An Analysis of the Generalized ID-Based ElGamal Signatures

Hatice Koyuncu
Information Security Department
ASELSAN INC
Ankara, 06172, Turkey
Email: hkoyuncu@aselsan.com.tr

Kamer Kaya
Department of Computer Engineering
Bilkent University
Ankara, 06800, Turkey
Email: kamer@cs.bilkent.edu.tr

Ali Aydın Selçuk
Department of Computer Engineering
Bilkent University
Ankara, 06800, Turkey
Email: selcuk@cs.bilkent.edu.tr

***Abstract*—There have been many ID-based signature schemes proposed in recent years, most of which are, in one way or another, variants of the ElGamal signature scheme. Kalkan et al. proposed the concept of "generalized ID-based ElGamal signatures" as a unifying framework for these schemes, which also produced many new variants. In this paper, we analyze the security of these signature schemes and show that some of the proposed variants are insecure.**

***Index Terms*—ID-based cryptography, ElGamal signatures, bilinear pairings.**

I. Introduction

In 1984, Shamir [11] introduced the concept of ID-based cryptography to simplify key management procedures in public key infrastructures. Following Joux's [7] discovery on how to utilize bilinear pairings in public key cryptosystems, Boneh and Franklin [2] proposed the first practical ID-based encryption scheme in Crypto 2001. Since then, ID-based cryptography has become one of the most active research areas in cryptography and numerous ID-based encryption and signature schemes have been proposed that use bilinear pairings.

ID-based cryptography helps us to simplify the key management process in traditional public key infrastructures. In ID-based cryptography any public information such as e-mail address, name, etc., can be used as a public key. Since public keys are derived from publicly known information, their authenticity is established inherently and there is no need for certificates in ID-based cryptography. The private key for a given public key is generated by a trusted authority and is sent to the user over a secure channel.

Recently, there have been many proposals for ID-based signatures [1], [3], [5], [9], [10], [12] and most of these schemes, in one way or the other, have been based on the ElGamal signature algorithm [4]. Horster et al. [6] showed that many variations of the basic ElGamal signature are possible by modifying the signature equation. Following their work, Kalkan et al. [8] extended those variants to the ID-based setting and observed that most of the existing ID-based signature schemes [1], [3], [5], [9], [10], [12] are special instances of a more general concept which they called the generalized ID-based ElGamal signature.

In this work, we analyze the security of these ID-based ElGamal signature variants and show that some of the schemes proposed by Kalkan et al. are actually insecure. We first show how an attacker, having observed a message-signature pair, can obtain the private key of the signer or forge signatures on new messages. Second, we propose certain modifications on some of these signatures to avoid the security flaws involved.

The rest of the paper is organized as follows: Background concepts including bilinear pairings and generalized ElGamal signatures are discussed in Section II. We describe Kalkan et al.'s generalized ID-Based ElGamal signatures in detail in Section III. Some security flaws and attacks for some of the variants in [8] are described in Section IV and modifications to fix these variants are proposed in Section V. Section VI concludes the paper.

II. Background

In this section, we present the tools that are used in generalized ID-based ElGamal signatures. We briefly discuss bilinear pairings, the ElGamal signature scheme and its generalizations.

A. Bilinear Pairings

Let G_1 be a cyclic additive group of order q generated by P. Let G_2 be a cyclic multiplicative group of the same order. A cryptographic bilinear pairing is defined as $e : G_1 \times G_1 \rightarrow G_2$ with the following properties:

1) *Bilinearity:* $e(aR, bS) = e(R, S)^{ab}$ where $R, S \in G_1$ and $a, b \in \mathbb{Z}_q$. This can also be stated as $\forall R, S, T \in G_1$ $e(R + S, T) = e(R, T)e(S, T)$ and $e(R, S + T) = e(R, S)e(R, T)$
2) *Non-degeneracy:* The map e does not send all pairs in $G_1 \times G_1$ to the identity of G_2. That is $e(P, P) \neq 1$.
3) *Computability:* There exists an efficient algorithm to compute $e(R, S)$ for any $R, S \in G_1$

B. ElGamal Signature Scheme

Let p be a large prime and g be a generator of $\mathbb{Z}_p^*$. The user chooses $\alpha \in \mathbb{Z}_{p-1}$ as his private key and then computes $\beta = g^\alpha \bmod p$ as his public key. The parameters p, g, and β are public whereas the user keeps α secret. To sign a message, the user generates a random $k \in_R \mathbb{Z}_{p-1}$. Then he computes

$r = g^k \bmod p$ and $s = k^{-1}(m - r\alpha) \bmod (p-1)$. The (r, s) pair is the signature of message m. The equation

$$m \equiv \alpha r + ks \pmod{p-1} \tag{1}$$

is called *the signature equation*, and verification is done by checking the congruence $g^m \stackrel{?}{\equiv} \beta^r r^s \bmod p$. Security of ElGamal signature relies on the discrete logarithm problem (DLP) since solving α from β or s from r, m, β can be reduced to solving the DLP in $\mathbb{Z}_p^*$.

C. The Meta-ElGamal Signature Scheme

Horster et al. [6] showed that many variations of the basic ElGamal signature are possible by modifying the signature equation. Instead of using ElGamal's original signature equation, one can use the general equation

$$\pm A \equiv \pm \alpha B \pm kC \pmod{q}$$

where A, B and C are functions of m, r and s, q is a divisor of $p-1$, and g is an element in $\mathbb{Z}_p^*$ of order q. The signature can be verified by checking the equation:

$$g^{\pm A} \stackrel{?}{\equiv} \beta^{\pm B} r^{\pm C} \pmod{p} \tag{2}$$

We refer the reader to [6] and [8] for further details.

D. An ID-Based ElGamal Signature Scheme

Let the private key generator (PKG) be a trusted party responsible for verifying the users' identities and generating their private keys. An ID-based signature scheme consists of four algorithms: SETUP, EXTRACT, SIGN, and VERIFY. As an example, consider the following ID-based version of the original ElGamal signature scheme:

- SETUP: Let G_1 be a cyclic additive group of order q generated by P. Let G_2 be a cyclic multiplicative group of the same order and $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing. The PKG chooses $s \in_R \mathbb{Z}_q^*$ as the global secret key and computes $P_{pub} = sP$ as the global public key. The PKG publishes system parameters $\langle G_1,\ G_2,\ e,\ P,\ P_{pub},\ H,\ H_1 \rangle$ where H and H_1 are secure hash functions.
- EXTRACT: PKG verifies the user's identity ID and computes $Q_{ID} = H_1(ID)$ and $S_{ID} = sQ_{ID}$ as user's public and private keys respectively.
- SIGN: To sign a message $m \in \mathbb{Z}_q$, a user with his private key S_{ID}, first chooses $k \in_R \mathbb{Z}_q$, then computes:

  $$r = H(kP)$$
  $$U = k^{-1}(mP - rS_{ID})$$

  The signature for the message m is (kP, U)
- VERIFY: Given ID, a message m, and a signature (kP, U), the signature is valid if the following equation holds:

  $$e(U, kP)e(Q_{ID}, P_{pub})^r \stackrel{?}{=} e(P, P)^m \tag{3}$$

The above scheme is the ID-based version of the original ElGamal signature scheme. The conversion process, which can also be used for the generalized signature equation, is described below:

In the original ElGamal scheme, the signature equation is $m \equiv \alpha r + ks \bmod (p-1)$ where $r = g^k$ and the signature is (r, s). The corresponding signing equation for the ID-based ElGamal signature is:

$$mP = rS_{ID} + kU$$

Here, the uppercase letters are used to denote elements of the elliptic curve group G_1. S_{ID} is the private key of the user; so it is a natural replacement for α in the original scheme. U is the part of the signature that replaces s. The message m cannot be used in the equation directly since it is not a member of elliptic curve group; therefore mP is used to replace m.

A natural choice for r in the ID-based scheme is to compute r as $r = kP$ since r equals g^k in the original scheme. However, r must be an integer in $\mathbb{Z}_p$ in the signature equation, hence, it can be computed as $r = H(kP)$. Since kP is needed for verification (3), the signature will be issued as (kP, U) instead of (r, U).

III. GENERALIZED ID-BASED ELGAMAL SIGNATURES

Kalkan et al. [8] discussed how the ID-based signature scheme above can be generalized by using the generalized signing equation

$$A = BS_{ID} + kC, \tag{4}$$

where (A, B, C) is a permutation of the parameters (m, r, U), instead of the basic equation $mP = rS_{ID} + kU$. Note that, not all the permutations generate useful variants considering U as a member of elliptic curve group, and $m, r \in \mathbb{Z}_p$. Hence, A and C should be members of the elliptic curve group, but not B. Also note that mP and rP can be used instead of m and r, respectively. So, by permuting the elements of (m, r, U), Kalkan et al. obtained four ID-based ElGamal signature variants. The signing equation for these variants are:

$$mP = rS_{ID} + kU \tag{5}$$
$$U = rS_{ID} + kmP \tag{6}$$
$$U = mS_{ID} + krP \tag{7}$$
$$rP = mS_{ID} + kU \tag{8}$$

Note that, the two variants where U is a coefficient of S_{ID} do not produce useful signing equations.

In the variants where kP is not needed for verification, r can be computed as $e(P, P)^k$ and the signature for m will be (r, U). For other variants, where kP is needed for verification, r will be computed as $r = H(kP)$ and the signature for m will be (kP, U). Kalkan et al. also proposed computing r as $H(m, kP)$ instead of $H(kP)$ or $e(P, P)^k$. In that case, m does not need to occur in the signing equations.

As in the work of Horster et al. [6], more variants can be produced by using different permutations. Instead of choosing (A, B, C) as a permutation of (m, r, U), one can also choose them as a permutation of $(mr, U, 1)$, $(mr, mU, 1)$ and $(mr, rU, 1)$. Signs of A, B, and C can be changed by

No.	r	U	Signature	Verification
ID I.1	$r = H(kP)$	$U = k^{-1}(mP - rS_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^r = e(P, P)^m$
ID I.2	$r = H(kP)$	$U = k^{-1}(rP - mS_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^m = e(P, P)^r$
ID I.3	$r = e(P, P)^k$	$U = kmP - rS_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^r = r^m$
ID I.4	$r = e(P, P)^k$	$U = rkP - mS_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^m = r^r$
ID I.5	$r = H(m, kP)$	$U = k^{-1}(P - rS_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^r = e(P, P)$
ID I.6	$r = H(m, kP)$	$U = k^{-1}(rP - S_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub}) = e(P, P)^r$
ID I.7	$r = H(m, kP)$	$U = kP - rS_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub})^r = e(P, kP)$
ID I.8	$r = H(m, kP)$	$U = rkP - S_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub}) = e(P, kP)^r$
ID II.1	$r = H(kP)$	$U = k^{-1}(P - mrS_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^{mr} = e(P, P)$
ID II.2	$r = H(kP)$	$U = k^{-1}(-S_{ID} + mrP)$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub}) = e(P, P)^{mr}$
ID II.3	$r = e(P, P)^k$	$U = kP - mrS_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^{mr} = r$
ID II.4	$r = e(P, P)^k$	$U = mrkP - S_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub}) = r^{mr}$
ID III.1	$r = H(kP)$	$U = k^{-1}(m^{-1}P - rS_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^r = e(P, P)^{m^{-1}}$
ID III.2	$r = H(kP)$	$U = k^{-1}(rP - m^{-1}S_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^{m^{-1}} = e(P, P)^r$
ID III.3	$r = e(P, P)^k$	$U = m^{-1}kP - rS_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^r = r^{m^{-1}}$
ID III.4	$r = e(P, P)^k$	$U = rkP - m^{-1}S_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^{m^{-1}} = r^r$
ID IV.1	$r = H(kP)$	$U = k^{-1}(mP - r^{-1}S_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^{r^{-1}} = e(P, P)^m$
ID IV.2	$r = H(kP)$	$U = k^{-1}(r^{-1}P - mS_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^m = e(P, P)^{r^{-1}}$
ID IV.3	$r = e(P, P)^k$	$U = mkP - r^{-1}S_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^{r^{-1}} = r^m$
ID IV.4	$r = e(P, P)^k$	$U = r^{-1}kP - mS_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^m = r^{r^{-1}}$
ID IV.5	$r = H(m, kP)$	$U = k^{-1}(P - r^{-1}S_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^{r^{-1}} = e(P, P)$
ID IV.6	$r = H(m, kP)$	$U = k^{-1}(r^{-1}P - S_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub}) = e(P, P)^{r^{-1}}$
ID IV.7	$r = H(m, kP)$	$U = kP - r^{-1}S_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub})^{r^{-1}} = e(P, kP)$
ID IV.8	$r = H(m, kP)$	$U = r^{-1}kP - S_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub}) = e(P, kP)^{r^{-1}}$
ID V.1	$r = H(kP)$	$U = k^{-1}r^{-1}(mP - S_{ID})$	(kP, U)	$e(U, kP)^r e(Q_{ID}, P_{pub}) = e(P, P)^m$
ID V.2	$r = H(kP)$	$U = k^{-1}r^{-1}(P - mS_{ID})$	(kP, U)	$e(U, kP)^r e(Q_{ID}, P_{pub})^m = e(P, P)$
ID V.3	$r = H(m, kP)$	$U = k^{-1}r^{-1}(P - S_{ID})$	(kP, U)	$e(U, kP)^r e(Q_{ID}, P_{pub}) = e(P, P)$
ID VI.1	$r = H(kQ_{ID})$	$U = (r + km)S_{ID}$	(kQ_{ID}, U)	$e(U, P) = e((r + km)Q_{ID}, P_{pub})$
ID VI.2	$r = H(kQ_{ID})$	$U = (m + kr)S_{ID}$	(kQ_{ID}, U)	$e(U, P) = e((kr + m)Q_{ID}, P_{pub})$
ID VI.3	$r = H(kQ_{ID})$	$U = (rm + k)S_{ID}$	(kQ_{ID}, U)	$e(U, P) = e((rm + k)Q_{ID}, P_{pub})$
ID VI.4	$r = H(kQ_{ID})$	$U = (1 + kmr)S_{ID}$	(kQ_{ID}, U)	$e(U, P) = e((1 + mkr)Q_{ID}, P_{pub})$
ID VI.5	$r = H(kQ_{ID})$	$U = r^{-1}(m + k)S_{ID}$	(kQ_{ID}, U)	$e(U, P)^r = e((m + k)Q_{ID}, P_{pub})$
ID VI.6	$r = H(kQ_{ID})$	$U = r^{-1}(1 + km)S_{ID}$	(kQ_{ID}, U)	$e(U, P)^r = e((mk + 1)Q_{ID}, P_{pub})$
ID VI.7	$r = H(m, kQ_{ID})$	$U = (r + k)S_{ID}$	(kQ_{ID}, U)	$e(U, P) = e((r + k)Q_{ID}, P_{pub})$
ID VI.8	$r = H(m, kQ_{ID})$	$U = r^{-1}(1 + k)S_{ID}$	(kQ_{ID}, U)	$e(U, P)^r = e((1 + k)Q_{ID}, P_{pub})$

TABLE I
THE GENERALIZED ID-BASED ELGAMAL SIGNATURES AND THEIR VERIFICATION EQUATIONS.

multiplying them by ± 1. To obtain more variants, a general function $f(m, r)$ can be used instead of just the product mr. The verification equations and other details for all signatures proposed in [8] are summarized in Table I. Group I lists the variants that are obtained by permuting (m, r, U) and $(1, r, U)$. Group II lists the variants that are obtained by permuting $(mr, U, 1)$. Group III lists the variants that are obtained by permuting $(mr, mU, 1)$. Group IV lists the variants that are obtained by permuting $(mr, rU, 1)$ and $(r, rU, 1)$. Group V shows the rU variants, and finally, group VI shows the variants those were not possible on the basic ElGamal signatures. We refer the reader to [8] for more information about the generalization of the ID-based ElGamal signature schemes.

IV. INSECURE VARIANTS

We found that some of the schemes in Table III are insecure. Their insecurity results mainly from two reasons:

- There are variants where all the terms in the signing equation are public except S_{ID}; hence, the private key S_{ID} can be extracted from the message-signature pair. Variants ID I.7, ID I.8, ID IV.7, and ID IV.8 have this kind of weakness.
- In some variants, r can be removed from the signature equation, which means that either the signature does not depend on the message or k can be modified according to a new message m'. Hence, one can forge a valid signature on a different message without knowing S_{ID}. Variants ID V.3, ID VI.5, ID VI.6, and ID VI.8 have this weakness.

Below, we describe our attacks in detail:

A. Variant ID I.7

The signature σ on a message m is computed as

$$r = H(m, kP)$$
$$U = kP - rS_{ID}$$
$$\sigma = (kP, U).$$

Seeing a message-signature pair (m, σ), an adversary can find S_{ID} by computing

$$r = H(m, kP)$$
$$S_{ID} = r^{-1}(kP - U).$$

B. Variant ID I.8

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(m, kP) \\ U &= rkP - S_{ID} \\ \sigma &= (kP, U). \end{aligned}$$

Seeing a message-signature pair (m, σ), an adversary can find S_{ID} by computing

$$\begin{aligned} r &= H(m, kP) \\ S_{ID} &= rkP - U. \end{aligned}$$

C. Variant ID IV.7

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(m, kP) \\ U &= kP - r^{-1}S_{ID} \\ \sigma &= (kP, U). \end{aligned}$$

Seeing a message-signature pair (m, σ), an adversary can find S_{ID} by computing

$$\begin{aligned} r &= H(m, kP) \\ S_{ID} &= r(kP - U). \end{aligned}$$

D. Variant ID IV.8

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(m, kP) \\ U &= r^{-1}kP - S_{ID} \\ \sigma &= (kP, U). \end{aligned}$$

Seeing a message-signature pair (m, σ), an adversary can find S_{ID} by computing

$$\begin{aligned} r &= H(m, kP) \\ S_{ID} &= r^{-1}kP - U. \end{aligned}$$

E. Variant ID V.3

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(m, kP) \\ U &= k^{-1}r^{-1}(P - S_{ID}) \\ \sigma &= (kP, U). \end{aligned}$$

Seeing a message-signature pair (m, σ), an adversary can forge a signature $\sigma' = (k'P, U')$ on a new message m' by first choosing a random $t \in_R \mathbb{Z}_q$. Then he can compute a valid $k'P$ an U' as follows:

$$\begin{aligned} k'P &= tkP \\ r' &= H(m', k'P) \\ U' &= t^{-1}r'^{-1}rU. \end{aligned}$$

Note that $U' = k'^{-1}r'^{-1}(P - S_{ID})$ hence, $\sigma' = (k'P, U')$ is a valid signature.

F. Variant ID VI.5

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(kQ_{ID}) \\ U &= r^{-1}(m + k)S_{ID} \\ \sigma &= (kQ_{ID}, U). \end{aligned}$$

Seeing a message-signature pair (m, σ), an adversary can forge a signature $\sigma' = (k'Q_{ID}, U')$ on a new message m' as follows:

$$\begin{aligned} k'Q_{ID} &= (m - m')Q_{ID} + kQ_{ID} \\ r' &= H(k'Q_{ID}) \\ U' &= r'^{-1}rU. \end{aligned}$$

Note that $U' = r'^{-1}(m' + k')S_{ID}$ hence, $\sigma' = (k'Q_{ID}, U')$ is a valid signature.

G. Variant ID VI.6

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(kQ_{ID}) \\ U &= r^{-1}(1 + km)S_{ID} \\ \sigma &= (kQ_{ID}, U). \end{aligned}$$

Seeing a message-signature pair (m, σ), an adversary can forge a signature $\sigma' = (k'Q_{ID}, U')$ on a new message m' as follows:

$$\begin{aligned} k'Q_{ID} &= mm'^{-1}kQ_{ID} \\ r' &= H(k'Q_{ID}) \\ U' &= r'^{-1}rU. \end{aligned}$$

Note that $U' = r'^{-1}(1 + k'm')S_{ID}$ hence, $\sigma' = (k'Q_{ID}, U')$ is a valid signature.

H. Variant ID VI.8

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(kQ_{ID}) \\ U &= r^{-1}(1 + k)S_{ID} \\ \sigma &= (kQ_{ID}, U). \end{aligned}$$

Seeing a message-signature pair (m, σ), an adversary can forge a signature $\sigma' = (kQ_{ID}, U')$ on a new message m' as follows:

$$\begin{aligned} r' &= H(k'Q_{ID}) \\ U' &= r'^{-1}rU. \end{aligned}$$

Note that $U' = r'^{-1}(1 + k)S_{ID}$ hence, $\sigma' = (kQ_{ID}, U')$ is a valid signature.

No.	r	U	Signature	Verification
ID I.7v2	$r = H(m, kP)$	$U = kP_{pub} - rS_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub})^r = e(P_{pub}, kP)$
ID I.8v2	$r = H(m, kP)$	$U = rkP_{pub} - S_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub}) = e(P_{pub}, kP)^r$
ID IV.7v2	$r = H(m, kP)$	$U = kP_{pub} - r^{-1}S_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub})^{r^{-1}} = e(P_{pub}, kP)$
ID IV.8v2	$r = H(m, kP)$	$U = r^{-1}kP_{pub} - S_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub}) = e(P_{pub}, kP)^{r^{-1}}$

TABLE II
THE MODIFIED SIGNATURE AND VERIFICATION EQUATIONS OF SOME INSECURE VARIANTS.

V. FIXING THE VARIANTS

As mentioned in Section IV, the first type of attack can be mounted since all terms in the signing equation are public except S_{ID}. Hence, seeing a message-signature pair, one can obtain the S_{ID}. To avoid this flaw, instead of P, we used P_{pub} in the signing equation for the variants ID I.7, ID I.8, ID IV.7 and ID IV.8. Note that even P_{pub} is public, kP_{pub} is secret since k is only known by the signer. The modified equations for these variants are given in Table II.

The variant ID I.7v2 is the same as the ID-Based ElGamal signature scheme of Yi [12]. Yi proved that the scheme is secure if the Diffie-Hellman problem is hard. The attacks proposed in this paper do not apply to the modified variants ID I.8v2, ID IV.7v2, and ID IV.8v2.

For other insecure variants, ID V.3, ID VI.5, ID VI.6 and ID VI.8, the main problem is that r can be eliminated from the signature equation with a single multiplication operation. We can change the signature equations by multiplying r^{-1} with only one term in the signature equation. For example, for variant ID V.3, the signature equation

$$U = k^{-1}r^{-1}(P - S_{ID})$$

can be modified as

$$U = k^{-1}(r^{-1}P - S_{ID})$$

or

$$U = k^{-1}(P - r^{-1}S_{ID}).$$

Although this modification prevents the attack to be mounted, the new variants are same as the variants ID IV.6 and ID IV.5, respectively. The same modification also generates the existing variants in the table for the remaining insecure variants ID VI.5, ID VI.6, and ID VI.8.

VI. CONCLUSION

In this paper, we revisited the generalized ID-based ElGamal signature schemes of Kalkan et al. [8] and showed that some of the proposed variants are insecure. We exploited the security flaws by proposing simple yet effective attacks in which an adversary can either obtain the private key of the signer or forge a signature on a message he desires. We then proposed some modifications to patch these variants. As this work shows, security proofs are necessary for the variants obtained in the generalization process of the ID-based signature schemes. For future work, we will try to prove the security of the remaining and the modified variants by using formal tools such as random oracles and zero-knowledge techniques.

REFERENCES

[1] P. S. L. M. Barreto, B. Libert, N.McCullagh, and J. Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In *Proc. of ASIACRYPT'05*, volume 3778 of *LNCS*, pages 515–532, 2005.

[2] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In *Proc. of CRYPTO'01*, volume 2139 of *LNCS*, pages 213–229. Springer-Verlag, 2001.

[3] J. Cha and J.H. Cheon. An identity-based signature from gap Diffie-Hellman group. In *Proc. of PKC 2003*, volume 2567 of *LNCS*, pages 18–30. Springer-Verlag, 2003.

[4] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Information Theory*, 31(4):469–472, 1985.

[5] F. Hess. Efficient identity based signature schemes based on pairings. In *Proc. of SAC'02*, volume 2595 of *LNCS*, pages 310–324. Springer-Verlag, 2003.

[6] P. Horster, H. Petersen, and M. Michels. Meta-elgamal signature schemes. In *Proc. of ACM Conference on Computer and Communications Security*, pages 96–107, 1994.

[7] A. Joux. A one round protocol for tripartite diffie-hellman. In *Proc. of ANTS-IV*, volume 1838 of *LNCS*, pages 385–394, 2000.

[8] S. Kalkan, K. Kaya, and A. A. Selçuk. Generalized ID-based ElGamal signatures. In *Proc. of ISCIS 2007*, pages 1–6, 2007.

[9] K. Paterson. ID-based signatures from pairings on elliptic curves. Cryptology ePrint Archive, Report. http://eprint.iacr.org/2002/004.

[10] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In *Proc. of SCIS'00*, 2003.

[11] A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. of CRYPTO'84*, volume 196 of *LNCS*, pages 47–53. Springer-Verlag, 1984.

[12] X. Yi. An identity based signature scheme from the Weil pairing. *IEEE Communication Letters*, 7(2):76–78, 2003.