WIKIPEDIA

Ring signature

In cryptography, a **ring signature** is a type of digital signature that can be performed by any member of a group of users that each have keys. Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people. One of the security properties of a ring signature is that it should be computationally infeasible to determine *which* of the group members' keys was used to produce the signature. Ring signatures are similar to group signatures but differ in two key ways: first, there is no way to revoke the anonymity of an individual signature, and second, any group of users can be used as a group without additional setup. Ring signatures were invented by Ron Rivest, Adi Shamir, and Yael Tauman, and introduced at ASIACRYPT in 2001.[1] The name, *ring signature*, comes from the ring-like structure of the signature algorithm.

Contents

Definition

Suppose that a group of entities each have public/private key pairs, (P_1, S_1), (P_2, S_2), ..., (P_n, S_n). Party i can compute a ring signature σ on a message m, on input $(m, S_i, P_1, ..., P_n)$. Anyone can check the validity of a ring signature given σ, m, and the public keys involved, $P_1, ..., P_n$. If a ring signature is properly computed, it should pass the check. On the other hand, it should be hard for anyone to create a valid ring signature on any message for any group without knowing any of the private keys for that group.[2]

Applications and modifications

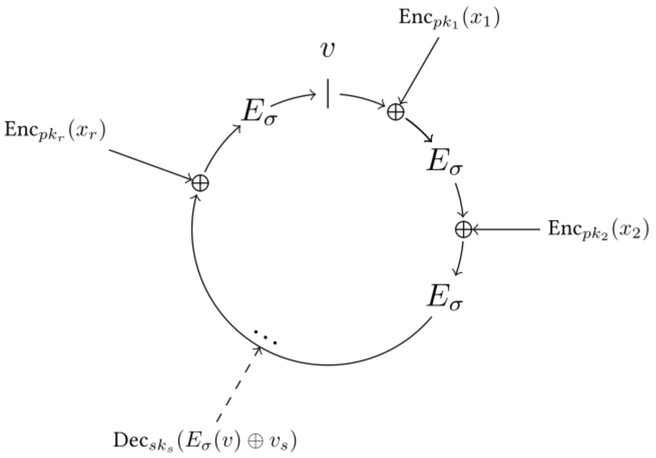
In the original paper, Rivest, Shamir, and Tauman described ring signatures as a way to leak a secret. For instance, a ring signature could be used to provide an anonymous signature from "a high-ranking White House official", without revealing which official signed the message. Ring signatures are right for this application because the anonymity of a ring signature cannot be revoked, and because the group for a ring signature can be improvised.

Another application, also described in the original paper, is for deniable signatures. Here the sender and the recipient of a message form a group for the ring signature, then the signature is valid to the recipient, but anyone else will be unsure whether the recipient or the sender was the actual signer. Thus, such a signature is convincing, but cannot be transferred beyond its intended recipient.

There were various works, introducing new features and based on different assumptions:

Threshold ring signatures

[3] Unlike standard "*t*-out-of-*n*" threshold signature, where *t* of *n* users should collaborate to decrypt a message, this variant of a ring signature requires *t* users to cooperate in the signing protocol. Namely, *t* parties (i_1, i_2, ..., i_t) can compute a (*t*, *n*)-ring signature, σ, on a message, *m*, on input (*m*, S_{i_1}, S_{i_2}, ..., S_{i_t}, P_1, ..., P_n).


$\mathrm{Enc}_{pk_1}(x_1)$
v
E_σ
$\mathrm{Enc}_{pk_r}(x_r)$
E_σ
$\mathrm{Enc}_{pk_2}(x_2)$
E_σ
$\mathrm{Dec}_{sk_s}(E_\sigma(v) \oplus v_s)$

Behaviour of the Rivest, Shamir, Tauman ring signature scheme

Linkable ring signatures

[4] The property of linkability allows one to determine whether any two signatures have been produced by the same member (under the same private key). The identity of the signer is nevertheless preserved. One of the possible applications can be an offline e-cash system.

Traceable ring signature

[5] In addition to the previous scheme the public key of the signer is revealed (if they issue more than one signatures under the same private key). An e-voting system can be implemented using this protocol.

Efficiency

Most of the proposed algorithms have asymptotic output size $O(n)$; i.e., the size of the resulting signature increases linearly with the size of input (amount of public keys). That means that such schemes are impracticable for real use cases with sufficiently large n (for example, an e-voting with millions of participants). But for some application with relatively small median input size such estimate may be acceptable. CryptoNote implements $O(n)$ ring signature scheme by Fujisaki and Suzuki[5] in p2p payments to achieve sender's untraceability.

More efficient algorithms have appeared recently. There are schemes with the sublinear size of the signature,[6] as well as with constant size.[7]

Implementation

Here is a Python implementation of the original paper using RSA.

```
import os, hashlib, random, Crypto.PublicKey.RSA

class ring:
    def __init__(self, k, L=1024):
        self.k = k
        self.l = L
        self.n = len(k)
        self.q = 1 << (L - 1)

    def sign(self, m, z):
        self.permut(m)
        s = [None] * self.n
        u = random.randint(0, self.q)
        c = v = self.E(u)
        for i in (range(z+1, self.n) + range(z)):
            s[i] = random.randint(0, self.q)
            e = self.g(s[i], self.k[i].e, self.k[i].n)
            v = self.E(v^e)
            if (i+1) % self.n == 0:
                c = v
        s[z] = self.g(v^u, self.k[z].d, self.k[z].n)
        return [c] + s

    def verify(self, m, X):
        self.permut(m)
        def _f(i):
            return self.g(X[i+1], self.k[i].e, self.k[i].n)
        y = map(_f, range(len(X)-1))
        def _g(x, i):
            return self.E(x^y[i])
        r = reduce(_g, range(self.n), X[0])
        return r == X[0]

    def permut(self, m):
        self.p = int(hashlib.sha1('%s' % m).hexdigest(),16)

    def E(self, x):
        msg = '%s%s' % (x, self.p)
        return int(hashlib.sha1(msg).hexdigest(), 16)

    def g(self, x, e, n):
        q, r = divmod(x, n)
        if ((q + 1) * n) <= ((1 << self.l) - 1):
            rslt = q * n + pow(r, e, n)
        else:
            rslt = x
        return rslt
```

To sign and verify 2 messages in a ring of 4 users:

```
size = 4
msg1, msg2 = 'hello', 'world!'

def _rn(_):
  return Crypto.PublicKey.RSA.generate(1024, os.urandom)

key = map(_rn, range(size))
r = ring(key)
for i in range(size):
    s1 = r.sign(msg1, i)
    s2 = r.sign(msg2, i)
    assert r.verify(msg1, s1) and r.verify(msg2, s2) and not r.verify(msg1, s2)
```

Crypto-currencies

The CryptoNote technology uses ring signatures.[8] It was first implemented by Bytecoin (BCN) in July 2012.[9]

The cryptocurrency ShadowCash uses traceable ring signature to anonymize the sender of a transaction.[10] However, these were originally implemented incorrectly, resulting in a partial de-anonymization of ShadowCash from their first implementation until February 2016 by Monero Research Labs researcher, Shen Noether.[11] Luckily only 20% of all the one-time keys in the system were affected by this bug, sender anonymity was compromised but receiver anonymity remained intact. A patch was submitted in a timely fashion to resolve the bug. [12]

References

1. *How to leak a secret* (http://www.springerlink.com/content/kxkndv9rgk8lu3h9/), Ron Rivest, Adi Shamir, and Yael Tauman, ASIACRYPT 2001. Volume 2248 of Lecture Notes in Computer Science, pages 552–565.
2. Debnath, Ashmita; Singaravelu, Pradheepkumar; Verma, Shekhar (19 December 2012). "Efficient spatial privacy preserving scheme for sensor network". *Central European Journal of Engineering*. **3** (1): 1–10. doi:10.2478/s13531-012-0048-7 (https://doi.org/10.2478%2Fs13531-012-0048-7).

3. E. Bresson; J. Stern; M. Szydlo (2002). "Threshold ring signatures and applications to ad-hocgroups" (http://www.di.ens.fr/~bresson/papers/BreSteSzy02.pdf) (PDF). *Advances in Cryptology: Crypto 2002*: 465–480.
4. Liu, Joseph K.; Wong, Duncan S. (2005). "Linkable ring signatures: Security models and new schemes". *ICCSA*. **2**: 614–623. doi:10.1007/11424826_65 (https://doi.org/10.1007%2F11424826_65).
5. Fujisaki, Eiichiro; Suzuki, Koutarou (2007). "Traceable Ring Signature". *Public Key Cryptography*: 181–200.
6. Fujisaki, Eiichiro (2011). "Sub-linear size traceable ring signatures without random oracles". *CTRSA*: 393–415.
7. Au, Man Ho; Liu, Joseph K.; Susilo, Willy; Yuen, Tsz Hon (2006). "Constant-Size ID-Based Linkable and Revocable-iff-Linked Ring Signature". *Lecture Notes in Computer Science*. **4329**: 364–378. doi:10.1007/11941378_26 (https://doi.org/10.1007%2F11941378_26).
8. CryptoNote Technology - Untraceable payments (https://cryptonote.org/inside#untraceable-payments)
9. Bytecoin profile (http://bravenewcoin.com/profiles/coins/bytecoin/) Bravenewcoin.com
10. Shadow - Zero-knowledge Anonymous Distributed Electronic Cash via Traceable Ring Signatures (http://shadow.cash/downloads/shadowcash-anon.pdf)
11. Broken Crypto in Shadowcash (https://shnoe.wordpress.com/2016/02/11/de-anonymizing-shadowcash-and-oz-coin/)
12. https://blog.shadowproject.io/2016/03/07/development-update-march-phoenix/

Retrieved from "https://en.wikipedia.org/w/index.php?title=Ring_signature&oldid=795547045"

This page was last edited on 14 August 2017, at 22:55.