THE UNIVERSITY of EDINBURGH
informatics

QCRYPT 2021

A Unified Framework For Quantum Unforgeability

Mina Doosti[1]; Mahshid Delavar[1]; Elham Kashefi[1,2] ; Myrto Arapinis[1]

[1]University of Edinburgh

[2]CNRS, Sorbonne University

ABSTRACT

In this paper, we continue the line of work initiated by Boneh and Zhandry at CRYPTO 2013 and EUROCRYPT 2013 in which they formally define the notion of unforgeability against quantum adversaries. We develop a general and parameterised quantum game-based security model unifying unforgeability for both classical and quantum constructions allowing us for the first time to present a complete quantum cryptanalysis framework for unforgeability. In particular, we prove how our definitions subsume previous ones while considering more fine-grained adversarial models, capturing the full spectrum of superposition attacks. The subtlety here resides in the characterisation of a forgery. We show that the strongest level of unforgeability in our framework, namely existential unforgeability, can only be achieved if only orthogonal to previously queried messages are considered to be forgeries. We further show that deterministic constructions can only achieve the weaker notion of unforgeability, that is selective unforgeability, against such adversaries, but that selective unforgeability breaks if more general quantum adversaries (capable of general superposition attacks) are considered. On the other hand, we show that PRF is sufficient for constructing a selective unforgeable classical primitive against full quantum adversaries. Moreover, we show similar positive results relying on Pseudorandom Unitaries (PRU) for quantum primitives.These results demonstrate the generality of our framework that could be applicable to other primitives beyond the cases analysed in this paper.

Arxiv: 2103.13994

Introduction

Recent advances in quantum technologies threaten the security of many widely-deployed cryptographic primitives. This calls for quantum-secure cryptographic schemes. In this work we attempt to formalize the notion of **unforgeability** in the quantum security model, where the adversary has further quantum access to the primitive, i.e. can issue quantum queries. This notion is the security property desired for many primitives such as **Message Authentication Codes**, **Digital Signatures**, or **Physical Unclonable Functions**.

We propose a general and unified definition of quantum unforgeability in the quantum-game based framework. The main features of our framework are:

- Unifying quantum and classical primitives
- Quantum analogue of other existing notions of classical unforgeability
- Exploring new attacks and vulnerabilities against quantum adversaries

Definition level \ Attack model	Chosen message attack (cma)	Random message attack (rma)	Adaptive universal attack (aua)
(Strong) Existential unforgeability	BZ[1,2], BU[3], this work	NA	NA
(Weak) Existential unforgeability	BU[3], this work	this work	NA
Selective unforgeability	this work	this work	NA
Universal unforgeability	this work	this work	this work

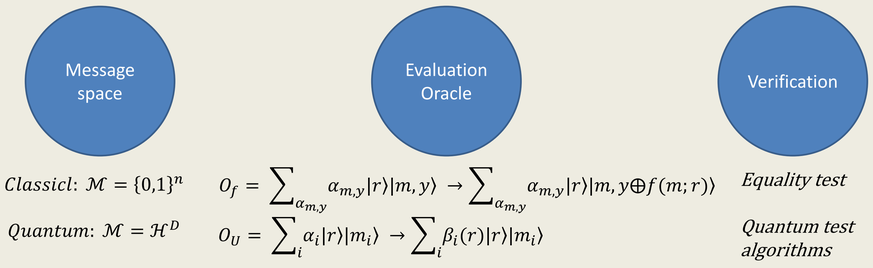
Table 1. Quantum unforgeability definitions from strongest to weakest.

Generalized Quantum Unforgeability

Generalized Quantum Unforgeability captures different levels of unforgeability definitions and is defined by a formal security game between an adversary A and an honest challenger C. It applies to a general quantum or classical primitive $F = (S, E, V)$ with setup, evaluation and verification algorithms.

Classical vs. Quantum primitive

Main differences between classical and quantum primitives can be formalized in the following aspects:



Intuitive meaning of unforgeability

Existential unforgeability is a security notion that formally describes conditions for a function to be **unpredictable**. Intuitively it means an adversary should not be able to produce the output of the function even for a **new** message of their choice.

What if the learning phase queries and the message are quantum state? What does it mean for the message to be "new"?

There are different approaches to answer this question:
BZ[1,2]: Count the queries! If the adversary queries **q** quantum queries, should output **q+1 classical** input/output pairs.
BU[3]: Define a blinding oracle. The oracle has a blinding region that never gives the answer to the messages in the blinding region even if the query include the message in superposition. Then the adversary needs to find the output for a message inside the blinding region.
Our approach: It depends! In the quantum world, it is more natural to capture this difference between the queries and challenge, by a **distance measure** between the quantum states. This leads to different degrees of unforgeability.

μ**-qGEU:** The adversary picks the forgery after the learning phase and the state should be μ**-distinguishable** from all the query states.
μ**-qGSU:** The adversary picks the forgery **before** the learning phase and the state should be μ**-distinguishable** from all the query states.
qGUU: The challenger picks the forgery message **at random** from the message space

Hierarchy and Relationship to other definitions

1-qGEU is equivalent to Blind unforgeability (BU) for classical primitives

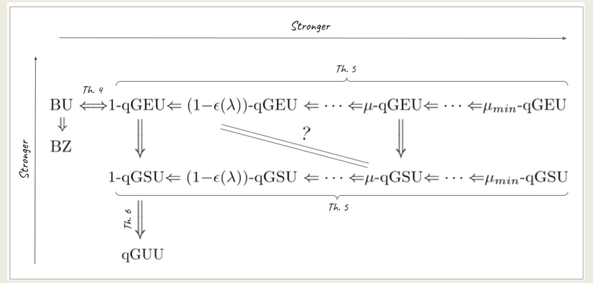


Figure 1. Hierarchy and relationships between different notions of unforgeability

Results

General impossibility results:

- No classical primitive can achieve μ**-qGEU** (generalized existential unforgeability) except for μ=1 (message is completely distinguishable or orthogonal to the learning phase)
- No classical or quantum non-randomized primitive can achieve μ**-qGSU** as there are non-trivial quantum attacks for a wide range of μ parameter.

Positive results for classical primitives:

- **Deterministic:** Classical quantum secure PRF (qPRF) schemes are 1-qGEU (1-qGSU) unforgeable.
- **Randomized:** We give a randomized PRF-based construction that satisfies generalized selective unforgeability (qGSU) which is μ-qGSU for any valid μ.

Construction 1. *Let $F : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$ be a PRF (or any other family satisfying Definition 14). Let $\mathcal{R} = \mathcal{K} = \{0,1\}^t$ be the randomness space. And let λ be the security parameter and l be polynomial in λ. The construction is defined by the following key generation algorithm, keyed evaluation algorithm, and keyed verification algorithm:*

- **Key generation:** *The secret key is picked uniformly at random from $\mathcal{K}$: $k \xleftarrow{\$} \mathcal{K}$*
- **Evaluation:** *The evaluation under key k on input m picks randomness r and applies $F(k \oplus r, \cdot)$ to m. Note that when responding to a quantum query, the same randomness is used for all the states of the superposition:*
  - *On input $m \in \mathcal{X}$:*
  - *$r \xleftarrow{\$} \mathcal{R}$*
  - *Return $F(k \oplus r, m)||r$*
- **Verification:** *The verification under key k of a pair $(m,(t,r))$, runs the evaluation algorithm on m under k with randomness r, and checks equality with t.*
  - *On input $(m,(t,r)) \in \mathcal{X} \times (\mathcal{Y} \times \mathcal{R})$:*
  - *If $F(k \oplus r, m) = t$ return $\top$, otherwise return $\bot$*

Positive results for quantum primitives:

- **Deterministic:** Pseudorandom Unitary (PRU) schemes are 1-qGEU (1-qGSU) unforgeable.
- **Randomized:** We give a randomized PRU-based construction that satisfies generalized selective unforgeability (qGSU).

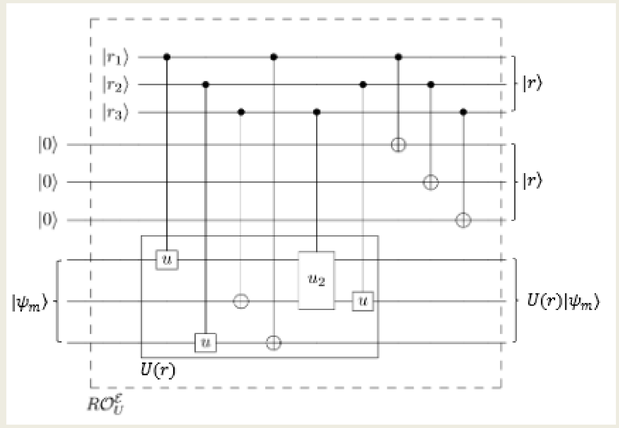


Figure 2. Sample circuit for a randomized quantum oracle for quantum primitive

Primitives	1-qGEU	μ-qGEU ($\mu \neq 1$)	1qGSU	μ-qGSU ($\mu \neq 1$)	qGUU
Classical	qPRF	X	qPRF	Det: X	qPRF
				Rand: PRF-based construction	
Quantum	PRU	X	PRU	Det: X	PRU UU
				Rand: PRU-based construction	

Table 2. Summary of results

References:

1. D. Boneh and M. Zhandry, "Quantum-secure message authentication codes," in Advances in Cryptology, EUROCRYPT 2013
2. D. Boneh and M. Zhandry, "Secure signatures and chosen ciphertext security in a quantum computing world," in Advances in Cryptology, CRYPTO 2013
3. G. Alagic, C. Majenz, A. Russell, and F. Song, "Quantum-access-secure message authentication via blind-unforgeability," in39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020,