AN ADVANCE TO NYMBLE FOR BLOCKING AND TRACKING MISBEHAVING USERS WHILE PRESERVING ANONYMITY

M.Durga prasad[1], Dr TVS Prasad gupta[2], N.Swapna[3]

[1]*M.tech student, Computer science &engineering, Vijay Rural Engineering College, AP, India,* ***durgamamidyala@gmail.com***
[2]*Professor, Head of the Department (Computer science), Vijay Rural Engineering College, AP, India,* ***prasadgupta_tvs@gmail.com***
[3]*Assoc Professor, Department of Information technology, Vijay Rural Engineering College, AP, India,* ***swapnanaralas@gmail.com***

Abstract

Anonymizing networks such as Tor allow users to access Internet services privately by using a series of routers to hide the client's IP address from the server. Web site administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but blocking IP addresses is not practical if the abuser routes through an anonymizing network. As a result, administrators block all known exit nodes of anonymizing networks, denying anonymous access to misbehaving and behaving users alike. To address this problem Nymble is developed, a system in which servers can "blacklist" misbehaving users. We present extensions to nymble framework for anonymizing blacklisting schemes. First, we provide a mechanism to nymble manager to track blacklisting of user in multiple linking windows while preserving anonymity of the users. Some users always look to misbehave with servers; there major intention is to make the server down. The problem with nymble is nymble manager blacklist a user for one likability window (i.e. 1 day), on the other day again he can misbehave with same server or other server. He can continue it as his everyday activity as Nymble manager doesn't have any mechanism to identify such type of users while preserving anonymity. To address this problem, we present a Mechanism which can identify such users, while preserving anonymity and nymble manager with identified information can decide upon how much time to blacklist a misbehaving user.

Index Terms: *Anonymous blacklisting, anonymizing networks, privacy, Nymble, pseudo tracker.*

---------- *** ----------

1. INTRODUCTION

Anonymizing networks such as Tor re-route a user's traffic between several nodes in different domains. Since these nodes are operated independently, users are able to trust the anonymizing network to provide anonymity. Real-world deployments of anonymizing networks, however, have had limited success because of their misuse. Websites Administrators are unable to blacklist malicious users' IP addresses because of their anonymity. Left with no other choice, these administrators opt to blacklist the entire anonymizing network. This approach eliminates malicious activity through such networks, but at the cost of the anonymity.

There are several solutions to this problem, each providing some degree of accountability. 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 unlinkability 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.

With dynamic accumulators, a revocation operation results in a new accumulator and public parameters for the group, and all other existing users' credentials must be updated, making it impractical. Verifier-local revocation (VLR) fixes this shortcoming by requiring the server ("verifier") to perform only local updates during revocation. Unfortunately, VLR requires heavy computation at the server that is linear in the size of the blacklist. For example, for a blacklist with 1,000 entries, each authentication would take tens of seconds, a prohibitive cost in practice. In contrast, our scheme takes the server about one millisecond per authentication, which is several thousand times faster than VLR. We believe these low overheads will incentivize servers to adopt such a solution when weighed against the potential benefits of anonymous publishing (e.g., whistle-blowing, reporting, anonymous tip lines, activism, and so on.).

All the problems that a user or server faces with anonymous networks is solved by Secure system called Nymble, which provide all the following properties such as anonymous authentication, backward Unlinkability, subjective blacklisting, fast authentication and so on. We have identified drawbacks in Nymble system and proposed Extended Nymble system. Nymble manager can blacklist a misbehaving user by collecting seed for a particular nymble and linking linkability window. This seed can be used to link future connections of this misbehaving user. Nymble manager makes misbehaving users linkable for one Linkability window (i.e. 1 day).After this Misbehaving users become unlikable. On the other day if the same user again misbehaves again he will be blacklisted, this Misbehaving can be a regular activity of certain users. In Existing Nymble we don't have any technique to track such users because of backward Unlinkability. We have proposed a model which can track users with anonymity and backward Unlinkability.

In the same way Nymble Manager generates Nymble and gives it to a user by given pseudonym–server pair, so a nymble changes when user connects to different server. If a user misbehaves with different servers we don't have any mechanism to blacklist misbehaving users, as nymble changes. Our proposed model deals to solve this problem

2. AN OVERVIEW OF EXTENDED NYMBLE APPROACH

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

2.1 Resource-Based Blocking

To limit the number of identities a user can obtain, the Nymble system binds nymbles to resources that are sufficiently difficult to obtain in great numbers. For example, we can use IP addresses as the resource in our implementation, but our scheme generalizes to other resources such as email addresses, identity certificates, and trusted hardware. Here, Pseudonym Manager maintains identity information of users such that chosen resource or combination of resources uniquely identifies the user.

2.2PseudoTracker-Based Tracking

Some users always look to misbehave with servers; there major intention is to make the server down. The problem with nymble is nymble manager blacklist a user for one likability window (i.e. 1 day), on the other day again he can misbehave with same server or other server. He can continue it as his everyday activity as Nymble manager doesn't have any mechanism to identify such type of users while preserving anonymity.

To address this problem, Pseudo Tracker is developed (as shown in Fig 1) as part of Pseudonym Manager in our Extended Nymble System. Pseudo tracker contains identity information of the user and Rating. A user registered newly is highly rated. This rating is used to track the users. If a user misbehaves with a server, server complaints to Nymble Manager (NM). NM Complaints the particular Pseudonym to Pseudonym Manager (NM complaints only Pseudonym of misbehaving user but not the server with which he misbehaved to preserve anonymity of user).Pseudonym Manager sends this information to Pseudo Tracker, where the rating of misbehaving user deteriorate depending on no of times he misbehaved. NM uses rating to blacklist a user for many linkability windows.

2.3 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), as shown in Fig. 1.We assume the PM has knowledge about Tor routers, for example, and can ensure that users are communicating with it directly. 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 not limited to mapping IP addresses (or other resources) to pseudonyms. Whenever a pseudonym is given for a particular user the PM enrolls the details of the user into pseudo tracker. Pseudo tracker contains Identity information and Rating. Identity information is provided by the user which is unique and used for tracking users. Whenever a new user registers with pseudonym manager by giving identity information PM maintains the identity details of the user and rating in pseudo tracker. For Newely registered user the rating will be high (For ex-10). The user as we will explain, the user contacts the PM only once per linkability window (e.g., once a day).On the other day as the registered users provide same identity, Pseudo tracker can be used to maintain identity and rating details of a user.

2.4 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. Whenever a user is blacklisted the pseudonym of the particular user is send to PM(note that only pseudonym is send but not the name of server the user misbehaved, to preserve anonymity and backward Unlinkability)

2.5 Time

Nymble tickets are bound to specific time periods. As illustrated in Fig. 2, time is divided into linkability windows of duration W, each of which is split into L time periods of duration T (i.e., W =L* T). We will refer to time periods and linkability windows chronologically as t1; t2; . . . ; tL and w1; w2; . . . , respectively. While a user's access within a time period is tied to a single nymble ticket, the use of different nymble tickets across time periods grants the user anonymity between time periods. Smaller time periods provide users with higher rates of anonymous authentication, while longer time periods allow servers to rate-limit the number of misbehaviors from a particular user before he or she is blocked. For example, T could be set to five minutes, and W to one day (and thus, L = 288) or many days (L=n*288)

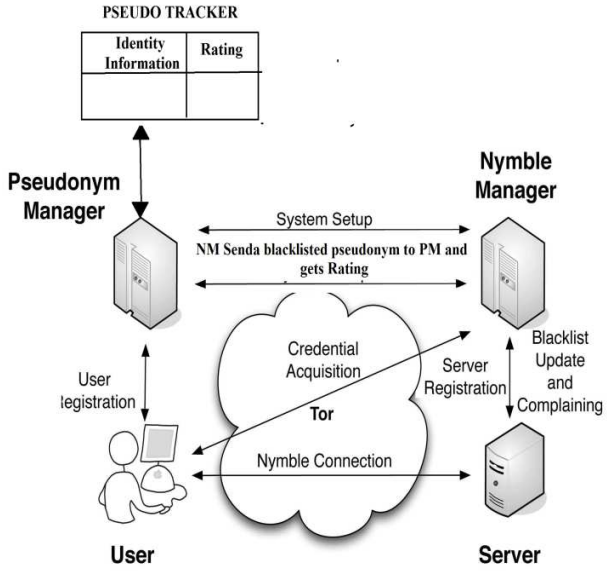

Fig 1: The Extended Nymble system architecture showing the various modes of Interaction. Note that users interact with the NM and servers though the anonymizing network.

2.6 Blacklisting and tracking a User anonymously

If a user misbehaves with a server then server complaints to Nymble Manager. The Nymble Manager before blacklisting a user gets the details of the user from Pseudonym manager. The pseudonym manager gets the details of the user from Pseudo tracker; Pseudo tracker maintains identity information and rating, if suppose a user misbehaved in past the rating of particular user moves down. Nymble manager gets the rating and if rating of particular user is high (For ex-10), it indicates that user misbehave for first or less frequent times. If rating is

Low then Nymble manager can decides upon no of linkability windows the user should be blacklisted.

Nymble manager sends the misbehaving user pseudonym but not the details of the server with which he misbehaved. So our Extended Nymble maintains Anonymous authentication.

If a user misbehaves with a server, server may link any future connection from this user from the current linkability window. Consider Fig. 2 as an example: A user connects and misbehaves at a server during time period t* within linkability window w*.The server later detects this misbehavior and complains to the NM in time period tc (t* < tc <= tL) of the same linkability window w*.

Whenever a server complaints NM about misbehaving user the NM identifies

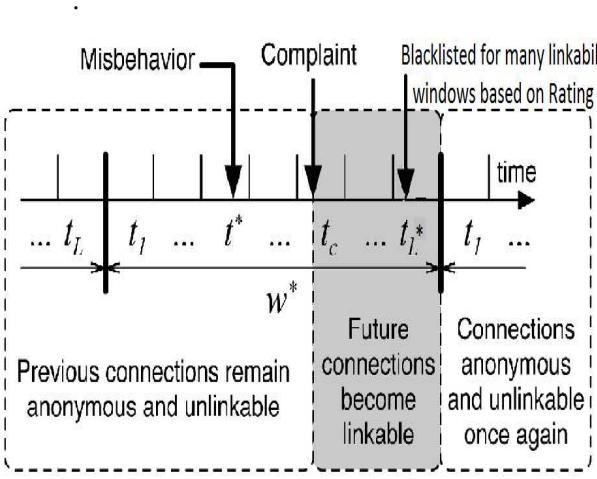

Fig 2: The life cycle of a misbehaving user. If the server complains in time period tc about a user's connection in t*, the user becomes linkable starting in tc. The user is blacklisted to many linkability windows based on rating.

Pseudonym of particular nymble 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 tc;(t*< tc<=tL*); tL* can be linkability window w* Or many linkability windows. Therefore, once the server has complained about a user, that user is blacklisted for the rest of the day, or many days depending on rating. For example (the linkability window).Note that the user's connections in t1; t2; . . . ; t*; t*+ 1; . . . ; tc 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.

2.7 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 user's 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 tnow"). 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.

2.8 Summary of Updates to the Extended Nymble Protocol

In extended Nymble we have eliminated repetitive misbehaviour of users. We have chosen pseudo tracker as a model which maintains rating of the users and this rating is used to track the misbehaving user anonymously. NM doesn't get the details of the user and PM doesn't get the details of the server with which the user misbehaved, we preserve the anonymity and all properties followed with nymble. Pseudo tracker maintains the rating by which NM can simply track users without user details.

Previously, we had proved only the privacy properties associated with nymbles as part of a two-tiered hash chain. Here, we prove security at the protocol level. This process gave us insights into possible (subtle) attacks against privacy, leading us to redesign our protocols and refine our definitions of privacy. For example, users are now either legitimate or illegitimate, and are anonymous within these sets. This redefinition affects how a user establishes a "Nymble connection" and now prevents the server from distinguishing between users who have already connected in the same time

period and those who are blacklisted, resulting in larger anonymity sets. A thorough protocol redesign has also resulted in several optimizations. We have eliminated blacklist version numbers and users do not need to repeatedly obtain the current version number from the NM. Instead servers obtain proofs of freshness every time period, and users directly verify the freshness of blacklists upon download. Based on a hashchain approach, the NM issues lightweight daisies to servers as proof of a blacklist's freshness, thus making blacklist updates highly efficient. Also, instead of embedding seeds, on which users must perform computation to verify their blacklist status, the NM now embeds a unique identifier nymble_, which the user can directly recognize. Finally, we have compacted several data structures, especially the servers' blacklists, which are downloaded by users in each connection, and report on the various sizes in detail.

3. SECURITY MODEL

Nymble aims for four security goals.

3.1 Goals and Threats

An entity is honest when its operations abide by the system's specification. An honest entity can be curious: it attempts to infer knowledge from its own information (e.g., its secrets, state, and protocol communications). An honest entity becomes corrupt when it is compromised by an attacker, and hence, reveals its information at the time of compromise, and operates under the attacker's full control, possibly deviating from the specification.

Trackability assures that NM can track misbehaving users without getting the details of the user we can track them anonymously with pseudo tracker .NM can track and blacklist without maintain user information, different nymbles generated for a particular user when connected to different servers..

Blacklistability assures that any honest server can indeed block misbehaving users. Specifically, if an honest server complains about a user that misbehaved in the current linkability window, the complaint will be successful and the user will not be able to "nymble-connect," i.e., establish a Nymble-authenticated connection, to the server

Successfully in subsequent time periods (following the time of complaint) of that linkability window. Rate-limiting assures any honest server that no user can successfully nymble-connect to it more than once within any single time period.
Nonframeability guarantees that any honest user who is legitimate according to an honest server can nymble-connect to that server. This prevents an attacker from framing a legitimate honest user, e.g., by getting the user blacklisted for someone else's misbehavior. This property assumes each user has a single unique identity. When IP addresses are used as the identity, it is possible for a user to "frame" an honest user who later obtains the same IP address.

Nonframeability holds true only against attackers with different identities (IP addresses). A user is legitimate according to a server if she has not been blacklisted by the server, and has not exceeded the rate limit of establishing Nymble connections. Honest servers must be able to differentiate between legitimate and illegitimate users.
Anonymity protects the anonymity of honest users, regardless of their legitimacy according to the (possibly corrupt) server; the server cannot learn any more information beyond whether the user behind (an attempt to make) a nymble connection is legitimate or illegitimate.

3.2 Trust Assumptions

We allow the servers and the users to be corrupt and controlled by an attacker. Not trusting these entities is important because encountering a corrupt server and/or user is a realistic threat. Nymble must still attain its goals under such circumstances. With regard to the PM and NM, Nymble makes several assumptions on who trusts whom to be how for what guarantee. We summarize these trusts assumptions as a matrix, Should a trust assumption becomes invalid, and Nymble will not be able to provide the corresponding guarantee. For example, a corrupt PM or NM can violate Blacklistability by issuing different pseudonyms or credentials to blacklisted users. A dishonest PM (resp., NM) can frame a user by issuing her the pseudonym (resp., credential) of another user who has already been blacklisted. To undermine the Anonymity of a user, a dishonest PM (resp., NM) can first impersonate the user by cloning her pseudonym (resp., credential) and then attempt to authenticate to a server—a successful attempt reveals that the user has already made a connection to the server during the time period. Moreover, by studying the complaint log, a curious NM can deduce that a user has connected more than once if she has been complained about two or more times. As already described in Section 2.3, the user must trust that at least the NM or PM is honest to keep the user and server identity pair private.

4. DISCUSSION

Users of anonymizing networks would be reluctant to use resources that directly reveal their identity (e.g., passports or a national PKI). Email addresses could provide more privacy, but provide weak blacklistability guarantees because users can easily create new email addresses. Other possible resources include client puzzles and e-cash, where users are required to

perform a certain amount of computation or pay money to acquire a credential. These approaches would limit the number of credentials obtained by a single individual by raising the cost of acquiring credentials.

As described, our system support varying linkability window anonymously. PM is not aware of the server the user wishes to connect to, yet it must issue pseudonyms specific to a linkability window. We do note that the use of resources such as client puzzles or e-cash would eliminate the need for a PM, and users could obtain Nymbles directly from the NM. In that case, server-specific linkability windows could be used.
Side-channel attacks. While our current implementation does not fully protect against side-channel attacks, we mitigate the risks.

CONCLUSION

We have proposed a comprehensive credential system called Extended Nymble, which can be used to add a layer of accountability to any publicly known anonymizing network. Servers can blacklist misbehaving users while maintaining their privacy, and we show how these properties can be attained in a way that is practical, efficient, and sensitive to the needs of both users and services. We suggested a method to track misbehaving users and blacklist them depending on rating. We hope that our work will increase the mainstream acceptance of anonymizing networks such as Tor, which has, thus far, been completely blocked by several services because of users who abuse their anonymity.

REFERENCES

[1] Patrick P. Tsang, Apu Kapadia, Member, IEEE, Cory Cornelius, and Sean W. Smith "Nymble: Blocking Misbehaving Users in Anonymizing Networks" IEEE transactions on dependable and secure computing, vol. 8, no. 2, march-April 2011.
[2] G. Ateniese, D.X.Song, and G. Tsudik, "Quasi-Efficient Revocation in Group Signatures," Proc. Conf. Financial Cryptography, Springer, pp. 183-197, 2002.
[3] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," Proc. Ann. Int'l Cryptology Conf.(CRYPTO), Springer, pp. 1-15, 1996.
[4] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption," Proc. Ann. Symp. Foundations in Computer Science (FOCS), pp. 394-403, 1997.
[5] M. Bellare and P. Rogaway, "Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols," Proc. First ACM Conf. Computer and Comm. Security, pp. 62-73, 1993.
[6] M. Bellare, H. Shi, and C. Zhang, "Foundations of Group Signatures: The Case of Dynamic Groups," Proc. Cryptographer's Track at RSA Conf. (CT-RSA), Springer, pp. 136-153, 2005.
[7] D. Boneh and H. Shacham, "Group Signatures with Verifier- Local Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 168-177, 2004.
[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 and J. Stern, "Efficient Revocation in Group Signatures," Proc. Conf. Public Key Cryptography, Springer, pp. 190-206,2001.
[10] J. Camenisch and 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 and 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 and 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 and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.
[16] C. Cornelius, A. Kapadia, P.P. Tsang, and S.W. Smith, "Nymble:Blocking Misbehaving Users in Anonymizing Networks," Technical Report TR2008-637, Dartmouth College, Computer Science, Dec. 2008.
[17] I. Damga°rd, "Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 328-335, 1988.
[18] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second- Generation Onion Router," Proc. Usenix Security Symp., pp. 303- 320, Aug. 2004.
[19] J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop on Peer-to-Peer Systems (IPTPS), Springer, pp. 251-260, 2002.
[20] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Schemes," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 26