From Digital Signature to ID-Based Identification/Signature

Kaoru Kurosawa[1] and Swee-Huay Heng[2]

[1] Department of Computer and Information Sciences, Ibaraki University,
4-12-1 Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan
kurosawa@cis.ibaraki.ac.jp

[2] Department of Communications and Integrated Systems, Tokyo Institute of Technology,
2-12-1 O-okayama, Meguro-ku, Tokyo 152-8552, Japan
shheng@crypt.ss.titech.ac.jp

Abstract. In this paper, we first formalize the concept of ID-based identification scheme. Secondly, we show a transformation from any digital signature scheme satisfying certain condition to an ID-based identification scheme. As an instance, we present the first provably secure ID-based identification scheme based on the hardness of discrete logarithm problem. (More precisely, the hardness of gap Diffie-Hellman (GDH) problem.) We further show that for the ID-based signature scheme which is obtained by the Fiat-Shamir heuristic, a tight security bound is easily derived due to our transformation.

Key words: ID-based cryptography, signature scheme, identification scheme, GDH group

1 Introduction

1.1 On ID-Based

In the last few years, research on identity (ID)-based *encryption* schemes [4, 8, 5] and *signature* schemes [18, 16, 13, 7] have been very active. In an ID-based scheme, the identity of each user is used as his public key string. Most of the schemes employed bilinear pairings in their constructions, motivated by the novel work of Boneh and Franklin [4].

On the other hand, an *identification* scheme enables prover holding a secret key to identify himself to a verifier holding the corresponding public key. Fiat and Shamir mentioned in the fundamental paper of identification scheme [11] that their scheme is ID-based. Since then, there have been a large number of practical identification protocols in the literature, to name a few [11, 10, 12, 17, 15]. However, to the best of our knowledge, there is no rigorous definition as well as security proof for "ID-based" identification schemes in the open literature.

1.2 On Equivalences, Relationships and Dualities

Many current research focus on drawing equivalences, relationships and dualities between different primitives, and these discoveries lead to new understanding and novel constructions of the related primitives.

For example, we have the paper on "From identification to signatures via Fiat-Shamir transform" by Abdalla et al. [1], where the idea was initially presented by Fiat and Shamir in 1986 [11]. In [14], Kiayias and Yung introduced new design methodologies for group signatures that convert a traitor tracing scheme into a group signature scheme.

1.3 Our Contribution

In this paper, we first formalize the concept of ID-based identification scheme. The main differences of ID-based identification schemes from the usual identification schemes are that: (1) The adversary can choose a target identity ID of her choice to impersonate as opposed to a random public key; (2) The adversary can possess private keys of some users which she has chosen.

Note that Schnorr's identification scheme [17] is not ID-based because each user must publicize his public key. (In other words, he cannot use his identity as his public key string.) In Guillou and Quisquater (GQ) identification scheme [12], each user can use his identity as his public key string. However, we cannot prove the security as mentioned above. Hence it is not ID-based, either.

Secondly, we show a transformation from a digital signature scheme (DS) to an ID-based identification scheme, where we require that the signature scheme has a three-move honest verifier zero-knowledge proof on knowledge. We then prove that the resulting ID-based identification scheme is secure against impersonation under passive attacks if the underlying signature scheme is secure against existentially forgery on adaptive chosen message attacks. An ID-based identification scheme can be further transformed to an ID-based signature scheme, following the Fiat-Shamir transform paradigm [11, 1]. That is,

$$\text{DS scheme} \rightarrow \text{ID-based identification scheme} \rightarrow \text{ID-based DS scheme.}$$

Tight security bounds are directly obtained by our transformation both for the ID-based identification scheme and the ID-based signature scheme if tight security proof is known for the underlying signature scheme.

As an instance, we present the first provably secure ID-based identification scheme based on the hardness of discrete logarithm problem. More precisely, it is based on the hardness of GDH problem. Our scheme uses Boneh et al.'s short signature scheme as a building block where the security is based on the GDH groups [6]. Similarly to Schnorr's (non ID-based) identification scheme, our scheme allows precomputation, reducing the real time computation of the prover to just one multiplication. It is thus particularly suitable for provers with limited computational ability.

We can further obtain an ID-based signature scheme from the ID-based identification scheme. The resulting signature scheme coincides with Cha and

Cheon's scheme [7]. However, we provide a tighter security bound due to our transformation: GDH signature scheme $\rightarrow$ ID-based identification scheme $\rightarrow$ ID-based signature scheme. This in turn improves the efficiency of the scheme since smaller modulus can be used for the same level of security.

We also prove that the proposed ID-based identification scheme is secure against active attacks under the one-more DH assumption, where the one-more DH assumption is a natural analogue of the one-more RSA inversion assumption introduced in [2].

Finally, we point out that we can easily obtain GQ type ID-based identification/signature schemes by combining the Full Domain Hash RSA (FDH-RSA) signature scheme with our transformation. By using the result of Coron [9], tight security bound is further obtained.

1.4 Organization

The rest of the paper is organized as follows. Section 2.1 recalls the formal definition of digital signature schemes. We give the definition of GDH groups, following with the GDH signature scheme proposed by Boneh et al. [6] in Section 2.2. We present the formal model and the security definition of ID-based identification schemes in Section 3. Next, we show how to transform a digital signature scheme to an ID-based identification scheme in Section 4. A security analysis of the transformation follows in Section 4.3. Subsequently, in Section 5 we present our proposed ID-based identification scheme and show that it is secure against impersonation under passive attacks. In Section 6 we present a tight security reduction of the ID-based signature scheme based on the GDH groups. In Section 7 we prove that the proposed ID-based identification scheme is also secure against active attacks under the one-more DH assumption. In Section 8 we briefly discuss the applicability of our proposed transformation method to GQ schemes. We conclude the paper in Section 9.

2 Digital Signature Scheme

2.1 Definition

The standard definition of digital signature schemes is decribed as follows.

Definition 1. *A digital signature scheme $\mathcal{DS}$ is denoted by a triple* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ *of polynomial-time algorithms, called key generation algorithm, signing algorithm and verification algorithm, respectively. The first two algorithms are probabilistic.*

- **Key Generation.** *On input 1^k (throughout this paper, k denotes the security parameter), the algorithm produces a pair of matching public and secret keys (pk, sk).*
- **Signing.** *On input (sk, m), the algorithm returns a signature $\sigma = \mathsf{Sign}_{sk}(m)$, where m is a message.*

– **Verification.** *On input* (pk, m, σ)*, the algorithm returns* 1 *(accept) or* 0 *(reject). We require that* $\mathsf{Verify}_{pk}(m, \sigma) = 1$ *for all* $\sigma \leftarrow \mathsf{Sign}_{sk}(m)$*.*

Security. We consider signature schemes that are secure against existential forgery under adaptive chosen message attacks. A forger F takes as input a public key pk, where $(pk, sk) \leftarrow \mathsf{Gen}(1^k)$, and tries to forge signatures with respect to pk. The forger is allowed to query messages adaptively to the signing oracle to obtain the corresponding signatures. A valid forgery is a message-signature pair (m, σ) such that $\mathsf{Verify}_{pk}(m, \sigma) = 1$ but m has never been queried by F.

Definition 2. *We say that a digital signature scheme* $\mathcal{DS}$ *is* (t, q_S, ϵ)*-secure against existential forgery on adaptive chosen message attacks if for any forger* F *who runs in time* t*,*

$$\Pr(F \textit{ can output a valid forgery}) < \epsilon,$$

where F *can make at most* q_S *signing queries.*

In the random oracle model, we consider a hash function H as a random oracle. Definition 2 is naturally generalized to the random oracle model: We say that a digital signature scheme $\mathcal{DS}$ is (t, q_S, q_H, ϵ)-secure if the condition of Definition 2 is satisfied, where F can make at most q_H random oracle queries.

2.2 GDH Signature Scheme

Boneh et al. proposed a signature scheme based on the GDH groups [6]. Let G be a (additive) cyclic group G generated by P with prime order q.

Computational Diffie-Hellman (CDH) Problem. Given (P, aP, bP) for some $a, b \in Z_q^*$, compute abP.
Decisional Diffie-Hellman (DDH) Problem. Given (P, aP, bP, cP) for some $a, b, c \in Z_q^*$, decide whether $c \equiv ab \bmod q$. (We say that (P, aP, bP, cP) is a DH-tuple if $c \equiv ab \bmod q$.)

We say that G is a GDH group if the CDH problem is hard, but the DDH problem is easy.

Key Generation. On input 1^k, generate an additive group G with prime order q where q is k-bit long. Choose an arbitrary generator $P \in G$. Pick a random $s \in Z_q^*$ and set $Q = sP$. Choose a cryptographic hash function $H : \{0,1\}^* \to G$. The public key is (P, Q, H) and the secret key is s.
Signing. Given the secret key s, a message $m \in \{0,1\}^*$, compute the signature $\sigma = sH(m)$.
Verification. Given the public key (P, Q, H), a message m and a signature σ, compute $H(m)$ and verify that $(P, Q, H(m), \sigma)$ is a valid DH-tuple.

GDH groups are defined formally as follows [6].

Definition 3. G *is a* τ*-decision group for Diffie-Hellman if the DDH problem can be computed in time at most* τ*, where* $P + Q$ *is computed in one time unit.*

Definition 4. *The advantage of an algorithm A in solving the CDH problem in group G is*

$$\mathsf{AdvCDH}_A \stackrel{def}{=} \Pr[A(P, aP, bP) = abP : a, b \stackrel{R}{\leftarrow} Z_q^*]$$

where the probability is over the choice of a and b, and the coin tosses of A. We say that an algorithm A (t, ϵ)-breaks CDH in G if A runs in time at most t, and $\mathsf{AdvCDH}_A \geq \epsilon$.

Definition 5. *A prime order group G is a (τ, t, ϵ)-GDH group if it is a τ-decision group for Diffie-Hellman and no algorithm (t, ϵ)-breaks CDH on it.*

The security of the scheme is derived as follows.

Proposition 1. *[6, Theorem, page 517] If G is a (τ, t', ϵ')-GDH group of order q, then the above GDH signature scheme is (t, q_S, q_H, ϵ)-secure against existentially forgery on adaptive chosen-message attacks, where*

$$t \geq t' - 2c_A \log_2 q(q_H + q_S),$$
$$\epsilon \leq 2eq_S\epsilon'$$

and c_A is a small constant. Here e is the base of the natural logarithm.

3 ID-Based Identification Scheme

In this section, we give a formal definition of ID-based identification schemes.

3.1 Model

An ID-based identification scheme $\mathcal{ID} = (\mathcal{S}, \mathcal{E}, \mathcal{P}, \mathcal{V})$ is specified by four probabilistic polynomial-time (PPT) algorithms, called setup algorithm, extract algorithm, proving algorithm and verification algorithm, respectively. $\mathcal{P}$ and $\mathcal{V}$ are interactive algorithms that implement the prover and verifier, respectively. Alternatively we call $(\mathcal{P}, \mathcal{V})$ an identification protocol.

- **Setup.** A probabilistic algorithm used by the private key generator (PKG) to set up all the parameters of the scheme. $\mathcal{S}$ takes as input 1^k and generates the global system parameters params and the $\mathsf{master\text{-}key}$. The system parameters will be publicly known while the $\mathsf{master\text{-}key}$ will be known to the PKG only.
- **Extract.** A probabilistic algorithm used by the PKG to extract a private key corresponding to a given public identity. $\mathcal{E}$ receives as input the $\mathsf{master\text{-}key}$ and a public identity ID, it returns the corresponding private key d.
- **Identification Protocol.** $\mathcal{P}$ receives as input $(\mathsf{params}, \mathsf{ID}, d)$ and $\mathcal{V}$ receives as input $(\mathsf{params}, \mathsf{ID})$, where d is the private key corresponding to the public identity ID. After an interactive execution of $(\mathcal{P}, \mathcal{V})$, $\mathcal{V}$ outputs a boolean decision 1 (accept) or 0 (reject). A legitimate $\mathcal{P}$ should always be accepted.

Specifically, we consider the following ID-based identification scheme having three-move protocol which is commonly called *canonical*.

1. $\mathcal{P}$ sends a *commitment* $\textsc{Cmt}$ to $\mathcal{V}$.
2. $\mathcal{V}$ returns a *challenge* $\textsc{Ch}$ which is randomly chosen from some set.
3. $\mathcal{P}$ provides a *response* $\textsc{Rsp}$.
4. On input (params,ID,$\textsc{Cmt}$,$\textsc{Ch}$,$\textsc{Rsp}$), $\mathcal{V}$ accepts or rejects.

3.2 Security

The security of ID-based identification schemes is almost the same as the security of standard identification schemes. However, it must be strengthened a bit as follows: (1) The adversary can choose a public identity ID of her choice to impersonate as opposed to a random public key; (2) When an adversary attacks a public identity ID, she might already possess the private keys of some users $\mathsf{ID}_1, \mathsf{ID}_2, \ldots$ of her choice. The system should remain secure under such an attack. Hence, the definition must allow the adversary to obtain the private key associated with any identity ID_i of her choice (other than the public identity ID being attacked).

The adversary goal is impersonation: an adversary succeeds if it interacts with the verifier in the role of a prover with public identity ID and can convince the verifier to accept with non-negligible probability.

There are two type of attacks on the honest, private key equipped prover, namely passive attacks and active attacks. These attacks should take place and complete before the impersonation attempt. In the passive attacks, the adversary does not interact with the prover. What the adversary does is eavesdropping and she is in possession of transcripts of conversations between the prover and the verifier. In the active attacks, the adversary gets to play the role of a cheating verifier, interacting with the prover several times, in an effort to extract some useful information before the impersonation attempt.

We describe the two-phase game between a passive (active) impersonator I and the challenger C. In Phase 1, the impersonator is allowed to make some extract queries. In addition, it can also make either some transcript queries (for passive attacks) or request to act as a cheating verifier (for active attacks). In Phase 2, I starts its impersonation attempt, plays the role as a cheating prover of a public identity ID of its choice, trying to convince the verifier.

- **Setup.** The challenger takes as input 1^k and runs the setup algorithm $\mathcal{S}$. It gives I the resulting system parameters params and keeps the $\mathsf{master\text{-}key}$ to itself.
- **Phase 1.**
  1. I issues some extract queries $\mathsf{ID}_1, \mathsf{ID}_2, \ldots$. The challenger responds by running the extract algorithm $\mathcal{E}$ to generate the private key d_i corresponding to the public identity ID_i. It returns d_i to I. These queries may be asked adaptively.
  2. I issues some transcript queries (for passive attacks) on ID_i or requests to act as a cheating verifier corresponding to some ID_i (for active attacks).

3. The queries on step 1 and step 2 above can be interleaved.

– **Phase 2.** I outputs a challenge identity ID on which it wishes to impersonate whereby I can act as a cheating prover now, trying to convince the verifier.

Definition 6. *We say that an ID-based identification scheme $\mathcal{ID}$ is (t, q_I, ϵ)-secure under passive (active) attacks if for any passive (active) impersonator I who runs in time t,*

$$\Pr(I \textit{ can impersonate}) < \epsilon,$$

where I can make at most q_I extract queries.

4 Transformation from $\mathcal{DS}$ to $\mathcal{ID}$

In this section, we show a transformation of a digital signature scheme $\mathcal{DS}$ to an ID-based identification scheme $\mathcal{ID}$. First, we state the requirement that a digital signature scheme $\mathcal{DS}$ must fulfill. Next, we present the transformation following by the security analysis.

4.1 Requirement for $\mathcal{DS}$

We require that a digital signature scheme $\mathcal{DS}$ has a canonical (three-move) zero-knowledge interactive proof system (ZKIP) on knowledge of signatures as follows.

Let pk be a public key, m be a message and σ be a signature on m. The common input to (P, V) is (pk, m). The secret input to P is σ. Let $view$ =(CMT,CH,RSP) be a transcript of the conversation between (P, V). Let $View$ be the random variable induced by $view$. We say that (CMT,CH,RSP) is acceptable if V accepts it.

Definition 7. *We say that a digital signature scheme $\mathcal{DS}$ has a Δ-challenge zero-knowledge (ZK) protocol if there exists a canonical protocol (P, V) as follows. For any (pk, m),*

Completeness. *If P knows σ, then* $\Pr(V \textit{ accepts}) = 1$.

Soundness.
- *The number of possible challenge* CH *is equal to Δ.*
- *σ is computed efficiently from any two acceptable transcripts* (CMT,CH_1,RSP_1) *and* (CMT,CH_2,RSP_2) *such that* $\mathrm{CH}_1 \neq \mathrm{CH}_2$.

Zero-knowledgeness. *(P, V) is perfectly ZK for the honest verifier. That is, there exists a simulator S such that its output follows the same probability distribution as $View$.*

4.2 Transformation

Any digital signature scheme $\mathcal{DS} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ satisfying the above requirement can be used as a building block to implement a canonical ID-based identification scheme $\mathcal{ID} = (\mathcal{S}, \mathcal{E}, \mathcal{P}, \mathcal{V})$.

Firstly, we point out the similarities between $\mathcal{DS}$ and $\mathcal{ID}$ and make a comparison between the algorithms associated with them. The setup algorithm $\mathcal{S}$ performs similar operations as the key generation algorithm Gen. Indeed, both of them take as input 1^k and generate:

– params or pk, respectively the system parameters or public key.
– master-key or sk, that will be used by the PKG in the extract algorithm or as a signing key by the user.

Thus, we can view that $\mathsf{params} = pk$ and $\mathsf{master\text{-}key} = sk$.

The extract algorithm $\mathcal{E}$ is similar to the signing algorithm Sign. They take ID and m, respectively, as input and produce the corresponding private key d and signature σ, respectively. In other words, we can set that $\mathsf{ID} = m$ and $d = \sigma$.

Now in $\mathcal{ID}$, the prover $\mathcal{P}$ holds a secret key $d = \sigma$ corresponding to his public identity ID. Then $\mathcal{P}$ and $\mathcal{V}$ runs the Δ-challenge ZK protocol of $\mathcal{DS}$. We give the detail description as follows:

Setup. On input 1^k, $\mathcal{S}$ generates $\mathsf{params} = pk$ and $\mathsf{master\text{-}key} = sk$ using Gen.
Extract. For a given public identity $\mathsf{ID} = m$, $\mathcal{E}$ uses Sign to generate the corresponding private key $d = \sigma$, by using the $\mathsf{master\text{-}key} = sk$.
Identification Protocol. The prover and verifier perform the Δ-challenge ZK protocol of $\mathcal{DS}$ and obtain the protocol as depicted in Fig. 1.

Prover		Verifier
Input: $d = \sigma$		Input: $(\mathsf{params} = pk, \mathsf{ID} = m)$
	$\xrightarrow{\textsc{Cmt}}$	
	$\xleftarrow{\textsc{Ch}}$	$\textsc{Ch} \xleftarrow{R} \Delta_{set}$
	$\xrightarrow{\textsc{Rsp}}$	$\mathrm{Dec} \leftarrow \mathcal{V}(\mathsf{params}, \mathsf{ID}, \textsc{Cmt}, \textsc{Ch}, \textsc{Rsp})$

Fig. 1. A canonical ID-based identification protocol

4.3 Security Analysis

Theorem 1. *Let $\mathcal{DS} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ be a digital signature scheme which has a Δ-challenge ZK protocol. Let $\mathcal{ID} = (\mathcal{S}, \mathcal{E}, \mathcal{P}, \mathcal{V})$ be the associated canonical ID-based identification scheme as per the transformation shown above. Then $\mathcal{ID}$ is (t, q_I, ϵ)-secure against impersonation under passive attacks if $\mathcal{DS}$ is (t', q_S, ϵ')-secure against existential forgery on adaptive chosen message attacks, where*

$$t \geq (t'/2) - poly(k),\ q_I = q_S,\ \epsilon \leq \sqrt{\epsilon'} + (1/\Delta).$$

Proof. (Sketch) Let I be an impersonator who (t, q_I, ϵ)-breaks the ID-based identification scheme $\mathcal{ID}$. Then we will show that $\mathcal{DS}$ is not (t', q_S, ϵ')-secure. That is, we will present a forger F who (t', q_S, ϵ')-breaks the signature scheme $\mathcal{DS}$.

The forger F receives pk as its input. It then gives pk to the impersonator I. In Phase 1, the impersonator I starts the extract queries. If I issues an extract query

ID_i, then the forger F queries ID_i to its signing oracle. F forwards the answer $d_i = \sigma_i$ of the signing oracle to I. These queries may be asked adaptively. I also issues some transcript queries on ID_i. Since $\mathcal{DS}$ has a Δ-challenge ZK protocol, there exists a simulator S whose output follows the same distribution as $View$. If I issues a request ID_i, F runs the simulator S on input (pk, ID_i). Suppose that S outputs (CMT$_i$,CH$_i$,RSP$_i$). Then F gives it to I.

Some time later, I decides that Phase 1 is over and it outputs a public identity ID on which it wishes to be challenged. I plays the role as the cheating prover, trying to convince the verifier $\mathcal{V}$ that she is the holder of public identity ID. F plays the role as $\mathcal{V}$. Immediately after the first run, F resets the prover I to after the step whereby I has sent the message CMT$_1$. F then runs the protocol again. Let the conversation transcripts for the first run and second run be (CMT,CH, RSP) and (CMT,CH', RSP'), respectively. Based on the Reset Lemma proposed by Bellare and Palacio in [3], we can extract the private key $d = \sigma$ from the two conversation transcripts with probability more than $(\epsilon - 1/\Delta)^2$.

Finally, when the impersonator I outputs σ, the forger F returns the message-signature pair (ID, σ) as its forgery. Thus it is clear that

$$t' \leq 2t + poly(k),\ q_S = q_I,\ \epsilon' \geq (\epsilon - \frac{1}{\Delta})^2.$$

□

5 Proposed ID-Based Identification Scheme

In this section, we show the first provably secure ID-based identification scheme by applying our transformation to the GDH signature scheme.

5.1 q-Challenge ZK Protocol

We first show that the GDH signature scheme as described in Section 2.2 satisfies the requirement in Section 4.1.

Theorem 2. *The GDH signature scheme has a q-challenge ZK protocol.*

Proof. For the GDH signature scheme, we show a three-move canonical protocol (P, V) which satisfies the requirement in Section 4.1.

1. P chooses $r \in Z_q$ randomly and sends $x = rH(m)$ to V.
2. V chooses $c \in Z_q$ randomly and sends c to P.
3. P computes $y = (r + c)\sigma$ and sends y to V.
4. V accepts if and only if $(P, Q, x + cH(m), y)$ is a DH-tuple.

It is clear that the above protocol satisfies the completeness. The soundness is proved as follows. Suppose that (x, c_1, y_1) and (x, c_2, y_2) are two acceptable conversations. Then it holds that

$$x + c_1 H(m) = l_1 P,\ y_1 = l_1 Q$$

$$x + c_2 H(m) = l_2 P,\ y_2 = l_2 Q$$

for some l_1 and l_2. From the above equations, we obtain

$$(c_2 - c_1)H(m) = (l_2 - l_1)P \text{ and } y_2 - y_1 = (l_2 - l_1)Q.$$

This shows that $\sigma = (c_2 - c_1)^{-1}(y_2 - y_1)$ is a signature on m. (Recall that $Q = sP$ and $\sigma = sH(m)$.)

Finally, we show a simulator S. The purpose of S is to output $(\tilde{x}, \tilde{c}, \tilde{y})$ such that $(P, Q, \tilde{x} + \tilde{c}H(m), \tilde{y})$ is a DH-tuple. That is, $(P, Q, \tilde{x} + \tilde{c}H(m), \tilde{y}) = (P, Q, lP, lQ)$ for some l. Hence S chooses $l \in Z_q$ and $\tilde{c} \in Z_q$ randomly. S then outputs $(lP - \tilde{c}H(m), \tilde{c}, lQ)$. Thus we have shown that (P, V) is perfect ZK for the honest verifier. □

5.2 ID-Based Identification Scheme Based on GDH

We can then obtain an ID-based identification scheme immediately from Section 4.2. Let $\mathcal{ID} = (\mathcal{S}, \mathcal{E}, \mathcal{P}, \mathcal{V})$ be four PPT algorithms as follows.

Setup. On input 1^k, generate an additive group G with prime order q. Choose an arbitrary generator $P \in G$. Pick a random $s \in Z_q$ and set $P_{pub} = sP$. Choose a hash function $H : \{0,1\}^* \to G$. Let the system parameters $\mathsf{params} = (P, P_{pub}, H)$ and the $\mathsf{master\text{-}key}$ is s which is known to the PKG only.
Extract. Given a public identity ID, compute the corresponding private key $d_{\mathsf{ID}} = sQ_{\mathsf{ID}}$ where $Q_{\mathsf{ID}} = H(\mathsf{ID})$.
Identification Protocol.

1. $\mathcal{P}$ chooses $r \in Z_q$ randomly, computes $U = rQ_{\mathsf{ID}}$ and sends U to $\mathcal{V}$.
2. $\mathcal{V}$ chooses $c \in Z_q$ randomly and sends c to $\mathcal{P}$.
3. $\mathcal{P}$ computes $V = (r + c)d_{\mathsf{ID}}$ and sends V to $\mathcal{V}$.
4. $\mathcal{V}$ verifies whether $(P, P_{pub}, U + cQ_{\mathsf{ID}}, V)$ is a DH-tuple.

Remark. Note that params is the public key of the GDH signature scheme and s is the secret key. d_{ID} is the signature on a message ID.

5.3 Security Against Passive Attacks

From Theorem 1 and Theorem 2, it is clear that the above ID-based identification scheme is secure against passive attacks if the GDH signature scheme is secure against existential forgery on adaptive chosen message attacks. The latter is indeed the case as shown in Proposition 1. Therefore, the above ID-based identification scheme is secure against passive attacks.

By combining these results quantitatively, we can obtain the concrete security. The security definition is generalized to the random oracle model as follows. We say that an ID-based identification scheme $\mathcal{ID}$ is (t, q_I, q_H, ϵ)-secure under passive (active) attacks if the condition of Definition 6 is satisfied, where the impersonator I can make at most q_H random oracle queries. (We can prove the random oracle version of Theorem 1 easily, where both F and I use the same random oracle H. If I makes a random oracle query, then F makes the same query to H and sends the obtained answer to I.)

Theorem 3. *If G is a (τ, t', ϵ')-GDH group, then the above ID-based identification scheme is (t, q_I, q_H, ϵ)-secure under passive attacks, where*

$$t \geq (t'/2) - c_A \log_2 q(q_H + q_I) - poly(k),$$
$$\epsilon \leq \sqrt{2eq_I\epsilon'} + (1/q),$$

and c_A is a small constant. Here e is the base of the natural logarithm.

6 ID-Based Signature Scheme Based on GDH

We can further transform our proposed ID-based identification scheme to an ID-based signature scheme. This transformation is direct as in other Fiat-Shamir transformations except that it involves ID-based transformation.

The resulting signature scheme coincides with Cha and Cheon's scheme [7]. However, we can give a much tighter security reduction due to our transformation: GDH signature scheme $\rightarrow$ ID-based identification scheme $\rightarrow$ ID-based signature scheme. This in turn improves the efficiency of the scheme since smaller modulus can be used for the same level of security. (In [7], the security proof relies on the forking lemma. Hence the reduction is not tight and the proof is very complicated.)

6.1 Scheme

Setup. On input 1^k, generate an additive group G with prime order q. Choose an arbitrary generator $P \in G$. Pick $s \in Z_q^*$ randomly and set $P_{pub} = sP$. Choose two cryptographic hash functions: $H : \{0,1\}^* \rightarrow G$, $H_1 : \{0,1\}^* \times G \rightarrow Z_q$. Let the system parameters, $\mathsf{params} = (P, P_{pub}, H, H_1)$ and the $\mathsf{master\text{-}key}$ is s which is known to the PKG only.
Extract. Given a public identity ID, compute the corresponding private key $d_{\mathsf{ID}} = sQ_{\mathsf{ID}}$ where $Q_{\mathsf{ID}} = H(\mathsf{ID})$.
Signing. Given the private key d_{ID} and a message m, pick a random number $r \in Z_q$. Return the signature $\sigma = (U, V)$ where $U = rQ_{\mathsf{ID}}, c = H_1(m, U)$ and $V = (r + c)d_{\mathsf{ID}}$.
Verification. Given the system parameters $\mathsf{params} = (P, P_{pub}, H, H_1)$, a message m and a signature $\sigma = (U, V)$ for an identity ID, compute $c = H_1(m, U)$ and verify that $(P, P_{pub}, U + cQ_{\mathsf{ID}}, V)$ is a valid DH-tuple.

6.2 Security

The security definition of ID-based digital signature schemes is given in [7]. We say that an ID-based digital signature scheme is $(t, q_I, q_S, q_H, q_{H_1}, \epsilon)$-secure if for any forger F who runs in time t,

$$\Pr(F \text{ can output a valid forgery}) < \epsilon,$$

where F can make at most q_I extract queries, at most q_S signing queries and at most q_H and q_{H_1} queries to the random oracle H and H_1, respectively.

Then from Theorem 3 and Lemma 1 of [1], we can obtain the following theorem.

Theorem 4. *If G is a (τ, t', ϵ')-GDH group, then the ID-based GDH signature scheme is $(t, q_I, q_S, q_H, q_{H_1}, \epsilon)$-secure, where*

$$t \geq (t'/2) - c_A \log_2 q(q_H + q_I) - poly(k),$$
$$\epsilon \leq \frac{(1 + q_{H_1})(q\sqrt{2eq_I\epsilon'} + 1) + (1 + q_{H_1} + q_S)q_S}{q},$$

and c_A is a small constant. Here e is the base of the natural logarithm.

7 Security Against Active Attacks of the Proposed ID-Based Identification Scheme

In this section, We show that our proposed ID-based identification scheme as described in Section 5.2 is secure against active attacks if the one-more DH problem is hard, where the one-more DH assumption is a natural analogue of the one-more RSA inversion assumption which was first introduced in [2]. The same assumption and the discrete-log related assumption were later used in [3] to prove the security against impersonation under active and concurrent attacks for GQ and Schnorr identification schemes, respectively.

7.1 One-More DH Assumption

We briefly describe the one-more DH adversary. An one-more DH adversary is a randomized, polynomial-time algorithm M that gets input $(P, P_{pub} = sP)$ and has access to two oracles, namely the DH-oracle that given $Q \in G$ returns $sQ \in G$ and a challenge oracle that each time it is invoked (it takes no input), returns a random challenge point $W \in G$.

First, run $M(P, P_{pub})$ with its oracles. Let $W_1, \ldots, W_n$ denote the challenges returned by M's challenge oracle. M can ask at most $n - 1$ DH-oracle queries. We say that M wins if its output is a sequence of points $sW_1, \ldots, sW_n \in G$, meaning M solves the DH problem of all the challenge points. In other words, the one-more DH assumption states that it is computationally infeasible for the adversary to solve the DH problem of all the challenge points if its DH-oracle queries are strictly less than its challenge oracle queries. (When the adversary makes one challenge query and no DH-oracle queries, this is the standard DH assumption.)

We say that the one-more DH problem is (t, ϵ)-hard if $\Pr(M \text{ wins}) < \epsilon$ for any M which runs in time t.

7.2 Security Proof

Theorem 5. *Let H be a random oracle from $\{0,1\}^*$ to G. If the one-more DH problem is (t', ϵ')-hard, then the ID-based identification scheme is (t, q_I, q_H, ϵ)-secure against active attacks, where*

$$t \geq (t'/2) - poly(k),\ \ \epsilon \leq \sqrt{e(1+q_I)\epsilon'} + (1/q).$$

The proof will be given in the full version of the paper.

8 ID-Based Variants of GQ Schemes

GQ identification scheme is not ID-based as mentioned in Section 1.3. However, we can easily obtain an ID-based variant of GQ identification scheme by combining the FDH-RSA signature scheme with our transformation. Further, Coron showed a very tight security proof for the FDH-RSA signature scheme [9]. Hence we can obtain a tight security proof for the ID-based variant of GQ identification scheme directly from Theorem 1. Similarly, we can obtain an ID-based variant of GQ signature scheme. In particular, they are obtained by our transformation: RSA signature $\rightarrow$ ID-based GQ identification scheme $\rightarrow$ ID-based GQ signature. The details will be given in the full version of the paper.

9 Conclusion

We have formalized the concept of ID-based identification scheme. We have also presented a transformation from any digital signature scheme having a Δ-challenge ZK protocol to an ID-based identification scheme. A concrete example is given based on Boneh et al.'s GDH signature scheme. Eventually, by using Fiat-Shamir transformation, we reached at an ID-based signature scheme which is coincided with Cha and Cheon's scheme. However, we can achieve a tighter security reduction due to our transformation.

References

1. M. Abdalla, J. An, M. Bellare and C. Namprempre. From identification to signatures via the Fiat-Shamir transform: minimizing assumptions for security and forward-security. *Advances in Cryptology — EUROCRYPT '02, LNCS 2332,* pp. 418–433, Springer-Verlag, 2002.
2. M. Bellare, C. Namprempre, D. Pointcheval and M. Semanko. The power of RSA inversion oracles and the security of Chaum's RSA-based blind signature scheme. *Financial Cryptography 2001, LNCS 2339,* pp. 319–338, Springer-Verlag, 2002.
3. M. Bellare and A. Palacio. GQ and Schnorr identification schemes: proofs of security against impersonation under attive and concurrent attacks. *Advances in Cryptology — CRYPTO '02, LNCS 2442,* pp. 162–177, Springer-Verlag, 2002.
4. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. *Advances in Cryptology — CRYPTO '01, LNCS 2139,* pp. 213–229, Springer-Verlag, 2001.

5. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. *Siam Journal of Computing, Vol. 32,* pp. 586–615, 2003. Updated version of [4].
6. D. Boneh, B. Lynn and H. Shacham. Short signatures from the the weil pairing. *Advances in Cryptology — ASIACRYPT '01, LNCS 2248,* pp. 514–532, Springer-Verlag, 2001.
7. J. C. Cha and J. H. Cheon. An identity-based signature from gap Diffie-Hellman groups. *Public Key Cryptography — PKC '03, LNCS 2567,* pp. 18–30, Springer-Verlag, 2003.
8. C. Cocks. An identity based encryption scheme based on quadratic residues. *Cryptography and Coding, LNCS 2260,* pp. 360–363, Springer-Verlag, 2001.
9. J. Coron. On the exact security of full domain hash. *Advances in Cryptology — CRYPTO '00, LNCS 1880,* pp. 229–235, Springer-Verlag, 2000.
10. U. Feige, A. Fiat and A. Shamir. Zero-knowledge proofs of identity. *Journal of Cryptology, Vol. 1,* pp. 77–94, Springer-Verlag, 1988.
11. A. Fiat and A. Shamir. How to prove yourself: practical solutions to identification and signature problems. *Advances in Cryptology — CRYPTO '86, LNCS 263,* pp. 186–194, Springer-Verlag, 1987.
12. L. Guillou and J. Quisquater. A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory. *Advances in Cryptology — EUROCRYPT '88, LNCS 330,* pp. 123–128, Springer-Verlag, 1989.
13. F. Hess. Efficient identity based signature schemes based on pairings. *Selected Areas in Cryptography — SAC '02, LNCS 2595,* pp. 310–324, Springer-Verlag, 2002.
14. A. Kiayias and M. Yung. Extracting group signatures from traitor tracing schemes. *Advances in Cryptology — EUROCRYPT '03, LNCS 2656,* pp. 630–648, Springer-Verlag, 2003.
15. T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. *Advances in Cryptology — CRYPTO '92, LNCS 740,* pp. 31–53, Springer-Verlag, 1993.
16. K. G. Paterson. ID-based signatures from pairings on elliptic curves. *Electronic Letters, Vol. 38, No. 18,* pp. 1025–1026, 2002.
17. C. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology, Vol. 4,* pp. 161–174, Springer-Verlag, 1991.
18. R. Sakai, K. Ohgishi and M. Kasahara. Cryptosystems based on pairing. *2000 Symposium on Cryptography and Information Security — SCIS '00,* Okinawa, Japan, Jan. 26–28, 2000.
19. Z.-F. Zhang, J. Xu and D.-G. Feng. Attack on an identification scheme based on gap Diffie-Hellman problem. *IACR Cryptology ePrint Archive, Report 2003/153.* Available from `http://eprint.iacr.org/2003/153/`.