Lightweight Public Key Encryption in Post-Quantum Computing Era

Peter Hillmann

University of the Bundeswehr Munich,
Department of Computer Science,
Werner-Heisenberg-Weg 39, 85577 Neubiberg, Germany

Abstract. Confidentiality in our digital world is based on the security of cryptographic algorithms. These are usually executed transparently in the background, with people often relying on them without further knowledge. In the course of technological progress with quantum computers, the protective function of common encryption algorithms is threatened. This particularly affects public-key methods such as RSA and DH based on discrete logarithms and prime factorization. Our concept describes the transformation of a classical asymmetric encryption method to a modern complexity class. Thereby the approach of Cramer-Shoup is put on the new basis of elliptic curves. The system is provable cryptographically strong, especially against adaptive chosen-ciphertext attacks. In addition, the new method features small key lengths, making it suitable for Internet-of-Things. It represents an intermediate step towards an encryption scheme based on isogeny elliptic curves. This approach shows a way to a secure encryption scheme for the post-quantum computing era.

Keywords: Cryptography, Public-Key Encryption, Post-Quantum Cryptography, Elliptic Curve, Isogeny Curve.

1 Introduction

More than 50 % of all internet traffic use the protocol combination of RSA with *Optimal Asymmetric Encryption Padding* (OAEP), i. e. in https. Also the financial market relies on RSA for online-banking, even if RSA is only cryptographic weak. Attacks on *Secure Sockets Layer* (SSL/TLS) following *Public-Key Cryptography Standards* (PKCS) #1 v1.5 show the weakness of the cryptosystem RSA. For example, the approaches of *Bleichenbacher* [1] could reveal the content of encrypted messages. In order to prevent such *Adaptive Chosen Ciphertext Attacks* (CCA2), it is necessary to use an encryption or encoding scheme that limits ciphertext malleability. To address this problem, RSA is combined with the coding scheme OAEP [2]. It is standardized in the updated PKCS#1 v2 (RFC 2437, RFC 8017). The security of OAEP has been proven secure in the random oracle model [3]. This model is typically used when the proof cannot be carried out using weaker assumptions compared to the *Standard Model of Cryptography* (SMC). The SMC uses only complexity assumptions for the verification. A growing body of evidence claims the insecurity of this approach [4]. Even the improved scheme OAEP+ is only proved secure against non-adaptive *Chosen Ciphertext Attacks* (CCA) in general. The security is still indistinguishability under CCA2 in the SMC [5, 6]. Furthermore, vulnerabilities still exist with slight variations like *Return Of Bleichenbacher's Oracle Threat* since 20 years [7]. The history shows that the current improvements have not solved the problem fundamentally by modified attacks [8, 9].

However, the combination of RSA with OAEP was favored instead of using a different encryption system with inherent strength against such attacks. Nevertheless, the confidentiality of crypto systems is threatened by the rising quantum computing era. This also has a significant impact on the trustworthiness of all current blockchain applications [10] due to the public-key procedures used. More complex mathematical problems need to be

David C. Wyld et al. (Eds): BIOM, CRBL, EDUPT, SIP, COMIT -2023
pp. 01-14, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.132101

identified for cryptography as large number factorization is developed. The algorithms of *Shore* and *Grover* allow fast factorization and search. This particularly affects public-key methods based on discrete logarithms and prime factorization such as RSA and DH. To address this problem fundamentally, we enhance a public-key encryption system for the *post-quantum cryptographic* (PQC) age. The direction of *Elliptic Curve Cryptography* (ECC) has yielded new algorithms, which provides increased security. Our base is the *Cramer-Shoup* crypto system, which is mathematical proven secure against CCA2 in SMC [11]. This security definition is currently the strongest confidentiality proof known for a public-key crypto system. This prevents such attacks like on RSA-OEAP from the beginning. Our contribution focuses on increasing security while keeping the keys small. In this paper, we highlight the requirements on modern crypto systems with focus on *Internet of things* (IoT). In our concept, we develop the *Cramer-Shoup* (CS) crypto system further to be resistant against quantum computing possibilities. Therefore, we adapt CS to the mathematical base of *Elliptic Curves* (EC). The main advantages are shorter keys, faster operations and increased security compared to the algorithms based on classical discrete logarithms. This is especially desired in lightweight cryptographic for mobile and wireless applications as in the IoT environments [12]. In addition, we provide an simple and detailed description for comprehensible implementation, also with regard to further research. Based on this approach, we will extend our solution to supersingular isogeny EC or graphs for higher protection class in a future step. This new mathematical construct is promising to be resistant to attacks via quantum computers in 21st century. Beside this, we give an overview about the development of public-key schemes and provide a performance comparison.

The structure of this paper is as follows: Section 2 describes a typical security scenario and lists the requirements for modern crypto systems. In Section 3, we provide an overview of the current state of the art with focus on EC. The main part in Section 4 describes our concept of a public-key crypto system. Then, we show the correctness of the our approach and evaluate the performance in comparison to other approaches in Section 5. Subsequently, we proof the fundamental security properties of the presented system in Section 6. A discussion on security in the post-quantum era is elaborated in Section 7. The last section summarizes our work and provides an outlook.

2 Scenario and Requirements

Our approach is based on the following common scenario for public-key encryption, see Figure 1. A sender wishes to send a confidential message to a particular recipient. For that purpose, the recipient has shared the public part of his asymmetric key on a free portal on the Internet (1). This is preferably included in a cryptographic certificate. The sender uses this public key (2) to encrypt the message (3). The encrypted message is then sent to the receiving party (4). The recipient can decrypt the message and process it based on knowledge of the corresponding private key (5). An omnipotent attacker can access both the public part of the key and the encrypted message. Therefore, the encryption method must provide cryptographically strong protection.

The following requirements are mandatory for modern crypto systems:

- Tiny keys for fast transmission
- Forward secrecy and reusable keys
- Integrated message validation
- No Malleability [14]
- Provable strong security against adaptive CPA and CCA2, highest possible security

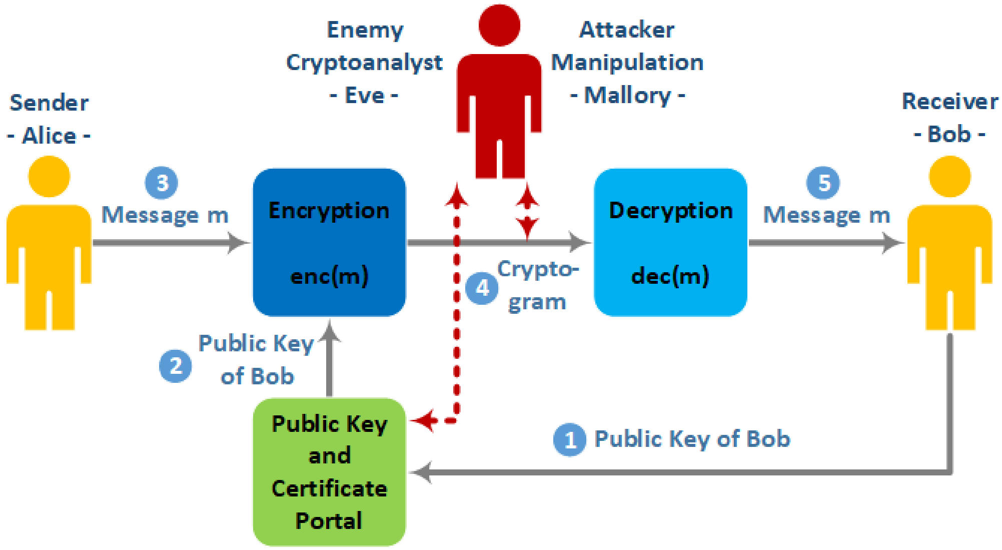
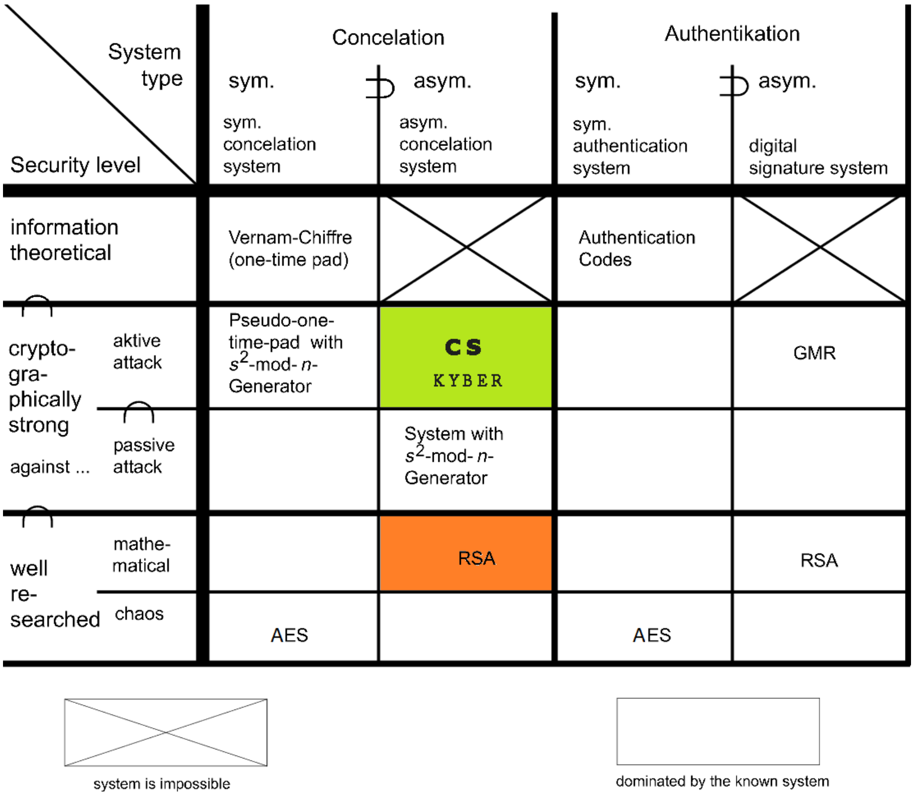


Fig. 1. General secrecy system scenario [13].

- Additionally in software engineering [15]:
  - No data flow from secrets to array indices
  - No data flow from secrets to branch conditions
  - No padding oracles
  - Centralizing randomness
  - Avoiding unnecessary randomness with focus on audited deterministic functions

3 History and Related Work

Advances in quantum computing have created a need for new methods in PQC. Over the past years, different cryptography systems have been developed. Many schema can be used and combined for multiple security operations. An overview about established cryptographic systems and their security level is given in Figure 2. It shows the theoretical limits for their level of security in the different categories. As this publication focus on public-key encryption, the highest security level can only be cryptographic strong. A public-key crypto system can never be information theoretical secure due to the public-key testing possibility. The following list of encryption methods illustrates the known security levels based on their historical development. One of the first public-key crypto systems was developed by Ralph Merkle with the Merkle Puzzle, later published in 1978 [17]. Nevertheless, James H. Ellis, Clifford Cocks, and Malcolm Williamson invented public-key cryptography for the British Government Communications Headquarters in 1970 [18]. The first wide spread protocol for asymmetric cryptography is the Diffie–Hellman(-Merkle) (DH) key exchange for a non-authenticated key-agreement, since 1976 [19]. Beyond that, the first public-key scheme was developed by Rivest, Shamir und Adleman (RSA) at the Massachusetts Institute of Technology in 1977 [20]. These are based on the assumption of the hardness of the factoring problem or discrete logarithm problem (DLP). Since these systems work deterministic, it is susceptible to simple attacks. Therefore, for example RSA has to be combined with OAEP in practice nowadays [2]. The unmodified RSA is not *indistinguishable for chosen plain-text attacks* (IND-CPA), which is mandatory for current systems. Beside these, there are many more Public-Key schemes with the following security problems (excerpt):



System type Security level		Concelation		Authentikation	
		sym.	asym.	sym.	asym.
		sym. concelation system	asym. concelation system	sym. authentication system	digital signature system
information theoretical		Vernam-Chiffre (one-time pad)	☒	Authentication Codes	☒
crypto-graphically strong against ...	aktive attack	Pseudo-one-time-pad with s^2-mod-n-Generator	CS KYBER		GMR
	passive attack		System with s^2-mod-n-Generator		
well re-searched	mathe-matical		RSA		RSA
	chaos	AES		AES	

☒ system is impossible

□ dominated by the known system

Fig. 2. Overview on cryptographical systems in relation to security level [16].

- Merkle-Hellman [21]: Trapdoor knapsacks; broken [22].
- McEliece [23]: Provable hardness of decoding a general linear code (IND-CPA); proposed PQC; comparable large keys.
- Rabin [24]: Provable for factoring problem; 4-to-1 output, which leads to decryption failure.
- Chor-Rivest [25]: no feasible attack known; comparable large key.
- Elgamal [26]: Provable hardness of decisional Diffie–Hellman assumption (IND-CPA); malleable.
- NTRUEncrypt [27]: Provable hardness for correctness *Ring Learning with Errors*; proposed PQC; comparable large keys.
- Paillier [28]: Provable hardness of decisional composite residuosity problem (IND-CPA); malleable.

American NIST and European ENISA are currently running a competition for new methods for quantum-resistant public-key cryptographic [29–31]. CRYSTALS-Kyber has been nominated as a possible finalist [32, 33]. Contrary to our EC or Isogeny approach, Kyber is based on the hardness of solving the learning-with-errors (LWE) problem over module lattices. Thus, the keys are slightly larger with comparable security and a side-channel attack is known [34]. Besides the ring-LWE and lattice-based approach, further promising approaches for POC are considered: multivariant polynomial, code-based, hash-based, and supersingular isogeny EC. Of these, the EC approach offers the most promising potential in terms of lightweight Cryptography. The key length in EC and supersingular isogeny EC cryptography is significantly smaller than in the other cryptosystems.

In the following, a retrospective of the development of supersingular isogeny EC cryptography is given:

– 1996 Couveignes [35] first mentioned about isogenies in cryptography.
– 2010 Rostovtsev and Stolbunov [36] presented first published isogeny-based public-key cryptosystem based on isogenies between ordinary curves.
– 2011 Jao and De Feo [37] presented the Supersingular Isogeny Diffie-Hellman (SIDH) [38].
– 2017 Jao et al. [39] proposed Supersingular Isogeny Key Encapsulaon (SIKE) as a submission to NIST PQC call.

The SIDH and SIKE approaches are the only known approaches based on supersingular isogeny. However, an active attack was found for SIDH [40, 38]. This type of adaptive attacks is fundamentally prevented with our concept. Furthermore, the NIST calls for *Lightweight Cryptography* to protect small electronics, we are focus on [41].

4 Concept of Cramer-Shoup with Elliptic Curve

This approach is premised on the general sender-receiver architecture, as shown in Figure 1. Our public-key encryption method is based on the approach of Cramer-Shoup (CS) [42, 43]. Here, we adapt the cryptographic strong procedure of CS to the promising base of ECC as an intermediate step to supersingular isogeny EC. The main benefit is that the key length scales linear in relation to the security level [44]. The new security relies on the *Elliptic Curve Discrete Logarithm Problem* (ECDLP) [45, 46]. This mathematical problem is more difficult to solve than the integer factorization problem or the classical DLP. Currently, no algorithm is known that solves the ECDLP in an efficient way. The known fastest approach is the parallelized Pollard-Rho Algorithms with approximately $O(\sqrt{p})$, where p is the largest prime factor of n [47].

4.1 Prerequisite

First of all, the following parameters are to be declared. The plain-text message to be secured, is described as the parameter m. Here it is a positive integer value, represented as binary.

For encryption, we chose two large prime numbers p and q secretly, where as $p = 1+2q$. This defines us the integer group Z over p and q, called Z_p and Z_q. The group G is defined as a subgroup of Z_p of order q. A plain-text input m need to be part of the Group G, representing the amount of possible input data.. Larger information need to be divided into chunks, so that $m \in G$.

Furthermore, publicly available is a hash function $Hash$, which is a collision resistant one-way function in Z. This hash function $Hash$ calculates for any input values in Z integer values as output. We suggest the standardized SHA3, the sponge function Keccak [48] for hardware or the more Side-Channel-Attacks robust package Skein [49] for software.

We use an EC $F_p(x)$ in the finite body modulo Z_p as the basis of our encryption system, whereas x is the input parameter to F_p. More specific, x is an integer coordinate of a point $P(x, y)$ in Cartesian coordinate system. We suggest an EC $F_p(x)$ fulfilling the Weierstrass form: $y^2 = x^3 + ax + b$ The factors a, $b \in Z_p$ specifies the field F_p, whereas $4a^3 + 27b^2\ ! = 0$.

For this purpose, the well-reviewed Koblitz curve *SECP256k1* [50] or Montgomery curve *ed25519* (RFC7748) [51] are suitable [52] for a $\tilde{1}$28-bit security level. Each EC comes with his own public starting-points, which has been identified as cryptographically fitting. These starting-points are generators of a large cyclic subgroup of the specific curve.

For these points applies $G_1, G_2 \in F_p(x)$. Currently, our two starting points $G_1(x_{g1}, y_{g1})$ and $G_2(x_{g2}, y_{g2})$ are chosen wisely random [53] in a large cyclic group.

For cryptographic operations, the following functions are described on an EC. The addition functions is defined with $pointAdd[]$ with the three parameter: the EC $F_p(x)$ itself, point P_1, and point P_2, so $F_p(P_1 + P_2) = pointAdd[F_p(x), P_1, P_2]$. The multiplication is described with $pointMult[]$ with the three parameter: the EC $F_p(x)$ itself, starting point P, and multiplication factor k, so $F_p(P_k) = pointMult[F_p(x), P, k]$. Beside these functions, we need the point conversion $pointNegate[]$, which invert the position of the point by changing the sign of the y-value.

4.2 Public Key Generation by Receiver

At the beginning, the receiver chooses the following five factors randomly, each $\in Z_q$: x_1, x_2, y_1, y_2, z. Each number should be large, favored about the same size. To create the public-key, the receiver calculates the following values, see Equation 1, 2, and 3:

$$\begin{aligned} Point\ C = F_p(x_1\ G_1\ +\ x_2\ G_2) = \\ pointAdd[F_p(x), \\ pointMult[F_p(x), G_1, x_1], \\ pointMult[F_p(x), G_2, x_2]] \end{aligned} \tag{1}$$

$$\begin{aligned} Point\ D = F_p(y_1\ G_1\ +\ y_2\ G_2) = \\ pointAdd[F_p(x), \\ pointMult[F_p(x), G_1, y_1], \\ pointMult[F_p(x), G_2, y_2]] \end{aligned} \tag{2}$$

$$\begin{aligned} Point\ H = F_p(z\ G1) = \\ pointMult[F_p(x), G_1, z] \end{aligned} \tag{3}$$

In summary, we obtain the following individual keys:

- Public-key - Points: C, D, H
- Private-key - Factors: x_1, x_2, y_1, y_2, z

In addition, we have in common the following parameters, which can also be public:

- Function $F_p(X)$ with generator points G_1, G_2
- Function $Hash$

For the public format, recommended representation is ANSI X.509, X9.62, and X9.63 syntax following ASN.1 structure.

4.3 Encryption by Sender

The sender would like to store or transmit the data m. For encryption, we secretly and randomly choose a multiplication factor $r \in Z_q$. The factor r is chosen anew for each data m. Even if q is unknown and therefore also Z_q, r should automatically be part of Z_q, because q is chosen accordingly large. This factor r is used to perform point multiplications on the EC as follows, see Equation 4, 5, and 6:

$$Point\ U_1 = F_p(r\ G_1) = pointMult[F_p(x), G_1, r] \tag{4}$$

$$Point\ U_2 = F_p(r\ G_2) = pointMult[F_p(x), G_2, r] \tag{5}$$

$$\begin{aligned} &Point\ E = F_p(r\ H\ +\ m) = \\ &\qquad pointAdd[F_p(x), pointMult[F_p(x), H, r], m] \end{aligned} \tag{6}$$

There we obtain the three points U_1, U_2, and E of the EC.

To protect against tampering and to ensure integrity, one hash value α is calculated over the three points, see Equation 7:

$$\alpha = H(U_1, U_2, E) \tag{7}$$

This hash value must also be encrypted before transmission, see Equation 8:

$$\begin{aligned} Point\ V_{enc} = {} & F_p(r\ C + r\ \alpha\ D) = \\ & pointAdd[F_p(x), \\ & pointMult[F_p(x), C, r], \\ & pointMult[F_p(x), D, r \times \alpha]\ ] \end{aligned} \tag{8}$$

The encrypted data $enc\{m\}$ for transmission consists of the following components, see Equation 9:

$$enc\{m\} = \{U_1, U_2, E, V\} \tag{9}$$

4.4 Decryption by Receiver

The recipient first verifies the integrity of the received message. For this purpose, we calculate alpha again and compare it with the encrypted version, see Equation 10 and 11:

$$\alpha = H(U_1, U_2, E) \tag{10}$$

$$\begin{aligned} &Point\ V_{dec} = F(V) = F_p(x_1\ U_1\ +\ \alpha\ y_1\ U_1\ +\ x_2\ U_2\ +\ \alpha\ y_2\ U_2) \\ &\quad pointAdd[F_p(x), \\ &\quad pointAdd[F_p(x), pointMult[F_p(x), U_1, x_1], \\ &\qquad\qquad pointMult[F_p(x), \\ &\qquad\qquad pointMult[F_p(x), U_1, y_1], \alpha]\ ] \\ &\quad pointAdd[F_p(x), pointMult[F_p(x), U_2, x_2], \\ &\qquad\qquad pointMult[F_p(x), \\ &\qquad\qquad pointMult[F_p(x), U_2, y_2], \alpha]\ ] \\ &\qquad\qquad] \end{aligned} \tag{11}$$

If V_{enc} and V_{dec} matches, the received message is unaltered and belongs to the same random number r.

For the decryption of the message, the factor r is extracted from the two points U_1 and E and the factor z is indirectly extracted from the point H, see Equation 12.

$$\begin{aligned} dec\{m\} = {} & F_p(E - z\ U_1) \\ & pointAdd[F_p(x), E, \\ & pointNegate[pointMult[F_p(x), U_1, z]]] \end{aligned} \tag{12}$$

5 Evaluation

In the following, the correct operation of the approach is first demonstrated. The subsequent performance comparison puts our approach in relation to comparable systems.

5.1 Proof of Correctness

For a better comprehensibility and compact notation, the description is done without the continuous specification of the elliptic curve $F(x)$. The correctness of our system is given by:

$$\begin{aligned} &(x_1 + y_1\ \alpha)\ U_1 + (x_2 + y_2\ \alpha)\ U_2 \\ &= x_1\ U_1 + x_2\ U_2 + y_1\ \alpha\ U_1 + y_2\ \alpha\ U_2 \\ &= r\ x_1\ G_1 + r\ x_2\ G_2 + r\ y_1\ \alpha\ G_1 + r\ y_2\ \alpha\ G_2 \\ &= r\ (x_1\ G_1 + x_2\ G_2) + r\ \alpha\ (y_1\ G_1 + y_2\ G_2) \\ &= r\ C + r\ \alpha\ D = V. \end{aligned} \tag{13}$$

Since $z\ U_1 = r\ H$, $dec\{m\} = \{U_1, U_2, E, V\}$

$$= E \times (-z\ U_1) = E \times (-r\ H) = m. \tag{14}$$

So, our system is working properly.

5.2 Preliminary Performance Comparision

The implementation of our schema is done from an academic perspective in Java without any special optimizations. It serves to verify and validate the correct functioning. The performance of the algorithms is highly dependent on proper implementation and mathematical realization. The Table 1 shows a preliminary comparison of the speeds of different encryption algorithms on an Intel Core i7-8565U CPU 1.80GHz. We used freely available sources as reference implementation for RSA with Chinese-Reminder-Theorem [1], ECDH [2], SIDH [3], and Kyber [4]. The time is measured in milliseconds.

Table 1. Comparison of our approach with common reference approaches.

	RSA	ECC	CS	*THIS*	ECDH	SIDH	Kyber
	(4096)	(256)	(256)	*(256)*	(secp256k1)	(P751)	(1024)
Size Pub. K.	512 B	32 B	1 KB	*64 B*	32 B	564 B	1.5 KB
Size Pri. K.	512 B	32 B	1 KB	*64 B*	32 B	48 B	3.1 KB
Agreement	-	-	-	-	2	416	-
Encryption	116	19	3	*41*	-	-	2
Decryption	4	7	1	*43*	-	-	4
Initialisation	17.700	397	3	*473*	682	687	152

The ECDH and SIDH [54] method require more computing power than our approach and the key cannot be reused. The speed of RSA depends heavily on the key size, especially the key generation. However, RSA requires further power through OAEP and key validation, which is not included here. The more complex basis of our schema requires correspondingly more computing power to guarantee the desired security. Only the optimized implementation of Kyber for the NIST competition is faster, requiring larger keys [5].

[1] https://github.com/YYZ/RSA

[2] http://www.academicpub.org/PaperInfo.aspx?PaperID=14496

[3] https://github.com/Art3misOne/sidh

[4] https://github.com/fisherstevenk/kyberJCE

[5] https://pq-crystals.org/kyber/

6 Proof: Secure against adaptive-choosen ciphertext attacks

Our presented crypto schema is cryptographic strong, so we can proven the resistance against CCA. The evidence for CPA is therefore obsolete. In short, even without having to get too deep into the proof, we refer to existing once for the fundamental CS schema [11, 55, 5]. However, against ECC have been identified some theoretical attack approaches [56]. A part of them use the currently strongest attack vector based on active attacks, which is directly countered by our schema.

The proof on security is given by contradiction based on the EC $F(x)$ and follows [55, 57]. The main advantage of the proof is that it does not relay on a zero-knowledge assumption.

6.1 DDH Assumption

The security is based on the mathematical problem of the Decisional Diffie-Hellman (DDH) triples as computational hardness assumption. This means that the triples $\{g^a, g^b, g^{ab}\}$ with random a, and b are independent from non-Diffie-Hellman triples $\{g^a, g^b, g^c\}$, where a, b, and c. In the multiplicative cyclic group G of order q with generator g, discrete logarithms are indistinguishable and cannot be computed efficiently.

6.2 CCA Assumption

We assume a decryption "oracle" that correctly decrypts any given ciphertext. An attacker chooses two messages m_1 and m_2, where $m_1 \neq m_2$. These both messages are send to an encryption service, which only returns randomly one of the messages encrypted. The attacker is allowed a polynomial-time access to our decryption "oracle", also after obtaining a ciphertext returned from the encryption service. The direct transmission of a ciphertext is excluded in this case. The attacker now guesses which message the encryption service has provided. If this fits better with a probability than $1/2 + \delta$, then the opponent has an advantage defined by δ.

A crypto system is said to be indistinguishable chosen ciphertext attacks (IND-CCA) secure, if the advantage δ is negligible for any polynomial time attacker.

6.3 IND-CCA 1 - non-adaptive Security

From the public key, the attacker can get the information:

$$D = G_1^{y_1} + w\ G_1^{y_2} \tag{15}$$

For a query $< U_1, U_2, E, V >$, we obtain

$$U_1 = G_1^{r_1},\ U_2 = G_2^{r_2}, r_1 \neq r_2 \tag{16}$$

If it is accepted, then $V = U_1^{y_1}\ U_2^{y_2}$, i. e. the following:

$$V = r_1\ G_1^{y_1} + r_2\ w\ G_1^{y_2} \tag{17}$$

Since these equations are linearly independent, this happens with only negligible probability. Based on the validity check, the cases can be proved and the schema is IND-CCA 1 secure.

6.4 IND-CCA 2 - adaptive Security (Validity Checking Failure)

For this proof, we need to divide the value of the secret key z in z_1 and z_2. From the public key V, the attacker can get the following information:

$$H = G_1^{z_1} \times w\ G_1^{z_2} \tag{18}$$

Suppose that this is not a DDH tuple:

$$D = \{U_1 = G_1^{r_1},\ U_2 = G_2^{r_2}, r_1 \neq r_2\} \tag{19}$$

Then the challenge ciphertext is as follows:

$$\begin{aligned} &enc\{m\} =< U_1, U_2, E_{DDH}, V_{dec} >= \\ &< U_1,\ U_2,\ U_1^{x_1}\ U_2^{x_2}\ m,\ U_1^{y_1}\ U_2^{y_2}\ U_1^{z_1\alpha}\ U_2^{z_2\alpha} >, \\ &where\ \alpha = Hash\{U_1,\ U_2,\ E\} \end{aligned} \tag{20}$$

Therefore, the attacker can get the following information:

$$H = r_1\ U_1^{y_1} + r_2\ w\ U_2^{y_2} + r_1\ G_1^{z_1\ \alpha} + r_2\ w\ G_1^{z_2\ \alpha} \tag{21}$$

If the attacker queries an invalid ciphertext to the decryption oracle, say:

$$\begin{aligned} &< U_1',\ U_2',\ E',\ V' >, \\ &where\ U_1' = G_1^{r_1'},\ U_2' = G_2^{r_2'}\ and\ r_1' \neq r_2' \end{aligned} \tag{22}$$

As for this decryption query, we should consider the followings cases:

- If $< U_1,\ U_2,\ E >=< U_1',\ U_2',\ E' >$ then $V \neq V'$.
  This query will always be rejected.
- If $< U_1,\ U_2,\ E >=< U_1',\ U_2',\ E' >$ then $V = V'$.
  Since $Hash$ is collision-resistant and the attack runs in polynomial time, this happens with only negligible probability.
- If $Hash\{U_1,\ U_2,\ E\} \neq Hash\{U_1',\ U_2',\ E'\}$:
  And if the ciphertext is accepted by the oracle, it should satisfy the following:
  $H' = r_1'\ U_1^{y_1} + r_2'\ w\ U_2^{y_2} + r_1'\ G_1^{z_1\ \alpha'} + r'2\ w\ G_1^{z_2\ \alpha'}$,
  where $\alpha' = Hash\{U_1', U_2', E'\}$.
  Since the above equations are linearly independent, this happens only with negligible probability.

Based on the validity check, all cases can be proved and the schema is IND-CCA 2 secure. This is currently the strongest notion of security. In addition, our cryptographic system is highly efficient in terms of computation, especially in the context of hybrid systems for encryption and signature. In addition, the comparatively small key size enables the system to be used in mobile and wireless applications with low transmission bandwidth, such as smart cards. This also makes it ideal for the Internet of Things and banking.

7 Security discussion: Post-Quantum Cryptography

Peter Shor developed a polynomial time quantum computer algorithm to solve integer factorization problem and DLP [58]. Cryptographic schemes based on pure EC might be not be secure for future, due to the rapid development of quantum technology and data storing possibilities. What cannot be cracked today can be stored for later decryption [59].

Currently, a quantum computer needs for breaking an ECC with 256 bit keys (128 bit security level) about 2330 qbits and 126 billion Toffoli gates [60]. This exceeds any current quantum computing approach of currently less than 400 Qbits and appears to be more than a decade in the future. According to NIST and the German BSI, a key length of 256 bit in ECC provide security beyond the year 2030 [61, 62]. Additionally, our approach can be made polymorphic in the sense of a variable usage of the underlying EC and the flexible choice of the starting points. This further complicates a cryptographic analysis and enlarges the possible space of cryptograms.

Nevertheless, the adaption of the CS scheme to EC was mandatory beforehand to enhance it to an supersingular isogeny EC base [63, 64]. ECC with Montgomery curves has usually corresponding isomorphic Weierstrass curve over a field K in the form: $F(x) : By^2 = x^3 + Ax^2 + x$ [65–67]. This is used to enhance our system to the base of supersingular isogeny EC cryptography in a next step. The security is related to the problem of finding the isogeny mapping between two supersingular EC with the same number of points. Best known attacks are Meet-in-the-Middle [68], collision search [69], and algorithmic computation [67]. The security will be $O(p^{1/4})$ for classical computers and $O(p^{1/6})$ for quantum computers. For a classical security level of 128 bit, we need primes of size at least of 768 bit [63, 56]

These isogeny approaches are promising and based on complex problems, which are also resistant in the post-quantum computing era, like SIDE and SIKE. Although, these new mathematical construction is not the mainstream research for post-quantum cryptography, it offers promising possibilities. The key sizes are significantly smaller in relation to other schemes. With key-compression techniques, the transmit information with coefficients defining the EC and two EC points is $<$ 517 Bytes [54]. So this fits easily in the payload of one IPv4 or v6 network packet. It is especially favorable for smart cards and low bandwidth communication as stated in ISO/IEC 7816-8.

8 Summary

Although there are not yet sufficiently powerful quantum computers to break the public-key methods currently in use, this could be the case in the distant future. Therefore, research is already being conducted on secure schemes in many different aspects. Our approach follows the transformation to EC and supersingular isgoeny EC like DH over ECDH to SIDH and SIKE. This paper adapt and enhances the cryptographic strong procedure of Cramer-Soup to the base of EC. In relation to other suggested crypto system, we focus on *Lightweight Cryptography*. The main advantage of our system is the comparable higher security than RSA or other approaches by small key size and linear key scaling. So, our schema can be used in mobile systems with limited bandwidth or less capacity like smart cards or RFID. Our public-key encryption schema is provable secure IND-CCA 2 without malleability to prevent attacks like from *Bleichenbacher* from the beginning. In the future, we will adapt our encryption system to supersingular isogeny EC to foster resist quantum computing capabilities.

References

1. Bleichenbacher, D.: Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1. In: Proceedings of the International Cryptology Conference on Advances in Cryptology (CRYPTO). pp. 1–12. Springer, London, UK (1998), `http://dl.acm.org/citation.cfm?id=646763.706320`
2. Bellare, M., Rogaway, P.: Optimal Asymmetric Encryption How to Encrypt with RSA. Advances in Cryptology - Eurocrypt (1994)

3. Fujisaki, E., Okamoto, T., Pointcheval, D., Stern, J.: RSA-OAEP Is Secure under the RSA Assumption. Journal of Cryptology 17(2), 81–104 (Mar 2004)
4. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. J. ACM 51(4), 557–594 (Jul 2004)
5. Paillier, P., Villar, J.L.: Trading One-Wayness Against Chosen-Ciphertext Security in Factoring-Based Encryption. In: Lai, X., Chen, K. (eds.) Advances in Cryptology – ASIACRYPT. pp. 252–266. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)
6. Brown, D.R.L.: What hashes make rsa-oaep secure? (2007)
7. Böck, H., Somorovsky, J., Young, C.: Return Of Bleichenbacher's Oracle Threat (ROBOT). In: USENIX Security Symposium. pp. 817–849. USENIX Association, Baltimore, MD (2018), https://www.usenix.org/conference/usenixsecurity18/presentation/bock
8. Manger, J.: A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized in PKCS #1 v2.0. In: International Association for Cryptologic Research (IACR), Proceedings of the International Cryptology Conference on Advances in Cryptology (CRYPTO). vol. 2139, pp. 260–274. Springer (2001), lecture Notes in Computer Science
9. Ronen, E., Gillham, R., Genkin, D., Shamir, A., Wong, D., Yarom, Y.: The 9 Lives of Bleichenbacher's CAT:New Cache ATtacks on TLS Implementations. Real World Crypto 2020 and IEEE Symposium on Security and Privacy (2019)
10. Heiland, E., Hillmann, P.: (B)LOCKBOX – Secure Software Architecture with Blockchain Verification. The European Multidisciplinary Society for Modelling and Simulation Technology (EUROSIS) (2022)
11. Cramer, R., Shoup, V.: Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack. Aarhus University, New York University (2003)
12. Hillmann, P., Knüpfer, M., Guggemos, T., Streit, K.: CAKE: An Efficient Group Key Management for Dynamic Groups. INFOCOMP Journal of Computer Science 18(2) (2019)
13. Shannon, C.E.: A Mathematical Theory of Cryptography. Communication Theory of Secrecy Systems (1946)
14. Bellare, M., Desai, A., Pointcheval, D., Rogaway, P.: Relations among notions of security for public-key encryption schemes. Springer, Advances in Cryptology (CRYPTO) (1998)
15. Bernstein, D.J.: The libpqcryptosoftware library forpost-quantum cryptography (2018), https://cr.yp.to/talks/2018.05.09/slides-djb-20180509-libpqcrypto-4x3.pdf
16. Pfitzmann, A.: Security in IT Networks: Multilateral Security in Distributed and by Distributed Systems (2006)
17. Merkle, R.C.: Secure Communications Over Insecure Channels. In: Communications of the ACM. 21. pp. 294–299 (1978)
18. Communications Electronics Security Group: The Possibility of Secure Non-Secret Digital Encryption. Research Report No. 3006 (1970), https://www.gchq.gov.uk/sites/default/files/document_files/CESG_Research_Report_No_3006_0.pdf
19. Diffie, W., Hellmann, M.E.: New Directions in Cryptography. IEEE Transactions on Information Theory (1976)
20. Rivest, R.L., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM (1978)
21. Merkle, R., Hellman, M.: Hiding information and signatures in trapdoor knapsacks. IEEE Transactions on Information Theory 24(5), 525–530 (1978)
22. Shamir, A.: A polynomial-time algorithm for breaking the basic merkle - hellman cryptosystem. IEEE Transactions on Information Theory 30(5), 699–704 (1984)
23. McEliece, R.J.: A Public-Key Cryptosystem Based on Algebraic Coding Theory. Deep Space Network Progress Report pp. 114–116 (1978)
24. Rabin, M.O.: Digitalized signatures and public-key functions as intractable as factorization. MIT-LCS-TR 212, MIT Laboratory for Computer Science (1979)
25. Chor, B., Rivest, R.L.: A Knapsack Type Public Key CryptosystemBased On Arithmetic in Finite-Fields. Advancesin Cryptology: Proceedingsof CRYPTO, Springer pp. 54–65 (1984)
26. ElGamal, T.: A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory pp. 469–472 (1985)
27. Hoffstein, J., Pipher, J., Silverman, J.: NTRU: A Ring-Based Public Key Cryptosystem. International Algorithmic Number Theory Symposium (1998)
28. Paillier, P.: Cryptosystems Based on Composite Residuosity (1999), École Nationale Supérieure des Télécommunications
29. National Institute of Standards and Technology: NIST Announces First Four Quantum-Resistant Cryptographic Algorithms (2022), https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

30. The European Union Agency for Cybersecurity (ENISA): Post-Quantum Cryptography - Integration study (2022), https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study/@@download/fullReport
31. Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D., Liu, Y.K.: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8413 (2022)
32. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. ACM symposium on Theory of computing (STOC) (2005)
33. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehle, D.: CRYSTALS-Kyber. IEEE European Symposium on Security and Privacy (EuroS&P) (2018), https://pq-crystals.org/kyber/resources.shtml
34. Dubrova, E., Ngo, K., Gärtner, J.: Breaking a fifth-order masked implementation of crystals-kyber by copy-paste. Cryptology ePrint Archive, Paper 2022/1713 (2022), https://eprint.iacr.org/2022/1713, https://eprint.iacr.org/2022/1713
35. Couveignes, J.M.: Hard homogeneous spaces. Cryptology ePrint Archive, Paper 2006/291 (2006), https://eprint.iacr.org/2006/291, https://eprint.iacr.org/2006/291
36. Rostovtsev, A., Stolbunov, A.: Public-Key Cryptosystem based on Isogenies (2006)
37. Feo, L.D., Jao, D., Plut, J.: Towards Quantum-Resistant Cryptosystems from Supersingulare Elliptic Curve Isogenies. PQCrypto, Springer (2011)
38. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. Cryptology ePrint Archive (2022), https://eprint.iacr.org/2022/975, https://eprint.iacr.org/2022/975
39. Azarderakhsh, R., Koziel, B., Campagna, M., LaMacchia, B., Costello, C., Longa, P., Feo, L.D., Naehrig, M., Hess, B., Renes, J., Jalali, R.A., Soukharev, V., Jao, D., Urbanik, D.: Supersingular Isogeny Key Encapsulation. NIST PQCrypto candidates (2018), https://csrc.nist.gov/CSRC/media/Presentations/SIKE/images-media/SIKE-April2018.pdf
40. Steven D. Galbraith, Christophe Petit, Barak Shani, Yan Bo Ti: On the security of supersingular isogeny cryptosystems. IACR Cryptol. ePrint Arch. (2016)
41. National Institute of Standards and Technology: NIST Issues First Call for Lightweight Cryptography to Protect Small Electronics (2018), https://www.nist.gov/news-events/news/2018/04/nist-issues-first-call-lightweight-cryptography-protect-small-electronics
42. Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure againstadaptive chosen ciphertext attack. Advaces in Cryptology (Crypto), LNCS Springer 1462, 13–25 (1998)
43. Zhu, H.: A Practical Elliptic Curve Public Key Encryption Scheme Provably Secure Against Adaptive Chosen-message Attack. Cryptology ePrint Archive, Paper 2003/087 (2003), https://eprint.iacr.org/2003/087, https://eprint.iacr.org/2003/087
44. Giry, D.: Cryptographic Key Length Recommendation. BlueKrypt (2023), https://www.keylength.com/en/4/
45. Miller, V.S.: Use of elliptic curves in cryptography. Lecture Notes in Computer Science 218, 417–426 (1986)
46. Koblitz, N.: Elliptic curve cryptosystems. Mathemathic Computation 48, 203–209 (1987)
47. Seet, M.Z.: Elliptic Curve Cryptography: Improving the Pollard-Rho Algorithm. Ph.D. thesis (2007)
48. Bertoni, G., Daemen, J., Peeters, M., Assche, G.V.: The Keccak reference (2011)
49. Ferguson, N., Lucks, S., Schneier, B., Whiting, D., Bellare, M., Kohno, T., Callas, J., Walker, J.: The Skein Hash Function Family (2010)
50. Brown, D.R.L.: SEC 2: Recommended Elliptic Curve Domain Parameters. Standards for efficient Cryptography 2 (SEC 2), Certicom Research (2010), http://www.secg.org/sec2-v2.pdf
51. Langley, A., Hamburg, M., Turner, S.: Elliptic Curves for Security (RFC 7748). Internet Research Task Force (IRTF) (2016), https://www.ietf.org/rfc/rfc7748.txt
52. Bernstein, D.J., Lange, T.: SafeCurves: choosing safe curves for elliptic-curve cryptography. Rigidity (2013), http://safecurves.cr.yp.to/rigid.html
53. Roy, M., Deb, N., Kumar, A.J.: Point Generation And Base Point Selection In ECC: An Overview. International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE) 3, 6711–6713 (2014)
54. Costello, C., Jao, D., Longa, P., Naehrig, M., Renes, J., Urbanik, D.: Efficient compression of SIDH public keys. Cryptology ePrint Archive: Report 2016/963 (2016)
55. Hastad, J.: A Provably Secure Public-Key Cryptosystem. Seminars in Theoretical Computer Science at NADA, KTH (2003)
56. D., S., Galbraith, Petit, C., Shani, B., Ti, Y.B.: On the security of supersingular isogeny cryptosystem. IACR (2016)
57. Chen, R.: Cramer-Shoup Encryption. University of Wollongong (2014)
58. Peter Wiliston Shor: Algorithms for quantum computation: Discrete logarithms and factoring. Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press pp. 124–134 (1994)

59. Burr, T.: Shhh ... NSA's Utah Data Center may be open already (2013), https://archive.sltrib.com/article.php?id=56915018&itype=CMSID
60. Roetteler, M., Naehrig, M., Svore, K.M., Lauter, K.: Quantum resource estimates for computing elliptic curve discrete logarithms. Quantum Physics (2017)
61. National Institute of Standards and Technology: Recommendation forKey Managem. NIST Special Publication 8 (2020)
62. Federal Office for Information Security: Cryptographic Mechanisms:Recommendations and Key Length. BSI Technical Guide, BSI TR-02102 (2023), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile
63. Jao, D., Feo, L.D.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: International Workshop on Post-Quantum Cryptography. pp. 19–34 (2011)
64. Feo, L.D., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, pp. 209–247 (2014)
65. Velu, J.: Isogenies entre courbes elliptiques. Comptesrendus de la Academie des Sciences (1971)
66. Montgomery, P.L.: Speeding the pollard and elliptic curve methods of factorization. Mathematics of computation 48, 243–264 (1987)
67. Biasse, J.F., Jao, D., Sankar, A.: A quantum algorithm for computing isogenies between supersingular elliptic curves. CACR (2014)
68. Tani, S.: Claw finding algorithms using quantum walk. Theoretical Computer Science (2009)
69. Adj, G., Cervantes-Vzquez, D., Chi-Domnguez, J.J., Menezes, A., Rodrguez-Henrquez, F.: On the cost of computing isogenies between supersingular elliptic curves. Cryptology ePrint Archive, Report 313 (2018)

Authors

Peter Hillmann is a postdoctoral researcher and scientific in computer science. He received a M.Sc. in Information-System-Technology from Dresden University of Technology (2011) and a Dr. rer. nat. (Ph.D. in science) degree in Computer Science (2018) from the Universität der Bundeswehr München. He provides expert reports for national and international organizations. His research interests include system and network security with focus on cryptography and IP geolocation as well as middleware technologies and enterprise architecture.