UDC 004.056.55

BLIND ELECTRONIC SIGNATURE MECHANISMS ON ELLIPTIC CURVES IMPROVEMENT

I. Gorbenko, M. Yesina, V. Ponomar

V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
gorbenkoi@iit.kharkov.ua, rinayes20@gmail.com, Laedaa@gmail.com

Reviewer: Alexandr Potii, Doctor of Sciences (Engineering), Full Professor, Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
potav@ua.fm

Received February 2016

Abstract. *The work is devoted to consideration the blind electronic signature mechanisms based on algorithms, described in ISO/IEC 14888-3:2006 and national standard DSTU 4145-2002. It is tested protocol security based on these algorithms by the anonymity criterion. It is proved, that the considered protocol is protected by the anonymity criterion, that is impossible to identify the author of the signed document.*

Keywords*: anonymity electronic signature, blind signature.*

1 Introduction

The requirement of providing electronic anonymity service (non-traceability), for example, in systems of secret electronic voting, electronic money and so on is mandatory in some applications of electronic trust services. Recognized mechanism of providing anonymity service is the use of blind signature mechanism. Blind is a signature, that is imposed on the previously disguised message by trust third face.

The recognition typical blind signature scheme involves, as usual, three faces [7]: signer – A, issuer of the document – B and verifier – C. The issuer creates a document that signer must sign anonymously. That is, the signer shouldn't know the document semantic content and final signature form. For this issuer masking document uses specific cryptographic conversion and sends it to the signer. Then signer signs the disguising document and sends it to the issuer. Issuer removes the disguising conversion from the document, and electronic signature (ES), created by the signer, remains under the document in an open type. Thus verifier gets signed document, that verifies its integrity, authenticity and sets authorship using the signer public key.

Considering the relevance, currently Committee ISO/IEC JTC1/SC27 (one of participant is Ukraine) developed the package of standards concerning electronic trust services. Blind signature is one of such services and concerning it is developing inter-national standard ISO/IEC DIS 18370-2 [2], which will regulate types of blind signature, its using and standardize the specific mechanisms, and blind signature protocols.

Blind ES mechanisms and protocols, based on GOST 34.10-2001, Schnorr and El Gamal algorithms are proposed in [7,8]. But nowadays in Ukraine ES algorithms, that defined in DSTU ISO/IEC 14888-3 and DSTU 4145-2002, are permitted or those, that are recommended for use. Therefore, the task of developing and detailed investigation of these ES algorithms in terms of their use in blind signature mechanisms is important. For this it is necessary to prove the safety of blind signature on elliptic curves mechanism and protocols in general, and the safety of protocols during their implementation using standards on ES, that are recommended for use. Also it is necessary to give the assessments to the cryptographic sustainability directly to ES methods and algorithms on elliptic curves.

The purpose of this article is identifying opportunities and conditions of implementation, justification and development of generalized mechanism of the safe blind ES on elliptic curves, and proof

the safety and determine the conditions of specific blind ES protocols implementation using specific algorithms, defined by DSTU ISO/IEC 14888-3 and DSTU 4145-2002.

2 General description of blind electronic signature mechanism on the elliptic curve

Let the blind ES on the elliptic curve mechanism (scheme) has interaction of three faces [7]: B – subscriber (issuer of the document/message m), A – the signer and verifier C. In this case verifier can be any of them, or a trusted third part. As indicated in the introduction, issuer creates a document m, that the signer has to sign anonymously, that is the signer doesn't have the access to its semantic content – in practice – to the real hash-value. For this purpose the issuer, getting the subscriber consent, disguising the document, and actually – hash-value, using specific cryptographic conversion and sends it to subscriber.

After signing the disguised document, signer sends it to the issuer. The issuer carries out the opposite, relatively disguise, transformation and removes it, leaving ES unharmed. Verifier, after receiving the signed document, verifies its integrity, authenticity and sets authorship using the signer public key.

The certain general parameters of cryptographic transformations on elliptic curves analysis must be previously generated and safe distributed by safe manner to ensure security of mechanism. The list of transformations and requirements to them are defined in the relevant standards [1,4]. Also, asymmetric key pairs for signers A must be generated, and verifier C must have access to signers public keys (certificates). The issuer must have general parameters and disguising and undisguising keys.

Signer A begins the signature statement stage directly [5-7]. He chooses a random or pseudo-random value of disposable ES key k, $1<k<(n-1)$ and calculates a point on elliptic curve $E=k\cdot G \bmod n=(x_E, y_E)$, where G – basic point with order n. Further signer A sends point E to the issuer B.

Issuer B computes hash-value h of message m and chooses a disguising parameter α, where $1<\alpha<(n-1)$. Then issuer calculates point $C=\alpha\cdot E \bmod n=(x_C, y_C)$, and also calculates values r and r' according to the following formulas:

$$r=x_C \bmod n \text{ and } r'=x_E \bmod n.$$

Issuer B uses to blind the valid hash-value h the obtained values r and r', for example, for EC DSA, gets h':

$$h'=(\frac{r'}{r}\cdot h) \bmod n.$$

Further issuer B sends the value h' to signer A, that using the obtained values h', r', session key k and his personal (private) key d, signs the disguised hash-value h' and gets s' for the selected standard, for example, for EC DSA:

$$s'=\frac{d\cdot r'+h'}{k} \bmod n,$$

and sends the value s' to the issuer B.

Issuer B authenticates the blinded signature s' using usual ES verification, that is defined in the relevant standard [1,4], using signer A public key Q. If s' is verified by B, that he forms from it message m blind signature in form $<r,s>$, that is undisguises s', turning it into s.

In signature $\{m,<r,s>\}$ verification, verifier calculates point $R=(x_R, y_R)$, using algorithm, that is specified in the relevant standard [1,4], and signer A public key Q.

Signature is considered to be authentic, if the following ratio is performed [7]:

$$r=x_R \bmod n,$$

where x_R – coordinate of point R.

3 Checking the protection mechanism for anonymity criterion

For blind signature schemes, unlike other varieties of ES, the attack of anonymity violation is actual. Assuming, that applied ES is resistant to all known and potential attacks, then blind signature mechanism have to prove the resistance to attack of anonymity violation for the proof its safety.

The essence of the attack on anonymity is concluded that it can be implemented by signer on condition, that he will have all known to him blind signature scheme parameters together with the issuer identifier for each signature statement session. Accumulated thereby database (DB) can be used in the attack, which is to try to determine the author of a certain document m with a signature $<r,s>$, which will be verified by the signer public key Q.

In the proposed protocol anonymous violation attack can be carried out, for example, as follows. Signer A for each row of his DB should calculate the possible blinding parameter α'. Then he, using calculated parameters (h',r',s'), for each DB row calculates point R'. Finally – row, in such way constructed DB, for which the ratio is executed

$$r = x_{R'} \bmod n,$$

indicates the message issuer. In practice point R' always coincides with the verification point R and does not depend on the parameters h',r',s' and, so, does not allow to identify the author of the document m. To prove this assertion in a standard electronic signature verification value R', that is calculated for the relevant standard is used. According to specified condition, the blind signature protocol is considered to protect for the anonymity criterion, because it is impossible to identify the author of the document m [7,8].

4 Safety analysis of blind ES against anonymity attack

As noted above, all algorithms are verified on anonymity and, even, if signer A will keep all parameters h',r',s', then later he can not establish a correspondence of these parameters for the issuer, for which the signature was made. But, if this is true for ECDSA algorithm fully, then for the other algorithms there is feature – α' is expressed by two ratios, that will take the same value only for the subscriber B, that formed final signature on these parameters. And the probability, that there will be yet another issuer, for which two expressions of α' will have the same value, equals 2^{-n}. So it is believed, that the blind signature mechanisms, implemented using, for example, EC GDSA, EC KCDSA and DSTU 4145-2002 provide a blind signature with traceability anonymity [6]. This is considered more detail below.

Point to a possible way of ensuring anonymity using hardware or hardware and software means of cryptographic information protection (CIP). The use of such means for blind signature, like the use of cryptographic modules for users key generation in the Certification Authority (CA). User can generate own key on the station in the center, but because of using certified means CIP, the user can be confident, that only he has the key and CA are not copies of this key.

Cryptographic means (module) for blind signature can be used in the same way. It is considered more detail. Let D be a micromodule, which will be recorded asymmetric key pair for signature implementation and ensure confidentiality on receipt blinded hash-value. In this case, signer A is only cryptographic module D operator, because he has no direct access to the keys. Also cryptographic module D can completely replace A, then the issuer B is granted access to work with the CIP means and signer is unnecessary in such condition.

In this case, the following operations are performed [6]:

1) subscriber B encrypts h' directly on the cryptographic module D public key;
2) obtained $E_D(h')$ is sent to D directly or using operator A;
3) D decrypts h' and creates s';
4) r' and s' sent to the issuer B, and h' is removed from D's memory.

Signer can not make an attack on anonymity, because he will not have one of the parameters, because of h' is processed only in D and A has not opportunity to decrypt $E_D(h')$.

The proposed mechanism, as the analysis revealed, can be used in providing services of blind ES in the clouds. Also it can be used at electronic voting. At the voting voter enters to the cabin, where there is an automated station and carries out a vote according to the paragraphs 1) – 4). The vote anonymity and confirmed the validity and integrity of each voice are ensured by using the blind signature mechanism and CIP means, that are programmed on this [6].

5 Blind electronic signature protocol based on DSTU ISO/IEC 14888-3:2006 (EC DSA)

At first it is built and performed detailed analysis of blind signature protocol for electronic signature algorithm EC DSA [1,5,6].

Signer A generates or chooses a random or pseudo-random value of private key d, $1 < d < (n-1)$ and calculates public key Q:

$$Q = d \cdot G \bmod n.$$

The signer A begins the signature statement stage directly. He chooses a random or pseudo-random value of one-time ES key k, $1 < k < (n-1)$ and calculates a point on elliptic curve E:

$$E = k \cdot G \bmod n = (x_E, y_E),$$

where G – basic point with order n.

After that signer A sends point E to the issuer B.

Issuer B computes hash-value h of message m:

$$h = H(m)$$

and chooses a disguising parameter α, where $1 < \alpha < (n-1)$.

Then issuer calculates point C:

$$C = \alpha \cdot E \bmod n = (x_C, y_C),$$

and also calculates values r and r' according to the following formulas:

$$r = x_C \bmod n \text{ and } r' = x_E \bmod n.$$

Issuer B uses to blind the valid hash-value h the obtained values r and r', gets h':

$$h' = (\frac{r'}{r} \cdot h) \bmod n.$$

Further issuer B sends the value h' to signer A, that using the obtained values h', r', session key k and his personal long-term key d, signs the disguised hash-value h', gets s' according to the ratio:

$$s' = \frac{d \cdot r' + h'}{k} \bmod n$$

and sends the obtained value s' to the issuer B.

Issuer B authenticates the blinded signature s' using usual ES verification, that is defined in the relevant standard, using signer A public key Q. For EC DSA [1]:

$$R' = (\frac{h'}{s'} \cdot G + \frac{r'}{s'} \cdot Q) \bmod n. \quad (1)$$

We're calculating R' according to (1) and point out, that the mathematical expression of the blind signature s' is verified by subscriber B:

$$R' = (\frac{h'}{\underline{d \cdot r' + h'}} \cdot G + \frac{r'}{\underline{d \cdot r' + h'}} \cdot Q) \bmod n = (\frac{h' \cdot k}{d \cdot r' + h'} \cdot G + \frac{r' \cdot k}{d \cdot r' + h'} \cdot dG) \bmod n =$$
$$= k \cdot G \frac{h' + d \cdot r'}{d \cdot r' + h'} \bmod n = E, \quad \textit{that is} \quad x_{R'} = x_E .$$

If s' is verified by B, that he forms from it message m blind signature in form $< r, s >$, previously turning s' into s:

$$s = \frac{s' \cdot (r / r')}{\alpha} \bmod n .$$

In signature $\{m, < r, s >\}$ verification, verifier calculates point $R = (x_R, y_R)$, using algorithm, that is specified in the relevant standard [1], and signer A public key Q:

$$R = (\frac{h}{s} \cdot G + \frac{r}{s} \cdot Q) \bmod n = (x_R, y_R) .$$

We point out, that the mathematical expression of the final signature s is verified by verifier:

$$R = (\frac{h}{s} \cdot G + \frac{r}{s} \cdot Q) \bmod n = \frac{dr + h}{s} \cdot G \bmod n = \frac{k\alpha G(dr + h)}{(dr' + h') \cdot r / r'} \bmod n =$$
$$= \frac{k\alpha G(dr + h)}{(dr' + \frac{r'}{r} \cdot h) \cdot r / r'} \bmod n = \frac{k\alpha G(dr + h)}{dr + h} \bmod n = k\alpha G \bmod n =$$
$$= \alpha E \bmod n = (x_R, y_R) = C = (x_C, y_C).$$

Signature is considered to be authentic, if the following ratio is performed [7]:

$$r = x_R \bmod n ,$$

where x_R – coordinate of point R.

In the proposed protocol anonymous violation attack can be carried out, for example, as follows. Signer A for each row of his DB should calculate the possible blinding parameter α':

$$\alpha' = \frac{s' \cdot (r / r')}{s} \bmod n .$$

Then he, using calculated parameters, for each DB row calculates point R':

$$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'}) .$$

Row, in such way constructed DB, for which the ratio is executed

$$r = x_{R'} \bmod n$$

indicates the message issuer. In practice point R' always coincides with the verification point R and does not depend on the parameters h', r', s' and, so, does not allow to identify the author of the document m.

To prove this assertion in a standard electronic signature verification value R', that is calculated for the relevant standard [1] is used. For EC DSA [1]:

$$R' = \alpha' \cdot E \bmod n = \frac{s' \cdot (r / r')}{s} \cdot E \bmod n = \frac{\underline{dr' + h'} \cdot \frac{r}{r'}}{s} \cdot E \bmod n =$$

$$= \frac{\frac{dr' + \frac{r'}{r} \cdot h}{k} \cdot \frac{r}{r'}}{s} \cdot E \bmod n = \frac{\frac{dr + h}{k}}{s} \cdot E \bmod n = \frac{dr + h}{ks} \cdot kG \bmod n =$$
$$= (\frac{dr}{s} \cdot G + \frac{h}{s} \cdot G) \bmod n = (\frac{r}{s} \cdot Q + \frac{h}{s} \cdot G) \bmod n.$$

According to specified condition, appropriate blind signature protocol is considered to protect for the anonymity criterion, because it is impossible to identify the author of the document m [7,8].

6 Determination the parameters for blind electronic signature protocol based on DSTU ISO/IEC 14888-3:2006 (EC GDSA)

The proof of blind electronic signature protocol safety for EC GDSA executes similarly to section 5. The results of analysis and parameters of blind signature protocol based on ES algorithm EC GDSA are shown in tables 1 and 2 [1].

Table 1 – Formulas for the blind and final signature and its verification

Parameters	EC GDSA
Blinded signature	$s' = (kr' - h')d \bmod n$
Blinded signature verification	$R' = (\frac{h'}{r'} \cdot G + \frac{s'}{r'} \cdot Q) \bmod n,\ r = x_{R'} \bmod n$
Final signature	$s = s' \cdot \frac{r}{r'} \cdot \alpha \bmod n$
Final signature verification	$R = (\frac{h}{r} \cdot G + \frac{s}{r} \cdot Q) \bmod n = (x_R, y_R),\ r = x_R \bmod n$

Table 2 – Parameters of blind electronic signature protocol and verification protocol protection for the anonymity criterion

Parameters	EC GDSA
Public key	$Q = d^{-1} \cdot G \bmod n$
Point E	$E = k \cdot G \bmod n = (x_E, y_E)$
Hash-value	$e = h(m)$
Point C	$C = \alpha \cdot E \bmod n = (x_C, y_C)$
Values r and r'	$r = x_C \bmod n,\ r' = x_E \bmod n$
Blinded hash-value	$h' = \frac{r'}{r} \cdot \frac{h}{\alpha} \bmod n$
Parameter for anonymity verification	$\alpha' = \frac{s}{s' \cdot \frac{r}{r'}} \bmod n,\ \alpha' = \frac{r}{r'} \cdot \frac{h}{h'} \bmod n$
Anonymity verification	$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'})$ => $R' = (\frac{h}{r} \cdot G + \frac{s}{r} \cdot Q) \bmod n$, $r = x_{R'} \bmod n$

7 Determination the parameters for blind electronic signature protocol based on DSTU ISO/IEC 14888-3:2006 (EC KCDSA)

The proof of blind electronic signature protocol safety for EC KCDSA executes similarly to section 5. The results of analysis and parameters of blind signature protocol based on ES algorithm EC KCDSA are shown in tables 3 and 4 [1].

Table 3 – Formulas for the blind and final signature and its verification

Parameters	EC KCDSA
Blinded signature	$s' = (k - e')d \bmod n$, $e = (r \oplus h) \bmod n$
Blinded signature verification	$R' = (e' \cdot G + s' \cdot Q) \bmod n$, $r = x_{R'} \bmod n$
Final signature	$s = s' \cdot \alpha \bmod n$
Final signature verification	$R = (e \cdot G + s \cdot Q) \bmod n = (x_R, y_R)$

Table 4 – Parameters of blind electronic signature protocol and verification protocol protection for the anonymity criterion

Parameters	EC KCDSA
Public key	$Q = d^{-1} \cdot G \bmod n$
Point E	$E = k \cdot G \bmod n = (x_E, y_E)$
Hash-value	$h = H(m)$
Point C	$C = \alpha \cdot E \bmod n = (x_C, y_C)$
Values r and r'	$r = H(x_C \parallel y_C) \bmod n$, $r' = H(x_E \parallel y_E) \bmod n$
Blinded hash-value	$h' = \frac{r \oplus h}{\alpha} \oplus r' \bmod n$
Parameter for anonymity verification	$\alpha' = \frac{s}{s'} \bmod n$, $\alpha' = \frac{r \oplus h}{r' \oplus h'} \bmod n$
Anonymity verification	$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'}) \Rightarrow$ $R' = (e \cdot G + s \cdot Q) \bmod n$, $r = x_{R'} \bmod n$

8 Determination the parameters for blind electronic signature protocol based on DSTU 4145-2002

The proof of blind electronic signature protocol safety for DSTU 4145-2002 executes similarly to section 5. The results of analysis and parameters of blind signature protocol based on ES algorithm DSTU are shown in tables 5 and 6 [4-6].

Table 5 – Formulas for the blind and final signature according to DSTU 4145-2002 and its verification

Parameters	DSTU
Blinded signature	$s' = (e + dr') \bmod n$
Blinded signature verification	$R' = (s' \cdot G + r' \cdot Q) \bmod n$, $r = x_{R'} \bmod n$
Final signature	$s = s' \cdot \alpha \bmod n$
Final signature verification	$R = (s \cdot G + r \cdot Q) \bmod n = (x_R, y_R)$

Table 6 – Parameters of blind electronic signature protocol and verification protocol protection by the anonymity criterion

Parameters	DSTU
Public key	$Q = -d \cdot G \bmod n$
Point E	$E = k \cdot G \bmod n = (x_E, y_E)$
Hash-value	$h = H(m)$
Point C	$C = \alpha \cdot E \bmod n = (x_C, y_C)$
Values r and r'	$r = h \cdot x_C \bmod n$, $r' = h' \cdot x_E \bmod n$
Blinded hash-value	$h' = \frac{x_C \cdot h}{x_E \cdot \alpha} \bmod n$
Parameter for anonymity verification	$\alpha' = \frac{s}{s'} \bmod n$, $\alpha' = \frac{x_C \cdot h}{x_E \cdot h'} \bmod n = \frac{r}{r'} \bmod n$
Anonymity verification	$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'})$ => $R' = (s \cdot G + r \cdot Q) \bmod n$, $r = x_{R'} \bmod n$

9 Safety analysis of blind signature protocol

It is necessary to perform blind signature verification on the protection from attacks on ES algorithms, because blind signature based on ordinary ES.

Blind signature uses ordinary ES algorithm, only when making final signature change of s' value is performed, using a special coefficient. Because this coefficient is not associated with key parameters, then this transformation not poses a threat to secret parameters at blind signature creation. That is such signature will have the same resistance as the ordinary ES.

9.1 Attack «Full Disclosure» based on signed data

The security of all ES algorithms, that were considered above, based on difficulty of solving discrete logarithm in the group of points an elliptic curve. It is necessary to solve the equations based on public key Q calculation, that are individual for each of the considered algorithms, relatively d, for finding the secret key [3].

As noted above, the same attacks exist for blind signature protocols, such as for standard ES algorithms.

Let's consider the possibility of finding private key d based on attack with known signed (intercepted) messages. Let intercept and sign messages [3,6].

Blind signature for EC DSA has the form:

$$s' = \frac{d \cdot r' + h'}{k} \bmod n,$$

that is, we get the following relatively d:

$$\begin{cases} d = \frac{k_1 s'_1 - h'_1}{r'_1} \bmod n \\ \dots \\ d = \frac{k_i s'_i - h'_i}{r'_i} \bmod n \end{cases}.$$

Blind signature for EC GDSA has the form:

$$s' = (kr' - h')d \bmod n,$$

that is, we get the following relatively d:

$$\begin{cases} d = \dfrac{s'_1}{k_1 r'_1 - h'_1} \bmod n \\ \dots \\ d = \dfrac{s'_i}{k_i r'_i - h'_i} \bmod n \end{cases}.$$

Blind signature for EC KCDSA has the form:

$$s' = (k - e')d \bmod n,\ e' = (r' \oplus h') \bmod n,$$

that is, we get the following relatively d:

$$\begin{cases} d = \dfrac{s'_1}{k_1 - e'_1} \bmod n \\ \dots \\ d = \dfrac{s'_i}{k_i - e'_i} \bmod n \end{cases}.$$

Blind signature for DSTU 4145-2002 has the form:

$$s' = (e + dr') \bmod n,$$

that is, we get the following relatively d:

$$\begin{cases} d = \dfrac{s'_1 - e'_1}{r'_1} \bmod n \\ \dots \\ d = \dfrac{s'_i - e'_i}{r'_i} \bmod n \end{cases}.$$

Thus, in the case of blind signature we also have a system of equations with order i equations with $i+1$ indeterminates. That has not any difference with standard algorithm [3].

Now we consider the situation with the final signature in the blind signature protocol.

The previously formed blind signature, relatively that is carried out opposite, relatively disguising, transformation is used at the final blind signature formation.

The final signature has the following form by using EC DSA:

$$s = \frac{s' \cdot (r / r')}{\alpha} \bmod n,$$

where α – random number from a specified range, $\frac{r}{r'}$ – the ratio of values of x_C and x_E coordinates [3,6].

Write the formula for s completely:

$$s = \frac{(e + dr') \cdot \dfrac{r}{r'}}{\alpha} \bmod n = \frac{e \cdot \dfrac{r}{r'} + dr}{\alpha} \bmod n$$

and obtain the following relatively d:

$$\begin{cases} d = \dfrac{s_1 \alpha - e_1 \dfrac{r_1}{r'_1}}{r_1} \bmod n \\ \dots \\ d = \dfrac{s_i \alpha - e_i \dfrac{r_i}{r'_i}}{r_i} \bmod n \end{cases}.$$

The final signature has the following form by using EC GDSA:

$$s = s' \cdot \frac{r}{r'} \cdot \alpha \bmod n .$$

Write the formula for s completely:

$$s = (kr' - h')d\frac{r}{r'}\alpha \bmod n = (kr\alpha - h'\alpha\frac{r}{r'})d \bmod n$$

and obtain the following relatively d:

$$\begin{cases} d = \dfrac{s_1}{k_1 r_1 \alpha - h'_1 \alpha \dfrac{r_1}{r'_1}} \bmod n \\ \ldots \\ d = \dfrac{s_i}{k_i r_i \alpha - h'_i \alpha \dfrac{r_i}{r'_i}} \bmod n \end{cases}.$$

The final signature has the following form by using EC KCDSA:

$$s = s' \cdot \alpha \bmod n .$$

Write the formula for s completely:

$$s = (k - e')d\alpha \bmod n = (k\alpha - e'\alpha)d \bmod n$$

and obtain relatively d the formula:

$$\begin{cases} d = \dfrac{s_1}{k_1\alpha - e'_1\alpha} \bmod n \\ \ldots \\ d = \dfrac{s_i}{k_i\alpha - e'_i\alpha} \bmod n \end{cases}.$$

The final signature has the following form by using DSTU 4145-2002:

$$s = s' \cdot \alpha \bmod n .$$

Write the formula for s completely:

$$s = (e + dr')\alpha \bmod n = (e\alpha + dr'\alpha)d \bmod n$$

and obtain relatively d the formula:

$$\begin{cases} d = \dfrac{s_1 - e_1\alpha}{r'_1\alpha} \bmod n \\ \ldots \\ d = \dfrac{s_i - e_i\alpha}{r'_i\alpha} \bmod n \end{cases}.$$

Thus, it is necessary to solve the system of i-th order with $i+1$ indeterminates for full disclosure, that is the definition of private key d by i received ES.

In case, if the message M is encrypted, hash functions values $h_1, h_2, ..., h_i$ are indeterminates. As the result, we obtain a system of equations with $2i+1$ indeterminates, so the encryption of signed messages allow to significantly increase the security [3].

9.2 Analysis of protection ES against attacks on implementation

Let the developer can lay a loophole in the software implementation of signature production. The theoretical and experimental results relatively the protection of blind signature in the blind signature protocols based on standard ES algorithms from such attacks for all mentioned above algorithms are given below [3,6].

For EC DSA the violator knows:

$$r'_1 = \pi(x_1, y_1) = x_1 \bmod n;$$
$$r'_2 = \pi(x_1, -y_1) = x_1 \bmod n.$$

Thereby:

$$r'_1 = r'_2 = x_1 \bmod n.$$

We have for s'_1 and s'_2:

$$s'_1 = \frac{dr'_1 + h'_1}{k_1} \bmod n;$$
$$s'_2 = \frac{dr'_2 + h'_2}{k_1} \bmod n.$$

Because $k_1 = k_2 = k$ and $r'_1 = r'_2 = x_1 \bmod n$, then:

$$s'_1 = \frac{dr' + h'_1}{k_1} \bmod n;$$
$$s'_2 = \frac{dr' + h'_2}{k_1} \bmod n.$$

We have the following, solving relatively d and k:

$$d = \frac{s'_1 h'_2 - s'_2 h'_2}{r'(s'_2 - s'_1)} \bmod n;$$
$$k = \frac{dr' + h'_1}{s'_1} \bmod n.$$

For EC GDSA:
The violator knows:

$$k_1 = k_2 = k \in (1, n-1);$$
$$r'_1 = r'_2 = x_1 \bmod n = r'.$$

We have for s'_1 and s'_2:

$$s'_1 = (k_1 r'_1 - h'_1) d \bmod n = (kr' - h'_1) d \bmod n; \quad (2)$$
$$s'_2 = (k_2 r'_2 - h'_2) d \bmod n = (kr' - h'_2) d \bmod n. \quad (3)$$

We have the following, solving (2) and (3) relatively (k, d):

$$k = \frac{h'_1 s'_2 - h'_2 s'_1}{r'(s'_2 - s'_1)} \bmod n;$$
$$d = \frac{s'_1}{kr' - h'_1} \bmod n.$$

For EC KCDSA:

$$k_1 = k_2 = k \in (1, n-1);$$
$$r'_1 = r'_2 = r' = H(c) = r';$$
$$w'_1 = r'_1 + h'_1 = r' + h'_1;$$
$$w'_2 = r'_2 + h'_2 = r' + h'_2.$$

We have for s'_1 and s'_2:

$$s'_1 = (k - w'_1) d \bmod n; \quad (4)$$
$$s'_2 = (k - w'_2) d \bmod n. \quad (5)$$

We have the following, solving (4) and (5) relatively (k, d):

$$k = \frac{w'_1 s'_2 - w'_2 s'_1}{s'_2 - s'_1} \bmod n;$$

$$d = \frac{s'_1}{(k - w'_1)} \bmod n .$$

We propose for DSTU 4145-2002:

$$k_1 = k_2 = k \in (1, n-1);$$
$$R_1 = R_2 = kG = (x_R, y_R) = R;$$
$$fk_1 = fk_2 = x_R = fk;$$
$$y_1 = h'_1 \, fk;$$
$$y_2 = h'_2 \, fk;$$
$$y_1 \Rightarrow r'_1; y_2 \Rightarrow r'_2 .$$

We have for s'_1 and s'_2:

$$s'_1 = (k + dr'_1) \bmod n; \quad (6)$$
$$s'_2 = (k + dr'_2) \bmod n . \quad (7)$$

We have the following, solving (6) and (7) relatively (k, d):

$$d = \frac{s'_1 - s'_2}{r'_1 - r'_2} \bmod n;$$
$$k = (s'_1 - dr'_1) \bmod n .$$

There are exist attacks on the ES program implementation for blind signature protocols based on ES algorithms EC DSA, EC GDSA, EC KCDSA, DSTU 4145-2002. If violator able to make the «production signature» program twice uses the same value k for the two messages, then he detects private long-term key d in real time and can impose the false messages and distort the true.

To protect against such attacks must use a reliable CIP means of ES type in the content of available for it conformity certificates, expert opinions and possibility of continuous monitoring of the integrity and authenticity of the production ES program. The best method to protect against such threat is a hardware implementation of ES production and verification procedures [3].

9.3 Analysis of protection ES against related keys attack

We will understand such key pair (k_1, k_2), with the knowledge of one of them with polynomial complexity uniquely or with necessary probability is determined another, as related keys.

Let's consider an attack on related keys on the above discussed ES algorithms [3,6].

At first we define the required input. We'll consider, that long-term key d is valid during some time ΔT. Make ES for messages m_1 and m_2, assuming, that the session data k_1 and k_2 are related, that is, $k_1 + k_2 = n$, where n – base point G order [3].

9.3.1 Analysis of protection algorithm EC DSA against related keys attack

Let's consider the attack with related keys on a blind signature:

$$s' = \frac{d \cdot r' + h'}{k} \bmod n .$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1	For message m_2
1) $h_1' = (\frac{r_1'}{r_1} \cdot h_1) \bmod n$	1) $h_2' = (\frac{r_2'}{r_2} \cdot h_2) \bmod n$
2) $k_1 \in [1, n-1]$	2) $k_2 = (n - k_1) \in [1, n-1]$
3) $(x_1, y_1) = k_1 \cdot G$	3) $(x_2, y_2) = k_2 \cdot G$

4) $r_1' = \pi(k_1 G) = \pi(x_1, y_1) = x_1 \bmod n$

5) $s_1' = \dfrac{d \cdot r_1' + h_1'}{k_1} \bmod n$

$r_2' = \pi(k_2 G) = \pi((n - k_1)G) \bmod n =$

4) $= \pi(nG - k_1 G) \bmod n = \pi(-k_1 G) \bmod n =$

$= \pi(x_1, -y_1) = x_1 \bmod n = r_1'$

5) $s_2' = \dfrac{d \cdot r_2' + h_2'}{k_2} \bmod n = \dfrac{d \cdot r_1' + h_2'}{k_2} \bmod n$

It is followed, that $r_2' = r_1'$ from the described above, because: $\pi(x_1, y_1) = \pi(x_1, -y_1) = x_1 \bmod n = r_1'$. Thereby, $r_2' = r_1'$ and messages m_1 and m_2 have the same first signature components r_1' and r_2'.

Next, we find the conditions, for that $s_1' = s_2'$, that is find private key d, for that the messages m_1 and m_2 ES are coincide:

$$s_1' = s_2';$$

$$\frac{d \cdot r_1' + h_1'}{k_1} \bmod n = \frac{d \cdot r_1' + h_2'}{k_2} \bmod n;$$

$$\frac{d \cdot r_1' + h_1'}{k_1} \bmod n = \frac{d \cdot r_1' + h_2'}{n - k_1} \bmod n;$$

$$(n - k_1)(dr_1' + h_1') \bmod n = k_1(dr_1' + h_2') \bmod n;$$

$$(dr_1' n - dr_1' k_1 + h_1' n - h_1' k_1) \bmod n = (dr_1' k_1 + h_2' k_1) \bmod n;$$

$$(-dr_1' k_1 - h_1' k_1) \bmod n = (dr_1' k_1 + h_2' k_1) \bmod n;$$

$$(-dr_1' k_1 - dr_1' k_1) \bmod n = (h_2' k_1 + h_1' k_1) \bmod n;$$

$$-2dr_1' k_1 \bmod n = k_1(h_1' + h_2') \bmod n;$$

$$-d = \frac{k_1(h_1' + h_2')}{2r_1' k_1} \bmod n;$$

$$d = -\frac{h_1' + h_2'}{2r_1'} \bmod n.$$

Thereby, if the user-violator generates itself long-term key by the defined rule, then the messages m_1 and m_2 will have the same blind signatures – $r_1' = r_2'$ and $s_1' = s_2'$.

Let's consider the attack with related keys on a final signature similarly:

$$s = \frac{s' \cdot (r / r')}{\alpha} \bmod n.$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1

1) $s_1 = \dfrac{s_1' \cdot (r_1 / r_1')}{\alpha} \bmod n$

For message m_2

1) $s_2 = \dfrac{s_2' \cdot (r_2 / r_2')}{\alpha} \bmod n = \dfrac{s_2' \cdot (r_1 / r_1')}{\alpha} \bmod n$

$$s_1 = s_2;$$

$$\frac{s_1' \cdot (r_1 / r_1')}{\alpha} \bmod n = \frac{s_2' \cdot (r_2 / r_2')}{\alpha} \bmod n;$$

$$\frac{(d \cdot r_1' + h_1') \dfrac{r_1}{r_1'}}{k_1 \alpha} \bmod n = \frac{(d \cdot r_1' + h_2') \dfrac{r_1}{r_1'}}{(n - k_1)\alpha} \bmod n;$$

$$(n - k_1)\alpha(dr_1' + h_1') \frac{r_1}{r_1'} \bmod n = k_1 \alpha (dr_1' + h_2') \frac{r_1}{r_1'} \bmod n;$$

$$(n\alpha dr_1' + n\alpha h_1' - k_1\alpha dr_1' - k_1\alpha h_1')\frac{r_1}{r_1'} \bmod n = (k_1\alpha dr_1' + k_1\alpha h_2')\frac{r_1}{r_1'} \bmod n;$$

$$(-k_1\alpha dr_1' - k_1\alpha h_1')\frac{r_1}{r_1'} \bmod n = (k_1\alpha dr_1' + k_1\alpha h_2')\frac{r_1}{r_1'} \bmod n;$$

$$-(k_1\alpha dr_1 + k_1\alpha \frac{r_1'}{r_1}\cdot\frac{r_1}{r_1'}h_1) \bmod n = (k_1\alpha dr_1 + k_1\alpha \frac{r_1'}{r_1}\cdot\frac{r_1}{r_1'}h_2) \bmod n;$$

$$-(k_1\alpha dr_1 + k_1\alpha h_1) \bmod n = (k_1\alpha dr_1 + k_1\alpha h_2) \bmod n;$$

$$(-k_1\alpha dr_1 - k_1\alpha dr_1) \bmod n = (k_1\alpha h_1 + k_1\alpha h_2) \bmod n;$$

$$-2k_1\alpha dr_1 \bmod n = k_1\alpha(h_1 + h_2) \bmod n;$$

$$-d = \frac{k_1\alpha(h_1 + h_2)}{2k_1\alpha r_1} \bmod n;$$

$$d = -\frac{h_1 + h_2}{2r_1} \bmod n.$$

Rules of long-term key formation for blind and final ES are coincide. Thereby, if the user-violator generates itself long-term key by the defined rule, then the messages m_1 and m_2 will have the same blind signatures too – $r_1' = r_2'$ and $s_1' = s_2'$.

It proves once again, that set of attacks on the final blind signature is the same as on the standard ES. Blind signature formation algorithm coincides with the usual ES construction algorithm, and the final signature formation in protocol uses a previously formed blind signature, relatively that is carried out opposite, relatively disguising, transformation [3,6].

9.3.2 Analysis of protection algorithm EC GDSA against related keys attack

Let's consider the attack with related keys on a blind signature:

$$s' = (kr' - h')d \bmod n.$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1	For message m_2
1) $h_1' = \frac{r_1'}{r_1}\cdot\frac{h_1}{\alpha} \bmod n$	1) $h_2' = \frac{r_2'}{r_2}\cdot\frac{h_2}{\alpha} \bmod n$
2) $k_1 \in [1, n-1]$	2) $k_2 = (n - k_1) \in [1, n-1]$
3) $(x_1, y_1) = k_1 \cdot G$	3) $(x_2, y_2) = k_2 \cdot G = (n - k_1)G = nG - k_1G$
4) $r_1' = \pi(k_1G) = \pi(x_1, y_1) = x_1 \bmod n$	$r_2' = \pi(k_2G) = \pi((n - k_1)G) \bmod n =$ 4) $= \pi(nG - k_1G) \bmod n = \pi(-k_1G) \bmod n =$ $= \pi(x_1, -y_1) = x_1 \bmod n = r_1'$
5) $s_1' = (k_1r_1' - h_1')d \bmod n$	5) $s_2' = (k_2r_2' - h_2')d \bmod n =$ $= ((n - k_1)r_2' - h_2')d \bmod n$

It is followed, that $r_2' = r_1'$ from the described above, because: $\pi(x_1, y_1) = \pi(x_1, -y_1) = x_1 \bmod n = r_1'$. Thereby, $r_2' = r_1'$ and messages m_1 and m_2 have the same first signature components r_1' and r_2'.

Next, we find the conditions for that $s_1' = s_2'$, that is find private key d, for that the messages m_1 and m_2 ES are coincide:

$$s_1' = s_2';$$

$$(k_1r_1' - h_1')d \bmod n = ((n - k_1)r_1' - h_2')d \bmod n.$$

Both parts can be reduced by d :

$$(k_1 r_1' - h_1') \bmod n = ((n-k_1) r_1' - h_2') \bmod n;$$
$$(k_1 r_1' + k_1 r_1') \bmod n = (-h_2' + h_1') \bmod n;$$
$$2k_1 r_1' \bmod n = (h_1' - h_2') \bmod n;$$
$$k_1 = \frac{h_1' - h_2'}{2r_1'} \bmod n = \frac{h_1' - h_2'}{2\pi(k_1 G)} \bmod n = \frac{h_1' - h_2'}{2x_1} \bmod n$$

or

$$(2k_1 x_1) \bmod n = (h_1' - h_2') \bmod n. \quad (8)$$

EC GDSA standard is more resistant to manipulation of ES means of creating collision and, in fact, selective forgery [3,6]. Thus, it is necessary to solve the equation (8) to determine s_1' and s_2' respectively.

Let's consider it in another representation:

$$x_1 = \frac{h_1' - h_2'}{2k_1} \bmod n$$

or

$$k_1 = \frac{h_1' - h_2'}{2x_1} \bmod n,$$

or

$$2k_1 \pi(k_1 G) = (h_1' - h_2') \bmod n. \quad (9)$$

The first method of solving this equation is the method of trials and errors [3,6]. Its essence is to form various k_1, calculation x_1 and verification condition (9).

Let's consider the attack with related keys on a final signature similarly:

$$s = s' \cdot \frac{r}{r'} \cdot \alpha \bmod n.$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1

1) $s_1 = s_1' \cdot \frac{r_1}{r_1'} \cdot \alpha \bmod n$

For message m_2

1) $s_2 = s_2' \cdot \frac{r_2}{r_2'} \cdot \alpha \bmod n = s_2' \cdot \frac{r_1}{r_1'} \cdot \alpha \bmod n$

$$s_1 = s_2;$$
$$(k_1 r_1' - h_1') d \frac{r_1}{r_1'} \alpha \bmod n = (k_2 r_2' - h_2') d \frac{r_2}{r_2'} \alpha \bmod n;$$
$$(k_1 r_1 - \frac{r_1'}{r_1} \cdot \frac{h_1}{\alpha} \cdot \frac{r_1}{r_1'}) d\alpha \bmod n = ((n-k_1) r_1 - \frac{r_1'}{r_1} \cdot \frac{h_2}{\alpha} \cdot \frac{r_1}{r_1'}) d\alpha \bmod n;$$
$$(k_1 r_1 - \frac{h_1}{\alpha}) d\alpha \bmod n = (-k_1 r_1 - \frac{h_2}{\alpha}) d\alpha \bmod n;$$
$$(k_1 r_1 d\alpha - h_1 d) \bmod n = (-k_1 r_1 d\alpha - h_2 d) \bmod n.$$

Both parts can be reduced by d :

$$(k_1 r_1 \alpha - h_1) \bmod n = (-k_1 r_1 \alpha - h_2) \bmod n;$$
$$(k_1 r_1 \alpha + k_1 r_1 \alpha) \bmod n = (h_1 - h_2) \bmod n;$$
$$2k_1 r_1 \alpha \bmod n = (h_1 - h_2) \bmod n;$$
$$k_1 \bmod n = \frac{h_1 - h_2}{2r_1 \alpha} \bmod n = \frac{h_1 - h_2}{2\alpha\pi(k_1 G)} \bmod n = \frac{h_1 - h_2}{2\alpha x_1} \bmod n$$

or

$$2k_1 \alpha x_1 \bmod n = (h_1 - h_2) \bmod n;$$

$$x_1 \bmod n = \frac{h_1 - h_2}{2\alpha k_1} \bmod n$$

or

$$k_1 \bmod n = \frac{h_1 - h_2}{2\alpha x_1} \bmod n,$$

or

$$2k_1\alpha\pi(k_1 G) \bmod n = (h_1 - h_2) \bmod n. \quad (10)$$

It is necessary to solve the equation (10) for determination s_1 and s_2 respectively. This equation for the blind and final ES is the same, only that for formation the final signature random parameter α [3] is attached.

9.3.3 Analysis of protection algorithm EC KCDSA against related keys attack

Let's consider the attack with related keys on a blind signature:

$$s' = (k - e')d \bmod n.$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1	For message m_2
1) $h_1' = \frac{r_1 \oplus h_1}{\alpha} \oplus r_1' \bmod n$	1) $h_2' = \frac{r_2 \oplus h_2}{\alpha} \oplus r_2' \bmod n$
2) $k_1 \in [1, n-1]$	2) $k_2 = (n - k_1) \in [1, n-1]$
3) $(x_1, y_1) = k_1 \cdot G$	3) $(x_2, y_2) = k_2 \cdot G = (n - k_1)G = (nG - k_1 G) \bmod n = = (O_E - k_1 G) \bmod n = (x_1, -y_1)$
4) $x_1 \to c_1$	4) $x_2 = x_1 \Rightarrow c_2 = c_1$
5) $r_1' = H(c_1)$	5) $r_2' = r_1' = H(c_2) = H(c_1)$
6) $e_1' = r_1' \oplus h_1'$	6) $e_2' = r_2' \oplus h_2' = r_1' \oplus h_2'$
7) $s_1' = (k_1 - e_1')d \bmod n$	7) $s_2' = (k_2 - e_2')d \bmod n$

Thereby, $r_2' = r_1'$ and messages m_1 and m_2 have the same first signature components r_1' and r_2'.

Next, we find the conditions for that $s_1' = s_2'$, that is find private key d, for that the messages m_1 and m_2 ES are coincide: $s_1' = s_2'$; $(k_1 - e_1')d \bmod n = (k_2 - e_2')d \bmod n$.

Both parts can be reduced by d:

$$(k_1 - e_1') \bmod n = (n - k_1 - e_2') \bmod n;$$
$$(k_1 + k_1) \bmod n = (n + e_1' - e_2') \bmod n;$$
$$2k_1 \bmod n = (e_1' - e_2') \bmod n;$$
$$k_1 = \frac{e_1' - e_2'}{2} \bmod n;$$
$$k_1 = \frac{(r_1' \oplus h_1') - (r_1' \oplus h_2')}{2} \bmod n = \frac{h_1' - h_2'}{2} \bmod n.$$

Let's consider the attack with related keys on a final signature similarly:

$$s = s' \cdot \alpha \bmod n.$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1	For message m_2
1) $s_1 = s_1' \cdot \alpha \bmod n$	1) $s_2 = s_2' \cdot \alpha \bmod n$

$$s_1 = s_2;$$

$$\alpha(k_1 - e_1')d \bmod n = \alpha(k_2 - e_2')d \bmod n;$$
$$\alpha d(k_1 - e_1') \bmod n = \alpha d(n - k_1 - e_2') \bmod n.$$

Both parts can be reduced by d and α:

$$(k_1 - e_1') \bmod n = (n - k_1 - e_2') \bmod n;$$
$$(k_1 + k_1) \bmod n = (e_1' - e_2') \bmod n;$$
$$2k_1 \bmod n = ((r_1' \oplus h_1') - (r_1' \oplus h_2')) \bmod n;$$
$$2k_1 \bmod n = (h_1' - h_2') \bmod n;$$
$$2k_1 \bmod n = ((\frac{r_1 + h_1}{\alpha} \oplus r_1') - (\frac{r_2 + h_2}{\alpha} \oplus r_2')) \bmod n;$$
$$2k_1 \bmod n = (\frac{r_1 + h_1}{\alpha} - \frac{r_1 + h_2}{\alpha}) \bmod n;$$
$$2k_1 \bmod n = \frac{h_1 - h_2}{\alpha} \bmod n;$$
$$k_1 = \frac{h_1 - h_2}{2\alpha} \bmod n.$$

So, ES algorithm EC DSA is vulnerable to attacks on related keys, and ES algorithms EC GDSA and EC KCDSA – protected, from the three algorithms of standard DSTU ISO/IEC 14888-3:2006 [3].

9.3.4 Analysis of algorithm DSTU 4145-2002 protection against related keys attack

Let's consider the attack with related keys on a blind signature:

$$s' = (k + dr') \bmod n.$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1	For message m_2
1) $k_1 \in [1, n-1]$	1) $k_2 = (n - k_1) \in [1, n-1]$
2) $f_{k_1} = \pi(k_1 G) = \pi(x_{E_1}, y_{E_1}) = x_{R_1}$	2) $f_{k_2} = \pi((n-k_1)G) = \pi(nG - k_1 G) = \pi(x_{E_1}, -y_{E_1}) = x_{R_1}$
3) $(k_1, f_{k_1}) = (k_1, x_{E_1})$	3) $(k_2, f_{k_2}) = (k_2, x_{E_1})$
4) $h_1' = \frac{x_{C_1} \cdot h_1}{x_{E_1} \cdot \alpha} \bmod n$	4) $h_2' = \frac{x_{C_1} \cdot h_2}{x_{E_1} \cdot \alpha} \bmod n$
5) $y_1 = h_1' x_{E_1} = r_1'$	5) $y_2 = h_2' x_{E_1} = r_2'$
7) $s_1' = (k_1 + dr_1') \bmod n$	6) $s_2' = (k_2 + dr_2') \bmod n$

Let's carry out an analysis of results, that are obtained in line 5. In this case $r_1' \neq r_2'$, but r_1' and h_1' are known, so:

$$x_{E_1} = \frac{y_1}{h_1'};$$
$$y_2 = r_2' = h_2' \frac{y_1}{h_1'} = y_1 \frac{h_2'}{h_1'} = r_1' \frac{h_2'}{h_1'}.$$

This means, that if we know r_1' and h_1', we can find x_{E_1}.

So, components r_1', r_2' are interconnected and computationally easy to find at known m_1 and m_2, although $r_1' \neq r_2'$.

Next, let's consider the conditions, for that $s_1' = s_2'$:

$$s_1' = s_2';$$
$$(k_1 + dr_1') \bmod n = (k_2 + dr_2') \bmod n;$$
$$(k_1 + dr_1') \bmod n = (n - k_1 + dr_1' \frac{h_2'}{h_1'}) \bmod n;$$
$$(dr_1' - dr_1' \frac{h_2'}{h_1'}) \bmod n = (n - k_1 - k_1) \bmod n;$$
$$d(r_1' - r_1' \frac{h_2'}{h_1'}) \bmod n = (-2k_1) \bmod n;$$
$$d = -\frac{2k_1}{(r_1' - r_1' \frac{h_2'}{h_1'})} \bmod n = -\frac{2k_1 h_1'}{r_1'(h_1' - h_2')} \bmod n.$$

Let's carry out an analysis of protection level to the case, when values y_1 and y_2 are calculated as sums:

$$y_1 = (h_1' + x_{E_1}); \qquad y_2 = (h_2' + x_{E_2});$$
$$r_1' = y_1 = (h_1' + x_{E_1}); \qquad r_2' = y_2 = (h_2' + x_{E_2});$$
$$r_2' = (h_2' - h_1' + h_1' + x_{E_1}) = (h_2' + x_{E_1}),$$

that is r_2' related with r_1' on x_{E_1}.

We have for the basic field in the case of product:

$$r_2' = h_2' x_{E_1} = h_2' \frac{y_1}{h_1'} = r_1' \frac{h_2'}{h_1'}, \quad \text{and} \quad r_1' = h_1' x_{E_1}.$$

Thus, we have in the case of calculation r_1' and r_2' due the sum h_1' and x_{E_1}, and h_2' and x_{E_1} the following:

$$r_1' = (h_1' + x_{E_1}(k_1)),$$

and

$$r_2' = (h_2' + x_{E_1}(k_1)) = ((h_2' - h_1') + r_1').$$

We have, in the case of calculation r_1' and r_2', due the multiplication the following:

$$r_1' = h_1' x_{E_1}(k_1);$$
$$r_2' = r_1' \frac{h_2'}{h_1'}.$$

Let's consider the attack with related keys on a final signature similarly: $s = s' \cdot \alpha \bmod n$.

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1

1) $s_1 = s_1' \cdot \alpha \bmod n$

For message m_2

1) $s_2 = s_2' \cdot \alpha \bmod n$

$$s_1 = s_2;$$
$$\alpha(k_1 + dr_1') \bmod n = \alpha(k_2 + dr_2') \bmod n;$$
$$\alpha(k_1 + dr_1') \bmod n = \alpha((n - k_1) + dr_1' \cdot \frac{h_2'}{h_1'}) \bmod n;$$
$$\alpha(k_1 + dr_1') \bmod n = \alpha(-k_1 + dr_1' (\frac{x_{C_1} h_2}{x_{E_1} \alpha} \Big/ \frac{x_{C_1} h_1}{x_{E_1} \alpha})) \bmod n;$$
$$\alpha(k_1 + dr_1') \bmod n = \alpha(-k_1 + dr_1' \cdot \frac{h_2}{h_1}) \bmod n;$$

$$(\alpha k_1 + \alpha d r_1') \bmod n = (-\alpha k_1 + \alpha d r_1' \cdot \frac{h_2}{h_1}) \bmod n;$$

$$(\alpha d r_1' - \alpha d r_1' \cdot \frac{h_2}{h_1}) \bmod n = (-\alpha k_1 - \alpha k_1) \bmod n;$$

$$d(\alpha r_1' - \alpha r_1' \cdot \frac{h_2}{h_1}) \bmod n = (-2\alpha k_1) \bmod n;$$

$$d = -\frac{2\alpha k_1}{\alpha r_1' - \alpha r_1' \cdot \frac{h_2}{h_1}} \bmod n;$$

$$d = -\frac{2\alpha k_1}{\alpha(r_1' - r_1' \cdot \frac{h_2}{h_1})} \bmod n = -\frac{2k_1}{r_1' - r_1' \cdot \frac{h_2}{h_1}} \bmod n = -\frac{2k_1 h_1}{r_1'(h_1 - h_2)} \bmod n.$$

It can make the conclusion that, as in the case of the multiplication r_1' depends on h_1' and $x_{E_1}(k_1)$, and r_2' depends on r_1', h_1' and h_2', that is depends are identical in its nature.

The above results of researches allow to make the conclusion that, the ES algorithm DSTU 4145-2002 has weak protection against attacks on related keys [3,6].

10 Conclusions

1. Improved blind ES mechanism provides documents authenticity confirmation without revealing their authorship and can be implemented using standard ES EC DSA, EC KCDSA, EC GDSA, and DSTU 4145-2002.
2. In case of given blind ES to the checking protection ES mechanism criteria the anonymity criterion adds. The inability to identify the document author by the signer is proved in its application, if he uses all known parameters, that were used at signature statement.
3. Should find out, can signer calculates the signature in not disguised form, using DB intermediate values, which he creates at signature statement on examination blind ES mechanism for the anonymity criterion.
4. It is shown that blind signature mechanisms, based on standards DSTU ISO/IEC 14888-3: 2006 (EC DSA, EC GDSA and EC KCDSA) and DSTU 4145-2002, ensure their security, that is they are stable for the anonymity criterion. Researches, also, have shown, that the ratios between the disguising parameters to be chosen so, that the signer could not identify the document author with their use.
5. The main advantage of the proposed blind signature mechanism, comparatively existing, is that the signer and validator actions are the same, as described in the relevant standards for ordinary signature and verification in the group of points of elliptic curves. The only difference is that the signer receives a hash-value instead of calculates its by himself. Steps, that distinguish blind signature from ordinary, are performed by the issuer. This technique makes blind signature functionality implementation into existing information and telecommunication systems so, that almost not to require additional efforts. It is only necessary to implement the protocol for the issuer, and signer and validator can use existing tools to develop and verify ES.
6. We can directly refer to existing standards and not to enter into conflict with them (signature verification by one standard, both for the ES and for the blind signature) on the considered approach.
7. The blind signature algorithms are vulnerable to the same attacks, as the standard ES algorithms, because the blind signature algorithms in blind signature mechanism coincide with the ES algorithms of relevant standards.
8. The final signature is formed from the blind, for that is carried out multiplication and division by a random number, which does not affect to the resistance to attacks, so in forming the final signature also using the same standard EP algorithm.

9. It is also found, that all reviewed algorithms provide only tracked anonymity. The CIP modules, that proposed in the section 4 of this article, must be used to ensure complete anonymity. The mechanism alteration can be able an alternative, but it will result in the loss of all its advantages.

References

[1] Information technology – Security techniques – Digital signatures with appendix. Part 3. Discrete logarithm based mechanisms: ISO/IEC 14888-3. - (Edition 2 (2006-11-15)): 2006. – 68 p.
[2] Information technology – Security techniques – Blind digital signatures. Part 2. Discrete logarithm based mechanisms: ISO/IEC DIS 18370-2:2014(E):2015. – 70 p.
[3] Gorbenko I.D. Applied cryptology. Theory. Practice. Application: monograph. / I.D. Gorbenko, U.I. Gorbenko. - Kh.: Fort, 2012. - 870 p.
[4] Information technology – Security techniques – Digital signature based on elliptic curves – Generation and verification: DSTU 4145-2002. – K.: State Standard of Ukraine, 2003. – 35 p. – (National standards of Ukraine).
[5] Yesina M.V. Blind digital signature protocol on elliptic curves based on international standard ISO/IEC 14888-3:2006 (EC DSA) and national standard DSTU 4145-2002 / M. V. Yesina // Theoretical and applied aspect of program systems development (TAAPSD'15): 12th International Conference Proceeding, 23-26 November 2015 – K.: National University of «Kyiv-Mohyla Academy», 2015. – P.65–69.
[6] Yesina M.V. Mathematical model of a protocol of electronic signature based on elliptic curves / M.V. Yesina // Applied Radioelectronics. – Kh.: Kharkiv National University of Radio Electronics, 2015. – Vol. 14. - № 4. – P.300–305.
[7] Nikulishchev H.I. Blind digital signature protocol on elliptic curves over vector finite field / H.I. Nikulishchev // Radioelectronics, informatics, management. – 2013. – № 2. – P.71–76.
[8] Nikulishchev H.I. Anonymity as a criterion of evaluation blind digital signature protocols security / H.I. Nikulishchev, G.L. Kozina // The legal, regulatory and metrological support of information security in Ukraine. – 2012. – № 2. – P.59–65.

Рецензент: Олександр Потій, доктор техн. наук, проф., Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна. E-mail: potav@ua.fm

Надійшло: лютий 2016.

Автори:
Іван Горбенко, д.т.н., проф., лауреат Державної премії України, Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна. Email: gorbenkoi@iit.kharkov.ua
Марина Єсіна, аспірантка, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
Email: rinayes20@gmail.com
Володимир Пономар, аспірант, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
Email: Laedaa@gmail.com

Удосконалення механізмів сліпої електронної підписи на еліптичних кривих

Анотація. Робота присвячена розгляду механізмів сліпого електронного підпису на основі алгоритмів, що описані у ISO/IEC 14888-3:2006 та національному стандарті ДСТУ 4145-2002. Проводиться перевірка захищеності протоколу на основі цих алгоритмів за критерієм анонімності. Доводиться, що розглянутий протокол є захищеним за критерієм анонімності, тобто неможливо визначити автора підписаного документу.

Ключові слова: анонімність, електронний підпис, сліпий підпис.

Рецензент: Александр Потий, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, г. Харьков, Украина. E-mail: potav@ua.fm

Поступила: февраль 2016.

Авторы:
Иван Горбенко, д.т.н., проф., лауреат Государственной премии Украины, Харьковский национальный университет имени В. Н. Каразина, г. Харьков, Украина. Email: gorbenkoi@iit.kharkov.ua
Марина Есина, аспирантка, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
Email: rinayes20@gmail.com
Владимир Пономарь, аспирант, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
Email: Laedaa@gmail.com

Усовершенствование механизмов слепой электронной подписи на эллиптических кривых

Аннотация. Работа посвящена рассмотрению механизмов слепой электронной подписи на основе алгоритмов, которые описаны в ISO/IEC 14888-3:2006 и национальном стандарте ДСТУ 4145-2002. Проводится проверка защищенности протокола на основе этих алгоритмов по критерию анонимности. Доказывается, что рассмотреный протокол является защищенным по критерию анонимности, то есть невозможно определить автора подписанного документа.

Ключевые слова: анонимность, электронная подпись, слепая подпись.