EUF-CMA of XMSS

https://youtu.be/88JAVjelfTo

Digital signature forgery

- Total break
  - 공격자가 서명자가 사용하는 개인 정보와 키를 복구 할 수 있을 때, 어떤 메시지에나 서명을 생성할 수 있는 공격
- Universal forgery(universal unforgeability, UUF)
  - 공격자가 주어진 메시지에 대한 유효한 서명 생성할 수 있는 것
  - 공격자는 무작위로 선택한 메시지나 서명 제공자가 제공한 특정 메시지에 서명하는 것이 가능
- Selective forgery(선택적 위조)
  - 원하는 메시지에 대해 서명자의 서명을 생성하는 것이 목적
- Existential forgery(실존적 위조)
  - 적어도 하나의 메시지와 이 메시지에 대응되는 서명자의 유효한 서명값을 생성하는게 목적
  - 메시지 m을 자유롭게 선택 가능
  - (메시지, 서명) 쌍이 유효한 경우, 공격자는 실존적 위조 가능
  - Existential forgery of RSA
    - $\sigma(m_1) * \sigma(m_2) = \sigma(m_1 * m_2)$
    - $m' = (m_1 * m_2)$, $\sigma(m') = \sigma(m_1 * m2) = \sigma(m_1) * \sigma(m_2)$

EUF-CMA

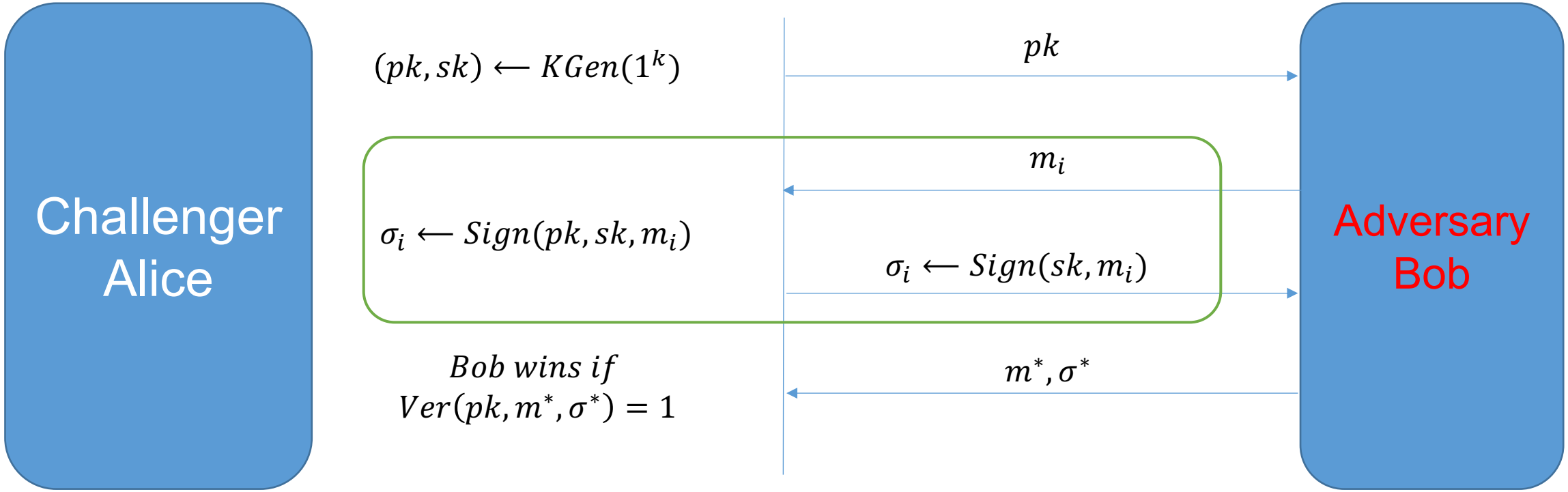
- Existentially Unforgeability under Chosen Message Attacks
  - 선택적 메시지 공격에서 존재하는 위조가 불가함을 실험하는 것
    - Chosen Message Attacks
      공격자가 선택한 메시지에 서명을 요청할 수 있음

- Setup: the challenger $\mathcal{C}$ runs the key generation $\texttt{SigKeyGen}$ to obtain a key pair $(vk, sigk)$ and hands the public key vk to $\mathcal{A}$.
- Queries: the adversary $\mathcal{A}$ is given access to a signing oracle. When queried for message m, the challenger runs algorithm $\texttt{Sign}$ on input m and $sigk$ and returns the corresponding output σ to the adversary.
- Forgery: the adversary $\mathcal{A}$ outputs a pair (μ, σ) and wins if and only $\texttt{Verify}_{vk}(\sigma, \mu) = 1$ and no query for a signature on μ was asked.

Figure 2. EUF-CMA security of a signature scheme.

https://www.researchgate.net/publication/337649509_From_Key_Encapsulation_to_Authenticated_Group_Key_Establishment-A_Compiler_for_Post-Quantum_Primitives

EUF-CMA



Adversary Bob wins if
1) (m^*, σ^*) is valid, and
2) Bob did not query a signature for m^*

EUF-CMA security of WOTS+

Experiment $\mathsf{Exp}^{\textit{EU-CMA}}_{\mathsf{A},\mathsf{Sig}}(n)$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Kg}(1^n)$
$(M^\star, \sigma^\star) \leftarrow \mathsf{A}^{\mathsf{Sign}(\mathsf{sk},\cdot)}(\mathsf{pk})$
Let $\{(M_i, \sigma_i)\}_1^{q_{\mathsf{Sign}}}$ *be the query-answer pairs of* $\mathsf{Sign}(\mathsf{sk}, \cdot)$.
Return 1 *iff* $\mathsf{Vf}(\mathsf{pk}, M^\star, \sigma^\star) = 1$ *and* $M^\star \notin \{M_i\}_1^{q_{\mathsf{Sign}}}$.

Sig *is* (t, ϵ, q)*-existentially unforgeable if there is no* t*-time adversary that succeeds with probability* $\geq \epsilon$ *after making* $\leq q$ *signature oracle queries.*

A $(t, \epsilon, 1)$-EU-CMA secure signature scheme is called one-time signature scheme.

Buchmann, Johannes, et al. "On the security of the Winternitz one-time signature scheme." *International conference on cryptology in Africa*. Springer, Berlin, Heidelberg, 2011.

Security of XMSS

- 원리 1
  - H(b) : second preimage resistant hash function family
  - F(n) : pseudorandom function family
- One-way function ⊂ secure signature scheme
- Second preimage resistant hash function family ⊂ collision resistant hash fucntion ⊂ secure signature scheme

→ EUF-CMA(EU-CMA) of XMSS

Rogaway, P., Shrimpton, T.: Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. In: Roy, B.K., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 371–388. Springer, Heidelberg (2004)
Rompel, J.: One-way functions are necessary and sufficient for secure signatures. In: STOC 1990: Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing, pp. 387–394. ACM Press, New York (1990)

Security of XMSS

- RSA와 같이 개인 서명키가 일정하지 않음

- 특정 시간이 지나면 개인 서명키가 변경
  - 일정한 서명키라고 가정 후, EUF-CMA 실행

Experiment $\mathsf{Exp}^{\text{EU-CMA}}_{\text{KES}(1^n,T)}(\mathsf{A})$

$i \leftarrow 0$, $\mathtt{state} \leftarrow \mathtt{null}$, $\mathtt{out} \leftarrow \mathtt{null}$, $(\mathsf{sk}_0, \mathsf{pk}) \leftarrow \mathsf{Kg}(1^n, T)$

while $i < T$ **and** $\mathtt{out} \neq \mathtt{halt}$

$(\mathtt{out}, \mathtt{state}) \leftarrow \mathsf{A}^{\mathsf{Sign}(\mathsf{sk}_i, \cdot, i)}(1^n, \mathtt{cma}, \mathsf{pk}, \mathtt{state})$

$\mathrm{i}{+}{+}$; $\mathsf{sk}_i \leftarrow \mathsf{KUpd}(\mathsf{sk}_{i-1}, i)$

$(M^\star, \sigma^\star, i^\star) \leftarrow \mathsf{A}(1^n, \mathtt{forge}, \mathtt{state})$

If $\mathsf{Vf}(\mathsf{pk}, M^\star, (\sigma^\star, i^\star)) = 1$ **and** Sign was not queried for a signature on $M^\star$ **return** 1

return 0

Security of XMSS

- 정리 1에 대한 검증

$time \leq t$, EUF-CMA 실험에서 최대 q개의 서명을 생성하는 오라클 쿼리를 만드는 공격자가 성공할 최대 확률

$$\mathrm{InSec}^{\mathrm{EU\text{-}CMA}}(\mathrm{Dss}; t, q) = \mathrm{InSec}^{\mathrm{PRF}}(F(n); (t' + \lambda), \lambda) + \mathrm{InSec}^{\mathrm{EU\text{-}CMA}}(\mathrm{Dss}^{\star}; t, q)$$

$$t' = t + \mathrm{t_{Kg}} + q\mathrm{t_{Sign}} + \mathrm{t_{Vf}}.$$

$runtime \leq t$, 공격자가 오라클을 쿼리할 수 있을 때, F(n)에서 임의의 요소를 임의의 함수와 구별할 때, 공격자가 성공할 최대 확률; 최대 q개 함수

DSS : digital signature scheme
$\lambda \in \{0,1\}^n$ yields

Security of XMSS

첫번째($InSec$) 박스에 대한 모순을 가정

$$\mathrm{Succ}^{\text{EU-CMA}}\left(\mathrm{Dss};\mathsf{A}\right) > \mathrm{InSec}^{\text{EU-CMA}}\left(\mathrm{Dss};t,q\right)$$

$$\mathrm{Succ}^{\mathrm{PRF}}\left(F(n);\mathsf{Dis}\right) > \mathrm{InSec}^{\mathrm{PRF}}\left(F;t',q\right) \qquad \mathrm{Succ}^{\text{EU-CMA}}\left(\mathrm{Dss}^{\star};\mathsf{A}\right) > \mathrm{InSec}^{\text{EU-CMA}}\left(\mathrm{Dss}^{\star};t,q\right).$$

$$\begin{aligned}
&\mathrm{InSec}^{\text{EU-CMA}}\left(XMSS\ ;t,q=2^H\right)\\
&\leq \mathrm{InSec}^{\mathrm{PRF}}\left(F(n);(t'+2^H),q=2^H\right)\\
&+2\cdot\max\left\{\begin{array}{l}(2^{H+\log\ell}-1)\cdot\mathrm{InSec}^{\mathrm{SPR}}\left(\mathcal{H}(n);t'\right),\\ 2^H\Big(\mathrm{InSec}^{\mathrm{PRF}}\left(F(n);(t'+\ell),q=\ell\right)\\ \quad+(\ell^2w^2\kappa^{w-1}\frac{1}{\left(\frac{1}{\kappa}-\frac{1}{2^n}\right)})\cdot\mathrm{InSec}^{\mathrm{PRF}}\left(F(n);(t'),q=2\right)\Big)\end{array}\right\}
\end{aligned}$$

where $t'=t+2^H\cdot t_{\mathsf{Sign}}+t_{\mathsf{Vf}}+t_{\mathsf{Kg}}$.

$time \leq t$,$H(n)$에서 second preimage를 찾기 위해 공격자가 성공할 최대 확률;

Q & A