On the Design and Implementation of Efficient Zero-Knowledge Proofs of Knowledge

SPEED-CC, Berlin (Germany), October 13th, 2009

Endre Bangerter[1], Stephan Krenn[1,2], Ahmad-Reza Sadeghi[3],
Thomas Schneider[3], and Joe-Kai Tsay[4]

[1] Bern University of Applied Sciences (Switzerland)
[2] University of Fribourg (Switzerland)
[3] Ruhr-University Bochum (Germany)
[4] Ecole Normale Supérieure de Cachan (France)

cace

Why to Avoid ZK-PoK in Hidden Order Groups

SPEED-CC, Berlin (Germany), October 13th, 2009

Endre Bangerter[1], Stephan Krenn[1,2], Ahmad-Reza Sadeghi[3],
Thomas Schneider[3], and Joe-Kai Tsay[4]

[1] Bern University of Applied Sciences (Switzerland)
[2] University of Fribourg (Switzerland)
[3] Ruhr-University Bochum (Germany)
[4] Ecole Normale Supérieure de Cachan (France)

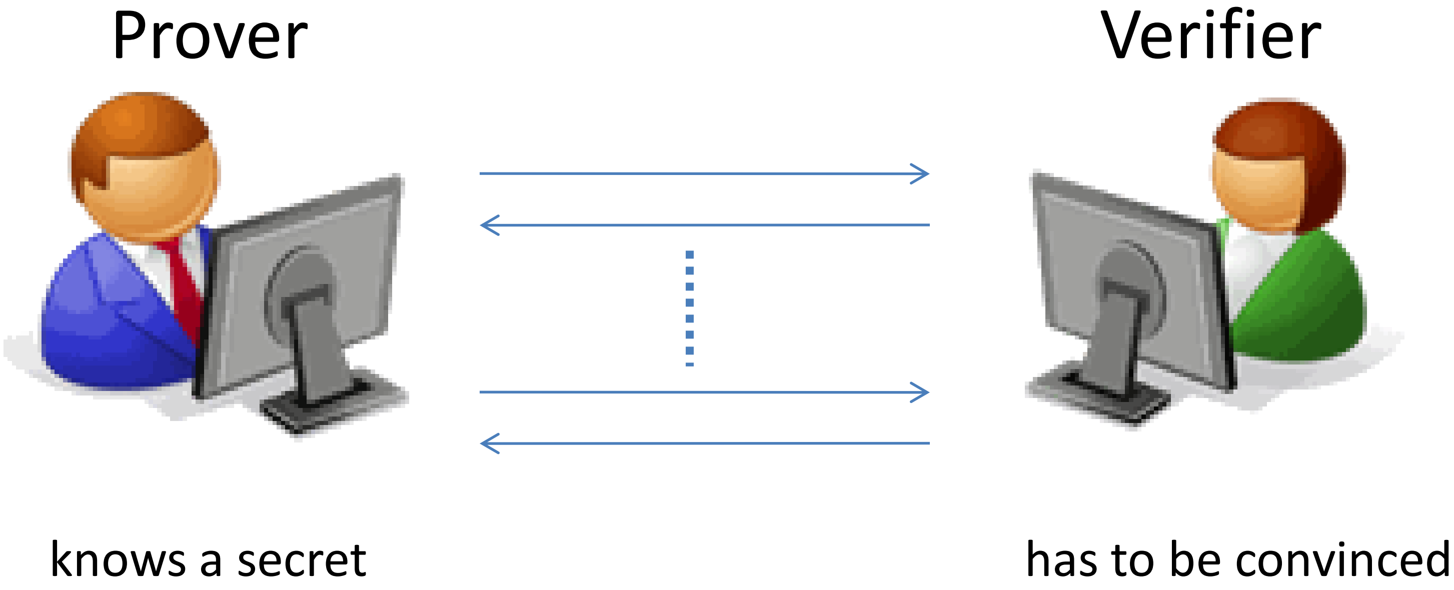
Outline

Proofs of knowledge in hidden order groups

Exact efficiency and security analysis

Conclusion

Introduction



Prover

knows a secret

Verifier

has to be convinced

Proof of Knowledge: Prover cannot cheat

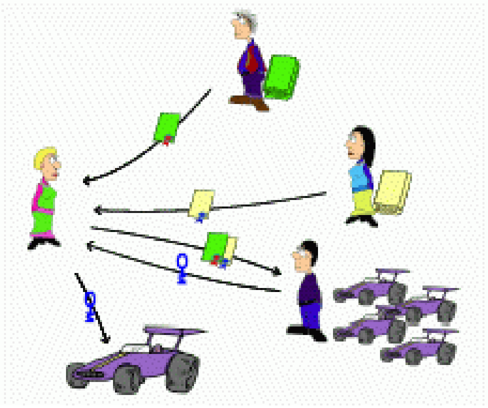
Zero-Knowledge: Verifier cannot learn secret

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

Applications

Remote Authentication

(e.g. DAA)



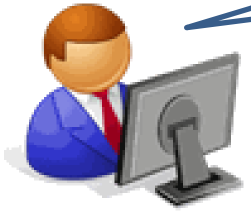
Credential Systems

(e.g. idemix)

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

The Schnorr Protocol

I know $x = \log_g y$.



$r \in_R \mathbb{Z}$

$t := g^r$ $\xrightarrow{\quad t \quad}$

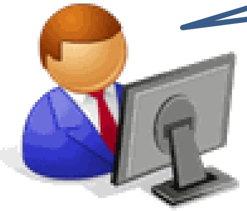
$\xleftarrow{\quad c \quad}$ $c \in_R C$

$s := r + cx$ $\xrightarrow{\quad s \quad}$ $g^s \overset{?}{=} t y^c$

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

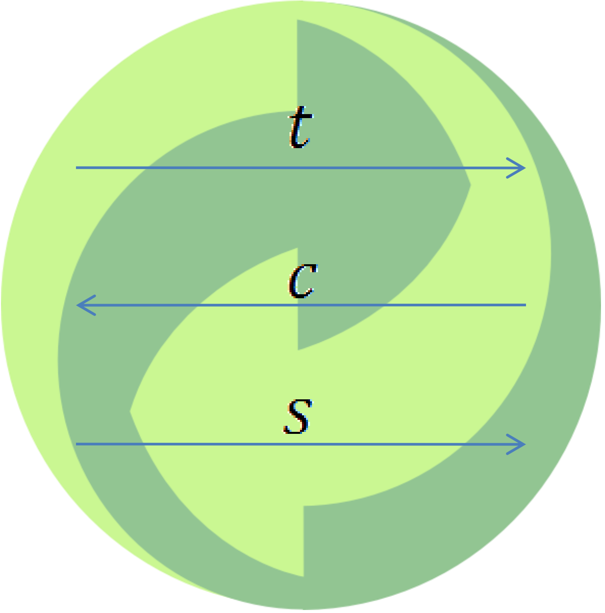
The Schnorr Protocol

I know $x = \log_g y$.



$r \in_R \mathbb{Z}$

$t := g^r$



$c \in_R C$

$s := r + cx$

$g^s \overset{?}{=} ty^c$

BUT: We must use $C = \{0,1\}$!

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

A Computationally Hard Problem

Given safe RSA modulus n, and $x, y \in_R \mathbb{Z}_n^*$,

cannot compute a, b, c, w such that $w^c = x^a y^b$ and ($c \nmid a$ or $c \nmid b$).

holds under: **Strong RSA Assumption**

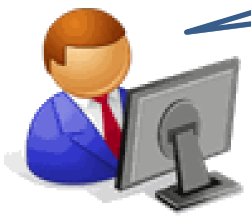
Given safe RSA modulus n, and $y \in_R \mathbb{Z}_n^*$,

cannot compute $a, e \neq 1$ such that $a^e = y$.

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

A Damgård/Fujisaki based Protocol

I know $x = \log_g y$.



$$r, \bar{r}, \bar{x} \in_R \mathbb{Z}$$
$$t := g^r$$
$$\bar{y} := \bar{h}_1^x \bar{h}^{\bar{x}}$$
$$\bar{t} := \bar{h}_1^r \bar{h}^{\bar{r}} \qquad \xrightarrow{t, \bar{t}, \bar{y}}$$

$$\xleftarrow{c} \qquad c \in_R C$$

$$s := r + cx$$
$$\bar{s} := \bar{r} + c\bar{x} \qquad \xrightarrow{s, \bar{s}} \qquad g^s \overset{?}{=} t y^c$$

$$\bar{h}_1^s \bar{h}^{\bar{s}} \overset{?}{=} \bar{t} \bar{y}^c$$

With large challenge set.

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

Why it works...

$g^{s_i} = ty^{c_i}$ $\qquad i = 1,2$ $\qquad \xrightarrow{\quad t \quad}$

➔ $g^{\Delta s} = y^{\Delta c}$ $\qquad \xleftarrow{\quad c \quad}$

➔ $x = \Delta s \, (\Delta c)^{-1}$ $\qquad \xrightarrow{\quad s \quad}$

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

Why it works...

$$g^{s_i} = ty^{c_i} \qquad i = 1,2$$

➔ $$g^{\Delta s} = y^{\Delta c}$$

➔ $$x = \Delta s\,(\Delta c)^{-1}$$

$$\xrightarrow{t,\bar{t},\bar{y}}$$

$$\xleftarrow{c}$$

$$\xrightarrow{s,\bar{s}}$$

$$\bar{h}_1^{s_i}\bar{h}^{\bar{s}_i} = \bar{t}\bar{y}^{c_i} \qquad i = 1,2$$

➔ $\bar{h}_1^{\Delta s}\bar{h}^{\Delta\bar{s}} = \bar{y}^{\Delta c}$ and $\Delta c \mid \Delta s$

➔ $$x = \frac{\Delta s}{\Delta c}$$

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

Outline

Proofs of knowledge in hidden order groups

Exact efficiency and security analysis

Conclusion

Intuitive Comparison

Schnorr protocol:

slow

looooong

DF-based protocol:

fast

elegant

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

A Closer Look

Common reference string

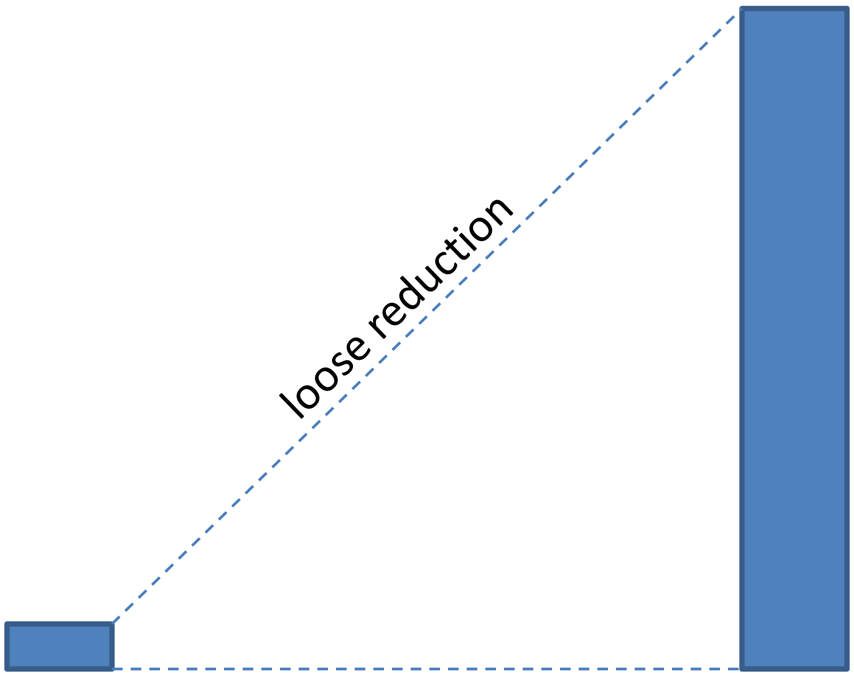
Only computationally sound

Bad complexity reductions

$\bar{y} := \bar{h}_1^x \bar{h}^{\bar{x}}$
$\bar{t} := \bar{h}_1^r \bar{h}^{\bar{r}}$

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

Bad Reductions



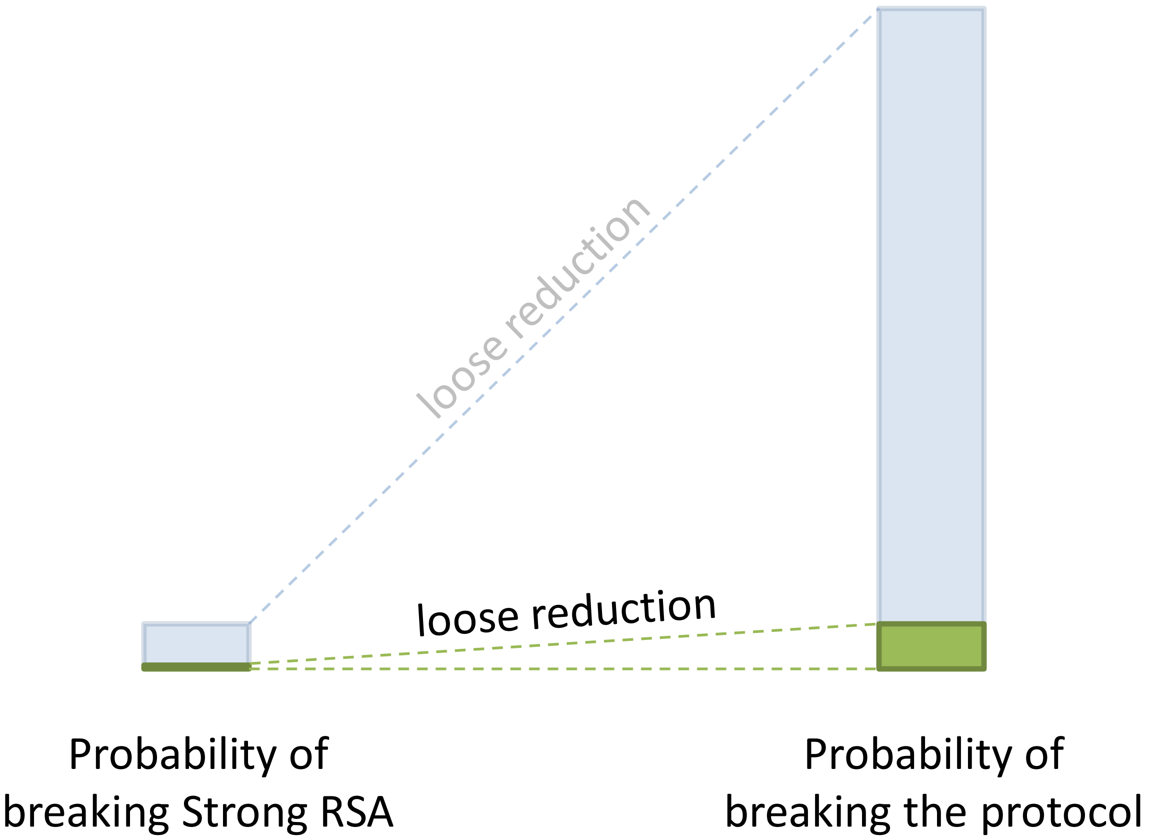
Probability of
breaking Strong RSA

Probability of
breaking the protocol

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

Is DAA broken?

Bad Reductions



loose reduction

loose reduction

Probability of
breaking Strong RSA

Probability of
breaking the protocol

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

Relative Costs

I know x, r, such that $y = g_1^{x^2} g_2^r$.

$$\frac{\text{Costs (Schnorr)}}{\text{Costs (DF-based)}}$$

for cheating probability of 2^{-80} and prover limited to 2^{80} steps.

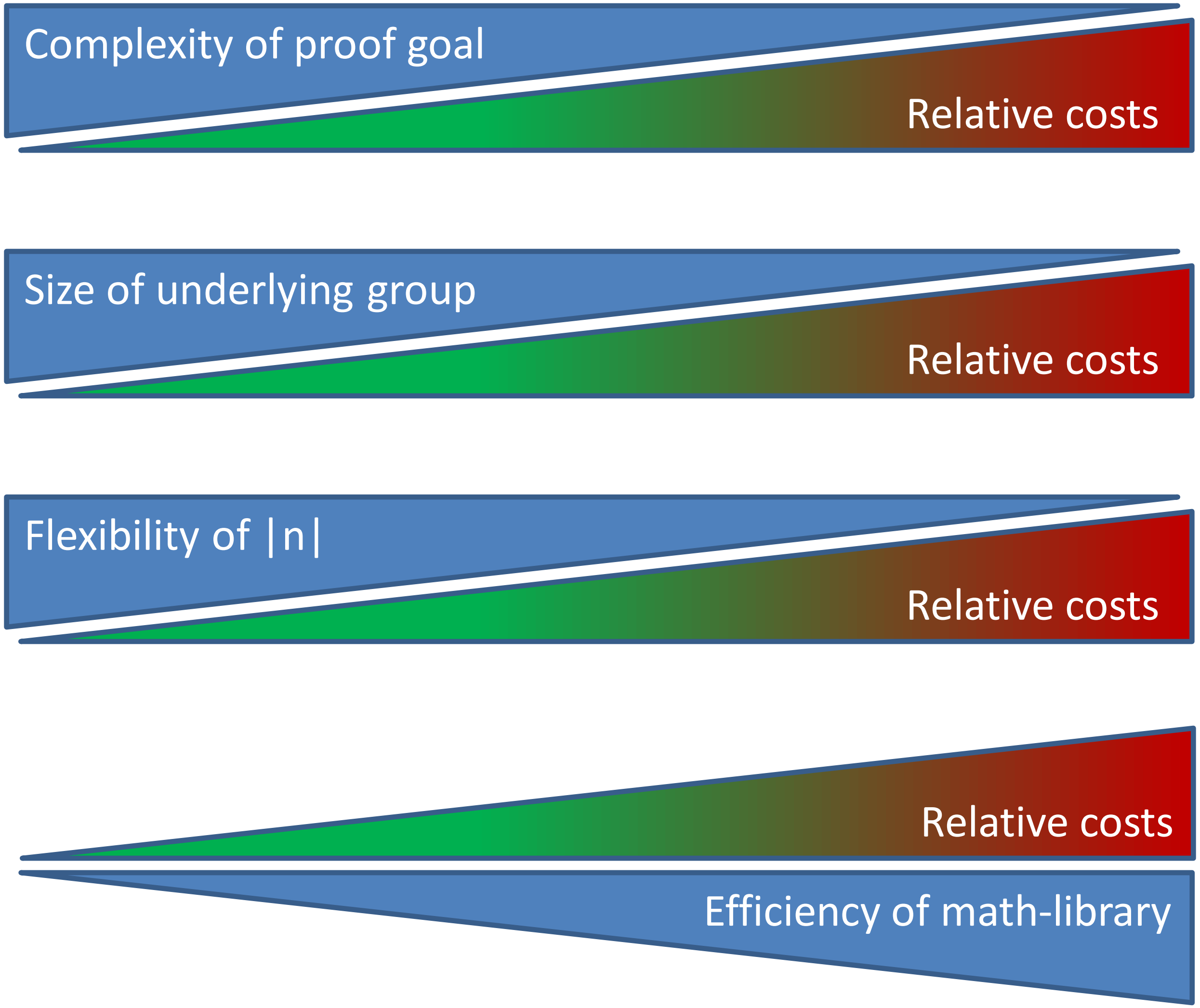
$\lvert n_0 \rvert$	$\lvert n \rvert$ = 15528	$\lvert n \rvert$ = 2048	optimal $\lvert n \rvert$
1024	42.7	2.7	1.9
1280	24.0	1.7	1.1
1536	13.1	1.0	0.7
2048	5.6	0.6	0.3

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

So…

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

Sources of Inefficiency



Complexity of proof goal

Relative costs

Size of underlying group

Relative costs

Flexibility of |n|

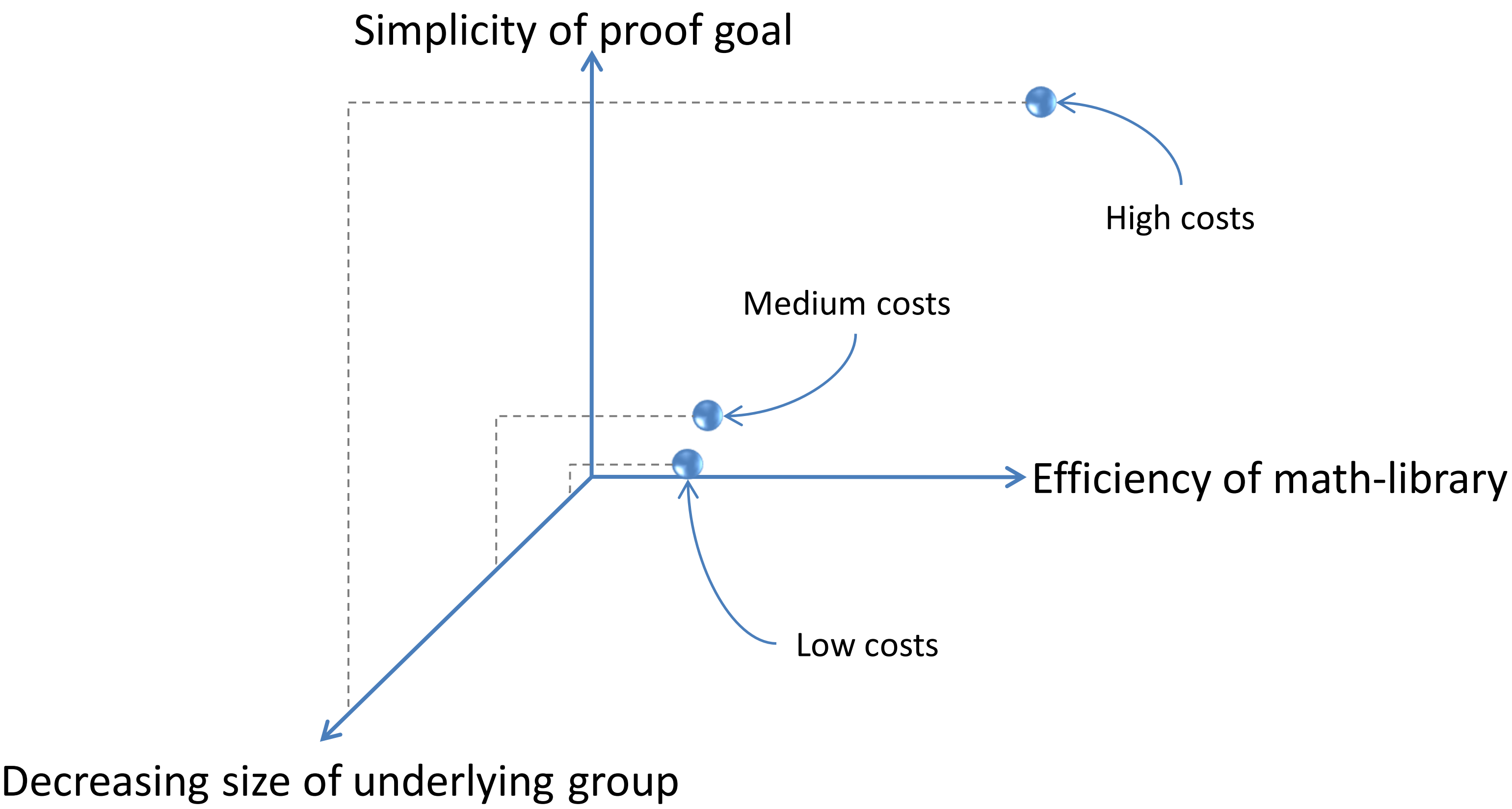
Relative costs

Relative costs

Efficiency of math-library

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

Dependencies of Relative Costs


Simplicity of proof goal
High costs
Medium costs
Efficiency of math-library
Low costs
Decreasing size of underlying group

Outline

Proofs of knowledge in hidden order groups

Exact efficiency and security analysis

Conclusion

Conclusion

Crypto folklore

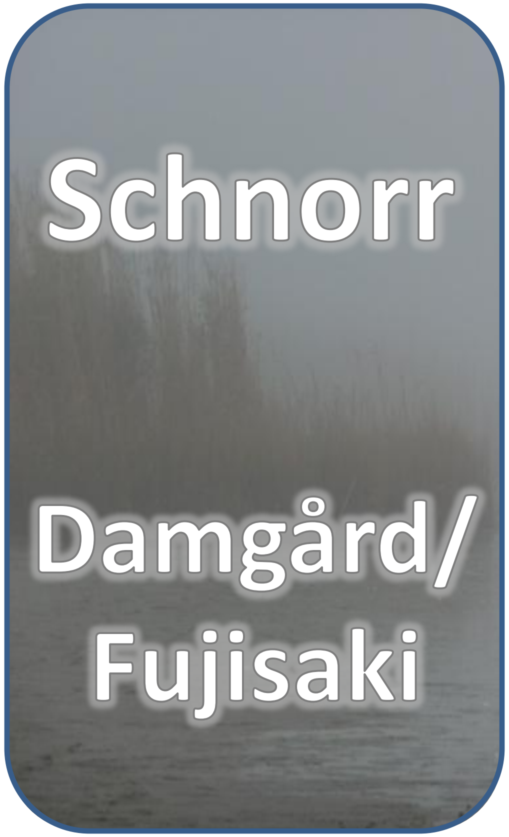
Design vs. implementation

RSA‘s legacy

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

Conclusion

Crypto folklore



Schnorr

Damgård/ Fujisaki

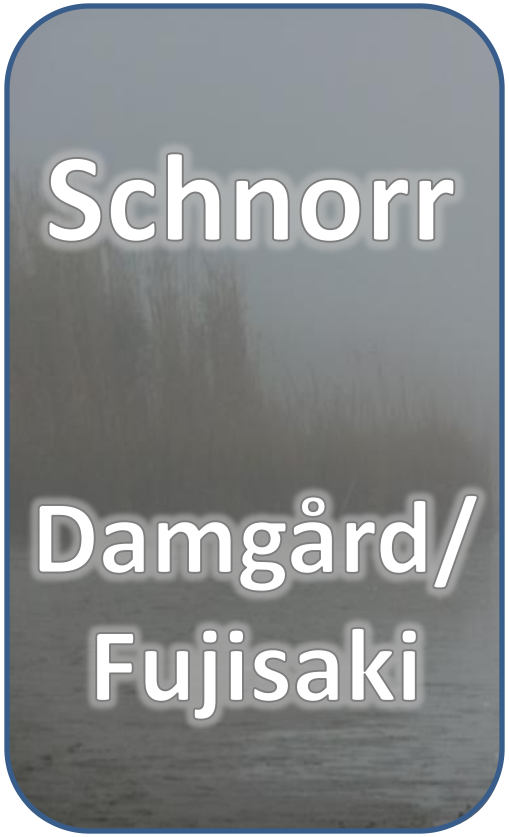
Design vs. implementation

RSA‘s legacy

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

Conclusion

Crypto folklore



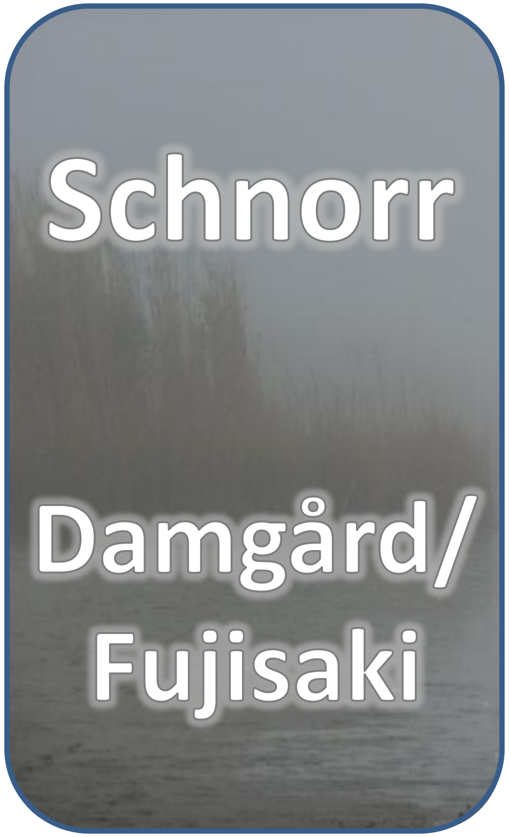
Design vs. implementation

RSA‘s legacy

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay

Conclusion

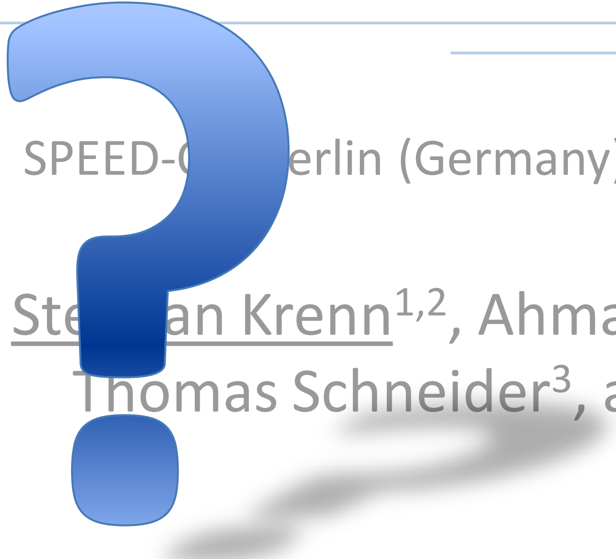
Crypto folklore



Design vs. implementation

RSA‘s legacy

On the Design and Implementation of Efficient Zero-Knowledge Proofs of Knowledge



SPEED-CC, Berlin (Germany), October 13th, 2009

Endre Bangerter[1], Stefan Krenn[1,2], Ahmad-Reza Sadeghi[3], Thomas Schneider[3], and Joe-Kai Tsay[4]

[1] Bern University of Applied Sciences (Switzerland)
[2] University of Fribourg (Switzerland)
[3] Ruhr-University Bochum (Germany)
[4] Ecole Normale Supérieure de Cachan (France)