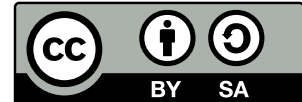

BUFF Transform

Bachelor's Thesis Proposal
by Marlena Müller

Research Group 
Codes and Cryptography

This work is licensed under a Creative Commons
“Attribution-ShareAlike 4.0 International” license.



1 Introduction

The goals of information security are commonly defined as the CIA triad. The CIA triad stands for: Confidentiality, Integrity and Availability. Often used tools to ensure authenticity and thus integrity are signature schemes. Signature schemes are considered secure, if they provide existentially unforgeability under adaptive chosen message attacks (EUF-CMA). This security notion protects against an attacker with access to a signing oracle, signing arbitrary messages for the attacker. If an attacker with this abilities cannot efficiently produce a valid signature for a new message with non negligible probability the signature scheme is called EUF-CMA secure. In reality, there are applications, that need additional security guarantees, like exclusive ownership or non Re-Signability, which is not guaranteed by commonly used signature schemes [PS05] [JCCGS19].

1.1 Exclusive Ownership

The notion of exclusive ownership as introduced by [PS05] guarantees, given a triple (pk, m, s) consisting of a public key pk , a message m and the signature s of m under pk , one cannot efficiently produce either a triple (pk', m', s) or (pk, m', s) with non negligible probability. In these triples pk' is a different public key and m' is a different message and the signature s must be valid under the corresponding public key and message. If a signature scheme is secure against generating a triple (pk', m', s) it is called secure against destructive exclusive ownership (DEO), if it is secure against generating a triple (pk, m', s) it is called secure against conservative exclusive ownership (CEO). If it satisfies both, we speak of universal exclusive ownership (UEO). The widely recommended RSA signature scheme ([SOG23]) does not provide exclusive ownership as shown by [PS05].

1.2 Non Re-Signability

[JCCGS19] introduced a new class of attacks against signature schemes, the so called “Re-Signing” attack. This attack was formalized by [CDF⁺21], by providing a formal game and security definition. A signature scheme is vulnerable against re-signing, if an adversary is given a secret key sk' , a signature $s = \text{Sign}(m, sk)$ for an unknown message m and an unknown key-pair (pk, sk) and some additional auxiliary information and the adversary can produce with high probability a forged signature s' for which $s' = \text{Sign}(m, sk')$ holds.

As the auxiliary information can be chosen arbitrarily depending on pk and m , we need to ensure, that the auxiliary information does not contain too much information about the message. We require in this attack that given the auxiliary information guessing the message correctly has negligible probability. This requirement is formalized using the computational HILL entropy introduced by [HILL99].

[JCCGS19] analyzed different signature schemes under this new attack and found out, that amongst other RSA signatures are susceptible to Re-Signing.

1.3 Message Bound Signatures

The idea of message bound signatures is, that for a given signature scheme an adversary cannot efficiently generate two messages m, m' and a signature σ , for which the verification algorithm accepts under some public key pk . This security definition was introduced in [SPMLS02] and was further refined in [JCCGS19] and [BCJZ21].

1.4 Random Oracle Model

To model (pseudo) random functions in theoretical proofs [BR93] introduced the so called “Random Oracle Model” (ROM). In this model (pseudo) random functions get replaced by a random oracle. A random oracle works as follows: If it is queried for a value, it has not seen before, it outputs a random value. If it is queried for a value it was already queried, it outputs the same value again. This random oracle is used in multiple ways in cryptographic proofs, e.g. modeling secure block ciphers or collision resistant hash functions.

2 Current state of research

In [CDF⁺21] there are two new ways presented to transform an EUF-CMA secure signature scheme into a new scheme with additional security properties using a collision resistant hash function. These new schemes are called BUFF-Transform (**beyond unforgeability features**) and BUFF-Lite-Transform.

2.1 BUFF-Lite-Transform

The idea of the BUFF-Lite-Transform was introduced in [PS05]. The in [PS05] discussed solutions to add CEO and DEO to an EUF-CMA secure signature scheme, were combined

<p>1: Gen[*](1^λ):</p> <p>2: $(sk, pk) \leftarrow \text{Gen}(1^\lambda)$</p> <p>3: return (sk, pk)</p>	<p>1: Sign[*](sk, m):</p> <p>2: $h \leftarrow H(m, pk)$</p> <p>3: $\sigma \leftarrow \text{Sign}(sk, m)$</p> <p>4: $\sigma^* \leftarrow (\sigma, h)$</p> <p>5: return σ^*</p>	<p>1: Verify[*](pk, m, σ^*):</p> <p>2: $(\hat{\sigma}, \hat{h}) \leftarrow \sigma^*$</p> <p>3: $h \leftarrow H(m, pk)$</p> <p>4: $d \leftarrow \text{Verify}(pk, m, \hat{\sigma})$</p> <p>5: return $d = 1 \wedge \hat{h} = h$</p>
--	---	---

Figure 1: BUFF-Lite-Transform as defined in fig. 5 in [CDF⁺21]

<p>1: Gen[*](1^λ):</p> <p>2: $(sk, pk) \leftarrow \text{Gen}(1^\lambda)$</p> <p>3: return (sk, pk)</p>	<p>1: Sign[*](sk, m):</p> <p>2: $h \leftarrow H(m, pk)$</p> <p>3: $\sigma \leftarrow \text{Sign}(sk, h)$</p> <p>4: $\sigma^* \leftarrow (\sigma, h)$</p> <p>5: return σ^*</p>	<p>1: Verify[*](pk, m, σ^*):</p> <p>2: $(\hat{\sigma}, \hat{h}) \leftarrow \sigma^*$</p> <p>3: $h \leftarrow H(m, pk)$</p> <p>4: $d \leftarrow \text{Verify}(pk, h, \hat{\sigma})$</p> <p>5: return $d = 1 \wedge \hat{h} = h$</p>
--	---	---

Figure 2: BUFF-Transform as defined in fig. 6 in [CDF⁺21]

in [CDF⁺21] to form the transform shown in fig. 1. They add to the signature a hash of the message and public key and additionally check in the verification algorithm, if the provided hash is the same as the expected one, effectively binding the signature to the message and public key. They show, that the BUFF-Lite-Transform is still EUF-CMA secure and additionally gives UEO and MBS. The BUFF-Lite-Transform does not interfere with the input of the underlying signature function, so the EUF-CMA proof can be directly adopted to prove the EUF-CMA property of the transformed signature scheme.

2.2 BUFF-Transform

In addition to the BUFF-Lite-Transform [CDF⁺21] also introduced the more sophisticated BUFF-Transform, which yields the same security properties (UEO and MBS) and claims also Non Re-Signability, while still being EUF-CMA secure. For the BUFF-Transform this time the input of the underlying signature scheme gets altered, instead of the message m the input is now $H(m, pk)$.

2.3 Salted-BUFF-Transform

In [DFHS24] there is an attack given against the Non Re-Signability (NR) of the BUFF-Transform, showing that the claim of [CDF⁺21] that BUFF-Transform provides NR is wrong. In the attack the adversary utilizes the auxiliary function, which can be used to calculate $\sigma' = \text{Sign}(sk', m)$ for a new key pair sk', pk' . The adversary can then just output σ', pk' as a forgery, breaking the NR property. This attack in the plain model can be adapted to the ROM effectively breaking it in this model as well.

As a fix of the broken BUFF-Transform [DFHS24] introduces a new variant of the BUFF-Transform called Salted-BUFF-Transform (or \$-BUFF-Transform), shown in fig. 3. They show, that the Salted-BUFF-Transform fullfills in the ROM a weaker NR notion, where it is not possible to use the oracle for calculating the auxiliary information.

1: Gen [*] (1 ^λ): 2: $(sk, pk) \leftarrow \text{Gen}(1^\lambda)$ 3: return (sk, pk)	1: Sign [*] (sk, m): 2: $s \leftarrow \{0, 1\}^l$ 3: $h \leftarrow H(m, pk, s)$ 4: $\sigma \leftarrow \text{Sign}(sk, h)$ 5: return (σ, h, s)	1: Verify [*] (pk, m, σ [*]): 2: $(\hat{\sigma}, \hat{h}, \hat{s}) \leftarrow \sigma^*$ 3: $h \leftarrow H(m, pk, s)$ 4: $d \leftarrow \text{Verify}(pk, h, \hat{\sigma})$ 5: return $d = 1 \wedge \hat{h} = h$
--	--	--

Figure 3: Salted-BUFF-Transform

2.4 Dilithium

In the search for Post-Quantum-Secure signature schemes [DKL⁺18] introduced a new signature scheme called DILITHIUM. This signature scheme is based on lattice cryptography and believed to be secure against all feasible classical and quantum attacks. DILITHIUM was submitted to the NIST and is currently evaluated in the 4th round.

[CDF⁺21] claims, that the DILITHIUM signature scheme uses the BUFF-Transform implicitly.

3 Goals of the thesis

The goal for this thesis is to analyze the implications of [DFHS24]. In order to do this, we will first look how the BUFF-Transform and its weaker counterpart BUFF-Lite-Transform work, and which security goals they want to meet respectively. After that we will present the positive and negative findings of [DFHS24], on both transforms. We will additionally look into the usage of the entropy notion introduced by [HILL99] and why usage of a statistical entropy notion is not sufficient for proving the security of the BUFF-Transform.

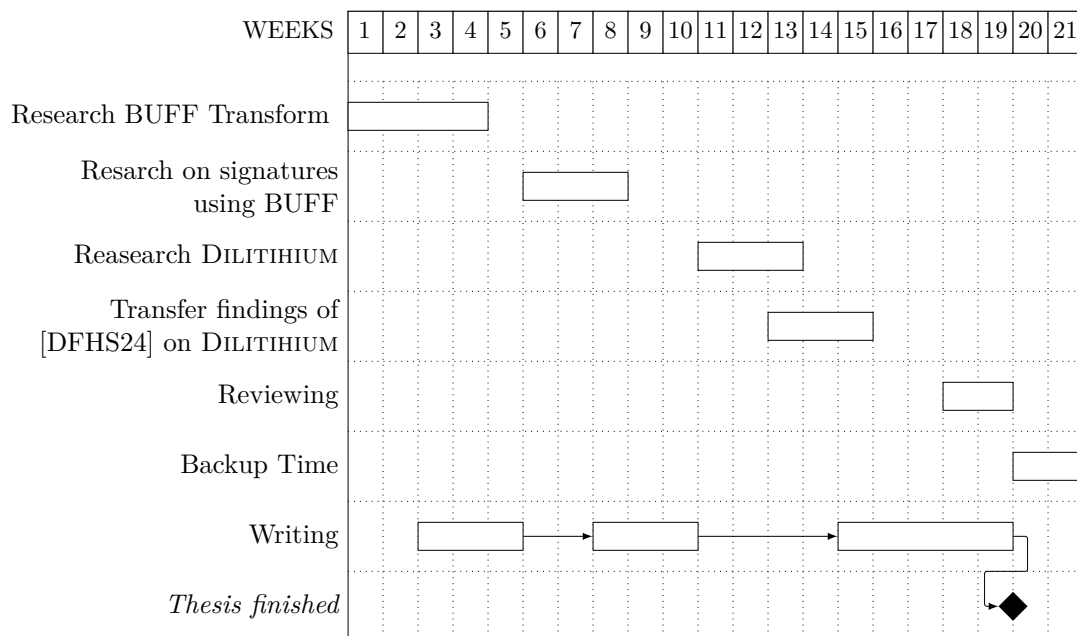
Furthermore we will research, if there are any signature schemes, that use the BUFF-Transform either explicitly or implicitly. For this we will at least look into DILITHIUM [DKL⁺18], as [CDF⁺21] claims, that this signature protocol uses implicitly the BUFF-Transform. During this we will check, if DILITHIUM really uses the BUFF-Transform, check if it is effected of the findings of [DFHS24], and if the salted BUFF-Transform can be applied to DILITHIUM.

4 Preliminary outline of the thesis

The following preliminary outline is planned for the thesis:

1. Introduction
2. Definitions and notation
3. BUFF-Transform and BUFF-Lite-Transform
 - a) Existential unforgeability
 - b) Message bound signatures
 - c) Non Re-Signability in the plain model and the ROM
4. Salted-BUFF-Transform
5. Signature schemes using the BUFF-Transform
6. Applying the Salted-BUFF-Transform

5 Work plan



Date:

Prof. Dr. Johannes Blömer

Marlena Müller

References

- [BCJZ21] Jacqueline Brendel, Cas Cremers, Dennis Jackson, and Mang Zhao. The provable security of ed25519: Theory and practice. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1659–1676, 2021.
- [BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security, CCS '93*, page 62–73, New York, NY, USA, 1993. Association for Computing Machinery.
- [CDF⁺21] Cas Cremers, Samed Düzlü, Rune Fiedler, Marc Fischlin, and Christian Janson. BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1696–1714, 2021.
- [DFHS24] Jelle Don, Serge Fehr, Yu-Hsuan Huang, and Patrick Struck. On the (in)security of the BUFF transform. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024*, pages 246–275, Cham, 2024. Springer Nature Switzerland.
- [DKL⁺18] Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018(1):238–268, Feb. 2018.
- [HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.
- [JCCGS19] Dennis Jackson, Cas Cremers, Katriel Cohn-Gordon, and Ralf Sasse. Seems legit: Automated analysis of subtle attacks on protocols that use signatures. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS '19*, page 2165–2180, New York, NY, USA, 2019. Association for Computing Machinery.
- [PS05] Thomas Pornin and Julien P. Stern. Digital signatures do not guarantee exclusive ownership. In John Ioannidis, Angelos Keromytis, and Moti Yung, editors, *Applied Cryptography and Network Security*, pages 138–150, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.
- [SOG23] SOG-IS crypto evaluation scheme agreed cryptographic mechanisms. Specification, SOG-IS Crypto Working Group, Feb 2023. <https://sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf>.

- [SPMLS02] Jacques Stern, David Pointcheval, John Malone-Lee, and Nigel P. Smart. Flaws in applying proof methodologies to signature schemes. In Moti Yung, editor, *Advances in Cryptology — CRYPTO 2002*, pages 93–110, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.