About Nguyen et al.'s vCCA security

Ahmad Charba

December 2023

1 Introduction

The topic of fully homomorphic encryption (FHE) has been of great interest to researchers in the last few years, due to its confidentiality and privacy-preserving properties. This type of encryption can allow any efficiently computable functions to be performed on encrypted data by a third party, without the possibility for that party to see the underlying plain data. This has many potential use cases, such as privacy-preserving machine learning [15], multiparty computation [16], and cloud computing [17].

For a long time, FHE has been an open problem; computation on encrypted data was first recognized in 1978 by Rivest et al. [14] While some crypto systems like Paillers' and RSA were shown to be homomorphic with respect to a limited set of operations, no practical fully homomorphic schemes were discovered for decades. The breakthrough was in 2009, when Gentry proposed the first plausible fully homomorphic encryption scheme, involving the concept of Bootstrapping - a method of btaining a fresh ciphertext from one that had accumulated noise [13].

There are now many FHE schemes, each with their own strengths and weaknesses. However, unlike in classical encryption where non-malleability of cyphertexts is an important property, leading to the use of CCA2 (Adaptive Chosen Ciphertext Attack) security - which implies non-malleability - in proofs, FHE in essence requires malleability. This means that the usual CCA2 security notion is not applicable to FHE, which lean many researcher to fall back to a much weaker notion, CPA (Chosen Plaintext Attack).

This is the problem Nguyen et al. attempt to resolve with their paper, "Fully Homomorphic Encryption beyond IND-CCA1 Security: Integrity through Verifiability." In this paper, which is the central topic of this report, the authors present a stronger security notion, which they call vCCA security (verifiable Chosen Cyphertext Attack). This report will go over previous work on this subject, present Nguyen and numerous findings, provide a critique of their work and highlight some possible ways forward based on their research.

2 Background and Previous Work

2.1 Conventional Security Notions

CPA security, or security against chosen cyphertext attacks, can be seen as follows:

For a given cryptosystem, an adversary has access to an encryption oracle. The adversary can ask this oracle to encrypt any arbitrary plaintext (apart from the challenge). A scheme is CPA secure if such an adversary is unable to reveal any information about the private key.

To prove security against CPA, one can show that if the attack is to pick two arbitrary messages, and receive a challenge cyphertext which is the encryption of one of the messages, then this adversary cannot guess with a probability non-negligibly higher than 1/2 which of the two messages has been encrypted.[12] The Chosen Plaintext Attack is very practical in public key cryptography, since an adversary with the public key can compute the encryption of arbitrary plaintexts.

CCA1 security, or security against nonadaptive chosen ciphertext attack, on the other hand, grants the adversary access to a decryption oracle, making it stronger than CPA security. This oracle decrypts any nonchallenge cyphertexts, but only before the attacker receives the challenge. We can then prove security against this attack by showing that the attacker cannot reveal anything of the challenge given access to this oracle. This notion is applicable to FHE, but it does not appear sufficient: most proposed schemes are not CCA1 secure, and there can be stronger applicable notions.

CCA2 security, or security against adaptive chosen ciphertext attack, is similar to CCA1 but allows the adversary to use the decryption oracle after receiving the challenge. This notion is stronger still than CPA and CCA1 security. It is easy to see that a Homomorphic Encryption (HE) scheme cannot be CCA2 secure, since malleability is in the essence of HE: an attacker could trivially ask the oracle to decrypt $F(challenge)$, where F is a homomorphically computable function in the scheme, obtaining information on the challenge ciphertext.

2.2 Other Proposed Semantic Security Notions for Homomorphic Encryption

Other researchers have previously proposed security notions to bridge the gap between CPA and CCA2 security for HE and FHE.

HCCA (Homomorphic-CCA), proposed in 2008 by Prabhakaran and Rosulek, is a notion which relaxes previous notions like RCCA and gCCA (which themselves are relaxations of CCA2 security)[10]. This notion only malleability under certain operations, limiting the ability of the decryption oracle after receiving the challenge when compared to CCA2. However, this makes it not applicable to general FHE schemes [12]. Similarely, the stronger notions RCCA and gCCA suffer of the same problem in our context.

Akavia et al. proposed in 2021 FuncCPA, a strengthening of CPA which allows the adversary access to a $Encpk(G(Decsk(.)))$ oracle for a family of functions G [9]. However, this notion does not imply CCA1 security, making it relatively weaker than others [12].

Das et al. defined CCA1.5, which stands in between CCA1 and CCA2 by granting the attacker access to the decryption oracle before getting the challenge ciphertext and a verification oracle after getting it. [6]

Recently, Li et al. defined CPA $^{\mathrm{D}}$ security for approximate FHE schemes[7]. Checri et al., as well as Cheon et al. around the same time in 2024, near the publishing of Manulis and Nguyen's paper, showed that this type of attack could also be applied to exact FHE[8][5], which was wrongly believed to not be the case. This was briefly mentioned in Manulis and Nguyen's paper, to which they say that starting with a CPA$^{\mathrm{D}}$ secure scheme before their proposed transformation should be done to protect against this attack when it comes to approximate FHE [12].

2.3 Semantic Security of Existing Fully Homomorphic Encryption Schemes

Fauzi et al. analyzed the security of CCA1 Security of FHE Schemes in 2022 [11]. They showed that many proposed schemes were not CCA1 secure, even though that level of security is not theoretically unfeasible for FHE. These included schemes based on various hardness problems, which they grouped in 5 categories: (R)LWE (Ring Learning With Errors), ideal lattices, AGCD (Approximate Greatest Common Divisor), NTRU (Nth-degree Truncated Polynomial Ring Units), and "other".

3 Contributions

Manulis and Nguyen contributed a number of things to the field in their paper. They proposed a new security notion, security against Verified Chosen Ciphertext Attack (vCCA), which is stronger than CCA1 but applicable to FHE, proved its relations with other notions and proposed a transformation which takes an arbitrary CPA secure FHE scheme and makes it vCCA secure.

3.1 vCCA Security

The authors proposed the notion of vCCA security, and defined it in two different ways: IND-vCCA (indistinguishability against verified chosen ciphertext-attack) and TNM-vCCA (Targeted Non-Maleability against verified chosen ciphertext-attack).

3.1.1 IND-vCCA

IND-vCCA requires the existence of an extraction algorithm which is able, if given as input a ciphertext which is the result of the evaluation of a function

and some auxiliary information, to extract the function and fresh ciphertexts that were used in that evaluation. These fresh ciphertext are then "liked" with the ciphertext which was the output of the evaluation.

A decryption oracle is then defined as an oracle which decrypts any ciphertext except those which are linked by the extraction algorithm to the challenge ciphertext. Similarly to CCA2, the attacker is granted access to this oracle after receiving the challenge, while having access to the standard CCA1 oracle before that happens. He then tries to distinguish which of the messages was encrypted, and a scheme is vCCA secure if the attacker has probability negligeably more than 1/2 to make the right guess.

3.1.2 TNM-vCCA

This alternate definition was based on Beneh et al.'s definitions of Targeted malleability, to which the authors added their modified decryption oracle like in IND-vCCA. [4] The authors then showed that TNM-vCCA and IND-vCCA were equivalent security notions which implied one another.

3.2 Relations to Other Notions

After defining vCCA, Manulis and Nguyen proved relationships between it and other existing notions, such as HCCA, RCCA, FuncCCA and CCA1.5.

In addition to showing that TNM-vCCA and IND-vCCA were equivalent as discussed above, the authors have shown that:

- vCCA implies CCA1.5, but vCCA is not implied by CCA1.5 (vCCA is a stronger notion than CCA1.5)
- vCCA implies FuncCPA, but vCCA is not implied by FuncCPA (vCCA is a stronger notion than FuncCPA)
- vCCA implies HCCA, but vCCA is not implied by HCCA (vCCA is a stronger notion than HCCA)
- RCCA implies vCCA, but RCCA is not implied by vCCA (vCCA is a weaker notion than RCCA)

This put vCCA security in the position of being the strongest security notion achievable by a FHE scheme at that time.

3.3 Construction of a vCCA-Secure FHE scheme

Manulis and Nguyen then proposed transformations to turn any CPA secure scheme into a vCCA secure one for both symmetric and asymmetric schemes, be it for designated verifier or publicly verifiable variants.

This was done by first embedding a FHE scheme in a CCA2 secure scheme, such that the ciphertext can be divided in two parts: a homomorphic part, which has the properties of the underlying FHE scheme, and a "CCA-security" part to which we cannot apply the homomorphic evaluation algorithm.

3.3.1 Embedding in Symmetric Scheme

In the case of symmetric, designated verifier schemes, embedding is done by using the Encrypt-then-MAC paradigm, where a MAC tag is added to the homomorphically encrypted ciphertexts, giving us a CCA2 secure encryption if the underlying FHE scheme is CPA secure and the MAC is SUF-CMA-secure .

For the publicly verifiable variant, the Encrypt-the-Sign paradigm is used in the same way. This gives us a CCA2 secure encryption system if the signature scheme is SUF-CMA-secure and the FHE sceme is CPA secure.

3.3.2 Embedding in asymmetric Scheme

For asymmetric schemes with designated verifier, the principle of double encryption was used instead. The CPA FHE and a CCA2-secure PKE scheme are combined, giving us a CCA2-secure PKE with fully homomorphic embedding.

In the publicly verifiable variant, the Naor-Yung paradigm was used, and the construction was presented for completeness but is not a novel contribution of the paper.

3.3.3 Transformation of a CCA2 secure encryption scheme with homomorphic embedding into a vCCA secure FHE scheme

Using a Succint Non-Interactive Argument of Knowledge (SNARK), we prove the correct execution of the evaluation algorithm. This proof becomes a requirement for the homomorphic decryption algorithm, allowing it to reject decryption without proof that they are the result of a certain evaluation.

The authors show that if the SNARK is black-box weak simulation-sound extractabile, then the resulting FHE of this transformation is vCCA secure. This shows that the notion is achievable.

4 Critique

This paper showed many powerful results. The authors proposed what was the strongest semantic security notion to date, vCCA security, and did much work to find how it relates to other notions. They also showed that the notion was feasible for FHE by proposing a plausible construction based on embedding FHE in a CCA2 secure scheme, giving strength to their proposal.

The way they constructed the scheme was also quite interesting and gave insights in the process of improving the security of schemes by utilizing existing techniques.

It is no surprise that this paper was quickly cited by other authors writing papers in the same field, such as Walter [3] and Takumi [2].

However, there were some weaknesses in this paper.

For instance, they mistakenly made the assumption that CPA^{D} only applied to approximate FHE, when authors soon wrote papers showing it could affect exact FHE [8][5].

Also, while it is a theoretical paper proposing a proof of concept, the lack of discussion about performance (which is one of the biggest reasons fully homomorphic encryption isn't used in practice) is something that could be improved. The addition of SNARKs on top of FHE may prove to considerably increase the computational complexity of their approach, leading to it being impossible to implement.

Another weakness is the lack of significant discussion about the practical implications of using this security notion rather than CPA or CCA1. It makes it difficult to assess the cost-benefit of the added complexity for a theoretically stronger model.

Lastly, while the organization of the paper was well thought out, much of the content was difficult to grasp without having to rely on reading the cited papers. Notation was not always clearly defined, and often assumed to be understood by the reader. Take for a light example TNM-vCCA, an acronym for which the meaning was never explicitly defined.

5 Future Enhancements

This paper seems to be an important milestone for secure FHE, and a lot of work can be done in light of it, such as:

- Implementing a vCCA secure scheme, as we only have a theoretical one for now,
- Searching for stronger security notions applicable to FHE, which is an endeavour some researchers have already put time in since this paper was published [1],
- Assessing the performance impact of the proposed transformation, and finding simpler and more efficient vCCA secure constructions,
- Assessing vCCA's applicability in fields other than FHE,
- Assessing the performance impact of vCCA in general, and comparing future vCCA secure schemes to non vCCA secure schemes,
- Assessing the practicality of attacks which are not possible under vCCA security but are possible under weaker notions,
- Analyzing the relationship between vCCA and CPA^{D}, now that we are aware that it is indeed applicable to exact FHE

6 Conclusion

"Fully Homomorphic Encryption beyond IND-CCA1 Security: Integrity through Verifiability." was a challenging but insightful read. It was a somewhat longer

paper at 36 pages, but had a lot of novel results and took into account the latest proposals and results.

I am looking forward to seeing the next steps in FHE security notions and the future works of Manulis and Nguyen!

References

[1] Brzuska, Chris, Sébastien Canard, Caroline Fontaine, Duong Hieu Phan, David Pointcheval, Marc Renard, and Renaud Sirdey. "Relations among new CCA security notions for approximate FHE." Cryptology ePrint Archive, Paper 2024/812, 2024. https://eprint.iacr.org/2024/812.

[2] Shinozaki, Takumi, Keisuke Tanaka, Masayuki Tezuka, and Yusuke Yoshida. "On the Relationship between FuncCPA and FuncCPA+." Cryptology ePrint Archive, Paper 2024/1166, 2024. https://eprint.iacr.org/2024/1166.

[3] Walter, Michael. "What Have SNARGs Ever Done for FHE?" Cryptology ePrint Archive, Paper 2024/1207, 2024. https://eprint.iacr.org/2024/1207.

[4] Boneh, Dan, Gil Segev, and Brent Waters. "Targeted Malleability: Homomorphic Encryption for Restricted Computations." Cryptology ePrint Archive, Paper 2011/311, 2011. https://eprint.iacr.org/2011/311.

[5] Cheon, Jung Hee, Hyeongmin Choe, Alain Passelègue, Damien Stehlé, and Elias Suvanto. "Attacks Against the IND-CPA$^{\mathrm{D}}$ Security of Exact FHE Schemes." In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security*, 2505-2519. New York: ACM, 2024. doi: 10.1145/3658644.3690341.

[6] Das, Angsuman, Sabyasachi Dutta, and Avishek Adhikari. "Indistinguishability against Chosen Ciphertext Verification Attack Revisited: The Complete Picture." In *Provable Security*, edited by Willy Susilo and Reza Reyhanitabar, 104-120. Lecture Notes in Computer Science, vol. 8209. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. doi: 10.1007/978-3-642-41227-1_6.

[7] Li, Baiyu, and Daniele Micciancio. "On the Security of Homomorphic Encryption on Approximate Numbers." In *Advances in Cryptology – EUROCRYPT 2021*, edited by Anne Canteaut and François-Xavier Standaert, 648-677. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-77870-5_23.

[8] Checri, Marina, Renaud Sirdey, Aymen Boudguiga, and Jean-Paul Bultel. "On the practical CPAD security of 'exact' and threshold FHE schemes and libraries." Cryptology ePrint Archive, Paper 2024/116, 2024. https://eprint.iacr.org/2024/116.

[9] Akavia, Adi, Craig Gentry, Shai Halevi, and Margarita Vald. "Achievable CCA2 Relaxation for Homomorphic Encryption." Cryptology ePrint Archive, Paper 2022/282, 2022. https://eprint.iacr.org/2022/282.

[10] Prabhakaran, Manoj, and Mike Rosulek. "Homomorphic Encryption with CCA Security." Cryptology ePrint Archive, Paper 2008/079, 2008. https://eprint.iacr.org/2008/079.

[11] Fauzi, Prastudy, Martin N. Hovd, and Håvard Raddum. "On the IND-CCA1 Security of FHE Schemes." *Cryptography* 6, no. 1 (2022): 13. https://www.mdpi.com/2410-387X/6/1/13.

[12] Manulis, Mark, and Jerome Nguyen. "Fully Homomorphic Encryption Beyond IND-CCA1 Security: Integrity Through Verifiability." In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 63-93. Cham: Springer Nature Switzerland, 2024. 10.1007/978-3-031-58723-8_3.

[13] Gentry, Craig. "Fully homomorphic encryption using ideal lattices." In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, 169-178. ACM, 2009. doi: 10.1145/1536414.1536440.

[14] Rivest, Ronald L., Len Adleman, and Michael L. Dertouzos. "On Data Banks and Privacy Homomorphisms." In Foundations of Secure Computation, edited by Richard A. DeMillo et al., 169-179. Academic Press, 1978.

[15] Kim, Dongwoo, and Cyril Guyot. "Optimized Privacy-Preserving CNN Inference With Fully Homomorphic Encryption." *IEEE Transactions on Information Forensics and Security* 18 (2023): 2175-2187. doi: 10.1109/TIFS.2023.3263631.

[16] Asharov, Gilad, Abhishek Jain, and Daniel Wichs. "Multiparty Computation with Low Communication, Computation and Interaction via Threshold FHE." Cryptology ePrint Archive, Paper 2011/613, 2011. https://eprint.iacr.org/2011/613.

[17] Martins, Paulo, and Leonel Sousa. "A methodical FHE-based cloud computing model." *Future Generation Computer Systems* 95 (2019): 639-648. doi: 10.1016/j.future.2019.01.046.

[18] Shoup, Victor, and Rosario Gennaro. "Securing Threshold Cryptosystems against Chosen Ciphertext Attack." *Journal of Cryptology* 15, no. 2 (2002): 75-96. https://doi.org/10.1007/s00145-001-0020-9.