# A new Direction for Research on Data Origin Authentication in Group Communication

Robert Annessi, Tanja Zseby, and Joachim Fabini

Institute of Telecommunications, TU Wien, Vienna, Austria,
{robert.annessi, tanja.zseby, joachim.fabini}@tuwien.ac.at

**Abstract.** Group communication facilitates efficient data transmission to numerous receivers by reducing data replication efforts both at the sender and in the network. Group communication is used in today's communication networks in many ways, such as broadcasting in cellular networks, IP multicast on the network layer, or as application layer multicast. Despite many efforts in providing data origin authentication for specific application areas in group communication, no efficient and secure all-purpose solution has been proposed so far.
In this paper, we analyze data origin authentication schemes from 25 years of research. We distinguish three general approaches to address the challenge and assign six conceptually different classes to these three approaches. We show that each class comprises trade-offs from a specific point of view that prevent the class from being generally applicable to group communication. We then propose to add a new class of schemes based on recent high-performance digital signatures. We argue that the high-speed signing approach is secure, resource efficient, and can be applied with acceptable communication overhead. This new class therefore provides a solution that is generally applicable and should be the foundation of future research on data origin authentication for group communication.

## 1 Introduction

Group communication is ubiquitous in today's communication networks. It facilitates transparent and efficient data transmission to numerous receivers by minimizing data replication efforts both at the sender and in the network. In this paper, we use the term group communication for any one-to-many communication such as multicast, broadcast, or point-to-multipoint communication. Group communication is a generic concept and can be implemented on different layers: data link (Ethernet, Asynchronous Transfer Mode (ATM), or Infiniband), network (IPv4, IPv6) and application layer using overlay networks). It is used in content broadcasting, video conferencing, information distribution (stock-market, software updates, etc.) and Massively Multiplayer Online Games (MMOGs). It is applied in Content Delivery Networks (CDNs), Peer to Peer (P2P), cellular and wireless sensor networks. In this way, the high-speed signing class proposed in this paper is applicable to a huge number of use cases as it is not tied to specific communication networks technologies, network topologies, or applications. While this work focuses on one-to-many communication, the high-speed signing class may be also applied to many-to-many communication settings as long as each sender uses its own signature or the signing key is shared among senders.

Group communication comprises various challenges, many of which stem from its unidirectional nature and dynamic group membership. Some challenges can be solved easier on higher layers, such as guaranteeing reliable delivery of packets. Other issues tend to reoccur, such as efficient and secure authentication of the sender, no matter on which layer group communication functionality is implemented. This reoccurring, fundamental problem in group communication – the authentication of the sender – is called data origin authentication[1]. Despite more than 25 years of research on data origin authentication for group communication, during which various ideas have been proposed, no sufficiently efficient and secure scheme as yet exists that could be deployed generally on a large scale. For this reason, application-specific solutions are developed that may employ sub-optimal or even insecure data origin authentication schemes.

In this position paper, we argue that the most promising research path for securing group communication is to design faster authentication schemes. Furthermore, we show that high-performance signature schemes significantly elevate the solution space and provide a general solution to the authentication challenge in group communication. We are especially concerned that unsuitable data origin authentication schemes may be deployed in future protocols, e.g., in time synchronization protocols [2] or Smart Grid communication [3, 4] and hope that this paper provides valuable details to future protocol designers to guide their decisions and encourages them to use high-speed signatures to solve the authentication challenge in their group communication scenarios.

## 2 Background

Since most communication networks lack strict access control and network nodes may be compromised, cryptographic methods are needed to assure receivers that packets have been indeed sent by a legitimate sender and data has not been modified by unauthorized entities. For group communication, two types of authentication have to be distinguished [5]: group authentication and data origin authentication.

*Group Authentication* assures that data originates from a legitimate but unidentified group member and has not been modified by entities outside the group. Message Authentication Codes (MACs) with a key shared by all group members are a well understood and efficient method for achieving group authentication. However, receivers cannot distinguish between the individual group members because they are all sharing the same key and can therefore generate valid MACs. This is of particular importance in group communication since there are usually many receivers involved, and a single dishonest or compromised receiver is sufficient to impersonate the sender. Besides this security issue, MACs are also rather inefficient in group communication as the shared key needs to be renewed and redistributed every time a receiver leaves or joins the group.

*Data origin authentication* allows receivers to verify that data was indeed sent by a specific sender (non-repudiation). This can be achieved by digital signatures using asymmetric cryptographic, because only the sender is in possession of the secret key required to generate signatures. Table 1 on the facing page summarizes the security prop-

[1] Sometimes still referred to as *source authentication*, a term considered deprecated [1].

erties provided by group authentication and data origin authentication. The main downside of today's digital signature schemes such as RSA [6], DSA [7], and ECDSA [8] is, however, that they come at high computational cost and therefore introduce substantial penalty in terms of delay, both in the sender and in the receiver. Consequently, it is widely believed that digital signatures are roughly 2 to 3 magnitudes slower than MACs [9] so that signing each packet is not a practical solution. We will revise this assumption as we show the potential of recently proposed high-performance digital signature schemes as foundation for data origin authentication in group communication.

**Table 1.** Group Authentication vs. Data Origin Authentication

| **Security Property** | **Group Authentication** | **Data Origin Authentication** |
|---|---|---|
| Integrity | ✓ | ✓ |
| Non-repudiation | ✗ | ✓ |
| Authenticity | Group | Sender |

## 3 Data Origin Authentication Schemes

Data origin authentication schemes for group communication have matured over more than 25 years, and many ideas were proposed to solve this challenging problem. None of the proposed schemes, however, satisfies all constraints and requirements of applications so that naming a single superior scheme seems non-trivial [10]. Challal, Bettahar, and Bouabdallah identified six distinct classes [11] in the sheer number of data origin authentication schemes: deferred signing[2], signature propagation, signature dispersal, secret-information asymmetry, time-based asymmetry, and hybrid asymmetry. In addition to these six classes, we wish to suggest a new class – high-speed signing – where recently proposed high-speed signature schemes are employed.

We identify three conceptional distinct approaches among the proposed data origin authentication schemes. The first approach aims to extend symmetric schemes to data origin authentication. The other two approaches aim to overcome the computational intensive nature of public-key based authentication schemes: reducing the cost of conventional signatures schemes and designing fast authentication schemes. Table 2 on the next page shows the six previously proposed classes as well as our new high-speed signing class assigned to the three approaches we identified.

In this section, we briefly introduce all six classes of data origin authentication schemes and show that each of them comprises a trade-off from a specific point of view. We then argue in Section 4 that our high-speed signing class does not require any of those trade-offs.

[2] Challal, Bettahar, and Bouabdallah originally used the term "*differed signing*" but we think that they actually meant "*deferred signing*" as it makes more sense in this context.

**Table 2.** Approaches to Data Origin Authentication and Classes of Schemes

| Approach | Class |
|---|---|
| Extend symmetric schemes to data origin authentication | Secret-information asymmetry |
| Reduce the cost of conventional signature schemes | Deferred Signing |
| | Signature propagation |
| | Signature dispersal |
| Design fast authentication schemes | Time-based asymmetry |
| | Hybrid asymmetry |
| | High-speed signing |

### 3.1 Extending Symmetric Schemes for Data Origin Authentication

**Secret-Information Asymmetry** With secret-information asymmetry schemes, such as $k$-MAC [12], the sender shares a set of keys with receivers (instead of only one key). The sender knows the entire set of keys and therefore can generate valid authentication information but each receiver's partial view allows just to verify (but not to generate) authentication information. The $k$-MAC scheme uses distinct keys to calculate receiver-specific MACs. Then, all MACs are appended to a packet. Upon reception of this packet, each receiver can verify one MAC it has the key for but cannot create valid authentication information on behalf of the sender as all the other keys are unknown.

The class of secret-information asymmetry schemes entails information-theoretically secure schemes, which means that they do not provide enough information to enable attacks. In this way, these schemes protect against adversaries with potentially unlimited computational power. However, secret-information asymmetry schemes are prone to collusion of receivers, where fraudulent receivers collaborate in order to reconstruct the sender's entire set of keys [11]. Furthermore, secret-information asymmetry schemes require substantial computational resources for signing (and for verification) and also need to distribute new keys individually to each receiver frequently.

### 3.2 Reducing the Cost of Conventional Signature Schemes

**Deferred Signing** With deferred signing, such as offline/online signing [13], the signing process is split into two steps: a slow offline and a fast online step. In the online step, each packet is signed using a one-time signature scheme, which is computationally very efficient. The one-time keys need to be certified to ensure that they originate from the claimed sender. For this purpose, a conventional signature scheme with a certified public key is used in the offline step to sign each one-time key. The generation and signing of the one-time keys is independent of the actual packet to be signed and, therefore, can be conducted offline in advance.

High performance in the online signing part can be achieved because packets are signed with a computationally very efficient one-time signature scheme. The computationally expensive part, precomputing the one-time keys and signing each of them with a conventional signature scheme, is conducted offline. The computational effort

required in the offline part, however, is substantial and the communication overhead is large because of the size of the one-time signatures.

**Signature Propagation** Another approach to reduce the cost of conventional signatures is followed by signature propagation schemes, such as Receiver driven Layered Hash-chaining (RLH) [14]. Instead of signing each packet individually, a signature from a conventional signature scheme is appended to one packet only, the signature packet. Hashes of non-signature packets are included in preceding packets such that a chain of packets is built in which each packet carries the hash of the subsequent packet. In this way, the digital signature propagates through all packets so that the computational cost of its generation is amortized as hash operations are computationally inexpensive. Signature propagation schemes, however, require packets to be buffered at the sender or at the receiver before they can be signed and their signature be verified, respectively. Such buffering introduces additional delay that may be intolerable to specific applications, such as real-time applications. Receiver-side buffering additionally increases the risk for Denial of Service (DoS) attacks as buffers may be filled with bogus packets by an attacker with access to the network. Furthermore, signature propagation schemes rely on the successful reception of signature packets and are, therefore, hardly resistant to packet loss.

**Signature Dispersal** The basic idea behind signature dispersal schemes, such as [15], is that packets are divided into fixed-size blocks, and each block is signed independently with a digital signature. The signature of a block is split, and each part of the signature is appended to one packet (from the same block). Also, additional information is appended to each packet, which helps receivers to reconstruct the signature even if some packets were lost. In this way, signature dispersal schemes improve packet loss resistance compared to signature propagation schemes that entirely rely on the reception of signature packets. Computational efficiency is reduced, however, and receivers need to wait for the whole block before they can verify its authenticity.

### 3.3 Designing Faster Authentication Schemes

Compared to reducing the computational cost of digital signature schemes, a conceptional distinct approach is designing fast authentication schemes. We distinguish three different classes that follow the approach of designing faster authentication schemes: time-based asymmetry, hybrid asymmetry, and the high-speed signing class we wish to suggest.

**Time-based Asymmetry** In time-based asymmetry schemes, such as Timed Efficient Stream Loss-tolerant Authentication (TESLA) [16, 17], key asymmetry is achieved through a common notion of time. In TESLA, the secret and the public key are identical - they are only separated through time. While the key is secret, it is used to sign messages. Meanwhile, clients buffer messages and can verify their authenticity after the (secret) key has been disclosed and therefore becomes public. Once the key is disclosed, the sender has to switch to another key to sign new messages. A common notion

of time guarantees that a key is known by clients only after it is not used anymore for signing messages. The keys are associated by a one-way chain such that only the initial key needs to be signed with a (certified) key from a conventional signature scheme.

Computational efficiency is achieved by basically employing symmetric keys (and introducing asymmetry through time). Also, packet loss resistance is provided as packets are signed independently from each other and receivers can recover from having lost keys due to the one-way chain. However, at some point the last key from the chain is used, and new keys need to be generated and distributed securely. Such secure out-of-band channel for key distribution may not be available to all applications. Furthermore, the clocks of the sender and of receivers are assumed to be strictly synchronized such that the accuracy of time synchronization becomes a security requirement. In case the assumed time synchronization accuracy does not hold, the security of the authentication scheme breaks entirely, which is a severe drawback for those applications that cannot guarantee accurately synchronized clocks.

**Hybrid Asymmetry** The aim of schemes in the hybrid asymmetry class, such as Time Valid Hash to Obtain Random Subsets (TV-HORS) [18], is to combine the strengths of secret-information asymmetry schemes (immediate signing and verification) and time-based asymmetry schemes (computational efficiency) while mitigating their limitations (no resistance to collusion attacks and strict dependency on time synchronization). Hybrid asymmetry schemes are computationally efficient, but they introduce additional communication overhead and still depend on loose time synchronization between sender and receivers. Like in time-based asymmetry schemes, the keys used in hybrid asymmetry schemes can only sign a fixed number of packets. Once this limit is reached, a new key has to be generated and distributed securely in order to sign more packets. Again, such secure out-of-band channel may not be available to all applications.

## 4 High-Speed Signing

Two classes of data origin authentication schemes, time-based asymmetry and hybrid asymmetry, already go into – what we consider to be – the right direction as they do not aim to reduce the computational cost of conventional signature schemes but aim to design fast authentication schemes in the first place. An implicit assumption from schemes in those classes is that digital signature schemes are computationally too expensive by nature. This assumption, however, only holds for conventional but not for novel high-performance signature schemes. For this reason, we argue to sign every single packet independently despite the common assumption that such approach is impractical due to the computationally expensive nature of (conventional) signature schemes. Employing high-performance signature schemes can mitigate the negative performance impact of conventional schemes.

For this purpose, signature schemes that offer previously unrivaled performance are needed such as Ed25519 [19], an elliptic-curve signature scheme *"carefully engineered at several levels of design and implementation to achieve very high speed without compromising security"* [19], or MQQ-SIG [20] a signature scheme based on

multivariate-quadratic (MQ) quasigroups. Both schemes are designed to provide extremely fast signing and verification operations. Since many MQ signature schemes have been broken (including MQQ-SIG [21]) and some of them have been fixed and broken again, it is safe to say that MQ schemes involve serious security challenges. For this reason, we do not recommend to use MQQ-SIG specifically in practice. Nevertheless, we include MQQ-SIG in our evaluation since MQ schemes have very attractive properties (specifically post-quantum security and high-performance), and MQQ-SIG is one of the fastest of MQ signature schemes. Furthermore, we hope that highlighting group communication use-cases spurs future research on MQ schemes even more.

**Performance Measurement** In a small experiment, we measured the speed of these high-performance signature schemes on Commercial Off-The-Shelf (COTS) hardware, an Intel Celeron CPU clocked at $2.26\ \mathrm{GHz}$ running Debian Linux 8 32-bit. We disabled Intel's Hyper-threading and Turbo Boost, CPU-frequency scaling, and CPU-sleep states to not interfere with the measurement. Ed25519 signed and verified about $13\mathrm{k}$ packets per second and has a communication overhead of $64\ \mathrm{B}$ per packet. MQQ-SIG signed and verified over $36\mathrm{k}$ packets per second with a communication overhead of $32\ \mathrm{B}$ per packet. In this way, high-speed signing outperforms[3] TV-HORS from the hybrid asymmetry class, which can sign and verify only $5\mathrm{k}$ packets per second with a communication overhead of $106\ \mathrm{B}$ per packet according to [4]. Table 3 summarizes the measurement results.

**Table 3.** Measurement Results

| Scheme | Signing and Verification | Overhead |
|---|---|---|
| Ed25519 | 13k packets / s | 64 B / packet |
| MQQ-SIG | 36k packets / s | 32 B / packet |
| TV-HORS [4] | 5k packets / s | 106 B / packet |

Because of this high computational efficiency and low communication overhead, there is no need to trade-off other properties like in all the other classes of data origin authentication schemes. High-speed signing provides immediate signing and verification as neither the sender nor the receivers need to buffer packets. It provides collusion resistance since every receiver has identical information, the sender's public key. Authentication schemes can obviously not be completely independent of time synchronization since the validity of the sender's public key needs to be verified. However, while the other classes that follow the same approach (of designing fast authentication schemes) depend on the time synchronization's accuracy in the order of seconds to minutes, the high-speed signing class' dependency is in the order of months to years and therefore practically as independent as possible. Furthermore, high-speed signing provides resistance to packet loss as each packet carries independent authentication information. Table 4 on the next page provides a summary of the classes of data origin authentication schemes.

[3] Admittedly, the measurements were not conducted under the exact same conditions.

**Table 4.** Summary of Data Origin Authentication Classes

| Class | Computational efficiency | Low communication overhead | Immediate signing and verification | Collusion resistance | Resistance against packet loss | Independence of time synchronization | Only initial key distribution | Information-theoretical security |
|---|---|---|---|---|---|---|---|---|
| Secret-Information Asymmetry | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ |
| Deferred Signing | ~ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Signature Propagation | ✓ | ~ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ |
| Signature Dispersal | ~ | ~ | ✗ | ✓ | ~ | ✓ | ✓ | ✗ |
| Time-Based Asymmetry | ✓ | ✓ | ~ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Hybrid Asymmetry | ✓ | ~ | ✓ | ✓ | ✓ | ~ | ✗ | ✗ |
| High-Speed Signing | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |

Property is either satisfied (✓), somewhat satisfied (~), or unsatisfied (✗).

## 5 Discussion

As highlighted in this paper, each previously existing class of data origin authentication schemes comprises a trade-off from a specific point of view. Secret-asymmetry schemes trade-off information-theoretical security against collusion resistance, which means that they protect against adversaries with unlimited computational resources but are prone to fraudulent receivers who collaborate in order to impersonate the sender. Deferred signing schemes trade-off online computational resources against communication overhead and offline computational resources. Signature propagation schemes trade-off computational efficiency and communication overhead against packet loss resistance as they rely on the successful reception of signature packets - from the moment a signature packet is missing the receiver cannot authenticate any more packets. Signature dispersal schemes trade-off packet loss resistance against computational efficiency and immediate signing and verification such that the sender and the receivers need to wait before they can sign and verify packets, respectively, which is a drawback to applications with real-time requirements. Time-based asymmetry schemes trade-off computational efficiency and communication overhead against independency of time synchronization and require a secure out-of-band channel for key distribution. Hybrid asymmetry schemes trade-off computational efficiency against a secure out-of-band channel for key distribution as well (and, by a smaller degree, also against independency of time synchronization). The high-speed signing class, on the other hand, provides all desired properties (except information-theoretical security) without having to trade-off one against the other.

## 6 Conclusion

In this position paper, we tackled a fundamental challenge in secure group communication – data origin authentication. We identified three basic approaches to data origin authentication: extending symmetric schemes to data origin authentication, reducing the cost of conventional digital signature schemes, and designing fast authentication schemes. For every approach, we investigated the associated classes of data origin authentication schemes and showed that schemes from each class comprise a trade-off from a specific point of view.

We introduced a new class of data origin authentication schemes, high-speed signing, that follows the approach of designing fast authentication schemes. This high-speed signing class employs a simple yet new approach to data origin authentication for group communication – signing every packet independently with a high-performance digital signature scheme. Signing every packet is commonly assumed to be impractical due to the high computational cost of conventional digital signature schemes. We revised this assumption, however, as we showed that recently proposed high-performance digital signature schemes are perfectly suitable as foundation to data origin authentication as they achieve computational efficiency, low communication overhead, as well as all other desired properties (besides information-theoretical security).

We hope that this position paper helps to avoid employing unsuitable data origin authentication schemes in various fields in the future such as in time synchronization [2], where a time-based asymmetry scheme is currently proposed in standardization, or in Smart Grids [3, 4], where a hybrid-asymmetry scheme and reducing the computational cost of a conventional digital signature scheme have been proposed just recently. Concluding, we argue that designing fast authentication schemes for group communication is generally the right direction but research should focus on high-speed digital signature schemes instead of other classes in order to solve the problem of data origin authentication for secure group communication.

## References


[1] R. Shirey. *Internet Security Glossary, Version 2*. RFC 4949 (Informational). Internet Engineering Task Force, Aug. 2007. URL: http://www.ietf.org/rfc/rfc4949.txt.

[2] Dieter Sibold, Stephen Roettger, and Kristof Teichel. *Network Time Security*. Internet-Draft draft-ietf-ntp-network-time-security-15. https://tools.ietf.org/html/draft-ietf-ntp-network-time-security-15. IETF Secretariat, Sept. 2016. (Visited on 08/03/2017).

[3] Yee Wei Law et al. "Comparative Study of Multicast Authentication Schemes with Application to Wide-area Measurement System". In: *ACM SIGSAC Symposium on Information, Computer and Communications Security*. ASIACCS '13. NY, USA: ACM, 2013, pp. 287–298. ISBN: 978-1-4503-1767-2. DOI: 10.1145/2484313.2484349.

[4] Teklemariam Tesfay and Jean-Yves Le Boudec. "Experimental Comparison of Multicast Authentication for Wide Area Monitoring Systems". In: *IEEE Transactions on Smart Grid* (2017). ISSN: 1949-3053, 1949-3061. DOI: 10.1109/TSG.2017.2656067.

[5] Thomas Hardjono and Gene Tsudik. "IP multicast security: Issues and directions". In: *Annales des télécommunications*. Vol. 55. 7-8. Springer. 2000, pp. 324–340.

[6] Ronald L. Rivest, Adi Shamir, and Len Adleman. “A method for obtaining digital signatures and public-key cryptosystems”. In: *Communications of the ACM* 21.2 (1978), pp. 120–126.

[7] Taher ElGamal. “A public key cryptosystem and a signature scheme based on discrete logarithms”. In: *Advances in cryptology*. Springer. 1985, pp. 10–18.

[8] Don Johnson, Alfred Menezes, and Scott Vanstone. “The elliptic curve digital signature algorithm (ECDSA)”. In: *International Journal of Information Security* 1.1 (2001), pp. 36–63.

[9] Jonathan Katz. *Digital Signatures*. Boston, MA: Springer US, 2010. ISBN: 978-0-387-27711-0 978-0-387-27712-7.

[10] Rainer Steinwandt and Viktória I. Villányi. “A One-time Signature Using Run-length Encoding”. In: *Information Processing Letters* 108.4 (Oct. 2008), pp. 179–185. ISSN: 0020-0190. DOI: 10.1016/j.ipl.2008.05.004.

[11] Y. Challal, H. Bettahar, and A. Bouabdallah. “A taxonomy of multicast data origin authentication: Issues and solutions”. In: *IEEE Communications Surveys Tutorials* 6.3 (2004), pp. 34–57. ISSN: 1553-877X. DOI: 10.1109/COMST.2004.5342292.

[12] R. Canetti et al. “Multicast Security: A Taxonomy and Some Efficient Constructions”. In: Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM ’99. Vol. 2. Mar. 1999, pp. 708–716. DOI: 10.1109/INFCOM.1999.751457.

[13] Shimon Even, Oded Goldreich, and Silvio Micali. “On-line/off-line digital signatures”. In: *Journal of Cryptology* 9.1 (1996), pp. 35–67.

[14] Yacine Challal, Abdelmadjid Bouabdallah, and Yoann Hinard. “RLH: receiver driven layered hash-chaining for multicast data origin authentication”. In: *Computer Communications* 28.7 (2005), pp. 726–740.

[15] C. Tartary, Huaxiong Wang, and San Ling. “Authentication of Digital Streams”. In: *IEEE Transactions on Information Theory* 57.9 (Sept. 2011), pp. 6285–6303. ISSN: 0018-9448. DOI: 10.1109/TIT.2011.2161960.

[16] Adrian Perrig et al. “Efficient authentication and signing of multicast streams over lossy channels”. In: *IEEE Symposium on Security and Privacy (S&P)*. 2000, pp. 56–73.

[17] A. Perrig et al. *Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction*. RFC 4082 (Informational). Internet Engineering Task Force, June 2005. URL: http://www.ietf.org/rfc/rfc4082.txt.

[18] Qiyan Wang et al. “Time Valid One-Time Signature for Time-Critical Multicast Data Authentication”. In: *IEEE INFOCOM 2009*. Apr. 2009, pp. 1233–1241. DOI: 10.1109/INFCOM.2009.5062037.

[19] Daniel J. Bernstein et al. “High-speed high-security signatures”. In: *Journal of Cryptographic Engineering* 2.2 (2012), pp. 77–89.

[20] Danilo Gligoroski et al. “MQQ-SIG”. In: *Trusted Systems*. Springer, 2011, pp. 184–203.

[21] Jean-Charles Faugere et al. “A polynomial-time key-recovery attack on MQQ cryptosystems”. In: *IACR International Workshop on Public Key Cryptography*. Springer, 2015, pp. 150–174.