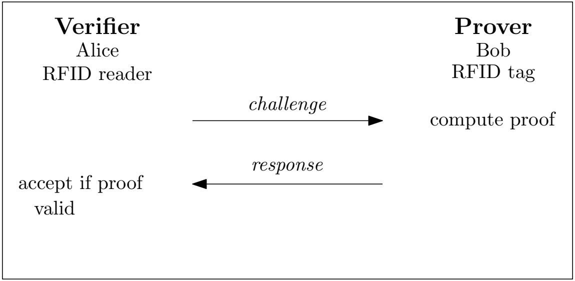
Algebraic Attacks on linear RFID Authentication Protocols

Matthias Krause and Dirk Stegemann

University of Mannheim (Germany)

10th GI-Kryptotag
March 20, 2009
Technische Universität Berlin, Germany

Challenge-Response Authentication Protocols



A passive attacker

- collects a set O of observed challenge/response pairs
- cannot manipulate the communication
- tries to forge valid responses

Idea of Linear Authentication Protocols

Prover and Verifier agree on L linear n-dim. subspaces of $\{0,1\}^m$.

Verifier Alice RFID reader		**Prover** Bob RFID tag
	$\xrightarrow{\textit{challenge}}$	choose $l \in_R [L]$
accept if $\exists l \in \{1, \ldots, L\}$ with $w \in V_l$	$\xleftarrow{w \in_R V_l}$	

Problems:

- $V_1 + \ldots + V_L$ too small $\Rightarrow$ responses w efficiently distinguishable from random values
- $V_1 + \ldots + V_L$ too large $\Rightarrow$ Pr[successful faugery] too high

Linear (n, k, L) Authentication Protocols

Prover and Verifier agree on L lin. n-dim. subspaces of $\{0,1\}^{n+k}$.

Observation: Any linear subspace $V_l \subseteq \{0,1\}^{n+k}$ can be represented by a linear mapping $f_l : \{0,1\}^n \rightarrow \{0,1\}^k$ and a permutation $\sigma_l \in \mathcal{S}_{n+k}$ such that $V_l = \{\sigma_l(v||f_l(v)), v \in \{0,1\}^n\}$.

Linear (n, k, L) Authentication Protocols

Prover and Verifier agree on L lin. n-dim. subspaces of $\{0,1\}^{n+k}$.

Observation: Any linear subspace $V_l \subseteq \{0,1\}^{n+k}$ can be represented by a linear mapping $f_l : \{0,1\}^n \to \{0,1\}^k$ and a permutation $\sigma_l \in \mathcal{S}_{n+k}$ such that $V_l = \{\sigma_l(v||f_l(v)), v \in \{0,1\}^n\}$.

Verifier Alice RFID reader		**Prover** Bob RFID tag
	challenge $\longrightarrow$	choose $l \in_R [L]$, $v \in_R \{0,1\}^n$
for $i := 1$ to L $(x\|\|y) := \sigma_l^{-1}(w)$ if $(y = f_l(x))$ accept reject	$\longleftarrow$ $w := \sigma_l(v\|\|f_l(v))$	

Special Case: The CKK^2 Protocol

proposed by Cichoń, Klonowski and Kutyłowski at Pervasive 2008

CKK^2 is a linear $(n+k, k, 2)$ protocol with

- $f_1 = f_2 = f$
- f depends only on the first n inputs.
- σ_1 exchanges the last two k-bit blocks.
  $\sigma_2 = \mathrm{id}$

Verifier Alice RFID reader		**Prover** Bob RFID tag
	challenge $\longrightarrow$	choose $l \in_R [L]$, $v \in_R \{0,1\}^n$
for $i := 1$ to L $(x\|\|y) := \sigma_l^{-1}(w)$ if $(y = f_l(x))$ accept reject	$\longleftarrow$ $w := \sigma_l(v\|\|f_l(v))$	

Special Case: The CKK^2 Protocol

proposed by Cichoń, Klonowski and Kutyłowski at Pervasive 2008

CKK^2 is a linear $(n+k, k, 2)$ protocol with

- $f_1 = f_2 = f$
- f depends only on the first n inputs.
- σ_1 exchanges the last two k-bit blocks.
  $\sigma_2 = \mathrm{id}$

Verifier Alice RFID reader		**Prover** Bob RFID tag
	$\xrightarrow{\textit{challenge}}$	choose $l \in_R [L]$, $v \in_R \{0,1\}^n$
for $i := 1$ to L $(x\|\|y) := \sigma_l^{-1}(w)$ if $(y = f_l(x))$ accept reject	$\xleftarrow{w := \sigma_l(v\|\|f_l(v))}$	

Implications:

- $V_1 = \{(v||a||b) | v \in \{0,1\}^n, a = f(v), b \in \{0,1\}^k\}$
  $V_2 = \{(v||a||b) | v \in \{0,1\}^n, a \in \{0,1\}^k, b = f(v)\}$
- $f(v)$ can be written as

$$
\begin{aligned}
f(v) &= c \cdot a \oplus (1 \oplus c) \cdot b \text{ with } c \in \{0,1\} \\
&= c(a \oplus b) \oplus b
\end{aligned}
$$

A polynomial Time Attack on CKK^2 — Basic Idea

Collect a set of responses $O = \{(v_1||a_1||b_1), \ldots, (v_m||a_m||b_m)\}$.

Observations:

- Already for m slightly larger than n, $\{v_1, \ldots, v_m\}$ contains a basis of $\{0,1\}^n$ with high probability.
- With a basis $\{v_1, \ldots, v_n\}$ of $\{0,1\}^n$, any $v \in \{0,1\}^n$ can be written as $v = \bigoplus_{d \in D} v_d$ with $D \subseteq \{1, \ldots, n\}$, and

A polynomial Time Attack on CKK^2 — Basic Idea

Collect a set of responses $O = \{(v_1||a_1||b_1), \ldots, (v_m||a_m||b_m)\}$.

Observations:

- Already for m slightly larger than n, $\{v_1, \ldots, v_m\}$ contains a basis of $\{0,1\}^n$ with high probability.
- With a basis $\{v_1, \ldots, v_n\}$ of $\{0,1\}^n$, any $v \in \{0,1\}^n$ can be written as $v = \bigoplus_{d \in D} v_d$ with $D \subseteq \{1, \ldots, n\}$, and

$$\begin{aligned} f(v) &= c(a \oplus b) \oplus b \\ \Leftrightarrow \bigoplus_{d \in D} f(v_d) &= c(a \oplus b) \oplus b \\ \Leftrightarrow \bigoplus_{d \in D} (c_d(a_d \oplus b_d) \oplus b_d)) &= c(a \oplus b) \oplus b \\ \Leftrightarrow \bigoplus_{d \in D} (c_d(a_d \oplus b_d)) \oplus c(a \oplus b) &= \bigoplus_{d \in D} b_d \oplus b \end{aligned}$$

yields k equations in the unknowns $c_1, \ldots, c_n, c$.

A polynomial Time Attack on CKK[2]

repeat

Obtain a response $(v||a||b)$.

until a basis $\{v_1, \ldots, v_n\}$ of $\{0,1\}^n$ is found.

Initialize a system of linear equations LES in $c_1, c_2, \ldots$

A polynomial Time Attack on CKK[2]

repeat
  Obtain a response $(v||a||b)$.
until a basis $\{v_1, \dots, v_n\}$ of $\{0,1\}^n$ is found.
Initialize a system of linear equations LES in $c_1, c_2, \dots$
repeat
  Obtain a response $(v||a||b)$ with $v \notin \{v_1, \dots, v_n\}$.
  Add the k equations given by

$$\bigoplus_{d \in D} (c_d(a_d \oplus b_d)) \oplus c(a \oplus b) = \bigoplus_{d \in D} b_d \oplus b$$

  to LES.
until LES has full rank.

A polynomial Time Attack on CKK[2]

repeat
  Obtain a response $(v||a||b)$.
until a basis $\{v_1, \ldots, v_n\}$ of $\{0,1\}^n$ is found.
Initialize a system of linear equations LES in $c_1, c_2, \ldots$
repeat
  Obtain a response $(v||a||b)$ with $v \notin \{v_1, \ldots, v_n\}$.
  Add the k equations given by

$$\bigoplus_{d \in D} (c_d(a_d \oplus b_d)) \oplus c(a \oplus b) = \bigoplus_{d \in D} b_d \oplus b$$

  to LES.
until LES has full rank.
Compute the images of the basis vectors as

$$f(v_i) = c_i(a_i \oplus b_i) \oplus b_i \text{ for } i \in \{1, \ldots, n\} \ .$$

Recover f w.r.t. the standard basis of $\{0,1\}^n$.

Another polynomial Time Attack on CKK[2]

Let f be defined by the component functions $f^r : \{0,1\}^n \rightarrow \{0,1\}$, $r \in \{1,\ldots,k\}$, i.e., $f(v) = (f^1(v),\ldots,f^k(v))$.

Observation: If a response $(v||(a^1,\ldots,a^k)||(b^1,\ldots,b^k))$ satisfies $a^r = b^r$ for some r, then we know that $f^r(v) = a^r = b^r$.

Another polynomial Time Attack on CKK^2

Let f be defined by the component functions $f^r : \{0,1\}^n \to \{0,1\}$, $r \in \{1, \dots, k\}$, i.e., $f(v) = (f^1(v), \dots, f^k(v))$.

Observation: If a response $(v||(a^1, \dots, a^k)||(b^1, \dots, b^k))$ satisfies $a^r = b^r$ for some r, then we know that $f^r(v) = a^r = b^r$.

Idea: Recover the component functions separately.

for $r \in \{1, \dots, k\}$ **do**
  repeat
    Obtain a response $(v||(a^1, \dots, a^k)||(b^1, \dots, b^k))$ with $a^r = b^r$
  until a basis of $\{0,1\}^n$ is found.
  Recover f^r w.r.t. the standard basis.
end for

Performance of the CKK^2 Attacks

Main observations:

- The most costly operations are Gaussian eliminations.
- Rather few responses are needed to recover the secret function f
- A straightforward Magma implementation shows

	(n, k)	#responses	attack time
first attack	$(128, 30)$	≈ 140	≈ 0.05 s
	$(1024, 256)$	≈ 1039	≈ 2.95 s
second attack	$(128, 30)$	≈ 311	≈ 0.3 s
	$(1024, 256)$	≈ 2197	≈ 179 s

- $(n, k) = (128, 30)$ was suggested for practical application.

$\rightarrow$ Don't use CKK^2 in practice.

Attacks on general $(n, k, 2)$ Protocols

Verifier Alice RFID reader		**Prover** Bob RFID tag
	$\xrightarrow{\textit{challenge}}$	choose $l \in_R [L]$, $v \in_R \{0,1\}^n$
for $i := 1$ to L $(x\|\|y) := \sigma_l^{-1}(w)$ if $(y = f_l(x))$ accept reject	$\xleftarrow{w := \sigma_l(v\|\|f_l(v))}$	

Problems of the general $(n, k, 2)$ case:

- A single response $\sigma_1(v||f_1(v))$ does not say anything about $\sigma_2(v||f_2(v))$ and vice versa.
- The positions of dependent bits (=bits that belong to v) and independent bits (=bits that belong to $f(v)$) in a single response are unknown.

First Step: Attack on linear $(n, 1, 2)$ Protocols

Assume that $\sigma_1 = \sigma_2 = \mathrm{id}$ and consider a set of responses

$$O = \{(v_1||w_1), \ldots, (v_m||w_m)\} \text{ with } w_i \in \{0, 1\} \ .$$

For $x_i := f_1(v_i)$ and $y_i := f_2(v_i)$ it holds that

$$(w_i \oplus x_i)(w_i \oplus y_i) = 0 \text{ for all } i \in \{1, \ldots, n\} \ ,$$

which leads to quadratic equations in the unknowns x_i, y_i.

First Step: Attack on linear $(n, 1, 2)$ Protocols

Assume that $\sigma_1 = \sigma_2 = \mathrm{id}$ and consider a set of responses

$$O = \{(v_1||w_1), \ldots, (v_m||w_m)\} \text{ with } w_i \in \{0, 1\} \ .$$

For $x_i := f_1(v_i)$ and $y_i := f_2(v_i)$ it holds that

$$(w_i \oplus x_i)(w_i \oplus y_i) = 0 \text{ for all } i \in \{1, \ldots, n\} \ ,$$

which leads to quadratic equations in the unknowns x_i, y_i.

Observation: A symmetry-avoiding linearization allows to recover the secret functions f_1 and f_2 efficiently.

Performance for $n = 128$: Approx. 8390 responses and 4 minutes of computation

Extension to linear $(n, k, 2)$ Protocols

Basic ideas:

repeat

Guess a dependent position w.r.t. V_1 and V_2 and apply the $(n + k - 1, 1, 2)$ attack.

until $(n + k - 1, 1, 2)$ attack successful

Use the result to distinguish responses from V_1 and V_2.

Recover specifications for V_1 and V_2 from the respective responses.

More details in M. Krause and D. Stegemann: *Algebraic Attacks against Linear RFID Authentication Protocols*, Workshop Record of the Dagstuhl Seminar on Symmetric Cryptogaphy, 2009.

Future Work

- How to extend the attack ideas to efficient attacks for $L > 2$?
- What about active attacks against linear (n, k, L) protocols?
- How do linear (n, k, L) protocols (and their security properties) relate to the HB family of authentication protocols?
- ...

The End.

krause@th.informatik.uni-mannheim.de
dstegema@th.informatik.uni-mannheim.de