Cryptography And Network Security Lecture Notes

So far, hash-based cryptography is used to construct digital signatures schemes such as the Merkle signature scheme, zero knowledge and computationally integrity proofs, such as the zk-STARK proof system and range proofs over issued credentials via the HashWires protocol. Hash-based signature schemes combine a one-time signature scheme, such as a Lamport signature, with a Merkle tree structure. Since a one-time signature scheme key can only sign a single message securely, it is practical to combine many such keys within a single, larger structure. A Merkle tree structure is used to this end. In this hierarchical...

Symmetric encryption and message authentication key material construction

Key agreement or establishment

Secured application-level data transport

Shamir similarly proposed identity-based encryption, which...

Elliptic-curve cryptography

Smart, N. P. (1999). "A Cryptographic Application of Weil Descent". A cryptographic application of the Weil descent. Lecture Notes in Computer Science. Vol

Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys to provide equivalent security, compared to cryptosystems based on modular exponentiation in Galois fields, such as the RSA cryptosystem and ElGamal cryptosystem.

Secret sharing...

In 2024 NIST announced the Module-Lattice-Based...

Lattice-based cryptography

or in the security proof. Lattice-based constructions support important standards of post-quantum cryptography. Unlike more widely used and known public-key

Lattice-based cryptography is the generic term for constructions of cryptographic primitives that involve lattices, either in the construction itself or in the security proof. Lattice-based constructions support important standards of post-quantum cryptography. Unlike more widely used and known public-key schemes such as the RSA, Diffie-Hellman or elliptic-curve cryptosystems—which could, theoretically, be defeated using Shor's algorithm on a quantum computer—some lattice-based constructions appear to be resistant to attack by both classical and quantum computers. Furthermore, many lattice-based constructions are considered to be secure under the assumption that certain well-studied computational lattice problems cannot be solved efficiently.

Cryptography

to Modern Cryptography. p. 10. Sadkhan, Sattar B. (December 2013). "Key note lecture multidisciplinary in cryptology and information security". 2013 International

Cryptography, or cryptology (from Ancient Greek: ???????, romanized: kryptós "hidden, secret"; and ??????? graphein, "to write", or -????? -logia, "study", respectively), is the practice and study of techniques for secure communication in the presence of adversarial behavior. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, information security, electrical engineering, digital signal processing, physics, and others. Core concepts related to information security (data confidentiality, data integrity, authentication, and non-repudiation) are also central to cryptography. Practical applications of cryptography...

Identity-based cryptography

Based Encryption Scheme Based on Quadratic Residues". Cryptography and Coding (PDF). Lecture Notes in Computer Science. Vol. 2260/2001. Springer. pp. 360–363

Identity-based cryptography is a type of public-key cryptography in which a publicly known string representing an individual or organization is used as a public key. The public string could include an email address, domain name, or a physical IP address.

Entity authentication, perhaps using a authentication protocol

White-box cryptography

Implementation Using Self-equivalence Encodings. Applied Cryptography and Network Security. Lecture Notes in Computer Science. Vol. 13269. pp. 771–791. doi:10

In cryptography, the white-box model refers to an extreme attack scenario, in which an adversary has full unrestricted access to a cryptographic implementation, most commonly of a block cipher such as the Advanced Encryption Standard (AES). A variety of security goals may be posed (see the section below), the most fundamental being "unbreakability", requiring that any (bounded) attacker should not be able to extract the secret key hardcoded in the implementation, while at the same time the implementation must be fully functional. In contrast, the black-box model only provides an oracle access to the analyzed cryptographic primitive (in the form of encryption and/or decryption queries). There is also a model in-between, the so-called gray-box model, which corresponds to additional information...

Security level

In cryptography, security level is a measure of the strength that a cryptographic primitive — such as a cipher or hash function — achieves. Security level

In cryptography, security level is a measure of the strength that a cryptographic primitive — such as a cipher or hash function — achieves. Security level is usually expressed as a number of "bits of security" (also security strength), where n-bit security means that the attacker would have to perform 2n operations to break it, but other methods have been proposed that more closely model the costs for an attacker. This allows for convenient comparison between algorithms and is useful when combining multiple primitives in a hybrid cryptosystem, so there is no clear weakest link. For example, AES-128 (key size 128 bits) is designed to offer a 128-bit security level, which is considered roughly equivalent to a RSA using 3072-bit key.

Cryptographic protocols are widely used for secure application-level data transport. A cryptographic protocol usually incorporates at least some of these aspects:

Cryptographic protocol

A cryptographic protocol is an abstract or concrete protocol that performs a security-related function and applies cryptographic methods, often as sequences

A cryptographic protocol is an abstract or concrete protocol that performs a security-related function and applies cryptographic methods, often as sequences of cryptographic primitives. A protocol describes how the algorithms should be used and includes details about data structures and representations, at which point it can be used to implement multiple, interoperable versions of a program.

The first implementation of identity-based signatures and an email-address based public-key infrastructure (PKI) was developed by Adi Shamir in 1984, which allowed users to verify digital signatures using only public information such as the user's identifier. Under Shamir's scheme, a trusted third party would deliver the private key to the user after verification of the user's identity, with verification essentially the same as that required for issuing a certificate in a typical PKI.

Delaram Kahrobaei

V. (2020). "Secure and Efficient Delegation of Elliptic-Curve Pairing". Applied Cryptography and Network Security. Lecture Notes in Computer Science

Delaram Kahrobaei is an Iranian-American mathematician and computer scientist. She is a full professor at Queens College, City University of New York (CUNY), with appointments in the Departments of Computer Science and Mathematics. Her research focuses on post-quantum cryptography, and the applied algebra.

As of 2025, quantum computers lack the processing power to break widely used cryptographic algorithms; however, because of the length of time required for migration...

Non-repudiation methods

In this context, security claim or target security level is...

Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. They are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic-curve factorization.

Post-quantum cryptography

Signature Scheme". In Ioannidis, John (ed.). Applied Cryptography and Network Security. Lecture Notes in Computer Science. Vol. 3531. pp. 64–175. doi:10

Post-quantum cryptography (PQC), sometimes referred to as quantum-proof, quantum-safe, or quantum-resistant, is the development of cryptographic algorithms (usually public-key algorithms) that are currently thought to be secure against a cryptanalytic attack by a quantum computer. Most widely used public-key algorithms rely on the difficulty of one of three mathematical problems: the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem. All of these problems could be easily solved on a sufficiently powerful quantum computer running Shor's algorithm or possibly alternatives.

Hash-based cryptography

with Virtually Unlimited Signature Capacity". Applied Cryptography and Network Security. Lecture Notes in Computer Science. Vol. 4521. pp. 31–45. doi:10

Hash-based cryptography is the generic term for constructions of cryptographic primitives based on the security of hash functions. It is of interest as a type of post-quantum cryptography.