A Computational Diffie–Hellman-Based Insider Secure Signcryption with Non-interactive Non-repudiation

Ngarenon Togde and Augustin P. Sarr

Abstract An important advantage of signcryption schemes compared to one pass key exchange protocols is non-interactive non-repudiation (NINR). This attribute offers to the receiver of a signcrypted ciphertext the ability to generate a non-repudiation evidence, that can be verified by a third party without executing a costly multi-round protocol. We propose a computational Diffie–Hellman based insider secure signcryption scheme with non-interactive non-repudiation. Namely, we show that under the computational Diffie–Hellman assumption and the random oracle model, our scheme is *tightly* insider secure, provided the underlying encryption scheme is semantically secure. Compared to a large majority of the previously proposed signcryption schemes with NINR, our construction is more efficient and it does not use any specificity of the underlying group, such as pairings. The communication overhead of our construction, compared to Chevallier Mâmes' signature scheme is one group element.

Keywords Signcryption · Non-interactive non-repudiation · Insider security · Computational Diffie–Hellman · Random oracle model

1 Introduction

A signcryption scheme provides simultaneously the functionalities of encryption and signature schemes [24]. A natural use of a signcryption scheme is to build an asynchronous secure channel i.e., a confidential and authenticated asynchronous channel. Given the similar uses of signcryption and (one pass) Key Exchange Protocols (KEP), to build confidential and authenticated channels, it appears, from a real world perspective, that the right security definition for signcryption schemes is insider security [3]. Informally, insider security ensures (i) *confidentiality* even if the

N. Togde · A. P. Sarr (✉)
Laboratoire ACCA, UFR SAT, Université Gaston Berger, Saint-Louis, Senegal
e-mail: augustin-pathe.sarr@ugb.edu.sn

N. Togde
e-mail: ngarenon.togde@ugb.edu.sn

B. Rushi Kumar et al. (eds.), *Mathematics and Computing*, Springer Proceedings in Mathematics & Statistics 415, https://doi.org/10.1007/978-981-19-9307-7_8

sender's static private key is revealed to the attacker, and (ii) *unforgeability* even if the receiver's static private key is disclosed.

A signcryption scheme is said to provide *non-repudiation*, if the receiver of a signcrypted ciphertext has the ability to generate a non-repudiation evidence, that can be verified by a third party (a judge, for instance); as a result, a message sender cannot deny having signcrypted the message. The non-repudiation attribute is said to be *non-interactive*, if a non-repudiation evidence can be *generated and verified without executing a multi-round protocol*. An important advantage of signcryption schemes, compared to one pass KEP, which often outperforms signcryption schemes, is non-interactive non-repudiation (NINR).

A signcryption scheme with the aim to provide NINR was proposed for the first time by Bao and Deng [5]; unfortunately their design fails in achieving confidentiality [19]. Malone–Lee [19] proposes an efficient design with NINR he analyzes in the Random Oracle (RO) model. The scheme achieves confidentiality under the computational Diffie–Hellman (cDH) assumption, and unforgeability under the gap Diffie–Hellman Assumption. Unfortunately, the security model he uses is closer to the outsider than to the insider model. Indeed, the scheme fails in providing insider confidentiality. In [8], Bjørstad and Dent (BD) propose a design based on Chevallier Mâmes' (CM) signature scheme they show to tightly achieve insider unforgeability under the cDH assumption and *outsider* confidentiality under the gap DH assumption. Unfortunately, as for the ML scheme, the BD scheme does not achieve insider confidentiality.

In subsequent works [2, 13, 14, 20, 23], several insider secure schemes with NINR have been proposed. The designs offer a superior security, compared to the ML or BD schemes. However, they are less efficient and often assume some specificities of the underlying groups, such as the existence of a bilinear pairing. In [2], Arriaga et al. propose a generic insider secure signcryption scheme, with randomness reuse, in the standard model. They exhibit an insider secure instantiation of their design, under the Decisional Bilinear and the q-Strong Diffie–Hellman (DBDH and q-sDH) assumptions. Unfortunately, the unforgeability is achieved in the registered key model [20], wherein an attacker is required to register the *keys pairs* it uses in its attack. Matsuda et al. [20] propose a generic composition of signature and tag-based encryption schemes, which yields to different shades of security depending on the security attributes of the base schemes. They exhibit two constructions with NINR that fully achieve insider confidentiality (under the cDH and the gap DH assumptions respectively) and unforgeability (under the co-cDH assumption). Chiba et al. [13] propose a generic construction of signcryption schemes, and exhibit two insider secure constructions with NINR under the DBDH and the q-sDH assumptions. In [14], Fan et al. propose a signcryption scheme with non-interactive non-repudiation (SCNINR), based on Boneh et al.'s signature scheme [10], they show to be insider secure under the DBDH assumption, without resorting the RO model. Sarr et al. [23] propose, over the group of signed quadratic residues, a SCNINR, based on a signature scheme of their own design, they show to be insider secure under the RSA assumption and the RO model.

The basic design principle in the SCNINR schemes from [8, 14, 19, 23], is (i) a Diffie–Hellman (DH) secret derivation, using ephemeral keys from the sender and the receiver's static public key, followed by (ii) an encryption using some part of the derived secret, and (iii) a signature generation, using the sender's private key, on the plain text and some part of the derived DH secret. One may notice also that these schemes assume rather specific groups or have loose security reductions. As tightly secure cDH-based signature schemes exist [12, 15, 17], we investigate whether such schemes can be leveraged as building blocks for tightly (multi-user) insider secure cDH based SCNINR schemes. As we aim at an efficient design, we use the random oracle (RO) model. We propose a new SCNINR, termed $\mathcal{SC}_{\mathsf{edl}}$, based on a variant of Chevallier–Mâmes' signature scheme [12], tailored to (i) be combined with Cash et al.'s twin Diffie–Hellman key exchange [11], (ii) and to allow a use of the same randomness in the DH key exchange and in the signature generation.

And, using the trapdoor test technique [11], we show that $\mathcal{SC}_{\mathsf{edl}}$ is tightly insider secure under the cDH assumption and the RO model, provided the underlying symmetric encryption scheme is semantically secure. Even better, we show the insider confidentiality attribute in the *secret key ignorant* multi-user model, i.e., when the sender public key is chosen by the adversary and the challenger does not know the corresponding private key. Compared to the ML and BD schemes, which do not require any specificity of the underlying group and do not achieve insider security, $\mathcal{SC}_{\mathsf{edl}}$ offers a stronger security, even if it is less efficient. And, compared to the schemes from [2, 13, 14, 20, 23], $\mathcal{SC}_{\mathsf{edl}}$ offers a tight security reduction, a better efficiency, and a comparable or a superior security.

This paper is organized as follows. In Sect. 2, we present some preliminaries on the syntax of SCNINR schemes and the insider security definitions for SCNINR. In Sect. 3, we propose the $\mathcal{SC}_{\mathsf{edl}}$ scheme. We propose our security results in Sect. 4, and compare our design with previous constructions in Sect. 5.

2 Preliminaries

Notations. $\mathcal{G} = \langle G \rangle$ is a cyclic group of prime order p, $\mathcal{G}^*$ denotes the set $\mathcal{G} \setminus \{1\}$. We denote by $\mathsf{Exp}(\mathcal{G}, t)$ the computational effort required to perform t exponentiations with $|p|$-bits exponents in $\mathcal{G}$; $\mathsf{Exp}(\mathcal{G})$ denotes $\mathsf{Exp}(\mathcal{G}, 1)$. For an integer n, $[n]$ denotes the set $\{0, \ldots, n\}$. If S is a set, $a \leftarrow_{\mathrm{R}} S$ means that a is chosen uniformly at random from S; we write $a, b, c, \ldots \leftarrow_{\mathrm{R}} S$ as a shorthand for $a \leftarrow_{\mathrm{R}} S$; $b \leftarrow_{\mathrm{R}} S$, etc. We denote by $\mathsf{sz}(S)$ the number of bits required to represent $a \in S$. For a probabilistic algorithm $\mathcal{A}$ with parameters $u_1, \ldots, u_n$ and output $V \in \mathbf{V}$, we write $V \leftarrow_{\mathrm{R}} \mathcal{A}(u_1, \ldots, u_n)$. We denote by $\{\mathcal{A}(u_1, \ldots, u_n)\}$ the set $\{v \in \mathbf{V} : \Pr(V = v) \neq 0\}$. If $x_1, x_2, \ldots, x_k$ are objects belonging to different structures (group, bit-string, etc.) $(x_1, x_2, \ldots, x_k)$ denotes a representation as a bit-string of the tuple such that each element can be unequivocally parsed.

The cDH *Assumption.* We assume the existence of an algorithm $\mathsf{Setup}_{\mathsf{grp}}(\cdot)$, which on input a security parameter k outputs a system parameter Π_k which fully

identifies a group $\mathcal{G} = \langle G \rangle$ together with its order. For $X \in \mathcal{G}$, we denote the smallest non-negative integer x such that $G^x = X$ by $\log_G X$. For, $X, Y \in \mathcal{G}$, we denote $G^{(\log_G X)(\log_G Y)}$ by $\mathsf{cDH}(X, Y)$; if $B \in \mathcal{G}$, we denote $(\mathsf{cDH}(X, B), \mathsf{cDH}(Y, B))$ by $\mathsf{2DH}(X, Y, B)$. The cDH assumption is said to hold in $\mathcal{G}$ if for all efficient algorithms $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{cDH}}_{\mathcal{A}}(\mathcal{G}) = \Pr[X, Y \leftarrow_{\mathrm{R}} \mathcal{G}; Z \leftarrow_{\mathrm{R}} \mathcal{A}(G, X, Y) : Z = \mathsf{cDH}(X, Y)]$ is negligible in k.

A Symmetric Encryption scheme $\mathcal{E} = (\mathsf{E}, \mathsf{D}, \mathbf{K}, \mathbf{M}, \mathbf{C})$ is a pair of efficient algorithms (E, D) together with a triple of sets $(\mathbf{K}, \mathbf{M}, \mathbf{C})$, which depend on the security parameter k, such that for all $\tau \in \mathbf{K}$ and all $m \in \mathbf{M}$, it holds that $\mathsf{E}(\tau, m) \in \mathbf{C}$ and $m = \mathsf{D}(\tau, \mathsf{E}(\tau, m))$. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary against $\mathcal{E}$ and let

$$\Pr(O_{i,i=0,1}) = \Pr\left[\begin{array}{l}(m_0, m_1, st) \leftarrow_{\mathrm{R}} \mathcal{A}_1(k); \tau \leftarrow_{\mathrm{R}} \mathbf{K}; c \leftarrow_{\mathrm{R}} \mathsf{E}(\tau, m_i); \\ \hat{b} \leftarrow_{\mathrm{R}} \mathcal{A}_2(k, c, st)\end{array} : \hat{b} = 1\right];$$

then $\mathsf{Adv}^{\mathsf{ss}}_{\mathcal{A},\mathcal{E}}(k)$ denotes the quantity $\mathsf{Adv}^{\mathsf{ss}}_{\mathcal{A},\mathcal{E}}(k) = |\Pr(O_0) - \Pr(O_1)|$, where m_0, $m_1 \in \mathbf{M}$ are distinct equal length messages. The scheme $\mathcal{E}$ is said to be $(t, \varepsilon(k))$-*semantically secure* if for all adversaries $\mathcal{A}$ running in time t, $\mathsf{Adv}^{\mathsf{ss}}_{\mathcal{A},\mathcal{E}}(k) \leqslant \varepsilon(k)$.

2.1 Insider Security for SCNINR

We recall the syntax of a SCNINR scheme and the insider security definitions in the Flexible Signcryption / Flexible Unsigncryption Oracle (FSO/FUO) model [4], also termed dynamic Multi-user model [2].

Definition 1 A *signcryption scheme* is a quintuple of algorithms $\mathcal{SC} = (\mathsf{Setup}, \mathsf{Gen}_S, \mathsf{Gen}_R, \mathsf{Sc}, \mathsf{Usc})$ where

(a) Setup takes a security parameter k as input, and outputs a public domain parameter dp.
(b) Gen_S is the sender key pair generation algorithm. It takes as input dp (an implicit parameter) and outputs a key pair (sk_S, pk_S), wherein sk_S is the signcrypting key.
(c) Gen_R is the receiver key pair generation algorithm; it takes dp as input and outputs a key pair (sk_R, pk_R).
(d) Sc takes as inputs dp, a sender private key sk_S, a receiver public key pk_R, and a message m, and outputs a signcryptext C. We write $C \leftarrow_{\mathrm{R}} \mathsf{Sc}(sk_S, pk_R, m)$.
(e) Usc is a deterministic algorithm. It takes as inputs dp, a receiver secret key sk_R, a sender public key pk_S, and a signcryptext C, and outputs either a valid message $m \in \mathbf{M}$ or an error symbol $\perp \notin \mathbf{M}$.

And, for all $dp \in \{\mathsf{Setup}(k)\}$, all $m \in \mathbf{M}$, all $(sk_S, pk_S) \in \{\mathsf{Gen}_S(dp)\}$, and all $(sk_R, pk_R) \in \{\mathsf{Gen}_R(dp)\}$, $m = \mathsf{Usc}(sk_R, pk_S, \mathsf{Sc}(sk_S, pk_R, m))$. The scheme is said to provide NINR if there are two algorithms N and PV, termed *non-repudiation evidence generation* and *pubic verification algorithms* such that:

– N takes as inputs a receiver secret key sk_R, a sender public key pk_S, and a signcrypted ciphertext C, and outputs a *non-repudiation evidence* nr or a failure symbol $\perp$; we write $nr \leftarrow \mathsf{N}(sk_R, pk_S, C)$.
– PV takes as inputs a signcryptext C, a message m, a non-repudiation evidence nr, a sender public key pk_S, and a receiver public key pk_R, and outputs $d \in \{0, 1\}$; we write $d \leftarrow \mathsf{PV}(C, m, nr, pk_S, pk_R)$.
– For all $dp \in \{\mathsf{Setup}(k)\}$, all $C \in \{0, 1\}^*$, all $(sk_S, pk_S) \in \{\mathsf{Gen}_S(dp)\}$, and all $(sk_R, pk_R) \in \{\mathsf{Gen}_R(dp)\}$, if $\perp \neq m \leftarrow \mathsf{Usc}(sk_R, pk_S, C)$ and $nr \leftarrow \mathsf{N}(sk_R, pk_S, C)$ then $1 = d \leftarrow \mathsf{PV}(C, m, nr, pk_S, pk_R)$.

Game 1 SKI–MU Insider Confidentiality in the FSO/FUO–IND–CCA2 sense

We consider the experiments E_0 and E_1, described hereunder, wherein $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ is a two–stage adversary against a SCNINR scheme $\mathcal{SC}$;

(1) The challenger generates $dp \leftarrow_{\mathrm{R}} \mathsf{Setup}(k)$ and $(sk_R, pk_R) \leftarrow_{\mathrm{R}} \mathsf{Gen}_R(dp)$;
(2) $\mathcal{A}_1$ is provided with dp and pk_R, and is given access to:
(a) an unsigncryption oracle $\mathcal{O}_{\mathsf{Usc}}(\cdot, \cdot)$, which takes as inputs a public key pk and a signcrypted ciphertext C, and outputs $m \leftarrow \mathsf{Usc}(sk_R, pk, C)$, and (b) a non–repudiation evidence generation oracle $\mathcal{O}_{\mathsf{N}}(\cdot, \cdot)$ which takes as inputs a public key pk and a signcrypted ciphertext C and outputs $nr \leftarrow \mathsf{N}(sk_R, pk, C)$.
(3) $\mathcal{A}_1$ outputs $(m_0, m_1, pk_S, st) \leftarrow_{\mathrm{R}} \mathcal{A}_1^{\mathcal{O}_{\mathsf{Usc}}(\cdot,\cdot), \mathcal{O}_{\mathsf{N}}(\cdot,\cdot)}(pk_R)$ where $m_0, m_1 \in \mathbf{M}$ are distinct equal length messages, st is a state, and pk_S is the attacked sender public key (sk_S is unknown to the challenger).
(4) In the experiment $E_{b,b=0,1}$, the challenger computes $C^* \leftarrow_{\mathrm{R}} \mathsf{Sc}(sk_S, pk_R, m_b)$.
(5) $\mathcal{A}_2$ outputs $b' \leftarrow_{\mathrm{R}} \mathcal{A}_2^{\mathcal{O}_{\mathsf{Usc}}(\cdot,\cdot), \mathcal{O}_{\mathsf{N}}(\cdot,\cdot)}(C^*, st)$ ($\mathcal{O}_{\mathsf{Usc}}(\cdot, \cdot)$ and $\mathcal{O}_{\mathsf{N}}(\cdot, \cdot)$ are as in step 2).
(6) For $E_{b,b=0,1}$, out_b denotes the event: (i) $\mathcal{A}_2$ never issued $\mathcal{O}_{\mathsf{Usc}}(pk_S, C^*)$ or $\mathcal{O}_{\mathsf{N}}(pk_S, C^*)$, and (ii) $b' = 1$.

And, $\mathsf{Adv}^{\mathsf{cca2}}_{\mathcal{A},\mathcal{SC}}(k) = \mid \Pr(\mathsf{out}_0) - \Pr(\mathsf{out}_1) \mid$ denotes $\mathcal{A}$'s CCA2 insider security advantage.

Definition 2 (*Secret Key Ignorant Multi-user Insider Confidentiality*) A SCNINR $\mathcal{SC}$ is said to be $(t, q_{\mathsf{Usc}}, q_{\mathsf{N}}, \varepsilon)$-secure in the Secret Key Ignorant Multi-user (SKI–MU) insider confidentiality in the FSO/FUO IND–CCA2 sense, if for all adversaries $\mathcal{A}$ playing Game 1, running in time t, and issuing respectively q_{Usc} and q_{N} queries to the unsigncryption and non-repudiation evidence generation oracles, $\mathsf{Adv}^{\mathsf{cca2}}_{\mathcal{A},\mathcal{SC}}(k) \leqslant \varepsilon$.

Definition 3 (*Multi-user Strong Insider Unforgeability*) A SCNINR is said to be $(t, q_{\mathsf{Sc}}, \varepsilon)$ *Multi-user Insider Unforgeable in the FSO/FUO–sUF–CMA sense* if for all attackers $\mathcal{A}$ playing Game 2, running in time t, and issuing q_{Sc} queries to the signcryption oracle, $\mathsf{Adv}^{\mathsf{suf}}_{\mathcal{A},\mathcal{SC}}(k) \leqslant \varepsilon$.

Confidentiality and unforgeability are natural security goals for signcryption schemes. The soundness and unforgeability of non-repudiation evidence attributes are specific to SCNINR schemes.

Game 2 MU Insider Unforgeability in the FSO/FUO–sUF–CMA sense

$\mathcal{A}$ is a forger, $dp \leftarrow_R \mathsf{Setup}(k)$ still denotes the public domain parameter.

(1) The challenger computes $(sk_S, pk_S) \leftarrow_R \mathsf{Gen}_S(dp)$.
(2) $\mathcal{A}$ runs with inputs (dp, pk_S) and is given a FSO $\mathcal{O}_{\mathsf{Sc}}(\cdot,\cdot)$, which takes as inputs a valid public receiver key pk and a message m and outputs $C \leftarrow_R \mathsf{Sc}(sk_S, pk, m)$.
(3) $\mathcal{A}$ outputs $((sk_R, pk_R), C^*) \leftarrow_R \mathcal{A}^{\mathcal{O}_{\mathsf{Sc}}(\cdot,\cdot)}(dp, pk_S)$. It succeeds if:
(i) $\perp \neq m \leftarrow \mathsf{Usc}(sk_R, pk_S, C^*)$, and
(ii) it never received C^* from $\mathcal{O}_{\mathsf{Sc}}(\cdot,\cdot)$ on a query on (pk_R, m).

$\mathsf{Adv}^{\mathsf{suf}}_{\mathcal{A},\mathcal{SC}}(k) = \Pr(\mathsf{Succ}^{\mathsf{suf}}_{\mathcal{A}})$ denotes the probability that $\mathcal{A}$ wins the game.

Game 3 Soundness of non–repudiation

(1) The challenger computes $dp \leftarrow_R \mathsf{Setup}(k)$.
(2) $\mathcal{A}$ runs with input dp and outputs $(C^*, pk_S, sk_R, pk_R, m', nr) \leftarrow_R \mathcal{A}(dp)$.
(3) $\mathcal{A}$ wins the game if:
(i) $\perp \neq m \leftarrow \mathsf{Usc}(sk_R, pk_S, C^*)$, and
(ii) $m \neq m'$ and $1 = d \leftarrow \mathsf{PV}(C^*, m', nr, pk_S, pk_R)$.

$\mathsf{Adv}^{\mathsf{snr}}_{\mathcal{A},\mathcal{SC}}(k)$ denotes the probability that $\mathcal{A}$ wins the game.

Definition 4 (*Soundness of non-repudiation*) A SCNINR is said to achieve (t, ε)-*computational soundness of non-repudiation* if for all attackers $\mathcal{A}$ playing Game 3 and running in time t, $\mathsf{Adv}^{\mathsf{snr}}_{\mathcal{A},\mathcal{SC}}(k) \leqslant \varepsilon$.

Game 4 Unforgeability of non–repudiation evidence

$\mathcal{A}$ is an attacker against $\mathcal{SC}$, $dp \leftarrow_R \mathsf{Setup}(k)$ is the domain parameter.

(1) The challenger computes $(sk_S, pk_S) \leftarrow_R \mathsf{Gen}_S(dp)$; $(sk_R, pk_R) \leftarrow_R \mathsf{Gen}_R(dp)$;
(2) $\mathcal{A}$ runs with inputs (dp, pk_S, pk_R), and outputs $(C^*, m^*, nr^*) \leftarrow_R \mathcal{A}^{\mathcal{O}_{\mathsf{Sc}}(\cdot,\cdot),\mathcal{O}_{\mathsf{Usc}}(\cdot,\cdot),\mathcal{O}_{\mathsf{N}}(\cdot,\cdot)}(dp, pk_S, pk_R)$.
(3) $\mathcal{A}$ wins if:
(i) C^* was generated through the $\mathcal{O}_{\mathsf{Sc}}(\cdot,\cdot)$ oracle on inputs (pk_R, m) for some m,
(ii) $1 = d \leftarrow \mathsf{PV}(C^*, m^*, nr^*, pk_S, pk_R)$, and
(iii) nr^* was not generated by the oracle $\mathcal{O}_{\mathsf{N}}(\cdot,\cdot)$ on a query on (pk_S, C^*).

$\mathsf{Adv}^{\mathsf{unr}}_{\mathcal{A},\mathcal{SC}}(k)$ denotes the probability that $\mathcal{A}$ wins the game.

Definition 5 (*Unforgeability of non-repudiation evidence*) A SCNINR is said to achieve $(t, q_{\mathsf{Sc}}, q_{\mathsf{Usc}}, q_{\mathsf{N}}, \varepsilon)$ *unforgeability of non-repudiation evidence* if for all adversaries $\mathcal{A}$ playing Game 4, running in time t, and issuing respectively q_{Sc}, q_{Usc}, and q_{N} queries to the signcryption, unsigncryption, and non-repudiation evidence generation oracles, $\mathsf{Adv}^{\mathsf{unr}}_{\mathcal{A},\mathcal{SC}}(k) \leqslant \varepsilon$.

3 The New Construction

We consider the following variant of Chevallier–Mâmes' (CM) signature scheme [12]; $\mathsf{H}_1 : \{0,1\}^* \to \mathcal{G}, \mathsf{H}_2 : \{0,1\}^* \to \mathbf{K}$, and $\mathsf{H}_3 : \{0,1\}^* \to [p-1]$ are hash functions, aux denotes some auxiliary information.

A Variant of Chevallier–Mâmes' signature scheme

1: $\mathsf{Setup}_{\mathsf{Sign}}(k)$: the setup outputs a description of the group $\mathcal{G}$, a generator G of $\mathcal{G}$, its prime order p, together with descriptions of the hash functions $\mathsf{H}_{i,i=1,2,3}$.
2: $\mathsf{Gen}(dp)$: $sk \leftarrow_{\mathrm{R}} [p-1]$; $pk \leftarrow G^{sk}$; **return** (sk, pk);
3: $\mathsf{Sign}(sk, m)$: $x_1, x_2 \leftarrow_{\mathrm{R}} [p-1]$; $X_1 \leftarrow G^{x_1}$; $X_2 \leftarrow G^{x_2}$; $R \leftarrow \mathsf{H}_1(X_1, X_2)$; $V \leftarrow R^{x_1}$;
4: $W \leftarrow R^{sk}$; $h \leftarrow \mathsf{H}_3(m, X_1, X_2, G, R, V, W, pk, \mathsf{aux})$; $\sigma \leftarrow x_1 + h \cdot sk$; **return** (X_2, W, σ, h);
5: $\mathsf{Vrfy}(pk, (X_2, W, \sigma, h), m)$: $X_1 \leftarrow G^{\sigma} pk^{-h}$; $R \leftarrow \mathsf{H}_1(X_1, X_2)$; $V \leftarrow R^{\sigma} W^{-h}$;
6: **if** $h = \mathsf{H}_3(m, X_1, X_2, G, R, V, W, pk, \mathsf{aux})$ **then return** 1; **else return** 0;

As for CM, in the RO model, the signature generation can be efficiently simulated, and the scheme can be shown to be unforgeable under cDH assumption. An interesting property of this scheme is that when it comes to extend it to a SCNINR, in a simulation of a signcrypted ciphertext generation, we can generate $X_1, X_2 \leftarrow_{\mathrm{R}} \mathcal{G}$ such that for all $(B, Z_1, Z_2) \in \mathcal{G}^3$, using the trapdoor test technique [11], we can efficiently decide whether $\mathsf{2DH}(X_1, X_2, B) = (Z_1, Z_2)$ or not. Then, if $(B_1, B_2) \in \mathcal{G}^2$ is a receiver public key, and a twin Diffie–Hellman key exchange [11] is performed using (X_1, X_2) and (B_1, B_2), we can use a trapdoor test at both the sender and the receiver. Then, as for the signature scheme's unforgeability, we can show the signcryption scheme to be tightly insider secure.

The $\mathcal{SC}_{\mathsf{edl}}$ Scheme

10: $\mathsf{Setup}(k)$: the algorithm defines a group $\mathcal{G} = \langle G \rangle$ of prime order p, together with an encryption scheme $\mathcal{E} = (\mathsf{E}, \mathsf{D}, \mathbf{K}, \mathbf{M}, \mathbf{C})$ and the hash functions $\mathsf{H}_1 : \{0,1\}^* \to \mathcal{G}, \mathsf{H}_2 : \{0,1\}^* \to \mathbf{K}$, and $\mathsf{H}_3 : \{0,1\}^* \to [p-1]$. The domain parameter is $dp = (\mathcal{G}, \mathcal{E}, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3)$. We assume $p \geqslant |\mathbf{K}|$.
11: $\mathsf{Gen}_S(dp)$: $a \leftarrow_{\mathrm{R}} [p-1]$; $(sk_S, pk_S) \leftarrow (a, G^a)$; **return** (sk_S, pk_S);
12: $\mathsf{Gen}_R(dp)$: $b_1, b_2 \leftarrow_{\mathrm{R}} [p-1]$; $(sk_R, pk_R) \leftarrow \big((b_1, b_2), (G^{b_1}, G^{b_2})\big)$; **return** (sk_R, pk_R);
13: $\mathsf{Sc}(sk_S, pk_R, m)$: Parse pk_R as (B_1, B_2); $x_1, x_2 \leftarrow_{\mathrm{R}} [p-1]$; $X_1 \leftarrow G^{x_1}$; $X_2 \leftarrow G^{x_2}$;
14: $R \leftarrow \mathsf{H}_1(X_1, X_2)$; $V \leftarrow R^{x_1}$; $W \leftarrow R^{sk_S}$;
15: $Z_1 \leftarrow B_1^{x_1}$; $Z_2 \leftarrow B_2^{x_1}$; $Z_3 \leftarrow B_1^{x_2}$; $Z_4 \leftarrow B_2^{x_2}$;
16: $\tau_1 \leftarrow \mathsf{H}_2(X_1, X_2, Z_1, Z_2, Z_3, Z_4, pk_S, pk_R)$; $\tau_2 \leftarrow \mathsf{H}_2(X_2, X_1, Z_3, Z_4, Z_1, Z_2, pk_S, pk_R)$;
17: $c \leftarrow \mathsf{E}(\tau_2, m)$; $h \leftarrow \mathsf{H}_3(m, \tau_1, c, X_1, X_2, G, R, V, W, pk_S, pk_R)$;
18: $\sigma \leftarrow x_1 + h \cdot sk_S \mod p$; **return** (X_2, W, σ, h, c);
19: $\mathsf{Usc}(sk_R, pk_S, C)$: Parse sk_R as $(b_1, b_2) \in [p-1]^2$;
20: Parse C as $(X_2, W, \sigma, h, c) \in \mathcal{G}^2 \times [p-1]^2 \times \mathbf{C}$.
21: $X_1 \leftarrow G^{\sigma} pk_S^{-h}$; $Z_1 \leftarrow X_1^{b_1}$; $Z_2 \leftarrow X_1^{b_2}$; $Z_3 \leftarrow X_2^{b_1}$; $Z_4 \leftarrow X_2^{b_2}$;
22: $\tau_1 \leftarrow \mathsf{H}_2(X_1, X_2, Z_1, Z_2, Z_3, Z_4, pk_S, pk_R)$; $\tau_2 \leftarrow \mathsf{H}_2(X_2, X_1, Z_3, Z_4, Z_1, Z_2, pk_S, pk_R)$;
23: $m \leftarrow \mathsf{D}(\tau_2, c)$; $R \leftarrow \mathsf{H}_1(X_1, X_2)$; $V \leftarrow R^{\sigma} W^{-h}$;
24: **if** $h = \mathsf{H}_3(m, \tau_1, c, X_1, X_2, G, R, V, W, pk_S, pk_R)$ **then return** m; **else return** $\perp$;
25: $\mathsf{N}(sk_R, pk_S, C)$: Parse sk_R as (b_1, b_2); Parse C as (X_2, W, σ, h, c).

26: $X_1 \leftarrow G^{\sigma} pk_S^{-h}$; $Z_1 \leftarrow X_1^{b_1}$; $Z_2 \leftarrow X_1^{b_2}$; $Z_3 \leftarrow X_2^{b_1}$; $Z_4 \leftarrow X_2^{b_2}$;
27: $\tau_1 \leftarrow \mathsf{H}_2(X_1, X_2, Z_1, Z_2, Z_3, Z_4, pk_S, pk_R)$; $\tau_2 \leftarrow \mathsf{H}_2(X_2, X_1, Z_3, Z_4, Z_1, Z_2, pk_S, pk_R)$;
28: $m \leftarrow \mathsf{D}(\tau_2, c)$; $R \leftarrow \mathsf{H}_1(X_1, X_2)$; $V \leftarrow R^{\sigma} W^{-h}$;
29: **if** $h = \mathsf{H}_3(m, \tau_1, c, X_1, X_2, G, R, V, W, pk_S, pk_R)$ **then return** (τ_1, τ_2); **else return** $\perp$;
30: $\mathsf{PV}(C, m, nr, pk_S, pk_R)$: Parse C as (X_2, W, σ, h, c) and nr as (τ_1, τ_2);
31: $m' \leftarrow \mathsf{D}(\tau_2, c)$;
32: **if** $m' \neq m$ **then return** 0;
33: $X_1 \leftarrow G^{\sigma} pk_S^{-h}$; $R \leftarrow \mathsf{H}_1(X_1, X_2)$; $V \leftarrow R^{\sigma} W^{-h}$;
34: **if** $h = \mathsf{H}_3(m, \tau_1, c, X_1, X_2, G, R, V, W, pk_S, pk_R)$ **then return** 1; **else return** 0;

For the consistency of $\mathcal{SC}_{\mathsf{edl}}$, one can observe that, as $\sigma = x_1 + h \cdot sk_S$, $G^{\sigma} pk_S^{-h}$ yields X_1; similarly $R^{\sigma} W^{-h}$ yields V. Then, if $C \leftarrow_{\mathrm{R}} \mathsf{Sc}(sk_S, pk_R, m)$ the same Z_i's are computed in the signcryption and unsigncryption algorithms. And, the same values of τ_1 and τ_2 are derived both in $\mathsf{Sc}(sk_S, pk_R, m)$ and $\mathsf{Usc}(sk_R, pk_S, C)$. The remaining part in the definition of Sc (resp. Usc) is essentially a proof (resp. verification) of equality of discrete logarithms (edl) modified to include m, τ_1 and c. Doing so, for all $dp \in \{\mathsf{Setup}(k)\}$, all $m \in \mathcal{M}$, all $(sk_S, pk_S) \in \{\mathsf{Gen}_S(dp)\}$, and all $(sk_R, pk_R) \in \{\mathsf{Gen}_R(dp)\}$, $m = \mathsf{Usc}(sk_R, pk_S, \mathsf{Sc}(sk_S, pk_R, m))$. Moreover, if $nr \leftarrow \mathsf{N}(sk_R, pk_S, \mathsf{Sc}(sk_S, pk_R, m))$ then $1 = d \leftarrow \mathsf{PV}(C, m, nr, pk_S, pk_R)$.

4 Security of the $\mathcal{SC}_{\mathsf{edl}}$ Scheme

We have the following results; detailed proofs are given in [21].

Theorem 1 *We assume the RO model. If q_X, with $X \in \{\mathsf{H}_2, \mathsf{Usc}, \mathsf{N}\}$, is an upper bound on the number of times $\mathcal{A}$ issues the $\mathcal{O}_X$ oracle in Game 1, the cDH problem is $(t(k), \varepsilon_{\mathsf{cDH}}(k))$-hard in $\mathcal{G}$, and the encryption scheme $\mathcal{E}$ is $(t(k), \varepsilon_{\mathsf{ss}}(k))$-semantically secure, then $\mathcal{SC}_{\mathsf{edl}}$ is $(t(k), q_{\mathsf{Usc}}, q_{\mathsf{N}}, \varepsilon(k))$-secure in the SKI–MU insider confidentiality in the FSO/FUO–IND–CCA2 sense, where*

$$\varepsilon(k) \leqslant \varepsilon_{\mathsf{cDH}}(k) + \varepsilon_{\mathsf{ss}}(k) + 4(q_{\mathsf{H}_2} + 2q_{\mathsf{Usc}} + 2q_{\mathsf{N}} + 1)/p + 2q_{\mathsf{H}_3}/|\mathbf{K}|. \quad (1)$$

Theorem 2 *Let q_X, where $X \in \{\mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{Sc}\}$, be an upper bound on the number of times $\mathcal{A}$ issues the $\mathcal{O}_X$ oracle in Game 2. Under the RO model, if the cDH problem is $(t(k), \varepsilon_{\mathsf{cDH}}(k))$-hard in $\mathcal{G}$, then $\mathcal{SC}_{\mathsf{edl}}$ is $(t(k), q_{\mathsf{Sc}}(k), \varepsilon(k))$-MU insider unforgeable in the FSO/FUO–sUF–CMA sense, where $\varepsilon \leqslant \varepsilon_{\mathsf{cDH}} + ((q_{\mathsf{Sc}} + q_{\mathsf{H}_3})^2 + q_{\mathsf{Sc}}^2)/2p + (q_{\mathsf{H}_3} + 2q_{\mathsf{H}_2} + 1)/p$.*

Theorem 3 *Under the RO model, the $\mathcal{SC}_{\mathsf{edl}}$ scheme achieves (t, ε)-computational soundness of non-repudiation, where $\varepsilon \leqslant q_{\mathsf{H}_3}^2/2p$ wherein q_{H_3}, is an upper bound on the number of times $\mathcal{A}$ issues queries to the $\mathcal{O}_{\mathsf{H}_3}$ oracle.*

Theorem 4 *Under the RO model, if the cDH problem is $(t(k), \varepsilon_{\mathsf{cDH}}(k))$ hard, then $\mathcal{SC}_{\mathsf{edl}}$ achieves $(t, q_{\mathsf{Sc}}, q_{\mathsf{Usc}}, q_{\mathsf{N}}, \varepsilon)$ unforgeability of non-repudiation evidence wherein $\varepsilon \leqslant \varepsilon_{\mathsf{cDH}} + 1/|\mathbf{K}| + 3/(2p)$.*

4.1 On the Concrete Choice of the Set of Domain Parameters

A concrete instance of a cryptographic problem is said to have k-bits of security if any adversary $\mathcal{A}$ running in time t and trying to solve the problem succeeds with probability $\varepsilon \leqslant t/2^k$. A cryptographic scheme is said to have k-bits of security with respect to some security attribute, if any attacker playing the security game that defines the attribute and running in time t, succeeds with probability $\varepsilon \leqslant t/2^k$.

In $\mathcal{SC}_{\mathsf{edl}}$, if the underlying group $\mathcal{G}$ and the encryption scheme $\mathcal{E}$ are chosen such that the cDH problem in $\mathcal{G}$ has $(k+1)$-bits of security and $\mathcal{E}$ has $(k+3)$-bits of security then, from (1), it follows that $\mathcal{SC}_{\mathsf{edl}}$ is $(t, q_{\mathsf{Sc}}, q_{\mathsf{Usc}}, q_{\mathsf{N}}, \varepsilon)$-secure in the SKI–MU insider confidentiality in the FSO/FUO–IND–CCA2 sense, where $\varepsilon \leqslant t/2^{k+1} + t/2^{k+3} + 4(q_{\mathsf{H}_2} + 2q_{\mathsf{Usc}} + 2q_{\mathsf{N}} + 1)/p + 2t/|\mathbf{K}|$. As an $\mathcal{O}(\sqrt{p})$ algorithm is known for the discrete logarithm problem, $\alpha\sqrt{p} \geqslant 2^{k+1}$ for some "moderate" constant α. As $q_{\mathsf{H}_2} + 2q_{\mathsf{Usc}} + 2q_{\mathsf{N}} + 1 \leqslant 2t$ and $|\mathbf{K}| \geqslant 2^{k+3}$, we obtain $\varepsilon \leqslant t/2^k$. Hence, $\mathcal{SC}_{\mathsf{edl}}$ has k-bits of security in the SKI–MU insider confidentiality in the FSO/FUO–IND–CCA2 sense. A similar analysis shows that under the same assumptions, $\mathcal{SC}_{\mathsf{edl}}$ has k-bits of security with regard to (i) (ii) the MU insider strong unforgeability in the FSO/FUO–sUF–CMA sense, (iii) the soundness of non-repudiation, and (vi) the unforgeability of non-repudiation evidence.

5 Comparison with Other Schemes

The design of $\mathcal{SC}_{\mathsf{edl}}$ integrates the randomness reuse idea suggested in [2, 20]. A $\mathcal{SC}_{\mathsf{edl}}$ sender (resp. receiver) key pair generation requires one (resp. two) exponentiations. An execution of the Sc algorithm requires $\mathsf{Exp}(\mathcal{G}, 8)$. Four of the 8 exponentiations can be performed *offline*, before the receiver public key and the plain text are provided. If the receiver public key is provided before the plain text (this may occur in email systems where the recipient is often typed before email text) *all* the 8 exponentiations can be performed before the plain text is provided The Usc and N algorithms require $\mathsf{Exp}(\mathcal{G}, 4)$ (two pairs of exponentiations with the same exponent) and two multi-exponentiations. The public verification algorithm requires two multi-exponentiations. If the encryption scheme $\mathcal{E}$ is such that a clear text and a corresponding ciphertext have the same length, the communication overhead of $\mathcal{SC}_{\mathsf{edl}}$, compared to the CM signature scheme is one group element. Notice that we neglected the group membership tests, as they have a negligible cost in $\mathbb{Z}_q^*$ and elliptic curve groups.

In [19], Malone–Lee (ML) proposes a very efficient design with NINR. Unfortunately, the design, which is analyzed in the RO model under de cDH assumption, does not achieve insider security. Also the reduction uses the Forking Lemma [6, 22]. Assuming $q_{\mathsf{H}} = 2^{32}$, for a security target of 128-bits, the underlying group $\mathcal{G}'$ must be chosen to offer 160-bits of security. In the case $\mathcal{G}'$ is a (sub)group of the rational points of an elliptic curve $\mathcal{G}' = E(\mathbb{F}_{q'})$, q' has to be chosen such that

$|q'| \approx 320$. An execution of the ML Sc or Usc algorithm requires two exponentiations. As a modular multiplication (performed with the Karatsuba–Ofman algorithm) in $\mathbb{F}_{q'}$ has complexity $\approx |q'|^{1.585}$. Given the tightness of our reduction, in ECC, we need $|q| = 256$ to have 128 bits of security. As $\mathsf{Mult}(\mathbb{F}_{q'}) \approx 1.42 \cdot \mathsf{Mult}(\mathbb{F}_q)$, assuming that a group operation in $\mathcal{G}'$ requires $14 \cdot \mathsf{Mult}(\mathbb{F}_{q'})$ (see[1] [16, p. 96]), $\mathsf{Exp}(\mathcal{G}') \approx 6720 \cdot \mathsf{Mult}(\mathbb{F}_{q'}) \approx 9570 \cdot \mathsf{Mult}(\mathbb{F}_q) \approx 1.78 \cdot \mathsf{Exp}(\mathcal{G})$. The ML design is about (a) 2.25 times faster for signcryption, and (b) 1.25 times faster for unsigncryption than ours.

Bjørstad and Dent's (BD) design [8] tightly achieves, in the RO model, insider unforgeability under the cDH assumption and *outsider* confidentiality under the gap DH assumption. The scheme does not achieve insider confidentiality. The Sc algorithm requires $\mathsf{Exp}(\mathcal{G}, 3)$ operations, the Usc algorithm requires two multi-exponentiations. The BD construction is about 2.5 times faster than $\mathcal{SC}_{\mathsf{edl}}$ for signcrypted ciphertext generation and about 3 times faster for unsigncryption.

Some of the designs we consider hereunder assume the existence of groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ together with a bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Recall that for a choice of the groups $\mathcal{G}, \mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_T$ (where $\mathcal{G}$ is a classical ECC group), with a target of 128-bits of security, the cost of a pairing evaluation is about $\approx \mathsf{Exp}(\mathcal{G}, 8)$, $\mathsf{Exp}(\mathbb{G}_1) \approx \mathsf{Exp}(\mathcal{G}, 3)$, and $\mathsf{Exp}(\mathbb{G}_2) \approx \mathsf{Exp}(\mathcal{G}, 6)$ [7, p. 126].

Arriaga et al.'s generic construction with NINR [2] is insider secure in the standard model. They propose an instantiation of their design which assumes the Decisional Bilinear and the q-Strong DH assumptions. Unfortunately, the unforgeability is achieved in the registered key model [20], wherein an attacker needs to register to the challenger the keys pairs it uses in its attack. The design assumes the existence of groups $\mathbb{G}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ such that (i) $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are of order q, (ii) there is a bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ and (iii) a one to one and efficiently invertible mapping from $\mathbb{G}$ to $\mathbb{Z}_q$.

An evaluation of the Sc algorithm requires $\mathsf{Exp}(\mathbb{G}, 2) + \mathsf{Exp}(\mathbb{G}_1)$ and one multi-exponentiation in $\mathbb{G}$. The Usc algorithm requires two multi-exponentiations, one in $\mathbb{G}$ and one in $\mathbb{G}_2$, and a pairing evaluation. For a target of 128 bits of security, we expect $\mathcal{SC}_{\mathsf{edl}}$ to be 1.5 times faster for signcryption and 2.8 times faster for unsigncryption.

Matsuda et al. [20]'s two generic constructions with NINR are insider secure in the FSO/FUO model. The security reduction is provided in the RO model. The most efficient among the instanciations that achieve insider security in the FSO/FUO model uses as base schemes, the DHIES encryption scheme [1] and the BLS signature scheme [9]. The construction assumes the existence of groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ together with a bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. A Sc operation requires $\mathsf{Exp}(\mathbb{G}_1, 3)$, an Usc operation requires $\mathsf{Exp}(\mathbb{G}_2)$ and two pairing evaluations. Compared to $\mathcal{SC}_{\mathsf{edl}}$, for a target of 128 bits of security (given that $\mathsf{Exp}(\mathbb{G}_1) \approx \mathsf{Exp}(\mathcal{G}, 3)$, $\mathsf{Exp}(\mathbb{G}_2) \approx$

[1] If $|\mathcal{G}| = 2^\lambda$, the cost of $\mathsf{Exp}(\mathcal{G})$ using the classical square-and-multiply algorithm is $\approx 1.5 \cdot \lambda$ operations in $\mathcal{G}$. And if $\mathcal{G}$ is such that the multiplication of two of its elements requires 14 multiplications in $\mathbb{F}_q$ then the computational cost of an exponentiation is $14 \cdot 1.5 \cdot \lambda$ multiplications in $\mathbb{F}_q$.

$\mathsf{Exp}(\mathcal{G}, 6)$ and the cost of a pairing evaluation $\approx \mathsf{Exp}(\mathcal{G}, 8)$) we expect our design to be 1.12 times faster for signcryption, and about 3.6 times faster for unsigncryption.

For a comparison with Chiba et al.'s generic construction with NINR [13], we consider the most efficient among the instantiations they propose. It achieves insider security in the FSO/FUO model, under the Decisional Bilinear and the q-strong DH assumptions. Although the insider security is shown in the standard model, the unforgeability is achieved in the registered key model. Besides, the scheme assumes the existence of a pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, with $\mathbb{G}_1 = \mathbb{G}_2$. The Sc algorithm requires $\mathsf{Exp}(\mathbb{G}_1, 3)$ together with a multi-exponentiation. The Usc operation requires one exponentiation, one multi-exponentiation, and one pairing evaluation. We expect $\mathcal{SC}_{\mathsf{edl}}$ to be about 1.5 times faster for signcryption, and about 2.3 times faster for unsigncryption.

Fan et al.'s design [14] assumes the existence of a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, where $\mathbb{G}$ and $\mathbb{G}_T$ are multiplicative cyclic groups. The Sc algorithm requires one pairing, $\mathsf{Exp}(\mathbb{G}, 4) + \mathsf{Exp}(\mathbb{G}_T)$, and $(n + 1)/2$ group operations in $\mathbb{G}$, where n is the bit-length output of some collision resistant hash function $\mathsf{H} : \mathbb{G} \to \{0, 1\}^n$ used in the design. The unsigncryption algorithm requires 3 pairings, $\mathsf{Exp}(\mathbb{G}, 2)$, and $(n/2 + 1)$ group operations in $\mathbb{G}$. A signcrypted ciphertext is an element of $\mathbb{G}_T \times \mathbb{G}^3$. For a choice of the groups $\mathcal{G}$, $\mathbb{G}$, and $\mathbb{G}_T$, with target 128-bits of security, we expect our design to be about (a) (b) 2.5 times faster for signcryption, and (c) 7.5 times faster for unsigncryption than Fan et al.'s construction, in addition to having shorter signcrypted ciphertexts.

In the scheme from [23], defined over the (RSA based) group of signed quadratic residues $\mathbb{J}_N^+$, the Sc algorithm requires $\mathsf{Exp}(\mathbb{J}_N^+, 6)$ and the Usc algorithm requires $\mathsf{Exp}(\mathbb{Z}_N, 3)$ (we ignore the exponentiation with the RSA public exponent, which is often small and sparse). Unfortunately, the security reduction uses the Forking Lemma, which implies a $1/q_{\mathsf{H}}$ security degradation, where q_{H} is the number of digest queries the attacker issues. For $q_{\mathsf{H}} = 2^{32}$, if the target security is 128-bits, the RSA modulus needs to have a bitlength $|N| \approx 7864$ [18][2]. Then, considering a square-and-multiply based exponentiation, $\mathsf{Exp}(\mathbb{J}_N^+) \approx 11796 \cdot \mathsf{Mult}(\mathbb{Z}_N)$, where $\mathsf{Mult}(\mathbb{Z}_N)$ denotes the cost of a multiplication in $\mathbb{Z}_N$. In contrast $\mathcal{SC}_{\mathsf{edl}}$ can be instantiated over an elliptic curve (sub)group $\mathcal{G} = E(\mathbb{F}_q)$ such that $|q| \approx 256$ and $\mathcal{G}$ has 128-bits of security. Assuming that a group operation in $\mathcal{G}$ requires $14 \cdot \mathsf{Mult}(\mathbb{F}_q)$ [16, p. 96], $\mathsf{Exp}(\mathcal{G}) \approx 5376 \cdot \mathsf{Mult}(\mathbb{F}_q)$. As $\mathsf{Mult}(\mathbb{Z}_N) > 30 \cdot \mathsf{Mult}(\mathbb{F}_q)$, for a 128-bits security target, we expect $\mathcal{SC}_{\mathsf{edl}}$ over $\mathcal{G}$ to be at least 13 times faster (for key generation, signcryption, unsigncryption, etc.) than the design from [23].

Compared to the ML and BD schemes, which do not require any specificity of the underlying group and do not achieve insider security, $\mathcal{SC}_{\mathsf{edl}}$ offers a stronger security, even if it is less efficient. And, compared to the schemes from [2, 13, 14, 20, 23], $\mathcal{SC}_{\mathsf{edl}}$ offers a tight security reduction, a better efficiency and a comparable or a superior security. We summarize in Table 1 some elements of comparisons. The column $\mathsf{Assumptions}$ indicates the computational assumptions used in the security reductions; FL and IS stand respectively for $\mathsf{Forking\ Lemma}$ and

[2] see also www.keylength.com

Table 1 Comparison of the proposed signcryption schemes with some SCNINR schemes from the litterature

Scheme	Assumptions	FL	IS	Computations	Overhead
ML [19]	RO, cDH	y	n	[2, 0, 0] [2, 0, 0]	$2 \cdot \mathsf{sz}(\mathbb{Z}_p)$
BD [8]	RO, cDH	n	p	[2, 0, 0] [0, 2, 0]	$\mathsf{sz}(\mathcal{G}) + \mathsf{sz}(\mathbb{Z}_p)$
ABF [2]	DBDH, q-sDH	n	y	[3, 1, 0] [0, 2, 1]	$\mathsf{sz}(\mathbb{G}) + \mathsf{sz}(\mathbb{G}_1)$
MMS [20]	RO, GDH, co–cDH	n	y	[3, 0, 0] [1, 0, 2]	$\mathsf{sz}(\mathbb{G}_1) + \mathsf{sz}(\mathbb{G}_2)$
CMSM [13]	DBDH, q-sDH	n	y	[3, 1, 0] [1, 1, 2]	$\mathsf{sz}(\mathbb{Z}_p) + 4 \cdot \mathsf{sz}(\mathbb{G}_1)$
FZT [14]	DBDH, DL	n	y	[5, 0, 1] [2, 0, 3]	$\mathsf{sz}(\mathbb{Z}_p) + 2 \cdot \mathsf{sz}(\mathbb{G}_1)$
SSN [23]	RO, RSA	y	y	[6, 0, 0] [3, 0, 0]	$\mathsf{sz}(\mathbb{Z}_p) + 2 \cdot \mathsf{sz}(\mathbb{Z}_N)$
Ours: $\mathcal{SC}_{\mathsf{edl}}$	RO, cDH	n	y	[8, 0, 0] [4, 2, 0]	$2 \cdot \mathsf{sz}(\mathbb{Z}_p) + 2 \cdot \mathsf{sz}(\mathcal{G})$

Insider Security (in the FSO/FUO model). The letters 'y' and 'n' stand for "yes" and "no", respectively; 'p' stands for "partial" (BD achieves insider unforgeability, but *outsider* confidentiality). In the column Computations $[a, b, c][a', b', c']$ means that a Sc (resp. Usc) operation requires a (resp. a') exponentiations, b (resp. b') multi-exponentiations, and c (resp. c') pairing evaluations. We recall that the number of exponentiations has to be considered in conjunction with the underlying mathematical structure. For instance, as previously said, if a scheme requires a bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, for a target of 128 bits of security, it holds $\mathsf{Exp}(\mathbb{G}_1) \approx \mathsf{Exp}(\mathcal{G}, 3)$ and $\mathsf{Exp}(\mathbb{G}_2) \approx \mathsf{Exp}(\mathcal{G}, 6)$. The column Overhead indicates the signcrypted ciphertext overhead compared to the *cleartext*.

References

1. Abdalla, M., Bellare, M., Rogaway, P.: The oracle Diffie-Hellman assumptions and an analysis of DHIES. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 143–158. Springer, Heidelberg (2001)
2. Arriaga, A., Barbosa, M., Farshim, P.: On the joint security of signature and encryption schemes under randomness reuse: efficiency and security amplification. In: Bao, F., Samarati, P., Zhou, J. (eds.), Applied Cryptography and Network Security. ACNS 2012. LNCS, vol 7341. Springer, Berlin, Heidelberg (2012)
3. Badertscher, C., Banfi, F., Maurer, U.: A constructive perspective on signcryption security. In: Catalano, D., De Prisco, R. (eds.), Security and Cryptography for Networks. SCN 2018. LNCS, vol. 11035. Springer, Cham (2018)
4. Baek, J., Steinfeld, R., Zheng, Y.: Formal proofs for the security of signcryption. J. Cryptol. **20**(2), 203–235 (2007)
5. Bao, F., Deng, R.H.: A signcryption scheme with signature directly verifiable by public key. In: Imai, H., Zheng, Y. (eds.), Public Key Cryptography. PKC 1998. LNCS, vol. 1431. Springer, Berlin, Heidelberg (1998)
6. Bellare, M., Neven, G.: Multi–signatures in the plain public–key model and a general forking lemma. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 390–399. ACM (2006)

7. Benhamouda, F., Couteau, G., Pointcheval, D., Wee, H.: Implicit zero-knowledge arguments and applications to the malicious setting. In: Gennaro, R., Robshaw, M. (eds.), Advances in Cryptology—CRYPTO 2015. CRYPTO 2015. LNCS, vol. 9216. Springer (2015)
8. Bjørstad, T.E., Dent, A.W.: Building better signcryption schemes with Tag-KEMs. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.), Public Key Cryptography—PKC 2006. PKC 2006. LNCS, vol. 3958. Springer, Berlin, Heidelberg (2006)
9. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. J. Cryptol. **17**(4), 297–319 (2004)
10. Boneh, D., Shen, E., Waters, B.: Strongly unforgeable signatures based on computational Diffie–Hellman. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.), Public Key Cryptography—PKC 2006. PKC 2006. LNCS, vol. 3958. Springer, Berlin, Heidelberg (2006)
11. Cash, D., Kiltz, E., Shoup, V.: The twin Diffie-Hellman problem and applications. J. Cryptol. **22**(4), 470–504 (2009)
12. Chevallier–Mames, B.: An efficient CDH–Based signature scheme with a tight security reduction. In: Shoup, V. (eds.), Advances in Cryptology—CRYPTO 2005. CRYPTO 2005. LNCS, vol. 3621. Springer, Berlin, Heidelberg (2005)
13. Chiba, D., Matsuda, T., Schuldt, J.C.N., Matsuura, K.: Efficient generic constructions of signcryption with insider security in the multi-user setting. In: Lopez, J., Tsudik, G. (eds.), Applied Cryptography and Network Security. ACNS 2011. LNCS, vol. 6715. Springer, Berlin, Heidelberg (2011)
14. Fan, J., Zheng, Y., Tang, X.: Signcryption with non–interactive non–repudiation without random oracles. In: Transactions on Computational Science X, pp. 202–230. Springer, Berlin, Heidelberg (2010)
15. Goh, E.J., Jarecki, S.: A signature scheme as secure as the Diffie–Hellman problem. In: Biham, E. (eds.), Advances in Cryptology—EUROCRYPT' 03. EUROCRYPT 2003. LNCS, vol. 2656. Springer, Berlin, Heidelberg (2003)
16. Hankerson, D., Menezes, A.J., Vanstone, S.: Guide to Elliptic Curve Cryptography. Springer (2004)
17. Katz, J., Wang, N.: Efficiency improvements for signature schemes with tight security reductions. In: Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 155–164. ACM (2003)
18. Lenstra, A.K.: Key lengths. Handbook of Information Security, vol. 2, pp. 617–635. Wiley (2005)
19. Malone–Lee, J.: Signcryption with non–interactive non–repudiation. Designs, Codes and Cryptography, vol. 37, no. 1, pp. 81–109. Springer (2005)
20. Matsuda, T., Matsuura, K., Schuldt, J.C.N.: Efficient constructions of signcryption schemes and signcryption composability. In: Roy, B., Sendrier, N. (eds.), Progress in Cryptology—INDOCRYPT 2009. INDOCRYPT 2009. LNCS, vol. 5922. Springer, Berlin, Heidelberg (2009)
21. Ngarenon, T., Sarr, A.P.: A Computational Diffie–Hellman based Insider Secure Signcryption with Non Interactive Non Repudiation (full version) (2022). https://hal.archives-ouvertes.fr/hal-03628351/
22. Pointcheval, D., Stern, J.: Security proofs for signature schemes. In: Maurer, U. (eds.), Advances in Cryptology—EUROCRYPT'96. EUROCRYPT 1996. LNCS, vol. 1070. Springer, Berlin, Heidelberg (1996)
23. Sarr A.P., Seye P.B., Ngarenon T.: A Practical and Insider Secure Signcryption with Non-interactive Non-repudiation. In: Carlet C., Guilley S., Nitaj A., Souidi E. (eds.), Codes, Cryptology and Information Security. C2SI 2019. LNCS, vol. 11445. Springer, Cham (2019)
24. Zheng, Y.: Digital signcryption or how to achieve cost(signature & encryption) $\ll$ cost(signature) + cost(encryption). In: Kaliski, B.S. (eds.), Advances in Cryptology—CRYPTO '97. CRYPTO 1997. LNCS, vol. 1294. Springer, Berlin, Heidelberg (1997)