23rd International Symposium on Mathematical Theory of Networks and Systems
Hong Kong University of Science and Technology, Hong Kong, July 16-20, 2018

Decryption failures as side channel attacks

Extended Abstract

Joanne Hall[1] and Margreta Kuijper[2]

Abstract— **Securing information involves multiple layers: mathematical encryption, protocol design, software implementation and hardware implementation. Multiple disciplines are involved, mathematicians, software developers, telecommunication technicians and cybersecurity engineers.**

Mathematical cryptanalysis analyses encrypted information, whereas side channel cryptanalysis analyses information leaked via software/hardware implementation. In this presentation we give an overview of reaction attacks due to protocol-based leaked information. We particularly look at McEliece Cryptosystems, also called Code Based Cryptography, using LDPC codes. The LDPC McEliece crypto system is vulnerable to reaction attacks.

We discuss reaction attacks that use decryption failure events to gather information about the decryption key. We propose to consider such decryption failures as a side channel from which information can be gathered. We conclude that any code-based cryptographic protocol requires careful cybersecurity engineering management of decryption failure events.

Index Terms— **Side channel, reaction attack, McEliece crypto system, LDPC, decoding failure.**
AMS subject classifications (2010): 94A60, 68P30.

I. Introduction and background

There are many aspects of securing information: the mathematical tools of encryption, the message management protocols, the software implementation and the hardware of the system, as illustrated in Figure 1. A security engineer considers all of these aspects in designing a secure communication system.

Mathematical crypt-analysis focusses on the encryption. *Side channel* crypt-analysis is crypt-analysis using information leaked through implementation data [10]. Many side channel attacks are due to hardware implementation data such as timing, power consumption, and magnetic field changes [5]. Other side channel attacks are due to software implementation data such as interference with other files (cache attack), and buffer overflows. A *reaction attack* uses information gleaned due to the reaction of the receiver to a message which failed to decrypt [7]. The reaction of the receiver is dictated by the protocol in which the encryption method is embedded.

Standard cryptography textbooks discuss mathematical attacks on the encryption, software-based side channel attacks, hardware-based side channel attacks [5] and protocol attacks [2]. A protocol attacker actively seeks to fool the protocol into accepting false instructions, leading to information leakage. It is different from a reaction attack which does not involve fooling the protocol.

We propose to consider reaction attacks as a new class of side channel attacks, namely protocol-based side channel attacks. Indeed, if the protocol requires the receiver to request retransmission of failed frames, then this is a side channel through which information can be leaked to the sender. More specifically, in a public key cryptosystem, or public key encapsulation mechanism, an attacker may send many messages and use the profile of failed decryption events to infer information about the private key [6], [4]. A reaction attack is distinct from replay attacks which send the same message multiple times, the McElice cryptosystem is particularly vulnerable to replay attacks [3]. The reaction of the receiver is independent of the plain text and the cipher text, and does not involve fooling the protocol.

[1]School of Science, RMIT University, Melbourne, Australia. joanne.hall@rmit.edu.au
[2]Department of Electrical and Electronic Engineering, University of Melbourne, Australia. mkuijper@unimelb.edu.au

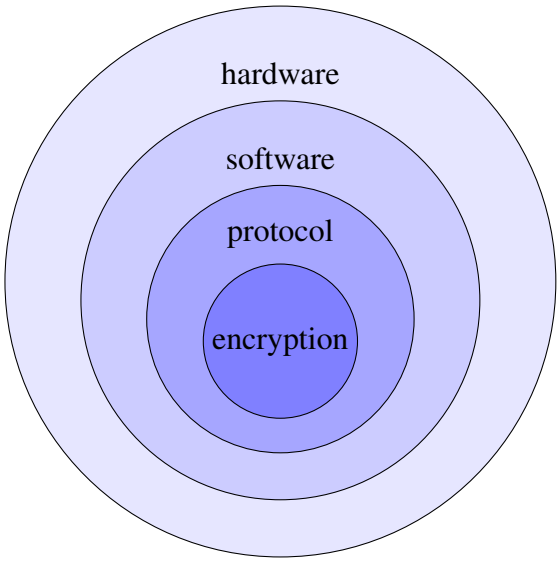

Fig. 1. The layers of a cryptographic implementation

II. Reaction to Decryption Failure as a Side Channel

Whenever information is transmitted over a noisy channel, there is always a small chance that the error control system fails, and a message is received incorrectly. Decryption is a sensitive operation, and hence decryption of incorrectly received messages is often not possible. Any crypto system will have a (small) amount of failed decryptions. With a frame that has failed to decrypt a protocol may perform one of the following actions:

- ask for re-transmission of the frame,
- reconstruct the frame from other decrypted frames,
- leave the frame blank.

In some protocols such as real time voice communication (VOIP), there is no time for retransmission and therefore failed frames are reconstructed from previous frames [17]. If there are only a few failed frames then reconstruction can be done without any human noticeable sound quality reduction. For transmission of data for which higher integrity is needed, a request for retransmission may be required.

Requesting retransmission alerts the sender to the decryption failure. If the pattern of failures is not random, then there is a possibility of information leakage about the decryption key.

There are several security metrics that can be used to analyse the viability of a side channel attack [19]. The *asymptotic success rate* of a side channel attack is the success rate of determining if the private key belongs to a specific class when the number of measurements tends to infinity. In the reaction attack of Fabsic etal [4], The asymptotic success rate of the reaction attack of Fabsic etal is equal to 1.

III. Successful reaction attacks

The McEliece and Niederreiter Cryptosystems, also called Code Based Cryptography is a candidate for a public key cryptosystem which may be resistant to attack by quantum computers [18]. For Code Based cryptosystems with iterative decoding, there will be a small percentage of failed decryptions due to the nature of iterative decoding. McEliece first wrote about the cryptosystem in 1978 [11], which was modified to be resistant to replay attacks by Niederreiter [13]. The Code Based cryptosystems have not yet been deployed in real world applications However quantum computers are coming: several of the recent entries into the NIST Post Quantum Cryptography competition are code based [14].

Whereas McEliece's original paper used Goppa Codes [11], several other code families have since been explored [15]. The use of LDPC codes was proposed as a variant on the McEliece system to reduce the key size [12]. The more recent proposal of Quasi-Cyclic-LDPC codes reduces key sizes even further [1]. One of the advantages of LDPC codes is their efficient iterative decoding algorithms. However it is iterative decoding that is vulnerable to reaction attacks.

A code based cryptosystem uses a code $\mathcal{C}$ with error tolerance t. Let G be a generator matrix and H a parity check matrix for $\mathcal{C}$. Computations are easier if H and G are in systematic form. A public key is constructed by scrambling G to form G', so it is no longer in systematic form. The public key is (G', t), and the private key is H and the scrambling mechanism. For LDPC codes scrambling can be achieved using an invertible binary matrix S, and invertible low density matrix Q so that $G' = SGQ$. The private key is is then (S, Q, H).

In the McEliece cryptosystem the plaintext message vector $\vec{m}$ is encrypted by encoding $\vec{m}$ using

the public key, G', and adding a randomly generated error vector $\vec{e}$ of weight t. The ciphertext is given by

$$\vec{c} = \vec{m}G' + \vec{e}.$$

When the ciphertext is received, it is decrypted by unscrambling, followed by correction of errors using a H with a suitable decoding algorithm. To circumvent the vulnerability to replay attacks we consider the use of the McEliece system in a Key Encapsulation Mechanism, where the message $\vec{m}$ is a randomly generated session key for a symmetric crypto system. The Niederreiter system encodes the message as a syndrome, thus cannot take advantage of fast iterative decoding algorithms [1]. Alas the iterative decoders have biased error patterns that enable successful reaction attacks.

Iterative decoders step through an algorithm and terminate when all conditions are satisfied, or terminate at a chosen max iteration count. If all conditions are satisfied then the message has been decoded correctly. If the max iteration count is reached, then decoding has failed. In a code based system decoder failure is decryption failure. Iterative decoders have an error floor[16], and hence decryption failures occur in a non-random way, allowing for information leakage.

The sender knows the plaintext vector $\vec{m}$, the public key G', and the ciphertext vector $\vec{c} = \vec{m}G' + \vec{e}$. Thus the sender also knows the error vector $\vec{e}$. The sender cannot control $\vec{e}$, but can observe $\vec{e}$. With a protocol that asks for retransmission upon decoding failure, the sender can also observe which error patterns cause decoding failures. Sending a large volume of messages, the sender can become an attacker by building up a profile of the error vectors that cause decoding failure. The profile of error patterns can then be used to infer information about the private key. It does not matter which message is sent, or whether the series of messages have any similarity information is still leaked via decryption failure.

Of the information the sender knows, G', t and the structure of the private key are fixed for all messages, and $\vec{m}$ does not impact on the success or failure of the decoder [8]. It is the relative failure rates of various error patterns that is the side channel through which information can be leaked. If elements of the private key are highly structured such as the check matrix of a Quasi-Cyclic Moderate Density Parity Check (QC-MDPC) code, the key may be completely recoverable [6], [4].

If the error tolerance t is high, then relatively few messages need to be sent to generate sufficient data for a successful key recovery attack. For a proposed '80 bit security' implementation with key size 4801 and error tolerance of 90, only $10,000$ decoding success/failure instances are needed to construct the distance spectrum [6]. In this instantiation approximately 10% of messages failed to decrypt. A 10% failure rate is not practical, but does illustrate that this is a real attack that needs to be considered as a security risk. Reducing the error tolerance to 84, reduced the failure rate to 0.1% and increased the number of decoding success/failure instances required to 100,000 for a successful attack.

IV. Possibilities of reaction to failed decryption side channel

Reaction attacks on the LDPC McEliece systems [6], [4] rely on the observation that an error pattern which contains a distance d will fail less frequently if the distance d is also present in the first row of the private key H. Much investigation into iterative decoding failure has determined that *trapping sets* in H are a major culprit in causing decoding failure [16], [20]. Catalogues of trapping sets for various types of LDPC codes are being compiled [21] making it plausible (though yet to be demonstrated) that the failure pattern could leak information about the nature of the trapping sets in the private key check matrix.

NTRUEncrypt is a lattice based public key cryptosystem and, like the McEliece system, decryption failures are an unavoidable part of the decryption algorithm [9]. Using the decryption failure information, an attacker is able to glean information about the private key.

With any crypto system there is a (small) probability of a failed decryption. The causes of the failures, and the reaction to a failure needs to be analysed for information leakage.

V. Conclusion

The reaction to a decryption failure should be considered as a side channel from which information can be leaked. Any cryptosystem protocol

should consider management of decryption failures to maintain message integrity whilst reducing information leakage. By considering reaction attacks as a class of side-channel attacks, security engineers are more likely to consider this type of attack when designing a communication system.

REFERENCES

[1] Marco Baldi. *QC-LDPC code-based cryptography*. Springer Science & Business, 2014.

[2] Colin Boyd and Anish Mathuria. *Protocols for authentication and key establishment*. Springer Science & Business Media, 2013.

[3] Anne Canteaut and Florent Chabaud. A new algorithm for finding minimum-weight words in a linear code: application to mceliece's cryptosystem and to narrow-sense bch codes of length 511. *IEEE Transactions on Information Theory*, 44(1):367–378, 1998.

[4] Tomáš Fabšič, Viliam Hromada, Paul Stankovski, Pavol Zajac, Qian Guo, and Thomas Johansson. A reaction attack on the QC-LDPC McEliece cryptosystem. In *International Workshop on Post-Quantum Cryptography*, pages 51–68. Springer, 2017.

[5] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno. *Cryptography engineering: design principles and practical applications*. John Wiley & Sons, 2011.

[6] Qian Guo, Thomas Johansson, and Paul Stankovski. A key recovery attack on mdpc with cca security using decoding errors. In *Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I 22*, pages 789–815. Springer, 2016.

[7] Chris Hall, Ian Goldberg, and Bruce Schneier. Reaction attacks against several public-key cryptosystem. In *International Conference on Information and Communications Security*, pages 2–12. Springer, 1999.

[8] S.S. Haykin and M. Moher. *Communication Systems*. Wiley, 2010.

[9] Nick Howgrave-Graham, Phong Q Nguyen, David Pointcheval, John Proos, Joseph H Silverman, Ari Singer, and William Whyte. The impact of decryption failures on the security of ntru encryption. In *CRYPTO*, pages 226–246. Springer, 2003.

[10] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Side channel cryptanalysis of product ciphers. *Journal of Computer Security*, 8(2-3):141–158, 2000.

[11] Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978.

[12] Chris Monico, Joachim Rosenthal, and Amin Shokrollahi. Using low density parity check codes in the McEliece cryptosystem. In *Information Theory, 2000. Proceedings. IEEE International Symposium on*, page 215. IEEE, 2000.

[13] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15:159–166, 1986.

[14] National Institute of Standards and Technology, First PQC Standardization Conference, 2018.

[15] Raphael Overbeck and Nicolas Sendrier. Code-based cryptography. In *Post-quantum cryptography*, pages 95–145. Springer, 2009.

[16] Tom Richardson. Error floors of ldpc codes. In *Proceedings of the annual Allerton conference on communication control and computing*, volume 41, pages 1426–1435. The University; 1998, 2003.

[17] Redwan Salami, Claude Laflamme, Bruno Bessette, and J-P Adoul. Itu-t g. 729 annex a: reduced complexity 8 kb/s cs-acelp codec for digital simultaneous voice and data. *IEEE Communications Magazine*, 35(9):56–63, 1997.

[18] Nicolas Sendrier. Code-based cryptography: State of the art and perspectives. *IEEE Security & Privacy*, 15(4):44–50, 2017.

[19] François-Xavier Standaert, Tal Malkin, and Moti Yung. A unified framework for the analysis of side-channel key recovery attacks. In *Eurocrypt*, volume 5479, pages 443–461. Springer, 2009.

[20] Bane Vasić, Shashi Kiran Chilappagari, and Dung Viet Nguyen. *Failures and Error Floors of Iterative Decoders*, pages 299–341. Elsevier Inc., 6 2014.

[21] Bane Vasić, Shashi Kiran Chilappagari, Dung Viet Nguyen, and Shiva Kumar Planjery. Trapping set ontology. In *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, pages 1–7. IEEE, 2009.