UDC 004.056.55

ESSENCE AND CONDITIONS OF IMPLEMENTATION OF THE ATTACK BASED ON RELATED KEYS RELATIVELY ELECTRONIC SIGNATURES IBS-1 AND IBS-2 DSTU ISO/IEC 14888-3

Marina Yesina[1], Yuriy Gorbenko [1], Vladislav Kulibaba[1]

[1] V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine
m.v.yesina@karazin.ua, gorbenkoU@iit.kharkov.ua, vlad.kulibaba1994@gmail.com

Reviewer: Roman Oliynikov, Doctor of Sciences (Engineering), Full Professor, V. N. Karazin Kharkiv National University,
6 Svobody Sq., Kharkiv, 61022, Ukraine
roliynykov@gmail.com

Received on July 2018

Abstract: *The paper deals with the state of protection electronic signatures based on the pairing of points of an elliptic curve against attacks based on the signing data with related keys. It is defined conditions and possibilities of the organization and implementation of these attacks. It is provided the recommendations on protection against these vulnerabilities, including in the post-quantum period.*

Keywords: *attack; electronic signature; elliptic curve; related keys; pairing.*

1 Introduction

Electronic signatures (ES) are now widespread, the stability of which is based on the complexity of discrete logarithm in finite fields and groups of elliptic curves (EC) points [3-5]. Also, researches were conducted and ES with appendix based on identity – the pairing of EC points are recommended for the application. Known conditions for implementation attacks based on related keys relative to ES based on standardized cryptographic transformations in finite fields and cyclic groups of supersingular curves. The conducted analysis of a large number of sources made it possible to conclude that there is no data regarding the security and conditions for implementation of attacks based on related keys with respect to ES IBS-1 and IBS-2 [1, 3-5], that are based on identity. At the same time, previous studies of the algorithms ES IBS-1 and IBS-2 stability showed that attack based on related keys can be implemented. Therefore, it is important to study the stability of these ES against attacks based on related keys.

Stability issues have become particularly relevant after statements and speeches of leading specialists about the potential vulnerabilities for the ES in the post-quantum period. Thus, the technical report of the US NSA [1] states that the ES, whose algorithms are based on transformation in the ring [1-2] and in the finite field [1-2], will be unstable with the appearance of quantum computers. The same suspicions are expressed in relation to cryptographic transformations in the group of elliptic curve points [1-2]. Therefore, the tasks and their solutions regarding the stability of the ES, which are now introduced in Ukraine and which operate on the international level, are important. Such standard should include DSTU ISO/IEC 14888-3:2014 [5].

One of the possible ways of solving this contradiction is to increase the size of the general parameters for the specified transformations. At the first stage of quantum cryptography development, this may work. But in the future it is necessary to apply other methods, for example, perhaps cryptographic transformation based on pairing of EC points and identification data. Such algorithms are offered in the DSTU ISO/IEC 14888-3:2014 in the form of algorithms ES IBS-1 and IBS-2 [5]. But the analysis showed that although they under certain conditions may qualify for post-quantum, further studies of their stability are needed. In our view, one of the vulnerabilities of the algorithms ES IBS-1 and IBS-2 is their vulnerability to attacks based on related keys.

The purpose of this article is to analyze the state of protection of the ES IBS-1 and IBS-2 against the attacks based on the signed data with related keys, determine the conditions and possibilities for their organization and implementation, as well as the development of recommendations for the protection against the specified vulnerabilities, including post-quantum period.

2 The essence of ES IBS-1 and IBS-2, defined and implemented in DSTU ISO/IEC 14888-3

Given the novelty and the need to formulation of research problem of the ES IBS-1 and IBS-2, first we will consider the essence of these ES mechanisms and setup stages.

For the use of ES IBS-1 and IBS-2, at first, the general parameters must be entered and configured and asymmetric key pairs are generated.

The general parameters of the ES IBS-1 and IBS-2 are [3-5]:

- U – secret master key – integer, $U \in [1, q-1]$;
- V – public master key – EC point, $V = [U]P \bmod q$, $V \in G_1$;
- X – private (secret) signer key – EC point, $X = [U]Y \bmod q$, $X \in G_1$;
- Y – signer public key (verification) – EC point, $Y = H_1(ID) \bmod q$, $Y \in G_1$;
- P – base point of the key certification center of the order q.

General parameters generation or computation must be carried out under the following conditions:

- the user personal key X is calculated at his request in the key center generation (KCG) and provided to the user through a secure channel;
- the user public key Y can be calculated by each user of the domain;
- ID – is a data string that contains the signer identifier;
- H_1 – the hash function, which converts the data string into the element of group G_1;
- H_2 – the hash function defined in DSTU ISO/IEC 10118-3:2005;
- G_1 – a cyclic group of simple order q whose elements are EC points over $GF(p)$;
- G_2 – a cyclic group of simple order q whose elements are elements of a finite field $GF(p^m)$.

Tables 1 and 2 show the signing and verification mechanisms of IBS-1 and IBS-2 [5].

Table 1 – ES IBS-1 mechanism

Message signing	Signature verification
1) Generate a random or pseudo-random one-time secret key – an integer K, $1 < K < (q-1)$.	1) Verifier receives integral general parameters and subscriber public key.
2) Pairing: $\Pi = < X, P >^K$, $\Pi \in G_2$ over the field $GF(p^m)$, Π – pre-signature	2) Restoring one-time public key: – R and S recovered from the addition; – bit length R should be equal to the length of the function output H_2; – $S \in G_1$. If at least one of these conditions is not fulfilled, the signature is rejected.
3) Message in the form of an integer M is divided into its parts: M_2 – empty part, $M_1 = M$ – a message that needs to be signed.	3) Preparing to verify the message: – recovery M from signed message; – splitting message on M_1 & M_2: M_2 – empty, $M_1 = M$.
4) Calculating one-time public key: $R = H_2(M_1 \| FE2BS(\Pi))$, $R \in G_2$.	4) Restore parameter T: $T = (T_1, T_2)$, $T_1 = -Y$, $T_2 = [R]Y$.

Continuation of Table 1

Message signing	**Signature verification**
5) Calculate parameter T: $T=(T_1,T_2)=(-Y,[R]Y)$.	5) Pairing: $\overline{\Pi}=<S,P>\times<Y,V>^{R}$.
6) Calculate signature component: $S=[K-R]X \bmod q$, $S\in G_1$. Signature is $\Sigma=(R,S)$.	6) One-time validation public key calculation: $\overline{R}=H_2(M_1 \,\|\, FE2BS(\overline{\Pi}))$.
7) Construction of the addition with the concatenation of the text in the form $(R,S)\,\|\,text$.	7) Comparison $\overline{R}=R$: if they do not match, the signature is false, otherwise – true.
8) Building the signed message in the form $M((R,S)\,\|\,text)$.	

Table 2 – ES IBS-2 mechanism

Message signing	**Signature verification**
1) Generate a random or pseudo-random one-time secret key – an integer K, $1<K<(q-1)$.	1) Verifier receives integral valid general parameters and valid subscriber public key.
2) Scalar Multiplication: $\Pi=[K]Y \bmod q$, $\Pi\in G_1$, Π – pre-signature, EC point.	2) Restoring one-time public key: – R and S recovered from the addition; – $R\in G_1$, $S\in G_1$. If at least one of these conditions is not fulfilled, the signature is rejected.
3) Message in the form of an integer M is divided into its parts: M_1 – empty part, $M_2=M$ – a message that needs to be signed.	3) Preparing to verify the message: – recovery M from signed message; – splitting message on M_1 & M_2: M_1 – empty, $M_2=M$.
4) Calculating one-time public key $R=\Pi$, $R\in G_1$.	4) Restore parameter T: $T=(T_1,T_2)$, $T_1=-Y$, $T_2=[-H]Y$, $H=H_2(M_2 \,\|\, FE2BS(R_x))$.
5) Calculate parameter T: $T=(T_1,T_2)=(-Y,[-H]Y)$, $H\in G_2$, $H=H_2(M_2 \,\|\, FE2BS(\Pi_x))$.	5) Calculating pre-signature: $\overline{\Pi}=R$, $\overline{\Pi}\in G_1$.
6) Calculate signature component: $S=[K+H]X \bmod q$, $S\in G_1$. Signature is $\Sigma=(R,S)$.	6) Calculating: $\overline{R}_1=<P,S>$ та $\overline{R}_2=<V,\overline{\Pi}+[H]Y>$.
7) Building the addition: $(R,S)\,\|\,text$.	7) Comparison $\overline{R}_1=\overline{R}_2$: if they do not match, the signature is false, otherwise – true.
8) Building the signed message: $M((R,S)\,\|\,text)$.	

3 Attack "Full Disclosure" against ES IBS-1 based on signed data and related keys

Let the cryptanalyst intercepts and has a full access to i signed messages [2,5]:

$$\begin{cases} S_1=[K_1-R_1]X \bmod q \\ \ldots\ldots \\ S_i=[K_i-R_i]X \bmod q \end{cases}. \qquad (1)$$

The system (1) includes i equations and $i+1$ unknowns.

Find an unknown EC point – a private long-term key X, which is permanent for all signatures. As a result, we obtain the system of the form:

$$\begin{cases} X = [K_1 - R_1]^{-1} S_1 \bmod q \\ \dots \\ X = [K_i - R_i]^{-1} S_i \bmod q \end{cases}. \tag{2}$$

In system (2) private long-term key X is unknown and i unknowns $K_1, K_2, ..., K_i$. For full disclosure, that is, the definition of a secret key X by i ES, it is necessary to solve the system of the i-th order with the $i+1$ unknowns. The analysis showed that it is practically impossible to reduce the system of equations order by the force method. Therefore, we can assume that the attack based on signed data has an exponential complexity [2, 5].

As the analysis showed, one of the possible variants of lowering the system of equations order can be the key related, for example, in the form [2]:

$$K_1 + K_2 = q \tag{3}$$

or otherwise. Consider an attack based on related keys.

We write the system (1) for the case of two equations, and consider the signature algorithms for the two messages M_1 and M_2, and keys that satisfy the condition (3).

For message M_1	For message M_2
$K_1 \in [1, q-1]$	$K_2 = (q - K_1) \in [1, q-1]$
$\Pi_1 = < X, P >^{K_1}$	$\Pi_2 = < X, P >^{K_2}$
$R_1 = H_2(M_1 \parallel FE2BS(\Pi_1))$	$R_2 = H_2(M_2 \parallel FE2BS(\Pi_2))$
$S_1 = [K_1 - R_1] X \bmod q$	$S_2 = [(q - K_1) - R_2] X \bmod q$

Next we find a condition in which $S_1 = S_2$, that is, we will find a personal key X, in which ES of messages M_1 and M_2 coincide. As a result, we have:

$$[K_1 - R_1] X \bmod q = [(q - K_1) - R_2] X \bmod q. \tag{4}$$

We reduce in (4) by X, as a result we obtain:

$$[K_1 - R_1] \bmod q = [(q - K_1) - R_2] \bmod q; \tag{5}$$

$$[K_1 - R_1] \bmod q = [-K_1 - R_2] \bmod q; \tag{6}$$

$$2K_1 \bmod q = [R_1 - R_2] \bmod q. \tag{7}$$

Next we will find from (7) a one-time key K_1, since R_1 and R_2 are known and are contained in the signature:

$$K_1 = \frac{R_1 - R_2}{2} \bmod q. \tag{8}$$

Thus, the system of equations order is reduced to an unknown one-time secret key, in our case K_1:

$$\begin{cases} X = [K_1 - R_1]^{-1} S_1 \bmod q \\ \dots \\ X = [K_i - R_i]^{-1} S_i \bmod q \end{cases}. \tag{9}$$

Substituting K_1, and in general K_j, into system (9), we have a system of i equations with i unknowns, which has a solution.

4 Attack "Full Disclosure" against ES IBS-2 based on signed data and related keys

Analogously to (1), for IBS-2, taking into account Table 2, we have [2,5]:

$$\begin{cases} S_1 = [K_1 + H_1]X \bmod q \\ \ldots\ldots\ldots \\ S_i = [K_i + H_i]X \bmod q \end{cases}. \tag{10}$$

Next, we will find from (10) a private long-term key X and we will receive the following for it:

$$\begin{cases} X = [K_1 + H_1]^{-1} S_1 \bmod q \\ \ldots \\ X = [K_i + H_i]^{-1} S_i \bmod q \end{cases}. \tag{11}$$

System (10) includes i equations and $i+1$ unknowns in receiving i signed messages. The main task of the cryptanalysis is to identify the private long-term key X.

As in the case (2), as shown by the analysis, it is practically impossible to reduce the system of equations (11) by force. Moreover, the complexity of a force attack is determined by the order of the cyclic group q. Therefore, we can assume that the complexity of the attack based on the signed data is exponential [2,5].

At the same time, as in the case (2), one of the possible options of the system of equations (11) reduction may be the key related, for example, in the form (3) or another way [2].

We write the system (11) for the case of two equations and specified key related, and consider the signature algorithms for the two messages M_1 and M_2, and keys that satisfy the condition (3).

For message M_1	For message M_2
$K_1 \in [1, q-1]$	$K_2 = (q - K_1) \in [1, q-1]$
$\Pi_1 = [K_1]Y \bmod q$	$\Pi_2 = [K_2]Y \bmod q =$
	$= [q - K_1]Y \bmod q =$
	$= [-K_1]Y \bmod q$
$R_1 = \Pi_1$	$R_2 = \Pi_2$
$S_1 = [K_1 + H_1]X \bmod q$	$S_2 = [K_2 + H_2]X \bmod q =$
	$= [(q - K_1) + H_2]X \bmod q =$
	$= [-K_1 + H_2]X \bmod q$

We find a condition in which $S_1 = S_2$. As a result, we have

$$[K_1 + H_1]X \bmod q = [(q - K_1) + H_2]X \bmod q. \tag{12}$$

Reduce (12) at X, we obtain that:

$$[K_1 + H_1] \bmod q = [(q - K_1) + H_2] \bmod q$$

or

$$[K_1 + H_1] \bmod q = [-K_1 + H_2] \bmod q$$

and

$$2K_1 \bmod q = [H_2 - H_1] \bmod q. \tag{13}$$

Finally, from (13) we obtain that

$$K_1 = \frac{H_2 - H_1}{2} \bmod q . \tag{14}$$

Thus, the system of equations (11) order is reduced, since the values of H_1 and H_2 can be used to define an unknown one-time secret key K_1.

5 An example of the "Full Disclosure" attack against the mechanisms ES IBS-1 and IBS-2 based on signed data and related keys

Let's show the correctness of the execution of attacks on the example. Determine the value of the required parameters – the value of the base point P, the user private key X and the order of the base point q: $X = (13,16)$, $P = (13,7)$, $q = 7$. EC over the main field: $y^2 = (x^3 + x + 1) \bmod 23$.

Consider an example for the mechanism IBS-1 [3-5].

We write the system (1) for the case of two equations and consider the signature algorithms for the two messages M_1 and M_2, and keys that satisfy the condition (3).

For message M_1

$K_1 = 6$

$\Pi_1 = < X, P >^{K_1}$

$R_1 = H_2(M_1 \,\|\, FE2BS(\Pi_1)); R_1 = 4$

$S_1 = [K_1 - R_1]X \bmod q$

$S_1 = [6-4](13,16) \bmod 7 =$

$= 2(13,16) \bmod 7 = (5,19)$

For message M_2

$K_2 = (q - K_1) = 1$

$\Pi_2 = < X, P >^{K_2}$

$R_2 = H_2(M_2 \,\|\, FE2BS(\Pi_2)); R_2 = 20$

$S_2 = [K_2 - R_2]X \bmod q$

$S_2 = [1-20](13,16) \bmod 7 =$

$= (-19)(13,16) \bmod 7 = (5,19)$

According to formula (8) for K_1 we obtain:

$$K_1 = \frac{4-20}{2} \bmod 7 = \frac{-16}{2} \bmod 7 = (-8) \bmod 7 = 6 .$$

Let's solve the equation from the system (2), by substituting the obtained value K_1:

$$X = [K_1 - R_1]^{-1} S_1 \bmod q ;$$

$$X = [6-4]^{-1}(5,19) \bmod 7 = (2)^{-1}(5,19) \bmod 7 .$$

Find the inverse element in the field:

$$z = \frac{1}{k} \bmod q ;\; z \cdot k = 1 \bmod q ; z \cdot 2 = 1 \bmod 7 ;\; z = 4 .$$

So, after finding the inverse element, we obtain the following:

$$X = 4(5,19) \bmod 7 = (13,16) .$$

We found the value of the signer private key X. Compare it with X:

$$X = (13,16), X = (13,16) \Rightarrow X = X .$$

Consequently, for mechanism IBS-1, the considering attack is realizing.

Consider an example for the mechanism IBS-2 [3-5].

We write the system (10) for the case of two equations and consider the signature algorithms for the two messages M_1 and M_2, and keys that satisfy the condition (3).

For message M_1

$$\begin{aligned}
&K_1 = 6\\
&\Pi_1 = [K_1]Y \bmod q\\
&\Pi_1 = 6(17,20) \bmod 7 =\\
&\quad = (17,3)\\
&R_1 = \Pi_1 = (17,3)\\
&S_1 = [K_1 + H_1]X \bmod q \quad H_1 = 3\\
&S_1 = [6+3](13,16) \bmod 7 =\\
&\quad = 2(13,16) \bmod 7 = (5,19)
\end{aligned}$$

For message M_2

$$\begin{aligned}
&K_2 = (q - K_1) = 1\\
&\Pi_2 = [-K_1]Y \bmod q\\
&\Pi_2 = -6(17,20) \bmod 7 =\\
&\quad = (17,20)\\
&R_2 = \Pi_2 = (17,20)\\
&S_2 = [(q-K_1) - R_2]X \bmod q \quad H_2 = 15\\
&S_2 = [-6+15](13,16) \bmod 7 =\\
&\quad = 2(13,16) = (5,19)
\end{aligned}$$

According to formula (14) for K_1 we obtain:

$$K_1 = \frac{15-3}{2} \bmod 7 = \frac{12}{2} \bmod 7 = 6 .$$

Let's solve the equation from the system (11), by substituting the obtained value K_1:

$$X = [K_1 + H_1]^{-1} S_1 \bmod q ;$$

$$X = [6+3]^{-1}(5,19) \bmod 7 = (9)^{-1}(5,19) \bmod 7 .$$

Find the inverse element in the field:

$$z = \frac{1}{k} \bmod q \, ; \, z \cdot k = 1 \bmod q \, ; \, z \cdot 9 = 1 \bmod 7 ; \; z = 4 .$$

So, after finding the inverse element, we obtain the following:

$$X = 4(5,19) \bmod 7 = (13,16) .$$

We found the value of the signer private key X . Compare it with X :

$$X = (13,16), X = (13,16) \Rightarrow X = X .$$

Consequently, for mechanism IBS-2, the considering attack is realizing.

6 An example of the "Full Disclosure" attack against the mechanisms ES IBS-1 and IBS-2 based on signed data and related keys: alternative approach

Let the cryptanalyst intercepts and has a full access to i signed messages: similar to (1) and (10).

Find an unknown point of the EC – a private long-term key X , which is permanent for all signatures. Consider an attack on the ES IBS-1 based on the key related. Input data will be the similar to those given in section 3 [5].

As a result, we obtain for IBS-1 the following system:

$$\begin{aligned}
&\begin{cases} S_1 = [K_1 - R_1]X \bmod q \\ S_2 = [-K_1 - R_2]X \bmod q \end{cases}\\
&S_1 + S_2 = [(K_1 - R_1) + (-K_1 - R_2)]X \bmod q\\
&S_1 + S_2 = [-R_1 - R_2]X \bmod q \qquad\qquad . \\
&X = (S_1 + S_2)[-R_1 - R_2]^{-1} \bmod q\\
&X = -[R_1 + R_2]^{-1}(S_1 + S_2) \bmod q
\end{aligned} \tag{15}$$

Consider an attack on the ES IBS-2 based on the key related. Input data will be similar to the data given in section 4 [5].

As a result, we obtain for IBS-2 the following system:

$$\begin{cases} S_1 = [K_1 + H_1]X \bmod q \\ S_2 = [-K_1 + H_2]X \bmod q \end{cases}$$
$$S_1 + S_2 = [(K_1 + H_1) + (-K_1 + H_2)]X \bmod q \,. \tag{16}$$
$$S_1 + S_2 = [H_1 + H_2]X \bmod q$$
$$X = [H_1 + H_2]^{-1}(\mathrm{S}_1 + \mathrm{S}_2) \bmod q$$

Now let's give a mathematical example and correctness of attacks execution on an example.

First, consider an example for the mechanism IBS-1. Input data will be similar to the data given in section 5.

Using system (15), to find the signer private key X, we have the following:

$$\mathrm{X} = -[\mathrm{R}_1 + \mathrm{R}_2]^{-1}(\mathrm{S}_1 + \mathrm{S}_2) \bmod q\,;$$

$$\mathrm{X} = -[4 + 20]^{-1}((5{,}19) + (5{,}19)) \bmod 7\,;$$

$$\mathrm{X} = (-24)^{-1}(2(5{,}19)) \bmod 7\,.$$

Find the inverse element in the field:

$$z = \frac{1}{k} \bmod q\,; z \cdot k = 1 \bmod q\,;$$
$$z \cdot (-24) = 1 \bmod 7\,;\; z = 2\,.$$

So, after finding the inverse element, we obtain the following:

$$X \;= 2(17, 3) \bmod 7 = (13{,}16)\,; \tag{17}$$

$$X = (13{,}16), X = (13{,}16) \Rightarrow X = X\,.$$

So, according to (17), for mechanism IBS-1, the considering attack is realizing.

Let’s consider an example for the mechanism IBS-2. Input data will be similar to the data given in section 5.

Using system (16), to find the signer private key X, we have the following:

$$\mathrm{X} = [H_1 + H_2]^{-1}(\mathrm{S}_1 + \mathrm{S}_2) \bmod q\,;$$

$$\mathrm{X} = [3 + 15]^{-1}((5{,}19) + (5{,}19)) \bmod 7\,;$$

$$\mathrm{X} = [4]^{-1}(17, 3) \bmod 7\,.$$

Find the inverse element in the field:

$$z = \frac{1}{k} \bmod q\,; z \cdot k = 1 \bmod q\,; z \cdot 4 = 1 \bmod 7\,;\; z = 2\,.$$

So, after finding the inverse element, we obtain the following:

$$\mathrm{X} = 2(17, 3) \bmod 7 = (13{,}16)\,; \tag{18}$$

$$X = (13{,}16), X = (13{,}16) \Rightarrow X = X\,.$$

So, according to (18), for mechanism IBS-2, the considering attack can be implemented with polynomial complexity.

7 Proposals for ES IBS-1 and IBS-2 algorithms protection against attacks based on related keys

The analysis allows to propose the following mechanisms for protecting the ES IBS-1 and IBS-2 from attacks based on related keys [2,5].

1. Based on encryption of signed messages using symmetric or asymmetric ciphers. In terms of the complexity (*performance*) of encryption and stability, it is better to use symmetric ciphers–block or stream. Then cryptanalysis will need to solve the system with $2i+1$ unknowns, but for a system with i equations. Such task is exponentially complicated with real parameter values.

2. Another mechanism for protecting ES IBS-1 and IBS-2 against attacks based on related keys is the exclusion of the ability to relate one-time keys K in the process of signing a message flow. This can be done on the basis of the use of hardware or hardware-software ES means, which would exclude the possibility of interference in the process of signing messages. Other mechanisms of ES are also possible.

8 Conclusions and recommendations

1. In the process of ES improving, ES algorithms IBS-1 and IBS-2 on identifiers with pairing of EC points are proposed, in them as a private key is proposed to use the elliptic curve point X. As a result, when intercepting i signed messages to determine the long-term key X, it is necessary to solve a system of equations with $i+1$ unknown, i of which there are large random numbers, one is the EC point X. In the process of analysis, no effective methods have been identified for the solution of such system.

2. It was discovered that the ES IBS-1 and IBS-2 cryptographic transformation do not provide cryptographic resistance against attacks based on related key. At that, two different variants of attack based on related key were obtained.

3. For ES IBS-1 algorithm, attack based on related key can be accomplished using the obtained relations (8) and (9). Moreover, its complexity is polynomial.

4. For ES IBS-2 algorithm, attack based on related key can be accomplished using the obtained relations (11) and (14). Its complexity is also polynomial.

5. The possibility of attacks against ES algorithms IBS-1 and IBS-2 is confirmed not only by software simulation, but also by the examples given in section 5 of this paper.

6. Another method of attacking ES algorithms IBS-1 and IBS-, the essence of which is described in section 6 of this paper, in particular using systems (15) and (16), is also revealed. The above attacks also have a polynomial complexity. The ability to perform these attacks is also demonstrated in the examples.

7. Thus, both theoretically and in the examples, it is shown that the ES algorithms IBS-1 and IBS-2 are unstable against attacks based on related key, so if they are used, they must use protection mechanisms against such attacks.

8. Suggestions on possible options for protecting the ES for algorithms DSTU ISO/IEC 14888-3:2014 – IBS-1 and IBS-2 against attacks based on related key are also outlined above. The main ones are the encryption of signed messages and the use of qualified hardware and software ES.

References

[1] Koblitz N., Menezes A.J. A riddle wrapped in an enigma. URL: https://eprint.iacr.org/2015/1018.pdf.

[2] Gorbenko I.D., Gorbenko Yu.I. Prykladna kryptologija. Teorija. Praktyka. Zastosuvannja: monografija. Harkiv: Fort, 2012. 870 p.

[3] Gorbenko Yu.I., Ganzja R.S., Akol'zina O.S. Elektronni pidpysy na osnovi identyfikatoriv ta binarnogo vidobrazhennja. Prikladnaya radioelektronika. 2015. T. 14, № 4. pp. 284–290.

[4] Gorbenko Yu.I., Jesina M.V., Kulibaba V.A. Sutnist' ta umovy zdijsnennja ataky na zv'jazanyh kljuchah vidnosno elektronnyh pidpysiv IBS-1 ta IBS-2 DSTU ISO/IEC 14888-3. Systemy obrobky informacii'. 2016. № 7(144). pp. 113–118.

[5] DSTU ISO/IEC 14888-3:2014 Informacijni tehnologii'. Metody zahystu. Cyfrovi pidpysy z dopovnennjam. Chast.3. Mehanizmy, shho g'runtujut'sja na dyskretnomu logaryfmi (ISO/IEC 14888-3:2008, IDT). 2014. 113 p.

Рецензент: Роман Олійников, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, майдан Свободи 6, м. Харків, 61022, Україна.
E-mail: roliynykov@gmail.com

Надійшло: Липень 2018.

Автори:
Марина Єсіна, к.т.н., старший викладач кафедри безпеки інформаційних систем і технологій, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: m.v.yesina@karazin.ua

Юрій Горбенко, к.т.н., провідний науковий співробітник, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: gorbenkoU@iit.kharkov.ua

Владислав Кулібаба, аспірант кафедри безпеки інформаційних систем і технологій, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: vlad.kulibaba1994@gmail.com

Сутність та умови здійснення атаки на зв'язаних ключах відносно електронних підписів IBS-1 та IBS-2 ДСТУ ISO/IEC 14888-3.

Анотація. У роботі розглядається стан захищеності електронних підписів на основі спарювання точок еліптичної кривої від атак на основі підписаних даних зі зв'язаними ключами. Визначаються умови та можливості організації та реалізації цих атак. Надаються рекомендації відносно захисту від вказаних вразливостей, в тому числі у постквантовий період.

Ключові слова: атака; електронний підпис; еліптична крива; зв'язані ключі; спарювання.

Рецензент: Роман Олейников, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина.
E-mail: roliynykov@gmail.com

Поступила: Июль 2018.

Авторы:
Марина Есина, к.т.н., старший преподаватель кафедры безопасности информационных систем и технологий, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина.
E-mail: m.v.yesina@karazin.ua

Юрий Горбенко, к.т.н., ведущий научный сотрудник, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина.
E-mail: gorbenkoU@iit.kharkov.ua

Владислав Кулибаба, аспирант кафедры безопасности информационных систем и технологий, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина.
E-mail: vlad.kulibaba1994@gmail.com

Сущность и условия выполнения атаки на связанных ключах относительно электронных подписей IBS-1 и IBS-2 ДСТУ ISO/IEC 14888-3.

Аннотация. В работе рассматривается состояние защищенности электронных подписей на основе спаривания точек эллиптической кривой от атак на основе подписанных данных со связанными ключами. Определяются условия и возможности организации и реализации этих атак. Предоставляются рекомендации относительно защиты от указанных уязвимостей, в том числе в пост квантовый период.

Ключевые слова: атака; электронная подпись; эллиптическая кривая; связанные ключи; спаривание.