28-3-2005

Privacy-enhanced Internet storage

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Fangguo Zhang
Sun Yat-Sen University, China

Yi Mu
University of Wollongong, ymu@uow.edu.au

Recommended Citation

Susilo, Willy; Zhang, Fangguo; and Mu, Yi: Privacy-enhanced Internet storage 2005.
https://ro.uow.edu.au/infopapers/122

Privacy-enhanced Internet storage

Abstract

One of the main important uses of Internet is its ability to connect people through the use of email or Internet storage. However, it is often desirable to limit the use of email or Internet storage clue to organization's restriction, avoiding spams, etc. In this paper, we propose cryptographic schemes that can be used to stop unwanted messages to be stored in the Internet server. We refer this technique as privacy enhancement for Internet storage, since the Internet server will not learn any information directed to its users, other than performing its task to deliver or stop the messages. Firstly, we describe a notion of non-interactive publicly verifiable 1-out-of-n encryption by proposing a model together with its security requirements. Then, we extend this notion to a publicly verifiable ring-to-1-out-of-n encryption, that provides sender anonymity. We note that the previously known interactive versions of the publicly verifiable 1-out-of-n encryption cannot be used to construct publicly verifiable ring-to-1-out-of-n encryption.

Keywords

Internet, data privacy, digital signatures, public key cryptography

Disciplines

Physical Sciences and Mathematics

Publication Details

This paper originally appeared as: Susilo, W, Zhang, F and Mu, Y, Privacy-enhanced Internet storage, 19th International Conference on Advanced Information Networking and Applications, 28-30 March 2005, vol 1, 603-608. Copyright IEEE 2005.

Privacy-Enhanced Internet Storage

Willy Susilo[1], Fangguo Zhang[2] and Yi Mu[1]
[1] School of IT and Computer Science
University of Wollongong, Wollongong, NSW 2522, Australia
{wsusilo, ymu}@uow.edu.au
[2] Department of Electronics and Communication Engineering
Sun Yat-Sen University, Guangzhou 5 10275, P.R. China
isdzhfg@zsu.edu.cn

Abstract

One d the main important uses of Internet **is its** *ability to connect people through the* **use** *of email or internet storage. However; it* **is** *often desirable to limit the use of email* **or** *Internet storage due to organization's restriction, avoiding spams, etc. In this paper, we propose cryptographic schemes that can be used to stop unwanted messages to be stored* **in** *the Internet server. We refer this technique* **as** privacy enhancement for Internet storage, **since** *the Internet server will* not *learn any information directed to its* **users.** *other than performing its task to deliver or stop the* **messages.** *Firstly,* **we** *describe a notion* d non-interactive publicly verifiable 1-out-of-n encryption *by proposing a model together with its security requirements. Then, we extend this notion to a* publicly verifiable ring-to-1-out-of-n encryption, *that provides* sender anonymity. *We note that the* ***previously known*** interactive *versions of the publicly verifiable 1-out-of-n encryption cannot be used to construct publicly verifiable ring-to-1-out-of-n encryption.*

Keywords: Internet storage. non-interactive, publicly verifiable 1-out-of-n encryption, publicly verifiable ring-to-I-out-ofn encryption. signature d knowledge

1. Introduction

The public Internet can be considered as a world wide computer network, that is, a network that interconnects millions of computing devices throughout the world. Most of these devices are traditional desktop PCs, Windows/Linux/Unix based workstations, laptops, tablet PCs, handheld devices and so forth. Among them, there are servers that store and transinit information such as web pages and email messages One of the most important uses of Internet is its ability to connect people through the use of email or Internet storage. However. it is often desirable to limit the use of email or Internet storage due to organization's restriction. avoiding spams, etc

Consider a situation where there is an Internet storage that can be used to store messages directed to a group of users, Γ In this situation. it would be desirable to install a secure gateway $\mathcal{G}$ to stop all messages that are not directed to its group members in Γ $\mathcal{G}$ will act as a mediator between a sender and a receiver of a message in group Γ. When **Al**ice wants to send a public-key encrypted message to Bob, who is a member of Γ, then $\mathcal{G}$ must be able to check that the message is directed to a group member in Γ and store the message in the Internet storage. However, the problem is $\mathcal{G}$ does not hold Bob's secret key This problem has been considered in [5] to create an anonymous ad hoc group In this scenario. by knowing only the public information of the group members in Γ, $\mathcal{G}$ must deterniine if the encrypted incoming data is for a group member in Γ without being able to identify the actual recipient Moreover. the other member in 1',together with $\mathcal{G}$ itself, must not be able to read the message directed to Bob. In [5] (or subsequently revised in [6]), this problem has been considered as publicly verifiable 1-out-of-n encryption (PV1nE) scheme. and they proposed an interactive protocol for PV1nE in [5]

In a different scenario, Alice does not want her identity to be revealed Instead. she would like to send **a** message to Bob on behalf of a group, which can be verified Suppose Alice is a worker in an insurance company who would like to send a message to Bob. then the message is considered to *belong* to the company instead of being sent by Alice The situation becomes more complex than the original scenario mentioned earlier. since $\mathcal{G}$ cannot perform an interactive protocol with Alice, and hence, the notion d *non interactive* PV1nE is essential and required We note that this scenario is essential, especially rf we would like to protect Alice's pnvacy Without having to assume that an anonymous routing (eg MIX-nets) exists. then the existence of non-ınteractıve PV1nE is essential

In a non-interactive PV1nE. a Prover (or Sender.respectively) wishes to send a public-key encrypted message to a Receiver through a Verifier The Prover arbitrarily forms a group Γ that consists of the Receiver together with other people that belong to the same group as the Receiver Then, the Prover conducts a special public-key encryption for the group of receivers in such a way that the public verifier can be sure that the message can be decrypted by one of the receivers ın the group. It is also required that l) the Verifier cannot read the message, 2) the Verifier cannot identify to whom the message is designated to, and 3) the Verifier does not need to perform an interactive piotocol with the Prover to check the validity of the message

Our Contribution
The schcme used in [5] is based on the *cut and-choose methodology* [8] and hence, ınteractıons between sender and verifier are required. In this paper, we firstly provide a notion of a Non-Interactive Publicly Verifiable l-out-of-n Encryption Scheme (PV1nE), and propose a non-interactive schcme *without* employing a cut-and-choose technique that satisfies our model Then. we extend this notion to create a Publicly Verifiable Ring-to-1-out-of-n Encryption (PVRTE) Scheme We shall point out that the interactive version of PVlnE *cannot* be used to generate a PVRTE schcme We also provide a generıc construction of PVRTE schemes from any PVlnE schemes. We provide a complete security proof for our schemes

1.1. Sotations

Throughout this paper. we will use the following notations. The ring of integers modulo a number p is denoted by $\mathbb{Z}_p$, and the multiplicative subgroup of integers relatively prıme to p, by $\mathbb{Z}_p^*$ Let |; denote a binary operator that concatenates two bit strings as inputs. The inputs will be converted to its binary representation where its length is determined by a security parameter ℓ.

2. Cryptographic Tools

In this section, we will review some cryptographic tools, together with proposıng some new cryptographic primitives, that will be used throughout this paper.

Let q be a large prime and $p = 2q-1$ be also a pnme Let G be a finite cyclic group of pnme order p. Let $9, h \in \mathbb{Z}_p^*$ be two elements of order q. Let y be a generator of G such that computing discrete logarithms ot any group element (apart from the identity element) with respect to one of the generators is infeasible Let $H \quad (0,1\}^* \rightarrow \{0 \ 1\}^\ell$ denote a strong collision-resistant hash function

2.1. Signature *of* Knowledge of Representation

The first signature of knowledge (SPK) was proposed in [3, 2] We will use the following definition of signature of knowledge from [3].

Definition 1 *[3]A paır* $(c.s) \in \{0,1\}^\ell \times \mathbb{Z}_q$ *satisfying*

$$c = H(S||V|'m) \ with \ S = g|,y \ and \ V = g^s y^c \pmod p$$

is a signature ***knowledge*** *of the discrete logarithm of a group element* y *to the base* g *of the message* $m \in \{0,1\}^*$ *and* **is** *denoted*

$$SPKLOG\{\alpha : y = g^\alpha\}(m)$$

An $SPKLOG\{\alpha \quad y = g^\alpha \bmod p\}(m)$ can be computed if the value (secret key) $\alpha = \log_g(y)$ is known, by selecting a random integer $r \in \mathbb{Z}_q$ and computing $t = g^r$ niod p and then c and s according to

$$c = H(g||y||t||m)$$

and

$$s = r - c\alpha \pmod y).$$

This is also known as a non-interactive proof of the knowledge α

3.2. Ring Signature Schemes

We adopt the notations proposed in [1] to define ring signature schemes. We note that the ring signature schemes are referred to 1-out-of-n in [1].

Definition 2 *[1]* A *ring signature scheme consists of three polynomial time algorithms*

- $(s_k, p_k) \leftarrow \mathcal{G}($1"$)$: **A** *probabilistic algorithm thut takes security parameter* κ *and outputs private* ***key*** s_k *and public key* p_k.
- $\sigma \leftarrow \mathcal{S}(m, s_k, L)$: **A** *probabilistic algorithm that takes a message* m*, a list L that contains public keys including the one that corresponds to* s_k *and outputs a signature* σ.
- {**True** *or* $\perp\} \leftarrow \mathcal{V}(m, \sigma. L)$: *A deterministic algorithm that takes a message* m **arid** *a signature* σ, *and outputs either* True *or* $\perp$ *meaning* accept *or* reject, *respectively. It is required to have* True +- $\mathcal{V}(m, \mathcal{S}(m, s_k, L), L)$ ***with*** *&irnoverwhelming probability.*

A ring that allows a mixture of factorization and discrete log based public keys has been constructed in [1].

3. A New Signature of Knowledge for Proving Equality of Discrete Logarithm and Double Discrete Logarithm

In this section, we extend the notion of signature of knowledge mentioned in the previous section to signature of knowledge for proving equality of discrete logarithm and double discrete logarithm.

Definition 3 *A signature of knowledge on* $m \in \{0.1\}^*$, ***de**noted b?*

$$SPK2LOG\{\alpha : y = g^{\alpha} \text{ A } z = \hat{g}^{(h^{\alpha})}\}(m),$$

is a signature of knowledge on equality proof that the knowledge of the discrete logarithm of y *to the base* $g \in \mathbb{Z}_p^*$ *equals the double discrete logarithm* of z *to the base* $\hat{g} \in G$ *and* $h \in Z_p^*$.

This signature of knowledge is represented by $(c, s_1, \cdots, s_\ell, \hat{s}) \in \{0,1\}^k \times Z^\ell$, whcre $\ell \leq k$ be a security parameter, satisfying equation

$$c = H(m \quad y||g| \hat{g}| g^s y^c||h||t_1|| \qquad t_\ell)$$

with

$$t_i = \begin{cases} \hat{g}^{(h^s \ )} & \text{i}f c[i] = 0 \\ z^{(h \ \ )} & \text{otherwise} \end{cases}$$

Note that $z = g^{(h^{\alpha})}$

To compute the above signature of knowledge, three conditions must hold

- The value of $x = \log_g(y)$ is known.
- The value of $x = \log_g(\log_h(z))$ is known
- $\log_g(y) = \log_g(\log_h(z))$ holds

We assume that there is an upper hound λ on the length of x, i e $0 \leq x < 2^\lambda$ The signature of knowledge is generated as follows

Firstly, compute the values of

$$t_i^* = \hat{g}^{(h^{r_i})}$$

for $i = 1 \qquad \ell$ with randomly chosen $r_i \in \{0, \qquad 2^{\epsilon\lambda} - 1\}$, where $\epsilon > 1$ be a constant. Then, select a random $r \in Z_q$ and compute c as

$$\text{c} = H(m\, |y \ \ g| \ \hat{g}||g^r \ |h \ |t_1| \qquad ||t_\ell)$$

Finally, we set the following values

$$\begin{cases} s_i \leftarrow r_i, & \text{if } c[i] = 0 \\ s_i \leftarrow r_i - x & \text{otherwise.} \end{cases}$$

and compute

$$= r - cx \pmod q$$

One can verify that the resulting tuple $(c, s_1, \cdots, s_\ell, \hat{s})$ satisfies the verification equation.

Based on the above signature of knowledge. we further extend it to $SPK2LOG(1,n)\{\alpha : y =$ </" $\wedge z = \hat{g}^{h_1^{\alpha}} \vee \hat{g}^{h_2^{\alpha}} \ldots \vee \hat{g}^{h_n^{\alpha}}\}(m)$ defined as follows.

Definition 4 A *signature of knowledge on* $m \in \{0,1\}^*$, *denoted by*

$$SPK2LOG(1,n)\{\alpha : y = g^{\alpha} \wedge z = \hat{g}^{h_1^{\alpha}} \vee \hat{g}^{h_2^{\alpha}} \ldots \vee \hat{g}^{h_n^{\alpha}}\}(m)$$

is *a 1-out-of-n knowledge equality proof that the knowledge of the discrete logarithm of* y *to the base* $g \in \mathbb{Z}_p^*$ *equals rhr double discrete logarithm of* z *to the base* $\hat{g} \in G$ *and one of* $h_1, h_2, \ldots, h_n \in Z_p^*$.

This signature of knowledge is represented by $(\hat{s}, c_1, c_2, \cdots c_n, s_1, s_2, \cdots, s_n)$, satisfying equation

$$\sum_{i=1}^{n} c_i = H(m||y||g||\hat{g}||g^{\hat{s}} y^{\sum_{i=1}^{n} c_i}||h_1|| \cdots ||h_n||t_{11}|| \\ ||t_{1\ell}|| \cdots ||t_{1\ell}|| \cdots ||t_{n\ell})$$

where

$$t_{ji} = \begin{cases} \hat{g}^{(h_j^{s_{ji}})} & \text{if } c_j[i] = 0, \\ z^{(h_j^{s_{ji}})} & \text{otherwise.} \end{cases}$$

for $j - 1, \qquad .n$

The signature of knowledge can only be computed if one of the valid α is known, whcre $\alpha = \log_{\hat{g}}(\log_{h_i} z)$ and $\alpha = \log_g(y)$. It can be computed as follows Without losing generality, we assume that the prover knows α where $\alpha = \log_{\hat{g}}(\log_{h_1} z)$ and $\alpha = \log_g (y)$

1 Firstly, select $n - 1$ random numbers. $c_2, \qquad c_n \in Z_q$.

2. Then. select ℓn random numbers, $t_{11}, \qquad .t_{1\ell}, \qquad .t_{n1} \qquad .t_{n\ell} \in \{0 \qquad , 2^{\epsilon\lambda} - 1)$

3 Select a random number r $\in Z,$

4 For $j = 2. \qquad , n$, compute

$$t_{ji} = \begin{cases} g^{h_j^{r_{ji}}} & \text{if } c_j[i] = 0, \\ z^{h_j^{r_{ji}}} & \text{otherwise.} \end{cases}$$

for all $i = 1 \qquad .\ell$.

5. Compute

$$t_{1i} = \hat{g}^{(h^{r_{1i}})}$$

6. Compute

$$c_1 = H(m||y||g||\hat{g}||g^r||h_1|| \cdots ||h_n|| \\ t_{11}|| \cdots ||t_{1\ell}|| \cdots ||t_{1\ell}|| \cdots ||t_{n\ell}) \\ -\sum_{i=2}^{n} c_i \pmod q$$

7. Let

$$s_{1i} = \begin{cases} r_{1i} & \text{if } c_1[i] = 0, \\ r_{1i} - x_1 & \text{otherwise.} \end{cases}$$

8. Compute

$$\hat{s} = r - x_1 \sum_{i=1}^{n} c_i \pmod q$$

One can verify that the resulting tuple $(\hat{s}, c_1, c_2, \ldots, c_n; s_1, s_2, \ldots, s_n)$ satisfies the verification equation.

4. Non-Interactive Publicly Verifiable 1-out-of-n Encryption Scheme (PV1nE)

4.1. Model

A PV1nE scheme involves three entities, namely a `Prover` P (or `Sender`. iespectively). a `Verifier` V and a `Receiver` R There are three algorithm involved. namely a probabilistic algorithm: `Verifiable Encryption` (VE). a deterministic algorithm. `Verification` (Ver) and a deterministic algorithm `Decryption` (Dec)

P accepts as inputs a security parameter k, a message $m \in \{0\ 1\}^*$, n public-key encryptions $\{E_i\}_{1 \leq i \leq n}$ By invohing `Verifiable Encryption` (VE) algorithm, it outputs a valid ciphertext C that can only be deciphered by one of the secret keys D_i associated with E_i, $1 \leq i \leq n$

V accepts a ciphertext C together with all public keys $\{E_i\}_{1 \leq i \leq n}$ By invoking the `Verification` (Ver) algorithm. it outputs {`True` ⊥} The output is `True` if C is *valid* which means that it will be able to be decrypted by one of the secret keys D_i, $1 \leq i \leq n$, otherwise it outputs $\perp$ When the output is $\perp$, then C is discarded (since it is tagged as 'invalid')

R accepts a ciphertext C and obtains the plaintext m by invoking the `Decryption` (Dec) algorithm

Security Requirements

1. Probability of a prover P to produce an invalid ciphertext C that will pass the verification test is negligible We require

$$\Pr \quad \{Ver(C\ \{E_i\}_{1 \leq i \leq n}, \forall i) = \texttt{True} | \\ C \leftarrow VE(k\ msg\ E_j \notin \{E_i\}_{1 \leq i \leq n})\} \\ = \epsilon$$

2. V will not have any knowledge about the plaintext msg after the verification test

3. *Targeted Decipherability.*
If both P and V are honest. at the execution of the `Decryption` algorithm, the plaintext msg can always be obtained. We require

$$\Pr \quad \{msg \text{ is valid} \\ C \leftarrow VE(k, msg, E_j \in \{E_i\}_{1 \leq i \leq n}), \\ msg \leftarrow Decrypt(C, D_j)\} \\ = 1$$

4 *Anonymity:*
Having observed several C's. V cannot observe to whom a ciphertext is diiectcd to.

4.2. Security Notions

In terms of security of PV1nE scheme. we need to consider two types of attackers. namely *outsider* and ***insider*** attacks We call an attack to be an *insider* attack **if** the attack is launched by an adversary who either compromises one of the player in the system, namely a receiver R_i, $i = 1, \ldots n$. a sender or a gateway We will describe the attacks launched by these players in more detail later. An outsider attack is an attack that **is** performed by an "outsider", who is not one of the player in the system. Formally, we define these attacks as follows

Outsider Attacks
Let ***A*** be an outside attacker, whose running time is bounded by t, that is polynomial in a security parameter k. We require that

$$\texttt{Pr}_{A(t,k)}[m \quad | \quad C \leftarrow VE(k, msg, E_j \notin \{E_i\}_{1 \leq i \leq n}), \\ \texttt{True} \leftarrow Ver(C, \mathcal{PK})] \leq \epsilon$$

Insider Attacks
In the following, we define three differen: attacks launched by insiders We relate these attacks with the sccurity notions for the participants in the system

Security for the Sender
Informally, the security for the sender is defined as follows We require that if a message is encrypted and directed for user R,, $1 \leq i \leq n$, then any other receiver R_j, $j \neq i$, will not he able to read the encrypted message We require that

$$\texttt{Pr}_{A(t,k)}[m \quad | \quad x_j, C \leftarrow VE(k, msg, E_i, i \neq j), \\ \texttt{True} \leftarrow Ver(C, \mathcal{PK})] \leq \epsilon$$

Slyurity for the Verifier
The main role of the verifier is to make sure that the encrypted message is directed to one of the receivers in the group Hence, informally, the security for the verifier is defined a5 follows Consider an attacker ***A*** who would like to send an encrypted message to a person, R_z, $z \notin (1 \ldots n\}$. His intention is to make the verifier believes that this message **is** intended to one of the receiver R_i, $1 \leq i \leq n$

We say this attack is successful, if the receiver believes that the mecsage **is** directed to one of the R_i $1 \leq i \leq n$. Intuitively, this attack is explained as follows The attacker wants to "flood" the server with junk messages, so that at some stage. the server will collapse since the messages will be stored forever in the server, but no receiver will retrieve it. The success probability of this attack is bounded by

$$\begin{aligned} \texttt{Succ}_{\mathcal{A}}(k) &= \Pr\{Ver(C, \{E_i\}_{1 \leq i \leq n}, \forall i) = \texttt{True} | \\ & C \leftarrow VE(k, msg, E_j \not\subset \{E_i\}_{1 \leq i \leq n})\}. \end{aligned}$$

Wc note that this security notion is related to the first security rcquircmcnt mentioned earlier. We also note that this attack is often referred to *Denial of Service* attack.

Security for the Receiver
In this attack, the attacker ***A*** controls the verifier and tries to *sabotage* encrypted message directed to a receiver R_j, $1 \leq j \leq n$. Intuitively, 4 **would** like to *reject* valid encrypted messages directed to R_j, but he will accept all other valid encrypted messages directed to different receivers Wc formally define this security notion as "IND-PV1nE-SCCA" (**SCCA** = "Signer Chosen Ciphertext Attack") as follows

Definition 5 (IND-PV1nE-SCCA). *Let **A** be an attacker whose running time is bounded by t, that* **is** *polynomial in a security parameter k. **A** controls the view* **of** *the verifier:* **We** *consider the following game:*

S1: *The* Setup *algorithm is run. A public parameters, p, q are generated. A set of private keys of the receivers x_i are generated, and the public keys $h_i = g^{x_i} \pmod{p}$, for $1 \leq i \leq n$ are published.*

S2: *$\mathcal{A}$ can query the encryption and decryption oracle for a message/ciphertext of his choice.*

S3: *$\mathcal{A}$ outputs a target message m^* and two receivers R_1, R_2, and sends it to the encryption oracle. The encryption oracle chooses $\beta \in \{1,2\}$ uniformly at random and creates a target ciphertext C_i^* that is an encrypted version of m^* directed to the receiver R_β and returned it to $\mathcal{A}$.*

S4: *$\mathcal{A}$ can issue some other ciphertexts C_i and message m_i and ask the decryption oracle to* **decrypt** *the message. The restriction here is $m_i \neq m^*$.*

S5: *$\mathcal{A}$ outputs its guess $\beta' \in \{1, 2)$.*

We define the attacker *A's* success by the probability $\texttt{Succ}_{\mathbf{A}}^{\texttt{IND--PV1nE SCCA}}(\texttt{k}) = \texttt{Pr}[\beta = \beta']$. $PV1nE$ scheme is said to be IND-PV1nE-SCCA secure if $\texttt{Succ}_{\mathcal{A}}^{\texttt{IND-PV1nE-SCCA}}(\texttt{k})$ is negligible in k.

4.3. The Scheme

In this section, we propose non-interactive PV1nE schemes based on the building blocks developed in the previous section The scheme is 35 follows

- `Setup`·
  Let q be a large prime and $p = 2q + 1$ Let G be a cyclic group of order p and g be an elcinent of $\mathbb{Z}_p^*$ with order q Each receiver R_i, $1 \leq i \leq n$, selects a random number $x_i \in \mathbb{Z}_q$ and sets his public key to $h_i = g^x \bmod p$
- `Verifiable Encrypticn`(VE):
  To encrypt a message $m \in \{0,1\}^*$ under the public key h_i & $\mathbb{Z}_p^*$ (that is one of h_1 h_2 h_n), the `Prover` does the following
  1 Selects a random element y from G;
  2 Computes $v = \hat{g}^m \in G$, $\boldsymbol{A} = g^\alpha \bmod p, B = m^{-1} h_i^\alpha \bmod p$
  3. Sets the ciphertext to be.

$$\begin{aligned} C = & [h_1 \quad h_n, g \; v, A, B, \\ & SPK2LOG(1 \; n)\{\alpha \quad A = g^\alpha \wedge \\ & v^B = \hat{g}^{h_1^\alpha} \vee \hat{g}^{h_2^\alpha} \quad \vee \hat{g}^{h_i^\alpha}\}(\iota)] \end{aligned}$$

- `Verification`(Ver)
  To verify a ciphertext, the `Verifier` tests whether

$$SPK2LOG(1, n)\{\alpha \quad \begin{aligned} & A = g^\alpha \wedge \\ & v^B = g^{h_1^\alpha} \vee \hat{g}^{h_2^\alpha} \\ & \vee \hat{g}^{h_n^\alpha}\}(\iota) \end{aligned}$$

  is correct If it is correct, then it outputs `True`. Otherwise. it outputs –
- `Decryption`(Dec)
  A receiver R_i $1 \leq i \leq n$, who holds the correct secret key D, associated with E_i can decrypt the message by computing

$$m = A^{x_i}/B$$

  Then. R_i needs to verify whether $v = \hat{g}^m$ holds. If it holds **with** equality, then R_i obtains the plaintext m.

4.4. Security Analysis

Theorem 1 (Security against Outsider Attacks). *If there exists a polynomial time algorithm to decrypt a ciphertext without any knowledge of a secret* key x_i, $1 \leq i \leq n$*, then Decisional Diffie-Hellman problem can be solved in polynomial time.*

Theorem 2 (Security for the Sender). *The probability of a polynomially bounded attacker $\mathcal{A}$ to decrypt a ciphertext directed to the receiver R_i, given a valid secret key* of x_j, $j \neq i$, is *negligible.*

Theorem 3 (Security for the Verifier).
There is no polynomially bounded attacker $\mathcal{A}$ who has $\mathrm{Succ}_{\mathcal{A}}(\mathrm{k}) \geq \epsilon$*, for a polynomial time t, and can break the security for the verifier in the $PV1nE$ scheme.*

Theorem 4 (Security for the Receiver).
Our scheme is secure in the sense of IND-PV1nE-SCCA.

The proofs are omitted due to space limitation.

5. An Extension: The Sender from A Ring

Model

As motivated in Section 1, the PVRTF scheme can be used to provide sender's (or prover's) privacy In PVRTE schemes the identity ofthe prover is ambiguous The prover can send an encrypted message on behalf of the group To make the model clearer, we assume there are n_p eligible provers (or senders, resp), denoted as P_i, $i = 1 \quad n_p$ The collection of provers is denoted as $\{P_i\}_{1 \leq i \leq n_i}$ There are n receiveis in the group, denoted as $R,$, $i = 1. \quad ,n$. The collection ol'receivers is denoted as $\{R_j\}_{1 < j \leq n}$.

Any P_i can send a message on behalf of the group $\{P_i\}_{1 \leq i \leq n_p}$ This encrypted message will then be verified by the verifier V

V docs not know about the identity ofthe prover P_i, but V can be assured that the encrypted message was send by $P_i \in \{P_j\}_{1 \leq j \leq n}$ and this encrypted message is intended to a receiver $R_i \in \{R_i\}_{1 \leq i < n}$ If V is assured with this tact. then the encrypted message is stored until it is retrieved by the designated verifier R Finally. $R, \in \{R_j\}_{1 \leq j \leq n}$ can retrieve the stored encrypted message by using his secret **key**

The Generic Construction for PVRTE Schemes

In this section, we provide a generic construction for PVRTE schemes from PV1nE schemes and ring signature schemes We will incorporate the following notations

- A PV1nE scheme consists of three main algorithms, namely `Verifiable Encryption` (VE), `Verification` (Ver) and `Decryption` (Dec)
- A PVRTE scheme consists of three main algorithms, namely `Verifiable Ring Encryption` (VRE) and `Ring Verification` (RV).
- Let $\mathcal{SK}_{U_i}$ denote U_i's secret key, and $\mathcal{PK}_{U_i}$ denote U s public key

The generic construction is as follows

- $\mathrm{VRE}(m, \{\mathcal{PK}_{\{P_j\}_{1 \leq j \leq n_p}}\}, \mathcal{SK}_{P_i}, \mathcal{PK}_{\{R_i\}_{1 \leq i \leq n}})$
$$\stackrel{\mathrm{def}}{=} \begin{cases} \gamma \leftarrow VE(m, \{\mathcal{PK}_{\{R_i\}_{1 \leq i \leq n_p}}\}, \mathcal{PK}_V) \\ \eta \leftarrow \mathcal{S}(\gamma, \mathcal{SK}_{P_i}, \mathcal{PK}_{\{P_j\}_{1 \leq j \leq n_p}}) \\ Output : (\gamma. \eta) \end{cases}$$
The Verifiable Ring Signature on m is the double $(\gamma. \eta)$.

- $RV(\gamma. \eta) \stackrel{\mathrm{def}}{=} \begin{cases} \texttt{Test1} \leftarrow \mathcal{V}(\gamma, \eta, \mathcal{PK}_{\{P_i\}_{1 \leq i \leq n_p}}) \\ \texttt{Test2} \leftarrow Ver(\gamma \ \mathcal{PK}_{\{R_i\}_{1 \leq i \leq n}}) \\ return(\texttt{Test1} \ and \ \texttt{Test2}) \end{cases}$
The result of this verification is either True or $\perp$
- If it returns True in the preceding step. compute $Dec(\gamma)$

We note that similar result can be obtained by employing a ring signcryption scheme. Since the main contribution of this paper is *to* demonstrate how to extend our PV1nE to PVRTE. then we will omit the detail of the ring signcryption scheme in this paper

6. Conclusion

We presented a new scerne *non-interactive publicly verifiable 1-out-of-n encryption* Our scheme is based on the non-interactive signature based on proof of knowledge on equality of discrete logarithms and double discrete logarithms that was proposed in this paper Our scheme can be easily extended *to* provide *sender anonymity*. that cannot be obtained using interactive schemes developed in the previous work We showed how to achieve it by combining a ring signature scheme with our non-interactive publicly verifiable 1-out-of-n encryption scheme

References

[1] M. Abe, M. Ohkubo, and K. Suzuki. 1-out-of-n Signatures from a Variety of Keys. *Adv in Cryptology - Asiacrypt 2002, LNCS 2501*, pages 415 – 432.2002.

[2] J Camenisch. Efficient and generalized group signatures. *Adv in Cryptology - Eurocrypt* '97, *LNCS 1233*. pages 465–479. 1997.

[3] J Camenisch. Group signature schemes and payment systems based on the discrete logarithm problem. *PhD thesis. ETH Zürich*, 1998.

[4] J. Camenisch and I. B. Damgård Verifiable encryption. group encryption. and their applications to separable group signatures and signature sharing schemes. *Asiacrypt 2000, LNCS* 1976.pages 331–345, 2000.

[5] J. K. Liu, V. K. Wei. and D. S. Wong. Verifiable encryption in anonymous ad hoc groups *Cryptology ePrint Archive, Report 2004/028*, 2004.

[6] J. K Liu, V. K. Wei, and D. S. Wong. Custodian-Hiding Verifiable Encryption. *Workshop on Information Security Applications (WISA 2004)*, 2004.

[7] D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, *2000*.

[8] M O. Rabin. Digitalized signatures. *Foundations of Secure Computations*, **Academic** *Press*. 1978.

[9] R. L. Rivest, A. Shamir, and Y. Tauman. How to Leak a Secret. *Adv in Cryptology - Asiacrypt 2001, LNCS 2248*, pages 552 – 565,2001.