RESUMO DO PLANO DE TRABALHOS

Título do Plano de Trabalhos

Bringing Post-Quantum Cryptography to Practice

Sumário

Quantum computers will break the public-key cryptosystems we use pervasively. This risk has led to the development of post-quantum cryptographic (PQC) systems, believed not to be vulnerable to quantum attacks. Some PQC constructions are being considered for standardisation, but many challenges remain: although we have competitive alternatives for low-level components such as digital signatures and encryption, we do not have a systematic way of upgrading complex protocols used in practice to a post-quantum security level.

The goal of this proposal is to contribute to the development of efficient post-quantum cryptographic systems that can replace existing protocols. We will focus on concrete applications, starting with passwordless authentication and messaging protocols, and progressing towards more complex protocols such as non-interactive proofs. We will focus on the challenges that arise in the provable security of such protocols, including security modeling, modular analysis for complex protocols, and proof techniques for efficient parameter selection.

Palavras-chave

post-quantum cryptography | applied cryptography | provable security | quantum computers

Objetivos de Desenvolvimento Sustentável (ODS)

- ODS 9: Indústria, Inovação e Infraestruturas
- ODS 16: Paz, Justiça e Instituições Eficazes

ESTADO DA ARTE

Estado da Arte

Trust in modern cryptography is based on two pillars. Cryptanalysis is used to understand the hardness of simple mathematical problems used in cryptographic systems, including the hardness of breaking basic cryptographic building blocks, such as block-ciphers. The security of cryptographic systems is then proved by showing that the only way to break the system is to solve one of the aforementioned hard problems [KL].

The last decade has seen a huge amount of progress in provable security for PQC schemes. We have many plausible candidate constructions for the core cryptographic components in the most widely used point-to-point connection protocols such as TLS; this includes key encapsulation mechanisms (i.e., public-key encryption schemes tailored to transport and establish session keys) and digital signature schemes [NIST]. The performance of such schemes, which was initially prohibitive, is now acceptable and it is likely that in the next few years we will have PQC solutions for these low-level components that are as good or even surpass our current solutions [MCTY].

However, identifying good candidates for low-level PQC components is only the first step. A major open question (and the drive for vibrant research) is how to integrate these components into higher-level protocols. In particular, this is the case for the provable security of hugely popular practical protocols such as TLS and Signal, emerging trends such as FIDO2 [FIDO] and block-chain infrastructures such as Ethereum, and many application-oriented standards for attestation [ATT], authenticated key exchange [PAKE], key management [AWS], etc.

The foundations for post-quantum provable security were established in the last decade. First works [QMAC,QSIG,QROM] highlighted the difference between quantum interaction with a system and a classical attack. In the former, the quantum attacker is present when the system is executing and is attacking a scheme running in a quantum computer. This is an interesting setting, but hardly the most realistic one in the near future, where quantum computers (if they come to be) will be a scarce resource. Nevertheless, quantum interaction is still relevant even for the schemes we use today. Shor's algorithm [SHO] can have devastating consequences, of course, but there are other subtle implications. For example, when we use the Random Oracle Model, this captures computations that the adversary does internally; hence, queries to a ROM when analysing the security of a PQC scheme that will be deployed today must account for superposition [QROM]. It follows that not all proof techniques and modular analysis approaches naturally transpose to the post-quantum setting, even when the attacker is not able to quantum interact with the system.

More recently, various proof techniques and well known classical protocols have been revisited from a post-quantum perspective, including hashing and block-ciphers, encryption and signatures [QFO], and more complex protocols such as zero-knowledge proofs [QZK], and secure multiparty computation [QMPC]. However, with notable exceptions [ZKB,QTLS], essentially all of these works focus on the theoretical aspects of the proofs, rather than on practically deployable complex post-quantum protocols.

OBJETIVOS

Objetivos

The goal of this proposal is to contribute to the development of efficient post-quantum cryptographic systems that can replace existing protocols. We will focus on concrete applications, starting with passwordless authentication and messaging protocols, and progressing towards more complex protocols such as non-interactive proofs. We will focus on the challenges that arise in the provable security of such protocols when considering quantum attackers:

- To adapt the current existing security models against classical attackers to post-quantum ones in the language of provable security, while maintaining these models adjusted to practical systems; here the distinction between quantum interaction and classical interaction with a system is crucial, and must be evaluated for each concrete protocol and application setting.

- To revisit modular analysis and proof techniques for parameter optimization used to justify existing complex protocols and evaluate whether the same principles apply to the post-quantum setting; in many cases, even if the techniques turn out to generalize to the post-quantum setting, this implies a loss in tightness, which may have implications on concrete security and performance.

The ultimate goal is to develop provably secure solutions that can serve as drop-in replacements of existing protocols; ideally this would be achieved by preserving the design rationale and modular structure of existing solutions, but the security and performance constraints may impose entirely new designs and proof techniques.

All proposed protocols will be prototyped and benchmarked for practical performance evaluation, and the goal is to publish the results in top-teer cryptography and security venues such as ACM CCS, IACR Crypto/Eurocrypt/Asiacrypt/PKE, IEEE Security and Privacy. The work plan will be carried out in collaboration with international researchers, and it will include short-term visits to international research partners.

DESCRIÇÃO DETALHADA

Descrição Detalhada

Our society and economy rely on the availability of secure digital networks, over which we run an ever increasing set of applications. Each application comes with its own set of security requirements, including secrecy, privacy, and authenticity, which are guaranteed via the use of cryptography.

These guarantees may be threatened if quantum computers become a reality: the hard mathematical problems that underlie all current public-key cryptography---i.e., those based on factoring and on discrete-logarithms---are efficiently solvable in a quantum computer using Shor's algorithm [SHO]. This possibility is driving the development of a new generation of cryptographic algorithms that may withstand attacks from quantum computers. These so-called post-quantum cryptography (PQC) algorithms are based on new mathematical problems, for which efficient quantum computing solutions are not known. This shift is urgent, as there are applications that require long-term security: data protected today must remain secure for decades into the future.

For these reasons PQC is currently making its way into standards; leading standardization bodies that deal with cryptography are looking into this topic, including the IETF, ETSI, ISO and NIST. The first RFCs on post-quantum cryptography were already published by IETF's research division IRTF [QRFC] and in 2016 NIST initiated a process to select post-quantum signature and key encapsulation systems for standardization [NIST].

The goal of this PhD project is to contribute to the development of a new generation of efficient applied cryptography protocols that are supported by adequate provable post-quantum security arguments. We outline the main challenges next.

The challenges we face today can be divided into three complementary classes:

1. Security models. Defining a security model adjusted to practical systems is a crucial part of modern cryptography: the model should be strong enough to prevent realistic attacks, but if it is too strong then efficient instantiations may not exist. When considering the possibility of quantum attackers, it is unclear what the correct adaptation of our existing models should be, and what performance/security trade-offs are possible. For example, the security notions for interactive protocols are often modelled as oracle systems, and adequately modeling the interaction of a quantum attacker with such systems is non-trivial and results in very complex security proofs. Conversely, if we are reasoning about information encrypted today, then it may be reasonable to assume that a quantum attacker will be launching a passive attack, where it only has access to a record of the conversation.

2. Proof techniques. Many proof techniques we use today need revisiting when considering quantum adversaries. For example, many symmetric schemes (which are believed to be post-quantum secure) are used close to their security bounds, so even a small optimization in attack effectiveness could compromise their security. As a concrete example, consider the case where an authenticated encryption scheme is used in an application that could bring the number of encryptions close to the birthday bound (e.g., 2^64); then, if this scheme is used in conjunction with a post-quantum-secure signature scheme, which may result in a verification error with some small probability, a naive replay solution may amplify the problem and introduce a security vulnerability. A crucial question is whether the composition and modular analysis paradigms that we use for classical attackers are still applicable/sufficient, since this is how we currently construct complex systems from simpler ones. This question applies both to the composition of low-level proof steps (as in game hops) and to the composition of provable security theorems by component instantiation. The ongoing NIST competition provides strong evidence that we need to go beyond proof techniques for classical cryptography, as otherwise the resulting protocols are not suitable for practical deployment.

3. Concrete protocols. With the prior challenges still unresolved, we are still pressed to look at concrete protocols, as we require suitable PQC replacements. Progress is being made by evaluating our current ability to construct *efficient* PQC replacements for critical cryptographic protocols supporting our society. The challenges here are the additional restrictions that constrain the design space: each protocol comes with its own security requirements and security models, and existing (classical) constructions also bring some legacy and backwards compatibility requirements. Contrary to what one might expect, existing security proofs for cryptographic protocols relying on lower-level components (e.g., TLS, Signal, etc) are not modular and robust to the extent that they allow for direct adaptation to a quantum setting (even when a natural PQC security model has been identified and assuming low-level PQC components). For example, messaging systems such as Signal use the same cryptographic key for several purposes, which breaks modularity and requires the use of non-standard assumptions. Replicating these designs in a PQC setting is therefore a non-trivial problem, and it may not even be the correct approach.

In this PhD project we will address these challenges by considering concrete practical applications and designing suitable PQC protocols. This will be done in collaboration with international research groups working on applied cryptography. The candidate’s background in post-quantum cryptography (master’s dissertation) will be critical to enable a fast growing learning curve. The supervisor’s long-term collaborations with international researchers in the area of applied cryptography will serve as a starting point for candidate protocols where the ideas outlined in this proposal will be applied; these include standard authentication protocols such as FIDO2 [FIDO], standard password-authenticated key exchange protocols such as SPAKE2 and CPACE [PAKE], privacy-preserving technologies such as SNARKS [ADSK] and secure multiparty computation [GARB]. A promising initial technical challenge for the work is the adaptation of PQC key encapsulation mechanisms to the setting of messaging apps, which has recently been identified as an application of the supervisor’s prior work on optimization via randomness reuse [RR1,RR2].

The work plan will be structured around concrete research projects focusing on specific applied cryptography protocols, and typically giving rise to a publication in an international conference with CORE ranking at least A. It is structured into three years, to match the curricular structure of the Doctoral Programme in Computer Science at FCUP, to which the candidate is applying.