

Coupon Recalculation for the Schnorr and GPS Identification Scheme: A Performance Evaluation

Christoph Nagl

`cnagl@sbox.tugraz.at`

Michael Hutter

`michael.hutter@iaik.tugraz.at`

IAIK - University of Technology Graz



RFIDSec 2009

Radio-Frequency Identification

Coupon Recalculation

EC Schnorr and ECGPS

Experimental Setup

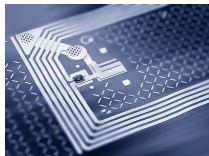
Deploying Schemes on RFID

Evaluation Results

Conclusions

Radio-Frequency Identification

- ▶ RFID tags become more and more established in everyday use where contactless identification is desired
 - ▶ supply chain management, inventory control, ...
- ▶ In general they consist of an integrated circuit (IC) that is attached to an antenna
- ▶ RFID-tag implementations are usually limited in chip area (costs), power consumption (reading range), and speed (some hundreds of kHz)



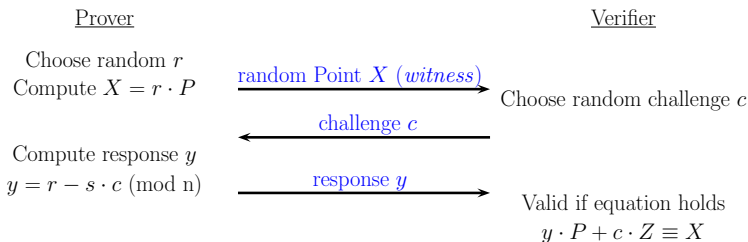
Cryptographic-Enabled RFID Tags

- ▶ State of the art
 - ▶ Identification of objects/entities
 - ▶ At most symmetric solutions using shared secrets (e.g. Mifare, CryptoRF, ..)
- ▶ Cryptography offers:
 - ▶ Counterfeit protection of goods
 - ▶ Access control
 - ▶ **Authentication instead of identification**

Asymmetric Cryptography on RFID Tags

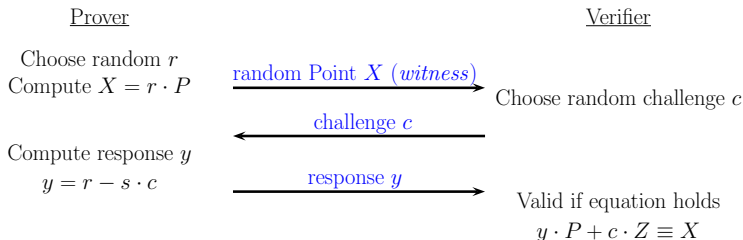
- ▶ Several ways to reach cryptographic services such as entity and message authentication
- ▶ Elliptic-curve cryptography (ECC) provides small key sizes with comparable security to other cryptographic primitives (e.g. RSA)
- ▶ Entity authentication through:
 - ▶ Signature schemes (e.g. ECDSA)
 - ▶ Identification schemes (e.g. Schnorr, GPS, Okamoto, ...)

Schnorr's Identification Scheme



- ▶ Introduced by C.P. Schnorr in 1989
- ▶ Three-way witness-challenge-response protocol
- ▶ Provides a zero-knowledge proof-of-knowledge
- ▶ Can be applied using ECC (ECSchnorr)

GPS Identification Scheme



- ▶ Proposed by Girault, Poupard, and Stern in 1991
- ▶ Based on Schnorr's identification scheme
- ▶ Leaves modular reduction in response-calculation step to save computation time / allows fast on-the-fly authentication
- ▶ A larger commitment and response is required to adequately hide the secret key s

- ▶ The elliptic-curve point multiplication is by far the most time consuming operation in this schemes.
→ Is there a way to circumvent long witness creation time?

- ▶ The elliptic-curve point multiplication is by far the most time consuming operation in this schemes.
→ Is there a way to circumvent long witness creation time?
Not really, but ..

Coupon Recalculation

- ▶ Witness creation is independent of external input
- ▶ Idea of pre-computing witnesses prior to actual authentication process.
 - ▶ Girault (Eurocrypt00), McLoone (CT-RSA07), Hofferek (Cardis08)
- ▶ Tuple of witness and commitment (X, r) can be stored on the tag as *coupon*
- ▶ DOS attack by extracting coupons is pointless if coupons can be recalculated by the tag itself *on-tag* (e.g. during idle time)
- ▶ Tags do not run out-of-operation and may be (re)used over long periods of time

Drawback: ECC operations on the tag need increased area, power and coupon-recalculation time.

Comparing the Schnorr and GPS Identification Scheme

- ▶ Schnorr scheme applies a modular reduction of modulus n
 - ▶ To compensate for the omitted reduction the GPS scheme introduces an additional factor of 2^{80} to the commitment
 - ▶ Commitment has advised order of $c \times s \times 2^{80}$
 - ▶ Large commitment size affects witness-creation time if witnesses are calculated on-tag
 - ▶ Commitment size also affects communication bandwidth
- $$y = r - c \cdot s$$

Description of our Test Setup

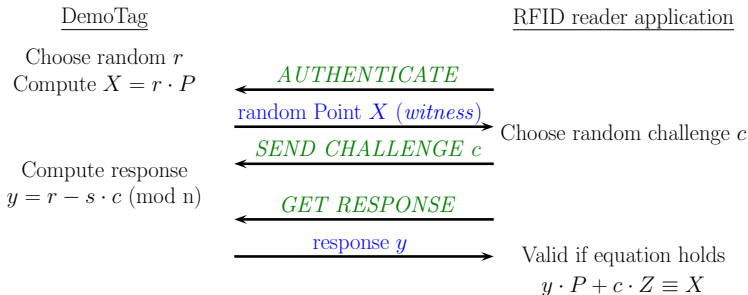
Implementation and evaluation of the coupon recalculation approach for ECSchnorr and ECGPS:

- ▶ Using elliptic curves over $GF(p_{192})$
- ▶ ATmega 128 platform programmed in ANSI C using Rowley Crossworks IDE for AVR
- ▶ IAIK DemoTag supporting several protocols such as ISO 14443-A, ISO 15693, and NFC
- ▶ Standard Multi-ISO RFID-Reader (controlled with Matlab/Maple)



Deploying Schemes on RFID

Slow tags can always use “*answer-on-demand*” approach (or use time-extension frame features of ISO 14443).



After Δt long enough for tag to compute challenge response, the reader polls the tag for the response.

Memory Usage

Static and dynamic memory consumption of ECSchnorr and ECGPS:

Project Item	ECSchnorr		ECGPS	
	Code [bytes]	Data [bytes]	Code [bytes]	Data [bytes]
ec_authentication.c	410	241	382	241
ec_arithmetic.c	1,824	289	1,824	289
finite_arithmetic.c	4,322	674	4,072	674
bitutils.c	320	24	320	24
main.c	1,152	628	1,152	659
Total memory usage	8,028	1,856	7,750	1,887

Computational Complexity (1)

Witness creation

GPS and Schnorr implemented on Demotag:

Operation	EC Schnorr	ECGPS
Single Point Addition [cycles]	561,863	561,863
Single Point Doubling [cycles]	560,604	560,604
Point Multiplication [cycles]	217,020,276	358,839,445
@13.56 MHz [seconds]	~16.0	~26.5
@1 MHz [seconds]	~217.0	~358.1

Both schemes use the same secret key and challenge

EC Schnorr performs multiplication with 192 bit scalar

ECGPS performs multiplication with 320 bit scalar

Computational Complexity (2)

Challenge-response calculation

Task	EC Schnorr	EC GPS
Witness creation [cycles]	217,020,276	358,839,445
Challenge-response calc. [cycles]	145,426	49,974

Composition of challenge-response calculation:

EC Schnorr: $MUL_{192 \times 48} + Reduction_{240 \rightarrow 192} + Mod_SUB_{192-192}$

EC GPS: $MUL_{192 \times 48} + SUB_{320-240}$

Computational Complexity (3)

Challenge-response calculation

Operation	Software [cycles]	Hardware estimates [cycles]
Modular Addition	1,296	26
Modular Subtraction	1,218	26
Modular Multiplication	144,330	936

Challenge-response computation time:

EC Schnorr: 962 cycles @13.56MHz \rightarrow 70.9 μ sec
 @3MHz \rightarrow 320.6 μ sec

Minimum frame delay of ISO 14443-A is 86 μ sec and of ISO 15693 is 320 μ sec.

Using *frame waiting time* (FWT) frame delay windows from about 300 μ sec up to about 5000 ms are possible

Communication Bandwidth

Transmission times

	EC Schnorr [ms]	ECGPS [ms]
Initialization and Anticollision	4.850	4.850
Witness transmission (192 bit)	2.311	2.311
Challenge transmission (48 bit)	0.578	0.578
Response transmission (24/40 byte)	2.311	3.851

Total identification time with EC Schnorr: 10 ms

Total identification time with ECGPS: 11.54 ms

Summary

- ▶ We focused on identification schemes in constrained environments implementing ECSchnorr and ECGPS
- ▶ Followed the approach of on-tag coupon recalculation
- ▶ Evaluation of our implementations
 - ▶ Memory size
 - ▶ Computational complexity
 - ▶ Communication bandwidth

Conclusions

- ▶ On-tag coupon recalculation provides an unlimited number of tag authentications
- ▶ When coupons are calculated on-tag EC Schnorr provides better performance

Thanks for your attention!

Contact: Christoph Nagl
cnagl@sbox.tugraz.at