Proposition de recherche doctorale

Symmetric Primitives in the Post-Quantum World

Symmetric Primitives in the Post-Quantum World

Mots clés :
- Directeur de thèse : MARIA NAYA PLASENCIA
- Co directeur de thèse : andré chailloux
- Co-encadrant(s) :
- Unité de recherche : INRIA-Paris
- Ecole doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal: Sciences et technologies de l'information et de la communication

Résumé du projet de recherche (Langue 1)

As years go by, the existence of quantum computers becomes more tangible and the scientific community is already anticipating the enormous consequences of the induced breakthrough in computational power. Cryptology is one of the affected disciplines. Indeed, the current state-of-the-art asymmetric cryptography would become insecure, and we are actively searching for alternatives. Symmetric cryptography, essential for enabling secure communications, seems much less affected at first sight: its biggest known threat is Grover’s algorithm, which allows exhaustive key searches in the square root of their classical complexity. Thus, so far, it is believed that doubling key lengths suffices to maintain an equivalent security in the post-quantum world. The security of symmetric cryptography is completely based on cryptanalysis: we only gain confidence in the security of a symmetric primitive through extensive and continuous scrutiny. It is therefore not possible to determine whether a symmetric primitive might be secure or not in a post-quantum world without first understanding how a quantum adversary could attack it. Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding cryptanalysis toolbox, which has only recently started to be studied. Next, doubling the key length is not a trivial task and needs to be carefully studied. The cryptographic community should propose efficient solutions secure in the post-quantum world with the help of the previously mentioned quantum symmetric cryptanalysis toolbox. This will help prevent the chaos that big quantum computers would generate: being ready in advance will definitely save a great amount of time and money, while protecting our current and future communications.

Résumé du projet de recherche (Langue 2)

As years go by, the existence of quantum computers becomes more tangible and the scientific community is already anticipating the enormous consequences of the induced breakthrough in computational power. Cryptology is one of the affected disciplines. Indeed, the current state-of-the-art asymmetric cryptography would become insecure, and we are actively searching for alternatives. Symmetric cryptography, essential for enabling secure communications, seems much less affected at first sight: its biggest known threat is Grover’s algorithm, which allows exhaustive key searches in the square root of their classical complexity. Thus, so far, it is believed that doubling key lengths suffices to maintain an equivalent security in the post-quantum world. The security of symmetric cryptography is completely based on cryptanalysis: we only gain confidence in the security of a symmetric primitive through extensive and continuous scrutiny. It is therefore not possible to determine whether a symmetric primitive might be secure or not in a post-quantum world without first understanding how a quantum adversary could attack it. Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding cryptanalysis toolbox, which has only recently started to be studied. Next, doubling the key length is not a trivial task and needs to be carefully studied. The cryptographic community should propose efficient solutions secure in the post-quantum world with the help of the previously mentioned quantum symmetric cryptanalysis toolbox. This will help prevent the chaos that big quantum computers would generate: being ready in advance will definitely save a great amount of time and money, while protecting our current and future communications. Therefore, an important challenge to solve is to redesign symmetric cryptography for the post-quantum world. We want to prepare ourselves for the post-quantum world. That is a fact, as shown by the effervescence about postquantum asymmetric cryptography. Due to environmental constraints, it is very likely that common users will never take advantage of quantum capabilities, but a powerful adversary will. It is therefore vital that we dispose of primitives that are efficient on classical computers and secure against quantum adversaries. This means that we have definitely a lot of work to do with respect to symmetric cryptography. As symmetric cryptography completely lies in the variety and ever-changing landscape of symmetric cryptanalysis, we are convinced that it is not possible to determine for instance whether doubling the key length might make a concrete cipher secure or not in a post-quantum world, without first understanding how a quantum adversary could attack the primitive. Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding symmetric cryptanalysis toolbox. This PhD is contributing to fill this gap. The aim of this toolbox is two-fold: 1) analyze existing cryptosystems / primitives, and 2) design new ones which will give us confidence in the post-quantum world. The direction of this PhD of adequately preparing symmetric cryptography for the post-quantum world can logically be decomposed in two main sequential objectives.
Informations complémentaires (Langue 1)

As years go by, the existence of quantum computers becomes more tangible and the scientific community is already anticipating the enormous consequences of the induced breakthrough in computational power. Cryptology is one of the affected disciplines. Indeed, the current state-of-the-art asymmetric cryptography would become insecure, and we are actively searching for alternatives. Symmetric cryptography, essential for enabling secure communications, seems much less affected at first sight: its biggest known threat is Grover’s algorithm, which allows exhaustive key searches in the square root of their classical complexity. Thus, so far, it is believed that doubling key lengths suffices to maintain an equivalent security in the post-quantum world. The security of symmetric cryptography is completely based on cryptanalysis: we only gain confidence in the security of a symmetric primitive through extensive and continuous scrutiny. It is therefore not possible to determine whether a symmetric primitive might be secure or not in a post-quantum world without first understanding how a quantum adversary could attack it. Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding cryptanalysis toolbox, which has only recently started to be studied. Next, doubling the key length is not a trivial task and needs to be carefully studied. The cryptographic community should propose efficient solutions secure in the post-quantum world with the help of the previously mentioned quantum symmetric cryptanalysis toolbox. This will help prevent the chaos that big quantum computers would generate: being ready in advance will definitely save a great amount of time and money, while protecting our current and future communications. Therefore, an important challenge to solve is to redesign symmetric cryptography for the post-quantum world. We want to prepare ourselves for the post-quantum world. That is a fact, as shown by the effervescence about postquantum asymmetric cryptography. Due to environmental constraints, it is very likely that common users will never take advantage of quantum capabilities, but a powerful adversary will. It is therefore vital that we dispose of primitives that are efficient on classical computers and secure against quantum adversaries. This means that we have definitely a lot of work to do with respect to symmetric cryptography. As symmetric cryptography completely lies in the variety and ever-changing landscape of symmetric cryptanalysis, we are convinced that it is not possible to determine for instance whether doubling the key length might make a concrete cipher secure or not in a post-quantum world, without first understanding how a quantum adversary could attack the primitive. Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding symmetric cryptanalysis toolbox. This PhD is contributing to fill this gap. The aim of this toolbox is two-fold: 1) analyze existing cryptosystems / primitives, and 2) design new ones which will give us confidence in the post-quantum world. The direction of this PhD of adequately preparing symmetric cryptography for the post-quantum world can logically be decomposed in two main sequential objectives.

Informations complémentaires (Langue 2)

As years go by, the existence of quantum computers becomes more tangible and the scientific community is already anticipating the enormous consequences of the induced breakthrough in computational power. Cryptology is one of the affected disciplines. Indeed, the current state-of-the-art asymmetric cryptography would become insecure, and we are actively searching for alternatives. Symmetric cryptography, essential for enabling secure communications, seems much less affected at first sight: its biggest known threat is Grover’s algorithm, which allows exhaustive key searches in the square root of their classical complexity. Thus, so far, it is believed that doubling key lengths suffices to maintain an equivalent security in the post-quantum world. The security of symmetric cryptography is completely based on cryptanalysis: we only gain confidence in the security of a symmetric primitive through extensive and continuous scrutiny. It is therefore not possible to determine whether a symmetric primitive might be secure or not in a post-quantum world without first understanding how a quantum adversary could attack it. Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding cryptanalysis toolbox, which has only recently started to be studied. Next, doubling the key length is not a trivial task and needs to be carefully studied. The cryptographic community should propose efficient solutions secure in the post-quantum world with the help of the previously mentioned quantum symmetric cryptanalysis toolbox. This will help prevent the chaos that big quantum computers would generate: being ready in advance will definitely save a great amount of time and money, while protecting our current and future communications. Therefore, an important challenge to solve is to redesign symmetric cryptography for the post-quantum world. We want to prepare ourselves for the post-quantum world. That is a fact, as shown by the effervescence about postquantum asymmetric cryptography. Due to environmental constraints, it is very likely that common users will never take advantage of quantum capabilities, but a powerful adversary will. It is therefore vital that we dispose of primitives that are efficient on classical computers and secure against quantum adversaries. This means that we have definitely a lot of work to do with respect to symmetric cryptography. As symmetric cryptography completely lies in the variety and ever-changing landscape of symmetric cryptanalysis, we are convinced that it is not possible to determine for instance whether doubling the key length might make a concrete cipher secure or not in a post-quantum world, without first understanding how a quantum adversary could attack the primitive. Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding symmetric cryptanalysis toolbox. This PhD is contributing to fill this gap. The aim of this toolbox is two-fold: 1) analyze existing cryptosystems / primitives, and 2) design new ones which will give us confidence in the post-quantum world. The direction of this PhD of adequately preparing symmetric cryptography for the post-quantum world can logically be decomposed in two main sequential objectives.