

Paper 2020/1484

Cryptanalysis of Aggregate Γ -Signature and Practical Countermeasures in Application to Bitcoin

Goichiro Hanaoka, Kazuo Ohta, Yusuke Sakai, Bagus Santoso, Kaoru Takemure, and Yunlei Zhao

Abstract

We present a sub-exponential forger by using a k -sum algorithm against the aggregate Γ -signature, which was proposed at AsiaCCS 2019 by Zhao. Our forger is a universal forger under a key-only attack and effective in the knowledge of secret key model. We also discuss the real impact of this attack in reality with Bitcoin applications. The discussions on the real impact of the attack also highlight the significant differences between the usage of individual signatures like EC-DSA and that of aggregate signatures in the blockchain systems like Bitcoin, which might be of independent interest and could bring forth interesting questions for future investigations.

Metadata

Available format(s)



Category

Public-key cryptography

Publication info

Preprint. MINOR revision.

Keywords

`k-sum algorithm` `aggregate signature` `universal forgery` `blockchain`

Contact author(s)

`takemure @ uec ac jp`
`yusuke sakai @ aist go jp`
`santoso bagus @ uec ac jp`

ylzhao @ fudan edu cn

History

2020-12-15: last of 2 revisions

2020-11-29: received

[See all versions](#)

Short URL


<https://ia.cr/2020/1484>

License



[CC BY](#)

BibTeX

 Copy to clipboard

```
@misc{cryptoeprint:2020/1484,  
  author = {Goichiro Hanaoka and Kazuo Ohta and Yusuke Sakai and Bagus Santoso and Kaoru  
  title = {Cryptanalysis of Aggregate  $\Gamma$ -Signature and Practical Countermeasures in  
  howpublished = {Cryptology ePrint Archive, Paper 2020/1484},  
  year = {2020},  
  note = {\url{https://eprint.iacr.org/2020/1484}},  
  url = {https://eprint.iacr.org/2020/1484}  
}
```



