Research Center for Information Security

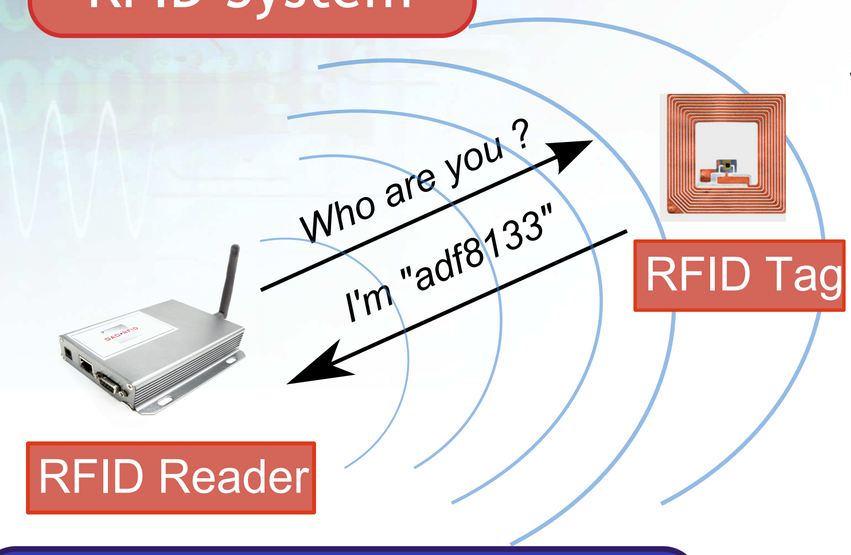
情報セキュリティ研究センター

Research Center for Information Security

Fast and Provably Secure Public Key Authentication for RFID Tags

Bagus Santoso

RFID System



Main Challenge: Resource vs. Security

Security Challenges:

* Impersonation, cloning, tracking & tracing, corruption DoS, side channel,etc.

Need public key for high security & privacy
(Vaudenay, ASIACRYPT 2007)

But : public key cryptography is **very expensive**, while....

Resource of RFID Tag:

*very small memory (~ 2 kb), very small circuit (~ 4k), very small power supply

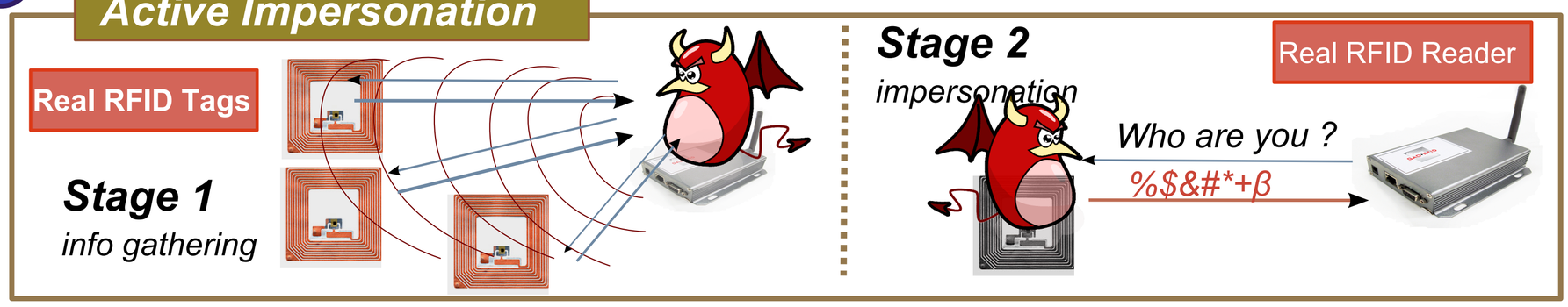
This Research's Target

Applications:

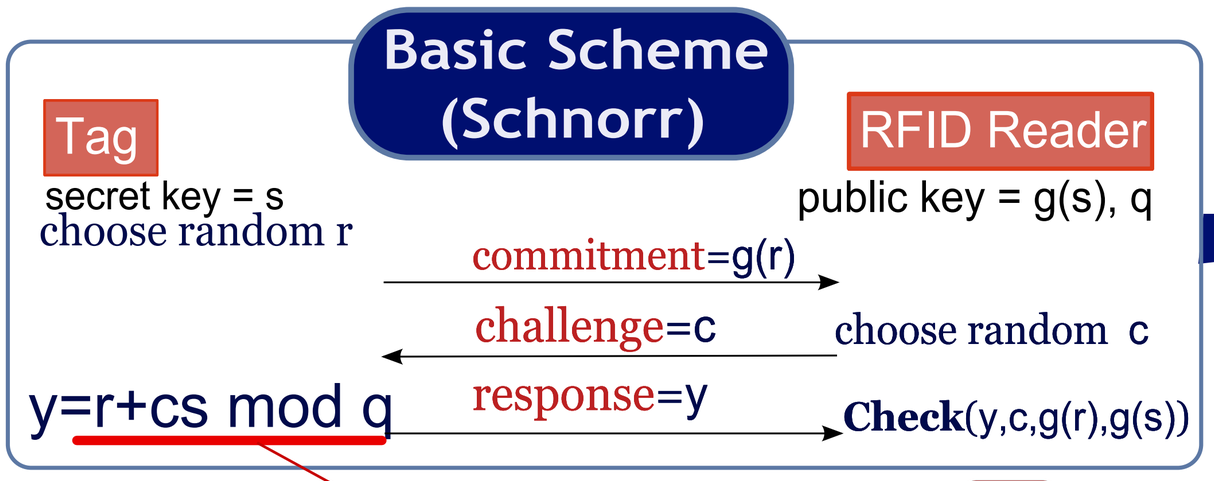
* mass transit systems (subway, ETC)
* fast genuineness checking (mass anti-piracy system)

Fast Tag Authentication Secure against Active Impersonation

Active Impersonation



Basic Scheme (Schnorr)



Too much Mask

Too Heavy for RFID Tag

No secret leakage

Girault-Poupard-Stern

y=r+cs mod q → y=r+cs

(WITHOUT Modulus No Mask AT ALL)

Very light

Secret may leak

Need very large r

Need very large memory

Too Open

Our New Scheme

Smart Masking

(1) set r in [0,A−1], c in [0,B−1], and s in [0,S−1] such that A mod q=0, BS<A.
(2) in response, if (r+cs)≧A, then y=r+cs−A, otherwise, y=r+cs.

Light enough for Tag

No secret leakage

No need very large r

No need very large memory

Performance Estimation on UMC 18nm 16-bit 100kHz w/ 80-bit offline security, 35 bit online security

		Gates (4.01 ms response calc.)	Memory Cost /use	Online Communication Cost	Total Response Time (1642 gates, 40kbps)
	AES	3595	—	—	10.16 ms
Public Key	Schnorr	5294 (too big for RFID Tag)	320 bits	160 bits	16.93 ms
Public Key	GPS	1642	435 bits	275 bits	10.89 ms
Public Key	New Scheme	**1970**	**355** bits	**195** bits	**9.65** ms

Bagus Santoso, Kazuo Ohta, Kazuo Sakiyama, and Goichiro Hanaoka,
"Improving Efficiency of An 'On the Fly' Identification Scheme by Perfecting Zero-Knowledgeness,"
In Proc. CT-RSA'10, LNCS 5985, Springer-Verlag, pp.284-301, March 2010.