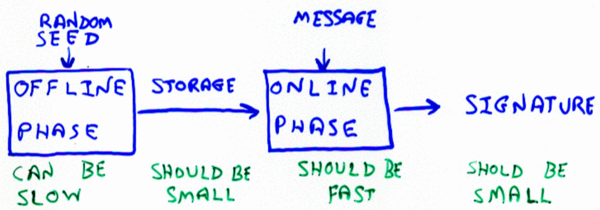
HOW TO TRANSFORM ANY SIGNATURE SCHEME INTO AN EFFICIENT ONLINE/OFFLINE SIGNATURE SCHEME

ADI SHAMIR, THE WEIZMANN INSTITUTE

YAEL TAUMAN, THE WEIZMANN INSTITUTE



- SOME SIGNATURE SCHEMES HAVE A NATURAL DECOMPOSITION
- EVEN GOLDREICH MICALI [90] PROVIDE A GENERAL TRANSFORMATION WHICH IS INEFFICIENT IN PRACTICE.

A NEW TOOL: TRAPDOOR HASH FUNCTIONS

- INTRODUCED IN KRAWCZYK AND RABIN [00]
- USED TO CONSTRUCT CHAMELEON SIGNATURES

$h(m,r)$ IS ASSOCIATED WITH PUBLIC AND PRIVATE KEYS:

- KNOWLEDGE OF THE PUBLIC KEY ENABLES EVALUATION, BUT COLLISIONS ARE HARD TO FIND:

$$h(m_1, r_1) = h(m_2, r_2)$$

- KNOWLEDGE OF THE SECRET KEY MAKES IT EASY TO FIND FOR ANY m_1, r_1, m_2 A COLLIDING r_2
- SEVERAL IMPLEMENTATIONS ARE KNOWN
- IN SOME IMPLEMENTATIONS COLLISION FINDING REQUIRES ONE MULTIPLICATION AND ONE ADDITION

FOR TECHNICAL REASONS, WE NEED THE ADDITIONAL UNIFORMITY PROPERTY:

FOR ANY GIVEN m_1, r_1, m_2, THE COLLISION FINDING ALGORITHM COMPUTES AN r_2 SUCH THAT $h(m_1, r_1) = h(m_2, r_2)$ IN SUCH A WAY THAT WHEN r_1 IS UNIFORMLY DISTRIBUTED, r_2 IS PERFECTLY/STATISTICALLY/COMPUTATIONALLY INDISTINGUISHABLE FROM RANDOM DISTRIBUTION.

REMARK:

IT IS NOT REQUIRED THAT GIVEN ONE COLLISION IT REMAINS DIFFICULT TO GENERATE ADDITIONAL COLLISIONS.

IN FACT, IN ALL THE CONSTRUCTIONS KNOWLEDGE OF A SINGLE COLLISION REVEALS THE SECRET KEY.

2.5

EXAMPLES OF TRAPDOOR HASH FUNCTIONS

- GMR [84] CLAW FREE FUNCTIONS
- SCHEMES BASED ON THE REPRESENTATION PROBLEM:

$$h(m,r) = a^m \cdot b^r \pmod{P}$$

- SCHEMES BASED ON FACTORING:

$$h(m,r) = g^{m \circ r} \pmod{n = p \cdot q}$$

- SCHEMES BASED ON MULTIVARIATE ALGEBRAIC EXPRESSIONS (KEEPING RESULTS CONSTANT IS POTENTIALLY EASIER THAN SOLVING THE EQUATIONS $\underline{E}(\underline{m}, \underline{r}) = \underline{V}$

HOW TO FIND COLLISIONS IN

$$h(m,r) = g^{m \circ r} \pmod{n = p \cdot q}, \quad 0 \leq r < n$$

$$h(m_1, r_1) = h(m_2, r_2) \pmod n$$

$$\Downarrow$$

$$g^{m_1 \circ r_1} = g^{m_2 \circ r_2} \pmod n$$

$$\Downarrow$$

$$m_1 \cdot 2^k + r_1 = m_2 \cdot 2^k + r_2 \pmod{\varphi(n)}$$

$$\Downarrow$$

$$r_2 = (m_1 - m_2) \cdot 2^k + r_1 \pmod{\varphi(n)}$$

- WHEN r_1 IS RANDOM, SO IS r_2
- THE DIFFERENCE BETWEEN n AND $\varphi(n)$ IS NEGLIGIBLE
- COLLISION FINDING REQUIRES ONE MODULAR REDUCTION OF A SHIFTED VALUE, AND ONE ADDITION.

THE STANDARD PARADIGM: HASH/SIGN

$$S(h(m,r))$$

THE NEW PARADIGM: HASH/SIGN/SWITCH

- THE OFFLINE PHASE: CHOOSE RANDOM m', r', AND COMPUTE $S(h(m', r'))$
- THE ONLINE PHASE: GIVEN AN ACTUAL m, FIND A COLLISION $h(m,r) = h(m', r')$ AND SEND THE PRECOMPUTED SIGNATURE AND r

ADVANTAGES:

- THE SIZE OF SIGNATURES ONLY DOUBLES
- THE ONLINE COMPLEXITY CAN BE ONE $*$, ONE $+$
- THE SIGNATURE SCHEME IS ONLY APPLIED TO RANDOM MESSAGES CHOSEN ENTIRELY BY THE SIGNER, SO $\nexists$ CHOSEN MESSAGE ATTACKS ON S

THE FORMAL SECURITY CLAIM:

THEOREM: LET (G, S, V) BE A SIGNATURE SCHEME AND LET (I, H) BE A TRAPDOOR HASH FAMILY. DENOTE BY (G', S', V') THE RESULTANT ONLINE/OFFLINE SIGNATURE SCHEME.

SUPPOSE THAT (G', S', V') IS EXISTENTIALLY FORGEABLE BY A Q-ADAPTIVE CHOSEN MESSAGE ATTACK IN TIME T WITH SUCCESS PROBABILITY ε.

THEN ONE OF THE FOLLOWING CASES HOLDS:

1. $\exists$ PROBABILISTIC ALGORITHM THAT GIVEN A HASH KEY HK, FINDS COLLISIONS OF h_{HK} IN TIME $T + T_G + Q \cdot (T_H + T_S)$ WITH SUCCESS PROBABILITY $\geq \frac{\varepsilon}{2}$.
2. THE ORIGINAL SIGNATURE SCHEME (G, S, V) IS EXISTENTIALLY FORGEABLE BY A GENERIC Q-CHOSEN MESSAGE ATTACK IN TIME $T + Q \cdot (T_H + T_{COL}) + T_I$ WITH SUCCESS PROBABILITY $\geq \frac{\varepsilon}{2}$.

THE PROOF TECHNIQUE (SIMPLIFIED):

- CONSIDER A SUCCESSFUL PROBABILISTIC FORGER F'.
- DENOTE BY $\{m_i\}_{i=1}^{Q}$ THE QUERIES IT SENDS TO THE NEW SIGNATURE ORACLE, AND BY $\{(r_i, \Sigma_i)\}_{i=1}^{Q}$ THE SIGNATURES IT PRODUCES.
- DENOTE BY $m, (r, \Sigma)$ THE NEW MESSAGE AND SIGNATURE PRODUCED BY F' $(\forall i,\ m \neq m_i)$.
- WE KNOW THAT $\text{PROB}(V(h(m,r), \Sigma) = 1) \geq \varepsilon$
- SO AT LEAST ONE OF THE FOLLOWING INEQUALITIES HOLD:

$$\text{PROB}(V(h(m,r), \Sigma) = 1 \text{ AND } \exists i \mid h(m_i, r_i) = h(m,r)) \geq \frac{\varepsilon}{2}$$

$$\text{PROB}(V(h(m,r), \Sigma) = 1 \text{ AND } \forall i\ h(m_i, r_i) \neq h(m,r)) \geq \frac{\varepsilon}{2}$$

- IN THE FIRST CASE, WE BUILD A COLLISION FINDER A BY CHOOSING OUR OWN SECRET/PUBLIC KEYS FOR (G,S,V) WHICH ENABLES US TO ANSWER THE SIGNATURE QUERIES
- IN THE SECOND CASE, WE BUILD A GENERIC FORGER F AGAINST THE ORIGINAL (G,S,V) BY CHOOSING OUR OWN SECRET/PUBLIC KEYS FOR (I,H), AND CHOOSING Q RANDOM (m'_i, r'_i) SUCH THAT $h(m'_i, r'_i)$ WILL BE THE INPUTS TO THE SIGNING ORACLE S.

- F NOW SIMULATES THE Q-ADAPTIVE FORGER F' (ACTING AGAINST (G', S', V')) IN THE FOLLOWING WAY

  WHEN F' MAKES THE i-TH QUERY TO THE SIGNATURE ORACLE, WITH MESSAGE m_i, F FINDS r_i SUCH THAT $h(m_i, r_i) = h(m_i', r_i')$ (BY USING THE KNOWN TRAPDOOR KEY OF h) AND PROCEEDS WITH THE PRECOMPUTED SIGNATURE (r_i, Σ_i). WITH PROBABILITY $\geq \frac{\varepsilon}{2}$, F IS ASSUMED TO FIND A NEW m AND (r, Σ) S.T

  $\forall i = 1, \cdots, Q \quad h(m, r) \neq h(m_i, r_i)$

  Σ IS A VALID SIGNATURE OF $h(m, r)$ W.R.T (G, S, V)

- CONSEQUENTLY, F SUCCEEDS IN FORGING A NEW SIGNATURE FOR A NEW MESSAGE $(h(m, r))$ WITH PROBABILITY $\geq \frac{\varepsilon}{2}$ BY USING ONLY GENERIC (NON ADAPTIVE) INITIAL QUERIES TO THE SIGNING ORACLE S OF THE ORIGINAL SIGNATURE SCHEME (G, S, V).