Matrix Games in Cryptography

Sven Laur
University of Tartu

swen@math.ut.ee

Motivation

Many proofs in cryptography can be reduced to matrix games.

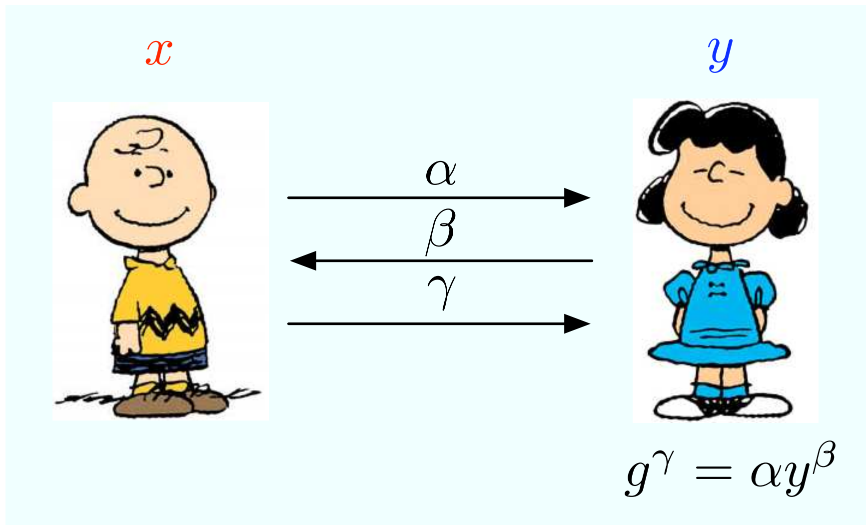
- ▷ Soundness analysis of sigma protocols
- ▷ Simulatability of zero-knowledge proofs
- ▷ White-box extractability of commitments
- ▷ Soundness and security of generic signatures
- ▷ Security of time-stamping schemes

$\Rightarrow$ Some matrix games are easier than others.

$\Rightarrow$ We explain what are the resulting limitations.

Simple Games

Sigma protocols for dummies



All sigma protocols satisfy the following conditions:

- ▷ The challenge message β is chosen uniformly from $\{0,1\}^k$.
- ▷ Given γ and β it is trivial to compute the corresponding α.
- ▷ Colliding valid triples $(\alpha, \beta_1, \gamma_1), (\alpha, \beta_2, \gamma_2), \beta_1 \neq \beta_2$ reveal the secret x.

Knowledge extraction

A priori it is not clear that a successful prover knows the secret x.

$\Rightarrow$ We have to extract some valid colliding triples $(\alpha, \beta_1, \gamma_1), (\alpha, \beta_2, \gamma_2)$.

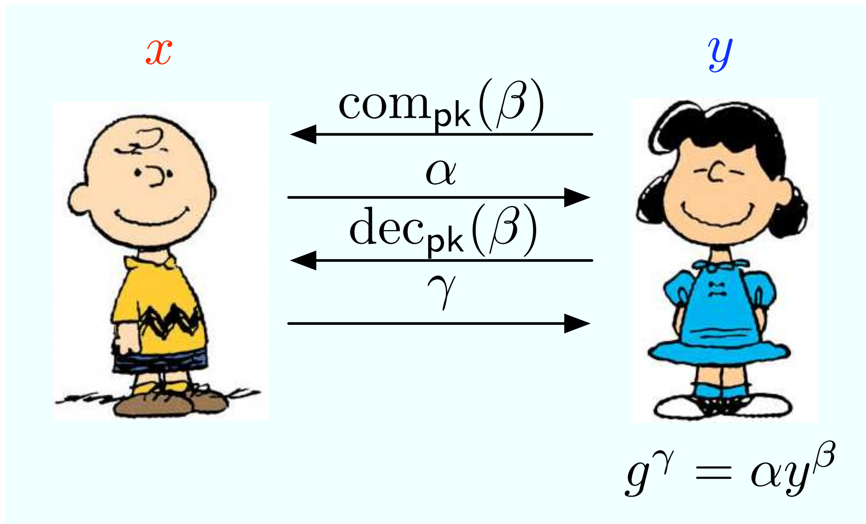
Matrix encoding

- ▷ Let ω denote the randomness of the prover
- ▷ Let ϕ denote the randomness of the verifier ($\phi = \beta$)
- ▷ Let $\mathsf{W}[\omega, \phi] = 1$ if the resulting protocol transcript was valid.
- ▷ Let $\mathsf{W}[\omega, \phi] = 0$ if the resulting protocol transcript was invalid.

Task. We have to find two ones in the same row.

- ▷ For theoretical reasons, the algorithm must work for all matrices.
- ▷ Natural random sampling algorithms run in expected time $\Theta(\frac{1}{\varepsilon})$.

Extractability and zero knowledge



If we guess the committed value β then it is easily compute $\alpha = \alpha(\beta, \gamma)$.

$\Rightarrow$ We need an extractor for commitment schemes

$\Rightarrow$ The latter is possible if the commitment scheme is binding.

Formal definition of binding

A commitment scheme is $(t, \varepsilon_{\mathrm{b}})$-binding if for any t-time adversary $\mathcal{A}$

$$\Pr\left[\begin{array}{l}\mathsf{pk} \leftarrow \mathsf{Gen} : (c, d_1, d_2) \leftarrow \mathcal{A}(\mathsf{pk}) : \\ \bot \neq \mathsf{Open}_{\mathsf{pk}}(c, d_1) \neq \mathsf{Open}_{\mathsf{pk}}(c, d_2) \neq \bot\end{array}\right] \leq \varepsilon_{\mathrm{b}} \enspace .$$

PROBLEM

- ▷ Formally, the definition does not provide a way to guess the committed value, since the adversary does not have to use the $\mathsf{Com}_{\mathsf{pk}}(\cdot)$ function.
- ▷ We have to extract $\beta \leftarrow \mathsf{Open}_{\mathsf{pk}}(c, d)$ by providing different values of α.

The corresponding matrix game

MATRIX ENCODING

- ▷ Let ϕ denote the randomness of the prover ($\phi = \alpha$).
- ▷ Let ω denote the randomness of the verifier and key generation.
- ▷ Let $\mathsf{W}[\omega, \phi] = \beta$ if the commitment opens to β.
- ▷ Let $\mathsf{W}[\omega, \phi] = 0$ if the opening of the commitment fails.

TASK. We have to predict a non-zero element for a given row ω.

SOLUTION.

⇒ It is sufficient to find a non-zero element in the row, as finding two different non-zero elements $\mathsf{W}[\omega, \phi_1] \neq \mathsf{W}[\omega, \phi_2]$ reveals *double opening*.

⇒ Sample ℓ elements from the row and return the first non-zero $\mathsf{W}[\omega, \phi_\star]$.

Analysis

- ▷ The simulation fails if extraction succeeds but does not match β. If the commitment scheme is $((\ell+1)t, \varepsilon_{\mathrm{b}})$-binding

$$\Pr[\mathsf{Fail}_1] = \Pr_{\omega,\phi}[\phi_\star \leftarrow \mathcal{K}(\omega) : 0 \neq \mathsf{W}[\omega,\phi] \neq \mathsf{W}[\omega,\phi_\star] \neq 0] \leq \varepsilon_{\mathrm{b}}$$

- ▷ The simulation fails if extraction fails but commitment is correctly opened

$$\Pr[\mathsf{Fail}_2] = \Pr_{\omega,\phi}[\mathcal{K}(\omega) = \perp \wedge \mathsf{W}[\omega,\phi] \neq 0] \quad .$$

- ▷ The latter can be reformulated as a pure combinatorial matrix game.
  - ◇ Find a matrix configuration $\mathsf{W}_\circ$ that maximises $\Pr[\mathsf{Fail}_2]$.

Combinatorial optimisation

Let ε denote the fraction of non-zero entries in the matrix and let ε_ω denote the fraction of non-zero entries in the row $\mathsf{W}[\omega, \star]$. Then we can express

$$\Pr[\mathsf{Fail}_2] = \Pr_{\omega,\phi}[\mathcal{K}(\omega) = \bot \wedge \neq \mathsf{W}[\omega,\phi]] = \mathop{\mathbf{E}}_{\omega}\left[\varepsilon_\omega(1-\varepsilon_\omega)^\ell\right] \quad .$$

Non-trivial observations.

- ▷ The failure probability decreases in the region $\varepsilon \in \left[\frac{1}{\ell+1}, 1\right]$.
- ▷ In the region $\varepsilon \in [0, \frac{1}{\ell+1}]$, we can establish a nice upper bound

$$\mathop{\mathbf{E}}_{\omega}\left[\varepsilon_\omega(1-\varepsilon_\omega)^\ell\right] \leq \varepsilon(1-\varepsilon)^\ell \leq \tfrac{1}{\ell+1} \quad .$$

Final result

Combining both bounds, we get a parametrised family of reductions

$$\Pr[\mathsf{Fail}] \leq \frac{1}{\ell + 1} + \varepsilon_{\mathrm{b}}(\ell t + t)$$

If we know the time-success profile of the commitment we can find the most optimal trade-off between failures probabilities $1/(\ell + 1)$ and $\varepsilon_{\mathrm{b}}(\ell t + t)$.

Alternative formulation

Find a predictor $\mathcal{K}$ that works well for all (random) inputs ϕ

$$\Pr\left[\mathsf{Fail}\right] = \max_{\phi}\left\{\Pr_{\omega}\left[w_\star \leftarrow \mathcal{K}(\omega) : 0 \neq \mathsf{W}[\omega,\phi] \neq w_\star\right]\right\}$$

There is a set of column indices $\Phi = \{\phi_1, \ldots, \phi_\ell\}$ such that

$$\max_{\phi}\left\{\Pr_{\omega}\left[\mathsf{W}[\omega,\phi] \neq 0 \wedge \mathsf{W}[\omega,\phi_1] = \ldots = \mathsf{W}[\omega,\phi_k] = 0\right]\right\} \leq \frac{1}{\ell}$$

As we can hardwire these column indices to $\mathcal{K}_{\mathcal{A}}$, we get a trade-off

$$\Pr\left[\mathsf{Fail}\right] \leq \frac{1}{\ell} + \varepsilon_{\mathrm{b}}(\ell t + t) \enspace .$$

Illustration

To find column indices Φ, pick columns that violate the premise.

▷ There can be at most ℓ of such columns.

0	1	0	0	1
1	1	1	0	0
1	0	1	0	0
0	1	1	1	0
0	0	1	1	1

0	1	0	0	1
1	0	0	0	0
1	0	0	0	0
0	1	1	1	0
0	0	1	1	1

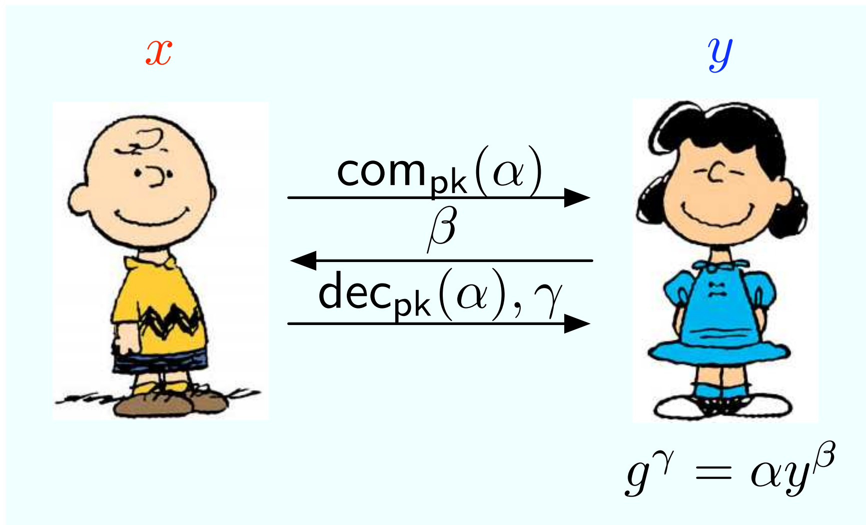
0	1	0	0	1
1	0	0	0	0
1	0	0	0	0
0	0	1	0	0
0	0	1	0	0

Difficult questions

- ▷ Both strategies give essentially the same trade-off formula. Is it possible to combine strategies to get better trade-off formula?
- ▷ Is it possible to use more efficient compact description for the locations of non-zero coefficients?
- ▷ For t-time algorithms only 2^{t+t} different matrix configurations are possible. Is it possible to construct more efficient extractors?

Difficult games

Equivocability and zero knowledge



We must open the commitment to $\hat{\alpha} = \alpha(\beta, \gamma)$ for bypassing checks.

$\Rightarrow$ We need an equivocator for commitment schemes.

$\Rightarrow$ The latter is possible only if the commitment scheme is hiding.

The corresponding matrix game

Assume that the commitment scheme is perfectly hiding and $\beta \in \{0, 1\}$.

MATRIX ENCODING

- ▷ Let ϕ denote the randomness of the verifier.
- ▷ Let $\omega = (\alpha, r, \gamma)$ denote the randomness of the naive simulator.
- ▷ Let $\mathsf{W}[\omega, \phi] = 1$ if the resulting protocol transcript was valid.
- ▷ Let $\mathsf{W}[\omega, \phi] = 0$ if the resulting protocol transcript was invalid.
- ▷ Then exactly half of the matrix entries are non-zeroes.

TASK. We have to uniformly sample non-zero entries in the matrix.

- ▷ For theoretical reasons, the algorithm must work for all matrices.
- ▷ Natural random sampling algorithms run in expected time $\Theta(2)$.

Scaling problem

In general, if $\beta \in \mathbb{Z}_k$ then we have to sample uniformly non-zero entries from the matrix that contains exactly $\frac{1}{k}$-fraction of nonzero entries.

- ▷ No general sampling algorithms can break the bound $\Theta(k)$.
- ▷ Since we have to sample all non-zero entries, we cannot use compact advice string to target the search.
- ▷ Is it possible to use the restrictions coming from the time-bound for limiting the number of possible search paths?

LOOPHOLE. For certain commitment schemes it is possible to find efficiently computable relation (equivocator) f_{sk} such that

$$(\alpha, r) = f_{\mathsf{sk}}(\gamma, \phi) \qquad \Longleftrightarrow \qquad \mathsf{W}[\omega, \phi] = 1 \enspace .$$

However, this is not a generally existing construction.

Conclusion

Equivocability is much stronger property than extractability.