# Proof of Plaintext Knowledge and (Deniable) Authentication

Michael Rabin

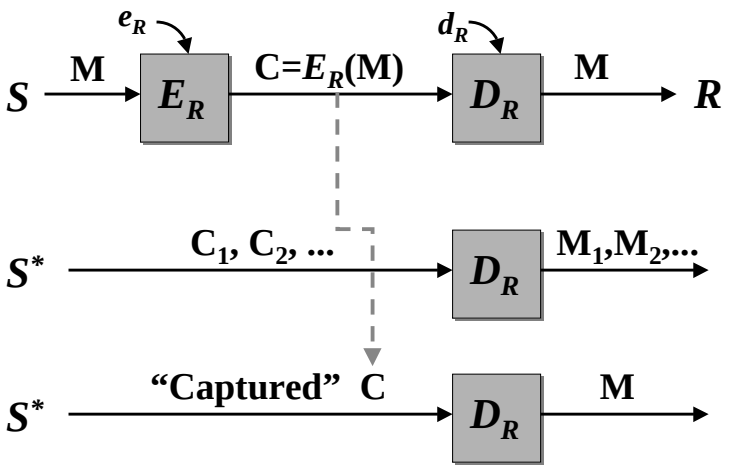
Joint work with Yonatan Aumann

Jump to first page

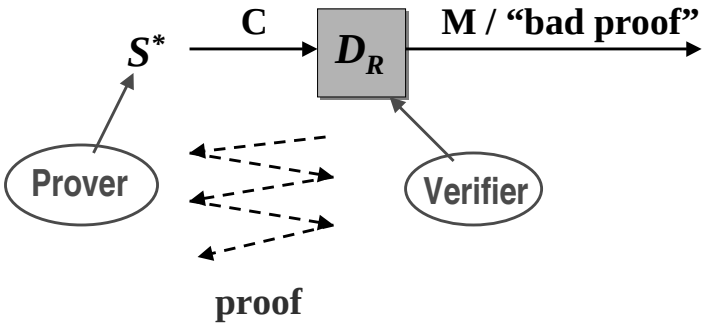
## Plan

- *Proof of PlainText Knowledge (PPTK)*
- Efficient Encryption Enhancement to PPTK for any public key encryption scheme
- Efficient protection against Chosen Ciphertext Attacks
- Efficient Authentication of long messages
- Deniable Authentication
- Classification of Adversaries

## Chosen Ciphertext Attacks




## Proof of PlainText Knowledge



## Properties of PPTK

- If $S^*$ proper (C=$E_R$(M)) then $S^*$ can prove PlainText Knowledge.
- With probability > 1-(7/8)$^n$, $S^*$ can compute $D_R$'s output on her own:
  - If $D_R$ outputs $\mathbf{M}=D_R(\mathbf{C})$ then $S^*$ can compute $\mathbf{M}$ on her own.
  - If $D_R$ outputs **"bad proof"** then $S^*$ knows this in advance.

## Encryption Enhancement

- Generic transformation

$$E_R \Rightarrow ENE_R \quad \textit{The Enhanced } E_R$$

***Theorem*:** For any semantically secure PK system $E_R(\bullet)$, the system $ENE_R(\bullet)$ is also semantically secure and has an efficient PPTK.

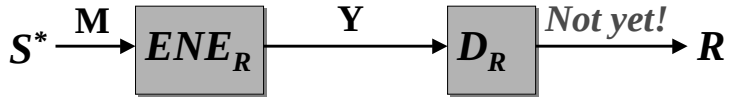
Cost: 4n computations of $E_R$ .

## Encryption Enhancement Procedure

$E_R(\bullet)$ - $R$'s public key encryption

1. $M < p$ prime
2. $n$ - security parameter, $m=4n$.
3. $S$ randomly chooses

   $f(t)=a_{n-1}t^{n-1}+ \ldots + a_1 t + M$ } Shamir Secret Sharing
4. $X_i=f(i)$ , $Y_i= E_R(X_i)$, $i=1,\ldots, m$
5. $ENE_R(M)=Y=(Y_1,\ldots,Y_m)$




## Proof of PlainText Knlowlege

**Phase I:**

1. $S^* \xrightarrow{Y=(Y_1,\ldots,Y_m)} D_R$
2. Verifier $D_R$ decodes $D_R(Y_i)=X_i$, $i=1,\ldots,m$.
   Sets $X=\{(1,X_1),\ldots,(m,X_m)\}$
3. Verifier (with Prover) randomly chooses

   $I=(i_1,\ldots,i_{n-1})$ , $S^* \xleftarrow{I=(i_1,\ldots,i_{n-1})} D_R$
4. $S^* \xrightarrow{X_{i_1},\ldots,X_{i\ n-1}} D_R$

   s.t. $E_R(X_{ij})=Y_{ij}$ , $j=1,\ldots,n-1$
5. If $S^*$ fails then $D_R$ aborts

**Phase II:**

$$H=\{ (i_1, X_{i_1}) , \ldots , (i_{n-1} , X_{i_{n-1}}) \}$$

- $D_R$ checks if exists $EH$

  $H \subset EH \subset \{(1,X_1), \ldots , (4n,X_{4n})\}$

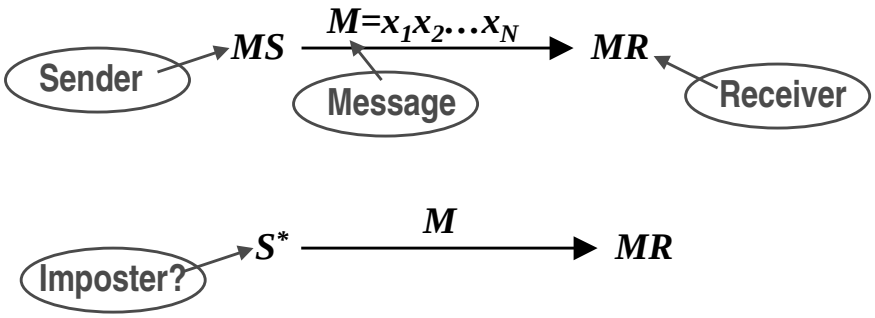
  such that:

  1. $|EH| = 3n$
  2. All $3n$ points of $EH$ are on the curve of some polynomial $f(t)$ of degree $n-1$
- If yes, $D_R$ outputs constant term $M$ of $f(t)$ .
- Otherwise, $D_R$ outputs "Failed proof".

## Key points of correctness proof

- If $S^*$ was able to decode $Y_{i_1}, \ldots, Y_{i_{n-1}}$ (with work $W$), then with probability $1-(7/8)^n$ $S^*$ can decode $3.5n$ $Y_j$'s (with work $4nW$).
- By use of these $3.5n$ points $(j,X_j)$, with overwhelming probability, $S^*$ can know on her own $D_R$'s reply in $S^*$ Phase II.

## Message Authentication

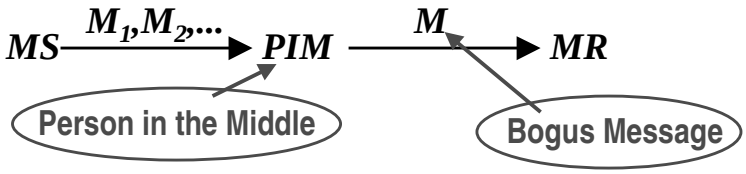



- ***MR*** wants to authenticate ***M*** as being authored by ***MS*** for ***MR, at this time***.

## Our Solution

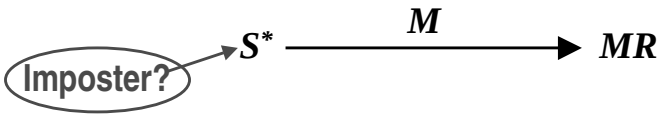
- Generic
- Efficient
- Long messages
- Resilient against Person-in-the-Middle attacks
- No cryptographic hashing
- Deniable Authentication

## Person in the Middle Attack

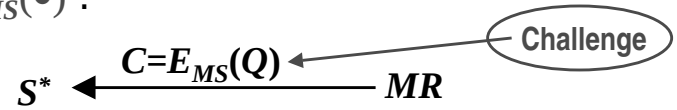



- ***PIM*** will not be able to authenticate ***M*** to ***MR*** , unless for some ***i, M=M***$_i$.

## Strategy




- ***MR*** will pose to ***S**** a question ***Q*** about ***M*** .
- The question ***Q*** is sent to S* encrypted by $E_{MS}(\bullet)$ .




- By correctly responding ***S**** proves ***S**=**MS*** , and authenticates ***M*** .

## Authentication Protocol

1. $MS \xrightarrow{M} MR$

2. $MR$ randomly chooses:
   - Irreducible polynomial $f(t)=t^{64}+b_1t^{63}+\ldots+b_{64}$
   - random $pad=c_1c_2\ldots c_{64}$.

3. $MS \xleftarrow{C=E_{MS}(f,\,pad)} MR$ (Challenge)

   with PPTK.

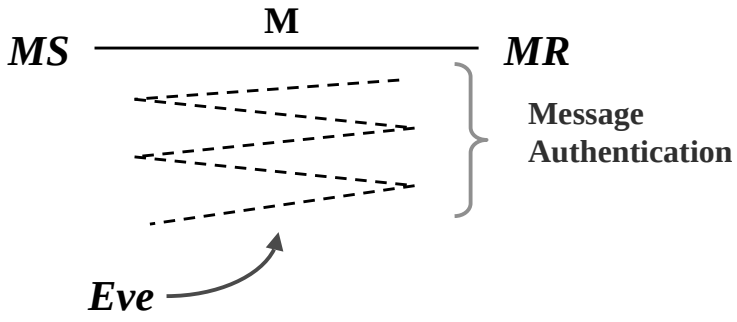
4. $MS \xrightarrow{(M \bmod f)\oplus pad} MR$ (Reply)

[Ra80]

## Properties

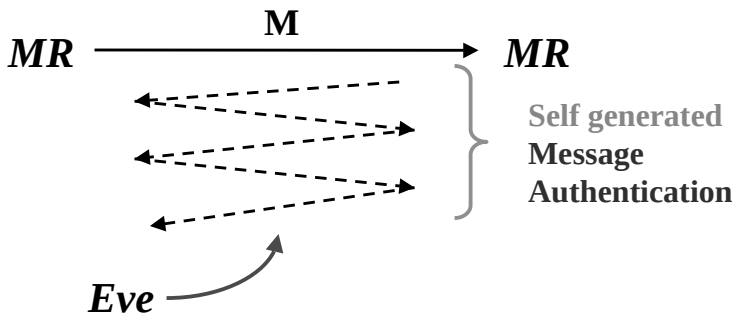
- Assuming $E_{MS}$ is *non-melleable*: **Prob( cheating )** $\leq N/2^{64}$ , $N=|M|$
- Computing $M \bmod f$ takes $|M|$ $XOR$ operations.
- As secure as $E_{MS}$

## Deniable Authentication




Eve: On line all powerful adversary, wants proof that *MS* authored *M*.

***MS*** can deny authorship of ***M.***

***MS*** will claim:

- Because of PPTK , ***MR*** *knows* question ***Q*** = **( *f* , *pad* ).**
- ***MR*** created ***M*** and gave the correct responses.