

Re: Encryption with broadcast-only server-timed release

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-08/1915.html>

From: David Wagner (daw_at_taverner.cs.berkeley.edu)

Date: 08/28/04

Date: Sat, 28 Aug 2004 17:07:50 +0000 (UTC)

Francois Grieu wrote:

>I am wondering if a cryptosystem can be setup that achieves the
>following "broadcast-only server-timed release":

>

>- A trusted server is setup; it publishes parameters and
> public key PK , then regularly a "timed release" value
> TR_p , with p increasing from 0, say each day. The server
> never receives any information.

>

>- Encrypters can use PK and p to encrypt a message M to
> $C = ENC(M, PK, p)$, and publish it independently of the
> server.

>

>- Decrypters having obtained C can decipher it back into M
> only with the help of TR_p when it is published, as
> $M = DEC(C, PK, TR_p)$ [preferably: that should work using
> any TR_q for $q \geq p$, rather than just TR_p]

Sure. Let PK be the master public key for an identity-based cryptosystem generated by the server. Let TR_p be the private key corresponding to identity p , as generated by the server. This achieves all of your requirements except the one in square brackets. I don't know how to satisfy the bracketed requirement, but perhaps there is a way.

I haven't read the eprint article you refer to, so I don't know what they do.