Convertible Authenticated Encryption Scheme Without Using Conventional One-Way Function

Hung-Yu CHIEN
Department of Information Management, Chaoyang University of Technology
Taichung, Taiwan, ROC
e-mail: redfish6@ms45.hinet.net

Received: January 2003

Abstract. An authenticated encryption allows the designated recipient to verify the authenticity while recovering the message. To protect the recipient's benefit in case of a later dispute, a convertible authenticated encryption scheme allows the recipient to convert the authenticated encryption into an ordinary signature so that it becomes a publicly verifiable. This paper shows a universal forgery attack on Araki *et al.*'s convertible authenticated encryption scheme, and proposes a new convertible authenticated encryption scheme. Without using any conventional one-way function, the proposed scheme simplifies its security assumption on only a public hard problem – the discrete logarithm problem.

Key words: authenticated encryption, discrete logarithm, one-way function.

1. Introduction

A digital signature scheme (Rivest *et al.*, 1978; Elgamal, 1985; Shamir, 1984; NIST, 1992) enables a signer to sign messages electronically such that any verifier can electronically verify the validity of the signature. In contrast, in authenticated encryption schemes (Araki *et al.*, 1999; Wu and Hsu, 2002; Horster *et al.*, 1994), only the designated recipient can recover the message and verify its authenticity. This property is desirable in the applications where a signer wants to keep the message secret from the public and only the designated recipient can recover the message and verify it. For example, we want to ensure to the bank our payments while keeping them secret from others.

However, in case of a later dispute, we would like to have some mechanism that makes an authenticated encryption become verifiable by everyone and the signer cannot repudiate his signature. The signcryption schemes (Zheng, 1997; Petersen and Michel, 1998; He and Wu, 1999) utilize an interactive repudiation settlement procedure between the recipient and the third party to settle such a dispute. This approach is costly due to its interactive communications, and it only convinces the third party, instead of any verifier, of the signer's dishonesty. Araki *et al.* (1999) proposed the *convertible authenticated encryption scheme* that allows the recipient to convert the authenticated encryption into an ordinary signature so that everyone can verify the signature. However, the conversion requires the co-operation of the signer, which is not practical sometimes. Recently, Wu and Hsu (2002) proposed their convertible encryption scheme in which the recipient can convert the encryption into an ordinary one without the co-operation of the signer. Both the security of Araki *et al.*'s scheme and Wu-Hsu's scheme are based on the discrete logarithm problem (DLP) (Elgamal, 1985; Horster *et al.*, 1994) and the conventional one-way function (Rivest, 1993; NIST, 1993).

The conventional one-way functions are widely employed in many digital signature schemes. In these schemes, the system will become insecure because of the forgery attacks if the conventional one-way function is not used or not secure (Harn and Lin, 1998; Dobbertin, 1996; Menezes *et al.*, 1997; Chien *et al.*, 2002). Furthermore, the security of these conventional one-way hash functions, like MD5 (Rivest, 1993), is based on the complexity of analysis of iterated functions but is not a public hard problem (the discrete logarithm problem is a public hard problem, and can be seen as a one-way function.) So, it may seem very difficult to break the security of these conventional one-way functions at the beginning, but it may become insecure to some special attacks later (Dobbertin, 1996). Therefore, some works have been devoted to propose secure cryptosystems without using conventional one-way function (Harn and Lin, 1998; Chien and Jan, 2003; Lee and Chang, 1995). In this article, we would like to propose a new convertible authenticated encryption scheme that is based on a simpler security assumption – the discrete logarithm problem only. We also show a universal forgery attack on Araki *et al.*'s scheme.

The rest of this paper is organized as follows. Section 2 reviews Araki *et al.*'s scheme, and shows a universal forgery attack (Chien *et al.*, 2002). Our new scheme is then presented in Section 3, which is followed by the security analysis and performance evaluation in Section 4. Finally, Section 5 states our conclusions.

2. The Security Weakness of Araki *et al.*'s Scheme

Araki et al., based on the conventional one-way function and the DLP, proposed a convertible authenticated encryption scheme. However, the scheme is vulnerable to the universal forgery attack. Araki et al.'s scheme is reviewed in Section 2.1, *and a universal forgery attack is shown in Section* 2.2.

2.1. *Review of Araki et al.'s Scheme*

Araki *et al.*'s scheme consists of two phases – the signing and verification phase, and the conversion phase. In the signing and verification phase, the signer prepares an authenticated encryption for a message m. The message m should contain the pre-defined redundancy for preventing the existential forgery attack. In the conversion phase, the signer is requested to submit some parameters for converting the encryption into an ordinary signature.

The following introduces the notations and the parameters.

$U_a/U_b:$ U_a denotes the signer and U_b denotes the designated receiver.

$p, q, g:$ p is a large prime, q a large prime factor of p, and g is a generator of order q over $GF(p)$.

$x_a/x_b:$ U_a/U_b's secret keys respectively.

$Y_a/Y_b:$ U_a's/U_b's public keys, where $Y_a \equiv_p g^{x_a}$, $Y_b \equiv_p g^{x_b}$ and $\equiv_p$ denotes the operation of $\mathrm{mod}\, p$.

$h(\,):$ a conventional one-way function.

The signing and verification phase

To sign a message m, the signer U_a performs the following steps.

Step 1. Chooses a random integer $k \in Z_q^*$.

Step 2. Computes $j = h(k)$, $r_1 \equiv_p Y_b^{k+j}$ and $r_2 \equiv_p m \cdot (r_1 + g)^{-1}$. He then verifies whether $r_1 + g \neq 0(\mathrm{mod} p)$ and $r_2 < q$.

Step 3. If the verification in *Step* 2 succeeds, he calculates $J \equiv_p g^j$ and $s \equiv_q (r_2 \cdot k - 1 - r_2) \cdot (1 + x_a)^{-1}$. Otherwise, he chooses another k and tries again. U_a then sends (r_2, s, J) as the encryption for message m to the recipient U_b.

Upon receiving the encryption, U_b performs the following steps to recover and verify the message.

Step 1. Computes $m' \equiv_p (Y_b^{(1+r_2+s)\cdot r_2^{-1}} \cdot (Y_a^{s \cdot r_2^{-1}} \cdot J)^{x_b} + g) \cdot r_2$.

Step 2. Checks whether the recovered message m' contains the pre-defined redundancy. If so, he accepts the message. Please notice that the recipient U_b should use his secret key x_b to recover the message.

The conversion phase

To convert the encryption into an ordinary signature, the signer U_a is requested to release a further parameter $u \equiv_q (s \cdot x_a \cdot r_2^{-1} + j)$. The recipient U_b then verifies the validity of u by checking whether $g^u \equiv_p Y_a^{s \cdot r_2^{-1}} \cdot J$. If it holds, U_b can reveal the converted signature for m as (r_2, s, J, u), in case of a dispute. Now any one can verify the signature by checking whether g^u equals $Y_a^{s \cdot r_2^{-1}} \cdot J(\mathrm{mod}\, p)$, computes $m \equiv_p (Y_b^{(1+r_2+s)\cdot r_2^{-1}+u} + g) \cdot r_2$, and checks whether the recovered m contains the pre-defined redundancy. If the verifications succeed, then the verifier accepts the signature; otherwise, the signature is invalid.

2.2. *Universal Forgery Attack on Araki et al.'s Scheme*

Here, we shows that Araki *et al.*'s scheme is vulnerable to the universal forgery attack. We demonstrate this by showing that an adversary can easily forge valid signatures for any messages on behalf of the signer U_a. Assume the attacker wants to forge, on behalf of U_a, a signature on a redundancy-contained message m for the recipient U_b. He performs the following steps.

Step 1. Randomly chooses $u, k \in Z_q^*$.

Step 2. Computes $r_2 \equiv_p m \cdot [Y_b^{1+k+u} + g]^{-1}$, $s \equiv_q k \cdot r_2 - 1$ and $J \equiv_p Y_a^{-s \cdot r_2^{-1}} \cdot g^u$. Checks whether $r_2 < q$. If not, he chooses another u, k and tries again. Finally, the (r_2, s, J, u) is the signature for message m.

Any verifier will accept this signature after performing the verification operations. This can be shown as follows.

$$
\begin{aligned}
&Y_a^{s\cdot r_2^{-1}} \cdot J\\
&\quad\equiv_p Y_a^{s\cdot r_2^{-1}} \cdot Y_a^{-s\cdot r_2^{-1}} \cdot g^u\\
&\quad\equiv_p g^u
\end{aligned}
$$

(The verifier will check this verification equation)

$$
\begin{aligned}
&(Y_b^{(1+r_2+s)\cdot r_2^{-1}+u} + g) \cdot r_2\\
&\quad\equiv_p (Y_b^{(r_2+k\cdot r_2)\cdot r_2^{-1}+u} + g) \cdot r_2\\
&\quad\equiv_p (Y_b^{1+k+u} + g) \cdot m \cdot (Y_b^{1+k+u} + g)^{-1}\\
&\quad\equiv_p m
\end{aligned}
$$

(The verifier will perform this calculation to recover the message)

Since the forged signature satisfies the verification equations above and the recovered message m contains the pre-defined redundancy, the verifier will accept this signature. Araki *et al.*'s scheme is vulnerable to the universal forgery attack.

3. New Convertible Authenticated Encryption Based on the DLP

Araki *et al.*'s convertible encryption scheme requires the co-operation of the signer and the designated recipient to convert the encryption into an ordinary signature. This requirement is not practical, since the signer may refuse to co-operate. Both of Araki *et al.*'s scheme and Wu-Hsu's scheme are based on the discrete logarithm problem (DLP) and the conventional one-way function, where the DLP is a public hard problem but the security of the conventional one-way function is not (Rivest, 1993; NIST, 1993). Therefore, we would propose a new convertible authenticated encryption scheme that does not require the signer's co-operation to convert the encryption and has a simpler security assumption – the DLP only.

The proposed scheme assumes the same system parameters as in Section 2. The scheme also consists of two phases – the signing and verification phase and the conversion phase.

The signing and verification phase

Assume U_a wants to prepare an authenticated encryption for message m, which contains the pre-defined redundancy and belongs to Z_p^*, for the recipient U_b. U_a performs the following steps.

Step 1. Chooses a random integer $k \in Z_q^*$.

Step 2. Computes $\overline{r}_1 \equiv_p g^k, r_1 \equiv_p m^{-1} \cdot g^k$, and $r_2 \equiv_p m \cdot g^{k\cdot K_{ab}}$, where $K_{ab} \equiv_p Y_b^{x_a} \equiv_p Y_a^{x_b} \equiv_p g^{x_a \cdot x_b}$ is the long-term secret key between U_a and U_b. The key K_{ab} can be pre-computed.

Step 3. Computes $s \equiv_q x_a - (k + k \cdot K_{ab}) \cdot (r_1 \oplus r_2)$, where $\oplus$ denotes the bitwise exclusive OR operation. The authenticated encryption for message m is $(\,\overline{r}_1, r_2, s)$.

Upon receiving the encryption, the recipient U_b performs the following steps to recover and verify the message.

Step 1. Computes $m \equiv_p r_2 \cdot (\overline{r}_1)^{-K_{ab}}$ and $r_1 \equiv_p m^{-1} \cdot \overline{r}_1$.

Step 2. The verifier checks whether the recovered message m in *Step* 1 contains the pre-defined redundancy, and verifies whether the following equation holds. If so, he accepts the message and the signature.

$$Y_a \equiv_p g^s \cdot (r_1 \cdot r_2)^{r_1 \oplus r_2}. \tag{1}$$

The conversion phase

In case of a later dispute, the recipient U_b can convert the encryption into an ordinary signature without the co-operation of U_a. U_b just releases $(m, \overline{r}_1, r_2, s)$ as U_a's ordinary signature.

Any verifier can validate the signature by computing $r_1 \equiv_p m^{-1} \cdot \overline{r}_1 \equiv_p m^{-1} \cdot g^k$ and verifying the Eq. 1. If the equation holds and the message contains the pre-defined redundancy, he accepts the signature.

The correctness of the proposed scheme can be confirmed through the following results.

Theorem 1. *If U_a follows the above procedure to generate the encryption $(\overline{r}_1, r_2, s)$, then the Eq.* 1 *should hold.*

Proof. From Eq. 1, we have

$$\begin{aligned} g^s \cdot (r_1 \cdot r_2)^{r_1 \oplus r_2} &\equiv_p g^s \cdot (m^{-1} \cdot g^k \cdot m \cdot g^{k \cdot K_{ab}})^{r_1 \oplus r_2} \\ &\equiv_p g^s \cdot g^{(k + k \cdot K_{ab}) \cdot (r_1 \oplus r_2)} \\ &\equiv_p g^{x_a - (k + k \cdot K_{ab}) \cdot (r_1 \oplus r_2)} \cdot g^{(k + k \cdot K_{ab}) \cdot (r_1 \oplus r_2)} \\ &\equiv_p Y_a. \end{aligned}$$

Application examples

Here, we show applications of the proposed scheme. A president of a company may assign a mission to one of his/her employees and only the designated recipient can receive the message and verify it. However, in case of a later dispute, the designated recipient may convert the encryption into an ordinary signature so that anyone can verify the signature. Another application is in the military. A supervisor secretly sends a message to his/her subordinate who can recover the message and verify it. However, he/she can prove it, in case of a dispute later.

A numerical example

Here, we show a numerical example to demonstrate how the scheme works. Let $p = 11$, $q = 5$, $g = 4$. Then g is a generator of order 5 in $GF(11)$. Assume $x_a = 3$ and $x_b = 4$. Then, we have $Y_a \equiv_{11} 4^3 \equiv_{11} 9$, $Y_b \equiv_{11} 4^4 \equiv_{11} 3$ $(4^4 \bmod 11 = 3 \bmod 11)$, and $K_{ab} \equiv_{11} 4^{3\cdot 4} \equiv_{11} 5$.

Assume U_a wants to prepares an authenticated encryption for message $m = 2$ (here, we may take the most significant bit $= 0$ as the redundancy. For a modulus of large prime, we can have many redundancy bits and strong security). He performs the following steps.

Step 1. Chooses a random number $k = 3$.

Step 2. Computes $\overline{r}_1 \equiv_{11} 4^3 \equiv_{11} 9$, $r_1 \equiv_{11} 2^{-1} \cdot 4^3 \equiv_{11} 6 \cdot 9 \equiv_{11} 10$, and $r_2 \equiv_{11} 2 \cdot 4^{3\cdot 5} \equiv_{11} 2$.

Step 3. Computes $s \equiv_5 3 - (3 + 3 \cdot 5) \cdot (10 \oplus 2) \equiv_5 3 - 18 \cdot 8 \equiv_5 4$. The authenticated encryption is (9, 2, 4).

Upon receiving the encryption, U_b performs the following steps to recover and verify the message.

Step 1. Computes $m \equiv_{11} 2 \cdot (9)^{-5} \equiv_{11} 2 \cdot (4^{15})^{-1} \equiv_{11} 2$ and $r_1 \equiv_{11} 2^{-1} \cdot 9 \equiv_{11} 10$.

Step 2. Checks whether the most significant bit of m equals 0. If so, performs the following verification equation.

$$g^s \cdot (r_1 \cdot r_2)^{r_1 \oplus r_2} \equiv_{11} 4^4 \cdot (10 \cdot 2)^{10 \oplus 2} \equiv_{11} 3 \cdot (20)^8 \equiv_{11} 9 \equiv_{11} Y_a.$$

So, U_b accepts the message. He can convert the encryption into an ordinary signature by releasing (2, 9, 2, 4).

4. Security Analysis and Performance Evaluation

The security of the proposed scheme is based on the well-known hard problem – the discrete logarithm problem (DLP). The security of the long-term secret key K_{ab} is based the well-known Diffie-Hellman assumption (Diffie and Hellman, 1976). We now examine its security by discussing some possible attacks.

(1) An outsider tries to derive either of the secret keys (x_a, x_b and K_{ab}) from the converted signature (m, $\overline{r}_1$, r_2, s).

From the public data $m, \overline{r}_1, r_2, s$ and Eq. 1, the secret parameters k and K_{ab} are well protected due to the DLP. From the data s, an outsider cannot derive the secret parameters k, K_{ab} and x_a, because there are three unknown variables in one equation.

(2) The recipient U_b tries to derive U_a's secret key from the encryption.

From U_a's encryption ($\overline{r}_1$, r_2, s), U_b cannot derive the secret parameters k and x_a for the same reasons in (1).

(3) The recipient or an outsider tries to forge U_a's signature.
If the recipient would like to forge U_a's signature satisfying Eq. 1, he may randomly selects some parameters and try to solve the rest parameters from Eq. 1. This approach is infeasible due to the DLP. The same result applies for an outsider, since he is not more powerful than the recipient.

(4) An outsider tries to derive the message from U_a's encryption.
This is infeasible since he cannot acquire the secret key K_{ab}.

We now evaluate the performance of our scheme. For a comparison, we adopt the same assumptions as (Dimitrov and Cooklev, 1995). With a modulus n, the computation for a modular exponentiation operation is taken as $0.3246\,|n|$ modular multiplications, where $|n|$ denotes the bit length of n. An inverse computation in Z_n^* demands the same amount of computation time as a modular exponentiation operation. A hashing computation requires no longer time than a modular multiplication computation. Since the computational cost of bit-wise XOR operation is negligible, we do not count them in the evaluation. The notation for different computational costs is introduced as follows, and the evaluation is listed in Table 1.

T_E: the computational time for performing a modular exponentiation.

T_I: the computational time for performing a modular inverse operation.

T_M: the computational time for performing a modular multiplication.

T_h: the computational time for performing a conventional one-way hashing operation.

Please notice that the long-term secret key K_{ab} can be pre-computed, and the message m has been computed when U_b performs the message recovery in Eq. 1 so that U_b does not need to compute it again for converting the encryption. According to Table 1, our scheme outperforms Araki *et al.*'s scheme in terms of computational cost. Araki *et al.*'s scheme is vulnerable to the universal forgery attack, and both of Araki *et al.*'s scheme and Wu-Hsu's scheme are based on the discrete logarithm problem and the conventional one-way functions. *The conventional one-way functions are not public hard problems and seem difficult to break at beginning but may be insecure to some special attacks later. Therefore, it would be better if we could build crypto-schemes, based on only public hard problems. The proposed scheme is based on only public hard problem. Its security assumption is simple and easier to prove the security.*

5. Conclusions

The security of existing convertible authenticated encryption schemes is widely dependent on the conventional one-way functions whose security is based on the complexity of analysis of iterated functions and may become insecure to some special attack later. The security weakness of Araki *et al.*'s scheme has been shown in this paper. To raise the security level, we have proposed a new convertible authenticated encryption scheme. Without using any conventional one-way function, the security of the proposed scheme is based on only the public hard problem and its performance is comparable to other existing schemes.

Table 1

Evaluation of convertible authenticated encryption

	Araki *et al.*	Wu-Hsu	The proposed scheme
Security assumptions	DLP + OWHF	DLP + OWHF	DLP
Vulnerability to universal forgery attack	Yes	No	No
The co-operation of signer when performing signature conversion	Yes	No	No
Length of original encryption	$2\,\lvert p\rvert + \lvert q\rvert$	$\lvert p\rvert + 2\lvert q\rvert$	$2\,\lvert p\rvert + \lvert q\rvert$
Length of converted signature	$2\,\lvert p\rvert + 2\lvert q\rvert$	$\lvert p\rvert + 2\lvert q\rvert$	$3\,\lvert p\rvert + \lvert q\rvert$
Computational cost for encryption generation	$2\,T_E + 2T_I + 3T_M + T_h$	$2\,T_E + T_I + 2T_M + 3T_h$	$3\,T_E + 4T_M$
Computational cost for message recovery and verification	$3\,T_E + T_I + 5T_M$	$3\,T_E + 2T_M + 3T_h$	$4\,T_E + 4T_M$
Additional computational cost for signature conversion	$2\,T_E + 2T_I + 4T_M$	0	0
Computational cost for verifying converted signature	$3\,T_E + T_I + 4T_M$	$2\,T_E + T_M + 2T_h$	$3\,T_E + 3T_M$

$*$ OWHF: conventional one-way hash function

Acknowledgements

We would like to thank the anonymous reviewers for their helpful comments. This research is partially supported by National Science Council with project number NSC91-2626-E-252-002.

References

Araki, S., S. Uehara and K. Imamura (1999). The limited verifier signature and its application. *IEICE Trans. On Fundamentals*, **E82A**(1), 63–68.

Chien, H.Y., and J.K. Jan (2003). Improved authenticated multiple-key agreement protocol without using conventional one-way function. *Accepted in Applied Mathematics and Computation.*

Chien, H.Y., J.K. Jan and Y.M. Tseng (2002). Forgery attacks on multi-signature schemes for authenticating mobile code delegates. *IEEE Transactions on Vehicular Technology*, **51**(6), 1669–1671.

Diffie, W., and M.E. Hellman (1976). New direction in cryptography. *IEEE Trans. On Information Theory*, **IT-22**(6), 644–654.

Dimitrov, V., and T. Cooklev (1995). Two algorithms for modular exponentiation using nonstandard arithmetic. *IEICE Trans. Fundamentals*, **E78-A**(1), 82–87.

Dobbertin, H. (1996). The status of MD5 after a recent attack. *CryptoBytes*, **2**(2), 1–6.

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. On Information Theory*, **IT-31**(4), 469–472.

Harn, L., and H.Y. Lin (1998). An authenticated key agreement protocol without using one-way function. In *Proc. 8th National Conf. Information Security*, Kaohsiung, Taiwan, May 1998. pp. 155–160.

He, W.H., and T.C. Wu (1999). Cryptanalysis and improvement of Petersen-Michel's signcryption scheme. In *IEE proceedings – Computers and Digital Techniques*, **146**(2). pp. 123–124.

Horster, P., M. Michel and H. Petersen (1994). Authenticated encryption schemes with low communication costs. *Electronics Letters*, **30**(15), 1212–1213.

Lee, W.B., and C.C. Chang (1995). Authenticated encryption scheme without using a one-way function. *Electronics Letters*, **31**(19), 1656–1657.

Menezes, A., P.V. Oorschot and S.A. Vanstone (1997). *Handbook of Applied Cryptography*. CRC Press.

NIST (1992). The digital signature standard by NIST. *Comm. ACM*, **35**(7), 36–40.

NIST FIP PUB 180 (1993). Secure hash standard, National Institute of Standards and Technology, US department of Commerce, DRAFT 1993.

Petersen, H., and M. Michel (1998). Cryptanalysis and improvement of sigcryption schemes. In *IEE proceedings – Computers and Digital Techniques*, **145**(2). pp. 149–151.

Rivest, R.L., A. Shamir and L. Adleman (1978). A method for obtaining digital signature and public-key cryptosystem. *Communications of the ACM*, **21**(2), 120–126.

Rivest, R.L. (1993). The MD5 message-digest algorithm. *RFC 1231*, Internet Activities Board, Internet Privacy Task Force.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In *Advances in Cryptography – CRYPTO'84*. Springer, New York. pp. 47–53.

Wu, T.S., and C.L. Hsu (2002). Convertible authenticated encryption scheme. *The Journal of Systems and Software*, **62**, 205–209.

Zheng, Y. (1997). Digital signcryption or how to achieve cost (signature & encryption) « cost (signature) + cost (encryption). In *Advances in Cryptology – CRYPTO'97*. Springer, New York. pp. 165–179.

H.-Y. Chien received the BS degree in computer science from National Chiao Tung University, Hsinchu, Taiwan, 1988, the MS degree in computer and information engineering from National Taiwan University, Taipei, Taiwan, 1990, and the doctoral degree in applied mathematics at National Chung Hsing University 2002. He was an assistant researcher at Telecommunication Laboratory, Ministry of Transportation and Communications, Taiwan, during 1992–1995. He was the director of Computer Center at Nan-Kei College. He is a member of the Chinese Association for Information Security, an IEEE member, and an ACM member. His research interests include cryptography, and network security.

Konvertuojamą tapatumą nustatanti šifravimo schema, nenaudojanti įprastinės vienkryptės funkcijos

Hung-Yu CHIEN

Tapatumą nustatantis šifravimas leidžia pranešimo gavėjui patikrinti tapatybę pranešimo gavimo metu. Kad būtų apsaugoti gavėjo interesai galimų ginčų atveju, konvertuojamą tapatumą nustatanti šifravimo schema leidžia gavėjui konvertuoti tapatumą nustatantį šifrą į įprastinį parašą, kuris gali būti viešai patikrintas. Šis straipsnis demonstruoja universalų Araki *et al.* pasiūlytos konvertuojamos tapatumą nustatančios šifravimo schemos klastojimą ir siūlo naują konvertuojamą tapatumą nustatančią šifravimo schemą. Siūloma schema nenaudoja įprastinių vienkrypčių funkcijų, tokiu budu sustiprina saugumo prielaidą, pagrįstą vien tik diskretaus logaritmo problemos, t.y. sunkios problemos, sprendimu.