OPRFs: notes and more

Sofía Celi

April 10, 2022

1 Introduction

From [NT22]:
"An oblivious pseudorandom function (OPRF) [FIPR05, JL09] allows a client holding a private input x and a server holding a key for a PRF f to engage in a protocol to *obliviously* evaluate f on x. The client learns (and optionally verifies) the evaluation $f_(x)$ while the server learns nothing."

OPRFS are used in many privacy-preserving protocols:

- Anti-Fraud systems [DGS+18], such Privacy Pass,
- Private set-intersecction for compromised credentials [LPA+19, TPY+19],
- Password-authenticated key exchange [JKX18, JKK14],
- De-identified authenticated logging [HIJ+21],
- Private click measurement (PCM) in the W3C [WTKW20],
- Private ad click or visualization [ZeQ19],
- Collecting user data [DSQ+21] [AD22],
- Contact tracing apps [SS21].

They are used to provide proof between sessions that a positive action took place.

2 Limitations

Some know limitations:

- Key management: the server often has to maintain a single main key, or a set of keys per client/user. This is prone to leakage or to problems with key rotation.
- Double spending protection: servers have to keep a large database of spent tokens per client. Each request for spending a token has to be checked with the database so tokens are not double-spent. Maintaining this database is cumbersome. Is there a better solution?
- Hoarding attacks: individual users (or groups of users) gather tokens over a long period of time and redeeming them all at once, e.g., in an attempt to overwhelm a service.
- Hoarding cookies: A successful token redemption could be exchanged for single-origin cookies. These cookies allow clients to avoid future challenges for a particular domain without using more tokens. In the case of a hoarding attack, an attacker could trade in their hoarded number of tokens for a number of cookies:
  - Cookies are bound to the domain they are issued, the IP address they are issued to, and have a fixed lifetime. Traded by tokens, they are not bounded anymore.
  - Mount a layer 7 DDoS attack with the "hoarded" cookies.
- Malicious servers: server can choose malicious keys.

- Lack of unification of security/privacy properties.
- Lack of knowledge of the effects of integrating OPRFs into protocols, like TLS.
- No post-quantum efficient proposal, as they rely on discrete-log- or factoring-type hardness assumption.

2.1 New applications?

- Token Theft: Session credentials for authenticated users are traditionally stored as cookies in the browser. "These are easily extracted by malware. Services traditionally defend against this by associating certain invariant client properties (screen size, webGL renderer, etc) with a user's cookie, and rejecting the session credential (forcing the use to re-authenticate) if it appears that the cookie is used on a new device" [W3C22]. Do we still have to use cookies for this?
- Fake engagement: "Fake engagements may be simulated (i.e. generated by something other than the honest platform), automated or hijacked (i.e. generated on the claimed platform, but without genuine user intent), or incentivized (i.e. generated by a human in exchange for an undisclosed incentive)." [W3C22]. Can we use anonymous tokens for this?
- Linking to private windows in a "private way".

2.2 What can we achieve?

- A SoK for the different needs for OPRFs. The best starting point is: [CHL22].
- A potential list of applications.
- A survey of fraud attacks and how anonymous tokens can help.
- Working group to explore these cases.

References

[AD22] Peter Snyder Alex Davidson, Shivan Sahib. STAR: Distributed Secret Sharing for Private Threshold Aggregation Reporting. Internet-Draft draft-dss-star-00, Internet Engineering Task Force, March 2022. Work in Progress.

[CHL22] Sílvia Casacuberta, Julia Hesse, and Anja Lehmann. Sok: Oblivious pseudorandom functions. Cryptology ePrint Archive, Report 2022/302, 2022. `https://ia.cr/2022/302`.

[DGS+18] Alex Davidson, Ian Goldberg, Nick Sullivan, George Tankersley, and Filippo Valsorda. Privacy pass: Bypassing internet challenges anonymously. *Proc. Priv. Enhancing Technol.*, 2018(3):164–180, 2018.

[DSQ+21] Alex Davidson, Peter Snyder, E. B. Quirk, Joseph Genereux, and Benjamin Livshits. STAR: distributed secret sharing for private threshold aggregation reporting. *CoRR*, abs/2109.10074, 2021.

[FIPR05] Michael J. Freedman, Yuval Ishai, Benny Pinkas, and Omer Reingold. Keyword search and oblivious pseudorandom functions. In *TCC*, volume 3378 of *Lecture Notes in Computer Science*, pages 303–324. Springer, 2005.

[HIJ+21] Sharon Huang, Subodh Iyengar, Sundar Jeyaraman, Shiv Kushwah, Chen-Kuei Lee, Zutian Luo, Payman Mohassel, Ananth Raghunathan, Shaahid Shaikh, Yen-Chieh Sung, and Albert Zhang. PrivateStats: De-Identified Authenticated Logging at Scale, January 2021.

[JKK14] Stanislaw Jarecki, Aggelos Kiayias, and Hugo Krawczyk. Round-optimal password-protected secret sharing and T-PAKE in the password-only model. In *ASIACRYPT (2)*, volume 8874 of *Lecture Notes in Computer Science*, pages 233–253. Springer, 2014.

[JKX18] Stanislaw Jarecki, Hugo Krawczyk, and Jiayu Xu. OPAQUE: an asymmetric PAKE protocol secure against pre-computation attacks. In *EUROCRYPT (3)*, volume 10822 of *Lecture Notes in Computer Science*, pages 456–486. Springer, 2018.

[JL09] Stanislaw Jarecki and Xiaomin Liu. Efficient oblivious pseudorandom function with applications to adaptive OT and secure computation of set intersection. In *TCC*, volume 5444 of *Lecture Notes in Computer Science*, pages 577–594. Springer, 2009.

[LPA+19] Lucy Li, Bijeeta Pal, Junade Ali, Nick Sullivan, Rahul Chatterjee, and Thomas Ristenpart. Protocols for checking compromised credentials. In *CCS*, pages 1387–1403. ACM, 2019.

[NT22] Thomas Ristenpart Nick Sullivan Stefano Tessaro Christopher Wood Nirvan Tyagi, Sofía Celi. A fast and simple partially oblivious prf, with applications. 2022.

[SS21] Tjerand Silde and Martin Strand. Anonymous tokens with public metadata and applications to private contact tracing. *IACR Cryptol. ePrint Arch.*, 2021:203, 2021.

[TPY+19] Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, Sarvar Patel, Dan Boneh, and Elie Bursztein. Protecting accounts from credential stuffing with password breach alerting. In *USENIX Security Symposium*, pages 1556–1571. USENIX Association, 2019.

[W3C22] W3C. W3C Anti-Fraud Community Group - Use Cases Threat Models. Technical report, W3C, 2022. Work in Progress.

[WTKW20] John Wilander, Erik Taubeneck, Andrew Knox, and Chris Wood. Consider using blinded signatures for fraud prevention - Private Click Measurement, 2020. https://github.com/privacycg/private-click-measurement/issues/41.

[ZeQ19] Yan Zhu and eV Quirk. A Brave new model for the web, 2019.