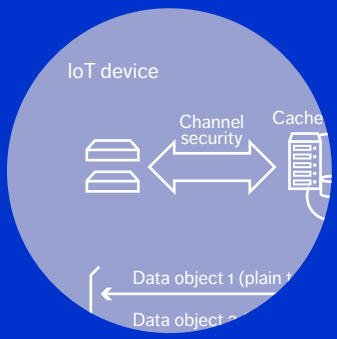
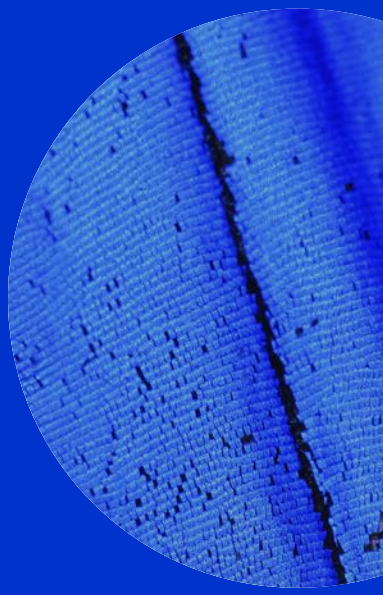
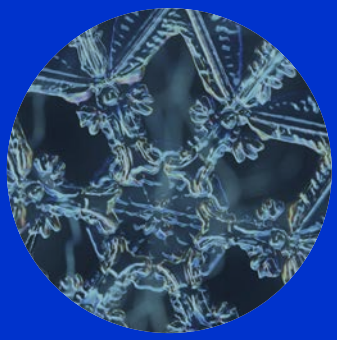
CHARTING THE FUTURE OF INNOVATION VOLUME 92 | #10•2015

Ericsson Technology Review





CRYPTOGRAPHY IN AN ALL ENCRYPTED WORLD



ERICSSON

Cryptography

IN AN ALL ENCRYPTED WORLD

Ensuring that communication is secure, including the ability to encrypt sensitive traffic, has always been a fundamental pillar of the telecom industry. Users expect their right to privacy to be respected, and operators expect to be able to protect themselves and their customers from various kinds of attacks. But the world is changing. Encryption technologies are advancing, regulations are changing, criminals are becoming highly tech savvy, and security awareness has become a popular conversation topic. So, in light of new threats and security demands, security protocols need a shake-up.

CHRISTINE JOST
JOHN MATTSSON
MATS NÄSLUND
BEN SMEETS

TRADITIONALLY, ENCRYPTION has been applied to data carried over the access network – other parts of the network being trusted inherently. But the shift to cloud networking, the increased awareness of threats, exposure of the weaknesses of traditional security algorithms, and the rise in the value of owning data, have all contributed to the need to protect data in all parts of the network, and tighten encryption methods against unwanted intrusion.

In the post-Snowden era, revelations relating to the apparently indiscriminate way pervasive surveillance is carried out have heightened public awareness of privacy issues. Security and privacy have since moved up on the list of top priorities for standardization groups in many industries. Strong reactions to the sabotage of an encryption standard have led to mistrust and eroded confidence in some standards that are widely used to protect data. Our collective dependence on networks has made protecting the data they carry a topic of concern for governments, regulators, and security companies,

but heightened public and media awareness is signaling a move to a more conservative approach.

As the sensitivity of data is not an easily defined concept, many standardization groups, such as the IETF, have chosen to adopt the same approach as modern mobile networks; in other words, encrypt everything – not just data as it is carried over the access network, but over the entire path, end-to-end.

Encryption-enforcing protocols such as HTTP/2, WEBRTC, and TLS 1.3 are essential for OTT service providers. They are also required when operators introduce IMS, VOLTE, RCS, CDN and cloud services on top of the core mobile network.

The increased use of encryption is good for enterprise security and privacy, but comes at the expense of more complicated network management, more complex content delivery optimization, and hampered ability to offer value-added services. Heuristic mechanisms, like those based on the frequency and size of packets, as well as IP-based classification, will help to overcome these difficulties and continue to work well in many cases, even where traffic classification is required.

The global rise in awareness and impending stricter regulations surrounding individual security and privacy requirements have driven the need for communication standards that enable levels of security. Industry use of encryption, however, is being driven by a desire to control delivery end-to-end. For example, enterprises need to be able to avoid potential problems caused by network intermediaries, such as ad injectors or application layer firewalls, ensuring that the integrity and exclusive ownership of valuable analytics data continue to be protected.

Communication security in cellular networks is changing. The algorithms developed by 3GPP and GSMA for confidentiality, integrity, authentication, and key derivation have evolved dramatically since they were first introduced. The original algorithms deployed in 2G/GSM networks were kept secret – security by obscurity – and designed to meet the import/export restrictions related to encryption of the time (early 1990s). These algorithms were subsequently leaked and found to have weaknesses. The encryption algorithms developed for 3G and LTE have been made available for public analysis. They use well-known and standardized cryptographic algorithms such as AES, SNOW, and SHA-3, and to date, no weaknesses have been found. Communication security has not only evolved in terms of how to encrypt data but also what to protect: traditionally, only the access part of the network was encrypted. In today's networks, protection has been extended to cover backhaul, core node communication links using IPSEC or TLS as well as services using SRTP, TLS, DTLS, or through object security provided by, for example, XML encryption.

Complementing protection on trusted interfaces and nodes provides additional assurance against unexpected compromises, secures operational

Terms and abbreviations

ABE–Attribute-Based Encryption | AEAD–Authenticated Encryption with Associated Data| AES–Advanced Encryption Algorithm | CDN–content delivery network | IRTF CFRG– IRTF Crypto Forum Research Group | DTLS–Datagram TLS | ECC–Elliptic Curve Cryptography | ECDSA–Elliptic Curve Digital Signature | GCM–Galois Counter Mode | IOT–Internet of Things | IPSEC–Internet Protocol Security | IRTF–Internet Research Task Force | OTT–over-the-top| PQC–post-quantum cryptography | QUIC– Google's Quick UDP Internet Connections | RCS–Rich Communication Services | RSA–Rivest-Shamir-Adelman cryptosystem | SHA–Secure Hash Algorithm | SNOW–synchronous stream cipher | SRTP–Secure Real-time Transport Protocol | TLS–Transport Layer Security

ownership, and enables end-to-end security – making it easier to create the right services for security-aware customers like the IT department of an organization.

From an ethical standpoint, strong user protection is probably the best guide to how to use security mechanisms in standardization as well as in products. At the same time, law enforcement authorities need to be able to intercept the communication of an individual or of an organization – in other words, networks need to support lawful intercept (LI) authorized by a court order. However, as the application of LI may intrude upon private communication, a trade-off between the overall safety of society and user/enterprise privacy is necessary. In many cases, it is sufficient to supply law enforcement with signaling and/or network management data; access to the actual content of a communication tends to be less frequent. However, in the light of the increasing threat of attack, the scope and concept of LI is changing, and some countries like France and the UK are already amending their regulations.

With the right technical solutions and standards in place, the need for next generation networks to work in an all-encrypted manner is not in conflict with providing value to all stakeholders. However, in a new world where encryption is applied in access networks, as well as in backhaul, core, and for services, new demands are placed on cryptographic primitives and how they are used. Ericsson is therefore actively pushing standardization, and the development of products and services with this goal in mind.

Developments and challenges

As algorithm design and technology develop, giving rise to powerful computers and large memory capacity, the need to strengthen current cryptography methods against brute-force key-recovery attacks has become a widely accepted fact.

At the same time, new capabilities resulting from advances in computing can be applied to increase the strength of encryption algorithms. Aside from the practical issues related to key management, strengthening encryption can be quite simply achieved by using longer keys. However, the heightened security environment of 2015 has drastically altered expectations from individuals and society as a whole. Demand for security and privacy capabilities has soared, and so the requirements placed on cryptographic techniques have risen accordingly. This situation has put existing algorithms into question, leading to efforts to standardize new algorithms and protocols.

Security issues are not the only factor shaping the design of new security protocols and cryptographic algorithms. Performance characteristics like latency and energy efficiency, as well as new business opportunities are significant factors that need to be included in the design. High-performance algorithms need to be developed, and challenges such as providing security in the virtualized world need to be overcome. But how will developments like these affect the ICT industry, and what business opportunities do they bring?

High-performance algorithms and protocols

Some legacy algorithms no longer meet the increased security and performance demands in today's technological environment. In some cases, they are perceived as too slow and consume too much energy. The ability to ensure the security of information is fundamental in an all-encrypted world. Yet in this environment, the performance and efficiency of cryptographic algorithms has become an additional essential, so that systems can deliver the expected service performance with minimum impact on the energy budget.

Keyed cryptographic algorithms come in two varieties: symmetric, and asymmetric (public key), and provide encryption and integrity protection. In a symmetric algorithm, the sender and the receiver share an identical secret key. Symmetric algorithms, such as AES, are relatively fast and are as such often used to protect traffic or stored data. To reveal the key, it would take an attacker 2^n evaluations of the decryption algorithm, where n is the key length, which for AES-128 is 2^{128} evaluations.

In legacy symmetric algorithms, the processes of encryption and integrity protection are separated. By instead combining them, newer AEAD algorithms

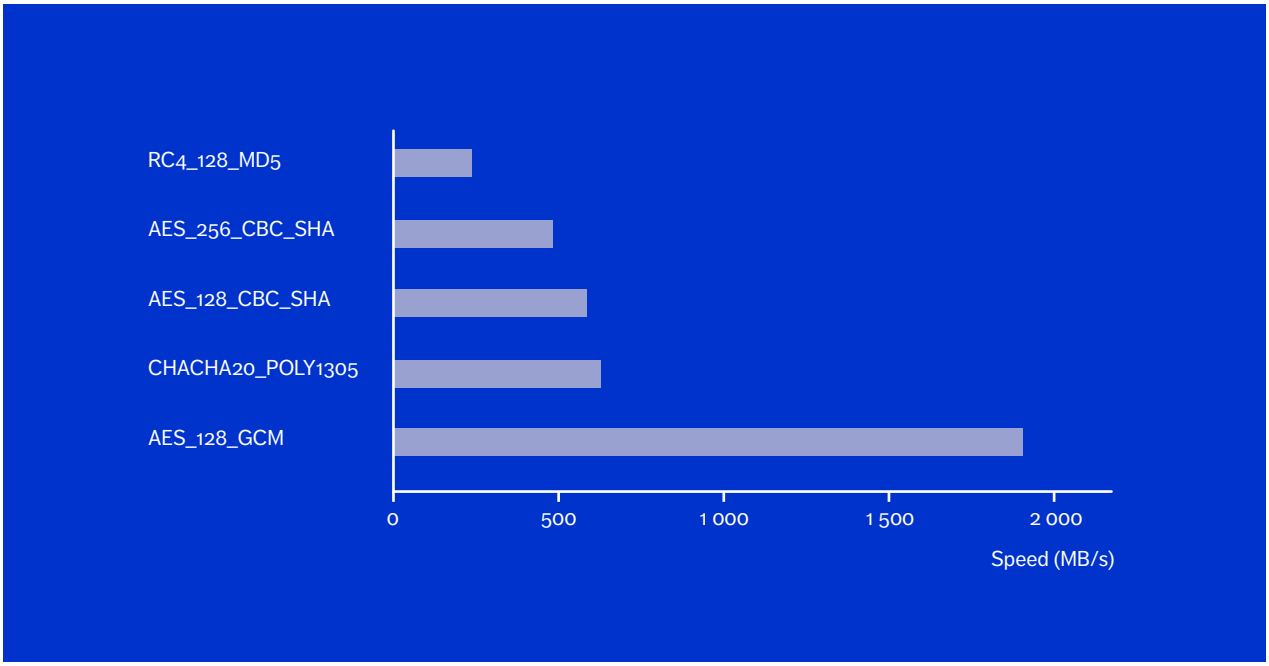


Figure 1
Data rate transfer of various ciphers

achieve huge performance gains over their legacy counterparts. For example, when AES is used in Galois Counter Mode (AES-GCM), it has outstanding performance on modern processors, and is today's solution of choice for many high-end software applications. However, alternative solutions are needed for constrained devices or devices without hardware support for AES. AEAD algorithms, such as AES-CCM or CHACHA20-POLY1305, might be preferable in such cases. To get a feeling for the gains that can be made, TLS 1.2 with AES-GCM is about three times faster than AES-CBC with SHA-1, and can be up to 100 times faster than TLS with 3DES. *Figure 1* shows the performance gains that can be achieved with various ciphers in OPENSSL running on a 2GHz Intel Core i7. In addition to the speed gains that AEAD algorithms can achieve, some of the security weaknesses found in older versions of TLS have also been resolved.

In asymmetric algorithms, data encrypted with the public key can only be decrypted by the private key, and signatures created with the private key can be verified with the public key. As its name implies, the public key is not secret and is freely distributed. Typically, public-key algorithms like RSA and DH are used for authentication and key exchange during session setup, and not for the protection of data traffic; these algorithms are far less performant for bulk encryption compared with symmetric cryptographic algorithms.

Similar to the way AEAD algorithms have led to improved security and performance of symmetric cryptography, Elliptic Curve Cryptography (ECC) is enabling smaller key sizes and better performance for public-key cryptography. The key sizes used in public-key algorithms need to be longer than those used in symmetric algorithms of comparable strength, and are chosen so that recovery takes roughly 2^{128} operations. Such key sizes are said to provide 128-bit security. To provide security at the 128-bit level, the ECC signature algorithm ECDSA (with the NIST P-256 curve) uses significantly smaller key sizes than RSA (256 bits compared with 3072 bits) and delivers significantly better

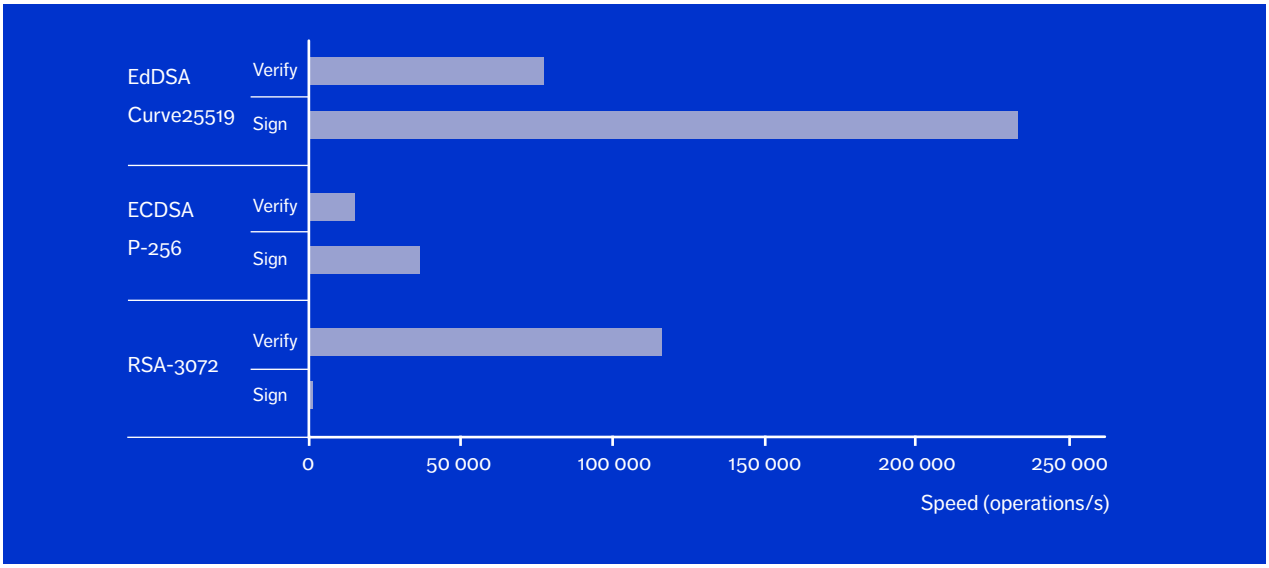


Figure 2:
Signing and verification speeds of 59 byte messages with 128-bit security algorithms on Intel Xeon E3-1275 [3]

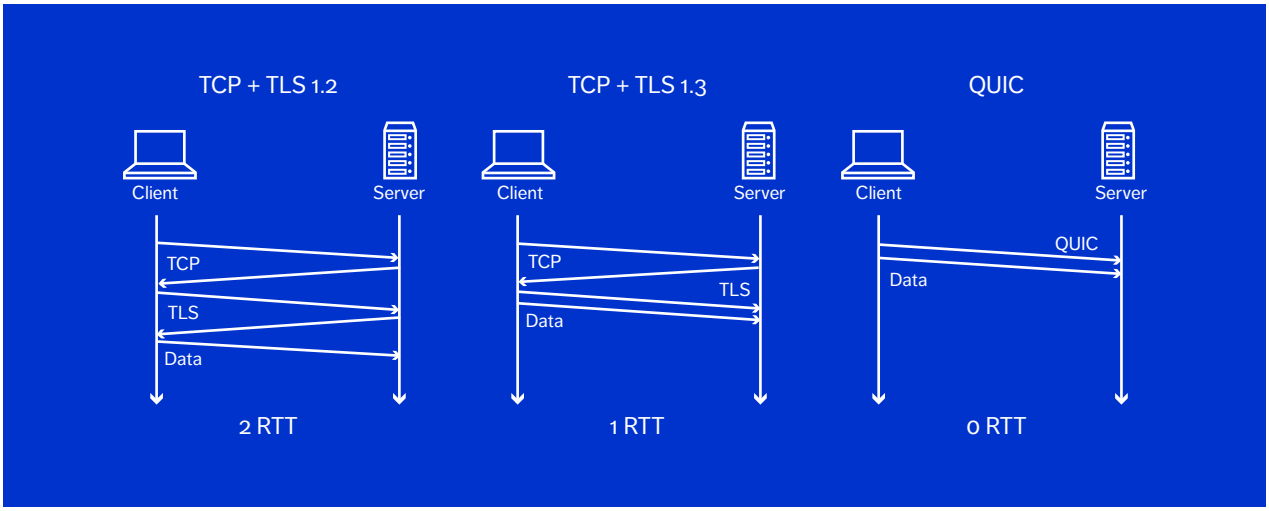


Figure 3:
Repeated connection establishment using TLS 1.2, TLS 1.3, or QUIC

performance in use cases where both signing and verification are needed. The new ECC curves [1] and signature algorithm ED25519 [2] standardized by the IRTF CFRG will further improve the performance of ECC, so that it will be able to offer over 100 times better signing performance than RSA. *Figure 2* shows the performance comparison of ECC to RSA. Not only are new standards such as CURVE25519 and EDDSA much faster than their predecessors, they are also more secure, as their designs take into account two decades worth of security improvement suggestions developed by the scientific community.

New protocols such as TLS 1.3 and the soon-to-be-standardized QUIC significantly reduce connection setup latency by lowering the number of messages needed to complete security association on setup. These protocols disable any options that weaken security and forward secrecy is on by default. Forward secrecy protects a communication session against future compromise of its long-term key. Old versions of TLS, except TCP, required two round trips to set up a connection to a new server, and one round trip for a repeat connection. Newer versions such as TLS 1.3 only use one round trip message exchange to set up a connection to a new server, and no additional trips for subsequent secure connection establishments. QUIC takes this improvement one step further, requiring just a one-directional (client to server) message link to establish server connections. *Figure 3* explains the latency reductions obtained by the improved connection establishment of TLS 1.3 and QUIC.

The ICT industry is in the process of abandoning the use of several legacy algorithms and protocols including 3DES, RC4, CBC-mode, RSA, SHA-1, and TLS 1.1 opting for newer, more secure, and faster algorithms such as AES-GCM, ECC, SHA-2, and TLS 1.2, and later versions.

This shift is embraced in Ericsson's strategy on the use of next generation cryptography and in the product roadmaps. In addition, Ericsson has recently initiated an upgrade of the 3GPP security profiles for certificates and security protocols such as TLS, IPSEC, and SRTP [4]. Ideally, all security should be implemented using efficient and well-tested algorithms that offer a cryptographic strength that is equivalent of at least 128-bit security for AES – even the world's fastest supercomputer, breaking this level of security by brute-force exhaustive search would be expected to take longer than the time that has elapsed since the Big Bang.

IOT and the Networked Society

The two prominent messaging patterns used in IOT device communication are store-and-forward and publish-subscribe. IOT device communication occurs in a hop-by-hop fashion and relies on middleboxes, which limits the possibility for end-to-end security. Traditional transport-layer security protocols, such as DTLS, have difficulty in providing end-to-end data protection for this IOT-type traffic – DTLS, for example, only offers hop-by-hop security. To overcome this issue, fully trusted intermediaries are necessary, which makes it harder to offer IOT communication services to enterprises and governments that are highly security and privacy sensitive.

The debate regarding pervasive monitoring has illustrated the need to protect data even from trusted intermediary nodes – as they can be compromised. To respond to this need, the IETF (supported by Ericsson) is working on object security for the IOT [5] – as illustrated in *Figure 4*. The aim of object security is to provide end-to-end protection of sensitive data, while at the same time enabling services to be outsourced. For example, data collection from a large IOT sensor deployment is a typical service that could be outsourced to a third party.

The security properties of cyber-physical systems (CPSs), such as a smart power grid, are quite different to those of a typical IOT deployment, which tend to contain a mass of sensors. The ability to control a CPS in a secure manner is essential in a world where billions of connected and networked things interact with the physical world. The purpose of a remote-controlled CPS, like a drone or a group of robots, can often be mission-critical. These systems tend to be open or closed-loop controlled, and any denial-of-service attacks such as the blocking, delaying, or relaying of messages can have serious consequences. For example, by relaying messages out-of-band,

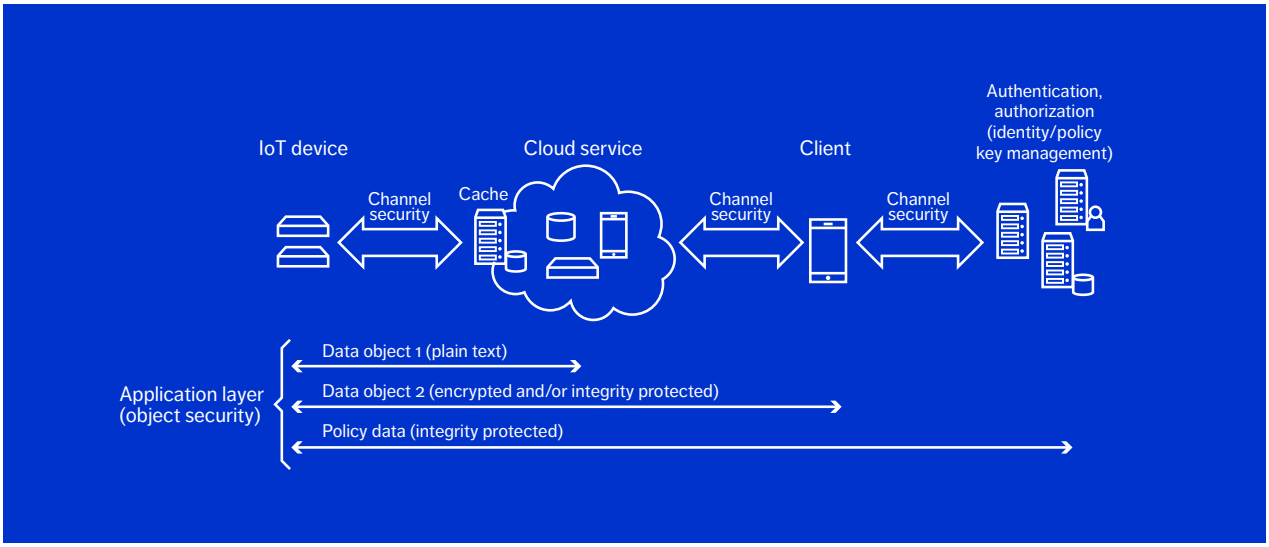


Figure 4:
Object security in the IOT

using say walkie-talkies, attackers can unlock and drive away with exclusive vehicles using automatic car keys based on proximity (an attack that has been executed against real assets).

Cloud data security

In the post-Snowden era, the significance of data security and privacy, as key selection criteria for cloud-infrastructure providers, has risen considerably [6]. To make it easier for organizations to outsource their communication solutions, Ericsson's approach is to push standardization, so that end-to-end protection of content can be combined with hop-by-hop protection of less sensitive metadata [7]. Many cloud-storage providers have adopted client-side encryption to prevent unauthorized access or modification of data, which solves the issues surrounding secure storage and forwarding for cloud data.

Data encryption has other benefits; in many jurisdictions users need to be informed of data breaches unless their information was encrypted. However, encryption does not necessarily mean better compliance with privacy regulations.

Homomorphic encryption is one of the key breakthrough technologies resulting from advances in cryptographic research. In contrast to AES, for example, this approach allows operations to be performed directly on encrypted data without needing to access data in its decrypted form. Unfortunately, fully homomorphic encryption, which includes methods that allow arbitrary computations on encrypted data, have yet to overcome some performance issues. However, a number of specialized methods like partially homomorphic encryption, deterministic encryption, order-preserving encryption, and searchable encryption allow a specific set of computations to be performed on encrypted data, with a sufficient level of performance so that they can be applied to real-life scenarios. By combining these methods, it is possible to cover many types of computations that arise in practice. For example, different proofs of concept have shown that by combining encryption methods, typical SQL operations such as `SUM`, `GROUP BY`, and `JOIN` can be carried out on encrypted databases [8].

Many computations, best outsourced to the cloud, use a restricted set of operations that can be dealt with using these specialized methods with good performance. For example, sums, averages, counts, and threshold checks can be implemented. However, further research is needed to make these methods applicable to real-world use cases. For example, data encryption performance is crucial for use cases with high data throughput. Ericsson's research [9] into the encryption performance of the most popular partially homomorphic cryptosystem (the Paillier system) has shown a performance increase of orders of magnitude, which makes Paillier suitable for high-throughput scenarios.

Specialized methods, like homomorphic encryption, used for carrying out computations on encrypted data, could also be used for preserving confidentiality in cloud computation and analytics-as-a-service. With these methods, clients with large datasets to be analyzed – such as network operators, health care providers, and process/engineering industry players – would be able to outsource both storage and analysis of the data to the cloud service provider. Once outside the client's network, data is encrypted, thereby preserving confidentiality, and allowing the cloud provider to perform analytics directly on the encrypted data. As illustrated in ***Figure 5,*** such an approach enables cloud computation for analysis of confidential data.

Identity and attribute-based encryption

Strong cryptography alone does not work without proper key management. Specifically, management covers how keys are generated and distributed, and how authorization to use them is granted.

Protecting data exchange between n endpoints using symmetric key cryptography requires the secure generation and distribution of roughly n^2 pair-wise symmetric keys. With the breakthrough invention of public key cryptography in the works of Diffie, Hellman, Rivest, Shamir, and Adleman in the mid-1970s, the use of asymmetric key pairs reduced the quadratic complexity, requiring only n key pairs. However, this reduction in the number of keys is offset by the need to often ensure that the public portion of the key pair can be firmly associated with the owner of its private (secret) portion. For a long time, a Public Key Infrastructure (PKI) was the main way to address this issue. But PKIs require management and additional trust relations for the endpoints and are not an optimal solution.

Identity-Based Encryption (IBE) allows an endpoint to derive the public key of another endpoint from a given identity. For example, by using an e-mail address (name.surname@company.com) as a public key, anyone can send encrypted data to the owner of the e-mail address. The ability to decrypt the content lies with the entity in possession of the corresponding secret/private key – the owner of the e-mail address – as long as the name space is properly managed.

Attribute-Based Encryption (ABE) takes this idea further by encoding attributes, for example, roles or access policies, into a user's secret/private keys. IBE and ABE allow endpoints without network connections to set up secure and authenticated device-to-device communication channels. As such, it is a good match for public safety applications and used in the 3GPP standard for proximity-based services for LTE.

Post-quantum cryptography

Although the construction of quantum computers is still in its infancy, there is a growing concern that in a not too distant future, someone might succeed in building much larger quantum computers than the current experimental constructions. This eventuality may have dramatic consequences for cryptographic algorithms and their ability to maintain the security of information. Attack algorithms have already been invented and are ready for a quantum computer to execute on.

For symmetric key cryptography, Grover's algorithm is able to invert a function using only $\sqrt{N}$ evaluations of the function, where N is the number of possible inputs. For a symmetric 128-bit key algorithm, such as AES-128, Grover's algorithm enables an attacker to find a secret key 200 quintillion times faster, using roughly 2^{64} evaluations instead of 2^{128} – the complexity of an exhaustive search. Quantum computing therefore weakens the effective security of symmetric key cryptography by

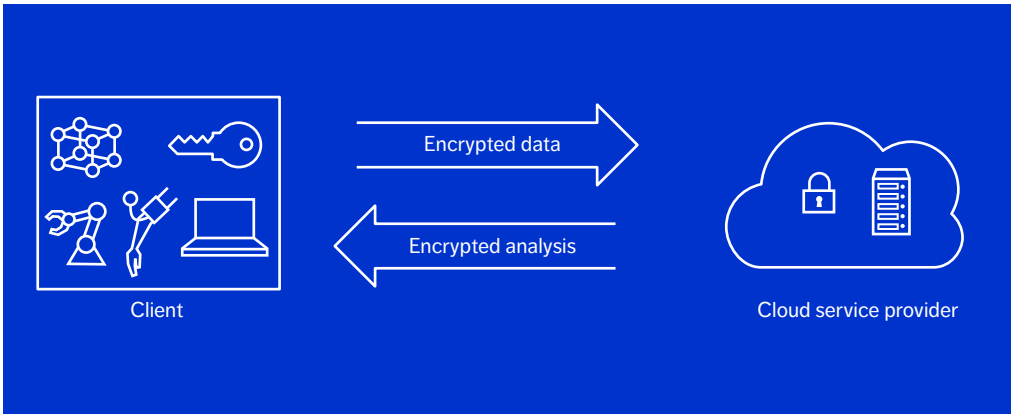


Figure 5: Cloud-based analytics on encrypted data

half. Symmetric key algorithms that use 256-bit keys such as AES-256 are, however, secure even against quantum computers.

The situation for public-key algorithms is worse; for example, Shor's algorithm for integer factorization directly impacts the security of RSA. This algorithm is also effective in dealing with all other standardized public-key crypto systems used today. With Shor's algorithm, today's public-key algorithms lose almost all security and would no longer be secure in the presence of quantum computing. ***Figure 6*** shows the effect of quantum computing on today's algorithms.

Although current research is far from the point where quantum computing can address the size of numbers used today in crypto schemes, the ability to perform quantum computing is increasing. The largest number factored by a quantum computer used to be the integer 21 (3 × 7), but in 2014, a quantum computer factored 56,153 (233 × 241). The term post-quantum cryptography (PQC) is used to describe algorithms that remain strong, despite the fledgling capabilities of quantum computing. In 2014, ETSI organized a workshop on quantum-safe cryptography, and in 2015 the US National Security Agency (NSA) said [10] it would initiate a transition to quantum-resistant algorithms. The potential impact of quantum computing has reached the level of industry awareness.

So, where does research stand today with respect to PQC? Understandingly, most effort is being focused on finding alternatives for the potentially broken public-key algorithms – particularly those that produce digital signatures. In their efforts, researchers follow different tracks such as the use of coding theory, lattices, hash functions, multivariate equations, and supersingular elliptic curves. For example, some schemes go back to ideas set forth by Merkle and use hash functions in Merkle trees as a component. As quantum computing becomes a reality, such schemes would reduce the effective key size by 33 percent, still enabling them to remain practically secure. The challenge for new schemes is to find solutions that have the same properties, such as non-repudiation, that digital signatures have today or provide data integrity with public verification. From this perspective, the blockchain construction used in Bitcoin is interesting. Although Bitcoin itself is not quantum immune, there is an interesting ingredient in its construction: when the chain has grown long enough, the integrity of hash value does not rely on verification against a digital signature but by having it endorsed by many users. By creating a public ledger, any tampering of a hash value is revealed by comparing it with the public value. The idea of a public ledger is significant in the KSI solution [11] for data integrity available in Ericsson's cloud portfolio. Yet the search for PQC schemes that can provide digital signatures with non-repudiation continues.

Today's systems that use or introduce symmetric schemes, should be designed with sufficient margin

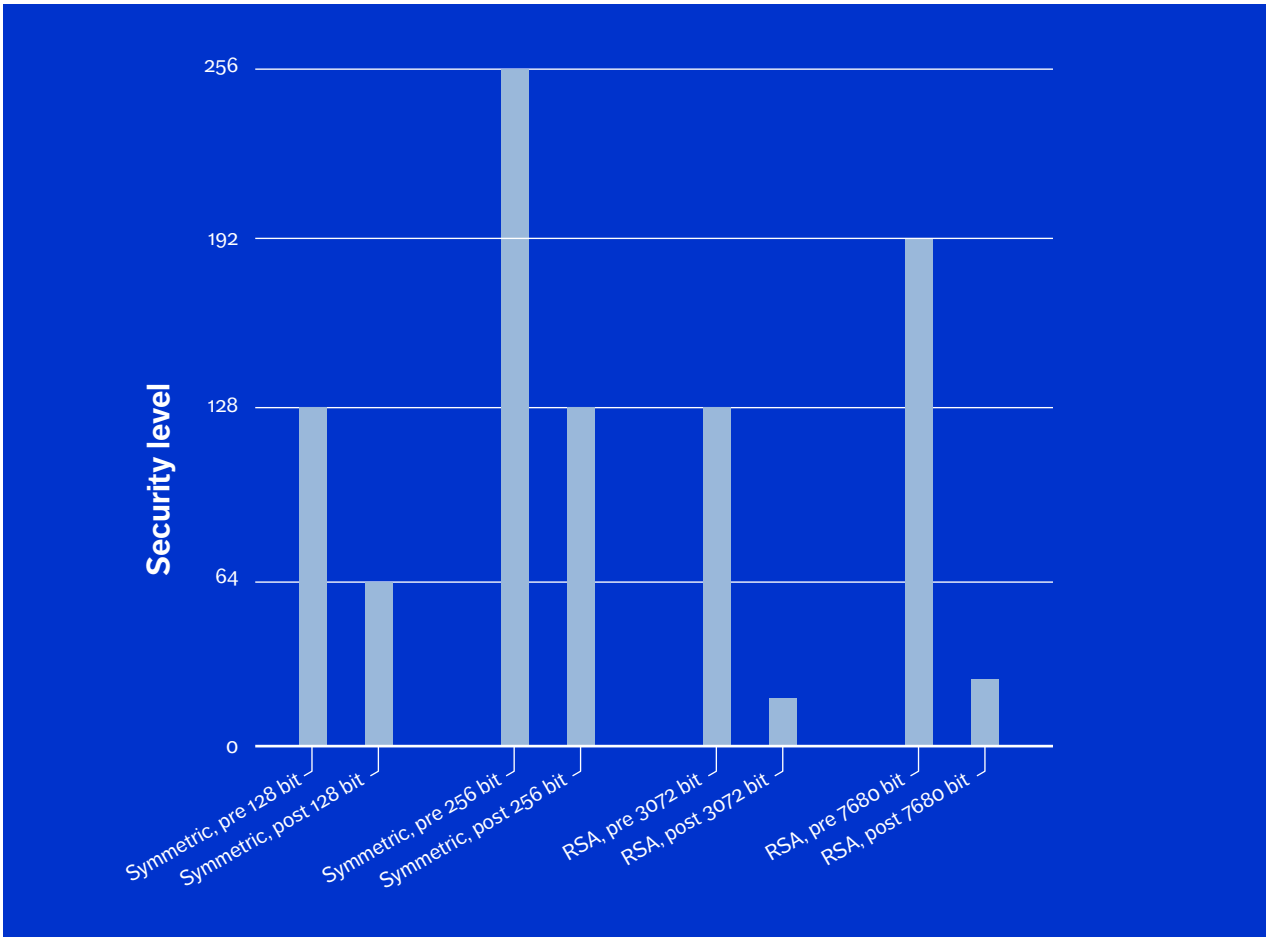


Figure 6:
Relative complexities for breaking cryptographic algorithms before quantum computers and post-quantum computers

in key size, so they can cope with the potential capability of quantum computers. However, just as advances have been made in the fields of computer engineering and algorithm design over the past half-century, developers may well bring us new cryptographic schemes that will change the security landscape dramatically.

Summary

Concerns about security and privacy now rank among the ICT industry's top priorities. For Ericsson, overcoming these concerns is a non-negotiable element of the Networked Society. The world is heading in the direction of comprehensive protection of data (in transit and at rest), where encryption techniques are not just reserved for access networks, but are applied across the entire communication system. This, together with new, more complex communication services places new demands on cryptography technology.

New cryptographic algorithms such as AEAD and ECC overcome the performance and bandwidth limits of their predecessors, in several cases offering improvements of several orders of magnitude. On the protocol side, TLS 1.3 and QUIC significantly reduce latency, as they require fewer round trips to set up secure communications.

Homomorphic encryption may create new business opportunities for cloud-storage providers. Should quantum computers become a reality, the future challenge will be to replace many established algorithms and cryptosystems. Ericsson has a deep understanding of applied cryptography, its implications, and the opportunities it presents for the ICT industry. We actively use this knowledge to develop better security solutions in standardization, services, and products, well in advance of their need in the world.✱

References

1. IRTF CFRG, October 2015, Elliptic Curves for Security, available at: https://tools.ietf.org/html/draft-irtf-cfrg-curves
2. IRTF CFRG, December 2015, Edwards-curve Digital Signature Algorithm (EdDSA), available at: https://tools.ietf.org/html/draft-irtf-cfrg-eddsa
3. ECRYPT, eBACS: ECRYPT Benchmarking of Cryptographic Systems, available at: http://bench.cr.yp.to/results-sign.html
4. 3GPP SA3 Archives, 2015, Update of the 3GPP Security Profiles for tls, IPsec and Certificates, available at: https://list.etsi.org/scripts/wa.exe?A2=3GPP_TSG_SA_WG3;cf1a7cc4.1506C
5. ACE WG, 2015, Object Security of CoAP (OSCOAP), available at: https://tools.ietf.org/html/draft-selander-ace-object-security
6. Gigaom Research, 2014, Data privacy and security in the post-snowden era, available at: http://www.verneglobal.com/sites/default/files/gigaom_research-data_privacy_and_security.pdf
7. PERC, 2015, Secure Real-time Transport Protocol (SRTP) for Cloud Services, available at: https://tools.ietf.org/html/draft-mattsson-perc-srtp-cloud
8. Proceedings of the 23rd ACM,2011, CryptDB: Protecting confidentiality with encrypted query processing, abstract available at: http://dl.acm.org/citation.cfm?id=2043566
9. Ericsson, 2015, Encryption Performance Improvements of the Paillier Cryptosystem, available at: https://eprint.iacr.org/2015/864.pdf
10. National Security Agency, 2009, Cryptography Today, available at: https://www.nsa.gov/ia/programs/suiteb_cryptography/
11. IACR, Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees, available at: https://eprint.iacr.org/2013/834.pdf

THE AUTHORS

Christine Jost

joined Ericsson in 2014, where she has been working with security research,

including applications of homomorphic encryption methods. She holds a Ph.D. in mathematics from Stockholm University, and an M.Sc. in mathematics from Dresden University of Technology in Germany.

John Mattsson

joined Ericsson Research in 2007 and is now a senior researcher. In 3GPP, he has heavily influenced the

work on IMS security and algorithm profiling. He is coordinating Ericsson's security work in the IETF, and is currently working on applied cryptography as well as transport and application layer security. He holds an M.Sc. in engineering physics from the Royal Institute of Technology in Stockholm (KTH), and an M.Sc. in business admin and economics from Stockholm University.

Mats Näslund

has been with Ericsson Research for more than 15 years and is currently a principal researcher. Before joining Ericsson he completed an M.Sc. in computer science and a Ph.D. in cryptography, both from KTH. During his time at Ericsson he has worked with

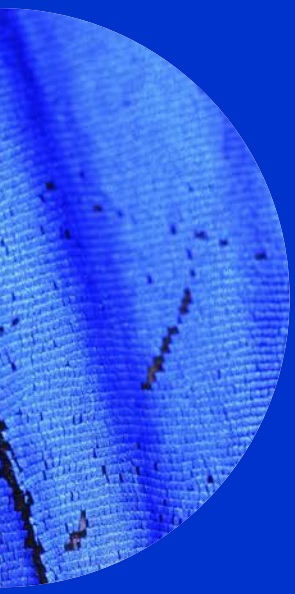
most aspects of network and information security, making contributions to various standards (3GPP/ETSI, IETF, ISO, CSA). He has taken part in external research collaborations such as EU FP7 ECRYPT (Network of Excellence in Cryptography). He is also a very active inventor, and was a recipient of Ericsson's Inventor of the Year Award in 2009. Recently, he was appointed adjunct professor at KTH in the area Network and System Security.

Ben Smeets

is a senior expert in Trusted Computing at Ericsson Research in Lund, Sweden. He is also a professor at Lund University, from where he holds a Ph.D.

in information theory. In 1998, he joined Ericsson Mobile Communications, where he worked on security solutions for mobile phone platforms. His worked greatly influenced the security solutions developed for the Ericsson mobile platforms. He also made major contributions to Bluetooth security and platform security-related patents. In 2005, he received the Ericsson Inventor of the Year Award and is currently working on trusted computing technologies and the use of virtualization.

The authors greatly acknowledge the support and inspiration of their colleagues Christoph Schuba, Dario Casella, and Alexander Pantus



ISSN 0014-0171
284 23-3275 | Uen

Ericsson
SE-164 83 Stockholm, Sweden
Phone: + 46 10 719 0000