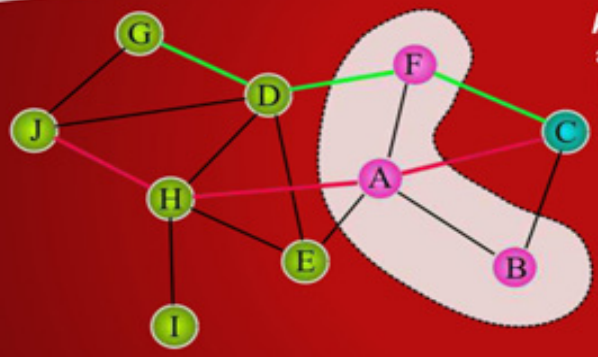
MELE GASAKIS & MAX SCHMIDT

BEYOND CRYPTOGRAPHIC ROUTING: THE ECHO PROTOCOL IN THE NEW ERA OF EXPONENTIAL ENCRYPTION

EEE



A comprehensive essay about the Sprinkling Effect of Cryptographic Echo Discovery (SECRED) and further innovations in cryptography around the Echo Applications Smoke, SmokeStack, Spot-On, Lettera and GoldBug Crypto Chat Messenger addressing Encryption, Graph-Theory, Routing and the change from Mix-Networks like Tor or I2P to Peer-to-Peer-Flooding-Networks like the Echo respective to Friend-to-Friend Trust-Networks like they are built over the POPTASTIC protocol.

A comprehensive essay
about the Sprinkling Effect of Cryptographic Echo Discovery (SECRED) and further innovations in cryptography around the Echo Applications Smoke, SmokeStack, Spot-On, Lettera and GoldBug Crypto Chat Messenger addressing Encryption, Graph-Theory, Routing and the change from Mix-Networks like Tor or I2P to Peer-to-Peer-Flooding-Networks like the Echo respective to Friend-to-Friend Trust-Networks like they are built over the POPTASTIC protocol.

Mele Gasakis & Max Schmidt

Structure

1 Introduction and summary: From Mixing to Flooding – Anonymous networks in the Spot

What was once thought, can not be withdrawn.
Friedrich Dürrenmatt, The Physicists.

After several years of development since 2011, the innovative models and processes of the Echo Protocol and the associated applications, such as the software program Spot-On, the original Client for the Echo Protocol, have been established by numerous releases.

We want to summarize these ideas and results of the individual protocols and projects as well as the existing analysis publications in an overview.

Thus the new perspectives - which lie far beyond 'cryptographic routing' - can be shown within cryptology and mathematics, network theory, graph theory and practical application design with Java, C ++ and the Qt framework.

The Echo Protocol has not only created innovative encryption and networking options as well as processes, functions and models, but these have also been extremely elaborately "brought to the road" and are materialized and put into concrete application programming for various software projects under a free and open source license.

The Echo Protocol is currently used for essential main functions of the Internet: for encrypted personal chat, for group chat forums, for secure E-Mails as well as for data transfers and even for a peer-to-peer (p2p) URL Web search.

This also distinguishes the Echo Protocol from other model concepts, which are described only on paper, which - especially after the first presentation of the Echo Protocol - took numerous references based on this innovation and could thus be called the 'Echo of the Echo' - as already described in a consolidated form by Adams/Mayer (2016:54), and is also deepened further below:

The Echo Protocol is already applied in practice in comparison to other thought models in numerous software applications and functions.

Thus, for example,

- the concept of calling in cryptography ('Cryptographic Calling') relates to the Echo Protocol as well as, which means to provide quickly an end-to-end encrypted channel,
- the specific structure of an Echo network, which can be found in other models as an emulation of the flooding character of the Echo Protocol: data packets are forwarded in the network without any purpose to any existing connection.
- The important feature of the Echo Protocol, the hybrid multi-encryption of the message and/or data packets, and their decoding processes will be discussed in more detail later also.

Firstly, we want to clarify the classification of the terms 'routing' and 'forwarding' in relation to the 'graph'- and 'network theory', and then refer to the innovations of the Echo Protocol which are beyond cryptographic routing.

It is, therefore, not to speak of "routing" in the Echo, but of "discovery" - as it is in the case of "Cryptographic Echo Discovery" (CRED), which will be explained in more detail below with the SE-CRED protocol within the Echo. This protocol represents a core element of the Echo for the development of encrypted messaging on mobile terminals (e.g. as utilized within the Android Java Messenger 'Smoke').

Then, these new directions, innovations, and developed functions are explained based on the Echo Protocol as described, e.g. for the functions E-Mail and chat in the area of messaging, in the area of URL storage and Web search as well as for file sharing and file (and website) hosting in the sense of the perspective of the establishment of a public, digital library.

As already mentioned, these functions are not only a theoretical model, but are continuously being programmed in several different software projects and applications that use the Echo Protocol. The best known are "Spot-On Communication Suite", the "GoldBug Messenger" as well as the mobile application "Smoke” and the E-Mail Client "Lettera".

In addition to the "Adaptive Echo (AE)", which allows specific nodes in the network to be excluded from receiving messages by a cryptographic token, as well as the "POPTASTIC protocol", which process chat and encryption via the email protocols IMAPS & POP3 - this document explains the complementary concept of "cryptographic Echo discovery".

The so-called "sprinkling effect" in the "cryptographic Echo discovery" is a specific design of an innovative information transfer, which in particular on mobile terminals can replace

processes of a distributed hash table (DHT) and identifies the recipient of a message using cryptographic processes.

The recipient information of a message packet is controlled by learning server nodes.

Together, the "sprinkling effect" (SE) in "Cryptographic Echo Discovery" (CRED) yields the acronym: SECRED, which gives the discovery protocol the name in regard as a complement to the Echo Protocol, respective as a complimentary function in the Echo network.

Then, in a further contextual outlook around the new “Era of the Exponential Encryption", the current developments within cryptography with their disruptions and value drivers are summarized in this term:

At numerous recent innovations and also requirements within cryptography one can speak of disruptive and innovative developments - leading to the "Era of Exponential Encryption".

We would therefore like to take readers on an analytical journey to determine what the criteria of the age of linear type of thinking are in an application of (or development process for) encryption versus the new Era of Exponential Encryption.

References to examples from the Echo Protocol supplement and refer to the described developments towards the age of Exponential Encryption. Numerous innovations and disruptions as well as four dimensions or arms characterize the "Era of Exponential Encryption" (in short: EEE).

In a technical outlook it is then about discussing or to consolidate the thesis, that the Echo Protocol, especially with respect to Quantum Computing and the RSA algorithm,

which has been officially stated as broken by the NIST Institute since 2016, can provide hardening and new perspectives.

Next to the specific hybrid multi-encryption and other innovative cryptographic processes, the Echo Protocol also offers its Clients more Quantum Computing-resistant algorithms such as NTRU and McEliece.

In addition, the Echo Protocol and its inherent flooding character also provide security when it comes to analyzing metadata: "The Echo is the true 'noise' of the 'matrix' ", as Adams/Maier (op. cit.) summarize. Mix networks are transforming into flooding networks.

This change in mathematical, technological and network-oriented cryptography towards an age of Exponential Encryption also influences security-oriented, development-related, social, economic and other contexts and requires further educational recommendations.

However, before we look at the aspect of encryption in the Echo, we first want to describe, why the Echo is or has not routing!

2 Routing- & Graph-Theory

In telecommunications, routing describes the definition of paths for message streams during message transmission in computer networks.

Routing is the basis of today's Internet - without routing the Internet would not exist, and all networks would be autonomous. The data packets can pass many different intermediate networks on their way to their destination. On the Internet, the routing (usually) is performed on the IP layer.

In particular, in packet-switched data networks, routing and forwarding are to be distinguished between the two different processes: routing determines the entire path of a message stream through the network. The forwarding, on the other hand, describes the decision process of a single network node, via which of its neighbors it is to forward a present message - if the data packet is not sent to every available neighbor connection in the same way as in the Echo Protocol.

In the case of routing, the view of the graph theory can also be included: Graph theory, originally a subset of mathematics, examines the properties of graphs and their relationships to each other. This is analyzed in detail in network theory.

The fact that many algorithmic problems can be traced back to graphs and, on the other hand, the solutions of graph-

theoretical problems are often based on algorithms, the theory of graphs is of great importance in computer science.

It is also found here, in particular, in the subfield of complexity theory, which deals with the complexity of algorithmically-analyzable and treatable phenomena on various formal computer and network models.

The complexity is then usually measured in resource consumption, such as computation time or storage space requirements, or even more specific measures such as the size of the network or the number of steps required.

The term 'graph' was first used in 1878 by the mathematician James Joseph Sylvester (op. cit.). Arthur Cayley (1874, op. cit.) is another founder of early graph theory. The first textbook on graph theory then appeared in 1936 by Dénes Koenig (op. cit.).

An important application of the algorithmic graph theory is thus the search for a shortest route between two locations in a road or airport network. Such problems can be modeled with the graph theory.

Since routers can only determine the best, that means shortest or fastest routes in relation to the number of packets to be moved, they will note the best possible, in some cases also further routes to specific networks and nodes, and the associated routing metrics (i.e., an evaluation scale of the path) in one or more routing tables.

The best way is often the shortest way; it can be found, for example, with the algorithm of Dijkstra (1959).

Routing and forwarding are, however, frequently intermingled with the term "routing"; in this case, routing

generally refers to the transmission of messages via message networks.

In packet-switched routing it is ensured that logically addressed data packets emerge from the originating network and are forwarded to their destination network.

Hubs and switches forward data only in the local network, while a router also knows neighboring networks.

Based on the entries in the routing table (s) (also called routing information base), a router calculates a so-called forwarding table; it contains entries of the form “target address pattern” → “output interface”. In its forwarding table, a router then checks for which interface it has to route the packet for each newly arrived packet.

Below we will also see the field of encryption in the Echo Protocol, that every packet with all the keys present in the node is also tested here. In this respect, this work of a kernel is not necessarily more intensive than the search for routing information for each individual packet.

A routing table therefore contains information on possible paths, the 'optimal' path, the status, the metric, and the age of the data. The basis is the linking of the target IP address with a directional indication in the form of the following router and the interface over which the packet stream is to be steered.

In order to be able to fill a routing table with life, entries are necessary with regard to the achievable networks. Routers can learn ways using three different methods, and then use this knowledge to generate the routing table entries:

- **Directly connected networks:** They are automatically transferred to a routing table if an interface is configured with an IP address.

- **Static routes:** These paths are entered by an administrator. On the one hand, they serve security, but on the other hand they are only manageable if their number is limited, that means, scalability is a limiting factor for this method.
- **Dynamic Routes:** In this case, routers can reach accessible networks through a routing protocol that collects and distributes information about the network and its subscribers to the members.

The routing protocols then provide for the exchange of routing information between the networks, allowing the routers to dynamically build their routing tables.

If we have described the Echo Protocol in detail below with its two additions "Adaptive Echo (AE)" and the "SECRED protocol", one can assign a corresponding assignment to the above three routing categories: The Echo Protocol covers the area of connected networks, the Adaptive Echo can be referenced to the concept of static routing and the dynamic routes should be discussed in the area of the SECRED protocol described below.

Thus, the Echo Protocol is to be regarded as complete in the sense of today's differentiations - with only the difference that the Echo Protocol encrypts the packets and - as we shall see - that it cannot be spoken of routing.

Traditional IP routing remains simple because the so-called 'next-hop routing' is used: the router sends the packet to the neighboring router, which it believes is the most convenient to the destination network. The router then needs not to worry about the further way of the package. Even if it was wrong and did not send the packet to the "optimal" neighbor, the package should arrive sooner or later at the destination.

Again, a parallel to the Echo Protocol can be seen, with the difference that the Echo Protocol tries to send the message to each available neighbor (farther). Therefore, it can be spoken of a hop-all paradigm or a flooding character.

Flooding refers to the transmission of data packets to all nodes of a network. In addition to the Echo Protocol, in which information is transmitted to all connected computers using this technique, such a 'hop paradigm' is also used to find a shortest path, as in the case of Open-Shortest-Path-First methods (OSPF) (see RFC 5340):

This is not about the route with the least hops, but the route with the least path costs - a corresponding decision criterion for the advantage of a path (and thus its metric) becomes a nominal data rate.

But also, from the old Usenet, in which the forum articles are distributed by sending the articles to all computers in the Usenet network, a sort of synchronizing redundancy is known as flooding.

Originally both Paul Baran and Donald Davies had the idea to decentralize not only the communication points of a network, but also to divide messages into blocks (according to Davies named as "packets").

For reasons of greater implementation, Donald Davies, as the often-named founder of this partially meshed network topology and packet-switched networks, entered the history of information technology. The term "packets" was used against the concept of "blocks".

With the innovation of the Echo Protocol, the time has now come to first encrypt these packets and secondly no longer to speak of routing - one therefore refers to encryption and

discovery in the Echo Protocol to a paradigm status: Beyond Cryptographic Routing.

3 Beyond Cryptographic Routing: The Echo-Protocol & Cryptographic Discovery

With cryptographic routing, IP addresses are not assumed as a destination, starting point or node for mapping in routing tables, but a cryptographic key and / or token represents a certain "constant" to be taken into account in the process. With that, it is not the term "address" meant because it is not a matter of replacing the IP address with a cryptographic key such as: route instead of the IP address 192.168.1.1 to the cryptographic key: c2J7IKRTVz XSydvewUP2X3xm/FsHDItH2pdTLG6+tyw=.

Instead, in the Echo Protocol the message is sent without classical routing information. There are no tables with graph information. Therefore, it must be spoken of "beyond cryptographic routing".

The Echo Protocol established since 2011 and implemented in the "Spot-On Communication Suite" and "GoldBug Messenger" from the application side since 2013 is a very simple protocol, which essentially comprises at least two characteristics:

1. First, all data packets are encrypted.
2. Secondly, each node sends a data packet to all connected nodes (farther).
3. A third criterion for the Echo Protocol can be added, that there is a special feature when unpacking the encrypted capsule: The capsules have neither a receiver nor sender information included - and here they are different from TCP packets. The message is identified by

the hash of the unencrypted message as to whether the message should be displayed and readable to the recipient in the UI or not. This is the so-called “echo match”, as described further below.

The Echo is a malleable concept. That is, an implementation does not require rigid dictated details. In this regard the malleable concept is a flexible concept.

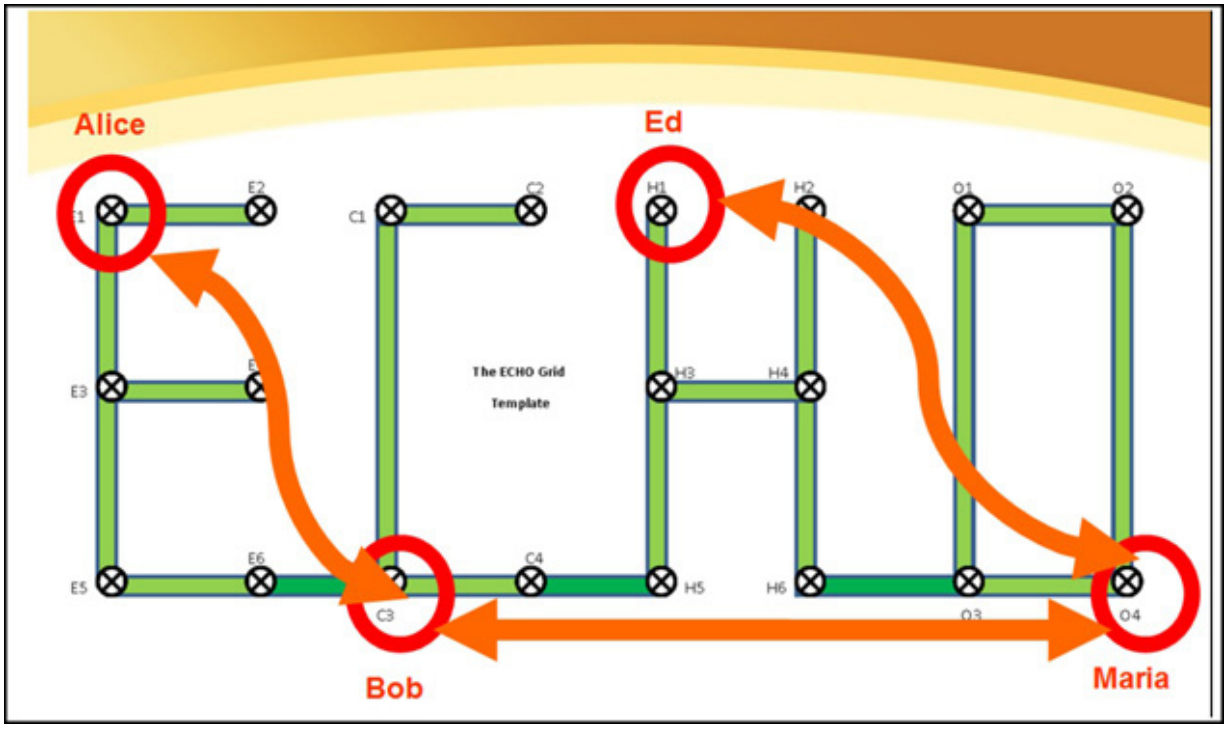
Further malleability refers in cryptography to the conversion of ciphertext to ciphertext. And this is then associated to the Echo-Client’s hybrid and/or multi-encryption. Malleability is for example also a property of some cryptographic algorithms. An encryption algorithm is malleable if it is possible for an analyst to transform a ciphertext into another ciphertext which decrypts to a related plaintext. That is, given an encryption of a plaintext m, it is possible to generate another ciphertext which decrypts to f (m), for a known function f, without necessarily knowing or learning m (comp. Dolev et al. 2000).

Even if the concrete mathematical calculations are not to be emphasized here, it becomes clear that the Echo brings ciphertexts into contact with numerous variants: encrypting ciphertext once again to ciphertext is one option in this process.

Encryption or even multiple encryption is thus a substantial constant of the Echo. Another is the specific sending of the encrypted packet:

Each Echo graph model may adhere to its own peculiar obligations (compare described Echo example graphs by Edwards 2014/2018).

Figure 01: The Echo grid



Source: Edwards, Scott: Manual (2014, update 2018).

The Echo functions on the elementary persuasion, that information is dispersed over multiple or singular passages and channel endpoints evaluate then the suitability of the received data on their own.

The Spot-On.sf.net application materialized at first the Echo-Protocol in concrete coding and development. These Clients of the Echo Protocol like Spot-On support Bluetooth, SCTP, TCP, and UDP (multicast and unicast) communication methods. For TCP-based communications, OpenSSL is supported. Spot-On distributes data with or without SSL/TLS. That means, the transmission of the encrypted data packets is done on the basis e.g. of HTTPS or also only HTTP.

Let's look at both the encryption and the sending of the packet in the Echo even in more detail.

3.1 Encryption in the Echo Protocol

The Echo-Kernel respective the Client Spot-On utilize for Public Key Infrastructure the libgcrypt (RSA / ElGamal) and libntru (NTRU) as well as McEliece libraries for permanent private and public key pairs.

Presently, the application generates twelve key pairs during the initialization process. Key generation is optional. Consequently, Spot-On does not require by force a public key infrastructure.

ElGamal, NTRU, McEliece and RSA encryption algorithms are supported. DSA, ECDSA, EdDSA, ElGamal, and RSA signature algorithms are supported. The OAEP and PSS schemes are used with RSA encryption and RSA signing, respectively.

Communications between nodes having diverse key types are well-defined if the nodes share common libgcrypt and libntru libraries. That means that users with ElGamal keys can communicate to users with RSA keys.

Non-NTRU private keys are evaluated for correctness via the gcry_pk_testkey() function. Public keys must also meet some basic criteria such as including the public-key identifier (fingerprint).

The Clients of the Echo Protocol use Block Cipher Modes of Operation: CBC with CTS to provide confidentiality. The file encryption mechanism supports the GCM algorithm without the authenticity property that's provided by the algorithm. To provide authenticity, the application uses the encrypt-then-MAC (EtM) approach. The “Encrypted and

Authenticated Containers” section in the Spot-On project documentation provides more details (Spot-On 2014ff).

With these prerequisites of established encryption libraries, a multi- or hybrid-encryption is implemented: multi-encryption is here the right term, since the original data is encrypted several times with the Echo Protocol. Hybrid encryption is also the right term because different encryption algorithms and methods can be used as an option: Thus, the data packet may be encrypted for example symmetrically, and then again asymmetrically before sending it through a (self-signed) HTTPS channel with asymmetric and symmetric encryption.

The following figure shows from inside to outside the process of how the encrypted capsule is formed in the Echo Protocol with or on three different levels: