


Authenticated cipher

 See *AEAD*.

Axolotl

The original name of the Signal application's end-to-end messaging protocol.

 See *Signal protocol*.




Backdoor

A covert feature to bypass an algorithm or protocol's security. Trapdoors are known by users to exist; backdoors usually are not. A backdoor was once defined as *a feature or defect that allows surreptitious access to data*. A good backdoor must be undetectable, NOBUS (no-one-but-us, or exclusively exploitable by its architects), reusable, unmodifiable, and deniable.

For these reasons, backdoors in cryptographic algorithms are difficult to design and are more easily added in implementations, especially when the internal logic isn't open and hard to deobfuscate. The NSA backdoor in Dual_EC_DRBG is a notable exception. Unfortunately, the most interesting research about backdoors isn't presented at IACR conferences.

Backtracking resistance


Term notably used by NIST to refer to a notion similar to forward secrecy. The opposite of prediction resistance.

 See *Forward secrecy*.

Backward secrecy

The opposite of forward secrecy: backward secrecy is the property that if an attacker compromises some secret keys, future messages remain protected. If an entire system's state is compromised—including long-term and short-term keys as well as any secret state or

counter—backward secrecy is often impossible. An exception is pseudo-random generators, where uncertainty can be brought into the system via reseeding from reliable entropy sources, preventing an attacker from determining future output bits from a past snapshot of the system. In the context of secure messaging, some models assume that an attacker would compromise only certain sets of keys, but not necessarily the entire local secret state: in this case, some form of backward secrecy might be guaranteed.

 See *Forward secrecy*.

BACKWARD SECRECIES

Often defined in an ad hoc manner, the concept of backward secrecy also appeared under the terms *post-compromise security* (in the context of secure messaging), *break-in recovery* (Signal protocol), *future secrecy* (Signal protocol), *healing* (ZRTP), and *prediction resistance* (NIST).

Base64

Not encryption.

BassOmatic

A cipher initially designed by Phil Zimmermann, the creator of PGP, to encrypt data in PGP. It was found to be insecure and replaced by IDEA in 1991. As Zimmermann commented in the source code, “BassOmatic gets its name from an old Dan Aykroyd *Saturday Night Live* skit involving a blender and a whole fish. The BassOmatic algorithm does to data what the original BassOmatic did to the fish.”

BB84

The first quantum key distribution (QKD) construction. It was described by Bennett and Brassard in 1984 and was based on ideas from the concept of quantum money, introduced a year earlier.

bcrypt

A hash algorithm: it doesn’t encrypt. Defined to address the obsolescence of the 1976 crypt utility in the 1999 paper “A Future-Adaptable

Password Scheme.” In this paper, the authors made the following prediction: “Failing a major breakthrough in complexity theory, these algorithms should allow password-based systems to adapt to hardware improvements and remain secure 20 years into the future.”

You can argue that this prophecy was accurate, because you can tune bcrypt to be slow enough to defeat password cracking. On the other hand, bcrypt’s 4KB memory usage is now too low to prevent efficient cracking.


Biclique cryptanalysis

An attack against cryptographic algorithms that works by searching for bicliques. In graph theory, a clique is a subset of nodes that are all connected to each other. A biclique is composed of two subsets of nodes; each node from the first subset is connected to all nodes from the second.

This concept was applied to refine differential attacks on AES and lead to attacks that, in theory, perform fewer operations than a brute-force search (2^{126} instead of 2^{127}). The bicliques used in this context are composed of a first set of bits from the internal state, a second set of bits from the ciphertext, and dependencies between these two sets conditioned by key bits. The idea of the attack is then to identify certain bits of the key as those for which the biclique conditions are satisfied (in terms of XOR differences).

BIKE (Bit Flipping Key Encapsulation)

Sounds like SIKE: also a KEM; also post-quantum, but based on a decoding problem rather than an isogeny problem.

 See *SIKE (Supersingular Isogeny Key Encapsulation)*.

BIP (Bitcoin improvement proposal)

A misleading name, because the most famous BIPs are no longer just proposals but de facto standards that apply to more cryptocurrencies than just Bitcoin. These BIPs include:

- ➔ BIP 32, which defines a tree-based mechanism to derive key pairs and addresses from a secret seed to create wallets of multiple accounts from a single secret value.

- ➔ BIP 44, which assigns semantics to BIP 32 tree levels and defines a syntax for paths within this tree (consisting of purpose, coin type, account, address type, and address index).
- ➔ BIP 39, which defines a representation of a secret value as a high-entropy list of dictionary words, or mnemonic, which is then hashed to a seed that will be the root of a BIP 32 hierarchy of accounts.

Bit Gold


The closest predecessor of Bitcoin.

Bitcoin

An experiment that went out of control, for better or for worse.

Black

In NSA jargon, a key that is encrypted, for example, by using some key wrapping mechanism and therefore that can be exposed on lower security level systems or networks. In the context of data-at-rest protection, black data is classified data that has been encrypted twice using appropriate encryption layers.

 See *EKMS (Electronic Key Management System)*.

BLAKE

A hash function submitted to the SHA-3 competition in 2008. It was one of the five finalists but wasn't selected (the winner was Keccak). BLAKE reuses the permutation of the ChaCha stream cipher with rotations done in the opposite directions. Some have suspected an advanced optimization, but in fact it originates from a typo in the original BLAKE specifications.

BLAKE2

A variant of BLAKE proposed shortly after the end of the SHA-3 competition in 2012. It was adopted in many software applications because it's faster than SHA-2 and SHA-3. Several cryptocurrencies' proof-of-work systems use BLAKE2.

BLAKE3

Another BLAKE variant. It combines a reduced-round BLAKE2 and a Merkle tree construction, making it significantly faster than BLAKE2. BLAKE3 was announced at the Real World Crypto 2020 conference.

Bleichenbacher attack

The epitome of a padding oracle attack. Discovered in 1998 by Daniel Bleichenbacher, this is an adaptive chosen-ciphertext attack against the PKCS#1 v1.5 RSA encryption method. Ironically, Bleichenbacher's attack exploits safeguards against other attacks (the mandatory padding bytes) to craft another attack, which after a few million chosen-ciphertext queries allows an attacker to recover a ciphertext's plaintext.

WHY BLEICHENBACHER IS UNPATCHABLE

Typically, when a software security bug and exploit is found and disclosed, a CVE might be issued, the bug is patched, a new version of the software application is released, and users sooner or later update to the new, corrected version. Of course, not all users will or can update immediately after the new release, but most of the time they eventually do.

Bleichenbacher's attack is different because software can't be patched to prevent it. The only effective mitigation is usually to use a different type of RSA encryption, namely PKCS#1 v2.1, aka OAEP, the evolution of the PKCS#1 standards series.

This is why, although Bleichenbacher published his attack in 1998, it was still exploited 20 years later on vulnerable devices as well as in the DROWN attack on legacy TLS versions.

Blind signature

A signature scheme where the signer (knowing the private key) creates a signature without knowing the number signed in a way that randomizes the value that the private key operation is applied to. This is clearer in the straightforward RSA blind signature construction: instead of using $md \bmod N$, the signer computes $s_0 = m_0 d$ where $m_0 = (m \cdot r) \bmod N$ where r is some random value. You can then get the real signature of m by dividing s_0 by r . Details are left as an exercise for you to complete.

This construction might look familiar because it's the same trick the blinding defense uses against side-channel attacks to prevent attackers from controlling the data the private-key operation processes.

Block cipher

A cipher that transforms a block of data to another block of the same length with a key as a parameter. It must be possible to decrypt the block. So the block cipher operation must be bijective (that is, one-to-one and reversible). That's why block ciphers are also *keyed permutations* or *pseudorandom permutations*.

To encrypt more than a single block, which is usually a 64-bit or 128-bit chunk, you need to use a mode of operation (using the ECB mode is usually a bad idea, CBC is better, and CTR or SIV might be even better).

Blockchain

Both a curse and a blessing to cryptography. Comparable to when a subculture goes mainstream and its pioneers miss the old days, and sadly and bitterly contemplate the newly acquired wealth of those who might not deserve it the most.

THANKS, BLOCKCHAIN?

If blockchain revolutionized anything, it's probably the practice, funding, and deployment of cryptography. Thanks to blockchains, we acquired:

- A wealth of new, interesting, nontrivial problems to solve—problems more exciting than designing an n th block cipher. For example, these problems relate to consensus protocols scalability, proof-of-stake security, transactions anonymity (via zk-SNARKS or bulletproofs), cross-blockchain operations, and so on.
- Innovative solutions being created not to be published at peer-reviewed conference and be later forgotten, but actually technologies being deployed at scale, challenged by real threats and engineering constraints rather than only abstract models.
- Large funding available with minimal bureaucracy and formalism, bypassing the traditional grant application systems and its flaws (slowness, misplaced incentives, and work overhead for researchers).
- Passionate people, some without much formal education let alone a PhD, learning advanced cryptography concepts and creating new solutions to new problems, and implementing them without caring about academic rewards.

Blockcipher

An alternative spelling of block cipher, introduced in research papers by Phillip Rogaway.

Blowfish

A popular block cipher. It owes its recognition to its memorable name and to its designer Bruce Schneier.

BLOWFISH IN HOLLYWOOD

The Blowfish cipher once made it into episodes of the television series

24. Here's an excerpt from the show's script:

Mr. O'Brian, a short time ago one of our agents was in touch with Jack Bauer. She sent a name and address that we assume is his next destination. Unfortunately, it's encrypted with Blowfish 148 and no one here knows how to crack that. Therefore, we need your help, please. (. . .)

Show me the file.

Where's your information. 16- or 32-bit word length? 32.

Native or modified data points? Native.

The designer of this algorithm built a backdoor into his code. Decryption's a piece of cake if you know the override codes.

Of course this dialogue makes little sense, and there's no backdoor in Blowfish. Blowfish is actually a secure block cipher due to the limitation of its 64-bit blocks and the core algorithm in the bcrypt password hashing scheme.

BLS (Boneh-Lynn-Shacham) signature

A signature scheme that leverages elliptic-curve pairings, allowing signatures to be shorter than ECDSA and Schnorr signatures. The reason is that each signature consists of a single group element. That is, for a similar security level as a 512-bit ECDSA signature, a BLS signature would be only 256 bits long.

BLS signatures have the useful property of supporting aggregation, whereby multiple public keys and signatures can be combined into a single public key and a single signature, and batch verification can be done efficiently.

Combined with distributed key generation, you can use BLS signatures to build threshold signature schemes, which proved useful in cryptocurrency applications to distribute transaction signatures.

Bob

Subversive stockbroker and Alice's co-conspirator.

 See *Alice*.

Boolean function

A function whose arguments are binary values (that is, either 0 or 1), and that returns a single 0 or 1 bit. For example, $f(a, b, c) = a + b + ac + bc + 1$, where a , b , and c are binary values, is a Boolean function. Here, the plus sign behaves like XOR (because there are only 0s and 1s in Boolean functions), and ab means a times b , which is equivalent to a logical AND operation (giving 1 if and only if $a = b = 1$).

WHY CRYPTOGRAPHERS CARE ABOUT BOOLEAN FUNCTIONS

Boolean functions look dumb until you notice that you could describe any operation—for instance, a hash function—in terms of only Boolean functions. For example, each bit in the output of a hash function is a Boolean function of the input bits. Such functions only exist in the mathematical ether; they're not explicit most of the time. It's practically impossible to compute their polynomial form, let alone to implement and calculate them.

Nonetheless, there are countless research papers about Boolean functions and their security properties: the reason is that when you break a cryptographic hash or block cipher into pieces (meaning rounds and their sub-components), you'll encounter Boolean functions of a more manageable size—for example, the Boolean functions associated with S-boxes mapping 4-bit blocks to 4-bit blocks. Understanding Boolean functions and their properties, such as nonlinearity and algebraic immunity, has proved critical for designing secure ciphers and breaking weak ones.

Boomerang attack

A differential cryptanalysis technique in which you first *throw* a pair of plaintexts with a given difference into the cipher. You then obtain

two ciphertexts and set another difference in these two ciphertexts to obtain two new ciphertexts. Finally, you *catch* the plaintexts obtained by decrypting them. The boomerang attack is essentially a trick to exploit differential characteristics that only cover part of the cipher.

BQP (bounded-probability quantum polynomial time)

The class of problems that quantum algorithms, and therefore a hypothetical quantum computer, can efficiently solve. BQP contains problems that classical computers can solve efficiently but also problems that today's computers cannot. The latter are problems for which a superpolynomial quantum speedup exists.

THE HIDDEN SUBGROUP PROBLEM

The most remarkable of the BQP problems, as far as cryptography is concerned, is called the *hidden subgroup problem (HSP)*. In particular, cryptographers care about its version for commutative (or Abelian) finite groups. We could solve the following problems if HSP for Abelian groups is easy:

- ☞ Find p and q given $N = pq$
- ☞ Find e given x , p , and $x^e \bmod p$

You recognized these problems—factoring and discrete logarithm—whose hardness is necessary to the security of RSA and elliptic-curve cryptography.

Braid group cryptography


An attempt to build a new type of public-key cryptography using non-commutative groups of elements. Such elements can be viewed as braids with a fixed number of strands, and group operations are computationally efficient. As a side benefit, braid group cryptosystems were expected to be resistant to quantum algorithms. But none of the proposed key agreement schemes proved very cryptographically valuable due to their insufficient security.

Brainpool curves

Elliptic curves designed by the German Federal information security authority (Bundesamt für Sicherheit in der Informationstechnik, BSI). Brainpool curves have some suboptimal security properties, but unlike other standards, they provide a 512-bit curve (rather than a 521-bit one).

Break-in recovery

A notion similar to backward secrecy and indistinguishable from future secrecy. The term was coined in the context of the Signal protocol.

 See *Backward secrecy*.

Broadcast encryption

A type of encryption where the same ciphertext is broadcast to a set of receivers so only authorized ones can decrypt it, and receivers can be revoked to no longer decrypt it. Challenges of broadcast encryption are to be secure against collusion of receivers and to minimize ciphertext and keys' lengths.

APPLICATIONS OF BROADCAST ENCRYPTION

Although broadcast encryption was motivated by pay-TV content protection, it was never deployed: the reasons are mainly due to the prohibitive length of ciphertexts or keys and general unsuitability to receivers' security model, where broadcast encryption only addresses a small part of the problems related to piracy.

But broadcast encryption has been used in the AACS content protection scheme used for Blu-ray Discs. However, it turned out to be of limited effectiveness against piracy, because the content decryption key (which was protected by broadcast encryption) could be extracted from software players.

Brute-force attack

A type of attack that attempts to recover a secret by consecutively trying all the possible values of that secret. You can start a brute-force attack against most ciphers. But as long as the secret is long enough, the attack will never terminate (unless you're impossibly lucky), because there are too many values to try.

Bulletproof

A zero-knowledge proof proposed as an efficient range proof for cryptocurrencies. The major advantage of bulletproofs is that they don't require a trusted setup. Specifically, they don't need an initialization of

the parameters, or *rules of the game*, which must be trusted for the protocol to be secure. Bulletproofs are notably used in Monero.

 See *Range proof*.

Byzantine fault tolerance

An umbrella term for a class of consensus protocols that don't directly rely on mining and proof-of-something. pBFT (and variants thereof) and Tendermint are such protocols; they work by having a fixed number of hosts working together to reliably maintain a common state while distributing trust across hosts.



CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness)

A non-NIST cryptographic competition that took place from 2014 to 2019. Partially funded by but not supervised by NIST, CAESAR identified new authenticated ciphers for several use cases, including *light-weight applications (resource constrained environments)*, *high-performance applications*, and *defense in depth*.

CAESAR'S DEFENSE IN DEPTH FOR Aead

Of the three use cases defined in the CAESAR competition, defense in depth is probably the least obvious to readers. It was also the most interesting in terms of cryptographic engineering, because it was defined as addressing the following needs:

- Authenticity despite nonce repetition
- Limited privacy damage from nonce repetition
- Authenticity despite release of unverified plaintexts
- Limited privacy damage from release of unverified plaintexts
- Robustness in more scenarios, such as huge amounts of data