IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future
Project No. 863129

Deliverable D3.6.2
Prototype of cryptographic library implementation

The IoT4CPS Consortium:

AIT – Austrian Institute of Technology GmbH

AVL – AVL List GmbH

DUK – Donau-Universität Krems

IFAT – Infineon Technologies Austria AG

JKU – JK Universität Linz / Institute for Pervasive Computing

JR – Joanneum Research Forschungsgesellschaft mbH

NOKIA – Nokia Solutions and Networks Österreich GmbH

NXP – NXP Semiconductors Austria GmbH

SBA – SBA Research GmbH

SRFG – Salzburg Research Forschungsgesellschaft

SCCH – Software Competence Center Hagenberg GmbH

SAGÖ – Siemens AG Österreich

TTTech – TTTech Computertechnik AG

IAIK – TU Graz / Institute for Applied Information Processing and Communications

ITI – TU Graz / Institute for Technical Informatics

TUW – TU Wien / Institute of Computer Engineering

XNET – X-Net Services GmbH

For more information on this document or the IoT4CPS project, please contact:

Mario Drobics, AIT Austrian Institute of Technology, mario.drobics@ait.ac.at

Feldfunktion geändert

Document Control

Title: Prototype crypto implementation

Type: Public

Editor(s): Sebastian Ramacher

E-mail: Sebastian.Ramacher@ait.ac.at

Author(s): Thomas Hinterstoisser (Siemens), Martin Matschnig (Siemens), Sebastian Ramacher (AIT), Raphael Schermann (IAIK), Robert Primas (IAIK), Christoph Striecks (AIT)

Doc ID: D3.6.2

Amendment History

Version	Date	Author	Description/Comments
v0.0	08.05.2020	Sebastian Ramacher	Initial version based on D3.6.1
V0.1	05.06.2020	Robert Primas	Update of ISAP Implementation
V0.2	16.06.2020	Christoph Striecks	Research report on low-latency and scalable cryptography carried out in IoT4CPS
V0.3	22.06.2020	Christoph Striecks	More technical details on the research output
V0.4	23.06.2020	Sebastian Ramacher	Details on forward-secret 0RTT key-exchange integration in OpenSSL
V0.5	26.06.2020	Christoph Striecks	Final adjustments, review of the document

The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.

Federal Ministry
Republic of Austria
Transport, Innovation
and Technology

FFG
Forschung wirkt.

Content

Abbreviations

FPGA	Field-Programmable Gate Array
DPA	Differential Power Analysis
COTS	Component Off-The-Shelf
ASIC	Application-specific integrated circuit
BFE	Bloom Filter Encryption
TLS	Transport Layer Security
0-RTT	0 round trip time
DPA	Differential power analysis
IND-CCA	Indistinguishability under chosen-ciphertext attacks
IoT	Internet of Things

Executive Summary

This deliverable describes the prototype implementations of the cryptographic primitives and protocols used as part of IoT4CPS. It will cover two implementations: First, we discuss the implementation of forward-secure zero round-trip time (0-RTT) key exchange protocols based on bloom filter encryption. The library implements the bloom filter encryption scheme which is also integrated as part of the widely-used TLS library OpenSSL. Thereby, we obtain an extension of the TLS protocol that allows resource constraint devices operating as clients to send data via a secure channel to a server without waiting for the server's reply. Latency is thus significantly reduced since it is no longer necessary to wait for the full handshake to be completed. Additionally, we discuss the research carried out in the IoT4CPS project on low-latency and scalable cryptography (in line with the WP3 and project objectives) resulting in three works currently under submission [26,27,28] extending bloom-filter encryption for more efficient and long-term secure 0-RTT key exchange as well as enhancing scalable (identity-based) key exchange with fine-grained access control and forward secrecy.

Secondly, the implementation of the authenticated encryption scheme ISAP for FPGAs and ASICs is reported. This scheme is especially useful for constraint devices, since ISAP allows on the one hand for fast software implementations, but more importantly in the context of IoT4CPS, also for fast and compact hardware implementations. Additionally, ISAP is designed to be resistant against passive side-channel attacks such as timing attacks, differential power analysis, and also against active attacks including fault attacks. This implementation will then later be integrated into a deployment consisting of legacy hardware which is already operating for many years and which cannot be replaced by new more powerful hardware. The ISAP core will be responsible for encrypting and decrypting data streams on the fly without requiring any changes to the remaining architecture and thus adds confidentiality and authenticity to the legacy system.

1. Introduction

Cryptographic solutions play a crucial role in enabling security in modern distributed systems, such as the Internet of Things (IoT). Most importantly, they ensure secure communication between all the participants of the system even when they have to communicate over the internet or other untrusted networks. Thereby, it can be ensured that all the transmitted data stays confidential against an attacker and, furthermore, the authenticity of the data is also guaranteed. To obtain these security guarantees, multiple different types of cryptographic primitives need to be integrated into the system: authenticated encryption for confidential and authentic data transfer, key exchanges to establish the key material used for the encryption scheme, and digital signatures to verify identities of the participants. Besides the standard security notions (c.f. D3.5) these schemes have to fulfill, the increasing abilities of attackers require more sophisticated schemes. From a cryptographic protocol point of view, a secure communication channel is required to be forward-secret, meaning that even if an adversary records all the network traffic and at some later point learns the involved key material of one channel, the security of all other channels remains intact, though. This feature can be achieved by building protocols based on forward-secret key exchange protocols, i.e. they produce completely fresh and independent shared keys for every execution of the key exchange protocol. In practice, also implementation-specific features become important. For example, implementations of the cryptographic schemes may suffer from side-channel attacks, i.e., attacks that are able to break the security of a system using data from the implementation such as timing data, power usage, or errors due to injected faults. Therefore, implementations are required to be resistant to these types of attacks. For example, software implementations are required to be constant-time, i.e., their runtime does not depend on any secret keys, or hardware implementations need to be resistant to power analysis and fault attacks.

These additional features come at a cost. They are more expansive in runtime, require more memory, or their hardware implementation leads to a higher hardware utilization. Therefore, efficient implementations are of particular importance to show that the primitives, protocols and schemes developed in theory, are indeed useful for applications in practice. Yet, in certain use-cases, e.g., use-cases involving strict hardware constraints, a straight-forward reference implementation of the primitives is often not enough. Instead, the implementations have to be adapted to these constraints. This often implies that implementations have to be built from the bottom up as programming paradigms differ between a typical desktop computer, smartphone or embedded devices in an IoT scenario. For example, when considering application-specific integrated circuit (ASIC) or field-programmable gate array (FPGA) implementations, a higher level of parallelism might change the performance picture completely [1]. On the other hand, a large number of constants or temporary variables become problematic when memory is scarce such as on embedded platforms.

We further describe cryptographic research carried out in the context of IoT4CPS. In consent with the concrete project and WP objectives regarding low-latency and scalable cryptography (including identity-based techniques), this results in:

1. A more efficient low-latency and forward-secure key-exchange scheme [26].
2. A low-latency and forward-secure identity-based scheme for a more scalable key-exchange scheme with fine-grained access control [27].
3. A post-quantum (i.e., long-term) secure low-latency key-exchange scheme from generic identity-based cryptography techniques [28].

The deliverable is structured as follows. In Section 2, we give an overview on the implementation of the forward-secret 0-RTT key exchange protocol by Derler et al. [2]. We present the current progress on the implementation of a software library in the C programming language and describe its integration in the handshake of the Transport Layer Security (TLS) protocol. Additionally, we discuss the implementation of this extension in OpenSSL. We also present research results obtained on scalable and low-latency cryptography in this section. In

Section 3, the focus lies on the lightweight authenticated encryption scheme ISAP [7]. There, we discuss the implementation progress of an ASIC/FPGA implementation and its integration in the demonstrator.

2. C Library for Forward-Secret 0-Round Trip Time Key Exchange

Key exchange protocols are essential for establishing secure communication channels over a (potentially untrusted) network. They enable two parties, that do not share a-priori established secret-key material, to establish a shared secret. This shared secret then serves as basis to derive secret keys for authentication encryption, providing confidential and authenticated communication between the two parties. Such key exchange protocols are then integrated into more complex protocols such as Transport Layer Security (TLS) version 1.3 [5] or Secure Shell (SSH). Currently, ephemeral Diffie-Hellman (EDH) key exchange is used in these protocols to provide forward-secret session key establishment, which is then used to derive all other keys required by the protocol.

2.1 Forward-Secret Key Exchange in TLS 1.3

In TLS 1.3, keys are established during the so-called handshake which describes the initial phase of the protocol (see Figure 1). First, a client sends a ClientHello message announcing its supported TLS versions, algorithms, etc. This message already includes the client's key share of the Diffie-Hellman key exchange protocol. When the server receives the client's message, it checks the supported algorithms and selects the suitable one. It then replies with a ServerHello message announcing the choice. The ServerHello message also contains the server's key share. The server can already compute the shared secret from the DH key exchange. The client, however, must wait until it received the server's answer. Once both parties completed the DH key exchange, the remaining handshake is already performed in an encrypted fashion. At the end of the handshake, client and server can optionally derive a shared secret that they can store and re-use for the next TLS connection between the same two parties. If the client then decides to use this shared secret on the next connection as pre-shared secret key (PSK), TLS 1.3 provides the possibility to send encrypted application data already after the ClientHello message. In this case, the PSK is used to derive the secret keys required for encryption. If one of the two parties are no longer in possession of this key, they fall back to the normal handshake.

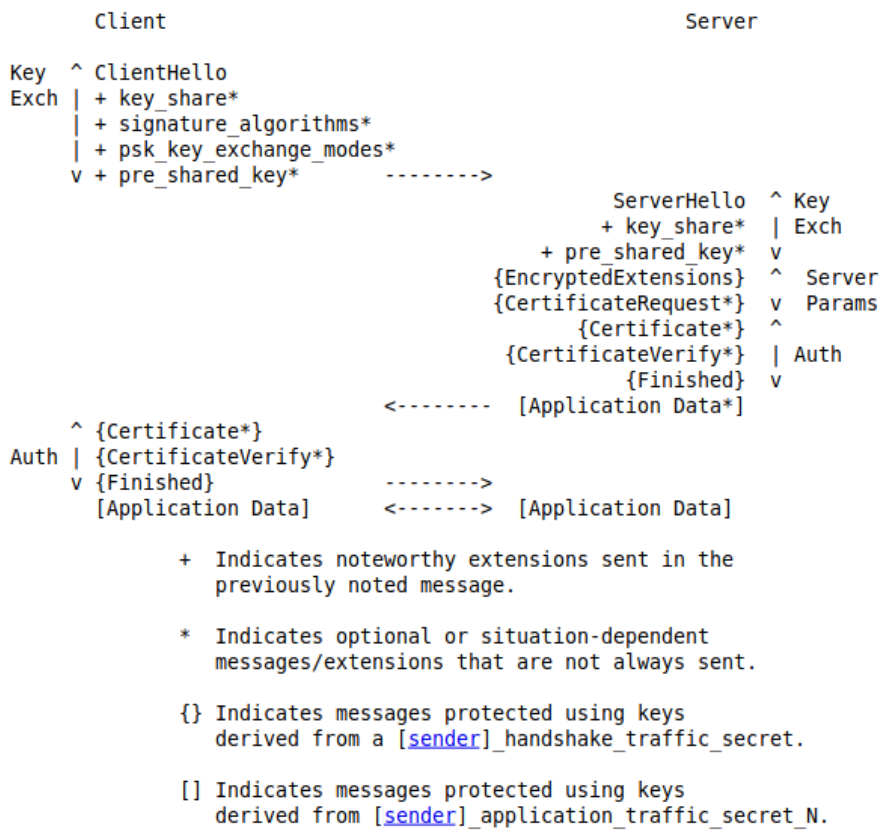

Figure 1: TLS 1.3 handshake [5]

As discussed above, EDH has the drawback that the key exchange requires one round-trip. Only after the two shares have been exchanged, the shared key can be derived and thus a secure channel be established. Recent work has explored alternatives to the PSK-based approach to reduce the number of round trips. In particular, the possibility to reduce the complexity to zero round trips using puncturable public-key encryption (PPE) or puncturable key encapsulation mechanisms (PKEM) has been investigated. In such a protocol, the client essentially encrypts a session key with respect to the public key of the server, and then sends it to the server. Therefore, the client can immediately start sending encrypted application data using the session key. The server decrypts the session key and can use the key as well. Note that, if such a protocol would be built trivially from public-key encryption, then the protocol would not provide forward secrecy. The latter is achieved by puncturing the secret key used to the decrypt the ciphertext in a way, that the server can no longer decrypt ciphertexts from past sessions. Besides providing forward secrecy, puncturing the key also provides replay protection.

This new approach (see Figure 2) requires that the client already knows the public key of the server before establishing the connection. In the context of IoT, we observe that often clients communicate only with a pre-configured server. Therefore, the public key of the server can already be deployed during provisioning of the devices (cf. D3.4). In the case, this is not possible, only during the first connection between a client and the server

a non-0-RTT key exchange has to be performed. The client will receive the public key during this connection and can store it for future use.

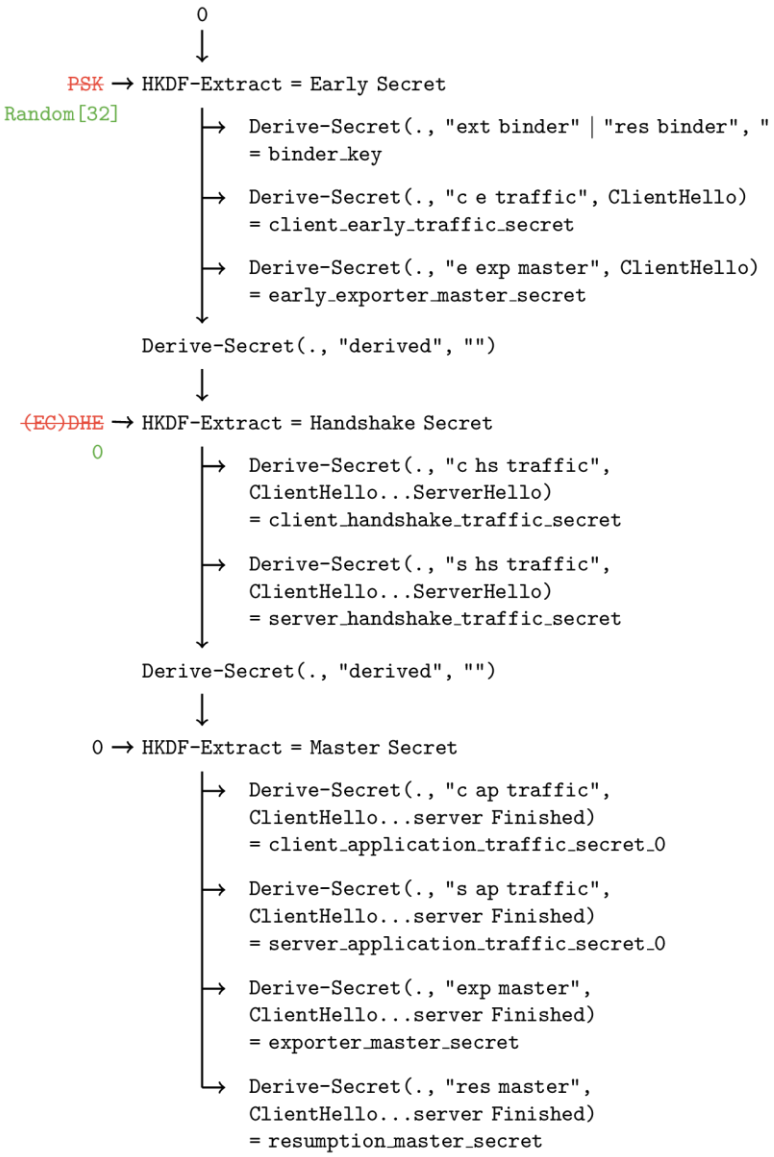

Figure 2: Potential modification of the key derivation in TLS when deploying BFE [19]

For the upcoming integration in TLS 1.3, we focus on a specific choice of such a forward-secret 0-RTT key exchange protocol, namely the one from Derler et al. [2]. Their protocol builds on top of bloom filter encryption (BFE). The idea there is that the ciphertexts have an attached tag which determines the key. The keys themselves are managed in a bloom filter. Once they are used and the corresponding bit is set in the bloom filter, the keys are removed and can no longer be used for decryption.

2.2 Bloom Filter Encryption Library

We provide an implementation of the IND-CCA secure version of BFE in the C programming language compatible with C11 [25].[1] The implementation explores the construction based on the Boneh-Franklin[2] identity-based encryption scheme [3] for BFE made CCA-secure using the Fujisaki-Okamoto transformation [13]. Derler et al. also provide time-based BFE built from Boneh-Boyen-Goh hierarchical identity-based encryption [6], which we indent to investigate at a later point.

The library includes a documentation produced with the help of doxygen [16]. The documentation also presents examples of the typical usage. The correctness of the implementation is tested with the unit testing framework Cgreen [17]. The library also includes an implementation of the interface for PKEMs as described in D3.5. In Figure 3, Figure 4, Figure 5 and Figure 6, the usage of the PKEM API is demonstrated.

```
// the public key
unsigned char pk[CRYPTO_PUBLICKEYBYTES];
// the secret key
unsigned char* sk = malloc(CRYPTO_SECRETKEYBYTES);

// generate key pair
if (crypto_kem_keypair(pk, sk)) {
  // handle error
}
```

Figure 3: Key generation

```
// the public key
unsigned char* pk;

// the ciphertext
unsigned char ct[CRYPTO_CIPHERTEXTBYTES];
// encapsulate a new key
unsigned char k[CRYPTO_BYTES];
if (crypto_kem_enc(ct, k, pk)) {
  // handle error
}
```

Figure 4: Key encapsulation

[1] The library is available on Github: https://github.com/sebastinas/bfe-bf.

[2] As in [2], we implement hashed Boneh-Franklin in the type 3 bilinear pairings setting.

```
// the secret key
unsigned char* sk;
// the cipher text
unsigned char* ct;

// decapsulate key
unsigned char k[CRYPTO_BYTES];
if (crypto_kem_dec(k, ct, sk)) {
  // handle error;
}
```

Figure 5: Key decapsulation

```
// the secret key
unsigned char* sk;
// the cipher text
unsigned char* ct;

// puncture secret key with respect to a ciphertext
if (crypto_kem_punc(sk, ct)) {
  // handle error;
}
```

Figure 6: Puncturing of the secret key

Alternatively, the library also provides an API that is more suitable for the use on the server side. This API allows users to control serialization and deserialization of the key material and ciphertexts explicitly. Thereby, the server can keep the relatively large secret key in memory without having to serialize and deserialize it all the time. An additional advantage is that this API also allows users to provide their choice of parameters for the bloom filter. Usage of this API is demonstrated in Figure 7, Figure 8, and Figure 9.

```
bfe_bf_secret_key_t sk;
bfe_bf_public_key_t pk;

// generate new keys
bfe_bf_init_secret_key(&sk);
bfe_bf_init_public_key(&pk);
if (bfe_bf_keygen(&pk, &sk, 32, 1 << 19, 0.0009765625)) {
  // handle error
}

// serialize public key
uint8_t serialized_pk[bfe_bf_public_key_size()];
bfe_bf_public_key_serialize(serialized_pk, &pk);

// serialize secret key
uint8_t* serialized_sk =
      malloc(bfe_bf_secret_key_size(&sk));
bfe_bf_secret_key_serialize(serialized_sk, &sk);

// clean up keys
bfe_bf_clear_secret_key(&sk);
bfe_bf_clear_public_key(&pk);
```

Figure 7: Key generation with explicit choice of the parameters and serialization of the keys

```
// the serialized public key
const uint8_t* serialized_pk;
bfe_bf_public_key_t pk;

// deserialize the public key
if (bfe_bf_public_key_deserialize(&pk, serialized_pk)) {
  // handle error
}

// encaps a new key
bfe_bf_ciphertext_t ciphertext;
bfe_bf_init_ciphertext(&ciphertext, &pk);
uint8_t key[pk.key_size];
if (bfe_bf_encaps(&ciphertext, K, &pk)) {
  // handle error
}

// serialize the ciphertext
const size_t csize = bfe_bf_ciphertext_size(&ciphertext);
uint8_t serialized_ct[csize];
bfe_bf_ciphertext_serialize(serialized_ct, &ciphertext);

// clean up
bfe_bf_clear_ciphertext(&ciphertext);
bfe_bf_clear_public_key(&pk);
```

Figure 8: Encapsulation of a new key and serialization of the ciphertext

```
// the serialized secret key
uint8_t* serialized_sk;
// the serialized public key
const uint8_t* public_key
// the serialized ciphertext
const uint8_t* serialized_ct;

// deserialize the secret key
bfe_bf_secret_key_t sk;
if (bfe_bf_secret_key_deserialize(&sk, serialized_sk)) {
  // handle error
}

// deserialize the public key
bfe_bf_public_key_t pk;
if (bfe_bf_public_key_deserialize(&pk, serialized_pk)) {
  // handle error
}

// deserialize the ciphertext
bfe_bf_ciphertext_t ciphertext;
if (bfe_bf_ciphertext_deserialize(&ciphertext,
      serialized_ct)) {
  // handle error
}

// decaps ciphertext
uint8_t key[pk.key_size];
if (bfe_bf_decaps(key, &pk, &sk, &ciphertext)) {
  // handle error
}

// puncture secret key and serialized it again
bfe_bf_puncture(&sk, &ciphertext);
bfe_bf_secret_key_serialize(seralized_sk, &sk);

// clean up
bfe_bf_clear_ciphertext(&ciphertext);
bfe_bf_clear_public_key(&pk);
bfe_bf_clear_secret_key(&sk);
```

Figure 9: Decapsulation of a key and puncturing of the secret key including deserialization

We will briefly describe some implementation aspects of the concrete BFE scheme. As Boneh-Franklin is a pairing-based scheme, we require a pairing implementation. We have chosen the highly optimized open-source pairing library RELIC [12]. This library is good choice for multiple reasons: (1) it includes implementation of currently recommended pairing-friendly curves such as BLS12-381,[3] (2) includes optimizations for desktop and server CPUs as well as embedded CPUs such as ARM and AVR processors, and (3) allows to configure memory handling suitable for the target platform. Note however, that a specific build of RELIC only supports one specific pairing-friendly elliptic curve, hence our implementation also does not provide any flexibility in choosing the curve.

Next, random oracles are required for applying the Fujisaki-Okamoto transformation. They are implemented via SHAKE [14]. Similarly, the hash functions used as part of the Bloom filter are implemented with SHAKE as well.[4] We have integrated the open-source implementation optimized for 64-bit systems [15]. The code package also includes many different implementations for other targets which can be selected depending on the target platform. When switching to a different platform, the BFE library just has to be built with a SHAKE implementation that is optimized for this platform to obtain the best results. No changes to the code-base of the library itself are required to adopt to this change.

Table 1 gives one choice of parameters for using the BFE library. The parameters are chosen in such a way that a TLS server can support one entirely new TLS connection per second over a timeframe of three months with an error probability of less than 2^{-10}. After this time period, a new key pair on the TLS server has to be generated. Note though, that the current TLS infrastructure is moving towards regenerating keys and reissuing certificates every three months due to the rise of Let's Encrypt [21].

Table 1: Potential choice of parameters for the BFE library

Parameter	Value
n (size of the Bloom filter)	524288
p (false-positive probability)	0.0009765625
Pairing-friendly elliptic curve	BLS12-381 (-DFP_PRIME=381 when building RELIC)

2.3 Benchmarks

Table 2 details the performance of the library using the parameters from Table 1. The benchmarks were performed on an Intel Core i7-8650U with 3 GHz and 16 GB of RAM. As expected, puncturing of the secret key is very efficient – it only requires removal of a specific subkey of the secret key. The key generation is slow, but it is never performed on a resource-constraint device. Decryption is little slower than encryption due to the nature of the Fujisaki-Okamoto transform.

Table 2: BFE library benchmark

Algorithm	Time (in ms)
KeyGen	941,857.77
Encrypt	3.66

[3] According to recent security estimations [18], this curve provides about 120 bits of security.

[4] Technically, collision-resistance and pre-image resistance are not required. To have well distributed Bloom filter indices we erred on the safe side and chose SHAKE. More lightweight hash functions with a close to uniform distribution would work as well.

Decrypt	4.94
Puncture	0.01

In Table 3, we present sizes of the secret key, the public key and the ciphertexts for the parameters given in Table 1. Note that the secret key shrinks with each puncturing as parts of it get deleted and no longer need to be stored.

Table 3: Key and ciphertext sizes

Type	Size (in bytes)
Secret key	101,253,128
Public key	109
Ciphertext	453

2.4 Integration into OpenSSL

For easier integration into existing applications and demonstrators, the BFE library was integrated into OpenSSL[5] as it is one of the most commonly used libraries for TLS which also provides TLS 1.3 support.[6] The integration follows the general outline of Section 2.1 where the BFE-based key exchange is implemented as a TLS extension. Additionally, the Diffie-Hellman-based input to the key derivation is not discarded or removed from the handshake, as the DH share is mandatory in a TLS 1.3 handshake.

The extension is defined in the following way:

- The client sends the current interval as 64 bit integer and the ciphertext.
  - uint64_t interval
  - uint8_t ciphertext[ciphertext_size]
- The server replies with a flag indicating whether it could successfully process the ciphertext.
  - uint8_t state: FS_0RTT_KEX_STATE_KEY_RECEIVED (server was able to decrypt the ciphertext), FS_0RTT_KEX_STATE_INVALID_CTX_RECEIVED (server was unable to decrypt the ciphertext), FS_0RTT_KEX_STATE_NOT_SUPPORTED (server does not support the extension)

The BFE key as master key for the session as indicated in Figure 2. In terms of OpenSSL, this means that a session is created based on that key. If the server replies with a state other than FS_0RTT_STATE_KEY_RECEIVED, the handshake must be re-started as it can happen with other errors during the handshake indicated by an HelloRetryRequest message by the server. If the server replied with FS_0RTT_KEX_STATE_NOT_SUPPORTED, the client must retry with the extension disabled, since the server is unable to process it correctly.

The implementation adds explicit functions to enable the FS-0RTT key exchange and to load the corresponding key material to OpenSSL:

- void SSL_CTX_enable_fs_0rtt_kex(SSL_CTX* ctx, int enable): enable FS-0RTT key exchange.

[5] OpenSSL version 1.1.1d as available in the Debian buster software repository was chosen as baseline, since the XNET demonstrator runs on Debian buster.

[6] The code is available on Github: https://github.com/sebastinas/openssl-bfe

- Int SSL_CTX_load_fs_0rtt_kex_pkey_from_file(SSL_CTX* ctx, const char* file): load public key from a file
- int SSL_CTX_load_fs_0rtt_kex_skey_pkey_from_file(SSL_CTX* ctx, const char* file): load key pair from a file

For an application to use the fs-0RTT key exchange extension, the application has to enable and load the respective keys. To ease integration with existing applications, the environment variables FS0RTT_SKEY (on the server side) and FS0RTT_PKEY (on the client side) can be set instead. In this case, the keys are loaded from the files referenced by these variables and the key exchange is enabled.

For the generation of the keys, OpenSSL is extended with an application to handle keys used for the extension: openssl fs0rtt. As arguments it accepts filenames for the public key (-pkey) and secret key (-skey). Additionally, the hostname needs to be specified via -hostname.

2.5 Discussion

In the context of IoT4CPS, this choice of parameters leads to some constraints when deploying the library in practice. First, the approach is only suitable when resource-constraint devices connect to more powerful servers that can hold (and generate) the large secret keys used in this scheme. On the client side, one can actually reduce the requirements: while any PSK-based solution would require secure storage for the PSK, this is not necessary in our case. Only the server's public key needs to be stored on the client. Since the public key can be verified at any time via a certificate chain, no special secure storage is required to store the public key. The clients need to be able to receive new public keys if the server's key changes, however. For example, updates of the public key can be distributed by performing one classical TLS handshake and storing the received public key. Note though, this requirement does not infer an additional constraint: clients need to be prepared to handle new public keys in case keys need to be rolled over for other reasons, e.g., due to key compromise. Additionally, for deployments where a software implementation of the pairing might not be efficient enough, a co-processor providing elliptic curve operations and the pairing evaluation is an option to speed up the protocol even further [20]. Similarly, the SHAKE implementation can be replaced with a suitable co-processor or FPGA version [22,23,24]

2.6 Research on Low-Latency and Scalable Cryptography in IoT4CPS

In this section, we describe cryptographic research carried out in the context of IoT4CPS. In consent with the concrete project and WP objectives regarding low-latency and scalable cryptography (including identity-based techniques), this results in:

1. A more efficient Bloom-Filter Encryption (BFE) scheme with shorter ciphertexts [26] building on the work by Derler et al. [2], for more efficient low-latency key exchange. Currently in submission. (See 2.6.1 for more details.)
2. An identity-based Puncturable Encryption scheme, dubbed Dual-Form Puncturable Encryption (DFPE) scheme, to have a more scalable encryption scheme with fine-grained access control and strong security guarantees such as forward secrecy [27]. Currently in submission. (See 2.6.2 for more details.)

While progressing with the IoT4CPS project, the aspect of long-term security (i.e., security even against powerful quantum computers) came up. This particular includes so-called post-quantum cryptography equipped with low latency guarantees and forward secrecy. Consequently, to progress with project's research output, we explored the topic of enhancing BFE (see 1. above) with post-quantum security guarantees and achieve:

3. A post-quantum secure BFE instantiation from identity-based cryptography techniques. Furthermore, we are able to reduce the decryption error generically present in many only weakly secure post-quantum key encapsulation mechanisms from the literature and show strongly secure variants thereof [28]. Currently in submission. (See 2.6.3 for more details.)

2.6.1 Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange

As also discussed above, forward secrecy is considered an essential design goal of modern key exchange (KE) protocols, such as TLS 1.3. Furthermore, efficiency considerations such as zero round-trip time (0-RTT), where a client is able to send cryptographically protected payload data along with the very first KE message, are motivated by the practical demand for secure low-latency communication.

For a long time, it was unclear whether protocols that simultaneously achieve 0-RTT and full forward secrecy exist. Only recently, the first forward-secret 0-RTT protocol was described by Günther et al. (Eurocrypt 2017). It is based on Puncturable Encryption. Forward secrecy is achieved by "puncturing" the secret key after each decryption operation, such that a given ciphertext can only be decrypted once (cf. also Green and Miers, S&P 2015). Unfortunately, their scheme is completely impractical, since one puncturing operation takes between 30 seconds and several minutes for reasonable security and deployment parameters, such that this solution is only a first feasibility result, but not efficient enough to be deployed in practice.

Derler et al. [2] introduce a new primitive that termed Bloom Filter Encryption (BFE), which is derived from the probabilistic Bloom filter data structure. A puncturing operation only involves a small number of very efficient computations, plus the deletion of certain parts of the secret key, which outperforms previous constructions by orders of magnitude. This gave rise to the first forward-secret 0-RTT protocols that are efficient enough to be deployed in practice (see also above for the discussed OpenSSL integration). In a continuing work within the IoT4CPS project, we were able to enhance the efficiency of the Derler et al. approach even further, in particular allowing for constant-size ciphertexts.

In the context of IoT4CPS: Compared to the work by Derler et al. [2], this version incorporates a BFE scheme with constant-size ciphertext based on identity-based broadcast encryption. This work is currently under submission [26].

2.6.2 I Want to Forget: Fine-Grained Encryption with Forward Secrecy Meets Decentralization

Managing sensitive data in decentralized environments is gaining a lot of attention recently. A minimum requirement is to keep distributed data confidential, but also allow for flexible collaborating and sharing possibilities. In particular, being able to "forget" in such environments constitutes a desired feature (also when looking at the European General Data Protection Regulation's "Right to be Forgotten"). As it turns out, securely deleting data in decentralized systems can often only be realizable with high strain.

In this work, we were motivated to look at cryptographic solutions that offer the possibility to wilfully lose access to data in modern decentralized environments (which can be seen equivalent to removing that data or mitigating data leakages in case of key compromises). We argue that simple and deployed encryption mechanisms do not suffice to cover all desired requirements and provide a solution that offers several strong security and privacy guarantees. In more detail, our proposed building block achieves forward secrecy for all system participants (i.e., confidentiality holds even when encryption keys leak), enables fine-grained access control (i.e., provide a one-to-many sharing relation), and ensures strong privacy against public observers (i.e., achieve meta-data key anonymity). Combining those features cryptographically in one solution was unknown from the literature and yields a new approach with interesting practical applications, including an enhancement of Cloudflare's Geo Key Manager.

We base our solution on a novel cryptographic primitive we dub *Dual-Form Puncturable Encryption (DFPE)* which significantly enhances previous ideas on Puncturable Encryption (PE) due to Green and Miers (IEEE S&P 2015) and Günther et al. (EUROCRYPT 2017). We argue that black-box constructions from Hierarchical Identity-Based Encryption (HIBE) do not seem to work, albeit we do know how to construct PE from HIBE. We further introduce an important feature being crucial in the setting of always accessible and public data, namely that of key privacy

for DFPE such that an DFPE ciphertext reveals nothing about the encryption key. We demonstrate the feasibility of our DFPE construction with a practical prototype implementation. Finally, we show that DFPE, besides direct applications, is also a very versatile tool to construct other cryptographic primitives by using it to generically instantiate forward-secret IBE and forward-secret digital signatures.

In the context of IoT4CPS: A preprint version is available [27]. Within the IoT4CPS context, this DFPE primitive ensures low-latency key exchange and flexible access-control at the same time which is particularly useful when many IoT devices in a decentralized environment are present. This work is currently under submission.

2.6.3 CCA-Secure (Puncturable) KEMs from Encryption with Non-Negligible Decryption Errors

Public-key encryption (PKE) or key-encapsulation (KEM) schemes are a fundamental cryptographic building block, e.g., for key exchange, to realize secure communication protocols. There are several known transformations that generically turn weakly secure schemes into strongly (i.e., IND-CCA) secure ones. While most of these transformations require the weakly secure scheme to provide perfect correctness, Hofheinz, Hövelmanns, and Kiltz (HHK) (TCC 2017) have recently shown that variants of the Fujisaki-Okamoto (FO) transform can work with schemes that have negligible correctness error in the (quantum) random oracle model (QROM). Many recent schemes in the NIST post-quantum competition (PQC) use variants of these transformations. Some of their CPA-secure versions even have a non-negligible correctness error and so the techniques of HHK cannot be applied.

We ask the question and study the setting of generically transforming PKE schemes with potentially large, i.e., non-negligible, correctness error to ones having negligible correctness error. While there have been previous treatments in an asymptotic setting by Dwork et al. (EUROCRYPT 2004), our goal is to come up with practically efficient compilers in a concrete setting and apply them in two different contexts: Firstly, we show how to generically transform weakly secure deterministic or randomized PKEs into CCA-secure KEMs in the ROM as well as the QROM using variants of HHK. This applies to essentially all candidates to the NIST PQC based on lattices and codes with non-negligible error, for which we provide an extensive analysis, and we show how to improve some of the code-based candidates.

Secondly, we study puncturable KEMs from Bloom Filter Encryption (BFE) proposed by Derler et al. (EUROCRYPT 2018), which inherently have a non-negligible correctness error. BFE schemes are a building block to construct fully forward-secret zero round-trip time (0-RTT) key-exchange protocols. In particular, we show how to achieve the first post-quantum secure BFE schemes generically from lattice and codes by applying our techniques to identity-based encryption (IBE) schemes with (non-)negligible correctness error.

In the context of IoT4CPS: Compared to the work by Derler et al. [26] as given in 2.6.1 and Derler et al. [2], this work also incorporates a low-latency key exchange protocol that is secure even in an advent of a powerful quantum attacker yielding long-term security guarantees with low-latency properties. This work is currently under submission [28].

3. ISAP for ASICs and FPGAs

In this section, we put the focus on enabling secure communication for legacy devices with limited resources, which operate in the field for years and cannot be replaced easily with new hardware. The specific challenge is to apply authenticated encryption on an existing FPGA-based legacy device without changing any hardware or applying additional connectivity. Limited resources of FPGA-based legacy devices (such as the number of logic cells and power dissipation) are a constraint caused then by choosing highly cost-optimized hardware components. This poses another challenge for the new communication link that shall be resistant against simple Differential Power Analysis (DPA) attacks.

DPA attacks exploit data through power consumption of cryptographic devices. They use a broad number of power traces to analyze the power consumption at a fixed moment of time as a function of the processed data [21]. There exists a general attack strategy and consists of following five steps:

1. Select an intermediate result of the executed algorithm
2. Measuring the power consumption
3. Calculating hypothetical intermediate values
4. Mapping intermediate values to power consumption values
5. Comparing the hypothetical power consumption value with the power traces

A special requirement within the current system is that the underlying protocol must support multicast telegrams that can be decoded by all participants. The FPGA in use does not offer inherent reliable security support such as modern devices by Xilinx or latest Intel parts. The only feature that can be directly exploited is bitstream encryption. On top, in the selected system only a very small Soft-CPU-Core is available, which is already heavily loaded by software tasks. Consequently, the available FPGA area, minimum throughput and maximum latency are given. All these constraints together leave only one way open - designing an optimized implementation of a suitable algorithm that must fit into the remaining programmable logic.

A very suitable solution for the problem above is offered by the ISAP encryption scheme, which is shown in the following section. Within the course of the IoT4CPS project, an optimized ISAP module for FPGA is being developed and applied within a demonstrator design in order to enable detailed analysis and assessment.

3.1 ISAP Module

ISAP is a family of nonce-based authenticated encryption algorithms designed with a focus on robustness against passive side-channel attacks [7]. Such robustness is essential whenever cryptographic devices are deployed in locations that are physically accessible by potential attackers – a typical scenario in IoT applications.

ISAP is a so-called lightweight authenticated encryption algorithm due to its small footprint in hardware, when compared to other encryption schemes that need additional algorithmic countermeasures against passive side-channel attacks. All ISAP family members are permutation-based designs that combine variants of the sponge-based ISAP mode with one of several published lightweight permutations.

The key features of ISAP are:

- Authenticated encryption using lightweight permutations
- Sponge-based mode of operation using well studied substitution-permutation-network (SPN) permutations
- Suitable for constrained devices: small state, simple permutation
- Side-channel resistance: Provably secure leakage-resilience for encryption and decryption
- Built-in hardening against fault attacks
- Easy to implement in software and hardware
- Compact in software: supports pipelined processing, bit-sliced 5-bit S-box
- Fast and compact in hardware
- Scalable for more conservative security or higher throughput

- Timing resistance: No table look-ups or additions
- Minimal overhead (ciphertext length = plaintext length)

The authors of ISAP recommended the four instances: ISAP-K-128A, ISAP-A-128A, ISAP-K-128, and ISAP-A-128, which mainly differ in the type of the underlying permutation, as well as parameter choices that control how many bits of data can be processed within a certain timespan. The two possible choices for the underlying permutation are Keccak-p[400] (used by ISAP-K-128A, ISAP-K-128) and Ascon-p (used by ISAP-A-128A, ISAP-A-128), both of which have already been extensively studied by the cryptographic community, e.g., during the SHA-3 [9] and CAESAR [10] competition. All ISAP instances are designed to provide 128-bit security against cryptanalytic attacks and protect the confidentiality of the plaintext (except its length) and the integrity of ciphertext including the associated data.

The implementation of the ISAP core, that is integrated into the demonstrator design, is written in VHDL and supports the commonly used hardware interface in the NIST standardization project for lightweight cryptography [8]. The main modules are:

- LWC: The top module that defines an AXI compatible interface for sending/receiving blocks of associated data, plaintext, ciphertext, nonce and key.
- LWC_TB: A testbench that can be used to test the ISAP core in a stand-alone fashion.
- CryptoCore: The actual hardware implementation of ISAP, together with the underlying cryptographic permutation Ascon-p.
- NIST_LWAPI_pkg: Contains various configuration parameters such as the width of the external bus of the top-level interface.
- design_pkg: Contains various configuration parameters such as the width of the internal bus of the ISAP core.

3.2 Demonstrator Architecture

The architecture of the demonstrator is based on smart nodes that communicate via an industrial standard interface (Figure 10). Each node consists of an independent processor subsystem, an encryption/decryption unit and additional peripheral elements. The master node can communicate with each slave node and vice versa.

For the demonstrator the Xilinx evaluation board ZCU102 with the Zynq Ultrascale+ MPSoC device is used. This FPGA platform provides an integrated hard-wired processor sub system (PS) together with a large programmable logic area (PL). For the sake of building a demonstrator that is easy to handle, the number of needed hardware devices is reduced by locating all nodes inside one big FPGA device. Internal communication is established with AXI stream interfaces instead of ethernet interfaces. Node addressing is handled with side channel information and is not part of the data transfer package. Optional external nodes can be connected via Ethernet (see optional external slave node in Figure 10). The external slave node is connected to the master node via a standard RJ45 (Ethernet) cable. Furthermore, each node has GPIO ports to signal status information via LEDs located on the FPGA board. Via UART port a terminal console on the Host PC can be used for standard input and output operations of the node CPUs.

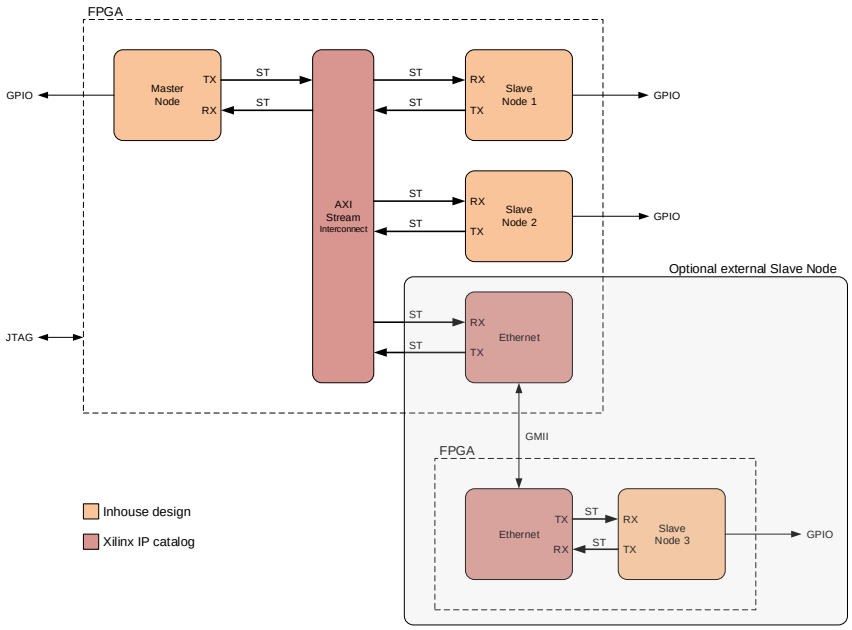

Figure 10: Architecture of demonstrator

3.2.1 Master Node

The master node is a completely independent CPU subsystem based on a hard-wired Quad-Core processor and a customized part inside the programmable logic. Standard components are used out of the Xilinx IP catalog, customized components are added manually to the Xilinx IP library for high reusability. Internally the AXI interconnect is used to connect memory mapped components that are visible to the processor in a defined address space. AXI streaming ports are applied for external data transfers that are handled by separate DMA units for each direction.

The streamed data packages are encrypted and decrypted on-the-fly by the ISAP module. Each outgoing package gets a unique session key for encryption. This session key and the transmitted nonce information for the slave node come from a generator unit, which derives the session key from the internally stored master key and a random number from the true random generator. For decrypting incoming packages, the received nonce value is used for regeneration of the session key.

Additionally, two partial reconfiguration blocks are used for individually checking the data stream before and after the ISAP module, and thus realize a hardware security checker. Different checking algorithms can be applied during normal operation. During the partial reconfiguration process the block will be decoupled from the rest of the logic to avoid undefined data on the streaming bus. Further details about the hardware checkers will be shown within Deliverable D4.2.

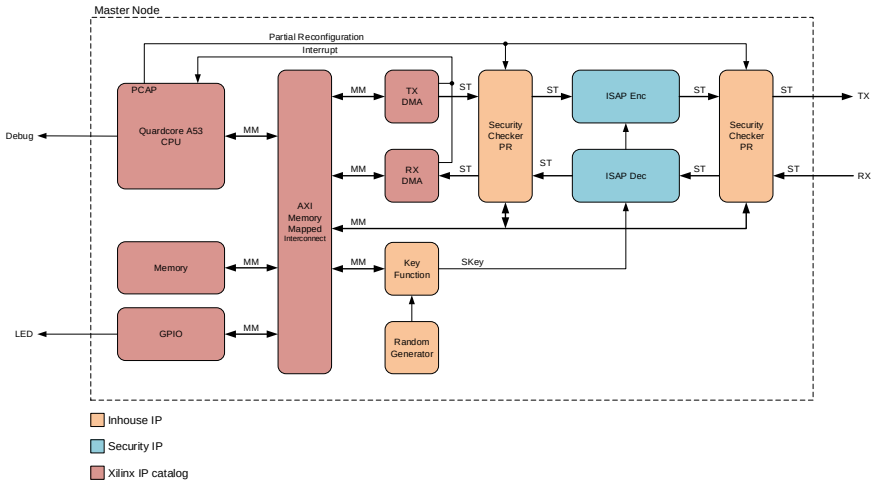

Figure 11: Master Node

The test application can either run as bare metal directly on one ARM core or under Linux on multi ARM cores. For the demonstrator software a simple program sends data packages to the slave nodes and waits for a response to check the correct behavior of data encryption and decryption between the master and the slave node. Visual observation is enabled by using the GPIO ports to show information on the board LEDs. Via the UART port an external terminal can be used for standard input and output interfaces. Loading the partial reconfiguration block for the security checker functionality is handled with predefined commands from the software library.

3.2.2 Slave Node

The slave node comprises the same AXI architecture as the master node, but with a reduced subset of components and functions (Figure 12). As processor core the Microblaze softcore is used, thus locating the complete slave node inside the programmable logic part. Furthermore, the slave node does not include partial reconfiguration blocks. All other components have the same functionality range as those within the master node (including the master key and key generator). In this way, equal timing behaviour of data processing for all nodes inside the system is guaranteed.

The slave node test application runs independently as bare metal software on the Microblaze processor. The program modifies the payload of the incoming data package and sends it back to the master node. With these changes inside the payload, the master node can check for correct behaviour of the secure communication. Blocking behaviour that might be caused by this cyclic data processing is avoided by an additional watchdog timer that resets the complete system after a defined timeout. Status information of the slave node can be displayed on the board LEDs. The UART interface can be used as debug port to show information on an external terminal.

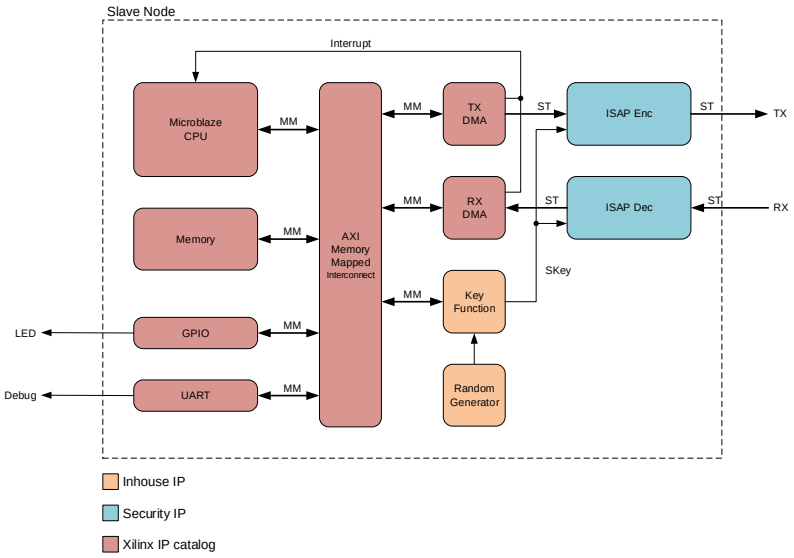

Figure 12: Slave Node

4. References

[1] D. Kales, S. Ramacher, C. Rechberger, R. Walch, „Efficient FPGA Implementations of LowMC and Picnic.”, CT-RSA (accepted), 2020

[2] D. Derler, T. Jager, D. Slamanig, C. Striecks. “Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange.” EUROCRYPT (3) 2018. pp. 425-455.

[3] D. Boneh, M. Franklin. “Identity-based encryption from the Weil pairing.” CRYPTO 2001.

[4] “CAESAR: Competition For Authenticated Encryption: Security, Applicability, and Robustness.” online: https://competitions.cr.yp.to/caesar.html

[5] E. Rescorla. “The Transport Layer Security (TLS) Protocol Version 1.3.” RFC 8446, 2018.

[6] D. Boneh, X. Boyen, E.-J. Goh. “Hierarchical identity based encryption with constant size ciphertext.”, EUROCRYPT 2005. pp. 440-456

[7] C. Dobraunig, M. Eichsleder, S. Mangard, F. Mendel, B. Mennink, R. Primas, T. Unterluggauer “ISAP v2.0 Submission to the NIST Lightweight Cryptography competition”, online: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/ISAP-spec.pdf. 2019

[8] Jens-Peter Kaps, William Diehl, Michael Tempelmeier, Ekawat Homsirikamol, Kris Gaj: "Hardware API for Lightweight Cryptography" online: https://cryptography.gmu.edu/athena/LWC/LWC_HW_API.pdf

[9] "SHA-3 Project" online: https://csrc.nist.gov/projects/hash-functions/sha-3-project

Feldfunktion geändert

Feldfunktion geändert

[10] "CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness" online: https://competitions.cr.yp.to/caesar-submissions.html

[11]

[12] D.F. Aranha, C. P. L. Gouvêa. "RELIC is an Efficient Library for Cryptography." https://github.com/relic-toolkit/relic

[13] E. Fujisaki, T. Okamoto. "Secure Integration of Asymmetric and Symmetric Encryption Schemes." CRYPTO 1999.

[14] NIST. "FIPS PUB 202: SHA3: Permutation-Based Hash and Extendable-Output Functions", 2015

[15] "eXtended Keccak Code Package." https://github.com/XKCP/XKCP

[16] D. van Heesch. "Doxygen: Generate documentation from source code." http://www.doxygen.nl/

[17] „Cgreen: Unit Tests, Stubbing and Mocking for C and C++." https://cgreen-devs.github.io/

[18] R. Barbulescu, S. Duquesne. "Updating Key Size Estimations for Pairings.", Journal of Cryptology, 2019

[19] M. Krmpotić. "Implementation and Evaluation of Low-Latency Key-Exchange Protocols", Master's thesis, 2019

[20] T. Unterluggauer, E. Wenger. "Efficient Pairings and ECC for Embedded Systems." CHES, 2014

[21] J. Aas, R. Barnes, B. case, Z. Durumeric, P. Echerskley, A. Flores-Lópes, J.A. Halderman, J. Hoffman-Andres, J. Kasten, E. Rescorla, S.D. Schoen, B. Warren. "Let's Encrypt: An Automated Certificate Authority to Encrypt the Enture Web.", ACM CCS, 2019

[22] H. Groß, D. Schaffenrath, S. Mangard. "High-Order Side-Channel Protected Implementations of KECCAK." DSD, 2017

[23] H. Mestiri, F. Kahri, M. Bedoui, B. Bouallegue, M. Machhout. „High throughput pipelined hardware implementation of the KECCAK hash function.", ISIVC, 2016

[24] T. Honda, H. Guntur, A. Satoh. „FPGA implementation of new standard hash function Keccak." GCCE, 2014

[25] ISO. "ISO/IEC 9899:2011: Information technology – Programming languages – C." https://www.iso.org/standard/57853.html

[26] D. Derler, K. Gellert, T. Jager, D. Slamanig, C. Striecks. "Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange." In submission, 2020.

[27] D. Derler, S. Ramacher, D. Slamanig, C. Striecks. "I Want to Forget: Fine-Grained Encryption With Forward Secrecy Meets Decentralization." Cryptology ePrint Archive 2019/912, https://eprint.iacr.org/2019/912. In submission, 2020.

[28] V. Cini, S. Ramacher, D. Slamanig, C. Striecks. "CCA-Secure (Puncturable) KEMs from Encryption With Non-Negligible Decryption Errors." In submission, 2020.

Feldfunktion geändert

Feldfunktion geändert

Feldfunktion geändert