

Uncorrelatable Electronic Transactions using Ring Signatures

Partha Das Chowdhury, Bruce Christianson,
Computer Science Department
University of Hertfordshire
England
{P.Das-Chowdhury, B.Christianson}@herts.ac.uk

December 5, 2003

1 Introduction

The Internet is conducive to large scale privacy invasion, identity theft [7], and target marketing [4]. We have seen instances in the past where people have suffered serious damage to the ready availability of digital dossiers [5]. Any centrally stored information can be abused. The use of fixed credentials (credit cards, key certificates) enables an adversary to correlate all the transactions conducted with the fixed credential. The threats of identity theft, correlatability can be countered using anonymous transaction protocols. Here we present a protocol for uncorrelatable electronic transaction based on ring signatures which also guards against identity theft as well as protects the privacy of the communicating partners. The organization of this paper is as follows. In section 2 we present the threat model which we are considering. This is followed in section 3 by an overview of ring signatures. In Section 4 we present our design goals and assumptions. The protocol which is the contribution of this paper is presented in section 5, which is followed by conclusions in section 6.

2 The Threat Model

When we buy goods or services or simply surf online we end up giving out lots of information about ourselves. All this information goes into databases somewhere. These records can be linked together to build a complete dossier

on an individual [7]. Thieves can steal credit card information and use it, terrorists can track their targets using government maintained address records, or servers at the other end can leak sensitive information about us. In many instances in the past people have suffered damage due to the malicious use of sensitive information [10], [9]. When we pay for goods using our credit card we present our card (which is the payment token) along with our identity (we provide our name and address for authorisation on the internet). This information is used to check the validity of the card and the creditworthiness of the customer. In other applications trustworthiness of communicating partners are established using certificates, a good example of which is the Globe System [11]. Using same fixed certificates to establish the trustworthiness of the communicating partners enables the grantor of access to any service to correlate all the transactions of a requestor. What happens in the process is that the merchant, in the case of online shopping, also obtains a unique identifier (the credit card number) which, as well as learning the credit card number, enables the merchant to correlate various transactions conducted under the same credit card. Customer information can be indexed using credit card numbers or they can be sold to marketing companies [4].

The problem is that we don't have a clue about how information about us would be used by the entities at the other end of the communication channel.

3 Ring Signatures

Ring signatures were designed Ron Rivest, Adi Shamir and Yael Tauman [6]. In this signature scheme the verifier doesn't learn who the signer is but can only learn that the signer is a member of group of certain possible signers called a ring. One of the members of the ring actually signs using his/her private key and the public keys of the other members. The example cited in [6] speaks of a situation where a government minister wants to leak information to a journalist. The journalist knowing the public keys of all the ministers can be sure that one of the ministers signed it without knowing who is the mole in the cabinet. In producing such a signature the signatory doesn't need the cooperation of any member of the group. All the signer needs to know is the public keys of all the members of the group. Let there be r members in the group. The signature is generated as:

1. The signer first computes the key as the hash of the message m to be signed.

2. Then the signer generates a random initialization value v .
3. The signer generates a random value x_i for each member of the group and computes y_i which is x_i encrypted with the public key of that ring member.
4. Then the signer solves the equation $F_{k,v}(y_1, y_2, \dots, y_r) = v$ for y_s where F is a combining equation.
5. Now the signer uses his private key in order to invert g_s on y_s to obtain x_s as $x_s = g_s^{-1}(y_s)$
6. The output of the signature is the set of values x_i , the random value v , and the public keys of the group members.

A ring signature can be verified as follows:

1. For each member of the group, we encrypt the the corresponding random value x_i with that member's public key to give y_i .
2. We obtain the hash of the message to obtain the key k as $k = h(m)$.
3. We verify that the combining equation F regenerates the random value v in Z_P .

4 Design Goals and Assumptions

4.1 Design Goals

We present a protocol for Uncorrelatable Electronic Transaction (UET) where we use surrogates. Our approach makes it hard for an adversary to correlate all the transactions conducted by the same customer. The transaction flow is outlined by means of an example as:

1. The bank prepares and sends the information Cathy needs to generate her surrogates.
2. Cathy goes to a website selling goods she wants to purchase.
3. Cathy generates the surrogate for the current transaction.
4. The seller authenticates locally whether or not Cathy is a valid customer of the bank.

5. The seller sends the customer information to the bank.

The next time Cathy goes to shop with the same seller she uses a different surrogate which can be verified as before but cannot be correlated with a previous surrogate. Our motivation has been that Cathy trusts her bank which is quite a practical thing to do. There is no communication between the bank and the seller for authorisation of payments and the seller can locally verify the validity of the customer.

4.2 Cryptographic and Infrastructural Assumptions

Communications between the bank and its clients (the customer and the seller) are not anonymous. We assume the existence of a secure authenticated communication channel between the bank and the seller and between the bank and the customer. This can be implemented by digital signatures where every communication between the bank and the customer and the bank and the seller are digitally signed. This provides authentication. The communication link between the customer, bank and the seller can be secured by for example SSL/TLS. All communications between the bank and the seller and between the bank and the customer are secured in this way.

An anonymous communication channel between the seller and the customer is also assumed for our purposes. This can be implemented by Chaum's mix nets [1] or Mixminion [2]. The mix network makes it harder for an adversary observing the network to gain any additional information about the communicating partners beyond its a priori belief. The communication channel between the customer and the entry point of the mix network should also be secure and prevent traffic analysis. Communications between the customer and the seller are made anonymous in this way.

4.3 Mathematical Assumptions

Our protocol depends on the difficulty to compute discrete logarithms in the multiplicative group Z_P^* where P is a large prime. P should be chosen such that $(P - 1)$ has one large prime factor. If $(P - 1)$ has small prime factors then computing discrete logarithm is easy [3]. The bank selects $A, O_\sigma \in Z_P^*$ and $\sigma_0 \in \{1..P - 1\}$.

The customer selects generator $g \pmod{P}$ and $s \in Z_P^*$, s is the secret key of the customer. We use the Linear Congruential Method to generate exponents where the offset O_σ and the modulus P are co-prime to each other. All operations are carried out \pmod{P} when not specified otherwise

explicitly. The method we use to generate surrogates is similar to the first group signature scheme presented in [8].

5 Protocol for Uncorrelatable Transactions

There are three parties in the protocol, the bank, the customer (Cathy) and the seller. We describe the protocol in three phases:

1. Preparation Phase
2. Transaction Phase
3. Synchronization Phase

5.1 Preparation Phase

Cathy sends the bank her public key.

1. *Cathy* \longrightarrow *Bank* : $X = g^s$

The bank sends Cathy the information she needs to generate her surrogates which is :

2. *Bank* \longrightarrow *Cathy* : $\delta = \prec \sigma_0, O_\sigma, A \succ$

The bank while issuing δ calculates the first surrogate the customer will be using as follows.

$$\begin{aligned} \sigma_1 &= (A * \sigma_0 + O_\sigma) \pmod{P-1} \\ S_1 &= X^{\sigma_1} \end{aligned}$$

The bank retains Δ for every customer where

$$\Delta = \prec O_\sigma, A, X, S_1, \sigma_1, P \succ$$

5.2 Transaction Phase

For transaction i Cathy calculates her surrogate S_i as well as the corresponding secret key in the following manner.

$$\begin{aligned}\sigma_i &= (A * \sigma_{i-1} + O_\sigma) \pmod{P-1} \\ S_i^- &= s * \sigma_i \pmod{P-1} \\ S_i^+ &= g^{S_i^-}\end{aligned}$$

1. Cathy chooses a subset r of the public surrogates of valid customers of the bank. The subset agreed forms the ring or the group of probable signers.
2. Let m be the transaction description something which uniquely identifies the transaction. Then Cathy hashes m to get the key k as:

$$k = h(m)$$

3. She selects a random number $v \in Z_P^*$.
4. The seller picks up $x_{1..r}$ for all the members of the group uniformly and independently from $\{0, 1\}^b$ and sends that to Cathy. She computes y_i s from the x_i s as:

$$\begin{aligned}Seller &\longrightarrow_{mix} Cathy : x_{(1..r)} \\ & y_i = g_i(x_i)\end{aligned}$$

5. Then the customer solves F for y_s where F is the same combining equation used in ring signatures.

$$F_{k,v}(y_1, y_2, \dots, y_r) = v$$

6. The customer then signs m and sends it to the seller as in the original ring signature scheme.

$$Customer \longrightarrow_{mix} Seller : (S_1, S_2, \dots, S_r; v; x_1, x_2, \dots, x_r)$$

where $S_{1..r}$ are the surrogate DH keys of the r valid customers of the bank who are members of the ring.

7. The seller then verifies the signature as mentioned in section 3. While verifying the seller gets the S_i which is the surrogate of the customer. The seller submits S_i to the bank. The bank locates the customer account S_i .

5.3 Synchronization Phase

We saw in the preparation phase that the bank retains the value of the first surrogate while issuing Δ to the customer. The bank, after it receives a surrogate for a customer, calculates and stores the surrogate the customer will be using for the next transaction. This helps the bank to locate the appropriate account after it receives a surrogate from the seller. The bank retains Y for every customer as we have seen in the preparation phase. Both the bank and the customer uses the same method to generate surrogates. This enables the bank to calculate the correct surrogate for every customer. This calculation of surrogates is done in this phase.

$$\begin{aligned}\sigma_{i+1} &= (A * \sigma_i + O_\sigma) \pmod{P - 1} \\ S_{i+1} &= X^{\sigma_{i+1}}\end{aligned}$$

The bank replaces in Δ .

$$\begin{aligned}\sigma_i &\longleftarrow \sigma_{i+1} \\ S_i &\longleftarrow S_{i+1}\end{aligned}$$

The bank updates its current list of valid surrogates with a new surrogate.

6 Conclusions

The use of various surrogates cannot be correlated with each other but at the same time the validity of the surrogates can be determined. It is also not possible for the bank to masquerade as the customer as the bank doesn't know s and cannot generate the private exponent. Surrogates cannot be transferred between customers as that requires sharing the secret key s .

References

- [1] David Chaum, Untraceable Electronic Mail Return Addresses and Digital Pseudonyms, Technical Report Programming Techniques and Data Structures R. Rivest eds.
- [2] George Danezis, Roger Dingledine, Nick Mathewson, Mixminion: Design of Type III Remailer, IEEE Security and Privacy 2003
- [3] S.Pohlig, M. Hellman, An improved algorithm for computing logarithms over $GF(P)$ and it's cryptographic significance, IEEE Transactions on Information Theory, vol IT-24 pp 106-110, 1978
- [4] Andrew Odylzko, Privacy Economics and Price Discrimination on the Internet,Fifth International conference on Electronic Commerce, N. Sadah eds, pp 355-366, ACM 2003
- [5] Bob Sullivan, The darkest side of ID theft, MSNBC news available as <http://www.msnbc.com/news/877978.asp>, 9th March, 2003
- [6] Ronald Rivest, Adi Shamir, Yael Tauman, How to Leak a Secret,Proceedings of Asiacrypt, pp 552-565, 2001
- [7] D.Chaum,Achieving Electronic Privacy, Appeared in the Scientific American ,pp 96-101, August 1992
- [8] David Chaum,Eugene Van Heyst, Group Signatures, Lecture Notes in Computer Science, Volume 547/1991 Eurocrypt, Workshop on Theory and application of Cryptographic Techniques, 1991
- [9] Tax Records for Sale Scandal, 16th, BBC news available as <http://news.bbc.co.uk/1/hi/business/2662491.stm>, January 2003
- [10] Ross Anderson, Security Engineering, Wiley Publications published 2001
- [11] Bogdan Popescu, Martin Van Steen, Andrew S. Tanenbaum, A Security Architecture for Object Based Distributed System, Proceedings of the 18th Annual Computer Security Applications Conference, December 2002