On the Practical Exploitability of Dual EC in TLS Implementations

Stephen Checkoway,[*] Matthew Fredrikson,[†] Ruben Niederhagen,[‡]
Matthew Green,[*] Tanja Lange,[‡] Thomas Ristenpart,[†]
Daniel J. Bernstein,[‡ §] Jake Maskiewicz,[¶] and Hovav Shacham,[¶]
[*] *Johns Hopkins University,* [†] *University of Wisconsin,* [‡] *Technische Universiteit Eindhoven,*
[§] *University of Illinois at Chicago,* [¶] *UC San Diego*

The paper has been temporarily removed. It will return shortly.