The Interval Revocation Scheme for Broadcasting Messages to Stateless Receivers

Anna Zych, Milan Petković, and Willem Jonker

Philips Research, Eindhoven, The Netherlands
anusiek@gmail.com,{milan.petkovic,willem.jonker}@philips.com

The Broadcast Encryption methods, often referred to as revocation schemes, allow data to be efficiently broadcast to a dynamically changing group of users. A special case is when the receivers are stateless [2,1]. Naor et al. [2] propose the Complete Subset Method (CSM) and the Subset Difference Method (SDM). Asano [1] puts forth two other methods, AM1 and AM2, which use public prime parameters to generate the decryption keys. The efficiency of broadcast encryption methods is measured by three parameters: (i) message size - the number of transmitted ciphertexts; (ii) storage at receiver - the number of private keys each receiver is required to store; and (iii) key derivation time - the computational overhead needed to access the decryption keys.

Let $\mathcal{N} = \{u_0, ..., u_{N-1}\}$ be the set of N receivers and $\mathcal{R} \subset \mathcal{N}$ be a group of r users whose decryption privileges should be revoked. The aim of a revocation scheme is to allow a transmission of a message M to all users in such a way, that any user $u \in \mathcal{N} \setminus \mathcal{R}$ can decrypt the message correctly, while even a coalition consisting of all members of $\mathcal{R}$ can not decrypt it.

We propose a new revocation scheme for transmitting secret messages to stateless receivers. In comparison to other schemes, our scheme improves private storage to one key per receiver and the size of the message to the number of revoked receivers r, while the time needed for deriving a key is of order of a logarithm of the number of all receivers $O(\log N)$. We push the storage requirements to the public space of N^2 parameters that are needed to derive the keys. We provide the comparison of CSM, SDM, AM1 and AM2 methods with our method in Table 1.

Table 1. Performance of methods in [2,1]

	CSM [2]	SDM [2]	AM1 [1]	AM2 [1]	Our method
Message size	$r \log \frac{N}{r}$	$2r-1$	$r(\frac{\log \frac{N}{r}}{log a}+1)$	$r(\frac{\log \frac{N}{r}}{log a}+1)$	r
Storage at rec.	$\log N$	$\frac{\log^2 N}{2}$	1	$\frac{\log N}{\log a}$	1
Key der. time	-	$O(\log N)$	$O(\frac{(2^{a-1}-1)\log N}{\log a})$	$O(2^{a-1}-1)$	$O(\log N)$

A typical revocation scheme (compliant to the framework provided in [2]) defines a collection of subsets $\mathcal{X} = S_1, ..., S_w, S_j \subseteq \mathcal{N}$. Each subset S_j is assigned a long-lived secret key K_j. Each user $u \in S_j$ should be able to deduce K_j from secret information assigned to her during the initiation phase. Deducing K_j however should be infeasible for any coalition of users $\{u_1 \dots u_t\} \subset \mathcal{N} \setminus S_j$. Given a revoked set $\mathcal{R}$, the remaining

S. Barker, G.-J. Ahn (Eds.): Data and Applications Security 2007, LNCS 4602, pp. 95–97, 2007.

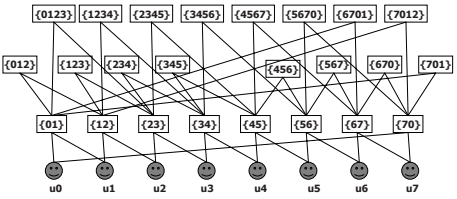

Fig. 1. Example of a digraph restricted to intervals of size $1 \ldots 4$

users $\mathcal{N} \setminus \mathcal{R}$ are partitioned into $S_{i_1}, \ldots, S_{i_m}$ so that $\mathcal{N} \setminus \mathcal{R} = \bigcup_{j=1}^{m} S_{i_j}$ and a session key K is encrypted m times with (hash values) of $K_{i_1}, \ldots K_{i_m}$. Such header is broadcasted together with the content encrypted with the session key. In the scheme's initiation phase, every receiver u is assigned private information $I[u]$, which allows to compute K_j for each group S_j such that $u \in S_j$.

Thus, a particular scheme is specified by the collection of subsets $\mathcal{X}$, a method to assign the keys to each subset of the collection, a method to cover non-revoked receivers $\mathcal{N} \setminus \mathcal{R}$ and a method that allows each user $u \in S_j$ to compute her key K_j from $I[u]$.

We propose here the interval revocation scheme. An interval $I \subset \mathcal{N}$ is a subset of $\mathcal{N}$ containing consecutive elements: $I[i,j] = \{u_{(i \mod N)}, u_{(i+1 \mod N)}, ..., u_{(j \mod N)}\}$ For example for $N = 6$ interval $I[2,5] = \{u_2, u_3, u_4, u_5\}$, but interval $I[2,1] = \{u_2, u_3, u_4, u_5, u_0, u_1\}$. The size of an interval is $|I[i,j]| = j - i + 1 \mod N$. Interval $I[i, i+s-1]$ of size s can be split uniquely into two intervals of size $\lceil \frac{s}{2} \rceil$ as follows: $I[i, i+s-1] = I[i, i + \lceil \frac{s}{2} \rceil - 1] \cup I[i + \lceil \frac{s-1}{2} \rceil, i+s-1]$ (1).

We define collection $\mathcal{X}$ as the collection of all intervals on $\mathcal{N}$. Based on (1), each interval $I \in \mathcal{X}$ of size s can be uniquely split into $I_{left}, I_{right} \in \mathcal{X}$ of size $\lceil \frac{s}{2} \rceil$. Furthermore, any two intervals never share the same set of children. A digraph representing the child relation for $N = 8$ is presented in Figure 1, restricted to intervals of size $1, 2, 3$ and 4. Let $\mathcal{R} = \{u_{i_1}, u_{i_2}, ..., u_{i_r}\} \subset \mathcal{N}$ be the set of revoked receivers. The cover of $\mathcal{N} \setminus \mathcal{R}$ consists of all intervals between revoked receivers. We have: $\mathcal{N} \setminus \mathcal{R} \subset I[i_r + 1, i_1 - 1] \cup \bigcup_{j=1, i_{j+1} > i_j + 1}^{r-1} I[i_j + 1, i_{j+1} - 1]$, and we define the cover as the set of intervals from this sum. Thus, the size of the cover is at most $r = |\mathcal{R}|$.

We apply the Diffie - Hellman (DH) key exchange protocol for key derivation. We label each interval $I \in \mathcal{X}$ with its private key S_I and its public key P_I. The key of interval I is a shared key obtained by applying the DH protocol on the private and public keys of its children I_{left} and I_{right}, treating children as the key exchanging parties. To derive a key of a descendant interval, a receiver needs his own secret key, as well as the public keys of the "other" children in the path to the target interval. Receiver u_i needs to store only the secret key S_I assigned to interval $I = I[i,i]$. The number of operations needed to derive one key from another is $O(\log N)$.

Given the achieved results, the direction for future research is to find an assignment of public parameters that can be generated efficiently in on-the-fly manner. This would allow to release the public space requirement for our scheme.

References

1. Asano, T.: A revocation scheme with minimal storage at receivers. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 433–450. Springer, Heidelberg (2002)
2. Naor, D., Naor, M., Lotspiech, J.B.: Revocation and tracing schemes for stateless receivers. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 41–62. Springer, Heidelberg (2001)