistant to attacks by hackers.

Overall, while this article provides an interesting proposal for improving smartphone security through the use of a scramble keypad, it is important to consider its potential biases and limitations. The authors should provide more evidence to support their claims and fully explore the potential drawbacks of this method before promoting it as a viable alternative to traditional PINs.

# Topics for further research:

* Effectiveness of shoulder surfing attacks on smartphone security
* Smudge attacks and their impact on PIN-protected smartphones
* Comparison of scramble keypad and biometric authentication for smartphone security
* Potential weaknesses of scramble keypad for unlocking smartphones
* Brute force methods for cracking scramble keypad passwords
* User behavior and password strength on scramble keypad versus traditional PINs

# Report location:

<https://www.fullpicture.app/item/29cb65d7061b70e551b685d80067e39e>