MALAYSIAN JOURNAL OF SCIENCE
MJS
ISSN 1394-3065

VIRTUAL SYMPOSIUM ON MULTIDISCIPLINARY SCIENCE 2021

Special Issue

Malaysian Journal of Science 41 (Special Issue 1): 1-8 (September 2022)

https://mjs.um.edu.my

AN UPDATED CRYPTANALYSIS ON THE BFHP-DLP SIGNING SCHEME

Amir Hamzah Abd Ghafar[1a,b*], Muhammad Rezal Kamel Ariffin[2a,b], Muhammad Asyraf Asbullah[3b,c], Idham Arif Alias[4a]

Abstract: The concept of public-key cryptography introduced the notion of a digital signature scheme. In the era of online and digital communications, a signature scheme that works perfectly to achieve the goals of cryptography- confidentiality, authentication, data integrity, and non-repudiation, is urgently needed. However, every cryptosystem, including a digital signature scheme requires a well-defined difficult mathematical problem as its fundamental security strength, as demonstrated by the Diffie-Hellman key exchange with its discrete logarithm problem (DLP). Another problem called BFHP used by the AA_{β}-encryption scheme, has also withstood any destructive cryptanalysis since the scheme was introduced in 2013. Later, a digital signature scheme was introduced that combines both BFHP and DLP as difficult mathematical problems. Mathematical cryptanalysis was also performed against this scheme to test its security strength. This paper presents new cryptanalysis of the signing scheme. While the previous cryptanalysis focused only on BFHP, the obtained new results showed some improvement by scrutinizing the other difficult mathematical problem, DLP. In addition, several potential attacks on the future implementation by introducing side-channel and man-in-the-middle attacks against the scheme also will be discussed in this work. The countermeasures for each attack to enable the best-practice implementation of the scheme are also presented.

Keywords: *digital signing scheme, discrete logarithm problem, number field sieve, fault analysis attack, man-in-the-middle attack*

1. Introduction

Most digital applications of today's use required a digital signature scheme embedded in their core functions. The scheme serves the cryptographic goals of verifying the authenticity, integrity, and non-repudiation of a digital document transmitted over an insecure Internet channel. Traditional signing schemes were already introduced by ElGamal (1985), Rivest et al. (1978), and Schnorr (1991). Today, various protocols of signing schemes have been derived from these schemes and refined for niche purposes, including threshold signature (Gennaro et al., 2018; Ergezer et al., 2020), group signature (Islamidina et al., 2019; Nick et al., 2020), and blind signature (Alam et al., 2016; Fuchsbauer et al., 2020;) schemes. Some of the variants have become the backbone of the latest digital technologies, including blockchain systems (Stathakopoulou & Cachin, 2017; Guo & Lan, 2020). In addition, a standard digital signature scheme that can be used by public users has been introduced, namely, Public-Key Cryptography Standard (PKCS) #1 and Elliptic Curve Digital Signature Algorithm (ECDSA), which have been documented by the Internet Engineering Task Force (IETF) (Moriarty et al., 2016; Pornin, 2013).

All of the mentioned schemes use either the Integer Factorization Problem (IFP) or the Discrete Logarithm Problem (DLP), which are considered by many to be one-way functions in the mathematical domain (Hoffstein et al., 2008). These functions ensure the previously mentioned cryptographic goals are achieved by satisfying the properties of a mathematical one-way function. The functions are also resistant to all feasible algorithms that can work with current computing power. The best algorithm for solving IFP is the quadratic sieve algorithm described by Pomerance (1984), while several algorithms, namely the index computation, Pollard's rho, and number field sieve algorithms explained by Paar and Pelzl (2009), are among the best-known algorithms for solving it. However, all of these algorithms run in subexponential time at best, which prevents any active attack in real cryptographic implementations.

Authors information:
[a]Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, UPM Serdang, MALAYSIA.
E-mail: amir_hamzah@upm.edu.my[1], rezal@upm.edu.my[2], idham_aa@upm.edu.my[4]
[b]Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, UPM Serdang, MALAYSIA. E-mail: ma_asyraf@upm.edu.my[3]
[c]Centre of Foundation Studies for Agricultural Science. Universiti Putra Malaysia, UPM Serdang, MALAYSIA.

*Corresponding Author: amir_hamzah@upm.edu.my

Received: January 21, 2022
Accepted: April 13, 2022
Published: September 30, 2022

DOI: https://doi.org/10.22452/mjs.sp2022no1.1
Malaysian Journal of Science 41 (Special Issue 1): 1-8 (September 2022)

The approach of combining two difficult problems to increase the security of a cryptosystem is not new. Smith and Lennon (1993) introduced the LUC cryptosystem based on DLP and IFP. However, the attacks conducted against this cryptosystem (Jin et al., 2013; Wong et al., 2015; Sarbini et al., 2018;) have shown that it should be carefully examined before using any implementation. In this paper, the scheme is discussed by combining the DLP with another difficult mathematical problem called the Bivariate Function Hard Problem (BFHP). The problem was introduced by Ariffin et al. (2013) and has been used previously to develop a new encryption scheme called the AA_{β}-algorithm. The scheme relies solely on BFHP as its security strength and is suitable to be applied on an embedded system device due to its high encryption speed compared to conventional encryption schemes (Adnan et al., 2016). Its decryption algorithm has also withstood several side-channel attacks, which can be remedied by minimal additional operation (Abd Ghafar & Ariffin, 2014; Abd Ghafar & Ariffin, 2016).

1.1. Contribution of This Paper

This paper presents a new signing scheme that combines BFHP and DLP as a key security strength. The scheme, named BFHP-DLP signing scheme, was introduced by Abd Ghafar & Ariffin (2019) and is comparable in its computational operations to existing signing schemes such as RSA, ElGamal, and Schnorr. In contrast to the original paper, the scheme is presented based on its modules. This form of presentation is better suited to control access to the modules given to the intended entity. Another important contribution of this work is that three new improved attacks on the BFHP-DLP signing method being performed. The improved cryptanalysis is based on the recent results on solving DLP and techniques of side-channel attack and man-in-the-middle attack, which can be used to retrieve the values of the private keys of the scheme.

The first attack refers to the recent attempt by Boudot et al. (2020), who successfully solved DLP using the Number Field Sieve algorithm with a 795-bits prime. Hence, the obtained result proved how this recent result can affect the size criteria used in the key generation algorithm of the BFHP-DLP scheme. The second attack assumes that an adversary can perform a side-channel attack on the device that carries out the signing scheme. In the third attack, the authors showed that the adversary can successfully break the scheme using a man-in-the-middle attack method.

1.2. Outline of the Paper

The outline of methods used in this paper is as follows; number field sieve algorithm, side-channel attack, and man-in-the-middle attack are discussed in Section 2. Then, Section 3 describes the reintroduce BFHP-DLP signing scheme. The three attacks, which are the primary basis of this paper, will be presented in Section 4. Finally, the conclusion will be discussed in Section 5.

2. Preliminaries

This section describes the methods used in improved cryptanalysis. Although all methods are little known in the literature, they are widely used in attacks on public-key cryptosystems.

2.1 Number Field Sieve (NFS)

Before describing the number field sieve method, the problem of the discrete logarithm that the method attempts to solve is first defined. The problem is also used in the BFHP-DLP signing scheme.

Definition 1 (Discrete logarithm problem). Let $\boldsymbol{p}$ be a prime. Suppose $\mathbb{F}_{\boldsymbol{p}}$ is a prime-order finite field. Given $\boldsymbol{g}, \boldsymbol{h} \in \mathbb{F}_{\boldsymbol{p}}^{*}$, discrete logarithm problem is a problem to find $\boldsymbol{x}$ such that $\boldsymbol{g}^{\boldsymbol{x}} \equiv \boldsymbol{h} \pmod{\boldsymbol{p}}$.

The goal of the NFS in the finite field of DLP is to compute a non-trivial homomorphism from $\boldsymbol{G}$ to $\mathbb{Z}/\boldsymbol{\ell}\mathbb{Z}$ such that $\boldsymbol{G}$ is a subgroup of prime order $\boldsymbol{\ell}$ within $\mathbb{F}_{\boldsymbol{p}}^{*}$. The strategy to achieve this goal is to find two irreducible polynomials $\boldsymbol{f_0}$ of degree $\boldsymbol{u}$ and $\boldsymbol{f_1}$ of degree $\boldsymbol{v}$ in $\mathbb{Z}_{\boldsymbol{x}}$. These polynomials should have a common root $\boldsymbol{\mu}$ modulo $\boldsymbol{p}$. Let $\mathbb{Q}(\boldsymbol{i})$ be the number field defined by $\boldsymbol{f}$ where $\boldsymbol{i} \in \mathbb{C}$ is a root of $\boldsymbol{f_1}$ such that $\boldsymbol{f_1}$ is an irreducible polynomial, then the most challenging task in NFS is to find a pair of integers $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ such that

$$\boldsymbol{\gamma} = \boldsymbol{\alpha} - \boldsymbol{\beta\mu} \text{ and } \boldsymbol{\delta} = \boldsymbol{\alpha} - \boldsymbol{\beta i}$$

are both decomposable into small factors, i.e. smooth numbers. Many papers in the literature are devoted to finding the relation between $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, since this step takes up most of the computations (computational power and computational storage. In this case, the result from this method is applied to fit into our key generation algorithm; as described in detail by Boudot et al. (2019)

2.2 Side-channel attack

This attack focuses on the implementation of cryptosystems in electronic devices. It relies on observable outputs such as computing time, power consumption, acoustic form and many more during cryptographic processes. The adversary can collect these outputs because the computation takes place in a 'black box' system, i.e. the adversary can only examine the functionality of the devices but has no access to the private functioning. The attack introduced by Kocher (1996) typically examines the private computations of the signing scheme. In this paper, the signing algorithm of the BFHP-DLP scheme is specifically become the main focus.

DOI: https://doi.org/10.22452/mjs.sp2022no1.1
Malaysian Journal of Science 41 (Special Issue 1): 1-8 (September 2022)

2.2.1 Fault Analysis

By the definition of a side-channel attack, an attacker cannot determine the internal states of the attacked cryptographic devices. However, by introducing unexpected environmental conditions that can lead to data corruption into a specific part of the processor executed by the devices, the attacker can cause errors in the targeted cryptographic computations. By neglecting the error, the attacker can then isolate the instructions executed by the devices and eventually determine the internal workings of computations.

In a seminal work by Bao et al. (1997), $\boldsymbol{p}$ is the public key of the ElGamal signature scheme and *M* is the message to be signed. This showed that an attacker can obtain the actual signature by flipping one bit of the private signing key, $\boldsymbol{d}$ at the $\boldsymbol{i}$-th bit position, thus forming an erroneous $\boldsymbol{d}'$, then

$$\boldsymbol{S} \equiv \boldsymbol{M^d} (\text{mod } \boldsymbol{p})$$

and the faulty signature,

$$\boldsymbol{S'} \equiv \boldsymbol{M^{d'}} (\text{mod } \boldsymbol{p}).$$

Both signatures then can be used to determine the bit of $\boldsymbol{d}$ at $\boldsymbol{the\ i}$-th position by computing the function

$$\frac{\boldsymbol{S'}}{\boldsymbol{S}} \equiv \boldsymbol{M^{d'-d}} \equiv \begin{cases} \boldsymbol{M^{2i}} \ (\text{mod } \boldsymbol{p}) \text{ if the } \boldsymbol{i} - \text{th bit of } \boldsymbol{d} = \boldsymbol{0} \\ \dfrac{\boldsymbol{1}}{\boldsymbol{M^{2i}}} (\text{mod } \boldsymbol{p}) \text{ if the } \boldsymbol{i} - \text{th bit of } \boldsymbol{d} = \boldsymbol{1} \end{cases}.$$

To extend the attack and determine the entire bits of the private key, each bit with $\boldsymbol{i} = \boldsymbol{1, 2, 3, \ldots, n}$ should be examined and a subexponential algorithm is needed. The attack shows the significance of thorough cryptanalysis to ensure that the signature cannot be compromised to obtain information about the private keys.

2.3 Man-in-the-middle attack

If the communication between two units is secretly intercepted by an adversary, the immediate consequence depends on whether the adversary is actively involved in the communication. For example, if the adversary surreptitiously forwards and modifies the communication, there is a man-in-the-middle attack on the communication.

A suitable authentication mechanism is required to prevent this attack. The standard mechanism currently used is the exchange of digital certificates issued and verified by a trusted Certificate Authority (CA). However, this CA can also be a target of a man-in-the-middle attack. Therefore, CA must be subjected to proper evaluation and security verification at regular intervals.

In this paper, a man-in-the-middle attack is constructed against the BFHP-DLP signature procedure. The existence of such an attack shows that it is necessary to first develop a suitable cryptographic protocol before this system can be used in an application.

3. BFHP-DLP Signing Scheme

In this study, our scheme is rewritten and compared to the original paper by (Abd Ghafar & Ariffin, 2019) in our to separate our schemes into their purported modules. This form is more suitable for cryptanalysis of our scheme, especially when the modules may have different access controls even though they are included in the same algorithm. It also reflects the actual use of a cryptographic scheme in a real scenario.

The initialisation and key generation algorithms of the scheme, as shown in Figure 1.

$\mathcal{I}$: Initialization algorithm $\rightarrow (\boldsymbol{p}, \boldsymbol{g})$
Select $\boldsymbol{p}$ randomly from $\mathbb{Z}_{\boldsymbol{2^m}}$ where $\boldsymbol{m}$ is a large integer Select $\boldsymbol{g}$ from $\mathbb{Z}_{\boldsymbol{p}}^*$ where $\boldsymbol{g}$ is a primitive root of group $\mathbb{Z}_{\boldsymbol{p}}^*$

$\mathcal{K}$: Key Generation algorithm $\rightarrow (\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{A}, \boldsymbol{B})$
Private key Given $\boldsymbol{n} > \boldsymbol{m}$. select $\boldsymbol{a}$ randomly from $\mathbb{Z}_{\boldsymbol{2^n}}$ select $\boldsymbol{b}$ randomly from $\mathbb{Z}_{\boldsymbol{2^n}}$ Public key compute $\boldsymbol{A} \equiv \boldsymbol{g^a} (\text{mod } \boldsymbol{p})$ compute $\boldsymbol{B} \equiv \boldsymbol{g^b} (\text{mod } \boldsymbol{p})$

Figure 1. Initialization and key generation algorithms of BFHP-DLP signing scheme

As in Figure 1, the algorithms are typically computed by isolated devices controlled by a Trusted Third Party (TTP). An example of such a TTP practice is CA (as referred to in Section 2.3), which is validated by government agencies. This approach ensures that only the authorised body can monitor the process. After the keys are generated, the private keys are securely stored in a tampered-resistant device, such as chips on a smartcard or a secure token carried by the authenticated owners.

Next, the algorithms for signing and verification of the scheme are shown in Figure 2.

In the signature algorithm, a hash function $\boldsymbol{H}$ creates a digital fingerprint of $\boldsymbol{M}||\boldsymbol{r}$, which is the concatenation of the original message, $\boldsymbol{M}$ with the private parameter, $\boldsymbol{r}$. The standard hash function used today is SHA-256 and its variants.

DOI: https://doi.org/10.22452/mjs.sp2022no1.1
Malaysian Journal of Science 41 (Special Issue 1): 1-8 (September 2022)

$\mathcal{S}$: Signature algorithm of $M \rightarrow (M, \sigma, e)$
Public ephemeral key
select x randomly from $\mathbb{Z}_{2^m}$
select y randomly from $\mathbb{Z}_{2^m}$
Private session key
compute $c = ax + by$
select k randomly from $\mathbb{Z}_{2^n}$ such that
$c - k > 2^m$ and $n > m$.
Private computation of signing M
compute $s = c - k$
compute $r \equiv g^k (\text{mod } p)$
$e = H(M \| r)$ where H is a hash function
Output public signature $\sigma = (x, y, s, e)$

$\mathcal{V}$: Verification algorithm of (M, σ)
Verification key
compute $r' \equiv A^x \cdot B^y \cdot g^{-s} (\text{mod } p)$
Check whether
$H(M \| r') = e \rightarrow$ Yes/No

Figure 2. Signing and verification algorithms of BFHP-DLP signing scheme

Proof of Correctness. It is easy to see that

$$A^x B^y \equiv g^{ax} g^{by} \equiv g^{ax+by} \equiv g^c (\text{mod } p). \quad (14)$$

If the correct c is obtained, r' will produce $H(M \| r') = e$.

4. The Updated Cryptanalysis

This section presents the updated cryptanalysis of BFHP-DLP discovered based on the new techniques described in Section 2. The cryptanalysis can be categorized into three different attacks. The first attack focuses solely on solving DLP, while the second and third attacks are based on the assumption of the complexity of the scheme's key generation algorithm is reduced.

4.1 First Attack: Number Field Sieve

Boudot et al. (2019) showed that a DLP over a 795-bit prime field can be computed in 18-days using the latest computational technologies, well-chosen parameters and suitable algorithmic variants. In this attack, the assumption is made that their result affects our signing scheme, especially the parameters selection criterion in algorithms $\mathcal{I}, \mathcal{K}$ and $\mathcal{S}$.

In the BFHP-DLP signing scheme, there are three instances of DLP, namely $A \equiv g^a (\text{mod } p)$ and $B \equiv g^b (\text{mod } p)$ of algorithm $\mathcal{K}$ and $r \equiv g^k (\text{mod } p)$ of algorithm $\mathcal{S}$. Although $a, b > k$, since $a, b \in \mathbb{Z}_{2^n}$ and $k \in \mathbb{Z}_{2^m}$, where $n > m$, but all computations of DLP take place in an m-bit prime field p, so that $p \in \mathbb{Z}_{2^m}$. From this observation with the results of Boudot et al. (2019), it can be noticed that those private keys a, b can be retrieved when $m \leq 795$. So, a larger m is required to ensure that the scheme can exploit the security strength of DLP.

Since the original work by (Abd Ghafar & Ariffin, 2019) did not mention the appropriate size of m and n, so it can be proposed that m is at least 2048 and $n = 2m = 4096$. This recommendation follows the NIST standard for cryptographic keys using DLP (Barker & Dang, 2015).

4.2 Second Attack: Fault Analysis

Every implementation of a cryptosystem attempts to reduce the complexity of the cryptographic algorithms. Reduced complexity leads to reduce computational time, power consumption, or memory capacity, making it attractive to be implemented in a smaller device. Based on this motivation, it assumed that the possibility to fix the value of the parameter k is an attractive solution. The fixed values result in a fixed r, since $r \equiv g^k (\text{mod } p)$. Furthermore, random selection can be omitted so less power and memory can be fixed for r. However, it can be seen that this approach can be advantageous for the adversary to determine the bits of k using the method described in Section 2.2.1.

Definition 2 (Fault analysis adversary, $\mathcal{A}_1$). $\mathcal{A}_1$ is defined as an adversary that is able to inject a faulty environment into the Algorithm $\mathcal{S}$ that can invert a bit of k at ith position (from the right), k_i to its complement bit, k_i'.

Example 1. Let $k = 3787$ with bits 111011001011. Given $i = 8$, then A_1can flip $k_5 = 1$ to $k_5' = 0$, which produces $k' = 3659$ with bits 111001001011.Noted that $|k - k'| = |3787 - 3659| = 128 = 2^7$.

The attack is stated in the following theorem.

Proposition 1. Let k be the private session key generated in algorithm $\mathcal{S}$. Let $\mathcal{A}_1$ be defined in Definition 2. If k is used more than $n - 1$ times, then the entire bits of k can be known.

Proof. Assume that $\mathcal{A}_1$ can change k_i in k is to its complement k_i' which produces k' during the signing process in Algorithm $\mathcal{S}$ as defined in Definition 2. Since the value of k differs from k' at i-th bit position, then $|k - k'| = 2^{i-1}$ or

$$k = \begin{cases} k' - 2^{i-1} \text{ if the } i - \text{th bit of } k = 0 \\ k' + 2^{i-1} \text{ if the } i - \text{th bit of } k = 1 \end{cases}$$

Observe that

$$s = \begin{cases} c - (k' - 2^{i-1}) \text{ if the } i - \text{th bit of } k = 0 \\ c - (k' + 2^{i-1}) \text{ if the } i - \text{th bit of } k = 1 \end{cases}. \quad (1)$$

DOI: https://doi.org/10.22452/mjs.sp2022no1.1
Malaysian Journal of Science 41 (Special Issue 1): 1-8 (September 2022)

Algorithm $\mathcal{S}$ computed that

$$\tilde{r} \equiv g^{k'} (\text{mod } p) \quad (2)$$

and output

$$e' = H(M \| \tilde{r})$$

to be included in the signature σ. Let

$$\begin{aligned} \tilde{s}_1 &= s - 2^{i-1} \\ \tilde{s}_2 &= s - 2^{i-1} \end{aligned} \quad (3)$$

then $\mathcal{A}_1$ can obtain the potential candidates for $\tilde{r}$ based on (1), (2), and (3) by computing

$$\begin{aligned} A^x \cdot B^y \cdot g^{-\tilde{s}_1} &\equiv g^{ax+by-(s-2^{i-1})} \\ &\equiv g^{ax+by-(c-(k'-2^{i-1})-2^{i-1})} \\ &\equiv g^{k'} \equiv \widetilde{r_1} (\text{mod } p) \end{aligned} \quad (4)$$

or

$$\begin{aligned} A^x \cdot B^y \cdot g^{-\tilde{s}_2} &\equiv g^{ax+by-(s+2^{i-1})} \\ \equiv g^{ax+by-(c-(k'+2^{i-1})+2^{i-1})} &\equiv g^{k'} \equiv \widetilde{r_2} (\text{mod } p) \end{aligned} \quad (5)$$

if the $i-$ th bit of $k = 1$. Noted that both (4) and (5) should be executed by $\mathcal{A}_1$ since, at this point, $\mathcal{A}_1$ still does not know if the $i-$ th bit of k is 0 or 1. By using the outputs from (4) and (5), now $\mathcal{A}_1$ can determine the original bits of k_i by checking whether

$$e' = \begin{cases} H(M \| \widetilde{r_1}) & \text{if the } i-\text{th bit of } k = 0 \\ H(M \| \widetilde{r_2}) & \text{if the } i-\text{th bit of } k = 1 \end{cases}$$

It can be shown how $\mathcal{A}_1$ can determine one bit of k at position i. If $\mathcal{A}_1$ repeats the same process for $n-1$ times, then $\mathcal{A}_1$ has the total bits of k since $k \in \mathbb{Z}_{2^n}$ or has n-bit size. This terminates the proof.

■

Theorem 1. Let (a, b) be the private keys generated from algorithm $\mathcal{K}$. Suppose (x, y) and k are randomized values from algorithm $\mathcal{S}$ and $s = c - k$ is one of the signature parameters from σ defined in algorithm $\mathcal{S}$. If full bits of k are retrieved from Proposition 1, then (a, b) can be known.

Proof. By knowing the entire bits of k, an adversary can compute $c = s + k$ since s is a public parameter obtained from σ. By knowing c, the adversary can retrieve (a, b) values using the Extended Euclidean algorithm since $ax + by = c$ and values of (x, y) are known from σ. This terminates the proof.

■

4.2.1 Countermeasures of the Second Attack

The attacks presented in Proposition 1 and Theorem 1 proved that it is possible for an adversary satisfying Definition 2 to retrieve the private keys of the BFHP-DLP signing scheme. Therefore, the apparent approach to avoid the attack is to never set k to a static value. Although this approach may be counterproductive to the implementation, exposing arbitrary bits of k can lead to a specified attack called a partial key exposure attack.

4.3 Third Attack: Man-in-the-Middle

Definition 3 (Active adversary, $\mathcal{A}_2$). Let $\sigma = (x, y, s, e)$ be defined as in Figures 1 and 2. An active adversary $\mathcal{A}_2$ is defined as a man-in-the-middle adversary who intercepts σ and then modifies it before sending it back to the intended recipient of σ.

The attack is described in the following theorem.

Theorem 2. Assume that (a, b) are the private keys generated from algorithm $\mathcal{K}$. Assume that (x, y) are random values from algorithm $\mathcal{S}$ and that signature $\sigma = (x, y, s, e)$ was computed using the same algorithm. If there is an active adversary $\mathcal{A}_2$ according to Definition 3, then $\mathcal{A}_2$ can forge a signature $\sigma' = (x, y, s', e')$, which is verified in algorithm $\mathcal{V}$.

Proof. Suppose that $\sigma = (x, y, s, e)$ was generated by Alice using algorithm $\mathcal{S}$. Assuming $\mathcal{A}_2$ is an adversary defined in Definition 3, then $\mathcal{A}_2$ can prevent σ from reaching the intended receiver, Bob. $\mathcal{A}_2$ can then compute

$$A^x \cdot B^y \cdot g^{-s} \equiv r' (\text{mod } p)$$

using algorithm $\mathcal{V}$ as in Figure 2 then modifies r' by computing

$$r' \cdot g^{\delta} \equiv g^k \cdot g^{\delta} \equiv g^{k+\delta} \equiv r'' (\text{mod } p)$$

for some $\delta \in \mathbb{Z}$. $\mathcal{A}_2$ also modifies s by computing

$$s - \delta = c - k - \delta = s'.$$

By using r' and a forged message, M', $\mathcal{A}_2$ then computes forged e' by computing

$$e' = H(M' \| r'')$$

using a hash function, H. $\mathcal{A}_2$ then sends $\sigma' = (x, y, s', e')$ and M' to Bob, acting like they are from Alice, the original sender. Then, Bob compute

$$\begin{aligned} A^x \cdot B^y \cdot g^{-s'} \equiv g^{ax} \cdot g^{by} \cdot g^{-s'} \equiv g^{ax+by-(c-k-\delta)} \equiv g^{k+\delta} \\ \equiv r'' (\text{mod } p) \end{aligned}$$

using algorithm $\mathcal{V}$ and verifies r'' by computing $H(M' \| r'')$ equal to e' sent along with the forged σ. It is shown that $\mathcal{A}_2$ has forged Alice's signature, σ, by converting it to σ' and then

DOI: https://doi.org/10.22452/mjs.sp2022no1.1
Malaysian Journal of Science 41 (Special Issue 1): 1-8 (September 2022)

sending it to Bob. Bob has also verified σ', without knowing σ' is a forgery signature. This terminates the proof.

■

4.3.1 Countermeasures of the Third Attack

The third attack is considered the most devastating attack on the BFHP-DLP signing scheme because it occurs during the most important process of the scheme, which is sending the signature to the intended recipient. The attack occurs because $\mathcal{A}_2$ can obtain r by computing $A^x \cdot B^y \cdot g^{-s} (\text{mod } p)$ and then modifying it. By depriving $\mathcal{A}_2$ of access to the values of x and y, it can be noticed that the modification can be prevented. Therefore, the modified signature scheme is proposed, which uses an encryption function Enc_{K_1} with the encryption key, K_1, and a decryption function Dec_{K_2} with the decryption key, K_2. The modified signature algorithms with their corresponding verification algorithms are shown in Figure 3.

S': Modified signature algorithm of $M \rightarrow (M, \sigma, e)$
Public ephemeral key
select x randomly from $\mathbb{Z}_{2^m}$
select y randomly from $\mathbb{Z}_{2^m}$
Private session key
compute $c = ax + by$
select k randomly from $\mathbb{Z}_{2^n}$ such that
$c - k > 2^m$ and $n > m$.
Encrypt verification key using Bob's public key, i
compute $X = Enc_{K_1}(x)$ and $Y = Enc_i(y)$
Private computation of signing M
compute $s = c - k$
compute $r \equiv g^k (\text{mod } p)$
$e = H(M \| r)$ where H is a hash function
Output public signature $\sigma = (X, Y, s, e)$

V': Modified verification algorithm of (M, σ)
Decrypt verification key using Bob's private key, j
compute $x = Dec_{K_2}(X)$ and y= $Dec_j(Y)$
Verification key
compute $r' \equiv A^x \cdot B^y \cdot g^{-s} (\text{mod } p)$
Check whether
$H(M \| r') = e \rightarrow$ Yes/No

Figure 3. Modified signing and verification algorithms of BFHP-DLP signing scheme

5. Conclusion

Three novel cryptanalyses against the BFHP-DLP signing scheme are presented in this study. The first attack applies the latest result that successfully solves DLP. This countermeasure sets the parameter size of n and m larger than the values attacked by the previous result. This countermeasure will not affect the efficiency of the scheme because the size of n and m is the appropriate cryptographic size specified in the NIST standard. Then, the second attack highlights the danger of specifying the values of k to be used multiple times, as this can expose the signing scheme to a side-channel method called fault analysis. To prevent this attack, the signing key algorithm must use an efficient pseudorandom number generator to ensure that k is generated randomly and not static. Finally, the last attack is considered the most devastating attack. It requires an active adversary to perform a man-in-the-middle method by modifying the transmitted signature σ to solve the private values of the scheme. The countermeasure to this attack introduces an encryption scheme that allows a seamless signing and verification process without intervention by the man-in-the-middle. Although the process can be redundant, it can be skipped once a shared private key is created, hence increasing its efficiency. These cryptanalyses not only focus on the hardness of BFHP, as in the existing cryptanalysis against the scheme but also cover the computational complexity of DLP and possible attacks against the real implementation of the scheme. The countermeasures presented will be of great use for the future deployment of the scheme.

6. Acknowledgment

The research was supported by the Ministry of Higher Education of Malaysia with the Fundamental Research Grant Scheme (FRGS/1/2020/STG06/UPM/02/2).

7. References

Abd Ghafar, A. H., & Ariffin, M. R. K (2014). Timing Attack Analysis on AA_β Cryptosystem. *Journal of Computer and Communications*, *2*(4), 1-9.

Abd Ghafar, A. H., & Ariffin, M. R. K. (2016). SPA on Rabin variant with public key $N = p^2q$. *Journal of Cryptographic Engineering*, *6*(4), 339-346.

Abd Ghafar, A. H., & Ariffin, M. R. K. (2019). A New Signing Scheme Based on BFHP and DLP. *International Journal of Cryptology Research*, *9*(2), 31-44.

Adnan, S. F. S., Isa, M. A. M., & Hashim, H. (2016). Implementation of the Aa-Beta (AAβ) lightweight asymmetric encryption scheme on an embedded system device. *Advanced Science Letters*, *22*(10), 2910-2913.

Alam, K., Alam, K. R., Faruq, O., & Morimoto, Y. (2016, January). A comparison between RSA and ElGamal based untraceable blind signature schemes. In *2016*

DOI: https://doi.org/10.22452/mjs.sp2022no1.1
Malaysian Journal of Science 41 (Special Issue 1): 1-8 (September 2022)

International Conference on Networking Systems and Security (NSysS) (pp. 1-4). IEEE.

Ariffin, M. R. K., Asbullah, M. A., Abu, N. A., & Mahad, Z. (2013). A New Efficient Asymmetric Cryptosystem Based on the Integer Factorization Problem of $= p^2q$. Malaysian Journal of Mathematical Sciences, 7, 19-37.

Bao, F., Deng, R. H., Han, Y., Jeng, A., Narasimhalu, A. D., & Ngair, T. (1997, April). Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults. In *International Workshop on Security Protocols* (pp. 115-124). Springer, Berlin, Heidelberg.

Barker, E., & Dang, Q. (2015). NIST special publication 800–57 part 3: Application-specific key management guidance. *NIST Special Publication*, *800*, 57.

Boudot, F., Gaudry, P., Guillevic, A., Heninger, N., Thomé, E., & Zimmermann, P. (2020, August). Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment. In *Annual International Cryptology Conference* (pp. 62-91). Springer, Cham.

Diffie, Whitfield, and Martin Hellman. "New directions in cryptography." IEEE transactions on Information Theory 22.6 (1976): 644-654.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4), 469-472.

Ergezer, S., Kinkelin, H., & Rezabek, F. (2020). A Survey on Threshold Signature Schemes. *Network*, *49*.

Fleischhacker, N., Jager, T., & Schröder, D. (2019). On tight security proofs for Schnorr signatures. *Journal of Cryptology*, *32*(2), 566-599.

Fuchsbauer, G., Plouviez, A., & Seurin, Y. (2020, May). Blind Schnorr signatures and signed ElGamal encryption in the algebraic group model. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 63-95). Springer, Cham.

Gennaro, R., & Goldfeder, S. (2018, October). Fast multiparty threshold ECDSA with fast trustless setup. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1179-1194).

Goldwasser, S., Micali, S., & Rivest, R. L. (1988). A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on computing, 17(2), 281-308.

Guo, L., & Lan, C. (2020, December). A New Signature Based on Blockchain. In *2020 International Conference on Intelligent Computing, Automation and Systems (ICICAS)* (pp. 349-353). IEEE.

Herrmann, M., & May, A. (2008, December). Solving linear equations modulo divisors: On factoring given any bits. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 406-424). Springer, Berlin, Heidelberg.

Hoffstein, J., Pipher, J., Silverman, J. H., & Silverman, J. H. (2008). *An introduction to mathematical cryptography* (Vol. 1). New York: Springer.

Islamidina, A. D. P., Sudarsono, A., & Dutono, T. (2019, September). Security System for Data Location of Travelling User using RSA based on Group Signature. In *2019 International Electronics Symposium (IES)* (pp. 88-93). IEEE.

Jin, W. T., Kamarulhaili, H., Said, M. R. M., Ariffin, M. R. K., Asbullah, M. A., Abu, N. A., ... & Jahani, S. (2013). On the Hastad's Attack to LUC4, 6 Cryptosystem and compared with Other RSA-Type Cryptosystem. *Malaysian Journal of Mathematical Sciences*, *7*, 1-17.

Joux, A. (2013, August). A new index calculus algorithm with complexity $$ l (1/4+ o (1)) $$ in small characteristic. In International Conference on Selected Areas in Cryptography (pp. 355-379). Springer, Berlin, Heidelberg.

Karatsuba, A. (1963). Multiplication of multidigit numbers on automata. In Soviet physics doklady (Vol. 7, pp. 595-596).

Kim, S., Kim, J., Cheon, J. H., & Ju, S. H. (2011). Threshold signature schemes for ElGamal variants. *Computer Standards & Interfaces*, *33*(4), 432-437.

Kocher, P. C. (1996, August). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Annual International Cryptology Conference* (pp. 104-113). Springer, Berlin, Heidelberg.

Kravitz, D. W. (1993). Digital signature algorithm. US Patent, 5(231), 668.

Lenstra, A. K., Lenstra, H. W., Manasse, M. S., & Pollard, J. M. (1993). The number field sieve. In *The development of the number field sieve* (pp. 11-42). Springer, Berlin, Heidelberg.

Montgomery, P. L. (1985). Modular multiplication without trial division. Mathematics of computation, 44(170), 519-521.

DOI: https://doi.org/10.22452/mjs.sp2022no1.1
Malaysian Journal of Science 41 (Special Issue 1): 1-8 (September 2022)

Moriarty, K., Kaliski, B., Jonsson, J., & Rusch, A. (2016). PKCS# 1: RSA cryptography specifications version 2.2. Internet Engineering Task Force, Request for Comments, 8017.

Nick, J., Ruffing, T., & Seurin, Y. (2020). *MuSig2: Simple Two-Round Schnorr Multi-Signatures*. Cryptology ePrint Archive, Report 2020/1261, 2020. https://eprint. iacr. org/2020/1261.

Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.

Pomerance, C. (1984, April). The quadratic sieve factoring algorithm. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 169-182). Springer, Berlin, Heidelberg.

Pornin, T. (2013). Deterministic usage of the digital signature algorithm (DSA) and elliptic curve digital signature algorithm (ECDSA). *Internet Engineering Task Force RFC*, *6979*, 1-79.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

Sarbini, I. N., Jin, W. T., Feng, K. L., Othman, M., Said, M. R. M., & Hung, Y. P. Garbage-man-in-the-middle (type 2) Attack on the Lucas Based El-Gamal Cryptosystem in the Elliptic Curve Group Over Finite Field. In *Cryptology and Information Security Conference 2018* (p. 35).

Schnorr, C. P. (1991). Efficient signature generation by smart cards. Journal of cryptology, 4(3), 161-174.

Seurin, Y. (2012, April). On the exact security of Schnorr-type signatures in the random oracle model. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 554-571). Springer, Berlin, Heidelberg.

Smith, P. J., & Lennon, M. J. (1993, May). LUC: A New Public Key System. In *SEC* (pp. 103-117).

Stathakopoulou, C., & Cachin, C. (2017). Threshold signatures for blockchain systems. *Swiss Federal Institute of Technology*.

Wong, T. J., Said, M. R. M., Othman, M., & Koo, L. F. (2015, May). On the common modulus attack into the LUC4, 6 cryptosystem. In *AIP Conference Proceedings* (Vol. 1660, No. 1, p. 090052). AIP Publishing LLC.

DOI: https://doi.org/10.22452/mjs.sp2022no1.1
Malaysian Journal of Science 41 (Special Issue 1): 1-8 (September 2022)