Homomorphic Signature for Network Coding

Li Chen

Xidian University

September 22, 2013

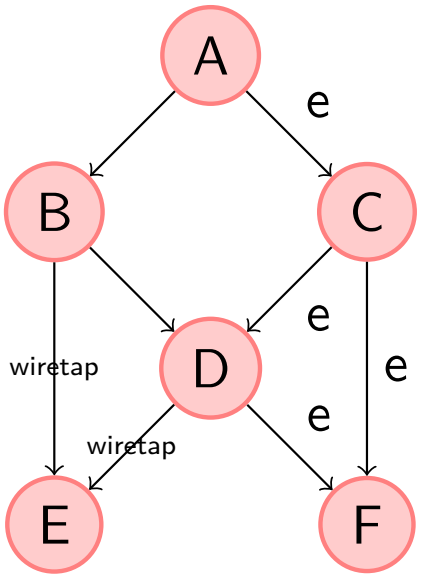
Outline

Threaten and protection

homomorphic Signature

Our discussion

Threaten and protection

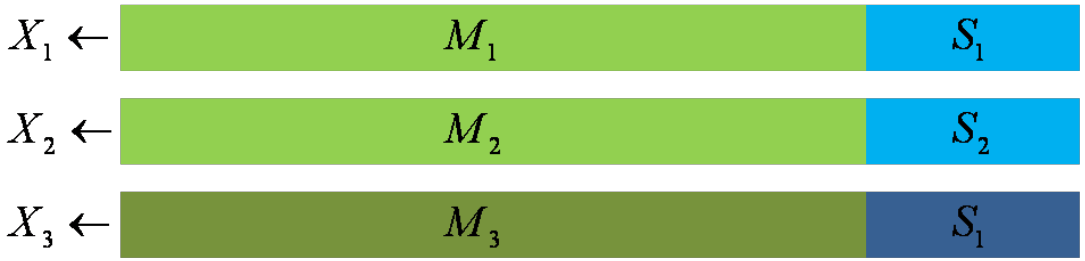


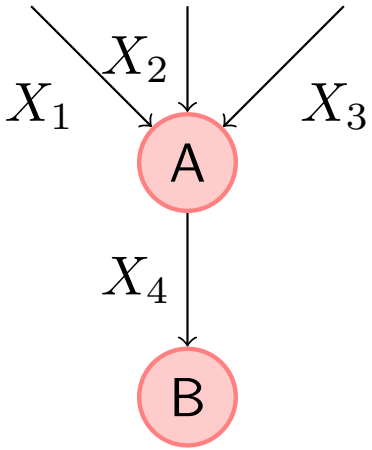
	Threaten	
Protection	Eavesdropping	Contamination
	CSWN	Error correction
	Encryption	Signature

Information Theory & Coding

Cryptography

All since the multicast mechanism!





$X_i = M_i \| S_i$

For $i = 1, 2$, $S_i \leftarrow \text{sign}(M_i)$, $1 \leftarrow \text{verify}(M_i, S_i)$

For $i = 3$, $0 \leftarrow \text{verify}(M_i, S_i)$

$M_4 = c_1 M_1 + c_2 M_2 + c_3 M_3$, c_1, c_2, c_3 IID from Uniform.

$S_4 \leftarrow \text{valuate}(c_1, c_2, c_3, S_1, S_2, S_3)$.

If $0 \leftarrow \text{verify}(M_4, S_4)$, then B will drop X_4.

Claim 0.1 Let $\mathcal{S} = \{Gen, Sign, Veri, Valu\}$ be a homomorphic signature scheme and unforgeable-CMA. Then

1. $1 \leftarrow \text{verify}(M_i, S_i) \Rightarrow 1 \leftarrow \text{verify}(M', S')$ when $M' = \sum c_i M_i$, and $S' = \text{valuate}(c_i, S_i)$

2. $Adv(1 \leftarrow \text{verify}(M', S')) = negl.$ when M', S' are chosen randomly.

homomorphic Signature

we describe a homomorphic signature scheme that presented in[1] by Yu et al.
Notions:

1. p, q are tow primes satisfying $q|p-1$.
2. G is a subgroup of Z_p^*, $\mathrm{order}(G) = q$.
3. $g_1, g_2, \cdots, g_t \in G$.
4. N is an RSA modulus of same bit length as p.
5. $ed = 1 \mod \phi(N)$.

Key Generation:

$pk \leftarrow \{p, q, g_1, g_2, \cdots, g_t, N, e\}$, $sk \leftarrow \{d\}$.

Signature:

given a packet $\mathrm{v} = (v_1, v_2, \cdots, v_t) \in Z_q$, the signature is calculated as

$$\sigma \leftarrow \mathsf{sign}(sk, \mathrm{v}) = \Big(\prod_{j=1}^{t} g_j^{v_j} \mod p\Big)^d \mod N \tag{1}$$

verification:

given a packet $\mathrm{v} = (v_1, v_2, \cdots, v_t)$, and the corresponding signature σ, then $1 \leftarrow \mathsf{verif}(pk, \mathrm{v}, \sigma)$ if

$$\sigma^e = \Big(\prod_{j=1}^{t} g_j^{v_j} \mod p\Big) \mod N \tag{2}$$

homomorphic?:
Yu et al[**?**] claim that this scheme is homomorphic in, but Yun et al[2] point out that this scheme is not homomorphic in general, and they give some advice to fix it.

Let σ_i be a valid signature for v_i, and $\mathrm{w} = \sum a_i \mathrm{v}_i$, $\tau = \prod \sigma^{a_i} \mod N$. If this scheme is homomorphic, then τ is supposed to be a valid signature for w. But it's not true in general.

Considering $\mathrm{w} = 2\mathrm{v}$,let σ be the signature for v, then σ^2 should be a valid signature for w, which means:

$$\sigma^e = (\prod_{j=1}^{t} g_j^{v_j} \mod p) \mod N \Rightarrow \sigma^{2e} = (\prod_{j=1}^{t} g_j^{2v_j} \mod p) \mod N \quad (3)$$

Let $X = \sigma^e$, $Y = \prod_{j=1}^{t} g_j^{v_j} \mod p$, then (3) equivalent to

$$X \equiv Y \mod p \Rightarrow X^2 \equiv (Y^2 \mod q) \mod N. \tag{4}$$

which is not true in general. If we set $p = N$, this modified scheme clearly is homomorphic, but unfortunately, Yun et al[**?**] also present some forgery attacks.

Our discussion

1. The signature scheme of Yu et al. follows the "hash-and-sign" paradigm. It is composed of a homomorphic hash function $\mathrm{v} \mapsto \prod g_i^{v_i} \mod q$ and a 'bare' RSA signature scheme $x \mapsto x^d \mod N$.

2. If we want this signature scheme homomorphic, then the hash and sign should have the same modulus.

3. But If the hash and sign should have the same modulus, it's simple to forge a signature.

4. other solution ... ...

References

[1] Zhen Yu, Yawen Wei, Bhuvaneswari Ramkumar, and Yong Guan. An efficient signature-based scheme for securing network coding against pollution attacks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 1409–1417. IEEE, 2008.

[2] Aaram Yun, Jung Hee Cheon, and Yongdae Kim. On homomorphic signatures for network coding. *Computers, IEEE Transactions on*, 59(9):1295–1296, 2010.

Thanks! & Questions?