

**From:** [Fisher, Bill \(Fed\)](#)  
**To:** [Kelsey, John M. \(Fed\)](#)  
**Cc:** [Sonmez Turan, Meltem \(Fed\)](#); [Perlner, Ray A. \(Fed\)](#)  
**Subject:** Re: Fractal Authentication?  
**Date:** Thursday, August 1, 2019 3:35:04 PM

---

Thanks John. I saw the same. And yes they had a patent pending way of handling it. They claimed that no two images on a mobile phone would be the same and used 2-3 input media from a mobile device (image, voice, video, etc...) as source data for a pad that generated keys.

Figured I would double check with you since I have never heard of it. As an FYI, it was part of a PSCR Prize challenge for using the SIM as hardware storage for FIDO keys, but they didn't actually do an implementation on the SIM so they won't make it past this round of the challenge and NIST won't be associated with the work.

Thanks! -Bill

--

Bill Fisher  
Security Engineer  
National Cybersecurity Center of Excellence  
Office: 303-497-5172  
Cell: 301-351-8493  
[William.Fisher@nist.gov](mailto:William.Fisher@nist.gov)

---

**From:** "Kelsey, John M. (Fed)" <[john.kelsey@nist.gov](mailto:john.kelsey@nist.gov)>  
**Date:** Wednesday, July 31, 2019 at 2:38 PM  
**To:** "Fisher, Bill (Fed)" <[william.fisher@nist.gov](mailto:william.fisher@nist.gov)>  
**Cc:** "Sonmez Turan, Meltem (Assoc)" <[meltem.turan@nist.gov](mailto:meltem.turan@nist.gov)>, "Perlner, Ray (Fed)" <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)>  
**Subject:** Re: Fractal Authentication?

I've never heard of it before, and a quick Google search didn't turn up anything more than some paper about using fractal encoding for some kind of image used in a user authentication scheme. It sounds like some kind of proprietary scheme someone came up with on their own, rather than a term of art in cryptography.

--John

---

**From:** "Fisher, Bill (Fed)" <[william.fisher@nist.gov](mailto:william.fisher@nist.gov)>  
**Date:** Wednesday, July 31, 2019 at 15:45  
**To:** "Kelsey, John M. (Fed)" <[john.kelsey@nist.gov](mailto:john.kelsey@nist.gov)>  
**Subject:** Fractal Authentication?

John,

Wondering if you know if NIST has any interest in fractal authentication methods. We had a company present to a PSCR prize challenge today that wanted to use a fractal algorithm for authentication. I personally had never heard of it before. Just reaching out to see if NIST has an opinion on this (potentially as a post-quantum algorithm) and if I should have it on my radar.

Thanks! -Bill

--

Bill Fisher

Security Engineer

National Cybersecurity Center of Excellence

Office: 303-497-5172

Cell: 301-351-8493

[William.Fisher@nist.gov](mailto:William.Fisher@nist.gov)