

# Evaluating the Working of Blocking Misbehaving Users in Anonymous N/Ws

<sup>1</sup>Lakshmi Jammulamada, <sup>2</sup>D. Kumar, <sup>3</sup>P. Pedda Sadhu Naik

<sup>1, 2, 3</sup>Dept. of CSE, Dr. Samuel George Institute of Engg & Technology, Markapur, Prakasam, Andhra Pradesh, India

## Abstract

Several anonymous authentication schemes allow servers to revoke a misbehaving user's ability to make future accesses. Traditionally, these schemes have relied on powerful, capable of deanonymizing (or linking) users' connections. Recent schemes such as Blacklist able Anonymous Credential and Enhanced Privacy ID support "privacy-enhanced revocation" | servers can revoke misbehaving users without a tor involvement, and without learning the revoked users' identities. In BLAC and EPID, however, the computation required for authentication at the server is linear in the size of the revocation list. We propose a new anonymous authentication scheme for which this bottleneck computation is independent of the size of the revocation list. Instead, the time complexity of authentication is linear in the size of a revocation window, the number of subsequent authentications before which a user's misbehavior must be recognized if the user is to be revoked. We prove the security of our construction, and have developed a prototype implementation to validate its eminency experimentally.

## Keywords

Anonymous authentication, privacy-enhanced revocation, subjective blacklisting, non-membership

## 1. Introduction

Anonymous authentication schemes allow users to authenticate to service providers as some anonymous member of a group. Fully-anonymous authentication, however, can give users the license to misbehave since they cannot be held culpable for their actions. For example, a website such as Wikipedia may allow anonymous postings, but then cannot hold users who deface webpages accountable. To mitigate this problem, several schemes support revocation of anonymous users, where a trusted third party can take action against misbehaving users. At a high level, authentication in these schemes requires users to send SPs their pseudonyms encrypted with the TTP's key; SPs can present a misbehaving user's escrowed identity to the TTP as part of a complaint procedure.

In pseudonymous credential systems users log into Web sites using pseudonyms, which can be added to a blacklist if a user misbehaves. Unfortunately, this approach results in pseudonymity for all users, and weakens the anonymity provided by the anonymizing network. Anonymous credential systems employ group signatures. Basic group signatures allow servers to revoke a misbehaving user's anonymity by complaining to a group manager. Servers must query the group manager for every authentication, and thus, lacks scalability. Traceable signatures allow the group manager to release a trapdoor that allows all signatures generated by a particular user to be traced; such an approach does not provide the backward unlink ability that we desire, where a user's accesses before the complaint remain anonymous. Backward unlinkability allows for what we call subjective blacklisting, where servers can blacklist users for whatever reason since the privacy of the blacklisted user is not at risk. In contrast, approaches without backward unlinkability

need to pay careful attention to when and why a user must have all their connections linked, and users must worry about whether their behaviors will be judged fairly. Subjective blacklisting is also better suited to servers such as Wikipedia, where misbehaviors such as questionable edits to a Webpage, are hard to define in mathematical terms. In some systems, misbehavior can indeed be defined precisely. For instance, double spending of an "e-coin" is considered misbehavior in anonymous e-cash systems following which the offending user is deanonymized. Unfortunately, such systems work for only narrow definitions of misbehavior it is difficult to map more complex notions of misbehavior onto "double spending" or related approaches.

## II. Proposed System

We present a secure system called Nymble, which provides all the following properties: anonymous authentication, backward unlink ability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation audit ability (where users can verify whether they have been blacklisted), and also addresses the Sybil attack to make its deployment practical. In Nymble, users acquire an ordered collection of nymbles, a special type of pseudonym, to connect to websites. Without additional information, these nymbles are computationally hard to link, and hence using the stream of nymbles simulates anonymous access to services.

Websites, however, can blacklist users by obtaining a seed for a particular nymble, allowing them to link future nymbles from the same user — those used before the complaint remains unlinkable. Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. Our system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted. Although our work applies to anonymizing networks in general, we consider Tor for purposes of exposition. In fact, any number of anonymizing networks can rely on the same Nymble system, blacklisting anonymous users regardless of their anonymizing network(s) of choice.

We now present a high-level overview of the Nymble system, and defer the entire protocol description and security analysis to subsequent sections.

## III. Contribution

### A. Resource-Based Blocking

To limit the number of identities a user can obtain (called the Sybil attack [19]), the Nymble system binds nymbles to resources that are sufficiently difficult to obtain in great numbers. For example, we have used IP addresses as the resource in our implementation, but our scheme generalizes to other resources such as email addresses, identity certificates, and trusted hardware. We address the practical issues related with resource-based blocking in Section 8, and suggest other alternatives for resources. We do not claim to solve the Sybil attack. This problem is faced by any credential system [19, 27], and we suggest some promising approaches based

on resource-based blocking since we aim to create a real-world deployment.

### B. The Pseudonym Manager

The user must first contact the Pseudonym Manager (PM) and demonstrate control over a resource; for IP-address blocking, the user must connect to the PM directly (i.e., not through a known anonymizing network). We assume the PM has knowledge about Tor routers, for example, and can ensure that users are communicating with it directly.<sup>6</sup> Pseudonyms are deterministically chosen based on the controlled resource, ensuring that the same pseudonym is always issued for the same resource. Note that the user does not disclose what server he or she intends to connect to, and the PM's duties are limited to mapping IP addresses (or other resources) to pseudonyms. As we will explain, the user contacts the PM only once per link ability window (e.g., once a day).

### C. The Nymble Manager

After obtaining a pseudonym from the PM, the user connects to the Nymble Manager (NM) through the anonymizing network, and requests nymbles for access to a particular server (such as Wikipedia). A user's requests to the NM are therefore pseudonymous, and nymbles are generated using the user's pseudonym and the server's identity. These nymbles are thus specific to a particular user-server pair. Nevertheless, as long as the PM and the NM do not collude, the Nymble system cannot identify which user is connecting to what server; the NM knows only the pseudonym-server pair, and the PM knows only the user identity-pseudonym pair. To provide the requisite cryptographic protection and security properties, the NM encapsulates nymbles within nymble tickets. Servers wrap seeds into linking tokens, and therefore, we will speak of linking tokens being used to link future nymble tickets. The importance of these constructs will become apparent as we proceed.

### D. Blacklisting a User

If a user misbehaves, the server may link any future connection from this user within the current linkability window (e.g., the same day). Consider an example: A user connects and misbehaves at a server during time period  $t_1$  within linkability window  $w_1$ . The server later detects this misbehavior and complains to the NM in time period  $t_c$  ( $t_1 < t_c \leq t_L$ ) of the same linkability window  $w_1$ . As part of the complaint, the server presents the nymble ticket of the misbehaving user and obtains the corresponding seed from the NM. The server is then able to link future connections by the user in time periods  $t_c; t_{c+1}; \dots; t_L$  of the same linkability window  $w_1$  to the complaint. Therefore, once the server has complained about a user, that user is blacklisted for the rest of the day, for example (the linkability window). Note that the user's connections in  $t_1; t_2; \dots; t_{c-1}; t_{c+1}; \dots; t_L$  remain unlinkable (i.e., including those since the misbehavior and until the time of complaint). Even though misbehaving users can be blocked from making connections in the future, the users' past connections remain unlinkable, thus providing backward unlinkability and subjective blacklisting.

### E. Notifying the User of Blacklist Status

Users who make use of anonymizing networks expect their connections to be anonymous. If a server obtains a seed for that user, however, it can link that user's subsequent connections. It is of utmost importance then that users be notified of their blacklist status before they present a nymble ticket to a server. In our system, the user can download the server's blacklist and

verify her status. If blacklisted, the user disconnects immediately. Since the blacklist is cryptographically signed by the NM, the authenticity of the blacklist is easily verified if the blacklist was updated in the current time period (only one update to the blacklist per time period is allowed). If the blacklist has not been updated in the current time period, the NM provides servers with "daisies" every time period so that users can verify the freshness of the blacklist ("blacklist from time period told is fresh as of time period now"). As discussed, these daisies are elements of a hash chain, and provide a lightweight alternative to digital signatures. Using digital signatures and daisies, we thus ensure that race conditions are not possible in verifying the freshness of a blacklist. A user is guaranteed that he or she will not be linked if the user verifies the integrity and freshness of the blacklist before sending his or her nymble ticket.

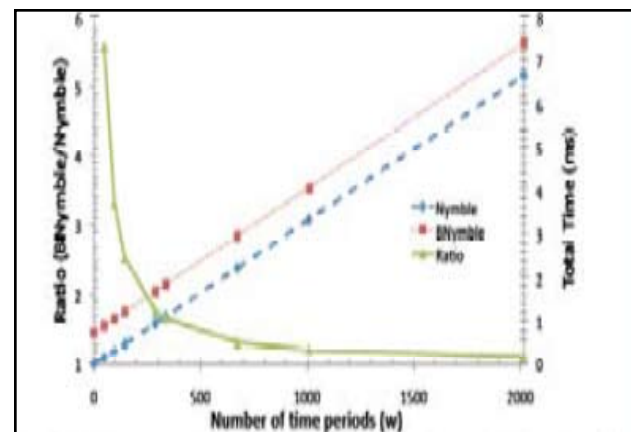


Fig. 1. Total cryptographic cost of user registration, nymble acquisition and nymble verification as a function of number of time periods per linkability window. With one week linkability windows and 5-minute time periods, the total cost of BNymble is only 1% higher than Nymble.

## IV. Valuation of Nymble

### A. Security Analysis

Security Analysis ENymble preserves Nymble's security properties: Blacklistability, Rate-limiting, Non-frameability and Anonymity, assuming the one-more RSA inversion problem is computationally intractable. Blacklistability. An honest Pseudonym Manager will only issue one bnym per user. Thus for a coalition of  $c$  users to authenticate after all have been blacklisted, they would either have to forge a bnym, violating the assumed intractability of the one-more RSA inversion problem, or they would have to break blacklistability using only  $c$  pseudonyms, violating the blacklistability of Nymble. Non-Frameability. Since distinct users have distinct uids, an honest PM will only refuse to grant a bnym to a user if that user has already received a bnym in that linkability window. Also, an honest NM will grant a different set of nymbles to each bnym. Thus there is no way for one user to frame another without violating the nonframeability of Nymble. Anonymity. Anonymity in is defined with respect to SPs only (that is, assuming non-colluding PM and NM). It is easy to see that since the nymbles in ENymble are generated according to the same process, the same property holds. We also can define anonymity in a much stronger sense: let the adversary control the PM, NM, and SP, and choose two users  $U$  and  $V$ . We allow the adversary to ask each user to register and acquire nymbles for any linkability window and any SP of the adversary's choosing, for any number  $k$  of window/SP pairs. The adversary then specifies a single, new linkability window;  $U$  and  $V$  execute the user registration protocol (with the

adversary), and then execute the credential acquisition protocol in a random ordering. The adversary wins if he can guess whether U or V acquired nymbles first. The protocol is anonymous if no adversary can win with probability non-negligibly greater than  $1=2$ . (Notice that since the adversary sees the nymbles issued, this implies that for any time period, the nymbles themselves are also indistinguishable.) Because bnyms are information theoretically independent of both uids and bnyms from other windows, every adversary wins this game with probability exactly  $\frac{1}{2}$

## B. Efficiency

In order to compare the cost of the various TTP-based anonymous blacklisting systems, we measured the costs of the basic cryptographic operations required of the users, NM, PM, and SP in each of the systems. Table 1 shows these costs. User registration in ENymble is obviously the most expensive phase, but it is also the least executed protocol - occurring once per linkability window. Figure 1 shows how this one-time cost compares to the total cost of authentication for various linkability window sizes. At  $w=288$ , as suggested by the total cost of authentication in ENymble is less than a factor of 2 greater than Nymble, compared to 5 orders of magnitude from Nymbler and Jack. Longer linkability windows decrease this difference further - with 5-minute time periods and a one-week linkability window ( $w=2016$ ), the difference is only 11%.

## V. Conclusion

We have proposed new enhancement for the original design of Nymble System. We present ENymble, a scheme which matches the anonymity guarantees of Nymbler and Jack while (nearly) maintaining the efficiency of the original Nymble. The key insight of ENymble is that we can achieve the anonymity goals of these more recent schemes by replacing only the infrequent "User Registration" protocol from Nymble with asymmetric primitives.

## References

- [1] Giuseppe Ateniese, Jan Camenisch, Marc Joye, Gene Tsudik, "A practical and provably secure coalition-resistant group signature scheme", In Mihir Bellare, editor, CRYPTO, Vol. 1880 of LNCS, pp. 255–270, Springer, 2000.
- [2] Mihir Bellare, Daniele Micciancio, Bogdan Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions", In Eli Biham, editor, EUROCRYPT, Vol. 2656 of LNCS, pp. 614–629, Springer, 2003.
- [3] Mihir Bellare, Haixia Shi, Chong Zhang, "Foundations of group signatures: The case of dynamic groups", In Alfred Menezes, editor, CT-RSA, Vol. 3376 of LNCS, pp. 136–153, Springer, 2005.
- [4] Stefan Brands, "Untraceable off-line cash in wallets with observers (extended abstract)", In Douglas R. Stinson, editor, CRYPTO, Vol. 773, pp. 302–318, Springer, 1993.
- [5] Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, Mira Meyerovich, "How to win the clonewars: efficient periodic n-times anonymous authentication", In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, ACM Conference on Computer and Communications Security, pp. 201–210, ACM, 2006.
- [6] Jan Camenisch, Susan Hohenberger, Anna Lysyanskaya, "Compact e-cash", In Ronald Cramer, editor, EUROCRYPT, Vol. 3494 of LNCS, pp. 302–321, Springer, 2005.

- [7] Jan Camenisch, Anna Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation", In Irgit Pfitzmann, editor, EUROCRYPT, Vol. 2045 of LNCS, pp. 93–118, Springer, 2001.
- [8] S. Brands, "Untraceable Off-Line Cash in Wallets with Observers (Extended Abstract)", Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 302–318, 1993.
- [9] E. Bresson, J. Stern, "Efficient Revocation in Group Signatures", Proc. Conf. Public Key Cryptography, Springer, pp. 190–206, 2001.
- [10] J. Camenisch, A. Lysyanskaya, "An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation", Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 93–118, 2001.
- [11] J. Camenisch, A. Lysyanskaya, "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials", Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 61–76, 2002.
- [12] J. Camenisch, A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Maps", Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 56–72, 2004.
- [13] D. Chaum, "Blind Signatures for Untraceable Payments", Proc. Ann. Int'l Cryptology Conf. (CRYPTO), pp. 199–203, 1982.
- [14] D. Chaum, "Showing Credentials without Identification Transferring Signatures between Unconditionally Unlinkable Pseudonyms", Proc. Int'l Conf. Cryptology (AUSCRYPT), Springer, pp. 246–264, 1990.
- [15] D. Chaum, E. van Heyst, "Group Signatures", Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 257–265, 1991.



Lakshmi Jmmulamadaka was born Ganikapudi, Guntur Dt, Andhra Pradesh, India. She received B.Tech in C.S.E from JNT University, Hyderabad, Andhra Pradesh, India. Presently, she is pursuing M.Tech in C.S.E from Samuel George College of Engineering and Technology, Markapur, Prakasam Dt, Andhra Pradesh, India. Her Research interest includes Computer Networks and NYMBLE:

BLOCKING MISBEHAVING USERS IN ANONYMIZING NETWORKS



D KUMAR was born in Terala, Guntur Dt, Andhra Pradesh, India. He received B.Tech in CSIT from JNTUH University, India. And He completed his M.Tech C S E from JNTU Kakinada, Andhra Pradesh, India. Currently he is working as Assoc. Professor in CSE .Department for Samuel George Institute Of Engineering And Technology, Markapur, Prakasam District, Andhra Pradesh , India.



P. Pedda Sadhu Naik received B.Tech (CSE) Degree from JNT University in 2003 and M.Tech (CS) Degree from JNTUCE Anantapur in 2007. He is doing Ph D from JNTUK, Kakinada in Computer Science under the guidance of Dr T. Venu Gopal. He is Associate Professor, JNTU College of Engineering, Jagityal, Karimnagar District. He has 9 years of teaching experience. He joined as Assistant Professor in Dr. Samuel George Institute of Engineering & Technology,

Markapur, India in 2003. Presently he is working as Associate Professor and Head of the Department of CSE. His Interested research areas are Image Processing and Soft Computing. He has life member of ISTE and IAENG. He organized various National level Technical Symposia as Convener. He attended Various National and International Workshops and Conferences on image Processing.